

Privacy e trattamenti automatizzati dei dati personali nell'esperienza giuridica europea e statunitense: il nesso tra tecnica e diritto nella tutela della sfera privata della persona umana¹

di Luca Coppola²

INDICE

INTRODUZIONE

Tecnica, privacy, diritto: una "tendenza fondamentale"

CAPITOLO PRIMO

NASCITA DI UNA “COSTELLAZIONE”: LA COSTRUZIONE GIURIDICA DELLA PRIVACY NEGLI STATI UNITI D’AMERICA

Cenni introduttivi. Alle fonti della *privacy*: *oïkos*, società borghese, liberalismo umanitario

1.1. “*The Right to Privacy*”: sviluppo tecnologico e divenire del diritto

1.1.1. “*Subtler and more far reaching means of invading privacy*”: la *privacy-property* fino al
dissent del giudice Brandeis in *Olmstead v. United States*

1.1.2. Una parentesi: “*Law in the Making*”, dinamismo culturale e prospettive dottrinali sulla
privacy tra primo e secondo Novecento

1.1.3. “*Privacy as an aspect of human dignity*”: l’evoluzione della dottrina e della giurisprudenza
costituzionale fino ai casi *Griswold* e *Katz*

1.2. Elaboratori elettronici e “*individual control*”: l’*information privacy* nella legislazione
federale settoriale dagli anni Settanta ad oggi

¹ Menzione speciale del Premio Jo Cox 2025 per la migliore tesi di laurea su argomenti
concernenti le istituzioni o le politiche dell’Unione Europea.

² Facoltà di Giurisprudenza Sapienza Università di Roma. Relatore: Prof. Gianluca Scarchillo.
A.A. 2023-2024.

CAPITOLO SECONDO

BANCHE DATI E VITA PRIVATA: LA PRIVACY NELL'ORDINAMENTO INTERNAZIONALE E IN EUROPA. IL CONTESTO TECNOLOGICO DELLA DATA DRIVEN SOCIETY

2.1. Dalla CEDU alla Convenzione 108 sul trattamento automatizzato dei dati «a carattere personale»

2.2. Vita privata e società dell'informazione. Le Costituzioni europee del secondo dopoguerra

2.2.1. *Individualrechte, protection de la vie privée*, diritto al riserbo: le origini della “vita privata” in Europa

2.2.2. Riservatezza, banche dati, autodeterminazione informativa: la costruzione della *privacy* nella legislazione, nella giurisprudenza e nella dottrina degli ordinamenti nazionali del "Vecchio Continente". In particolare, uno sguardo all'Italia

2.2.3. Dalla Direttiva 95/46/CE al Trattato di Lisbona: il processo di “costituzionalizzazione europea” del diritto fondamentale alla protezione dei dati personali

2.2.4. L'approdo: il ruolo della Corte di Giustizia come “giudice dei diritti fondamentali”, il Pacchetto Protezione Dati e l'*EU-U.S. Data Privacy Framework*

2.3. *Big Data*, trattamenti algoritmici e Intelligenza Artificiale: alcuni concetti fondamentali nel contesto tecnologico della *data-driven society*

CAPITOLO TERZO

IL TRATTAMENTO AUTOMATIZZATO DEI DATI PERSONALI: LA DISCIPLINA EUROPEA

3.1. Contesto giuridico: il GDPR nel quadro dell'Agenda Digitale Europa

3.1.1. Il Regolamento Generale sulla Protezione dei Dati, tra tutela della persona fisica e sviluppo del Mercato Unico Digitale. Le motivazioni giuridiche

3.1.2. Ambito di applicazione, definizioni generali e principi di protezione dei dati: *risk-based approach* e autodeterminazione informativa

3.1.3. *Accountabilty, privacy by design e privacy by default*. I nuovi istituti del GDPR nella società delle ICTs

3.2. Il trattamento automatizzato dei dati personali: la disciplina del GDPR alla luce delle linee guida del Gruppo di Lavoro 29

3.2.1. Trattamento automatizzato, profilazione e processi decisionali automatizzati: definizioni essenziali

3.2.2. Le disposizioni generali: principi, basi giuridiche e diritti dell'interessato

3.2.3. Processi decisionali interamente automatizzati, compresa la profilazione: l'art. 22, par. 1 e i nodi interpretativi

3.2.4. Le eccezioni al divieto generale e le "misure appropriate" per tutelare i diritti dell'interessato. *Right to explanation*: essere o non essere?

3.2.5. La sentenza del 7 dicembre 2023 della Corte di Giustizia nel caso *SCHUFA* (e i suoi precedenti nazionali): il *leading case* europeo in materia di processi decisionali interamente automatizzati

3.3. Uno sguardo all'Italia. La trasparenza algoritmica nella giurisprudenza della Corte di Cassazione e del Consiglio di Stato

3.3.1. Orientamenti fondamentali del Garante per la Protezione dei Dati Personali in materia di trattamenti algoritmici: dal caso *Mevaluate* al provvedimento del 7 luglio 2022 in materia di pubblicità personalizzata nei confronti di *TikTok*

CAPITOLO QUARTO

DATA PRIVACY E AUTOMATED DECISION-MAKING SYSTEMS: LA DISCIPLINA STATUNITENSE

4.1. Il modello settoriale di *data privacy and protection law statunitense*, tra *technology dependence* e flusso transfrontaliero di dati. L'assenza di una legislazione federale unitaria

4.1.1. *Automated decision making systems*: sulle tracce di una disciplina frammentaria. I rilievi della Commissione Europea nelle decisioni di adeguatezza del *Privacy Shield* e del *Data Privacy Framework*

4.2. *Automated data processing* nei rapporti tra *Governement* e *Citizen*: la giurisprudenza della *Supreme Court* sul Quarto Emendamento nella società degli algoritmi. "*Is there any reasonable expectation of privacy in there*"?

4.2.1. *Electronic Communication Privacy Act*: le proposte della dottrina circa un divieto di monitoraggio automatizzato delle comunicazioni elettroniche

4.3. La disciplina federale degli *automated decision making systems* nei rapporti tra privati: *sector specific statutes* e *consumer protection*

4.3.1. ADM e *consumer credit system*: i regimi di *consumer disclosure* e di *adverse action notice* nel *Fair Credit Reporting Act* e nell'*Equal Credit Opportunity Act*

4.3.2. Discriminazione algoritmica ed *Equal Protection Laws*: in particolare, il Titolo VII del *Civil Rights Act* e il *Fair Housing Act*

4.3.3. La Sezione 5 del *Federal Trade Commission Act*: *unfairness, deception* e processi decisionali automatizzati

4.4. *California Consumer Privacy Act*: il modello giuridico di riferimento della legislazione statale in materia di *data privacy*. Un passo avanti: il recente *Draft for Automated Decisionmaking Technology Regulations*

CONCLUSIONI

Aprire la scatola nera: una "prospettiva fondamentale" per una società della dignità

BIBLIOGRAFIA

INTRODUZIONE

Tecnica, privacy, diritto: una “tendenza fondamentale”

«Gli strumenti di cui l'uomo dispone hanno la tendenza a trasformare la propria natura. Da mezzi tendono a diventare scopi. Oggi questo fenomeno ha raggiunto la sua forma più radicale. L'insieme degli strumenti delle società avanzate diventa lo scopo fondamentale di queste società. Nel senso che esse mirano soprattutto ad accrescere la potenza dei propri strumenti. Già gli antichi sapevano che se lo scopo della ricchezza è di vivere bene, può però anche accadere che come scopo della vita ci si proponga la ricchezza. In questo modo la ricchezza, che inizialmente funziona come mezzo, strumento, diventa scopo, fine»³.

Si intende aprire la presente trattazione con le imperiture parole di una delle più acute menti dell'età contemporanea per illuminare subito l'orizzonte culturale in cui si colloca il tema che ne costituisce oggetto: la comparazione tra le discipline del trattamento automatizzato dei dati personali vigenti, rispettivamente, nel contesto ordinamentale statunitense e in quello, in senso lato, europeo. Comparazione, tuttavia, che ci si propone di svolgere a partire da un

³ E. SEVERINO, *La tendenza fondamentale del nostro tempo*, Adelphi, Milano 1988, p. 38.

punto di vista preciso, che costituisce insieme anche l'obiettivo dell'indagine condotta e, in definitiva, la tesi che in questo lavoro si sostiene.

La prospettiva in questione consiste nell'evidenziare il filo conduttore che, a parere di chi scrive, unisce tutto il discorso filosofico, antropologico e infine giuridico sviluppatosi intorno al concetto di *privacy*: il nesso indissolubile, reciproco, plurivoco che intercorre tra sviluppo tecnologico, trasformazioni sociali ed evoluzione del diritto in punto di protezione della *sfera privata* della persona umana. A tale scopo, si è deciso di assumere come punto di partenza la descrizione del composito istituto della *privacy*, a cominciare dalla sua nascita *in senso giuridico* e dalle principali e distinte linee evolutive da esso seguite nei diversi ordinamenti considerati, offrendo così un dettagliato quadro della dottrina, della giurisprudenza e della legislazione succedutesi nel Nuovo e nel Vecchio Continente in materia di "riservatezza". Ciò, in prima battuta, allo scopo di sottolineare come il nesso suddetto sia consustanziale all'istituto in parola, e pertanto lo animi sin dai suoi "albori giuridici"⁴. Compiuto tale affresco, ci si sposterà su un piano maggiormente specialistico, e dunque ci si addentrerà nell'analisi della disciplina oggi vigente nelle suddette distinte e caleidoscopiche esperienze giuridiche in relazione al fenomeno che rappresenta il prodotto più emblematico della rivoluzione prima informatica e successivamente digitale occorsa dalla seconda metà del Novecento e tutt'ora in pieno rigoglio: l'elaborazione per mezzo dell'*automazione*, ed oggi principalmente *algoritmica*, dei dati personali⁵. La principale ragione per cui si è scelto di focalizzare

⁴ La ricerca in questione occuperà il cap. 1, per quanto attiene agli Stati Uniti d'America, e il cap. 2, per quanto attiene all'ordinamento internazionale, a quello comunitario e all'esperienza di alcuni dei suoi Stati membri, con particolare riguardo all'Italia. Un ultimo, denso paragrafo (par. 2.3) sarà dedicato all'analisi del contesto tecnologico, e parimenti epistemologico, di riferimento, indispensabile per avere chiara la cornice in cui si iscrive il fenomeno dell'*automated data processing* e cogliere la *ratio* della sua disciplina.

⁵ L'analisi di dettaglio della disciplina dei trattamenti automatizzati occuperà tutto il cap. 3 (per quanto riguarda l'Europa, e nel suo contesto essenzialmente il livello eurounitario; un dettagliato sguardo conclusivo sarà dedicato poi alla giurisprudenza e alle decisioni del

l'attenzione su tale fenomeno risiede nel fatto che esso, nella contemporaneità, sembra costituire la più cristallina espressione del rapporto tra innovazione tecnologica e crescente vulnerabilità della sfera privata dell'individuo. Rapporto, peraltro, che della disciplina del fenomeno in questione permea anche la *ratio*: come vedremo, interrogarsi sullo *stato del diritto* in materia vuol dire interrogarsi sullo *stato dei diritti fondamentali* nel nostro tempo.

Alcune, ulteriori seppur sintetiche considerazioni introduttive possono essere utili per illuminare la prospettiva teorica che orienta il presente lavoro.

Come si cercherà di dimostrare nelle seguenti pagine, è dall'incessante trasformazione della tecnica e dal suo progressivo affinamento che scaturiscono nel corpo sociale bisogni sempre nuovi di tutela: dai beni materiali al corpo fisico, fino alla "dimensione spirituale" dell'essere umano. E ciò vale altrettanto, anzi soprattutto, nell'ambito in cui si muove il presente lavoro, perché nel corso della storia si sono moltiplicate le invenzioni di «*subtler and more far reaching means of invading privacy*»⁶, a causa delle quali sempre maggiori sono le zone dell'intimità dell'individuo esposte all'intelligenza della scienza, e per suo tramite a quella del pubblico. I bisogni che ne derivano, nel nostro presente connotato dal dominio ontologico della tecnica e dall'affermazione di quello che è stato efficacemente definito un «autonomo ordine sociale e giuridico delle macchine», hanno raggiunto proporzioni e insieme declinazioni inimmaginabili agli inizi dello scorso secolo⁷. Se è vero, infatti, che l'identità di una persona deve essere

Garante della Privacy in materia nell'ordinamento italiano), e tutto il cap. 4 (per quanto riguarda gli Stati Uniti, con un'attenzione particolare riservata al livello federale, mentre a livello statale sarà preso in esame il "modello giuridico di riferimento", rappresentato dal California Consumer Privacy Act (CCPA)).

⁶ La citazione, lungimirante, è di L. BRANDEIS, «Dissenting Opinion», in *Olmstead v. United States*, 277, U. S., p. 473, su cui v. *infra* par. 1.1.2.

⁷ Sul dominio della tecnica come carattere originale del nostro tempo, è d'obbligo il riferimento a M. HEIDEGGER, *Saggi e discorsi*, Milano 1991, p. 19 ss.; sul nuovo ordine socio-

intesa come «processo», come frutto di una sintesi tra le «maschere informazionali» che questa dissemina nei più disparati contesti interazionali, oggi per lo più *virtuali*; e se è altrettanto vero che nella contemporaneità i dati di cui si compongono tali «maschere» sono oggetto di raccolta e di analisi incrociata pressoché costante da parte delle *macchine intelligenti*, che li utilizzano per adottare decisioni, anche sensibili, riguardanti la persona stessa; risulta allora evidente l'esistenza del pericolo che la tecnica si sostituisca all'uomo nella «costruzione della [sua] identità individuale e sociale»⁸. Di conseguenza, si delinea la fisionomia di una nuova, inedita esigenza: quella di conservare in capo all'individuo la sovranità sul proprio «corpo elettronico» (da intendersi, oggi, principalmente come eterogenea moltitudine di *bit* informatici), di cui quello fisico è solo il substrato materiale; e, attraverso di essa, la libertà di autodeterminarsi nella costruzione e nella proiezione esterna della propria personalità⁹.

Di fronte a questo fenomeno, a questa vera e propria “mutazione antropologica”, le capacità del diritto di governare il conflitto sociale sono state, e continuano ad essere, sempre più interrogate. Ma proprio il tentativo indefesso del diritto quale perfettibile, indispensabile scienza sociale di offrire un'adeguata risposta ai suddetti, crescenti e sempre più complessi bisogni ha rappresentato il motore dell'evoluzione che andremo descrivendo nei seguenti capitoli. E continua, ancora, a rappresentarlo, se si guarda all'acceso dibattito che circonda

giuridico basato sull'autonomia delle macchine, cfr. S. RODOTÀ, *Il diritto di avere diritti*, Editori Laterza, Roma-Bari 2015, p. 323 ss.

⁸ Rilevi che saranno più ampiamente sviluppati nel prosieguo della trattazione, v. *infra* par. 3. Per le considerazioni qui svolte, si rinvia subito a S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Roma Bari 2004, in particolare p. 139 ss.; ID., *Il diritto di avere diritti*, cit., in particolare p. 402.

⁹ Allo stesso modo di cui alla nota precedente, cfr. S. RODOTÀ, *Tecnopolitica*, cit., p. 141; ID., *Riservatezza*, cit., p. 100-101; G. MARINI, «Diritto alla privacy», in *Commentario del Codice Civile*, (diretto da) E. GABRIELLI, UTET, Milano, 2013, pp. 207-208; G. RESTA, «Identità personale e identità digitale», in *Dir. Inform.*, 2007, III, p. 524 ss.

l'interpretazione delle attuali disposizioni del *General Data Protection Regulation* (GDPR) in materia di processi decisionali *interamente* automatizzati (profilo della *data protection* la cui problematicità è emersa prepotentemente negli ultimi vent'anni), e alle molteplici soluzioni applicative cui tale dialettica dà origine, nel senso del potenziamento o piuttosto del detrimento della tutela apprestata in favore di quel "prisma" che è la persona umana¹⁰.

In poche parole, si intende dire che l'evoluzione del concetto di *privacy* è legata a doppio filo all'evoluzione della tecnica: se la prima reagisce, per sopravvivere, al divenire della seconda, esprimendo nuove e più complesse dimensioni, quest'ultima, confrontandosi con i presidi apprestati alla sfera privata, si trasforma a sua volta, assurgendo a strumento (o, appunto, ad autonomo *agente*) capace di invadere o piuttosto di salvaguardare più efficacemente l'intimità "cinta" dal diritto¹¹.

Alla luce del quadro sinteticamente delineato, si può in conclusione affermare che, nel valorizzare l'esistenza del nesso tra tecnica, *privacy* e diritto come *tendenza fondamentale*, il fine ultimo del presente lavoro risulta quello di scandagliare l'idoneità della disciplina vigente a regolare gli usi potenzialmente distorti della tecnologia nel trattamento dei dati personali, e conseguentemente a scongiurarne i riflessi pregiudizievoli sulla capacità della *persona interessata* di autodeterminarsi nelle scelte relative alla propria esistenza. Idoneità, in definitiva,

¹⁰ Vedi ampiamente *infra*, cap. 2.

¹¹ Per quanto riguarda i possibili scenari di implementazione della tecnica *pro privacy* cfr. le interessanti considerazioni rilasciate da M. RASETTI (*Institute for Scientific Interchange* di Torino) in un'intervista su *Capital*, n. 341 del marzo 2016, 18 e ss: ««Usati grosso modo al contrario, gli algoritmi creano metodi di anonimizzazione dell'informazione a prova di bomba. Per questo, però, ci vogliono delle leggi che abbiano la volontà e la capacità di proteggere la nostra privacy»; il passo è riportato nella versione qui citata da S. CALZOLAIO, «Protezione dei dati personali», in *Dig. disc. pubbl., Agg.*, (a cura di) R. SACCO, Milano, 2017, p. 608. Sulla dialettica tra c.d. *privacy enhancing* e *privacy invading technologies*, cfr. già da ora D'ACQUISTO G., DOMINGO-FERRER J., KIKIRAS P., TORRA V., DE MONTYOJE Y.A., BOURKA A., *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, European Union Agency for Network and Information Security, dicembre 2015

a conservare in capo alla tecnologia, alla macchina, lo status di *strumento*, non già di *scopo* dell'agire umano. In questo senso, possiamo dire che nell'osservare il rapporto tra persona umana e tecnica, ed il diritto stesso nel suo tentativo di governare il complesso conflitto di interessi che tale rapporto circonda, aderiremo ad una *visione personalistica*, o anche *antropocentrica*¹².

A orientare il percorso, come bussola, interviene allora un fondamentale dilemma: è ancora la disciplina della *privacy*, e in particolare la disciplina di quella sua dimensione dinamica che, come vedremo, trova oggi espressione nelle formule *informational privacy* (in contesto nordamericano) ed autodeterminazione informativa (in contesto europeo), in grado di concorrere alla costruzione di una «*società della dignità*»¹³ di fronte alla nuova morfologia algoritmica, quasi *soggettiva*, e certamente transnazionale della tecnica?

A questo interrogativo, lo anticipiamo, non può darsi una risposta definitiva, né il presente lavoro coltiva l'ambizione di farlo. E esso, piuttosto, intende *porsi* la domanda, fondamentale, in questione. E individuare un ventaglio

¹² Una precisazione terminologica. Nel corso della trattazione, quando faremo riferimento alla visione (o alla prospettiva, o all'approccio) in questione, il termine *antropocentrico* sarà utilizzato essenzialmente come sinonimo di *umanitario*, e dunque nell'accezione più vicina al significato principale del sostantivo greco *ánthropos*: nel senso, dunque di "uomo al centro", e allora di promozione della *persona umana* quale *valore* insieme *presupposto* e *fine* del discorso e dell'agire giuridico. La visione in parola, insomma, saldamente riposa sul *principio personalista* sancito dall'art. 2 della Costituzione Italiana. Per un'analisi sulla promozione della prospettiva suddetta nel contesto eurounitario, quanto meno in punto di *privacy*, cfr. da subito M. BASSINI, «La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali», in *Quad. cost.*, 2016; F. BRAVO (a cura di), *Dati Personali. Protezione, libera circolazione e governance. Vol. 1: i principi*, Pacini Giuridica, p. 23 ss. Per più approfondite considerazioni, v. cap. 2., parr. 2, 2.2 e ss.; e cap. 3, par. 1.1. Sul punto, in ogni caso, si tornerà spesso.

¹³ L'espressione, a suo modo divenuta celebre, così come l'intervento da cui è tratta, è di S. RODOTÀ, *Privacy, libertà, dignità*, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati del 16 settembre 2004, Wroclaw, Polonia, 2004. Ci troveremo ad utilizzarla spesso nel corso della trattazione. Per ulteriori riflessioni svolte dall'illustre autore sul concetto di dignità (sul quale torneremo altrettanto spesso, individuando nella *privacy* un suo *aspetto essenziale*), quale principio fondante «l'antropologia moderna della persona», cfr. anche ID., *Il diritto di avere diritti*, cit., p. 179 ss.

di risposte possibili, a seconda delle diverse soluzioni esegetiche adottate nel quadro dei *formanti giuridici* scandagliati¹⁴. Manifestando, al più, un'educata preferenza per quelle che paiano riflettere l'impostazione assiologica che abbiamo poc'anzi descritto.

Per farlo, indispensabile sarà procedere con l'affresco storico che tenterà di evidenziare l'esistenza della suddetta biunivoca corrispondenza sin dalle fonti *giuridiche* dell'istituto in esame, nonché le sue diverse declinazioni nei contesti ordinamentali considerati. Solo a quel punto, muniti di una maggiore consapevolezza delle ragioni che hanno condotto alla loro elaborazione, si affronterà nel merito la rispettiva disciplina dei trattamenti automatizzati dei dati personali: con indosso le lenti del comparatista, che nel confine, geografico, assiologico o giuridico che sia, non vedono mai un *limes*, bensì riconoscono un *limen*.

Non un limite, non una frontiera fortificata; bensì una linea da oltrepassare, la soglia di un nuovo orizzonte culturale che invita a proiettarvi la propria sensibilità.

Una nuova *domus*. Intanto, e soprattutto, per i diritti.

¹⁴ Sulla teoria dei formanti (o *legal formants*) intesi, secondo un approccio strutturalista e in conseguenza dell'applicazione di tale metodologia al diritto comparato, quali strutture o insiemi omogenei di "componenti giuridiche interrelate" alla base di qualsiasi fenomeno giuridico (e qui essenzialmente riferite all'ordinamento nel suo complesso, e pertanto suddivisibili in formante *giurisprudenziale*, *legislativo* e *dottrinale*), immediato e d'obbligo è il riferimento al suo illustre padre, R. SACCO, *Introduzione al diritto comparato*, UTET, 1992, passim.

CAPITOLO PRIMO

NASCITA DI UNA “COSTELLAZIONE”: LA COSTRUZIONE GIURIDICA DELLA PRIVACY NEGLI STATI UNITI D’AMERICA

SOMMARIO: Cenni introduttivi - 1.1. “The Right to Privacy”: sviluppo tecnologico e divenire del diritto. – 1.1.1. “Subtler and more far reaching means of invading privacy”: la privacy-property fino al dissent del giudice Brandeis in Olmstead v. United States – 1.1.2. Una parentesi: “Law in the Making”, dinamismo culturale e prospettive dottrinali sulla privacy tra primo e secondo Novecento – 1.1.3. “Privacy as an aspect of human dignity”: l’evoluzione della dottrina e della giurisprudenza costituzionale fino ai casi Griswold e Katz – 1.2. Elaboratori elettronici e “individual control”: l’information privacy nella legislazione federale settoriale dagli anni Settanta ad oggi

Cenni introduttivi. Alle fonti della *privacy*: *oikos*, società borghese, liberalismo umanitario

Privacy è concetto tanto evocativo quanto sfuggente. Attestato come esistente nella lingua inglese, in senso generico, già a partire dal 1450, ha assunto un proprio autonomo significato giuridico nell’ambito della tradizione giuridica occidentale solo sul finire del diciannovesimo secolo, come a breve vedremo nel dettaglio¹⁵. Tuttavia, la sua duttilità e la sua *vis* espansiva sono testimoniate dalla circostanza che esso, in poco più di un secolo di vita “istituzionale”, si è arricchito (e continua ad arricchirsi) di significati giuridici complementari e insieme

¹⁵ Il riferimento è, ovviamente, a S. WARREN, L. BRANDEIS, «The Right to Privacy», in *Harvard Law Review*, 1890, vol. V, n. 5, pp. 193-220, su cui vedi ampiamente *infra*.

trascendenti rispetto a quello originariamente attribuitogli dai suoi “padri fondatori”; significati che, a fronte dell’incessante progresso tecnologico che la civiltà occidentale ha conosciuto specialmente dalla seconda rivoluzione industriale in poi, gli hanno progressivamente consentito di rispondere a nuove istanze di tutela, relative ad aspetti dell’*intimità* individuale diversi dal solo interesse negativo ad “essere lasciati indisturbati”.

Questa graduale, crescente polisemia è solo in parte rispecchiata dalle diverse formule adottate dalla lingua italiana per tradurre, nel gergo comune, il vocabolo in questione: per citarne solo alcuni, *privatezza*, *riservatezza*, *vita privata*. E se il primo rappresenta una mera italianizzazione del lemma anglosassone, gli ultimi due identificano concetti che nel nostro ordinamento assumono un proprio significato giuridico: concetti, tuttavia, che del *valore* in esame sembrano rendere, rispettivamente, solo alcune sfumature. Non è un caso, dunque, che raffinata dottrina abbia definito la *privacy*, intesa come *istituto giuridico*, quale «costellazione di diritti»¹⁶. O che altra l’abbia piuttosto descritta come un «diritto inquieto - perché mai uguale a sé stesso, dinamico nel suo tentativo di governare presente e futuro»¹⁷.

Ma procediamo con ordine.

Il concetto di riservatezza, o meglio ancora di vita privata, appare costituire oggetto di indagine filosofica sin dall’età della *Polis*. Lo testimonia la riflessione svolta da Aristotele nella sua *Politica*, in cui il filosofo greco distingue tra *Polis*, o (in estrema sintesi) sfera pubblica dell’individuo, ed *Oikos*, o sfera privata associata alla vita domestica e familiare: sebbene quest’ultima nel discorso

¹⁶ F. MODUGNO, *I “nuovi diritti” nella giurisprudenza costituzionale*, Giappichelli, Torino 1995, pp. 20-21.

¹⁷ A. SORO, «Un diritto di libertà», in S. RODOTÀ, *Riservatezza*, Treccani, Roma 2021, p.12

aristotelico rilevi soprattutto come unità istituzionale di base di una società politica, lo Stagirita offre comunque un primo ritratto di quel «contenuto minimo d'intimità» che per natura l'uomo sarebbe incline a ricercare e a difendere¹⁸.

Tuttavia, si può affermare che le condizioni socioeconomiche che hanno poi consentito l'effettivo affermarsi della *privacy*, intesa come pretesa innanzitutto sociale di riservatezza e dunque esigenza bisognosa di autonoma tutela (anche, molto più avanti, giuridica), siano maturate soltanto a partire dalla fine del medioevo. Il graduale disgregarsi dell'organizzazione feudale della società, in virtù delle trasformazioni socioeconomiche in atto, quali l'urbanizzazione e la contestuale fioritura dei commerci, culminate nella prima (e ancora più emblematicamente nella seconda) rivoluzione industriale, avrebbe smantellato quella fitta rete di relazioni che univa gli individui nella quotidianità, favorendo lo sviluppo del senso di intimità, inteso come «la possibilità di appartarsi a volontà dalla vita e dalle occupazioni in comune con i propri associati»¹⁹. In tal modo, la capacità di isolarsi dal mondo, da privilegio di pochi eletti, sarebbe diventata appannaggio di quanti possedessero i neonati mezzi materiali idonei a garantire, anche in ambiente urbano, le condizioni necessarie a soddisfare il nuovo bisogno d'intimità. Ossia, in poche parole, tale capacità sarebbe divenuta privilegio di un nuovo gruppo sociale: la classe borghese in ascesa, che proprio nella *privacy* come “condizione materiale” avrebbe individuato il proprio connotato differenziale rispetto alle altre classi,

¹⁸ Cfr. ARISTOTELE, *Politica*, Laterza, Bari 2007, I, 1252a-1253b; l'autore intende l'*oikos* in una pluralità di accezioni: casa, proprietà e, per ciò che qui più interessa, famiglia, ossia comunità articolata in rapporti di tipo padronale, matrimoniale e genitoriale, deputata a soddisfare i bisogni primari dell'uomo. Sull'ipotetica necessità biologica di una «sfera riservata», cfr. A. F. WESTIN, *Privacy and Freedom*, Atheneum Press, New York 1967, pp. 8-11.

¹⁹ Per la citazione, così come per il periodo che precede, cfr. L. MUMFORD, *La cultura delle città*, Edizioni di Comunità, Milano 1954, p. 29 ss.

difendendola per più di due secoli attraverso i medesimi strumenti enucleati dal *common law* per la difesa del *property right* (su tutti, il *physical trespass*)²⁰.

In ogni caso, la prima moderna teorizzazione del diritto alla “sfera privata” deve ascriversi all’opera del più importante ed influente tra i “critici” del liberalismo classico, artefice di una sua reinterpretazione in chiave umanitaria: John Stuart Mill²¹. Profondamente avveduto dei mutamenti sociali ed istituzionali verificatisi (fino a quel momento, in Europa; ma a partire dalla metà dell’Ottocento, anche nel Nord America) con l’avvento della società industriale, caratterizzata tra l’altro dal prepotente emergere della classe operaia, l’illustre filosofo inglese fonda la propria critica al liberalismo classico sulla constatazione che il mercato appaia sempre più come area di promozione delle disuguaglianze nelle ricchezze e di rottura del «giusto equilibrio tra gli esseri umani»²². Perciò, la proprietà privata, che ormai contraddice il suo principio di giustificazione, ossia lo sviluppo di una «giusta libertà individuale»²³, non può più essere usata come sinonimo della libertà stessa, in sé e per sé²⁴. Occorre dunque individuare un diverso fondamento alla libertà privata del singolo cittadino: e l’autore lo individua proprio nel più sicuro valore della *persona umana*, di cui la *privacy* è attributo fondamentale, in quanto «cerchio attorno ad ogni essere umano che non

²⁰ S. RODOTÀ, *Riservatezza*, Treccani, Roma 2021, p. 62 ss.

²¹ Cfr. A. BALDASSARRE, *Privacy e Costituzione. L’esperienza statunitense*, Bulzoni Editore, Roma 1974, p. 22 ss., che compie un sontuoso affresco del pensiero del suddetto autore, basandosi in particolare sull’analisi di molteplici passi di alcune delle più importanti opere di J. S. MILL; su tutte: *Sulla “Democrazia in America” di Tocqueville*, tr.it di Valsi, Napoli 1971; *Principi di economia politica*, tr. it. di Campolongo, Torino 1953; *La libertà* (1859), a cura di L. Einaudi, Torino 1925. Di esso si riporta di seguito un succinto distillato.

²² La citazione è tratta da J.S. MILL, *Principi di economia politica*, cit., II, p. 204

²³ *Ibidem*.

²⁴ Corrispondenza biunivoca libertà-proprietà privata che rappresentava uno dei principali postulati del liberalismo classico; cfr. J. LOCKE, *Due trattati sul governo*, tr. it. a cura di L. Pareyson, Torino 1960, II, 123, p. 339.

dovrebbe essere permesso ad alcun governo [né individuo] (...) di oltrepassare»²⁵. Così, Mill rovescia il significato di privilegio della classe borghese che la *privacy* aveva assunto fino a quel momento, specialmente nell'Inghilterra del liberalismo classico. L'illustre filosofo, al contrario, le riconosce la qualità di sicuro baluardo di cui l'uomo comune possa disporre per difendere la propria libertà morale, la capacità di «dominare sé stessi»: e tale capacità, secondo Mill, costituisce il presupposto per l'esercizio di qualsiasi altra libertà individuale di fronte ai crescenti processi di massificazione in atto nella società industriale²⁶.

Il lucido, innovativo pensiero del filosofo inglese penetrò certamente nel Nord America della seconda metà del diciannovesimo secolo, come risposta al suo rapido e improvviso sviluppo industriale, caratterizzato dal conseguente acquisto di autonoma soggettività politica da parte del ceto medio e della classe operaia urbana. Appare, allora, assai probabile che proprio la teorizzazione milliana rientri tra le principali fonti d'ispirazione di quello che è unanimemente considerato l'atto fondativo, sul piano giuridico, dell'istituto della *privacy*, quale autonomo diritto soggettivo preordinato alla difesa dell'intimità come *attributo fondamentale* della personalità umana. Ci si riferisce al saggio monografico pubblicato nel 1890 da due giovani e celebri avvocati di Boston, sotto forma di articolo, sull'*Harvard Law Review*, intitolato proprio "*The Right to Privacy*"²⁷.

1.1. "The Right to Privacy": sviluppo tecnologico e divenire del diritto

²⁵ J. S. MILL, *Principi di economia politica*, cit., I, 893 ss.

²⁶ J. S. MILL, *Sulla "Democrazia in America" di Tocqueville*, cit., 147.

²⁷ S. WARREN, L. BRANDEIS, «The Right to Privacy», cit. Merita ricordare che diversi autori non concordano sull'ispirazione liberal umanitaria dell'opera, interpretando piuttosto la proposta dei due giuristi come una ricostruzione della *privacy* in termini di mero privilegio della *ruling class*. Su tutti, A. WESTIN, *Privacy and Freedom*, cit., 348 ss.; MARTINOTTI, «La difesa della *privacy*», in *Pol. dir.*, 1971, p. 771 ss.

Lo scritto di Samuel Warren e di Louis Brandeis, lungo poco più di trenta pagine, rappresenta una delle prime interpretazioni americane del liberalismo umanitario di ispirazione milliana, di cui abbiamo appena discusso. Il pensiero di Mill, penetrato nel contesto dell'ascendente capitalismo finanziario statunitense, aveva determinato la nascita di un movimento informato all'ideologia del *pluralismo democratico*, secondo cui l'ordinamento sarebbe un sistema articolato di gruppi sociali, unificato da svariati motivi (economici, politici ecc.) ed edificato sui fondamentali principi di tolleranza del dissenso politico e, per quel che qui più interessa, di non interferenza nella *privacy* individuale e di gruppo²⁸.

Nel saggio, i due giuristi, partendo da tali premesse concettuali (non senza molteplici ambiguità determinate dalla loro appartenenza alla classe borghese, nonché dall'estrazione conservatrice di Warren), sostenevano l'opportunità di introdurre, nel sistema giuridico statunitense, un "nuovo" diritto". Sotto il termine *privacy*, essi presentavano allora un diritto soggettivo fondamentale, azionabile davanti ad un giudice terzo ed imparziale, soprattutto nei confronti dei privati cittadini. Quanto al suo contenuto sostanziale, tale diritto, a seconda dei casi concreti, avrebbe dovuto declinarsi innanzitutto come *right to be let alone*, ossia come posizione giuridica che garantisse l'interesse ad essere lasciati «indisturbati» (*privacy* come *non intrusione*)²⁹. Allo stesso tempo, esso avrebbe

²⁸ Cfr. A. BALDASSARE, *Privacy e Costituzione*, cit., pp. 33-35, che rinvia tra gli altri a V. L. PARRINGTON, *Storia della cultura americana*, tr. it. di Rossi Landi, Torino 1969, III, 516 s.; e a R. P. WOLF, H. MARCUSE, B. JR. MOORE, *Critica della tolleranza*, Einaudi, 1970, p. 14 ss. e 40 ss.

²⁹ S. WARREN, L. BRANDEIS, «The Right to Privacy», cit., p. 195. I due autori rinviavano all'autorità dei precedenti del giudice Thomas C. Cooley, il cui *Law of Torts* era giunto alla seconda edizione già nel 1888 e che per primo aveva utilizzato, sebbene in una diversa e più limitata accezione, l'espressione *right to be let alone*: cfr. sul punto A. BALDASSARE, *Privacy e Costituzione. L'esperienza statunitense*, cit., p. 40. Da notare che, nel contesto in questione, parrebbe poi opportuno tradurre l'espressione inglese *alone* con il termine italiano "indisturbato", e non già con il termine "solo", che ne restringerebbe altrimenti la portata semantica: cfr. U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa. Modelli giuridici a confronto*, Giuffrè, Milano 2008.

dovuto presidiare in senso stretto l'esigenza, sino a quel momento ricondotta nell'alveo della tutela accordata al tradizionale *right to property*, di «ritirarsi dal mondo»³⁰ e di vivere isolati in casa propria, con l'obiettivo di «impedire che della propria vita (...) [un] ritratto sia in alcun modo eseguito» (*privacy* come *esclusione* o *seclusion*)³¹.

Occorre aprire una parentesi. La più attenta dottrina, ancorché divisa al suo interno, è da sempre concorde nel sostenere che l'"illesa intimità", o piuttosto l'"integrità della sfera privata", sebbene non ancora concepita come autonomo bene giuridico, già prima della comparsa del saggio in esame godesse di una specifica protezione giuridica al pari di altri interessi inerenti alla persona umana. Tale protezione sarebbe stata garantita attraverso strumenti embrionali di tutela, o l'estensione di quelli già previsti per i beni giuridici nel cui alveo tali interessi fossero ricompresi (non essendo a tali interessi ancora riconosciuta dignità di autonomo bene giuridico).

Alcuni autori sottolineano come «la stessa configurazione di Warren e Brandeis costituisca, a sua volta, un originale adattamento al suolo americano di una idea che trova le sue radici proprio in Europa nella elaborazione degli *Individualrechte* [intesi come «signoria sopra una parte della propria sfera della personalità»]: diritti [che, in origine, garantivano la pretesa] di utilizzare liberamente le proprie forze ed i risultati della propria attività, e ai quali i tedeschi [dovevano e] devono ricorrere per offrire tutela al diritto d'autore»³².

³⁰ S. WARREN, L. BRANDEIS, «The Right to Privacy», cit., pp. 198, 213 ss.

³¹ Ivi, p. 200.

³² La citazione è di G. MARINI, «Diritto alla privacy», in *Commentario del Codice Civile*, (diretto da) E. GABRIELLI, UTET, Milano, 2013, p. 199 ss.; come esponenti più importanti di tale dottrina, cfr. FERRARA, SANTAMARIA, «Il diritto alla illesa intimità privata», in *Riv. dir. privato*, 1937, p. 171.; e G. RESTA, «I diritti della personalità», in G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, in UTET Giuridica, Torino, 2006.

Altri sottolineano come già alcuni Stati, tra il diciottesimo e il diciannovesimo secolo, principalmente di *civil law*, si fossero dotati di una legislazione o avessero maturato giurisprudenza in materia di violazioni della “vita privata” in senso lato: in particolare, vengono richiamate la legislazione svedese per l’accesso agli atti pubblici del 1776; il caso *Rachel* in Francia del 1858 sui limiti della pubblicazione di fatti personali; il codice penale norvegese del 1889, che espressamente puniva la pubblicazione di dati o fatti relativi agli «affari personali o domestici»³³.

Per quanto riguarda specificamente il *common law* poi, autorevole dottrina, in uno dei più importanti saggi monografici scritti sul tema, asserisce che un diritto alla *privacy* fosse già riconosciuto dall’ordinamento americano a partire dal periodo immediatamente precedente la guerra civile, seppur nei limiti dei meccanismi di indebita invasione dell’*intimacy* allora conosciuti³⁴.

Tuttavia, anche alla luce dei rilievi già svolti, si può affermare che l’articolo di Warren e Brandeis abbia svolto l’importante funzione di offrire la prima esauriente *fondazione giuridica* dell’istituto della *privacy*, basata sull’elaborazione di una prima consaputa (sebbene ancora generica, come vedremo a breve) teoria del diritto cui l’istituto dà il nome: e, dunque, di determinare l’effettiva nascita di un modello giuridico, poi circolato negli altri paesi della tradizione giuridica occidentale³⁵.

Come è stato limpidamente scritto, «in nessun modo può affermarsi che un diritto alla *privacy* sia stato riconosciuto dalla giurisprudenza o dalla dottrina [esplicitamente] prima della pubblicazione del saggio di Warren e Brandeis (...)»

³³ Cfr. U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 4, nota 4.

³⁴ Cfr. A. WESTIN, *Privacy and Freedom*, cit., p. 337.

³⁵ Di tali aspetti, e dunque delle radici della *privacy* “giuridica” in Europa ci occuperemo più avanti, nel nostro *excursus* storico riguardante il Vecchio Continente: v. cap. 2, par. 2.1.

del 1890»: infatti, esaminando le decisioni e i contributi precedenti al 1890, «non solo non si riesce a definire unitariamente la qualità dei beni complessivamente protetti da quel diritto, ma addirittura non si mostra di conoscere quale principio ispiratore (...) ne legittimi [il riconoscimento]»³⁶. E lo stesso discorso, *mutatis mutandis*, varrebbe per la tradizione di *civil law*, in cui il modello giuridico in tal modo nato negli Stati Uniti sarebbe poi circolato³⁷.

Si può chiudere la parentesi affermando che «grazie a questa pubblicazione (...) il termine *privacy* acquisisce una propria autonomia, disancorandosi dal diritto di proprietà, in virtù del quale, fino ad allora, aveva ricevuto protezione giuridica»³⁸.

Occorre approfondire ulteriormente l'analisi del saggio in commento, poiché molti dei motivi ad esso sottesi, dai quali scaturì l'urgenza dei due giuristi di Boston di dedicarvisi, sono comuni a quelli che animano le riflessioni intorno alla disciplina dei trattamenti automatizzati dei dati personali condensate nel

³⁶ Le citazioni, e più in generale la riflessione, sono sempre di A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 9 ss., che nelle pagine seguenti la approfondisce ulteriormente. In sintesi, a sostegno del riportato assunto, l'autore adduce da una parte il fatto che il diritto alla privacy, stante il contenuto che gli sarebbe stato riconosciuto allora, non avrebbe potuto trovare autonoma collocazione in una delle categorie fondamentali individuate da William Blackstone, uno dei padri del moderno sistema di common law, a proposito dei diritti di libertà: *personal security, personal liberty e personal property* (per la tripartizione cfr. W. BLACKSTONE, *Commentaries on the laws of England*, 11 ed., London 1791, I, 129 ss.). E dall'altra il fatto ancor più rilevante che il complesso dei "beni della vita" ricompresi nell'ambito del presunto archetipo del moderno diritto alla *privacy* trovasse protezione solo attraverso gli strumenti tradizionalmente apprestati per la "costellazione" dei diritti di proprietà e, residualmente, ma pur sempre in forza del principio unitario della *property*, per il contratto (inteso nel senso generico di patto, anche implicito): su quest'ultimo punto, vedi *infra*.

³⁷ Cfr. *supra*, MARINI e altri, nota 30; e PAGALLO, nota 31; inoltre, cfr. tra gli altri S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. Conti, Editori Laterza, 2005; ID., *Riservatezza*, cit., p. 65; A. DI MARTINO, *Profili Costituzionali della Privacy in Europa e negli Stati Uniti*, Jovene Editore, Napoli 2017, p. 37 ss.; M. LUCIANI, *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, studio commissionato dal Servizio Ricerca del Parlamento Europeo (EDPRS), 10/2018, p. 6 ss.

³⁸ G. GARDINI, *Le regole dell'informazione*, Milano, 2009, p. 241.

presente lavoro: su tutti, il nefasto impatto della tecnologia sulla sfera di “autodeterminazione” del singolo, specialmente sotto il profilo della potenziale mercificazione cui essa, nella sua incessante evoluzione, è in grado di esporre l’intimità.

Alla base della proposta dei due autori, si collocava infatti il potente sviluppo dei mezzi di informazione e di comunicazione, diventati gradualmente *mass media*: accanto al vertiginoso aumento dei giornali stampati e alla loro sempre più “massiva” circolazione, si collocavano l’invenzione del telegrafo, risalente al 1844, e quella del telefono, datata convenzionalmente 1876, anno in cui Alexander Graham Bell aveva ottenuto il rilascio negli Stati Uniti di un brevetto avente ad oggetto un dispositivo capace di “trasmettere” integralmente la riproduzione della voce di una persona ad un secondo apparecchio³⁹. Ma la rivoluzione più profonda interessava certamente le tecniche di realizzazione del ritratto, nella loro più moderna declinazione ampiamente sfruttate proprio dalla crescente ala del giornalismo sensazionalistico, anche detto *yellow journalism*: in particolare, i due giuristi nel loro lavoro avevano ben a mente la diffusione delle prime fotografie istantanee che, per citare a titolo di esempio solo una delle prime e più note aziende del settore, la Eastman Kodak Company andava producendo sin dal 1884⁴⁰.

Fin dall’inizio del loro saggio, Warren e Brandeis, facendo proprio un approccio non solo, come già abbiamo detto, liberal-umanitario, bensì anche genetico-evolutivo, e preconizzando uno dei tratti unificanti del successivo

³⁹ Per un quadro generale sulla storia e sullo sviluppo dei media in generale, o di alcuni di essi nello specifico, cfr. ad es. L. G. PACE, «The Origins of Mass Media in the United States», in A. WELLS; E. A. HAKENEN (a cura di), *Mass media & society*, Greenwood Publishing Group, 1997 p. 10; LIBRARY OF CONGRESS, «Who is credited with inventing the telephone?», 18 ottobre 2020, consultabile qui: <https://www.loc.gov/everyday-mysteries/technology/item/who-is-credited-with-inventing-the-telephone>.

⁴⁰ S. WARREN, L. BRANDEIS, «The right to privacy», cit., p. 195 ss.

percorso di affermazione e trasformazione dell'istituto della *privacy*, insistono proprio sulla idoneità del progresso tecnologico a suscitare nuove esigenze nel corpo sociale, tra le quali ricade la tutela giuridica della “dimensione spirituale” dell'uomo, e dunque di beni della vita di natura piuttosto immateriale che fisica, tra cui la reputazione, i prodotti dell'intelletto e, per quanto qui concerne, esprimendoci con le parole dei due stessi giuristi, «l'inviolata personalità»⁴¹. Progresso tecnologico e conseguenti trasformazione sociali che, insieme, sarebbero in tal modo idonei a determinare l'evoluzione «necessaria» (e spontanea) del diritto⁴².

Il motore della trasformazione dei bisogni sociali, e conseguentemente delle risposte del diritto alle nuove domande di tutela giuridica del *quivis ex populo*, è individuato dai due autori nelle scoperte o «*recent inventions*» dell'uomo. Da tale inciso si evince che i due autori fossero ben consapevoli che le innovazioni della tecnica -e, segnatamente, le macchine fotografiche- avrebbero configurato il rischio di una circolazione abusiva delle immagini personali, per la prima volta utilizzabili e riproducibili con facilità su scala industriale: con la conseguente, potenziale esplosione di delicati conflitti tra interessi economici, interesse “morboso” del pubblico ed istanze degli individui circa la garanzia di una nuova “riservatezza”. E proprio tale bene della vita il *common law*, nella visione dei due giuristi, avrebbe saputo e dovuto soddisfare per mezzo del riconoscimento del diritto nel saggio teorizzato⁴³.

Per intendere pienamente quest'ultimo punto, fondamentale ai fini della giusta comprensione dell'intero ragionamento svolto dai due giuristi, occorre ricordare che una delle matrici teoriche del saggio consiste in quello che abbiamo

⁴¹ Ivi, p. 205.

⁴² Ivi, p. 195.

⁴³ Sul punto, U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, op. cit., pp. 5-7.

definito un *approccio genetico-evolutivo*. Secondo tale impostazione, in generale, l'ordinamento giuridico deve essere concepito come qualcosa di «vivo», che «evolve»; ciò premesso, i due giuristi affermano che, nonostante il principio dello *stare decisis* su cui è imperniata la tradizione giuridica di *common law*, proprio «la splendida abilità di crescere che caratterizza [il] common law (...) permett[e] ai giudici di apprestare la protezione necessaria senza l'intervento del legislatore»: principio applicabile, di conseguenza, anche all'istituto oggetto della loro proposta⁴⁴.

In sintesi, la seconda rivoluzione industriale e l'avvento dei nuovi mezzi di comunicazione hanno rappresentato il contesto storico, sociale ed economico in cui la borghesia ha sentito la necessità di tutelare il proprio spazio vitale - inizialmente identificato con il solo spazio racchiuso all'interno delle mura domestiche- da intrusioni esterne⁴⁵. Necessità di cui i due avvocati di Boston si sono fatti abilmente interpreti, proponendo, per interposizione della giurisprudenza - attraverso lo strumento dell'*overruling* - il riconoscimento di un diritto di “nuova generazione”, adatto a soddisfarla⁴⁶.

⁴⁴ Cfr. S. WARREN, L. BRANDEIS, «The Right to Privacy», cit., p. 213.

⁴⁵ E. BRUGIOTTI, «La privacy attraverso le “generazioni dei diritti”». Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico», in *dirittifondamentali.it*, 2/2013, p. 6

⁴⁶ Occorre svolgere una sintetica digressione sul punto. Pur con le fisiologiche differenze intercorrenti da sistema a sistema, infatti, il *proprium* dei sistemi di *common law* è rappresentato dal fatto che, accanto al formante legislativo, la giurisprudenza costituisce fonte di diritto: tali sistemi riconoscono dunque ai giudici il ruolo che fisiologicamente essi svolgono nella sfera della produzione normativa. Tuttavia, nella sua attività creativa, la giurisprudenza è soggetta al principio di vincolatività dei precedenti giudiziari (c.d. *stare decisis*), come declinato in senso moderno nel diciottesimo secolo dalla teoria c.d. dichiarativa del celebre giurista inglese William Blackstone (v. ad es. *Commentaries on the Law of England*, 1765/1769, 70-71). Gli unici strumenti a disposizione della collettività per superare l'autorità della precedente decisione sul simile caso sono, da una parte, il prodotto dell'attività legislativa (lo *statute*); e, dall'altra (quanto meno nel modello di *common law* ad oggi più circolante nel mondo, ossia quello americano), l'*overruling* giurisprudenziale, nelle sue diverse specie individuate dalla consuetudine (*anticipatory* e *prospective*), ossia l'abbandono del precedente

Merita considerare un punto molto importante. Nella prospettiva teorica di Warren e Brandeis, il *right to privacy* è posizione giuridica soggettiva che, sotto il profilo contenutistico, resta comunque legata al modello (teorico) del *property right* anglosassone⁴⁷. Ciò significa che tale nuovo *right* viene concepito pur sempre quale *ius excludendi alios*, e dunque quale diritto che esprime una dimensione essenzialmente negativa (al pari, appunto, del diritto di proprietà). Dritto, dunque, ad escludere qualsiasi ingerenza esterna all'interno del proprio spazio d'intimità, inteso come insieme dei pensieri e dei sentimenti espressi in qualsiasi modo nell'ambito di relazioni personali, domestiche o comunque non conosciute da terzi (c.d. *seclusion*)⁴⁸.

Tale costruzione del *right to privacy* è dunque ancora lontana dalla prima definizione dottrinale “moderna” di *privacy*, che della libertà in esame valorizzerà anche l'aspetto positivo, intendendo la *privacy* come *controllo* sulle informazioni riguardanti la propria persona, e che porrà le basi per la successiva emancipazione

indirizzo (della precedente *rule of – judiciary- law*) attraverso l'enunciazione di un nuovo principio di diritto ad opera di una Corte a ciò, entro precisi limiti oggettivi e soggettivi, legittimata. Per una buona introduzione sui temi del *common law* angloamericano, si v. C. F. ABERNATHY, *Law in the United States*, Thomson/West, St. Paul, MN, 2006; U. MATTEI, *Common Law. Il diritto anglo-americano*, in *Trattato di diritto comparato*, (diretto da) R. SACCO, Utet, Torino 1992. Per un'introduzione sull'ordinamento anglo-americano in generale, si v. V. VARANO, V. BARSOTTI, *La tradizione giuridica occidentale. Testo e materiali per un confronto tra civil law e common law*, G. Giappichelli Editore, Torino 2021, 3, sez. I e III.

⁴⁷ La *property*, nel *common law* anglosassone, è principio che informa tanto l'istituto della proprietà-appartenenza, quanto quello del contratto, inteso principalmente come strumento giuridico di utilizzazione e di disposizione della cosa posseduta: v. sul punto A. BALDASSARRE, *Privacy e Costituzione*, cit., p.15-16.

⁴⁸ Cfr. S. WARREN, L. BRANDEIS, «The Right to Privacy», cit., p. 211 ss.; secondo gli autori, anche a livello concettuale, tra *privacy* come autonomo diritto e proprietà esisterebbe in qualche modo una corrispondenza, purché si intenda quest'ultima nel suo più “ampio e inusuale” significato di *appartenenza*.

dal suo alveo, in Nord America, del concetto di *information privacy*; e, in Europa, dell'autonomo diritto fondamentale alla protezione dei dati personali⁴⁹.

È inoltre da ricordare che i due giuristi, a sostegno della tesi proposta nel saggio, collocano la secolare casistica anglosassone in materia di *trespass* e di *breach of trust or contract*, seppur richiamata attraverso la sola citazione delle pronunce del giudice Cooley e dei pochi altri casi in cui le Corti, nel diciottesimo e diciannovesimo secolo, avessero rilevato una lesione della “privatezza” quale profilo del bene giuridico rappresentato dal binomio appartenenza-godimento del bene immobile o piuttosto dal rapporto fiduciario o dalla buona fede contrattuale. In questo senso, sono emblematici i casi del *Principe Alberto contro Strange*, ampiamente esaminato nell'articolo, e quello di *Abernethy contro Hutchinson*⁵⁰. Tuttavia, proprio nel riconoscere la *privacy* quale attributo fondamentale della più generale *immunità personale*, e segnatamente come “inviolata personalità” o

⁴⁹ Il riferimento è ai contributi di A. WESTIN, *Privacy and Freedom*, cit., tesi ripresa da C. FRIED, «Privacy: A Rational Context», in *Computers, Ethics and Society*, (a cura di) M.D. ERMANN, M.B.WILLIAMS, e C.GUTIERREZ, Oxford University Press, New York 1990, p. 54. Cfr. sul punto S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 320; U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 41-42.

⁵⁰ Cfr. *Prince Albert v. Strange*, 1 Mac Naghten and Gordon Reports 25 (1849) e *Abernethy v. Hutchinson* del 1825, cit. in S. WARREN, L. BRANDEIS, «The Right to Privacy», p. 207 ss. Secondo A. BALDASSARRE, *Privacy e Costituzione*, cit., nel constatare come le decisioni giudiziarie precedenti alla compiuta fondazione giuridica dell'istituto operata da Warren e Brandeis evidenziassero come proprietà-appartenenza e contratto, informate all'unificante principio liberale della *property*, fossero le due sole categorie attraverso cui gli ordinamenti anglosassoni del diciottesimo e del diciannovesimo secolo giustificassero la tutela di *common law* della vita privata: «si prospetta così [fino alla fine del diciannovesimo secolo] una teoria della *privacy* sorretta da un duplice principio portante: quello della *proprietà privata*, allargato fino a comprendervi ogni rapporto di appartenenza, e quello del *contratto*, inteso nel senso ampio e comprensivo di ogni patto, anche implicito. Così concepiti, l'uno e l'altro principio appaiono dotati di una tal forza espansiva da poter permettere ai giudici di *common law* di incasellare la varia problematica della *privacy* in uno dei loro innumeri profili», p. 13; e ancora: «una volta che la violazione della sfera privata individuale è equiparata a quella della proprietà privata, appare consequenziale estendere alla prima le regole che presiedono alla tutela del pacifico godimento dei possessi dominicali», p. 16. Cfr. anche, sul punto, brevemente G. C. FERONI, «I dati personali come oggetto di un diritto fondamentale», in *I “poteri privati” delle piattaforme e le nuove frontiere della privacy*, (a cura di) P. STANZIONE, Giappichelli, Torino 2022, pp. 59 e 60; e U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 5.

“illesa intimità”, essi rilevano l’inadeguatezza degli strumenti di tutela tradizionali, che non si attagliano al *proprium* di un diritto che protegga un interesse squisitamente personale, qual è quello a non subire interferenze nella propria sfera di intimità, e dunque un contenuto “spirituale” quanto al suo valore⁵¹.

Il merito storico dei due autori, allora, non sta tanto nella definizione specifica del contenuto del neo-fondato *right to privacy*, che resta estremamente generica: come rilevato dallo stesso Westin, infatti, l’unica “determinazione” che si desume dal saggio è che esso, come autonomo diritto soggettivo a contenuto negativo, ha la sua essenza nella libertà di decidere se rendere pubblici o meno i propri pensieri e i propri sentimenti.⁵² Esso mutua la dimensione negativa del *right to be let alone* già individuato dal giudice Cooley, sebbene mostri la novità di emanciparsi dal diritto di proprietà e in generale dai rapporti patrimoniali cui la giurisprudenza l’aveva fino a quel momento legato, e più in generale dall’interpretazione che l’illustre giudice aveva dato di tale diritto, quale aspetto comune a tutti i diritti di libertà civile, consistente nella *libertà negativa* di rifiutarsi di esercitare il diritto medesimo⁵³.

Il vero, autentico merito storico dei due autori risiede piuttosto nell’aver configurato la violazione della *privacy* (quale bene della vita, lo ripetiamo, giuridicamente tutelato da un autonomo diritto soggettivo a contenuto negativo) come *tort*, ossia come autonoma fattispecie di illecito civile (extracontrattuale), dimostrando così la totale inadeguatezza degli schemi del *property right*, della

⁵¹ Cfr. S. WARREN, L. BRANDEIS, «The Right to Privacy», cit., p. 200 ss.; e commento di A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 42 ss.

⁵² Cfr. A. WESTIN, *Privacy and Freedom*, cit., p. 337 ss..

⁵³ Sulla definizione di *right to be let alone* adottata dal giudice Cooley, vedi A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 40; e anche *supra*, nota 15. Sulle sue applicazioni giurisprudenziali, vedi A. WESTIN, *Privacy and Freedom*, cit., p. 340; M. C. SLOUGH, *Privacy, Freedom and Responsibility*, Thomas, 1969, p. 29.

breach of trust, confidence or contract e del *physical trespass* cui era stata fino a quel momento ricondotta la tutela della prima. Per i due giuristi di Boston, infatti, l'interferenza nella *privacy* produce un danno, identificabile nel turbamento della "pace dello spirito" del soggetto che subisce l'invasione della propria sfera privata, resa ancora più facile dai nuovi mezzi d'informazione: danno che, avendo le caratteristiche del *damnum inuria datur*, autorizza all'azione di inibizione o di risarcimento⁵⁴. Il profilo in questione è rilevante, perché consente di enfatizzare, nella teoria dei due giuristi, la funzione di critica – di stampo democratico - alla concezione tradizionale di *common law* che considerava la *sfera privata* meritevole di protezione solo nell'alveo e secondo gli schemi di tutela del *property right*: concezione che fino a quel momento aveva elevato la *privacy* a mero privilegio dei proprietari, e dunque della *ruling class* borghese e, prima ancora, aristocratica⁵⁵.

Allo stesso tempo, il principale limite della teoria dei due giuristi consisterebbe nella stessa qualificazione giuridica della violazione della *privacy* come autonomo *tort*. In questo modo, essi non riescono infatti a svincolarsi dalla logica privatistica del loro tempo, di cui pur sembrano avvertire l'insufficienza (e in particolare dalla suddetta identità tradizionale *privacy-property*, che pur intendevano definitivamente erodere); e così a rifondare in chiave -veramente-umanitaria i diritti di libertà⁵⁶. Essi, elaborando una teoria della *privacy* interamente negativa, e dunque circoscritta agli angusti confini della *private law of torts*, inevitabilmente ottengono che il diritto di cui auspicano il riconoscimento resti essenzialmente conformato nella sua struttura e nel suo contenuto al modello dominicale, dunque alla stregua di *ius excludendi alios*, che assume consistenza solo nel momento e nella misura in cui venga violato. Così, nel momento in cui

⁵⁴ Cfr. in particolare S. WARREN, L. BRANDEIS, «The Right to Privacy», cit., p. 196 ss.

⁵⁵ Cfr. A. BALDASSARRE, *Privacy e Costituzione*, cit. p. 59 ss.

⁵⁶ Ivi, p. 37 e ss., e in particolare p.48.

pur qualificano quest'ultimo come diritto a presidio di un attributo del "nucleo essenziale della personalità umana", essi non riescono a percepirne la dimensione "superindividuale"; e pertanto nemmeno si interrogano sul fondamento costituzionale del medesimo⁵⁷.

In conclusione, sembra che il saggio esaminato esprima il suo massimo valore e la maggior carica innovativa nella sua *verve* polemica nei confronti della dottrina dominante del tempo, d'impostazione liberal-proprietaria, che individuava il baricentro della tutela della privacy nel *property right* e nei mezzi tradizionalmente apprestati a sua difesa. Ma non solo. Preziosa eredità del medesimo è anche la notevole lungimiranza dei due autori, che sembrano intuire chiaramente l'inarrestabile sviluppo cui fosse destinata la tecnologia moderna, e come ciò avrebbe determinato una esponenziale moltiplicazione delle interferenze e delle invasioni della sfera privata, senza la minima partecipazione della persona offesa.

Tale eredità appare quanto mai attuale, se si considera il vertiginoso *exploit* conosciuto dalle ICTs⁵⁸ dalla fine del ventesimo secolo ad oggi e l'accelerazione

⁵⁷ Del limite dell'impostazione dei due giuristi sotto tale profilo parla M. C. SLOUGH, *Privacy, Freedom and Responsibility*, cit., 28; attribuisce quest'ultima storicamente al noto fatto che la vita giuridica dello "Stato Liberale" ottocentesco fosse imperniata strutturalmente sul diritto privato, e segnatamente sul diritto di proprietà, motivo per cui tutti i "diritti della personalità" venivano concepiti e inquadrati nel livello subcostituzionale del diritto privato di common law, A. BALDASSARRE, *Privacy e Costituzione*, cit., 64 ss. Merita subito anticipare che sul fondamento costituzionale del right to privacy verrà ad interrogarsi la dottrina americana a partire dalle prime sentenze della Corte Federale Suprema di Washington sul tema, e ancor più dal fondamentale caso *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965): sul punto, v. *infra*.

⁵⁸ Acronimo di *Information and Communication Technologies* (tecnologie dell'informazione e della comunicazione), definite come "[le] tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software [oggi comprensive di *smartphones* e *smart objects*], che permettono agli utenti di creare, immagazzinare e scambiare informazioni": v. la voce «ICT (Information and Communication Technologies)», in *Dizionario di Economia e Finanza*, Treccani, Enciclopedia online, 2012, consultabile qui: https://www.treccani.it/enciclopedia/ict_%28Dizionario-di-Economia-e-Finanza%29/.

da esso impressa alle attività di *Big Data analytics* e di *data mining*, a loro volta motore di un'implementazione senza precedenti delle soluzioni applicabili di Intelligenza Artificiale. Rispetto a tali fenomeni, che compongono quella *grande trasformazione*⁵⁹ implicata dalla digitalizzazione del mondo, il diritto si trova costantemente in una posizione di asimmetria, epistemologica prima ancora che precettiva, che il legislatore e l'interprete sono chiamati, ciascuno con i propri strumenti, a risolvere con tutte le proprie forze, componendo nel proprio sguardo tradizione e innovazione: ciò, allo scopo ultimo di salvaguardare nel quadro della *società liquida*⁶⁰ contemporanea l'irrinunciabile nucleo essenziale della personalità umana, limpidamente ritratto dall'art. 2 della nostra Costituzione e già echeggiante nelle righe di questo breve e illuminato articolo del 1890⁶¹.

Per le suddette ragioni, allora, appare necessario interrogarsi sull'effettiva *portata storica* del saggio di Warren e Brandeis, e pertanto sull'incidenza che esso abbia avuto rispetto alle successive evoluzioni del diritto comune statunitense.

⁵⁹ L'espressione è tratta dalla celebre opera di K. POLANYI, *La grande trasformazione. Le origini economiche e politiche della nostra epoca*, Torino 1974.

⁶⁰ La fortunata espressione è di Z. BAUMAN, *Modernità Liquida*, trad. it. di Sergio Minucci, Editori Laterza, Roma-Bari 2002, che intende con essa sottolineare il carattere strutturalmente incerto, provvisorio e dunque volubile dell'esperienza individuale e delle relazioni sociali contemporanee, immerse in un contesto ambientale globalizzato in cui «l'unica costante è il cambiamento».

⁶¹ Per una panoramica sui problemi e sui concetti ivi accennati, v. *infra*, paragrafo 3. Per un'analisi dettagliata dei medesimi si rinvia subito, in generale, a F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Shape Our Minds*, Harvard University Press, 2005; L. FLORIDI, *The Fourth Revolution: How Infosphere Is Reshaping Human Reality*, Oxford University Press, 2014; VANNUCCHI, *Internet e le dinamiche dei ruoli degli OTT (Over The Top) e Telco nel panorama ICT, Mondi digitale*, n. 5/ 2015, in <http://mondodigitale.aicanet.net/>; F. DI PORTO (a cura di), «Big Data e Concorrenza», in *Concorrenza e Mercato*, Giuffrè Editore, n. speciale 23/2016, p. 5 ss. ; HILDEBRANDT, «The Dawn of a Critical Transparency Right for the Profiling Era», in *Digital Enlightenment Yearbook 2012*, (a cura di) HILDEBRANDT ET AL., Amsterdam 2012; S. ZUBOFF, *Il Capitalismo della Sorveglianza. Il Futuro dell'Umanità nell'Era dei Nuovi Poteri*, Luiss University Press, 2019.

1.1.1. «*Subtler and more far reaching means of invading privacy*»: la *privacy-property* fino al *dissent* del giudice Brandeis in *Olmstead v. United States*

Se l'auspicio dei due giuristi era quello che l'ordinamento statunitense, stante la «meravigliosa capacità di evolvere» che gli stessi attribuivano al *common law*, recepisce la proposta del nuovo diritto in questione, quest'ultima al contrario non penetrò immediatamente nella cultura giuridica e nella giurisprudenza statunitensi del tempo. Anzi, si può dire che per almeno un decennio essa non fu quasi oggetto di considerazione alcuna.

Lo dimostra innanzitutto il caso *Roberson*, deciso nel 1902 dalla Corte d'Appello di New York, in cui una giovane donna di nome Abigail Roberson, dopo aver scoperto che una sua fotografia era stata litografata a sua insaputa su più di ventimila volantini allo scopo di pubblicizzare la vendita di una certa marca di farina, aveva proposto ricorso, lamentando che l'esposizione pubblica della sua immagine le aveva procurato una sofferenza psicofisica tale da esser dovuta ricorrere alle cure di un medico specialista⁶². Nella decisione, la *Court of Appeal*, rovesciando il dispositivo di due pronunce emesse da giudici inferiori che accoglievano senza riserve la tesi proposta dalla difesa, ossia l'esistenza del *right to privacy* postulato dal saggio del 1890, rigettava il ricorso, sottolineando, innanzitutto, con un argomento di tipo formalistico, la circostanza secondo cui «*there [was] no precedent for such an action to be found in the decision of this court*». La Corte poi evidenziava, seppur amplificandola, l'indiscutibile incertezza del contenuto del diritto alla *privacy* rielaborato nella teoria di Warren e Brandeis, in particolare insistendo sull'opacità caratterizzante la distinzione,

⁶² Cfr. *Roberson v. Rochester Folding Box Co.*, 171 U. Y. 538 (1902).

compiuta nel saggio secondo un criterio quasi tautologico, tra sfera pubblica e sfera privata. Infine, i giudici rilevavano la non trascurabile circostanza che il riconoscimento del diritto in esame avrebbe potuto rappresentare un'indebita restrizione del diritto di libertà di manifestazione del pensiero o *Freedom of Expression* tutelato a livello costituzionale dal Primo Emendamento⁶³.

La sentenza in questione, tuttavia, suscitò uno sdegno tale nell'opinione pubblica da determinare lo Stato di New York a promulgare nel 1903 una legge passata alla storia come la prima legislazione sulla *privacy* negli Stati Uniti d'America⁶⁴. In realtà, essa aveva la ben più limitata funzione di consolidare a livello statuario il principio di diritto comune, già affermato nel caso *Pope v. Curl* o in quello *Prince Albert v. Strange*, che si limitava a vietare l'uso commerciale o pubblicitario del nome, dell'immagine o di scritti propri senza il previo consenso del titolare, in quanto beni oggetto di diritti della personalità già ampiamente riconosciuti dal *common law* statunitense.

Allo stesso modo, nel 1905 la Corte Suprema di Georgia, nel famoso caso *Paveish v. New England Life Insurance Company*, molto simile nei fatti al caso *Roberson* (l'attore lamentava che una sua fotografia fosse stata utilizzata per fini pubblicitari da una compagnia assicuratrice senza il suo consenso), rovesciò completamente la decisione presa in quest'ultimo dalla *Court of Appeal* di New York, riconoscendo esplicitamente l'esistenza nel *common law* di un diritto alla *privacy*⁶⁵. L'importanza di tale decisione sta, soprattutto, nel fatto che la Corte tenta anche una collocazione sistematica del diritto in questione, affermando che esso, ponendosi a presidio di un interesse, quello alla "vita privata", fondato sull'«istinto naturale», deriverebbe niente meno che dal *diritto naturale*, e come

⁶³ Cfr. *Ibidem* e BALDASSARE, *Privacy e Costituzione*, cit., p 49-51.

⁶⁴ Cfr. *New York Laws* 1903, cap. 132, par. 1-2.

⁶⁵ Cfr. CORTE SUPREMA DI GEORGIA, *Paveish v. New England Life Insurance Co.*, 122, Georgia 190 (1905).

tale si supporrebbe richiamato dalle Costituzioni, dalle leggi civili e dalle consuetudini non solo della Georgia, bensì degli stessi Stati Uniti d'America a livello federale.

Tuttavia, nonostante il pregevole tentativo chiarificatore, non si deve sopravvalutare il contributo di quest'ultima sentenza all'effettivo accoglimento della teoria della *privacy* di Warren e Brandeis - come presidio al patrimonio spirituale comune ad ogni uomo - da parte della giurisprudenza di diritto comune, e dunque al riconoscimento del *right to privacy* quale parte di esso. Infatti, ad una lettura più attenta, ci si accorge che la sentenza in questione, sotto l'etichetta del diritto alla *privacy*, accomuna tutta una serie di diritti della personalità già pacificamente garantiti dal *common law* statunitense, riguardanti l'uso esclusivo del nome o dell'immagine o l'appropriazione commerciale di alcuni elementi della personalità umana. Impiego di un nuovo nome per indicare diritti già noti, dunque. E autorevole dottrina, nonostante le voci discordanti della letteratura del tempo⁶⁶, ritiene che dello stesso segno siano quasi tutte le sentenze che fino agli anni cinquanta del ventesimo secolo pongono a fondamento delle proprie soluzioni l'esistenza di un diritto alla *privacy* di *common law*, a tal proposito riportando un dato sorprendente: fra le circa trecento sentenze apparse tra il 1880 e tutta la prima metà del novecento, solo due riguarderebbero casi di azioni contro privati per motivi di "invasione" della propria sfera privata, e nello specifico di sorveglianza tecnica⁶⁷. E vedremo tra poco che lo stesso varrà per la giurisprudenza costituzionale di quegli anni.

Nonostante ciò, alla sentenza *Paveisch* deve riconoscersi l'importante merito storico di aver promosso una prospettiva idonea a superare il limite forse

⁶⁷ Cfr. W. L. PROSSER, «Privacy, a legal analysis», in *California Law Review*, n. 48, 1960, p. 386 ss; A. F. WESTIN, *Privacy and Freedom*, cit., p. 347; entrambi i casi riguarderebbero ipotesi di indebito ascolto e di clandestina intercettazione di conversazioni private.

principale, già evidenziato, della teoria di Warren e Brandeis: nell'ancorare, infatti, l'esistenza del diritto alla *privacy* al diritto naturale, la Corte dimostra di avvedersi della insufficienza della dimensione del *common law*, e pertanto di essere consapevole della rilevanza propriamente costituzionale dell'interesse all'integrità della vita privata, a cominciare dalla problematica relativa alla sua esistenza e al suo fondamento giuridico⁶⁸. Proprio ciò che i due avvocati di Boston non erano stati capaci di fare, vittima dell'impostazione della problematica relativa alla *privacy* esclusivamente al livello del *private law of torts* ⁶⁹.

La sentenza *Paveisch*, allora, rappresenta solo uno dei tasselli che compone il lento percorso intrapreso dalla giurisprudenza di diritto comune per giungere all'accoglimento di una teoria positiva e *constitutionally oriented* del *right to privacy*, basata sulla "riscoperta" del contributo di Warren e Brandeis.

Lo stesso lento percorso interessò, peraltro, anche la giurisprudenza costituzionale, che solo nel secondo dopoguerra – come ampiamente vedremo – avrebbe sancito, attraverso il definitivo superamento dei precedenti ancorati alla regola del *physical trespass*, l'inquadramento nella gerarchia dei valori costituzionali della "vita privata"⁷⁰.

Sebbene la presidenza Roosevelt iniziata nel 1933, e ancor più l'avvento del *New Deal* a partire dal 1937, avessero avviato la definitiva crisi del paradigma proprietario e promosso una vera e propria "rivoluzione costituzionale", che vedeva la *Supreme Court* di Washington superare progressivamente i precedenti che garantivano l'assoluta intangibilità del diritto costituzionale di proprietà

⁶⁸ A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 55 ss.

⁶⁹ Sembra riconoscere i limiti di tale impostazione M. C. SLOUGH, *Privacy, Freedom and Responsibility*, p.28 ss.

⁷⁰ Sul punto, vedi diffusamente A. BALDASSARRE, *Privacy e Costituzione*, cit.; U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 70 ss.; sul tema si tornerà ampiamente *infra*.

privata, portato dunque a mediazione con altri diritti di libertà⁷¹; al contempo quest'ultima, per quanto attiene alla *privacy* nello specifico, nella vicende giurisprudenziali della prima metà del ventesimo secolo continuò a mostrare un attaccamento alle teorie “possessive” o dominicali, e pertanto un’inflexibile adesione al maggioritario orientamento che disconosceva l’esistenza di un diritto costituzionale di *privacy*.

Ciò deve forse imputarsi al clima di elevata conflittualità sociale causato dalla transizione (ancor più repentina dopo la grande depressione del '29 e la “svolta” roosveltiana) da una “società di proprietari” alla “società di massa”, e così dalla vittoria dell’ideologia democratico-pluralista sanzionata nel modello dello Stato parzialmente interventista, mediatore tra le classi e tra i loro principali esponenti, ossia oligopolisti ed organizzazioni sindacali, realizzato proprio dalla presidenza roosveltiana⁷². Tutte le istituzioni pubbliche erano, così, impegnate nel tentativo di garantire l’ordine pubblico e la sicurezza collettiva, e a tale compito partecipava anche la *Supreme Court*: cosicché ad un effettivo allargamento, sul piano politico, della libertà individuale ad una platea sempre più ampia di persone, non più ancorata al privilegio della proprietà privata, faceva contraddittoriamente riscontro un’interpretazione restrittiva del *Bill of Rights* e degli emendamenti costituzionali. In particolare, ad essere pregiudicata continuava ad essere soprattutto la possibile declinazione della libertà personale in termini di “riservatezza”⁷³. In piena epoca proibizionista, essa veniva infatti giudicata dagli

⁷¹ Sul trauma provocato dalla rivoluzione del new deal, cfr. CROWNIN, *La Costituzione degli Stati Uniti nella realtà odierna*, tr. It. di Oriani, Pisa, 1958, p. 182 ss.

⁷² Sulla posizione dello Stato nell’era roosveltiana, cfr. F. MANCINI (a cura di), *L’età di Roosevelt*, Bologna 1962, p. 102 ss.

⁷³ Con l’espressione *United States Bill of Rights*, lo si ricorda, si intende il documento, adottato dal *1st United States Congress* e ratificato in 15 dicembre del 1791, contenente i primi dieci emendamenti alla Costituzione, adottata già nel settembre del 1787 ma entrata in vigore solo il 4 marzo del 1789. In estrema sintesi, primi dieci emendamenti codificano i principi emersi dall’aspro dibattito invalso tra federalisti ed antifederalisti tra il 1787 e il 1788, e segnatamente sanciscono specifici, fondamentali diritti di libertà della persona umana,

esponenti più conservatori della Corte, fiancheggiatori in tal senso delle autorità governative, come strumento potenzialmente utilizzabile dai delinquenti - in primis dunque da sindacalisti rivoluzionari e da criminali mafiosi - per sfuggire all'applicazione della legge e alle *search and seizures*, ossia alle perquisizioni e ai sequestri in presenza di una probabile causa (*probable cause*) di reato compiute dalla polizia statale o federale, su mandato dell'autorità giudiziaria o di propria iniziativa nei casi di particolare urgenza, a scopo di ricerca del mezzo di prova, di repressione e di prevenzione di (ulteriori, almeno in via ipotetica) reati⁷⁴.

Detto ciò, deve peraltro evidenziarsi come la *Supreme Court*, dagli anni Venti fino agli anni Sessanta, in punto di tutela della libertà personale e di riconoscimento costituzionale del *right to privacy*, fosse attraversata da una profonda spaccatura, che ad una maggioranza a sostegno di orientamenti restrittivi e illiberali vedeva contrapporsi una nutrita e autorevole minoranza a difesa della libertà personale, la cui voce avrebbe continuato ad esprimersi nelle *dissenting opinions* fino a rovesciare l'indirizzo vigente e a determinare l'accoglimento di una teoria positiva della *privacy*, come diritto costituzionalmente tutelato (in particolare, nella "penombra" degli altri diritti garantiti dalla costituzione, come limpidamente sintetizza il fondamentale principio enunciato in *Griswold*, sul quale più avanti ci soffermeremo)⁷⁵. In un primo periodo, a comporre tale frangia

innanzitutto quali limiti invalicabili all'esercizio delle funzioni assegnate dalla Costituzione al governo federale. Per un'efficace panoramica storica, cfr. CONGRESSIONAL RESEARCH SERVICE LIBRARY OF CONGRESS, *The Constitution of the United States of America: Analysis and Interpretation, Centennial Edition, Interim Edition: Analysis of Cases Decided by the Supreme Court of the United States to June 26, 2013*, U.S. Government Printing Office, Washington D.C., 2013, p. 1047 ss.

⁷⁴ Vedi ad es. la testimonianza del *Chief Justice* del caso *Olmstead*, su cui subito *infra*, William Taft, che tra i motivi che lo indussero a negare la tutela della *privacy* nel caso suddetto cita espressamente la preoccupazione di non togliere alla polizia preziosi strumenti d'indagine nella lotta a favore del proibizionismo e ai fini della repressione dei reati contro l'ordine pubblico fiorenti in quel tempo: cfr. A. WESTIN, *Privacy and freedom*, cit., p. 340 ss.

⁷⁵ A. BALDASSARRE, in *Privacy e Costituzione*, p. 79, propone una periodizzazione in tre fasi della giurisprudenza della corte fino agli anni Sessanta: la prima fase, che giunge sino agli anni Trenta, caratterizzata da un atteggiamento pienamente conservatore della Corte, teso

progressista furono i giudici Brandeis (coautore del fortunato articolo del 1890), Holmes e Stone; più tardi, con i mutamenti apportati nella composizione della corte, principalmente i giudici Murphy, Warren e soprattutto Douglas, che con le sue *opinions* avrebbe guidato la maggioranza alla scrittura di alcune delle sentenze più rivoluzionarie, in punto di garanzia dei diritti civili, della storia degli Stati Uniti ⁷⁶.

Procedendo per ordine, il caso certamente più importante nella storia della giurisprudenza costituzionale degli anni Trenta per i profili che qui interessano è *Olmstead v. United States*. Nell'ambito di tale controversia, decisa nel 1928, la Corte si fa promotrice di un indirizzo esegetico restrittivo in relazione al Quarto e al Quinto Emendamento, stabilendo a chiare lettere alcune regole di applicazione di questi ultimi che, in relazione quantomeno alla *privacy* individuale, saranno seguite dalla stessa (con poche e generiche aperture) per almeno un trentennio ⁷⁷. Regole che rappresentano soltanto il prodotto della traduzione sul piano costituzionale di tratteggiati principi di *common law*, relativi ai limiti della libertà individuale (ancora incardinata, nella visione della Corte, sul principio della proprietà privata) rispetto ai poteri dell'autorità governativa, e in particolare all'istituto delle *search and seizures*.

a riaffermare i principi tradizionali di *common law* contro ogni interpretazione evolutiva del *Bill of Rights*; la seconda, che si estende ai primi anni del dopo-guerra, in cui la Corte rivela un atteggiamento contraddittorio, mostrando alcune brecce nei propri orientamenti consolidati; la terza, infine, che vede un fiorente sviluppo delle *dissenting opinions* appena ricordate, e vede la Corte, sulla loro scorta, cominciare a minare i propri precedenti, attraverso tuttavia riconoscimenti ancora solo generici del diritto alla privacy: come esempio può citarsi *Wolf v. Colorado*, del 1949. Per un pieno *overruling*, dovranno attendersi gli anni Sessanta e la penna dell'autorevole *Associate Justice* Douglas.

⁷⁶ Si citano solo, a titolo di esempio, il fondamentale caso *Griswold v. Connecticut*, ritenuto il primo in cui la Corte abbia riconosciuto l'esistenza di un diritto costituzionalmente tutelato di privacy; il caso *Roe v. Wade* del 1973; il caso *Lawrence v. Texas* del 2003: per una panoramica su queste vicende giurisprudenziali e sulla loro portata innovativa in punto di privacy, v. subito *infra*.

⁷⁷ Cfr. *Olmstead v. United States*, 277, U.S. (1928)

Descrivendo brevemente il contesto normativo di riferimento, bisogna ricordare che il Quarto Emendamento contiene le disposizioni costituzionali che stabiliscono la disciplina fondamentale dei rapporti fra la libertà del singolo e l'intervento dei pubblici poteri nel campo della libertà personale e del domicilio, considerato da numerosi precedenti come fondamento della legittimità, e dei relativi limiti, delle perquisizioni e dei sequestri compiuti dalle autorità preposte alle attività di polizia (appunto, le c.d. *search and seizures*)⁷⁸. Il Quinto, invece prevede espressamente il privilegio contro l'autoincriminazione, inteso restrittivamente dalla giurisprudenza tradizionale maturata fino a quegli anni come mero privilegio di tacere, e non come assoluto diritto sostanziale al silenzio⁷⁹.

Il caso in esame è particolarmente importante anche sul piano dei fatti, perché ancora una volta evidenzia il legame già lucidamente individuato da Warren e Brandeis, e che il presente lavoro intende scandagliare, tra "invadenza" della tecnica e aspetti più inviolabili dell'intimità personale.

La controversia opponeva infatti il Sig. Olmstead, capo di una grande organizzazione criminale dedita all'importazione e allo spaccio clandestino di liquori (in violazione del *National Prohibition Act*), e il Governo degli Stati Uniti, che per mezzo di un esperto aveva applicato dei captatori sulle parti esterne della linea telefonica installata nell'ufficio del primo al fine di intercettarne le conversazioni: intercettazioni che avevano costituito la base probatoria principale per il rinvio a giudizio dell'indagato e per la sua successiva condanna in primo grado e in Appello. La Corte, adita da Olmstead con il rituale *writ of certiorari*,

⁷⁸ Promulgato nel 1790 come parte del *Bill of Rights*, il Quarto Emendamento così dispone « *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*».

⁷⁹ Cfr. ad es. *Boyd v. United States*, 112, 6, U.S., 116 (1886)

era chiamata a giudicare se la produzione come prove in giudizio di conversazioni telefoniche private, intercettate per mezzo di un apparecchio applicato al filo, costituisse violazione del Quarto e del Quinto Emendamento.

Ebbene la Corte, anzitutto, riafferma rigidamente la regola tradizionale del *physical trespass* di *common law*, secondo la quale solo nel caso di interferenza *materiale* (cioè esplicantesi su un oggetto fisicamente tangibile) nella proprietà o nel domicilio o nella sfera personale può individuarsi una violazione del diritto – costituzionalmente tutelato dalla disposizione in questione – alla libertà personale. Nel far ciò, essa trascura le stesse aperture contenute in *Boyd* che pur questa regola riproduceva e specificava in relazione alle *search and seizures*, ed ovviamente la stessa interpretazione evolutiva fornita a suo tempo da Warren e Brandeis. Su tali presupposti, la Corte afferma dunque la legittimità delle prove raccolte nei modi suddetti, e più in generale rigetta recisamente la prospettazione della *privacy* come diritto a sé stante costituzionalmente garantito da una delle disposizioni vigenti e dai precedenti che le interpretano in funzione applicativa⁸⁰.

Tuttavia, nelle *dissenting opinions* del caso emerge una decisa rottura con la tradizione: su tutte, a brillare è il *dissent* di Louis Brandeis, ormai giudice costituzionale, fra i più riusciti in tutta la lunga storia delle motivazioni apparse nella giurisprudenza della *Supreme Court*⁸¹. L'illustre giurista, sviluppando i temi già trent'anni prima svolti nel saggio scritto a quattro mani con Samuel Warren, afferma che «il tempo produce cambiamenti (...) porta ad esistenza nuove condizioni e nuove finalità», e segnatamente determina la nascita di nuove tecnologie, sempre più sottili e invasive per la *privacy* individuale, ancor più temibili se al servizio del potere politico (anche a fin di bene), come nel caso in questione. Ciò deve indurre dunque l'interprete a determinare il significato delle

⁸⁰ Cfr. *Olmstead v. United States*, 277, U. S. 457 ss. (1928)

⁸¹ Cfr. BRANDEIS, «Dissenting Opinion», in *Olmstead v. United States*, 277, U. S., p. 472 ss.

parole delle stesse disposizioni costituzionali in dipendenza dei mutamenti storici, e dunque alla luce di un criterio, ancora una volta, *evolutivo*; e questo discorso, a fronte dei sempre più sofisticati strumenti di scandaglio della personalità umana («*subtler and more far reaching means of invading privacy*» è l'efficace e lungimirante espressione utilizzata dal giudice), riguarda in primis le disposizioni che disciplinano i rapporti tra libertà individuale e pubblica autorità, tra interesse dello Stato alla sicurezza collettiva, la cui realizzazione viene perseguita in primo luogo attraverso le attività di polizia, e interesse dell'individuo a salvaguardare la propria libertà personale⁸². Alla luce di tutte queste considerazioni, Brandeis afferma allora che la risposta più corretta alle crescenti esigenze di tutela dell'inviolabilità della sfera privata sia proprio l'interpretazione del Quarto e del Quinto Emendamento come legittimo fondamento costituzionale di un diritto di *privacy* individuale, rivolto a tutelare il nucleo più intimo della personalità umana. Disposizioni che risulterebbero dunque violate, assieme al diritto cui garantiscono tutela, a fronte di qualsiasi tipo di intrusione ingiustificabile nella sfera privata: qualunque sia il mezzo, qualunque sia il fine e soprattutto qualunque sia l'oggetto "colpito" dall'intrusione medesima e dunque portato a conoscenza di terzi, anche (a maggior ragione, verrebbe da dire) laddove fosse semplicemente "immateriale", come un pensiero oralmente espresso⁸³.

L'affermazione di Brandeis nel contesto in esame ha un peso ancora maggiore di quella contenuta nel famoso saggio del 1890. Egli, in quanto giudice della Corte Suprema, può finalmente collocare la problematica del diritto in questione sul piano che le è proprio: non più quello dei rapporti interindividuali, bensì quello del diritto costituzionale, nell'ambito del quale l'interesse in

⁸² Ivi, p. 473 ss. Quasi profetico, se si pensa alle attuali tecniche di profilazione algoritmica implementate dal connubio tra informatica e neuroscienze, il passaggio in cui esplicitamente afferma che «*advances in psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions*».

⁸³ Ivi, p. 478.

questione assume un valore più ampio, “politico”, ossia correlato alla struttura globale della società. E tale interesse, conoscendo tutela innanzitutto nei confronti dei pubblici poteri, può più facilmente “irradiarsi” quale bene giuridico autonomamente presidiato da un autonomo diritto soggettivo nell’ambito dei rapporti individuali disciplinati dal *common law* (nel cui ambito fa dunque ingresso un diritto costituzionalmente tutelato)⁸⁴.

Conviene subito evidenziare che l’eredità della *dissenting opinion* in questione sarà considerevole: rappresenterà la base di tutti i successivi *dissents* della minoranza *liberal* in senso alla Corte Suprema; delle limitate aperture di quest’ultima negli anni Cinquanta al “riconoscimento generico” di un diritto di *privacy*; e dell’esplicita, circostanziata affermazione da parte del giudice Douglas del diritto costituzionale di *privacy* nel caso *Griswold v. Connecticut* del 1968.

1.1.2. Una parentesi: “*Law in the Making*”, dinamismo culturale e prospettive dottrinali sulla *privacy* tra primo e secondo Novecento

Alla luce di quanto detto nel paragrafo precedente, a breve si procederà ad una sintetica rassegna della giurisprudenza che dagli anni Sessanta ha affermato i principi tutt’ora validi su cui si fonda il riconoscimento costituzionale del diritto alla *privacy* statunitense, e successivamente ad un essenziale quadro della legislazione federale dagli Settanta fiorita in materia, con il progressivo delinearsi di un c.d. modello settoriale di tutela della *privacy* (articolato oggi sul doppio binario federale-statale).

Prima, tuttavia, partendo dalle considerazioni appena svolte, è bene rivolgerci, una volta per tutte, ad uno degli strumenti metodologici più utili per

⁸⁴ A. BALDASSARRE, *Privacy e Costituzione*, cit., pp. 104, 105.

studiare l'ordinamento angloamericano, e in particolare per tracciare la fisionomia del "modello" di *privacy* progressivamente affermatosi nel contesto in esame: strumento che, lo si anticipa, consente di cogliere nitidamente il carattere "evolutivo" di tale modello, e dunque la corrispondenza biunivoca di cui poco fa si parlava. Mi riferisco a quel dato "fotografato" dall'espressione coniata da Carleton Kamp Allen, e che ha dato il nome ad un popolare saggio dall'autore pubblicato nel 1927: "*Law in the Making*"⁸⁵.

Quest'ultimo è concetto che da una parte, contrapposto al *Law in the Books*, indica un approccio alternativo al formalismo tipico del *civil law* continentale, fondato sulla corrispondenza tra diritto e volontà positiva del legislatore, e dunque individua uno dei connotati tipici dei sistemi giuridici di *common law*, ossia la natura di fonte del diritto esplicitamente riconosciuta alla giurisprudenza⁸⁶. Dall'altra, ed è questo il significato che più interessa ai presenti fini, *Law in the Making* è espressione che individua il carattere fluido, provvisorio, cangiante dell'esperienza giuridica: è dunque un concetto che, identificando il *diritto* come *processo*, riflette lo stesso approccio evolutivo coltivato da Warren e Brandeis nella loro opera di fondazione giuridica della *privacy*, e invita pertanto a studiare il diritto così come esso concretamente evolve e si sviluppa nel corso del tempo⁸⁷. Tale *prospettiva* prevalentemente *diacronica* sul fenomeno giuridico impone allora di concentrarsi sul processo, appunto, di trasformazione dei problemi giuridicamente rilevanti, e conseguentemente delle soluzioni normative adottate e degli istituti vigenti, e quindi delle risposte elaborate dal diritto, nei diversi periodi storici considerati; e di individuare le tendenze e le ragioni che alla base

⁸⁵ Cfr. C. K. ALLEN, *Law in the Making*, Clarendon Press, Oxford 1955; e U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 65 ss., che nel volume in questione offre una descrizione compiuta del concetto e torna spesso sulle sue possibili declinazioni.

⁸⁶ Per più analitiche, sebbene sintetiche, considerazioni, e per i riferimenti bibliografici in materia, v. nota 30.

⁸⁷ U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 66.

di tali trasformazioni si collocano. Se, allora, negli ordinamenti di *civil law* queste ultime vanno ricondotte al diritto positivo, come fonte -scritta- di legittimità delle decisioni giudiziarie e dunque del *diritto vivente*, nei sistemi di *common law*, come quello angloamericano (e qui sta il dato più importante), stante la fisiologica funzione di produzione normativa riconosciuta alla giurisprudenza, l'evoluzione dei concetti giuridici e del diritto oggettivo sono da imputarsi all'opera incessante con cui i giudici filtrano tutta l'instabile, mutevole serie di fattispecie concrete sottoposte al loro scrutinio alla luce dei principi fondamentali dell'ordinamento, raccordando a questi ultimi tanto gli *statutes*, statali e federali, quanto i precedenti che compongono il diritto comune e il diritto costituzionale⁸⁸. Principi che, a loro volta, e questo specialmente nel contesto nordamericano, sono interpretati alla luce del paradigma culturale e dei valori prevalenti nella dialettica che, in ciascun periodo storico di riferimento, si dipana in seno alla società: le vicende riguardanti i primi trent'anni dell'istituto americano della *privacy* sono emblematiche a riguardo⁸⁹.

La tendenza appena descritta risulta evidente se si guarda al paradigmatico caso *statunitense* della *privacy*: la nozione in questione, a partire dalla iniziale rielaborazione in chiave autonoma e negativa di Warren e Brandeis, è stata, a seconda delle teorie succedutesi, ampliata, rimodulata, sviluppata per rispondere ad esigenze insussistenti, e insieme difficilmente immaginabili, a fine Ottocento. Così, dall'iniziale definizione si è giunti ad una pletora di concetti derivanti dal contributo di giurisprudenza, *statutes* e soprattutto dottrina, che la prima e i secondi da sempre influenza; concetti spesso incoerenti tra di loro. Ciò tuttavia

⁸⁸ Ivi, p. 66 ss.

⁸⁹ CH. F. ABERNATHY, «Defining Privacy: The Power of culture in the Digital Age», in *Privacy digitale. Giuristi e informatici a confronto*, (a cura di) F. BERGADANO, A. MANTELERO, G. RUFFO, G. SARTOR, Giappichelli, 2006

non ha fatto altro che realizzare il fine implicito nell'approccio genetico-evolutivo propugnato dai due "padri" dell'istituto: non già definire l'essenza immutabile di un concetto mutevole, come mutevoli sono tutti i fenomeni istituzionali sottostanti ai primi, a cominciare dall'ordinamento giuridico⁹⁰; bensì delineare i tratti di un dispositivo di protezione capace di adattarsi alle sempre nuove esigenze del corpo sociale, prima di tutto determinate dai *mirabilia* della tecnologia. Dispositivo la cui estensione e il cui contenuto, conformemente all'evoluzione intervenuta, sempre dovrà essere periodicamente ridefinito; ma che consentirà ai consociati di godere di uno strumento elastico ed efficiente, sensibile rispetto ai sempre nuovi bisogni scaturiti dalle insidie della tecnica. Ieri, le macchine fotografiche Kodak; oggi, gli algoritmi e le reti neurali artificiali.

Addentrandoci un poco più nel dettaglio nel contesto statunitense, questo dinamismo del sostrato culturale, e conseguentemente della sovrastruttura giuridica, in punto di *privacy* si riflette innanzitutto nell'ipertrofia della giurisprudenza di diritto comune che dal famoso caso *Paveisch* ha richiamato a vario titolo il *right to privacy* come fondamento delle proprie decisioni. Se, come abbiamo già ricordato (ed è un punto molto importante), Prosser ha correttamente evidenziato che solo in pochissimi casi il *thema decidendum* attenesse in senso stretto alla protezione della sfera privata, resta il fatto che le corti di *common law*, nelle circa trecento controversie "originali" decise nella prima metà del Novecento cui l'autore fa riferimento, hanno fatto espressa menzione dell'istituto della *privacy*, pur richiamando sotto tali spoglie attributi della personalità già

⁹⁰ Sulla concezione di ordinamento giuridico quale istituzione sociale, prima ancora che normativa, cosicché *ubi societas, ibi ius*, e dunque sulla c.d. teoria istituzionalistica del diritto v. l'opera capitale di S. ROMANO, *L'ordinamento giuridico*, Sansoni, Firenze 1946 (prima ed. 1918), in particolare p. 16 e ss.; significativo ai presenti fini il passo cristallino a p. 29, che recita: «(...) Il diritto, prima di essere norma, prima di concernere un semplice rapporto o una serie di rapporti sociali, è organizzazione, struttura, posizione della stessa società in cui si svolge e che essa costituisce come unità, come ente per sé stante».

storicamente tutelati, nell'ambito del *right to property* o come oggetto di autonomi "diritti della personalità", in seno al diritto comune⁹¹. E che tale reticolo di riferimento giurisprudenziali ha certamente inciso, quanto meno sul piano del *common law*, sulla concezione della *privacy* quale interesse meritevole di tutela; sul dibattito intorno all'esistenza e alla latitudine di un autonomo diritto a presidio del medesimo; e prima ancora sull'accoglimento e sul progressivo affinamento di una concezione della violazione della *privacy* quale autonoma categoria di *tort*, già propugnata dai due avvocati di Boston. Lo dimostra il fatto che l'indirizzo giurisprudenziale emerso da queste sentenze sarebbe stato consolidato dall'*American Law Institute* nell'edizione del *Restatement of Torts* del 1939⁹²; e che lo stesso Prosser sulla loro base ha potuto individuare quattro "tipologie" di interessi dalla giurisprudenza della prima metà di secolo ricondotti al concetto di *privacy*, e conseguentemente proporre una quadripartizione delle fattispecie di *torts* (e dunque di responsabilità civile) ascrivibili alla composita categoria della lesione della *privacy*: *inclusion upon seclusion*, *public disclosure of private facts*, *false light in public eye* e *appropriation*⁹³. Nonostante altra dottrina abbia immediatamente criticato la concezione di *privacy* quale *cluster of rights*, sostenendo un'interpretazione invero più moderna dell'istituto quale diritto unitario, in quanto la *privacy*, come sintesi di tutti i suddetti interessi, rappresenterebbe un preciso aspetto della *human dignity*, la quadripartizione di Prosser sarà integralmente recepita nell'edizione del *Restatement of Torts* del

⁹¹ W. L. PROSSER, «Privacy, a legal analysis», cit. p. 386 ss; v. anche *supra*, nota 58.

⁹² Cfr. U.M. UMBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, CEDAM, Pavia 2005; i *Restatements of the Law* sono una serie di trattati riguardanti diverse materie giuridiche redatti e pubblicati dall'*American Law Institute* al fine di informare gli operatori del diritto statunitense, dai giudici agli avvocati, sui vigenti principi di *common law*: rappresentano dunque, essenzialmente, una rassegna dei precedenti giudiziari, tradizionali e recenti, intervenuti nel settore materiale preso in considerazione. Per una panoramica, cfr. C. BIONDO, «Secondary Sources: ALRs, Encyclopedias, Law Reviews, Restatements, & Treatises», in *Harvard Law School Library*, (a cura di) Deanna, 12/09/23.

⁹³ W. L. PROSSER, «Privacy, a legal analysis», cit., p. 383.

1977, di cui quest'ultimo sarà peraltro curatore; anche se successivamente, a sua volta, sarà superata sulla scorta degli indirizzi dottrinali nel frattempo maturati, a dimostrazione della tendenza evolutiva della cultura giuridica statunitense di cui stiamo discutendo ⁹⁴.

Allo stesso modo, il suddetto dinamismo si riflette nel conflitto tra orientamento tradizionale “*property-centrico*” e *dissenting opinions* maturate in seno alla giurisprudenza della *Supreme Court* di Washington, che ha a sua volta contribuito ad affinare il ragionamento logico, le motivazioni culturali e le argomentazioni giuridiche alla base, rispettivamente, dell'iniziale disconoscimento e del successivo riconoscimento di un diritto costituzionale di *privacy*⁹⁵.

Ma il terreno in cui forse la vivacità dell'esperienza giuridica si manifesta più prepotentemente è proprio quella della dottrina, che a partire dalla fine degli anni Cinquanta sempre più assiduamente si interroga sull'esistenza, sul contenuto e sulla latitudine del *right to privacy*, alimentando un fecondo dibattito, di natura filosofica prima ancora che giuridica, che a propria volta si rifletterà sui

⁹⁴ Sulla *privacy* come aspetto della dignità umana, cfr. E. J. BLOUSTEIN, «Privacy as an aspect of Human Dignity: an answer to Dean Prosser», in *N.Y.U.L. Rev.*, 1964; l'autore si esprime con le seguenti parole: «(...) *the man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity*». Da ciò deriverebbe che i rimedi apprestati a fronte di una violazione della *privacy* dovrebbero essere individuati in analogia a quelli previsti a fronte di *torts* consistenti in minacce, aggressioni e detenzioni illegittime, e non già a quelli previsti per le ipotesi di diffamazione o appropriazione indebita. Su quest'ultimo punto, e anche sull'influenza della teoria della *privacy* di Prosser, nonché sul suo progressivo superamento, cfr. la minuta analisi di M. SURACE, *Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di Internet*, in particolare cap. 2, par. 2.4, consultabile al sito internet <https://www.adir.unifi.it/rivista/2005/surace/cap2.htm>.

⁹⁵ Cfr. A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 78 ss.

mutamenti della giurisprudenza costituzionale e di diritto comune⁹⁶. Infatti, accanto all'originaria teoria privatistica di Warren e Brandeis; a quella, già brevemente citata, di William Prosser, celebre *Dean* della *School of Law* alla *UC Berkeley* dal 1948 al 1961, che grande influenza ebbe nella dottrina degli anni Sessanta; e a quella di Bloustein, che per primo rispose criticamente a Prosser, evidenziando con attitudine notevolmente progressista la relazione stretta tra *privacy* e dignità dell'essere umano; accanto a queste, appunto, si sono susseguite e stratificate fino ai nostri giorni una serie di prospettive teoriche che, sommandosi, hanno composto un panorama fitto e articolato, tutt'ora in espansione. Panorama che taluni giuristi si sono sforzati di ridurre a sistema, proponendo tassonomie ispirate ciascuna a criteri sinottici diversi, tra le quali, ad esempio, spicca per chiarezza quella di Herman T. Tavani⁹⁷. In ogni caso, il suddetto inesausto dibattito ha reso il concetto di *privacy* nell'esperienza giuridica statunitense lontano dalla geometrica razionalità delle definizioni e degli istituti dei sistemi di *civil law*, e piuttosto suscettibile di adattarsi alle pratiche istanze della collettività, e dunque alle più diverse ipotesi di interferenza nella sfera di autodeterminazione del singolo.

Partendo da una prospettiva diacronica, procediamo allora ad un sintetico quadro delle teorie che animavano il dibattito americano degli anni Sessanta, e di

⁹⁶ Sulla rassegna che seguirà, cfr. specialmente U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 40 ss.; M. SURACE, *Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di internet*, cit., cap. 2.

⁹⁷ H. T. TAVANI, «Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy», in *Metaphilosophy*, 2007, p.4; l'autore propone una suddivisione delle "scuole" in quattro gruppi, incentrati ciascuno rispettivamente sulle nozioni di (privacy come) "non intrusione", "esclusione", "limitazione" e "controllo"; e contestualmente, criticando le suddette teorie, propone una propria nozione di privacy come *restricted access/limited control*, su cui v. *infra*. Altra diffusa classificazione, sempre a titolo di esempio, è quella proposta da D. JOHNSON, H. NISSENABUM, *Computers, Ethics and Social Values*, Prentice Hall, Englewood Cliffs, 1995, che si fonda sulla divisione delle teorie in due fondamentali macro-gruppi.

alcune tra le più importanti succedutesi fino ad oggi, premettendo che le definizioni sembrano non tanto aver lo scopo di *esaurire*, bensì quello più prammatico di *illustrare* alcune caratteristiche del prismatico istituto con cui si confrontano.

Tralasciando, appunto, la visione di Prosser, e la puntuale critica svolta da Bloustein, entrambe già ricordate, una delle prime e più moderne definizioni della *privacy* proviene da Alan F. Westin, che nel suo già più volte citato *Privacy and Freedom* per la prima volta illumina la dimensione positiva dell'istituto rielaborato da Warren e Brandeis: non più (soltanto) libertà (negativa) di essere lasciati "indisturbati" o di escludere chiunque dalla conoscenza dei fatti relativi alla propria sfera privata, personale e familiare, e così di rendersi completamente inaccessibili agli altri; bensì (anche) libertà (attiva) di esercitare un controllo sulle proprie informazioni⁹⁸. Non più, soltanto, solitudine e segretezza; bensì, anche, controllo: concetto che esalta il momento della scelta personale dell'individuo. La tesi in questione sarà ripresa e sviluppata da altra autorevole dottrina negli anni Novanta⁹⁹. Ma i più attenti studiosi noteranno come la teoria in questione non chiarisca il tipo di informazione oggetto del controllo, né tantomeno la natura del potere di controllo garantito all'individuo: confondendosi *privacy* ed autonomia, è facile infatti cadere nell'errore iperbolico di identificare il consenso quale condizione sempre sufficiente, oltre che necessaria, ai fini del "rispetto" della

⁹⁸ Cfr. A. F. WESTIN, *Privacy and Freedom*, cit., che a p. 7 scrive: «*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*». Alla stessa prospettiva teorica in questione si può ricondurre anche il contributo dell'illustre giurista A. R. MILLER, *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Cambridge, 1971; quest'ultimo sarà tuttavia trattato *infra*, per sottolinearne l'importanza nel percorso di individuazione della dimensione (anche) sociale della *privacy*.

⁹⁹ C. FRIED, «Privacy: A Rational Context», in *Computers, Ethics and Society*, cit., p. 54.

privacy (e segnatamente, per il modo in cui oggi si pone dogmaticamente il problema, di liceità del trattamento dei dati personali)¹⁰⁰.

Successivamente, nel dibattito che andiamo ricostruendo è fiorita un'altra fortunata tesi, che identifica il contenuto del diritto alla *privacy* con il potere di limitare o restringere l'accesso all'informazione su di sé: identificandosi *privacy* e segretezza, la condizione ideale sussisterebbe quando “nessuno ha informazioni su un soggetto determinato”¹⁰¹. Tuttavia, questo approccio scontrerebbe il grave limite di trascurare il ruolo che l'autodeterminazione svolge nel processo di costruzione intima e di rappresentazione esteriore della propria sfera privata, al contrario esaltato dalla nozione di *privacy* come “controllo”. Se la prima, dunque, difetta di una riflessione sulla possibile insufficienza della volontà individuale a giustificare l'“intrusione” nella vita privata, la seconda manca di considerare l'essenziale rilievo che ai fini della piena esplicazione della libertà morale dell'individuo assume la possibilità, giuridicamente garantita, di decidere chi ammettere o meno alla conoscenza di una informazione che lo riguardi¹⁰².

Per ovviare ai limiti propri di ciascuna delle teorie fin ora richiamate, partendo da queste ultime lo stesso Tavani ha proposto all'alba del nuovo millennio una teoria “unificata” della *privacy*, come “accesso ristretto e controllo limitato”, a sua volta ispirata alle ricerche condotte da James Moor¹⁰³. La *privacy*

¹⁰⁰ Cfr. H. T. TAVANI. «Philosophical Theories of Privacy», cit.; oggi, il problema si declina nello specifico in relazione al rispetto dei requisiti di libertà, consapevolezza e specificità del consenso, nonché alla garanzia del principio di minimizzazione dei dati e di limitazione delle finalità che, almeno nel contesto europeo, informano la disciplina del trattamento dei dati personali, in quanto essenziali per garantire una piena tutela della libertà di «autodeterminazione informativa» dell'individuo: v. *infra*, cap. 2.

¹⁰¹ La citazione è di una delle principali fautrici della teoria, A. ALLEN, *Uneasy Access: Privacy for Women in a Free Society*, Rowman and Littlefield, Totowa, N.J., 1988, p. 269; l'elaborazione della tesi sembra invece da tributarsi a R. GAVISON, «Privacy and the Limits of the Law», in *Yale Law Journal*, 89, 1980.

¹⁰² Cfr. H.T.TAVANI, «Philosophical Theories of Privacy», cit.

¹⁰³ Cfr. J. H. MOOR, «Towards a Theory of Privacy in the Information Age», in *Computers and Society*, 27, 3, 1997; a p. 30, l'autore sembra instaurare un parallelismo tra

viene da Tavani intesa allora come protezione integrale a fronte di una determinata situazione, alla luce delle sue specificità, in modo che sia possibile per l'interessato graduare il controllo sull'informazione che lo riguarda attraverso il consenso, la scelta (del trattamento da autorizzare e delle sue finalità) e la revoca del primo¹⁰⁴. Tuttavia, dal punto di vista filosofico la tesi in questione lascia irrisolta l'atavica, cruciale questione su cui il moderno giurista è tenuto ad interrogarsi: ovverosia se la *privacy* abbia o meno valore in sé e per sé, e dunque se la stessa rappresenti un bene giuridico presidiato da un autonomo diritto soggettivo, costituzionalmente fondato, o se piuttosto non sia che un interesse ricondotto nell'ambito di tutela disegnato da taluno dei diritti di libertà riconosciuti, negli Stati Uniti, dal *Bill of Rights*. E ciò, soprattutto, con riguardo alla dimensione positiva della stessa (dal momento che, come sappiamo, seppur nei soli termini di una libertà negativa, già la teoria di Warren e Brandeis riconosceva la *privacy* come presupposto sostanziale dell'autonomo *right to be let alone*).

Per concludere l'affresco, occorre allora quantomeno accennare alla più recente teoria che a partire dagli anni Dieci del nostro secolo è venuta a delinearsi negli ambienti dell'Università di Oxford, e che particolare eco ha avuto nel contesto americano. Mi riferisco alla "teoria informazionale" sviluppata da Luciano Floridi nel quadro della *Filosofia dell'Informazione*, moderna branca della filosofia che lo stesso Floridi ha concorso a delineare, e che muove dall'assunto secondo cui, interpolando la nota sentenza hegeliana, «tutto ciò che è reale è informazionale, e tutto ciò che è informazionale è reale»¹⁰⁵. Alla luce di

privacy e situazione in cui un individuo è protetto "dall'intrusione, dall'interferenza o dall'accesso alle informazioni da parte di altri".

¹⁰⁴ H. T. TAVANI, «Philosophical Theories of Privacy», cit., p. 11 ss.

¹⁰⁵ Cfr. uno dei molteplici testi in cui l'autore espone i principi della filosofia dell'informazione, L. FLORIDI, *The Fourth Revolution: How Infosphere is Reshaping Human Reality*, cit., in particolare p. 4 ss.; per una breve disamina di quest'ultima disciplina, alla cui luce numerosi studiosi ritengono opportuno rileggere tanto i problemi legati alla *privacy* e alla

ciò, Floridi concepisce la *privacy* come pretesa di immunità da cambiamenti sconosciuti, indesiderati o non intenzionali dell'identità personale (quale processo in costante sviluppo) intesa come entità informazionale: ogni forma di indesiderata invasione della sfera privata dell'individuo non è allora che un'indebita alterazione del suo (informazionale, appunto) fondamento ontologico, della sua natura informativa, e pertanto della sua dignità¹⁰⁶. La tesi in questione, seppur, su un piano filosofico, di ispirazione prevalentemente analitica, ha il merito di affermare icasticamente la natura di autonomo diritto fondamentale della *privacy*, e segnatamente della sua “declinazione” positiva, quale (diritto di) libertà di gestire il flusso di informazioni, in entrata e in uscita, relative alla propria persona: quella declinazione che in ambito americano è ormai identificata come “*data privacy*”, a cui si lega la disciplina della c.d. *data protection*; e che riecheggia le sembianze di quel diritto fondamentale, sancito nel contesto europeo dalla nota sentenza del Tribunale Federale Costituzionale tedesco del 1983 sulla scorta di una lunga e transnazionale elaborazione dottrinale, definito come diritto all'autodeterminazione informativa, successivamente identificato tanto a livello comunitario quanto a livello nazionale con la più nota formula “diritto alla protezione dei dati personali”¹⁰⁷.

data protection quanto le soluzioni normative adottate anche in contesto europeo, rinvio al par. 3.

¹⁰⁶ Cfr. L. FLORIDI, «Four Challenges for a Theory of Informational Privacy», in *Ethics and Information Technology*, 2006, 8.3, 109-119; Floridi, nell'evidenziare la corrispondenza tra natura informativa dell'essere umano e nucleo essenziale della sua persona, e dunque dignità, rinvia a E.J.BLOUSTEIN, «Privacy as an aspect of Human Dignity», citato sopra.

¹⁰⁷ Ci si riferisce alla nota «decisione sul censimento» del *Bundesverfassungsgericht*, 15-12-1983, in *Entscheidungen des Bundesverfassungsgericht*, 1984, 65, p 1-71; su quest'ultima e su tutto il dibattito dottrinale e giurisprudenziale negli ordinamenti di *civil law* europei relativo all'esistenza e al fondamento costituzionale del diritto alla *privacy* e di un autonomo diritto alla protezione dei dati personali, v. a breve par. 2.

Partendo da tutte le considerazioni svolte fino ad ora, se si adotta allora la prospettiva di *Law in the Making* precedentemente descritta, la quale esalterebbe il carattere non già geometrico e razionale, bensì caotico ed esperienziale del *common law* in generale e ancor più densamente di quello americano, è possibile evidenziare nitidamente uno dei principali elementi strutturali del modello “americano” della *privacy*: ovverosia, come già anticipato, la natura *evolutiva* del modello. Quest’ultimo non consiste in una teoria generale, completa e coerente, definita in astratto e dalla quale poi dedurre sistematicamente, in particolare in sede giurisdizionale, le possibili applicazioni ai casi emersi nell’esperienza concreta. Piuttosto, esso si caratterizza per il fatto che «l’insieme dei concetti etichettati come *privacy* [costituisce il] (...) riflesso (...) della cultura e dei valori americani, un insieme, cioè, di valori e scelti dominanti ancorché incoerenti che riflettono le tendenze sulle appropriate regolazioni sociali», nel momento storico considerato¹⁰⁸. Sotto una sola etichetta, allora, sono ricondotti una pluralità di concetti, ciascuno dei quali riflette talune delle tendenze esistenti nella cultura e nella società americana in un determinato momento storico: questo appare il *proprium* del modello americano della *privacy*, e la base del suo successivo sviluppo per mezzo di interventi statutari (e, ancora, giudiziari) di tipo settoriale¹⁰⁹.

Seguendo le autorevoli indicazioni di metodo che nel paragrafo abbiamo richiamato, possiamo ora riprendere il discorso sul riconoscimento nella giurisprudenza costituzionale statunitense dell’esistenza di un diritto alla *privacy* costituzionalmente fondato.

¹⁰⁸ Cfr. CH. F. ABERNATHY, «Defining Privacy: The Power of culture in the Digital Age», in *Privacy digitale. Giuristi e informatici a confronto*, (a cura di) F. BERGADANO, A. MANTELERO, G. RUFFO, G. SARTOR, Giappichelli, 2006.

¹⁰⁹ Sulla natura e sulle ragioni del modello americano di tutela della *privacy*, v. ampiamente *infra*, cap. 4.

1.1.3. «*Privacy as an aspect of human dignity*»: l'evoluzione della dottrina e della giurisprudenza costituzionale fino ai casi *Griswold* e *Katz*

Continuando a seguire un itinerario cronologicamente orientato, occorre partire appunto dalle vicende che hanno interessato la *Supreme Court* di Washington. Come abbiamo già detto in sede di analisi del caso *Olmstead*, fino al secondo dopoguerra la Corte, pur attraversata da una profonda spaccatura e “scossa” a suon di *dissents*, resta fondamentalmente ancorata alla regola tralatizia di *common law* incentrata sul *trespass* e ribadita in *Olmstead*: in tal modo, di fatto, continuando ad avallare l'orientamento tradizionale della giurisprudenza delle corti federali inferiori e di quelle statali¹¹⁰. Il lento ma inesorabile cammino con cui la Corte procede al riconoscimento del fondamento costituzionale del diritto alla *privacy* inizia, in senso proprio, negli anni Quaranta, attraverso una serie di pronunce che incrinano l'orientamento tradizionale in cui la stessa principia ad ammettere la rilevanza costituzionale della *privacy* come autonomo bene

¹¹⁰ Cfr. ad es. *Goldestein v. United States*, 316 U. S. 114 (1942); *Schwartz v. Texas*, 344, U. S. 199 (1952); e soprattutto *Goldmann v. United States*, 316, U. S. 129 (1942), in cui la Supreme Court estende al campo delle microspie gli stessi principi enunciati in *Olmstead* con riguardo alle intercettazioni a mezzo *wire tapping*. Ciononostante, l'incrinatura nell'orientamento illiberale maggioritario appare aprirsi sin dalla promulgazione del *Federal Communications Act* del 1934, adottato dalla presidenza Roosevelt in risposta alla sentenza *Olmstead*: in una serie di casi successivi, come il celebre *Nardone v. United States*, 308 U. S. (1937), la Corte sembra infatti promuovere un'interpretazione garantistica delle disposizioni costituzionali sulla libertà personale, sentenziando ad es. che l'espressione “qualsiasi persona” contenuta nel suddetto non esenti l'agente federale dal divieto di intercettare in qualsiasi forma le comunicazioni tra due o più persone espresso nell'atto; o sostenendo l'inammissibilità delle prove illecite. Tuttavia, l'orientamento in questione (pur tornando a manifestarsi in alcune pronunce dei primi anni Cinquanta), sarà sconfessato nei giudizi immediatamente successivi, come quelli ad inizio nota citate, a dimostrare la tenace resistenza dell'orientamento tradizionale; e in ogni caso, nota SLOUGH, *Privacy, Freedom and Responsibility*, cit., p. 259 che esso è sempre rimasto lettera morta presso le corti statali. Il caso *On Lee v. United States*, 343 U. S. 747 (1952) è invece considerato dalla dottrina l'ultimo in cui la Corte Suprema ribadisca la regola del *trespass* nella *search situation*, e dunque l'identità tra *privacy* e proprietà privata, senza sfumature: cfr. ad es. A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 133 ss.

giuridico, distinto dalla proprietà privata¹¹¹. A cavallo tra questo periodo e l'inizio degli anni Cinquanta, poi, si pongono basi ancor più solide per il successivo ineluttabile *revirement*: fondamentali sono i casi *Wolf*, *Irvine* e *Rochin*, tutti riguardanti la legittimità dell'introduzione nel giudizio penale di prove ottenute in violazione delle garanzie costituzionali previste dal Quarto Emendamento, nei quali esplicitamente la Corte nelle sue motivazioni ascrive all'ambito di tutela disegnato da quest'ultimo il diritto alla *privacy*, designandolo come uno dei valori fondamentali della civiltà occidentale¹¹². Sebbene poi tali principi siano contraddetti dal tenore ancora "illiberale" delle decisioni, appaiono evidenti i primi segni di rottura con la dottrina tradizionale della *privacy-property* e l'assunzione di una posizione interlocutoria rispetto alla teoria costituzionale della *privacy*.

Ma il contributo forse più importante per la definitiva spallata all'orientamento conservatore e per la successiva affermazione della teoria costituzionale della *privacy*, intesa come diritto fondamentale della persona umana, è dato dal giudice Douglas, che nella sua opinione dissenziente nell'ambito del caso *Public Utilities v. Pollak* traccia una nuova dottrina sul diritto al rispetto della "vita privata", con riguardo tanto al suo contenuto quanto alla sua consistenza giuridica e al suo fondamento costituzionale, articolando forse la più moderna e puntuale difesa della *privacy* fino a quel momento intervenuta¹¹³.

¹¹¹ Emblematico è il caso *West Virginia State Board of Education v. Barnette*, 319 U.S. 624 (1943), in cui la Corte mostra con incertezza di aprirsi alla possibilità di riconoscere una qualche rilevanza costituzionale all'inviolabilità della sfera privata, attraverso il riconoscimento del *right to silence*, seppure declinato (nel caso di specie) come libertà di astenersi dal manifestare il proprio pensiero con riguardo alla (o a causa della) propria fede religiosa.

¹¹² Cfr. *Wolf v. Colorado*, 338, U.S. 25 (1949); a p. 27 la Corte si esprime in tal modo: "The security of one's *privacy* against arbitrary intrusion by the police – which is at core of the Fourth Amendment – is basic to the free society. It is therefore implicit in the concept of ordered liberty, and as such enforceable against the States through the *Due Process Clause*"; *Rochin v. California*, 324, U. S. 165 (1952); *Irvine v. California*, 347 U. S. 128 (1954).

¹¹³ Cfr. W. O. DOUGLAS, «Dissenting Opinion», in *Public Utilities v. Pollak*, 343, U. S. 467 ss.; la teoria ivi esposta è ribadita nel suo *dissent* nel caso *Irvine v. California*, prima citato.

Discostandosi dai precedenti *dissents* del giudice Frankfurter, in cui il concetto di vita privata resta eccessivamente vago nella sua assimilazione a quel “minimo etico” che deve ritenersi assicurato dalla clausola generale del *Due Process*¹¹⁴, il giudice Douglas afferma innanzitutto che la *privacy* debba essere intesa non già come una generica libertà, bensì come il *principio*, il presupposto indefettibile, di ogni altra libertà, e segnatamente della libertà personale quale capacità di scegliere e di decidere (e dunque, in definitiva, di autodeterminarsi) immuni da condizionamenti: per esprimersi con le incisive parole dell’illustre giurista, che appaiono tanto profetiche quanto quelle scritte poco meno di un ventennio prima da Brandeis nel *dissent* del caso *Olmstead*, «*the right of privacy (...) is a powerful deterrent to anyone who would control men’s mind*»¹¹⁵. Allo stesso tempo, e questo rappresenta l’altro forte pilastro della sua teoria, la *privacy* come autonomo bene giuridico non sarebbe tutelata da una sola disposizione costituzionale: il diritto fondamentale che ne presidia l’integrità sarebbe piuttosto desumibile da una serie di disposizioni riguardanti le libertà fondamentali del cittadino, ovvero il Primo, il Quarto e il Quinto Emendamento¹¹⁶.

Concludendo sul punto, si può affermare che per mezzo del citato *dissent*, l’orientamento (fino ad allora minoritario, ma sempre più forte sul piano argomentativo) a favore dell’esistenza di un diritto costituzionale alla “vita privata” può finalmente poggiare su una teoria solida, capace di rappresentare un’alternativa concreta alla regola del *trespass* ed alla concezione della *privacy-property*, sulla quale far leva per rovesciare l’ormai “scricchiolante” orientamento

¹¹⁴ Cfr. in particolare F. FRANKFURTER, «Dissenting Opinion», in *Irvine v. California*, 347, U. S. 128, p. 142 ss.

¹¹⁵ W. O. DOUGLAS, «Dissenting Opinion», in *Public Utilities v. Pollak*, 343 U. S., p. 469

¹¹⁶ Ivi, p. 467 ss. Da notare che la prospettiva in questione, ripresa nella formula della «penombra delle disposizioni costituzionali», rappresenterà una delle fondamentali teoriche del riconoscimento del diritto costituzionale di *privacy*, in materia di aborto, nel rivoluzionario caso *Griswold v. Connecticut*, in cui l’opinione di Douglas figurerà come la più influente ai fini della decisione. V. *infra*.

tradizionale. E di fatti, a partire dalla fine degli anni Cinquanta ed emblematicamente con il caso *Griswold*, la Corte demolirà definitivamente l'edificio instabile della *privacy-property*, per accogliere la costruzione - cominciata dalle ricordate opinioni dissenzienti - di quello più moderno, duraturo e illuminato della *privacy-dignity*¹¹⁷. Vediamo come.

Potrebbe apparire singolare che il diritto di *privacy*, sebbene non ancora suffragato da una compiuta teoria positiva, faccia effettivamente ingresso nella giurisprudenza costituzionale nell'ambito di una serie di casi relativi alla vita pubblica delle persone e all'interesse - garantito dal Primo Emendamento - ad associarsi liberamente, come diritto a svolgere in comune attività, di natura politica, in forma anonima. Ciò però non stupisce, se si focalizza l'attenzione sulla rivoluzione intervenuta - come molti autori hanno lucidamente colto - negli anni immediatamente successivi al secondo conflitto mondiale, con riferimento all'organizzazione della società civile e alla sua interazione con i pubblici poteri intervenuta. Negli anni in questione, infatti, si afferma definitivamente il modello dello stato pluralistico di massa, con la conseguente disgregazione dei tradizionali rapporti di dominio in una fitta rete di influenze fra gruppi sociali (o corpi intermedi) che a loro volta si istituzionalizzano in senso corporativo, suscitando una dialettica che in special modo contrappone sindacati e grandi gruppi industriali, mediata dai "nuovi" partiti politici di massa¹¹⁸.

Di fronte a questi mutamenti e al connesso, crescente fenomeno dell'associazionismo, lo Stato, per continuare a svolgere il suo ruolo di controllo

¹¹⁷ Cfr. A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 159.

¹¹⁸ Su questi temi e sulle conseguenze della trasformazione dello "Stato lockiano" in "Stato democratico pluralista", cfr. soprattutto C. WRIGHT MILLS, «Società di massa e istruzione liberale», in ID., *Sociologia e Conoscenza*, tr. It. Barghini, Milano 1971, 123 ss.; R. DAHRENDORF, *Classi e conflitto di classe nella società industriale*, Laterza, Bari 1977, p. 336 ss.

pubblico sui rapporti sociali, scivola sempre più verso un regime di “sorveglianza istituzionale”, esercitando un controllo pervasivo sulla struttura interna di partiti e associazioni allo scopo di individuare e contrastare i potenziali “ricettacoli” di sovversione (politica o religiosa). In tale operazione, il governo viene inizialmente fiancheggiato dalla dominante frangia conservatrice della Corte Suprema, che in alcune importanti sentenze nega la segretezza e la riservatezza delle associazioni considerate “sovversive” e dei suoi singoli membri¹¹⁹. Tuttavia, proprio su questo terreno si svolge il passaggio dall’orientamento conservatore a quello liberale, e conseguentemente dal modello della libertà controllata a quello della garanzia universale dei diritti fondamentali, senza più distinzione tra «*cives e dediticii*»: e questo passaggio coinvolge immediatamente l’interesse all’integrità della sfera privata.

Nel primo di una serie di casi riguardanti la N.A.A.C.P. (*National Association for Advancement of Colored People*) risalente al 1958, infatti, la Corte riconosce per la prima volta positivamente un diritto alla *privacy* costituzionalmente garantito nella forma di un c.d. *right of associational privacy*, ossia come diritto delle persone singolarmente considerate di associarsi con la contestuale garanzia della segretezza e della riservatezza del proprio nome¹²⁰. Se il caso aveva ad oggetto la legittimità di una disposizione che imponeva anche a suddetta organizzazione l’obbligo di comunicare la lista dei propri membri e quella dei propri finanziatori, la Corte, applicando restrittivamente la regola del *balancing test*, dà ragione all’associazione attrice, contestando la fondatezza dell’interesse dello Stato di Alabama a controllare l’attività di tale associazione: la Corte, pur non enunciando ancora una teoria compiuta dell’istituto, riprende i

¹¹⁹ Cfr. soprattutto *Viereck v. United States*, 318 U. S. 236 (1943); *Communist Party v. Subversive Activities Control Board*, 367 U. S. 1 (1961)

¹²⁰ Ci si riferisce al caso *N.A.A.C.P. v. Alabama*, 357 U. S. 449 (1958). Il precedente viene poi confermato, in relazione alla stessa associazione, nel caso *Louisiana ex rel. Gremmilon c. N.A.A.C.P.*, 366 U.S. 293 (1961).

rilievi già esposti della teoria di Douglas sulla *privacy* come nucleo essenziale o “clausola implicita” di qualsiasi libertà fondamentale garantita dalla Costituzione, sottolineando la “relazione vitale” esistente tra riservatezza e libertà di espressione e di associazione tutelata dal Primo Emendamento, dal momento che «l’inviolabilità della *privacy* può risultare in molte circostanze *indispensabile* per preservare la libertà di associazione, soprattutto quando un gruppo aderisce ad opinioni dissenzienti»¹²¹.

L’orientamento che colloca il *right to privacy* nell’ambito dei diritti fondamentali, sempre in relazione ad una fattispecie che coinvolge la *freedom of association* tutelata dal Primo Emendamento, viene confermato nel caso *Talley v. California* del 1960, in cui la Corte su tale base dichiara l’incostituzionalità di una legge statale che proibiva la distribuzione di volantini anonimi: la *ratio* del riconoscimento consiste nell’impedire sanzioni o ritorsioni da parte di qualsiasi soggetto, sia questo un’autorità pubblica o un qualunque cittadino che entri eventualmente in possesso di tali informazioni¹²².

Spianata in questo modo la strada, a completare il quadro delle condizioni necessarie ai fini dell’affermazione di una piena teoria costituzionale della *privacy* è probabilmente il subentro nell’organico della *Supreme Court* di taluni giudici (in rapido avvicendamento, Goldberg e Fortas, al posto di Frankfurter) d’ispirazione liberale: da quel momento in poi, sotto l’illuminata presidenza del giudice Warren, in seno alla Corte fiorisce una rigogliosa serie di pronunce particolarmente favorevoli per i diritti di libertà, alla luce di un mutato indirizzo interpretativo del *Bill of Rights*, di natura decisamente più estensiva e progressista¹²³. La *privacy* ne beneficia a trecentosessanta gradi.

¹²¹ Ivi, p. 462.

¹²² Cfr. *Talley v. California*, 362 U.S. 60 (1961)

¹²³ Cfr. A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 248 ss.

Risale allora a quel periodo radioso per i diritti individuali la sentenza che è pacificamente riconosciuta dalla letteratura come la pietra angolare del sistema costituzionale americano della *privacy*: ci riferiamo alla sentenza che decide il famoso caso, fin qui più volte accennato, *Griswold v. Connecticut*, del 1965¹²⁴. Occorre analizzare un poco nel dettaglio il caso, considerata la sua importanza storica, anche sotto un profilo più squisitamente culturale: esso, infatti, appare profondamente collegato ad uno dei fenomeni più delicati del periodo storico considerato, ovvero la rivoluzione sessuale, caratterizzata da una dura contrapposizione tra sostenitori di un diritto costituzionalmente fondato all'interruzione volontaria della gravidanza e "antiabortisti".

Il caso prende spunto da una legge, promulgata nel 1879, con cui lo Stato del Connecticut vietava l'utilizzo di qualsiasi farmaco, dispositivo medico o altro strumento a fini di contraccezione, compresi i profilattici: sebbene raramente applicata, su tale base erano stati arrestati e penalmente condannati un ginecologo della *Yale School of Medicine* ed Estelle Griswold, direttrice del *Planned Parenthood* in Connecticut, che insieme avevano fondato in New Heaven una "*birth control clinic*", ossia una clinica deputata ad offrire consulenza e servizi per la prevenzione della gravidanza e, più in generale, per la pianificazione familiare. La condanna era stata confermata anche dalla Suprema Corte statale, ma la coppia aveva deciso di adire la Corte Suprema di Washington per confutare la legittimità costituzionale dello *statute* in questione alla luce del Quattordicesimo emendamento. Quest'ultimo, bisogna ricordarlo, configura la c.d. *Due Process Clause*, che da sempre è stata interpretata dalla giurisprudenza come valvola attraverso cui imporre ai singoli Stati federati l'osservanza di determinati principi sanciti a livello federale, ma ritenuti universalmente vincolanti in quanto connaturati alle esigenze fondamentali di una società libera e

¹²⁴ Cfr. ampiamente *Griswold v. Connecticut*, 381, U. S. 479 (1965).

civile. Se è vero che, nella storia del diritto americano, il punto più controverso (e tutt'ora oggetto di contrasti) è stato quello della determinazione di tali principi e diritti, sanciti o meno nella Costituzione e nei suoi emendamenti, così universali da rendersi vincolanti per le singole comunità statali, è vero allo stesso tempo che, nel periodo in cui sopravviene il caso *Griswold*, la Corte aveva ormai interpretato la clausola in questione quale “valvola permanente d’ingresso” negli ordinamenti statali di pressoché tutti i diritti previsti dal *Bill of Rights*, nonché di quelli indirettamente garantiti dagli stessi (indirizzo rafforzato dalla dottrina della *penumbra* che andremo ad analizzare)¹²⁵. Come emerge implicitamente dalle motivazioni, la *Supreme Court* nel decidere il caso parte da tale premessa, cui aggiunge un’interpretazione “nuova” della *Due Process Clause*, nei termini di una mera clausola di rinvio rispetto a *tutte* le altre previsioni costituzionali fatte ricadere nel suo ambito, e, come appena ricordato, a tutti i diritti da esse implicitamente desumibili: con ciò rifiutando qualsiasi riferimento ai criteri di *judicial review* rappresentati dal *balancing* o dal *rationality test* tradizionalmente applicati dalla Corte¹²⁶. Pertanto, nell’accogliere siccome fondata la questione di costituzionalità posta dai ricorrenti, la Corte svolge un ragionamento giuridico di più ampio respiro, sfruttando il caso quale pretesto per compiere un fondamentale passo avanti nella configurazione giuridica dell’istituto della *privacy*, e più in generale nella tutela costituzionale dei diritti inviolabili dell’uomo.

Guidata dalla sapiente *opinion* del giudice Douglas, che riprende ed approfondisce la teoria enunciata nel suo prestigioso *dissent* del caso *Public Utilities*, la Corte afferma il famoso e tutt’ora ampiamente influente principio secondo cui, pur mancando (per la *privacy*, così come per molte altre situazioni

¹²⁵ Cfr. sul punto P. G. KAUPER, «Penumbras Peripheries, Emanations, Things fundamental and Things forgotten: the Griswold Case», in *Michigan Law Review*, 1965, vo. 64, p. 235 ss.

¹²⁶ Ivi, pp. 479, 482.

giuridiche a presidio di interessi inerenti alla persona che il mutato contesto storico susciti nel corpo sociale) un esplicito riferimento testuale nella Costituzione, è nella “penombra” configurata dalle garanzie testuali della legge che si stagliano zone in cui “affiorano” ulteriori diritti tutelabili costituzionalmente, a cominciare appunto dal *right to privacy*: quest’ultimo inteso, a maggior ragione, quale presupposto indefettibile per l’esercizio di qualsiasi diritto inviolabile garantito dalla Costituzione¹²⁷. Per quanto attiene, in particolare, alle “*marriage relationships*” (ed invero solo a queste, poiché relazioni che si esprimessero fuori dall’istituto del matrimonio, nella logica dell’*opinion* in parola, non risulterebbero meritevoli di tutela sotto il profilo della riservatezza), il giudice Douglas, nel riepilogare i precedenti giudiziari che letti alla luce della teoria appena esposta suffragherebbero la generale “natura costituzionale implicita” del *right to privacy*, richiama quali precipui fondamenti costituzionali del diritto in questione il Primo, il Quarto, il Quinto e il Nono Emendamento¹²⁸.

A partire da tale premessa teorica, la Corte attraverso la penna di Douglas può, nel caso di specie, riconoscere l’illegittimità costituzionale della legge incriminata: nel ribadire che «*the present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees*», essa ne deduce che una legge che vieti penalmente l’utilizzo di contraccettivi possa con molta probabilità avere «*a destructive impact upon that*

¹²⁷ Per esprimersi con le limpide parole del giudice Douglas, «*[the present case] suggest[s] that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance*»; cfr. *ivi*, p. 484. La concezione di privacy come «*penumbra*» era già stata proposta dal giudice O. W. HOLMES, «Dissenting Opinion», in *Olmstead v. United States*, 277 U. S., 438, 469.

¹²⁸ *Ibidem*. Ricordiamo che il Nono Emendamento stabilisce che «*the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.*». Sul fatto che la sentenza accoglierebbe una teoria dei c.d. «diritti impliciti» negli Emendamenti costituzionali, cfr. anche A. BALDASSARRE, *Privacy e Costituzione*, cit., p. 322.

relationship». A tal proposito, l'*opinion* fa leva sulla "sacertà" della dimensione privata in cui il rapporto coniugale si svolge: «*marriage*», scrive Douglas, «*is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred*»¹²⁹. Sacertà del "domicilio intimo" di due coniugi che rappresenta un aspetto della *privacy* quale nucleo essenziale della pluralità di diritti inviolabili appena richiamati, e dunque di un diritto presupposto negli stessi, tale da impedire ad uno Stato di vietare penalmente l'utilizzo di contraccettivi da parte di una coppia unita in matrimonio.

Con la sentenza commentata, la Corte enuncia, o sarebbe meglio dire accoglie, una volta per tutte una teoria positiva del diritto fondamentale di *privacy*, sebbene lo qualifichi non già come autonomo diritto, quanto piuttosto - lo ribadiamo - come nocciolo duro, sfera irrinunciabile di qualsiasi diritto esplicitamente tutelato dagli emendamenti costituzionali. Coerente con la teoria espressa anni prima in *Public Utilities v. Pollak*, il giudice Douglas, in mancanza di un espresso riferimento testuale nella Costituzione, concepisce la *privacy* come diritto la cui esistenza giuridica si fa derivare per emanazione da quasi tutti gli altri diritti fondamentali ivi tutelati, come garanzia implicita che dà loro, come egli scrive in *Griswold*, «vita e sostanza»¹³⁰. Ciò, tuttavia, rende il diritto in questione "plastico", e, in linea con l'approccio evolutivo inaugurato da Warren

¹²⁹ Ivi, p. 485, 486. Con espressione un poco enfatica, Douglas pone la seguente domanda retorica, in cui è implicita la risposta: «*Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship*». Sull'elemento della "sacertà" il giudice insiste più volte nel corso dell'*opinion*, in particolare nella parte in cui, richiamando un passaggio della nota sentenza *Boyd v. United States*, sostiene che il Quarto e il Quinto Emendamento garantirebbe all'individuo, a fronte di ogni invasione del governo federale o statale, «*protection against all governmental invasions "of the sanctity of a man's home and the privacies of life"*».

¹³⁰ Su *Public Utilities v. Pollak* e il *dissent* di Douglas, v. *supra*. Per la citazione, cfr. *Griswold v. Connecticut*, 381 U. S., p. 483 ss.

e Brandeis, capace di adattarsi ai (o, sarebbe meglio dire, di declinarsi nei), più disparati settori materiali¹³¹. Anzi, l'interpretazione suddetta quasi trasforma la *privacy* in un "puntello" per qualsiasi altra posizione giuridica soggettiva che la giurisprudenza intenda inferire in termini di "diritto implicito" dai dettami costituzionali, alla luce, lo abbiamo detto, di una loro interpretazione umanitaria prima ancora che evolutiva. Così, se nel caso di specie la Corte ha potuto servirsi della *privacy* per riconoscere una sorta di diritto all' "integrità" delle relazioni familiari o coniugali, considerata sotto il profilo della libertà di utilizzare i contraccettivi, in un caso ben più controverso come *Roe v. Wade* del 1973 la stessa Corte, facendosi interprete politico del limite di tolleranza raggiunto dall'opinione pubblica in materia, ha potuto riconoscere sostanzialmente l'esistenza di un diritto costituzionalmente fondato all'aborto, affermando che «il diritto di *privacy* è sufficientemente esteso da comprendere la decisione della donna se porre fine o meno alla gravidanza»¹³². E sempre sulla stessa base, e quindi nel nome di un *right to privacy* avvolto nella *penumbra* dei citati Emendamenti, nell'altrettanto celebre e più recente caso *Lawrence v. Texas* la Corte ha dichiarato l'illegittimità costituzionale di una legge che puniva penalmente i rapporti carnali omosessuali, ed ha affermato l'aprioristica incostituzionalità di qualsiasi legge che allo stesso modo punisca qualsiasi tipo di rapporto privato, consensuale, non procreativo tra due individui¹³³.

È proprio a causa dell'eccessiva "vaghezza concettuale" denunciata da taluni studiosi, che hanno reso la teoria in questione suscettibile di una certa "eterogenesi

¹³¹ D'altronde, tra i precedenti, i *dissents* e la dottrina richiamati dal giudice Douglas nella sentenza *Griswold* figura proprio la luminosa *dissenting opinion* del giudice Brandeis nel caso *Olmstead v. United States* del 1928, che tale approccio ulteriormente difende e articola. V. *supra*.

¹³² Cfr. *Roe v. Wade*, 410 U.S., 113 (1973), cit. tratta da p. 153.

¹³³ Cfr. *Lawrence v. Texas*, 539 U.S. 558 (2003); perentorie le parole del giudice Kennedy, che afferma: «Quando la sessualità si manifesta palesemente nell'intimo comportamento con un'altra persona, tale comportamento non è che un elemento nel legame personale [costituzionalmente protetto]», cit. tratta da p. 567.

dei fini”, che l’orientamento enunciato in *Griswold*, pur rappresentando il principale basamento su cui poggia l’attuale edificio statunitense di garanzie costituzionali costruito in materia di *privacy*, non incontra tutt’ora l’unanime favore dottrina. Ed anche con stretto riguardo alla decisione stessa, nonostante la maggioranza di 7 a 2 con cui fu deciso il caso, non si può tacere il fatto che alcuni dei giudici a favore espressero opinioni separate in punto di fondamento dell’illegittimità costituzionale della legge. Ciononostante, la sentenza in questione deve considerarsi il primo formale riconoscimento di un diritto positivo di *privacy* collocato nella gerarchia dei diritti di libertà sanciti, direttamente o indirettamente, in Costituzione, e la teoria che lo sostiene, di impronta umanitaria e incentrata sul binomio *privacy-dignity*, provvista di un intramontabile valore nella storia americana dei diritti civili.

Chiudiamo definitivamente il quadro dei precedenti giudiziari che si pongono a fondamento dell’attuale sistema costituzionale statunitense di tutela della *privacy* analizzando il caso *Katz v. United States* del 1967: assai importante perché, a differenza di *Griswold*, il caso in esame riguardava strettamente la controversa materia delle interferenze del governo nella “vita privata” attraverso perquisizioni o sequestri illegittimi, e dunque l’interpretazione del Quarto Emendamento, in relazione al quale vigeva autorevole e pressoché incrollabile la *rule of law* trent’anni prima enunciata dalla Corte, sotto la conservatrice presidenza Thaft, in *Olmstead v. United States*¹³⁴. La questione prendeva avvio dal procedimento penale intentato dal governo federale avverso un allibratore che piazzava illecitamente scommesse per mezzo di un telefono pubblico: senza mandato, ma al contempo senza introdursi fisicamente nella cabina, gli agenti vi avevano inserito un captatore, con cui avevano intercettato una serie di

¹³⁴ Cfr. da subito *Charles Katz v. United States*, 389 U. S., 347 (1967); sul caso *Olmstead v. supra*,

conversazioni, ammesse poi da una Corte Distrettuale della California e dai giudici di grado successivo come prove sulla cui base emettere la condanna dell'imputato. Dopo che anche la Corte d'appello confermava la sentenza, richiamando la giurisprudenza *Olmstead* e ritenendo alla sua luce che il Quarto Emendamento non fosse applicabile al caso di specie, non individuandosi alcun bene tangibile che fosse stato perquisito o ricercato - e d'altronde la cabina telefonica, in quanto pubblica, non costituendo un'area costituzionalmente protetta -, Katz proponeva ricorso davanti alla Corte Suprema. Ebbene, quest'ultima con la propria decisione rovescia il precedente *Olmstead*, valorizzando la c.d. *expectation of privacy* dell'imputato (intesa, nell'opinione portante del giudice Stewart, in senso generico), e più in generale dell'individuo di fronte all'esercizio dei poteri autoritativi da parte dei soggetti pubblici. La Corte, per mano del giudice Stewart, per la prima volta dichiara che le garanzie costituzionali accordate alla *privacy* in nome del Quarto Emendamento valgono *indipendentemente* dalla natura pubblica o privata dei luoghi: ad essere tutelato è infatti l'interesse del singolo alla tutela del nucleo intimo, essenziale della propria personalità, «non i luoghi»; e quando tale interesse si confronta con quello pubblico, nazionale, alla sicurezza collettiva, il primo può essere sacrificato (e dunque il provvedimento della pubblica autorità che impone tale limitazione può considerarsi costituzionalmente legittimo) solo alla luce di un rigoroso giudizio circa la ragionevolezza dell'atto autoritativo e restrittivo, e dunque circa la sua concreta idoneità e insieme la sua indispensabilità ai fini della realizzazione di tale interesse. Così, il Quarto Emendamento proteggerebbe qualsiasi informazione, espressa o meno attraverso un mezzo tangibile, che la persona intenda mantenere riservata, anche laddove “sopravvenga” in un'area accessibile al pubblico.

Servendosi delle parole della Corte, «al pari di un individuo nel proprio ufficio o (...) in un taxi, una persona che si trovi in una cabina telefonica può far

affidamento sulla protezione del Quarto Emendamento. Colui che occupa la cabina (...) è sicuramente *autorizzato a credere che le parole dette durante la telefonata non saranno diffuse nel mondo*. Leggere in maniera più ristretta la Costituzione significa ignorare il ruolo vitale che il telefono pubblico ha finito per avere nelle comunicazioni private»¹³⁵. Ancora, emerge un argomento di tipo evolutivo: come una più recente sentenza in materia ha avuto modo di sottolineare, la protezione accordata dal Quarto Emendamento rispetto alle interferenze potenzialmente illegittime nella *privacy* individuale attraverso i più recenti “*subtle means*” perpetrate dal governo deve essere sempre aggiornata, poiché il grado di *privacy* assicurato ai cittadini dall’emendamento in questione (e più in generale da qualsiasi disposizione costituzionale) non resta mai immune di fronte all’incessante progresso tecnologico¹³⁶.

La sentenza in questione è importante anche per il particolare criterio di bilanciamento tra *privacy* e interessi pubblici concorrenti quale quello alla sicurezza collettiva introdotto dalla *concurring opinion* del giudice Harlan, che il concetto di *expectation of privacy* (utilizzato in maniera solo generica dal giudice Stewart) sviluppa in senso tecnico: una sorta di “test legale”, articolato in due momenti, che vedremo ampio utilizzo avrà in tutti i più recenti casi in cui *privacy* e interessi pubblici o economici concorrenti, anche per effetto delle sempre crescenti minacce configurate dallo sviluppo della tecnica, in primis della cibernetica e delle ICTs, sono venuti in conflitto. La tesi in questione, nel quadro di una *opinion* che rispetto a quella di Stewart ha uno spessore concettuale ben maggiore, propone di individuare il perimetro della “sfera privata” tutelata nei rapporti con la pubblica autorità dal Quarto Emendamento a partire da un «duplice requisito, il primo dei quali è stabilire se la persona ha mostrato un'effettiva (e

¹³⁵ Ivi, p. 351-352.

¹³⁶ Cfr. il fondamentale e più recente caso *Kyllo v. United States* 533 U.S. 27 (2001), sul quale torneremo più nello specifico nel cap. 4.

soggettiva) aspettativa di *privacy*; mentre il secondo è che quell'aspettativa sia riconosciuta dalla società come ragionevole»¹³⁷. Di conseguenza, soltanto nel caso in cui la Corte risponda affermativamente ad entrambe le questioni, la semplice aspettativa di *privacy* assurgerà a diritto (implicitamente) protetto dal Quarto Emendamento.

Sebbene il criterio in questione abbia, negli anni successivi, ispirato numerose pronunce garantiste della Corte, quest'ultimo a partire dalla seconda metà degli anni Settanta ha conosciuto un indirizzo esegetico restrittivo, che piuttosto comprime i confini della riservatezza protetta ai sensi del Quarto Emendamento: indirizzo che, all'evidenza, risulta incapace di assicurare alla persona un livello sufficiente di *information privacy*, di controllo sulle informazioni che la riguardano, di fronte all'evoluzione tecnologica. Risale infatti al 1976 il caso *United States v. Miller*, in cui la Corte stabilisce per la prima volta esplicitamente il principio noto come *third party doctrine*, in forza della quale la persona che *volontariamente* condivide informazioni con una "terza parte" non gode in ordine a queste ultime di quella legittima *expectation of privacy* garantita dal Quarto Emendamento ai sensi del precedente *Katz*, di modo che l'attività del governo intesa ad acquisire le medesime informazioni presso il terzo non sarebbe giuridicamente qualificabile come *search* e pertanto non contrasterebbe con uno degli "aspetti" del *constitutional right to privacy* previsto, nei rapporti tra pubblica autorità e individui, dalla disposizione costituzionale in questione: ovvero, non necessiterebbe ai fini della sua legittimità (e dell'utilizzabilità degli elementi di prova così raccolti) di legale mandato di perquisizione dell'autorità giudiziaria, fondato su una *probable cause*¹³⁸. Ciò implica che le autorità di polizia possano procurarsi direttamente presso la "terza" persona fisica o giuridica, senza i suddetti vincoli, tutte le informazioni condivise

¹³⁷ Cfr. *Charles Katz vs. United States*, 389 US 347 (1967), p. 361 ss.

¹³⁸ Cfr. *United States v. Miller*, 425 U.S. 435 (1976)

dal primo con essa¹³⁹. E se il caso *Miller* si riferisce alle sole informazioni condivise volontariamente con le banche nell'ambito delle proprie *business operations* (depositi in conto corrente, riscossione di assegni ecc.), nel 1979 la *third party doctrine* viene ulteriormente articolata e più precisamente delineata, poiché estesa alle “informazioni numeriche” condivise dal fruitore di una linea telefonica con la compagnia di riferimento. La Corte infatti, nel famoso caso *Smith v. Maryland*, afferma che non ricadrebbero nel concetto di *search*, agli effetti del Quarto Emendamento, nemmeno l'installazione e l'utilizzo di un *pen register* da parte della polizia per ottenere informazioni sulle conversazioni telefoniche tenute da un sospettato: nel momento stesso in cui quest'ultimo abbia acconsentito a condividere le informazioni sui numeri chiamati con la compagnia telefonica, usufruendo dei suoi servizi, i numeri in questione, comunque registrati e memorizzati dal *network provider*, cesserebbero per definizione di essere “privati”, e lo stesso non potrebbe vantare su questi ultimi alcuna costituzionalmente tutelata *expectation of privacy*¹⁴⁰.

Il principio configurato dal combinato disposto tra tali sentenze da ultimo citate sarà recepito e progressivamente allargato, quanto al suo raggio applicativo, da una nutrita parte della giurisprudenza di diritto comune, la quale, come vedremo più nel dettaglio nel quarto capitolo, interpreterà in modo estensivo i precedenti in questione (e, dunque, in senso restrittivo il concetto di *expectation of privacy*), considerando inapplicabili le garanzie del Quarto Emendamento anche in relazione alle informazioni condivise dal singolo con *e-mail servers* ed *Internet Service Providers* (ISP)¹⁴¹. Tuttavia, ancora oggi, nell'ambito del

¹³⁹ Cfr. ad es. D. J. SOLOVE, *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, CT, 2013, pp. 102–110.

¹⁴⁰ Cfr. *Smith v. Maryland*, 442 U.S. 735 (1979).

¹⁴¹ Cfr. ad es. *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012) in cui la Corte Distrettuale del Maryland ha stabilito che i dati storici relativi alla localizzazione spaziale di un telefono cellulare non ricadrebbero nell'alveo del diritto alla *privacy* garantito, a fronte di perquisizioni e sequestri illegittimi, dal Quarto Emendamento. Critica la tendenza “estensiva”

problematico rapporto tra interesse individuale alla riservatezza e interesse alla sicurezza nazionale perseguito dal governo, perdura una tensione insanabile tra le due opposte prospettive dell’*expectation of privacy* e della *third-party doctrine* (a cui si aggiunge, come vedremo più avanti, il tradizionale “esonero” sintetizzato nella c.d. *plain sight doctrine*): cosicché tutt’ora il perimetro del *right to privacy* garantito nella difficile relazione tra singolo e autorità, statale o federale, continua ad essere “indeterminato”¹⁴². Ciò, nel contesto della *società datificata*, stretta nella morsa della sorveglianza governativa e della profilazione di massa, assume un significato ancora più problematico. Filosofico, prima ancora che giuridico.

Per ora, tuttavia, è opportuno chiudere la nostra disamina della storia della giurisprudenza costituzionale in materia di *privacy*: giunti al riconoscimento positivo del *right to privacy* secondo la dottrina della “*penumbra*” delle disposizioni costituzionali sui diritti di libertà, e individuati alcuni precisi, problematici limiti entro cui la giurisprudenza successiva ha imbrigliato le garanzie suddette, possiamo rinviare al quarto capitolo una sintetica catalogazione, secondo un criterio di ordine “materiale”, dei precedenti intervenuti dagli anni Settanta ad oggi.

Ci si concentrerà ora, seppur brevemente, sulla legislazione federale, che si sviluppa a partire proprio dalle prime pronunce con cui la Corte ascrive alla costellazione dei diritti costituzionali il *right to privacy*.

della giurisprudenza di *common law* H. NISSENBAUM, «Protecting Privacy in an Information Age: The Problem of Privacy in Public», in *Law and Philosophy*, 17 (5), 1998, pp. 559–596.

¹⁴² A dimostrazione della vivacità della dialettica sul punto, cfr. sin d’ora, sempre in materia di *historical cell site location data* il recente caso *Carpenter v. United States*, 138 S. Ct. 2206 (2018), sul quale ci soffermeremo nel cap. 4; la Corte sembra ivi riaffermare una più rigorosa interpretazione delle garanzie rappresentate dal criterio del *reasonable expectation of privacy* inaugurato dal caso *Katz*, e pertanto sconfessare l’orientamento estensivo promosso dalla *District Court* del Maryland nel caso citato nella nota precedente.

1.2. Elaboratori elettronici e “*individual control*”: l’*information privacy* nella legislazione federale settoriale dagli anni Settanta ad oggi

Abbiamo già fatto sinteticamente riferimento al carattere “settoriale” del modello statunitense di tutela della *privacy*. Oltre ai rilievi già svolti sui connotati “ontologici” dell’ordinamento americano, sul dinamismo che ne caratterizza l’esperienza giuridica, laddove osservato da una prospettiva di *law in the making*, possiamo ora aggiungere che parte della dottrina sostiene come tale settorialità, sul piano legislativo, sia storicamente dipesa dalla necessità di rispondere tempestivamente sia agli scandali occorsi sempre più spesso a partire dagli anni Settanta, sia, lo si ripete, ai vuoti normativi prodotti dal progresso e dall’evoluzione tecnologica¹⁴³. Imperniato sulla fiducia che diritto e società ripongono nelle capacità dell’ordinamento di “adattarsi”, per mezzo della sensibilità degli operatori giuridici e segnatamente dei giudici, alle nuove esigenze del corpo sociale, il legislatore è intervenuto solo nel momento in cui anche l’esperienza di diritto comune, nel quadro del sistema costituzionale della *privacy* di natura esclusivamente giurisprudenziale, è apparsa inidonea ad offrire una regolamentazione specifica dei singoli aspetti del rapporto tra sfera privata e tecnologia. E tuttavia, la mancanza di un quadro normativo - di un *legal framework* – di ordine generale, e pertanto di una fonte normativa unitaria *a livello federale* a tutela della *privacy*, anche nella sua declinazione più recente - ossia come *data privacy* -, si è rivelata sempre più grave: ciò, da una parte, alla luce dei poteri di emergenza negli anni Duemila “abusati” dal governo federale nel quadro della lotta al terrorismo; dall’altra, anche e soprattutto a fronte dell’incalzare della rivoluzione tecnologica e dell’autoregolamentazione privata, specialmente in seguito all’avvento del *World Wide Web* (autoregolamentazione che ha quasi

¹⁴³ Cfr. U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 61-62.

raggiunto, oggi, l'anomia nel contesto dei *social network*, essenzialmente “normati” dalle Condizioni Generali di Contratto predisposte dalle piattaforme).

Prima di delineare la storia della legislazione federale, occorre fare alcune premesse, su cui torneremo nel quarto capitolo. Innanzitutto, bisogna aver chiaro il sistema statunitense delle fonti del diritto, che si articola principalmente su due livelli, quello costituzionale e quello ordinario (a propria volta diviso in *statutes* e *common law*, distribuito sul duplice binario federale e statale): al suo interno, la legislazione si pone chiaramente su un piano gerarchicamente subordinato a quello su cui insistono i principi, le disposizioni, gli emendamenti costituzionali e i precedenti della Corte Suprema di Washington che li interpretano in funzione applicativa. A questi due livelli, si aggiungono le fonti secondarie di produzione del diritto, che comprendono le *regulations*, gli atti di *law enforcement* e le prassi degli organi dell'esecutivo, in particolare delle Agenzie Governative, federali e statali, su cui avremo modo di tornare in seguito. Nell'ordinamento statunitense, lo ripetiamo, vige poi il modello del controllo diffuso di legittimità costituzionale, funzione di cui sono investite tutte le corti, tanto federali quanto statali¹⁴⁴.

In secondo luogo, bisogna considerare che controverso e ancora discusso nella giurisprudenza della Corte Suprema, che ha diversamente declinato nella sua storia la dottrina del *balance of power*, è il rapporto tra diritto positivo federale e diritto ordinario statale, composto da *statutes* e *common law*. Non essendo questa la sede per dilungarsi sul punto, appare comunque indispensabile ricordare che, nella specifica materia della *privacy*, vige un principio anch'esso sancito nel richiamato caso *Katz*, in forza del quale «la tutela del diritto generale alla *privacy* spettante all'individuo dipende in gran parte dalla legge dei singoli Stati [federati]», che sono dunque liberi, dove lo ritengano opportuno, nell'esercizio della propria discrezionalità normativa, di estendere la sfera di tutela della *privacy*

¹⁴⁴ Principio desunto dal fondamentale precedente *Marbury v. Madison*, 5 U.S. 137 (1803).

rispetto al *minimo* costituzionalmente previsto¹⁴⁵. Conseguenza di ciò è che, mentre la legislazione federale si è da sempre maggiormente occupata dei rapporti tra individuo e pubblici poteri, agli Stati è stata lasciata la regolamentazione della *privacy* e della *data protection* nei rapporti interprivati, il che ha evidentemente determinato discrasie nella disciplina prevista dall'uno e dall'altro Stato, pur essendosi soprattutto negli ultimi anni registrato un fenomeno di circolazione “interfederale” di specifici modelli giuridici statali. Resta comunque evidente che il principio enunciato in *Katz* rende la materia dei rapporti tra i due binari in cui si articola il diritto ordinario, quello federale e quello statale, in punto di *privacy* particolarmente delicata.

Ancora una breve premessa, inerente all'arco temporale e all'estensione dell'oggetto della nostra indagine storica. Considerato l'elevato numero di Stati federati (cinquanta, di cui ben dieci contengono nelle loro Costituzioni statali un riferimento alla *privacy*), e la circostanza che quasi tutti (quarantasette) dispongono ormai di una più o meno recente *data privacy legislation*, per ora si riepilogheranno soltanto le principali normative succedutesi a livello federale. Allo stesso modo, l'indagine si fermerà agli anni Dieci del nostro secolo: infatti, a partire dallo scandalo *Datagate* occorso a seguito delle rivelazioni di Edward Snowden del 2013, che hanno reso noto al mondo il sistema di sorveglianza di massa posto in essere dalla *National Security Agency* (NSA), il panorama normativo americano ha subito indirettamente, quasi per un “effetto boomerang”, le conseguenze delle politiche adottate dall'Unione europea al fine di arginare i rischi per la riservatezza dei suoi cittadini configurati dal trattamento transfrontaliero dei loro dati personali, culminate nella promulgazione del *General Data Protection Regulation* (GDPR), nelle sentenze *Schrems* e, più di

¹⁴⁵ Cfr. infatti ancora una volta *Charles Katz v. United States*, 389 U.S. 347 (1967).

recente, nella stipulazione del nuovo *EU-U.S. Data Privacy Framework*¹⁴⁶. Non si può dunque ripercorrere lo sviluppo della legislazione americana, statale così come federale, degli ultimi anni senza aver prima studiato la storia della *privacy* nel Vecchio Continente. Rinvieremo, dunque, l'analisi di questi aspetti al quarto capitolo.

La storia della legislazione federale “moderna” in materia di *privacy* comincia alla fine degli anni Sessanta, proprio in conseguenza del rapido e inaudito sviluppo delle tecnologie informatiche, e del loro massiccio impiego ad opera di grandi imprese e, soprattutto, di agenzie del governo federale e di pubbliche amministrazioni statali: proprio in quegli anni si registra un incremento dei *database* computerizzati utilizzati da tali soggetti, che se da una parte semplificano e “sburocratizzano” la vita del cittadino, dall'altra mostrano quanto sia facile rendere i più intimi aspetti della sua vita privata, a cominciare dalla condizione economica o dall'orientamento religioso o sessuale, pubblicamente visibili. E se la pubblica amministrazione di quei nuovi mezzi si serve per implementare la gestione della cosa pubblica e preservare la sicurezza nazionale, le *companies* li considerano piuttosto una preziosa leva per i profitti, consentendogli questi di raccogliere e di utilizzare più agilmente le informazioni (e soprattutto i dati da cui estrarle) per finalità di marketing o di controllo sui propri lavoratori¹⁴⁷. In entrambi i casi, il risultato è quello di un sempre più

¹⁴⁶ Sul *Datagate*, sul suo impatto cruciale sull'opinione pubblica e sul ripensamento della disciplina della *data protection* da esso indotta nell'intero occidente, cfr. D. LYON, «The Snowden Stakes: Challenges for Understanding Surveillance Today», in *Surveillance and Society*, 13, 2015, 139 ss; ma v. anche *infra*. Sul GDPR, sulle sentenze *Schrems I* e *Schrems II* e sugli accordi succedutisi tra USA e UE ai fini del trasferimento transfrontaliero di dati personali, v. *infra*, par. 2.4 e cap. 2.

¹⁴⁷ Come già dimostra la disamina del contesto da cui prende l'avvio il caso *Olmstead*, sul piano delle interferenze governative in quegli anni aumentavano gli strumenti per intercettare le conversazioni, le c.d. *bug* (microspiee), le *parabolic microphone*, le *wiretap*; mentre nel contesto dei rapporti tra privati già nel 1920 la General Motors, per fare un esempio

sistematico *dossieraggio* degli individui, senza che gli stessi ne siano fino in fondo consapevoli. Si assiste dunque alla nascita del problematico fenomeno che progressivamente determinerà quella condizione che è stata acutamente definita una vera e propria «mutazione antropologica» dell'essere umano, la cui dimensione esistenziale si arricchisce di un «corpo elettronico»: l'elaborazione, o, con terminologia più moderna, il trattamento “elettronico”, che oggi definiremmo piuttosto “automatizzato” o ancora meglio “algoritmico”, dei dati personali¹⁴⁸.

Tra i primi ad accorgersi della *dimensione sociale* assunta dalla categoria della *privacy*, e del rischio di *secret surveillance* da parte del governo e delle imprese cui risulta sempre più esposta, per effetto della nuova tecnologia, l'intera collettività, c'è sicuramente il celebre giurista Arthur Miller, che nel 1971 pubblica un saggio intitolato *The Assault on Privacy* in cui sottolinea il carattere esponenziale del fenomeno in atto. Riferendosi al contesto che veniva prendendo forma in quegli anni, Miller afferma che «*[t]he computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of casual observers, including the morbidly curious and the maliciously or commercially intrusive*»¹⁴⁹. Alla luce di ciò, e per farvi fronte, l'autore ritiene opportuno ripensare l'istituto della *privacy*, enucleando, accanto alla pretesa ad essere lasciati “indisturbati”, un

eloquente, aveva cominciato a registrare i propri clienti: cfr. sul punto T. M. UMBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, cit.

¹⁴⁸ Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 318 ss., che nel descrivere la dinamica evolutiva innescata dalla rivoluzione informata introduce i concetti di *identità dilatata* e di *identità «dispersa»*, sul presupposto che «le informazioni riguardanti la stessa persona sono contenute in banche dati diverse, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva».

¹⁴⁹ A. MILLER, *The Assault on Privacy*, cit., p. 3.

diverso contenuto che consiste in «*the individual's ability to control the circulation of information relating to him – a power that often is essential to mantaining social relationship and personal freedom*»¹⁵⁰.

Questo passaggio è fondamentale, perché testimonia la mutata percezione della “questione *privacy*” nella cultura statunitense, con particolare riferimento alle tecniche giuridiche più idonee a tutelare il “cuore” della sfera privata. Miller, infatti, come tutti i sostenitori delle più recenti teorie che dagli anni Sessanta in poi cominciano ad individuare quale oggetto precipuo del *right to privacy* l’informazione personale, e che pertanto del diritto in questione valorizzano la dimensione positiva, del “controllo” sull’informazione stessa, sembra individuare il rapporto che intercorre tra costruzione dell’identità personale, intesa qui tanto come intima personalità quanto come sua proiezione esterna, e controllo sulle informazioni riguardanti la propria persona¹⁵¹. Proprio per questo, di fronte ai *computers*, agli elaboratori elettronici, e più in generale ai nuovi strumenti di “sorveglianza elettronica”, egli sembra unirsi alle voci che sostengono come l’unica efficace protezione della vita privata risieda nell’ampliare il contenuto del *right to privacy*, di declinarlo *anche* in un diritto ad esercitare un controllo sul proprio “patrimonio informativo”: una concezione che, *mutatis mutandis*, nel contesto europeo rinvia a quel diritto all’*autodeterminazione informativa* frutto di una lunga elaborazione dottrinale post bellica e consacrato come diritto fondamentale nel 1983 dalla Corte Costituzionale tedesca; e, ancor più, a quel concetto di *habeas data*, che a sua volta richiama l’*habeas corpus* inteso come libertà personale sancito dalla *Magna Charta Libertatum* del 1215, coniato dalla preziosa voce di Stefano Rodotà¹⁵².

¹⁵⁰ *Ibidem*.

¹⁵¹ Cfr. A. WESTIN, *Privacy and Freedom*, cit.; più di recente, CH. FRIED, *A Rational Context*, cit.; v. in generale *supra*, in part. note 87 e 88

¹⁵² Cfr. la già citata, epocale sentenza del Bundesverfassungsgericht, 15-12-1983, in *Entscheidungen des Bundesverfassungsgericht*, 1984, 65, p 1-71, su cui v. *infra*. Sul concetto

L'inarrestabile progresso tecnologico della società industriale di massa dischiude, allora, agli occhi dell'opinione pubblica e dei suoi più sensibili interpreti il valore sociale della *privacy*: in un mondo in cui *wiretaps* e cimici possono infiltrarsi nell'intimità di ognuno, e immateriali banche dati possono indelebilmente conservare le tracce degli acquisti, delle chiamate, della corrispondenza, delle attività di ordinaria amministrazione compiute dal singolo, la protezione della *privacy*, specialmente nella forma del controllo sui proprio dati, diventa strumento per tutelare le società democratiche dalla degenerazione del controllo globale, pubblico e privato ¹⁵³.

In ogni caso, proposte come quella di Miller, in concorso con l'affermarsi della dottrina dell'"emanazione" del *right to privacy* dagli emendamenti costituzionali inaugurata dalla *Supreme Court*, contribuiscono anche in ambito statunitense alle prime "aggettivazioni" della *privacy*, e quindi all'emancipazione dal *cluster* di categorie più specifiche: nello specifico, venendo sempre più alla luce l'importanza dei *dati personali*, sempre più intesi quali *tradable commodities*, beni giuridici provvisti di valore patrimoniale, si individua il concetto di *information privacy*. Il centro di gravità della *privacy* comincia ad arricchirsi: alla tradizionale pretesa all'"*aloneness*", si affianca quella di controllare, come abbiamo detto, il proprio patrimonio informativo. E proprio all'esigenza di garantire quest'ultima, di fronte al sempre più difficile rapporto tra singolo e autorità pubblica, tenta di rispondere il legislatore federale.

di *habeas data*, cfr. S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Editori Laterza, Roma Bari, 2014; ID., *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, Wroclaw (PL), 14-16 settembre 2004, disponibile sul sito del Garante Privacy italiano: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293>.

¹⁵³ Cfr., in generale, il profetico lavoro di S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Jovene Editore, Bologna 1973; ma oggi rist. anast., Jovene Editore, Napoli 2018; e anche F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento Europeo*, Torino 2016, p. 12 ss.

Si può affermare che il primo atto normativo federale indirettamente dedicato alla regolamentazione della *privacy informativa* sia il *Freedom of Information Act* (FOIA), datato 1966¹⁵⁴. Scopo precipuo, infatti, è quello di soddisfare un'esigenza di trasparenza che al suddetto controllo sul proprio sé informativo si collega. Le sue norme mirano a garantire al cittadino l'accesso a tutte le informazioni sugli enti pubblici, e in particolare sull'organigramma, sulle funzioni e sui metodi dell'attività dell'ente, nonché sulle norme e sulle modalità di partecipazione ai procedimenti amministrativi: tra queste (ecco l'indiretto collegamento), sono necessariamente comprese quelle sulle modalità di accesso alle informazioni personali detenute dall'ente medesimo.

In realtà, la dottrina è concorde nel ritenere che la prima effettiva *data privacy legislation* intervenuta nell'ordinamento statunitense sia il *Fair Credit Reporting Act* (FCRA), promulgato nel 1970¹⁵⁵. Se il FOIA persegue l'interesse dei cittadini alla trasparenza amministrativa, e di conseguenza risulta applicabile ai soli rapporti tra questi e la pubblica amministrazione, il FCRA ambisce a riformare il sistema del *consumer credit reporting* in modo da garantirne l'accuratezza e la trasparenza, assoggettando a precisi limiti la raccolta, la gestione e la diffusione delle informazioni sui consumatori, comprese quelle relative al credito al consumo, e rendendo più facile per l'interessato la correzione degli errori nel *reporting*. Esso viene considerato, pertanto, l'archetipo di tutta la successiva legislazione statunitense in materia di *data privacy*. In particolare, tra gli istituti divenuti paradigmatici, oltre all'obbligo di avvisare il consumatore sul tipo di *data record* effettuato e al *consent* quale fondamento generale di liceità

¹⁵⁴ Cfr. *Freedom of Information Act* (FOIA), 5 U.S.C. § 552.

¹⁵⁵ Public Law No. 91-508, tit. VI, 84 Stat. 1114 (1970). Per un'analisi puntuale degli istituti rilevanti in punto di *data privacy*, e più specificamente di sistemi automatizzati di trattamento di *personal information*, v. ampiamente *infra*, cap. 4.

dello stesso, figura la tipizzazione di una procedura amministrativa attraverso cui il singolo possa lamentare la violazione della disciplina in esame ed ottenere la riparazione, con la contestuale attribuzione della competenza ad una specifica agenzia governativa federale: nella specie, così come per tutte le successive normative in materia commerciale incidenti sulla *data privacy*, la *Federal Trade Commision* (FTC)¹⁵⁶.

Tuttavia, sia il FOIA che l'FCRA presentano delle gravi lacune in punto di garanzia della *privacy* individuale.

Per quanto attiene al secondo, il principale limite consiste proprio nella sua settorialità. Se, infatti, è vero che questo costituisce il primo atto normativo federale disciplinante la *privacy* nei rapporti tra privati, è tuttavia evidente che lo stesso risulti applicabile al solo, limitato settore della *credit industry*, e ancor più nello specifico del *consumer credit reporting*. Esso è, appunto, il primo di tutta quella serie di *statutes* settoriali che contraddistingue il *legal framework* in materia di *data privacy*, a livello federale.

Allo stesso modo, il perimetro applicativo del FOIA, pur avendo questo una portata più generale in virtù del suo scopo, è limitato al settore pubblico. Ma il vero punto dolente di tale disciplina è la deroga che l'atto in questione prevede per le Agenzie Governative Federali, quali CIA, FBI e Pentagono, laddove le stesse ritengano di essere in possesso di informazioni rilevanti per la *national security*: indeterminata clausola generale che, di fatto, consente alle stesse di respingere o di sospendere la richiesta di *disclosure*, avanzata dal singolo, fino a cinque anni. E la mancanza di un apparato sanzionatorio a fronte di abusi sul punto rende il FOIA, negli anni successivi alla sua promulgazione, spesso in concreto privo di effettività proprio laddove il cittadino necessiterebbe di maggiori

¹⁵⁶ Cfr. S. COBB, «Data Privacy and Data Protection: U.S. Law and Legislation», in *WeLiveSecurity*, 2016, p. 2.; S. H. BOYNE, «Data Protection in the United States», in *The American Journal of Comparative Law*, vol. 66, 2018.

garanzie. Non bisogna dimenticare peraltro che anche l'FCRA prevede determinate ipotesi, sebbene meglio specificate, in cui l'interesse alla sicurezza nazionale o esigenze di *law enforcement* possono giustificare, in deroga agli obblighi informativi e alla regola del *consent*, l'accesso degli organi dell'esecutivo ai dati altrimenti protetti¹⁵⁷.

L'esigenza più avvertita in quegli anni è, certamente, quella di colmare il vuoto ignorato dal FOIA: ovverosia quella di riconoscere positivamente ai cittadini un "diritto di conoscere" le informazioni in possesso di soggetti pubblici, sempre più distribuite in un dedalo di banche dati computerizzate, e quello conseguente di accedervi, circondando il diritto medesimo di sanzioni e dunque dotandolo di effettività. E sono proprio le turbolente vicende politiche che interessano gli Stati Uniti in quegli anni a far avvertire come indispensabile una integrazione, se non proprio una modifica, della disciplina dal FOIA introdotta.

Il 17 giugno 1972, cinque uomini vengono arrestati nel tentativo di inserire delle cimici nei telefoni degli uffici del Comitato Nazionale del Partito Democratico, con sede presso l'Hotel Watergate: grazie anche all'inchiesta di due giornalisti del noto quotidiano Washington Post, due dei cinque uomini arrestati vengono ben presto identificati come ex agenti della CIA, molto vicini al presidente repubblicano Nixon. A ciò segue uno scandalo di immani proporzioni, denominato, in "omaggio" al luogo del misfatto, «*Watergate*»: l'opinione pubblica chiede a gran voce le dimissioni del presidente e reclama l'adozione di

¹⁵⁷ Cfr. ad es. § 626, rubricato «Disclosures to FBI for counterintelligence purposes [15 U.S.C. § 1681u]»; e § 627, rubricato «Disclosures to governmental agencies for counterterrorism purposes [15 U.S.C. § 1681v]».

una legge che vieti abusi di potere ed interferenze nella vita privata di simile portata¹⁵⁸.

È questo allora lo scenario sociopolitico in cui germoglia e viene approvato dal Congresso, il 31 dicembre 1974, il famoso *Privacy Act* (PA), dalla gran parte della dottrina considerato il primo atto *generale* in materia di *privacy* degli Stati Uniti, e tutt'ora perno della legislazione vigente¹⁵⁹. La legge è composta da un solo articolo, il § 552 del Titolo Quinto del Codice degli Stati Uniti, suddiviso in ventuno sottoparagrafi. Le norme ivi previste traggono ispirazione dal dibattito intorno alle c.d. *Fair Information Practices* (FIPs), una serie di pratiche standard ai fini della corretta predisposizione di *personal data systems*, delineate da un comitato (il *Secretary's Advisory Committee on Automated Personal Data Systems*) istituito all'interno dello *U.S. Department of Health, Education and Welfare* già nel 1969 e da quest'ultimo successivamente pubblicate in un report del 1973. Già tale lavoro pone particolare attenzione alla natura (ormai) automatizzata dei sistemi suddetti e dei rispettivi trattamenti: a testimoniare la sua importanza, inoltre, parte della letteratura americana sostiene che esso abbia avuto risonanza ed influenza anche oltre i confini statunitensi, cosicché le FIPs avrebbero ispirato tanto le Linee Guida in materia di *data privacy* elaborate dall'OCSE nel 1980 quanto la stessa, fondamentale Convenzione n.108 del Consiglio d'Europa¹⁶⁰. Le norme del *Privacy Act*, codificando le cinque “pratiche

¹⁵⁸ Per una panoramica sullo scandalo, tra i più noti e i più gravi della storia americana, ci si permette di rinviare alla pagina di Wikipedia dedicata al tema: https://en.wikipedia.org/wiki/Watergate_scandal#.

¹⁵⁹ Public Law No. 93-579, 88 Stat. 1897, in 5 U.S.C. § 552. (1974)

¹⁶⁰ Cfr. ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens*, Washington D.C., 1973, xx-xxi, su cui torneremo nel cap. 4; per quanto attiene all'influenza che le FIPs avrebbero avuto sulla successiva disciplina della *data protection* anche al di fuori degli U.S.A., v. *infra*, cap. 2 e cap. 3. Cfr. S. COBB, «Data Privacy and Data Protection», cit., p 2 ss., che sottolinea come, sorprendentemente, lo stesso Regan prima di *Watergate* in una serie di discorsi pubblici avesse sottolineato l'importanza del report in questione; D.J. SOLOVE-P.M. SCHWARTZ, *Information Privacy Law*, New York, 2011, 37-40.

standard” enucleate dall’HEW, in generale mirano, da una parte, ad arginare l’indiscriminata circolazione delle informazioni riguardanti il cittadino, e dall’altra ad agevolare il diritto di “accesso” degli indagati agli atti investigativi e agli altri elementi raccolti nell’ambito del procedimento penale a loro carico.

Architrave della normativa è certamente il paragrafo (b), che stabilisce come nessun ente pubblico possa trasmettere a persone o ad organizzazioni terze dati relativi ad un soggetto *senza averne ottenuto il previo consenso o la richiesta scritta*, salve alcune eccezioni (es. uso statistico dei dati o obblighi di legge) previste espressamente dalla normativa. Inoltre, la lettera (d), codificando una delle più innovative *fair practices* elaborate dall’HEW, garantisce al cittadino un vero e proprio diritto di accesso, e in particolare di ottenere copia dei documenti relativi ai dati che lo riguardano; ed eventualmente ad esigere la modifica e la correzione degli stessi¹⁶¹. Tutti principi che, effettivamente, rappresenteranno saranno consacrati già nella prima architettura generale in materia di trattamento (e, conseguentemente, protezione) dei dati personali edificata dalla Convenzione n. 108 del 1981 del Consiglio d’Europa, e pertanto poi ripresi, affermati e amplificati nella loro portata nelle principali normative dell’Unione europea e dei suoi Stati membri in materia di *privacy* e di protezione dei dati personali¹⁶².

Tuttavia, nonostante questi preziosi contributi all’edificazione di un *right to information privacy* dell’individuo, la disciplina che risulta dal *Privacy Act* (il *legal framework*) non è interamente garantistica per la *privacy* del cittadino, né può considerarsi in senso proprio “generale”. E ciò per un duplice ordine di ragioni. Innanzitutto, sebbene lo stesso report dell’HEW raccomandasse l’implementazione di un codice applicabile ad «*all automated personal data systems*», il Congresso nell’adottare il PA ha soggettivamente limitato l’ambito di

¹⁶¹ Per una panoramica sul punto, cfr. D.J. SOLOVE, M. ROTENBERG, P.M. SCHWARZ, *Privacy, Information and Technology*, Aspen Law & Business, 2006, pp. 180 ss.

¹⁶² V. ampiamente *infra*, cap. 2 e cap. 3.

applicazione ai soli rapporti tra individuo e pubblici poteri; anzi, ancor più nello specifico, il suo oggetto è rappresentato dalle sole informazioni contenute nei *database* delle amministrazioni federali¹⁶³. E questo, probabilmente, per timore che introdurre limitazioni al trattamento dei dati ad opera delle imprese potesse avere un impatto negativo sul libero dispiegarsi dell'iniziativa economica privata¹⁶⁴. Ciò ha tuttavia profondamente influenzato la successiva evoluzione in materia del diritto positivo statunitense, favorendo la persistenza di *lobbies* rappresentative di interessi commerciali che ritengono il potenziamento della tutela degli attributi fondamentali della persona umana, e conseguentemente dei diritti della personalità, compreso dunque un olistico regime di protezione dei dati personali che includa il settore privato, come un ostacolo al libero commercio e come un *unfair burden for business*¹⁶⁵. In secondo luogo, pur essendo stato previsto (principalmente) come strumento per irrobustire le garanzie del Quarto Emendamento, lo stesso *statute* prevede alle lettere (j) e (k), al di là degli specifici fondamenti di liceità del trattamento alternativi al consenso già ricordati, una generale e verrebbe da dire indiscriminata esenzione per le corti nell'esercizio dell'azione penale, per gli organi dell'esecutivo e per le altre agenzie governative (come, appunto, la CIA): e come nel FOIA, tale esenzione è sintetizzata nelle amplissime clausole delle "esigenze di sicurezza nazionale e di ordine pubblico". Questo ennesimo, considerevole limite posto alla *privacy* individuale ha costretto il legislatore statunitense ad intervenire negli anni per aggiornare alcuni punti chiave della normativa, così da adeguarla ai maggiori rischi configurati dal progresso tecnologico (e in particolare dalla digitalizzazione di massa), che ha

¹⁶³ V. infatti 5 U.S.C. § 551(a).

¹⁶⁴ Cfr. M. SURACE, *Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di internet*, cit., cap. 2.

¹⁶⁵ Cfr. S. COBB, «U.S. Data Privacy Legislation», cit., p. 3; P.M. REGAN, «Personal information policies in the United States and Britain: The dilemma of implementation considerations», in *Journal of Public Policy*, 4(01), 1984, pp. 19-38.

concorso ad incrementare le forme di intrusione governativa nella *privacy* individuale.

Già a questo punto appare delinearci quel modello privo di alcuna *general privacy legislation* che caratterizza il modello americano di tutela della *privacy*: da questo momento in poi, il Congresso procede con interventi mirati a regolare, di volta in volta, specifiche categorie di dati personali, o meglio l'*information privacy* in relazione a sempre specifici settori materiali (c.d. *sector specific legislation*). Tuttavia, si configura da subito un grande problema: l'assenza di una comune *Independent Supervisor Authority*. Se abbiamo ricordato come l'FCRA ricada sotto la *jurisdiction* della FTC, dobbiamo al contempo sottolineare che ciò dipende dal fatto che la Sezione 5 del *Federal Trade Commision Act*, da cui l'Agenzia suddetta ricava primariamente la propria *legal authority*, le attribuisce competenza in materia di "protezione" del consumatore"¹⁶⁶. Pertanto in linea di principio, a seconda dell'ambito materiale cui la singola *data privacy legislation* inerisca, la competenza in punto di *enforcement* e *redress* a fronte di violazioni della *privacy* ricade nella sfera di attribuzione di una diversa *Federal Law Enforcement Agency* (sia questa un'autorità indipendente come la FTC o piuttosto un dipartimento federale). Allo stesso tempo, bisogna sin d'ora evidenziare la tendenza seguita fino ad oggi dal Congresso ad estendere i poteri amministrativi attribuiti all'FTC a tutta una serie di *statues* su cui non avrebbe goduto, di regola, di "giurisdizione", molti dei quali riguardanti proprio la *privacy* individuale: ciò a dimostrazione della volontà politica di trasformare l'FTC nella «*leading privacy enforcement agency in the United States*»¹⁶⁷. Torneremo su questi profili nel quarto capitolo.

¹⁶⁶ V. infatti Federal Trade Commission Act, 15 U.S.C. §§ 41–58.

¹⁶⁷ Cfr. S.H. BONE, «Data Protection in the United States», cit., p. 305.

Il cammino della legislazione federale statunitense in materia di *privacy* prosegue con il *Family Educational Rights and Privacy Act* del 1974 (FERPA), relativo al controllo sulle informazioni degli studenti contenute in *education records*. Il potere di vigilare sulla sua applicazione è attribuito al *Department of Education*, e ai fini dell'accesso ai dati ivi contenuti da parte della pubblica autorità viene richiesto un ordine giudiziario officioso o su richiesta di parte (*lawfull subpoena*)¹⁶⁸.

Particolarmente importanti, in questo periodo, risultano in realtà quegli atti promulgati dal governo federale in risposta alle decisioni della *Supreme Court of the United States*, alcune delle quali poc'anzi analizzate, che promuovevano un'interpretazione restrittiva delle garanzie costituzionali in materia di *privacy* nei rapporti tra *citizen* e *government*: in particolare, ci si riferisce a quelle in cui la Corte enuclea e articola la c.d. *third-party doctrine*.

Il primo tra questi risulta essere il *Right to Financial Privacy Act* del 1978 (RFPA), specificamente adottato per tutelare quella categoria di *personal data* rappresentata dalle informazioni bancarie o finanziarie, o più in generale in possesso di una banca o di un istituto finanziario, a fronte di due restrittive sentenze della *Supreme Court* in materia di “*reasonable and legitimate expectation of privacy*”: quella sul caso *United States v. Miller* del 1976, già analizzata; e quella sul caso *Fisher v. United States*, in cui la Corte aveva ritenuto che non ricadessero sotto la protezione assicurata alla *privacy* dal privilegio contro l'autoincriminazione sancito dal Quinto Emendamento le informazioni registrate relative alle operazioni finanziarie di un individuo «*if an accountant maintains those records*»¹⁶⁹. Il RFPA contrasta le decisioni in questione estendendo le

¹⁶⁸ Cfr. E. MURPHY, «The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment and Statutory Law Enforcement Exceptions», in *Michigan Law Review*, 111, 2013 and 20 USC, 1232g (2012)

¹⁶⁹ Cfr. *United States v. Miller*, 425 U.S. 435 (1976); *Fisher v. United States*, 425 U.S. 391 (1976)

garanzie previste dal Quarto e dal Quinto Emendamento, a livello ordinario, agli *accounts* e alle relative informazioni conservati da o presso terzi; il suo *enforcement* è affidato al Dipartimento del Tesoro¹⁷⁰.

Continuando a seguire un approccio settoriale, il Congresso adotta nel 1984 il *Cable Communication Policy Act* (CCPA), confrontandosi così con l'emergente fenomeno dell'industria delle comunicazioni e della TV via cavo, e il *Video Privacy Protection Act* (VPPA), con cui reagisce alle decisioni della Corte Suprema che andavano riconoscendo il libero accesso - pubblico prima ancora che governativo - ai registri delle prenotazioni, nel quadro del recente *video rental* business.

Al 1988 risale il *Computer Matching and Privacy Protection Act*, con cui, prendendo atto delle novità introdotte dai programmi di ricerca automatizzati, il Congresso provvede ad emendare parte del *Privacy Act*. In sostanza, il legislatore interviene soprattutto sui punti 8-13 della lettera (a), al fine di assicurare l'uniformità procedurale nell'elaborazione dei dati, estendendo ed adattando le garanzie ivi previste ai trattamenti effettuati con mezzi automatizzati, ed istituendo specifici comitati a salvaguardia dell'integrità dei dati trattati.

Ancora, sulla spinta dell'evoluzione tecnologica, il Congresso adotta nel 1996 l'*Health Insurance Portability and Accountability Act* (HIPAA), con cui disciplina la crescente informatizzazione delle cartelle cliniche e degli archivi medici; a tale disciplina farà seguito nel 2008 il fondamentale *Genetics Information Non-Discrimination Act*, o GINA, che nell'ambito delle diverse prescrizioni introdotte vieta severamente l'uso dell'informazione genetica da parte delle compagnie assicurative. Nella nostra rapida carrellata sugli atti adottati a livello federale fino ai primi anni del ventunesimo secolo, è opportuno menzionare poi il *Children's Online Protection Act* del 1998, il *Gramm-Leach-*

¹⁷⁰ Cfr. 12 USC 3401-3422.

Bliley Act del 1999, che risponde alla nascita di nuove figure di istituto finanziario, e il *CAN-SPAM Act* del 2003.

Prima di concludere, bisogna concentrare l'attenzione su due fondamentali *statutes* fino ad ora non citati, la cui succinta analisi si è ritenuto di lasciare per ultima perché consente facilmente di evidenziare, in prima approssimazione, le lacune e le fragilità di un sistema, come quello statunitense, che difetti di una disciplina generale in materia di *privacy*. Lacune e fragilità che, di fronte all'inarrestabile progresso tecnologico e all'esercizio dei poteri di emergenza da parte del Presidente degli Stati Uniti in risposta agli attacchi terroristici dei primi anni Duemila, sembrano aver gravemente pregiudicato l'integrità della sfera privata degli ignari cittadini statunitensi (e non solo). Ci si riferisce all'*Electronic Communications Privacy Act* (ECPA)¹⁷¹, adottato nel 1986, e al *Patriot Act*¹⁷² del 2001, entrambi riconducibili a quella categoria di provvedimenti deputati a costruire un pervasivo sistema di garanzie per la sicurezza nazionale, anche attraverso disposizioni potenzialmente restrittive della *privacy* individuale, e dunque promuovendo lo sviluppo di tecnologie che parte della dottrina ha definito “pubblico-protettive”¹⁷³.

L'ECPA, invero, nasce con lo scopo di modificare e implementare l'*Omnibus Crime Patrol and Safe Streets Act*, adottato nel 1968 successivamente al caso Katz per cristallizzare a livello normativo l'interpretazione ivi sancita del

¹⁷¹ Pub. L. No. 18 U.S.C. § 2510 e ss

¹⁷² H.R. 3162.

¹⁷³ Cfr. A. ETZIONI, *How Patriotic is the Patriot Act? Freedom versus Security in the Age of Terrorism*, Routledge, New York-London 2004; lo studioso distingue tra quelle tecnologie che soddisfano un'esigenza di libera ma confidenziale condivisione delle informazioni, come i cellulari, le e-mail e le tecniche crittografiche, definite “liberalizzanti”, e tecnologie preordinate al controllo sociale in funzione di tutela della sicurezza pubblica, quali i programmi informatici impiegati dalle autorità di polizia a scopo di sorveglianza “preventiva o repressiva” (basti pensare ai celebri programmi *Carnivore* o *Magic Lantern* in quegli anni in uso all'FBI, e più di recente a *Prism*), denominate appunto “pubblico-protettive”.

Quarto Emendamento, e pertanto estendere alle comunicazioni telefoniche e ad altre forme di comunicazione via cavo le garanzie che ne derivavano: in particolare, nel suo Titolo III, meglio noto come *Wiretap Act*, esso prescriveva che la legittimità delle intercettazioni di tali comunicazioni fosse anch'essa subordinata a un *legal warrant* giudiziario fondato su una *probable cause*, poiché ricomprese nella fattispecie di *search*, o perquisizione, prevista dalla disposizione costituzionale suddetta. Ebbene, l'ECPA novella il precedente *Wiretap Act*, estendendo le garanzie del Quarto Emendamento, alla luce della *rule of law* enunciata in *Katz*, anche alle nuove forme di comunicazione elettronica nel frattempo emerse: l'insieme di disposizioni in materia è raggruppato nel Titolo II, denominato *Stored Communications Act*. Per avere chiaro il carattere di “novità” della legge, bisogna tenere presente che per “comunicazioni elettroniche” l'ECPA intende ogni trasferimento di segni, segnali, scritti, suoni, dati, e quindi qualunque tipo di informazione, che venga trasmessa attraverso le reti di telecomunicazione e via cavo, inclusi i cellulari e le comunicazioni attraverso reti private, che riguardino il commercio interstatale o con l'estero; sono incluse, all'evidenza, anche le e-mail¹⁷⁴. Per quanto attiene a ciascuna comunicazione ricadente in tale ampio bacino, l'ECPA vieta allora qualsiasi attività intercettazione, lettura o rivelazione del loro contenuto “informativo”, sanzionandole civilmente e penalmente in quanto illecite. Tuttavia, la normativa prevede una serie di eccezioni non poco rilevanti, che lo hanno reso facilmente aggirabile, oltre che controverso; e che ne ha trasformato negli anni la funzione, fino a renderlo strumento utilizzato dall'Esecutivo per fondare la legittimità dei trattamenti compiuti senza il *consent* dell'interessato, celandosi dietro il paravento delle “esigenze di sicurezza nazionale”¹⁷⁵. Innanzitutto, ai fini della legittimità della divulgazione, in ossequio alla *third party doctrine*, è sufficiente il consenso del

¹⁷⁴ V. infatti 18 U.S.C. § 2510 (12)

¹⁷⁵ V. 18 U.S.C. § 2511 (2) (g) (i) e (3) (b) (iv), che analizziamo di seguito.

destinatario (non è dunque indispensabile quello del mittente); e se la comunicazione è “facilmente accessibile”, anche in difetto del consenso è altrettanto legittima la sua rivelazione. Ma le più importanti eccezioni sono certamente quelle che si riferiscono nello specifico alle agenzie governative, alcune delle quali rafforzate dal combinato disposto con la Sezione 101 del *Foreign Intelligence Surveillance Act* del 1978. In primo luogo, gli agenti della polizia statunitense, in caso di presunta commissione di delitti, possono intercettare le informazioni contenute nelle suddette comunicazioni, attenendosi tuttavia alle specifiche procedure previste dall’ECPA a pena di inutilizzabilità delle prove nel relativo procedimento penale. Poi, è previsto che, in presenza di un mandato, gli stessi *providers* forniscano informazioni ed assistenza tecnica a soggetti autorizzati. Soprattutto, il combinato disposto con l’atto sopra menzionato consente a qualunque agenzia governativa (CIA, FBI o Pentagono indifferentemente) di avere accesso alle comunicazioni in questione o di intercettarle *anche senza un legale mandato*, laddove l’operazione persegua lo scopo di reperire informazioni dei servizi segreti stranieri ritenute essenziali per la sicurezza nazionale o per proteggere la nazione contro atti ostili (e dunque nell’ambito di – presunte - attività di controspionaggio).

Proprio le deroghe da ultimo menzionate, e in particolare il combinato disposto con la Sezione 101 del *Foreign Intelligence Surveillance Act*, hanno determinato un caso di indebita interferenza su larga scala nella *privacy* dei cittadini, in conseguenza dell’impiego indiscriminato da parte dell’FBI di *Carnivore*, uno dei più potenti sistemi di intercettazione esistenti all’inizio degli anni Duemila. *Carnivore* rappresentava una tecnologia d’intercettazione, o meglio un *software* dedicato alla raccolta di informazioni che viaggiano in una rete telematica, particolarmente all’avanguardia: non si limitava a “setacciare” le comunicazioni elettroniche, e in specie la posta elettronica, ma era capace di isolare dati su tutti i protocolli di Internet comprese le comunicazioni via *instant*

messenger e le *chat*. Impostando infatti come filtro la modalità “*full*”, il programma era in grado di visionare l’intero contenuto della comunicazione. Alla luce di alcune indagini giornalistiche, nell’anno 2000 l’FBI era stata costretta a divulgare alcuni dettagli sul funzionamento del programma medesimo; e successivamente, incalzata dalle formali richieste presentate al Congresso dall’*Electronic Privacy Information Center* (EPIC), aveva dovuto rivelare il contenuto di quasi duemila pagine di documenti secretati. Dal materiale condiviso è emerso allora che le agenzie di sicurezza governative avevano utilizzato il programma per sondare una considerevole quantità di comunicazioni private, derogando alle altrimenti stringenti procedure previste dal *Wiretap Act* in forza del combinato disposto tra ECPA e Sezione 101 del *Foreign Intelligence Surveillance Act*, adducendo come base giuridica le ricordate esigenze di sicurezza nazionale nell’ambito del controsospionaggio e talvolta disponendo del solo “informale” mandato del Ministro della Giustizia. La vicenda ha avuto ampia eco mediatica, ed ha originato una lunga sequela di proteste da parte delle associazioni per i diritti civili. Ma ciò non ha impedito alla storia di ripetersi poco dopo; e, se pensiamo al *Datagate* e al caso *Cambridge Analytica*, anche assai di recente.

Prima di chiudere questo ampio sguardo diacronico sul panorama americano della *privacy*, veniamo al secondo degli atti sopra ricordati. Successivamente ai macabri attentati dell’11 settembre 2001, culminati nella distruzione delle Torri Gemelle, il legislatore federale adotta, il 26 ottobre dello stesso anno, il *USA Patriot Act*, votato quasi all’unanimità da Congresso e dal Senato. Esso rappresenta uno dei più limpidi esempi della legislazione di emergenza varata in quegli anni negli Stati Uniti in risposta al riprovevole attacco subito, e ancor più in generale allo scopo di intraprendere la “guerra al Terrore” annunciata da George W. Bush. Esso è infatti carico di tutte le contraddizioni

proprie di tale “specie normativa”: nell’ortodosso tentativo di massimizzare l’obiettivo della sicurezza nazionale, esso compromette il bilanciamento tra quest’ultima e diritti inviolabili, nelle cui fila si colloca in posizione preminente la *privacy*; e nell’assegnare poteri ancora più ampi alle agenzie di sicurezza statunitensi, si risolve in un complesso di misure liberticide, che minano uno dei principi costitutivi di un ordinamento democratico¹⁷⁶. Contraddizioni, queste, che a ben vedere “contagiano” anche la legislazione che al di là dei confini americani tale atto ha ispirato, su pressione diplomatica del Dipartimento di Giustizia

¹⁷⁶ Occorre subito fare una precisazione sul punto, sul quale si tornerà spesso. È pressoché pacifico nella dottrina occidentale che nel difficile rapporto tra interessi pubblici particolarmente rilevanti, quali la sicurezza e la salute collettiva, e interessi individuali inerenti alla persona costituzionalmente tutelati, nessuno dei due termini risulti astrattamente prevalente sull’altro nella gerarchia dei valori costituzionali “fondamentali”. Entrambi, al contrario, debbono costituire oggetto di una inesausta opera di bilanciamento nel singolo caso concreto, o comunque nel contesto materiale, in cui interagiscono ed entrano in conflitto. Ciò, con riferimento alla *privacy* a livello europeo appare recepito già sul piano normativo, dal momento che è lo stesso articolo 8 della CEDU (adottata, lo si ricorda, nel 1950) a prescrivere, al secondo comma, che il diritto al rispetto della vita privata, del domicilio e della corrispondenza di cui al primo comma incontra come limite «gli interessi della sicurezza nazionale», che possono far apparire come «necessario nella società democratica» una legittima interferenza dell’autorità pubblica. Il disposto dell’art. 8 è stato integralmente recepito nell’art. 7 della Carta dei diritti fondamentali dell’Unione europea, in cui il bilanciamento siffatto si specifica alla luce dell’ulteriore fondamentale principio di proporzionalità consacrato nell’art. 51. È poi la stessa Corte EDU ad avere affermato in numerose pronunce che la tutela della sicurezza nazionale (es. caso *Leander v. Svezia*, 26 marzo 1987), anche ai fini di lotta al terrorismo (caso *Murray v. Regno Unito*, 28 ottobre 1994) non è a priori in contrasto con la tutela della *privacy*. La Corte, nelle medesime sentenze, ha tuttavia sottolineato come la limitazione posta in essere dal legislatore nell’esercizio della propria discrezionalità debba osservare precisi parametri di legittimità giuridica, quali il *rispetto del contenuto essenziale* del diritto individuale limitato e il criterio del minor sacrificio necessario. Parametri che, in definitiva, rappresentano un’articolazione del suddetto *principio di proporzionalità*. Alla luce di tale quadro, riservatezza protezione dei dati personali non sono dunque da intendersi come beni della vita assolutamente indisponibili, quantomeno di fronte ad interessi dalla cui integrità dipende l’esistenza stessa della comunità che esprime l’ordinamento giuridico. Ma, al contempo, la loro limitazione non può di fatto risolversi in una compressione che li *annulli*: ed è proprio questo, tuttavia, è il risultato che provvedimenti “draconiani” come il *Patriot Act* rischiano di produrre. Sul punto cfr. M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana, Relazione alla Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola*, Roma, 24-26 ottobre 2013; A. GAMBINO, «La protezione “multilevel” dei diritti fondamentali (tra Costituzioni, trattati comunitari e giurisdizioni)», in *Scritti in onore di Michele Scudiero*, AA.VV., Napoli, 2007, p.1007 ss.

americano: ci si riferisce in particolare alla c.d. Direttiva *E-Privacy* sul trattamento dei dati personali nell'ambito delle comunicazioni elettroniche, adottata nel 2002 dalla allora Comunità Europea e modificata negli anni successivi proprio per ovviare ad alcuni dei suoi profili più illiberali (come la conservazione dei dati degli utenti da parte di ISP per lungo tempo); e, a titolo di esempio tra gli Stati del continente europeo, alla normativa antiterroristica promulgata nel 2001 dal Regno Unito¹⁷⁷.

Venendo ad un sintetica disamina della sua disciplina, il rilievo storico del *Patriot Act* sta innanzitutto nell'aver esteso i poteri investigativi dei giudici sul piano federale: se una volta gli ordini di consultare gli *electronic records* (tabulati elettronici) erano validi solo per la sfera di competenza territoriale di tale giudice, con l'atto in questione la sua vincolatività è estesa a tutto il territorio nazionale (per sfruttare al massimo, è stato ipotizzato, le potenzialità della modalità “*full*” del programma *Carnivore*)¹⁷⁸. Ma forse ancor più rilevanti sono, come già anticipato, le misure fortemente restrittive per le libertà fondamentali garantite dal Primo e, soprattutto, dal Quarto Emendamento che esso introduce, molte delle quali tutt'ora vigenti. Accanto a quelle che introducono il reato di “terrorismo domestico” e che consentono nei procedimenti relativi a questi ultimi, e più in generale riguardanti casi di terrorismo, di dilazionare la comunicazione delle ricerche a carico dell'indagato, spiccano le disposizioni che, aggiungendo il paragrafo 501 al *Foreign Intelligence Surveillance Act*, configurano l'istituto nel gergo comune noto come “lettere di sicurezza nazionale”. Esso in sostanza legittima le agenzie federali (tra cui, lo ricordiamo, CIA ed FBI) a condurre

¹⁷⁷ Cfr. Direttiva 2002/58/CE del Parlamento e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, su cui torneremo *infra*; e *Anti-terrorism, Crime and Security Act* 2001, c. 24, approvato dal Parlamento di Westminster nel dicembre 2001.

¹⁷⁸ V. infatti H.R. 3162, Sez. 216A. Cfr. U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 24 ss.

investigazioni senza mandato né controllo giudiziario, e dunque ad ottenere informazioni da “terzi” sulla base di una semplice richiesta scritta, nei casi riguardanti la “sicurezza nazionale”¹⁷⁹. L’effetto di tali disposizioni è stato allora quello di estendere anche ai cittadini americani misure restrittive già previste (in primis dal *Foreign Intelligence Surveillance Act*) per i cittadini stranieri, e di renderle così applicabili anche al di fuori delle ipotesi di controspionaggio in senso stretto.

E tuttavia, sono state proprio le disposizioni in questione, unite a quelle del *Privacy Act* che ampie esenzioni garantiscono alle amministrazioni federali, a determinare ulteriori scandali, successivi a quello appena ripercorso e altrettanto caratterizzati dall’ingiustificata violazione della *privacy* individuale attraverso sistemi automatizzati di sorveglianza elettronica. Andiamo a descriverli brevemente.

Nel 2003 il Dipartimento di sicurezza nazionale statunitense annuncia il finanziamento del c.d. programma MATRIX, acronimo di *Multistate Anti-Terrorism Information Exchange*: si tratta del progetto di un *data mining system*, ovvero di edificare una banca dati a garanzia della protezione del territorio nazionale, che dovrebbe incorporare tutte le informazioni contenute nei più disparati *database* commerciali rese accessibili alle agenzie federali per effetto delle deroghe alla disciplina generale a tutela della *privacy* previste dalle disposizioni poc’anzi analizzate. Reso operativo senza che fossero predisposte adeguate misure a tutela della riservatezza, e pertanto subito fonte di critiche e perplessità sollevate da numerose associazioni, tra le quali figura in primo piano l’*American Civil Liberties Union*, nel 2004 si è poi scoperto che, facendo leva sulle finalità di salvaguardia della sicurezza nazionale, nel quadro di tale programma le agenzie federali avevano svolto attività di indiscriminata

¹⁷⁹ V. H.R. 3162, Sez. 215.

profilazione e “schedatura” nei confronti di milioni di cittadini americani, raccogliendo sistematicamente dati di ogni specie, compresi quelli riconducibili, nell’ambito dell’ordinamento europeo, alla categoria dei dati “sensibili” o “particolari” (ad esempio dati sulla fedina penale, sulla situazione patrimoniale e sui numeri del servizio sanitario nazionale dei singoli individui). Grazie alle pressioni e alle lotte civili delle suddette associazioni, nel 2005 il governo ha annunciato la definitiva dismissione del progetto MATRIX. Ma ciò non ha a quest’ultimo impedito di finanziare, negli anni successivi, ulteriori e più pericolosi progetti deputati alla profilazione e al *data mining* attraverso programmi informatici anche più potenti di *Carnivore*: e tutto ciò sempre sulla base dell’assunto - di dubbia validità logica prima ancora che scientifica - che tali strumenti fossero efficaci allo scopo di prevedere una presunta “propensione al crimine” dell’individuo e a prevenirne la conseguente condotta penalmente illecita.

Proprio nel 2004 diventa infatti operativo il *Security Fly Program*, gestito dall’Agenzia per la sicurezza dei trasporti, con l’obiettivo di integrare le informazioni sui passeggeri in volo negli USA a disposizione del governo con i database commerciali di alcune compagnie private: tra le informazioni richieste, ci sono anche i dati sul sesso, sulla data di nascita e sul numero del sistema di sicurezza sociale del passeggero. Ebbene, nonostante le rassicurazioni del *Department of Homeland Security* circa la predisposizione di misure di contrasto ad eventuali *data breach*, nel 2005 il *Government Accountability Office* indirizza una lettera al Congresso affermando che la *Transportation Security Agency* era incorsa nella violazione delle disposizioni presenti nel *Privacy Act*: essa non solo non avrebbe provveduto a garantire le specifiche protezioni richieste nella raccolta e nella conservazione dei dati, ma si sarebbe persino rivolta a società d’informazione professionale per ottenere dalle compagnie private ulteriori dati sui passeggeri. Nel 2006, l’uso illecito di tali banche dati commerciali è stato

esplicitamente ammesso con il *Report to the Public on the Transportation Security Agency's Security Flight Program and Privacy Recommendations*¹⁸⁰; ed anche tale programma è stato interrotto, sebbene poi successivamente ripreso sotto le spoglie del c.d. *Secure Flight Program*, entrato formalmente in vigore nel 2010 e avente oggi funzione di *pre-screening program* nel quadro della strategia di *security screening* implementata dalla *Transportation Security Administration*¹⁸¹.

Ripercorriamo ora in conclusione gli scandali più recenti, a decorrere dai quali la storia della legislazione americana in materia di *privacy* si è intrecciata alla storia della legislazione europea, e segnatamente all'approvazione del *General Data Protection Regulation* (GDPR)¹⁸². Il primo, che ha fortemente inciso sulla sopravvivenza degli accordi sul trasferimento transfrontaliero dei dati in vigore tra USA ed Unione europea, ossia, in ordine, *Safe Harbor* e *Privacy Shield*, è passato alla storia come *Datagate*¹⁸³. Con tale espressione si fa

¹⁸⁰ Cfr. U.S. DEPARTMENT OF HOMELAND SECURITY, *Report to the Public on the Transportation Security Agency's Security Flight Program and Privacy Recommendations*, Washington D.C., Dicembre 2006; consultabile qui: <https://www.dhs.gov/xlibrary/assets/privacy/privacy-secure-flight-122006.pdf>.

¹⁸¹ Sul programma *Secure Flight* come attualmente concepito, nel quadro dell'attività di security screening condotta dalla TSA, maggiori informazioni istituzionali sono disponibili nella pagina dedicata sul sito dell'amministrazione federale medesima: <https://www.tsa.gov/travel/security-screening>.

¹⁸² Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE; c.d. *General Data Protection Regulation* (GDPR), su cui v. ampiamente *infra*.

¹⁸³ Il caso in questione, qui in Europa, ha infatti dato origine ad una delle sentenze della Corte di Giustizia dell'Unione Europea più incisive in materia di riconoscimento del diritto alla protezione dei dati personali come diritto fondamentale e di maggior impulso alla successiva adozione del GDPR: v. infatti sin d'ora C. Giust. UE, 6-10-2015, C-362/14, *Schrems*, c.d. *Schrems I*, con cui la CGUE ha sanzionato l'invalidità della decisione di adeguatezza della Commissione Europea in merito all'accordo *U.S.-EU Safe Harbor*; e v. anche la successiva C. Giust. UE, 16-07-2020, C-311/18, *Data Protection Commissioner/Maximilian Schrems e Facebook Ireland*, c.d. *Schrems II*, con cui la Corte ha dichiarato l'invalidità della decisione di

riferimento ad una serie di inchieste giornalistiche dirette a rivelare i dettagli sulle operazioni di sorveglianza di massa poste in essere dall'Agenzia per la Sicurezza Nazionale Statunitense (NSA). A seguito delle rivelazioni di un ex agente dell'amministrazione in questione, Edward Snowden, sono stati infatti pubblicati sul *Washington Post* e su *The Guardian*, a partire dal 6 giugno 2013, alcuni documenti riservati (attinti tra i circa ventimila consegnati) da Snowden conservati durante la propria attività al servizio dell'Agenzia: questi proverebbero lo svolgimento di operazioni di profilazione su larga scala sin dagli anni Quaranta, di molto accentuatesi a partire dagli anni Settanta, nel quadro del c.d. programma *Echelon*; e, soprattutto, hanno svelato l'esistenza di nuovi e più sofisticati programmi di sorveglianza di massa, noti col nome di *PRISM*, *Xkeyscore* e *Tempora* e attuati in collaborazione con agenzie di intelligence straniere; programmi che potrebbero aver coinvolto anche cittadini europei. Confermate parzialmente dall'allora direttore dell'NSA, Keith B. Alexander, le rivelazioni in questione hanno provocato una colossale reazione dell'opinione pubblica in tutto il mondo, influenzando anche sulle successive politiche normative dell'Unione europea nel quadro dell'Agenda Digitale 2020, e accelerando l'iter di approvazione del c.d. pacchetto *privacy*¹⁸⁴.

adeguatezza del successivamente intervenuto accordo *Privacy Shield*, e contestualmente ritenuto la validità della decisione sulle *Standard Contractual Clauses*. V. nel dettaglio *infra*.

¹⁸⁴ Per una panoramica generale sul caso, cfr. già da ora G. GREENWALD, «NSA collecting phone records of millions of Verizon customers daily», in *The Guardian*, 6 giugno 2013; B. GELLMAN, «Edward Snowden, after months of NSA revelations, says his mission's accomplished», in *The Washington Post*, 24 dicembre 2013; per approfondire contenuti e conseguenze delle rivelazioni, cfr. G. GREENWALD, *No place to hide. Edward Snowden e la sorveglianza di massa*, Rizzoli, Milano, 2014; D. LYON, *Surveillance After Snowden*, Polity, 2015; sul coinvolgimento dei cittadini europei nei programmi suddetti, cfr. Commissione Europea, *Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*, COM(2013) 847 final, 27 novembre 2013; sul c.d. "pacchetto protezione dati Ue", cfr. C. RATCLIFF, M. WOSKYA, B. MARTINELLO, D. FRANCO, «L'Agenda Digitale Europea», in *Note Tematiche sull'Unione Europea*, <https://www.europarl.europa.eu/factsheets/it/sheet/64/un-agenda-digitale-europea>, 2023.

Le ultime, assai recenti vicende di *mass surveillance* cui facciamo riferimento sono quelle riguardanti il cosiddetto scandalo *Facebook-Cambridge Analytica*, che, sebbene non coinvolgano direttamente l'Esecutivo in quel momento in carica, tuttavia hanno avuto un'influenza determinante sull'esito delle elezioni politiche americane del 2016, con la vittoria dell'allora candidato repubblicano alla Presidenza degli Stati Uniti d'America Donald Trump. Cambridge Analytica era una società dedita all'attività di profilazione di utenti digitali a scopo, principalmente, di marketing elettorale, e dunque di predisposizione di campagne politiche personalizzate: essa era parte della più ampia realtà degli *Strategic Communication Laboratories*, società che offriva servizi di marketing e di comunicazione politica basandosi su tecniche psicometriche, spesso richiesti dalla Difesa e da altre realtà del governo britannico. Nel 2016, grazie al *whistleblowing* dell'ex dipendente Christopher Wylie, si è scoperto che la stessa aveva ottenuto e trattato illecitamente, e segnatamente in difetto del loro consenso, i dati di quasi cinquanta milioni di fruitori di Facebook, mediante l'utilizzo di un test della personalità (l'app *Thisisyourdigitallife*) capziosamente proposto a migliaia di utenti dietro autorizzazione ad accedere a tutti i dati riguardanti non solo i medesimi, ma anche i terzi di cui risultassero "amici" sulla piattaforma. I profili elaborati a partire dai dati in questione sarebbero stati poi utilizzati per suggerire contenuti e somministrare annunci personalizzati agli utenti coinvolti, in particolare riguardanti la campagna a favore del referendum in ordine al recesso dai trattati istitutivi dell'Unione europea del Regno Unito (c.d. Brexit) e, come già anticipato, la campagna di Trump nel quadro delle elezioni presidenziali americane del 2016, orientando così il consenso popolare in ordine a questi e ad altri rilevanti fenomeni elettorali. A seguito di tali rivelazioni, una tempesta di critiche ha travolto Facebook e il suo fondatore e CEO Mark Zuckerberg, chiamato a testimoniare sui fatti davanti al Congresso di Washington;

parallelamente, la società suddetta ha dichiarato fallimento¹⁸⁵. La vicenda, in ogni caso, ha avuto al pari del *Datagte* un profondo impatto sull'opinione pubblica globale, tanto che il Parlamento Europeo l'ha definita come uno spartiacque nella comprensione pubblica del valore dei dati personali: presupposto per la libera costruzione della propria personalità, prima ancora che risorsa economica¹⁸⁶.

Ora che abbiamo tracciato sinteticamente anche il profilo di quei fenomeni che, originati sul suolo americano, hanno assunto una dimensione transnazionale, mutando per sempre la sensibilità della società civile e l'attenzione dedicata dai legislatori alla protezione dei dati personali, possiamo lasciare le sponde del Nuovo Continente, per procedere con l'esplorazione dei terreni della "vita privata" nell'ordinamento internazionale e nel Vecchio Continente. Dove la *privacy*, all'esito di un lungo percorso teorico, si sdoppia anche sul piano positivo, facendosi *anche* diritto fondamentale alla protezione dei dati personali, esplicitamente sancito tanto dagli Stati Membri quanto dalle norme "supreme" dell'ordinamento europeo: un diritto autonomo, di rango costituzionale, che brilla intensamente nel *pantheon* dei diritti di "nuova generazione"¹⁸⁷.

¹⁸⁵ Sul caso in generale, si veda H. PARKINSON, «Click and Elect: How Fake News Helped Donald Trump Win a Real Election», in *The Guardian*, 14 novembre 2016; N. CONFESSORE, «Cambridge Analytica and Facebook: The Scandal and the Fallout So Far», in *The New York Times*, 4 aprile 2018; A.G. PARISI, «Dati, proliferazione e social network: l'emersione di un nuovo modello giuseconomico», in P. Stanzone (a cura di), I "poteri privati" delle piattaforme, cit., p. 192 ss.

¹⁸⁶ Cfr. PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo sull'utilizzo dei dati degli utenti Facebook da parte di Cambridge Analytica e l'impatto sulla protezione dei dati*, 2018/285, 28 ottobre 2018, consultabile qui: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_IT.html.

¹⁸⁷ Ci si riferisce qui alla nota classificazione dei diritti umani in generazioni: la prima sarebbe costituita dalle libertà negative, la seconda dai diritti economici e sociali (libertà positive), e la terza dai diritti di solidarietà, quale i diritti alla pace e alla tutela dell'ambiente. Per un quadro generale, cfr. cfr. L. FAVOREAU, «Diritti dell'uomo», in *Enciclopedia Treccani*, Roma, 1998. Si discute in epoca recente anche di diritti di quarta generazione, in cui ricadrebbero quei diritti collegati ai progressi della tecnica e della scienza, ad esempio nel campo delle biotecnologie e dell'informatica: cfr. ad es. S. M. HELMONS, «La quatrième

génération des droits de l'homme», in *Les droits de l'homme au seuil du troisième millénaire*, Bruxelles, Bruylant, 2000.

CAPITOLO SECONDO

BANCHE DATI E VITA PRIVATA: LA *PRIVACY* NELL'ORDINAMENTO INTERNAZIONALE E IN EUROPA. IL CONTESTO TECNOLOGICO DELLA *DATA DRIVEN SOCIETY*

SOMMARIO: 2.1. Dalla CEDU alla Convenzione 108 sul trattamento automatizzato dei dati «a carattere personale» - 2.2. Vita privata e società dell'informazione. Le Costituzioni europee del secondo dopoguerra - 2.2.1. Individualrechte, protection de la vie privée, diritto al riserbo: le origini della “vita privata” in Europa – 2.2.2. Riservatezza, banche dati, autodeterminazione informativa: la costruzione della privacy nella legislazione, nella giurisprudenza e nella dottrina degli ordinamenti nazionali del «Vecchio Continente». In particolare, uno sguardo all'Italia – 2.2.3. Dalla Direttiva 95/46/CE al Trattato di Lisbona: il processo di “costituzionalizzazione europea” del diritto fondamentale alla protezione dei dati personali – 2.2.4. L'approdo: il ruolo della Corte di Giustizia come “giudice dei diritti fondamentali”, il Pacchetto Protezione Dati e l'EU-U.S. Data Privacy Framework – 2.3. Big Data, trattamenti algoritmici e Intelligenza Artificiale: alcuni concetti fondamentali nel contesto tecnologico della data driven society

2.1. La costruzione giuridica della *privacy* nell'ordinamento internazionale e in Europa. Dalla CEDU alla Convenzione 108 sul trattamento automatizzato dei dati «a carattere personale».

La composita categoria filosofica e giuridica della *privacy* fa la sua prima apparizione nei documenti internazionali a partire dal secondo dopoguerra; e, tuttavia, non già come autonomo istituto, bensì quale specificazione, evidenziata dalla dottrina e progressivamente dalla giurisprudenza, di un più generale (o sarebbe meglio dire generico) *diritto al rispetto della vita privata e familiare*.

Il riferimento va innanzitutto alla Dichiarazione universale dei diritti dell'uomo del 1948, il cui articolo 12 si esprime nei seguenti termini: «Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua *vita privata*, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni»¹⁸⁸. Successivamente, è la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali che nel 1950 delinea nel suo articolo 8 una delle più perentorie e cristalline affermazioni del diritto all'integrità della vita privata dell'individuo, la cui portata semantica e il cui perimetro applicativo saranno progressivamente allargati dalla Corte Europea per la salvaguardia dei diritti dell'uomo (CEDU). L'art. 8, rubricato eloquentemente "*Diritto al rispetto della vita privata e familiare*" recita infatti, al primo comma: «Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza», salvo prevedere poi al secondo comma alcune eccezioni per lo più motivate da esigenze di tutela di interessi pubblici particolarmente rilevanti per la collettività o di altri interessi individuali presidiati da uno dei diritti fondamentali consacrati nella

¹⁸⁸ V. Dichiarazione Universale dei Diritti Umani, 1948, art. 12. Ricordiamo che, sebbene le Dichiarazioni di Principi dell'Assemblea Generale delle Nazioni Unite non costituiscano un'autonoma fonte formale di produzione del diritto nell'ordinamento internazionale, la dottrina è unanime nel riconoscergli, accanto al comune valore persuasivo e alla funzione talvolta "ricognitiva" di norme consuetudinarie già vigenti, anche un ruolo attivo nella formazione del diritto internazionale in quanto *prassi degli Stati*: su questi e su altri effetti dell'istituto suddetto, cfr. B. CONFORTI, *Diritto Internazionale*, (a cura di) Massimo Iovine, Editoriale Scientifica, Napoli 2018, XI Edizione, p. 67 ss..

Convenzione: «Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui»¹⁸⁹. La stessa CEDU offre del diritto in questione una declinazione anche in ambito processuale, nel contesto dell'art.6: «Ogni persona ha diritto ad un'equa e pubblica udienza entro un termine ragionevole (...). La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o una parte del processo (...) quando lo esigono gli interessi dei minori o *la tutela della vita privata* delle parti in causa (...)».

Allo stesso modo, nel 1966 la vita privata è riconosciuta quale oggetto di un diritto fondamentale, la cui promozione e la cui difesa sono imposte agli Stati contraenti, dal Patto Internazionale per i diritti civili e politici, che all'art. 17 stabilisce: «Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione»¹⁹⁰.

Secondo parte della dottrina, proprio la suddetta impostazione adottata in seno al diritto internazionale avrebbe dato impulso affinché mutasse la sensibilità dei legislatori nazionali, in particolare europei, in ordine alla concezione di vita privata da accogliere, e consequenzialmente del regime giuridico cui assoggettarla: se infatti fino più o meno al secondo conflitto mondiale essa aveva ininterrottamente rappresentato quel paradigma di decoro e di rispettabilità

¹⁸⁹ V. Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (CEDU), Roma, 1950, art. 8.

¹⁹⁰ V. Patto internazionale sui diritti civili e politici, adottato dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966, entrato in vigore internazionale il 23 marzo 1976, art. 17.

borghese tipico degli Stati liberali ottocenteschi, a partire dalle “Carte” che configurano - o piuttosto consolidano - principi che paiono “comuni alle nazioni civili”, e dunque *imperativi* sul piano internazionale, la “vita privata” comincia ad assurgere ad autonomo bene giuridico, coincidente con la sfera più intima del soggetto¹⁹¹. Non è un caso allora che la Corte Costituzionale italiana già nel 1969 affermasse come la CEDU abbia «nei confronti delle correlative norme della Costituzione, qualche sfumatura di migliore precisazione della tutela della riservatezza»¹⁹². E, potremmo aggiungere, non solo della riservatezza.

L'impostazione cui abbiamo appena fatto riferimento, infatti, è stata avallata ripetutamente anche dalla Corte Europea per la salvaguardia dei diritti dell'uomo, che nella sua opera di incessante interpretazione (anche evolutiva) delle disposizioni della CEDU ha progressivamente ampliato, nel corso degli anni, il perimetro della nozione giuridicamente rilevante, a livello internazionale, di vita privata, e dunque le situazioni protette nell'alveo dell'art.8 della CEDU; rendendola, in tal mondo, una nozione plastica, capace di accogliere nel suo bacino molteplici aspetti del “prisma” persona umana, che corrono dall'integrità psicofisica fino, come vedremo, alla protezione in senso stretto dei dati che «esprimono informazioni personali»¹⁹³. Un rapido sguardo alle pronunce della

¹⁹¹ Cfr. M. LUCIANI, *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, studio commissionato dal Servizio Ricerca del Parlamento Europeo (EPRS), 10/2018, p. 3 ss. Sull'orientamento che ascrive allo *jus cogens*, ossia al diritto internazionale generale inderogabile, il nucleo essenziale dei diritti umani, stante la loro radice consuetudinaria e quindi indipendentemente dalla relativa inclusione nei dettagliati elenchi previsti dalle Dichiarazioni di principi dell'Assemblea Generale dell'ONU (documenti non aventi valore giuridico vincolante) o dalle molteplici convenzioni internazionali in materia (quali fonti secondarie di diritto internazionale), cfr. in particolare, B. CONFORTI, *Diritto Internazionale*, cit., p. 214 ss.; VILLANI, *Dalla Dichiarazione universale alla Convenzione europea dei diritti dell'uomo*, Bari, 2015.

¹⁹² C. Cost., 26 Giugno 1969, n. 104, in *Foro It.*, vol. 92, no. 9, 1969, p. 2083/2084 ss.

¹⁹³ Cfr. S. BARTOLE, P. DE SENA, G. ZAGREBELSKY, *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, Art. 8. Si riferisce alla persona umana come a un “prisma” di attributi fondamentali G. FINOCCHIARO, «Identità personale (diritto alla)», in *Digesto/civ.*, Agg., Torino, 2010, come vedremo meglio *infra*.

Corte consente di rilevare, senza pretese di esaustività, come essa abbia ricompreso nell'ambito dell'art. 8 il diritto al nome¹⁹⁴; alla protezione degli elementi che si riferiscono alla propria immagine, in particolare a fronte della sua pubblicazione, ricadendo nel "margine di apprezzamento" degli Stati contraenti la definizione del giusto equilibrio tra rispetto della vita privata e libertà di espressione e di stampa, tutelata ai sensi dell'art.10¹⁹⁵; ed anche il diritto al riconoscimento e all'accertamento del legame di filiazione con il padre biologico e quello a "conoscere le proprie origini"¹⁹⁶. Per quel che qui più interessa, la Corte ha poi definitivamente ricompreso nella nozione di vita privata il "bene giuridico" rappresentato dalla protezione dei dati personali, così da ritenere i due interessi, se non in rapporto di genere a specie, quanto meno *tangenti*¹⁹⁷. Esso viene gradualmente inteso dalla Corte, in seguito alla lunga elaborazione teorica che come diremo coinvolgerà dottrina e giurisprudenza di tutti gli ordinamenti del Vecchio Continente, quale referente oggettivo di un diritto "moderno", che presidia la dimensione attiva della libertà personale quale pretesa di instaurare un sistema di controlli e di equilibri nella gestione delle informazioni che la persona medesimo riguardano; e la Corte stessa amplierà a mano a mano il catalogo delle informazioni personali rilevanti ai sensi dell'articolo 8 medesimo¹⁹⁸. Merita poi sul punto ricordare come la Corte abbia con forza affermato il principio, desumibile dal sistema oltre che dalla lettera delle disposizioni della Convenzione (compreso dunque l'art. 8), per cui la norma in questione non solo obblighi gli Stati ad astenersi da qualsiasi azione possa risolversi in una violazione della vita

¹⁹⁴ V. Corte EDU, *Henry Kismoun c. Francia*, V sez., 5 dicembre 2013.

¹⁹⁵ V. Corte EDU, *Von Hannover c. Germania*, V. sez., 19 settembre 2013.

¹⁹⁶ V. Corte EDU, rispettivamente, *Mennesson c. Francia*, Grande Camera, 26 giugno 2014; *Godelli c. Italia*, 2 sez., 25 settembre 2012.

¹⁹⁷ Si possono citare tra le molte Corte EDU, *Malone c. Regno Unito*, 2 agosto 1984 e *Leander c. Svezia*, 26 marzo 1987.

¹⁹⁸ Cfr. Corte EDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008, su cui vedi sinteticamente a breve.

privata dei loro cittadini, bensì anche, a seconda delle fattispecie, ad intraprendere azioni positive al fine di garantirne l'effettivo rispetto sul proprio territorio¹⁹⁹. Tutti questi rilievi hanno avuto negli anni significative ricadute sul diritto interno, tanto oggettivo quanto *vivente*, degli Stati contraenti, contribuendo all'affermazione nei rispettivi ordinamenti di una costellazione di autonomi, e tuttavia complementari, diritti della personalità costituzionalmente fondati, e alla contestuale compiuta elaborazione di un diritto alla protezione dei dati personali emancipato dal diritto alla riservatezza, quest'ultimo inteso come presidio della dimensione solo negativa della "vita privata". Tale contributo pare ulteriormente amplificato dal valore giuridico riconosciuto dagli stessi al prodotto dell'incessante attività esegetica svolta dalla Corte di Strasburgo. Limitandoci qui a porre l'attenzione sull'ordinamento italiano, risalgono infatti al 2008 le celebri sentenze gemelle con cui la Corte ha esplicitamente riconosciuto, dopo un lungo percorso ermeneutico, il carattere di norme interposte nel giudizio di legittimità costituzionale, rispetto all'art. 117, delle regole sancite dalla Convenzione (al pari di qualsiasi altro accordo internazionale), ed ha al contempo individuato con parole cristalline come, alla luce delle specificità del sistema CEDU, «tra gli obblighi internazionali assunti dall'Italia con la sottoscrizione e la ratifica della CEDU vi è quello di adeguare la propria legislazione alle norme di tale trattato, *nel significato attribuito dalla Corte specificamente istituita per dare ad esse interpretazione ed applicazione*»²⁰⁰.

In materia, poi, la Corte europea dei diritti dell'uomo ha svolto un altro ruolo di capitale importanza storica, cui abbiamo già fatto incidentalmente cenno:

¹⁹⁹ Cfr., per esempio, Corte EDU, *I c. Finlandia*, n. 20511/03, 17 luglio 2008.

²⁰⁰ Cfr. Corte Cost., sentt. nn. 348 e 349 del 2007. Nel mare di letteratura esistente sulle fondamentali sentenze in parola, cfr. ad es. F. DONATI, «La CEDU nel sistema italiano delle fonti del diritto alla luce delle sentenze della Corte costituzionale del 24 ottobre 2007», in *www.osservatoriosullefonti.it*, n. 1/2008; M. CARTABIA, «Le sentenze "gemelle": diritti fondamentali, fonti, giudici», in *Giur.cost.*, 2007, 3565 ss.

essa ha rappresentato, nel contesto “regionale” europeo, il primo arbitro “sovrannazionale” della naturale e incessante dialettica, e insieme di garante del delicato ma imprescindibile equilibrio, tra “integrità” della vita privata e interessi pubblici -prima ancora che individuali, sebbene di carattere fondamentale-concorrenti, quale appunto l’interesse alla sicurezza nazionale, reso sempre più insidioso dall’escalation tecnologica in corso, su cui tanto abbiamo insistito alla fine del primo capitolo. È infatti lo stesso secondo comma dell’art. 8 a prescrivere che il diritto al rispetto della vita privata, del domicilio e della corrispondenza, con forza affermato al primo comma, incontra come limite «gli interessi della sicurezza nazionale», che possono far apparire come «necessario nella società democratica» una legittima interferenza dell’autorità pubblica. Pur rientrando nella discrezionalità normativa degli Stati contraenti la positiva definizione delle tassative ipotesi in cui derogare al suddetto divieto di “ingerenza”, la Corte ha prontamente risposto negli anni alle ripetute richieste di vagliare la legittimità delle disposizioni interne restrittive della vita privata, segnatamente sotto il profilo della riservatezza e dell’“inaccessibilità” dei dati personali, svolgendo una sistematica operazione di bilanciamento deputata ad assicurare il rispetto del contenuto essenziale di questo e degli altri diritti a difesa dell’inviolabilità degli attributi fondamentali della personalità umana²⁰¹. La stessa Corte ha quindi avuto modo di conoscere numerose vicende in cui riservatezza e “autodeterminazione informativa” si confrontassero con interventi nazionali restrittivi in funzione della tutela degli interessi alla sicurezza collettiva e all’ordine pubblico: da quelle riguardanti l’intercettazione indebita di comunicazioni (come il già citato caso

²⁰¹ Vedi retro, nota 174. Cfr. poi, ad esempio, in materia di vita privata, Corte EDU (Grande Camera), nn. 12738/10, *Jeunesse c. Olanda*, 3 ottobre 2014, in cui la Corte, nell’offrire un quadro della propria funzione di equo contemperamento tra diritto inviolabile ed interesse pubblico e dei criteri alla luce del quale svolgerlo, ha ricordato come debba sussistere «un principio di proporzionalità tra la misura [restrittiva introdotta dallo Stato contraente] e lo scopo [d’interesse pubblico] perseguito».

Malone c. Regno Unito del 1987) fino a quelle inerenti alle garanzie nella conservazione dei dati da parte della pubblica amministrazione (ad es. *Roman Zakharov c. Russia* del 2015). E in tutti questi casi la Corte, sottolineando il ruolo di custode della funzione appena descritta, non ha esitato ad affermare che le attività di sorveglianza configurano gravi rischi di interferenza nel rispetto della vita privata (es. *Klass e a. c. Germania*, 1978), contribuendo ad arginare in questo modo fenomeni di profilazione sistematica sempre più comuni nella società della “sorveglianza liquida”²⁰². Per citare solo uno tra i casi che più emblematicamente testimoniano quanto detto, basti pensare alla sentenza adottata dalla Corte in tempi non più recentissimi (4 dicembre 2008) nel già poc’anzi ricordato caso *S. e Marper contro Regno Unito*: nella specie, essa ha condannato lo Stato britannico per le modalità di conservazione di taluni dati sensibili degli individui, tra cui, soprattutto, campioni di materiale biologico nel *National Dna Database*, e segnatamente perché la conservazione illimitata nel tempo di dati appartenenti a cittadini nei confronti dei quali fosse intervenuta sentenza irrevocabile di proscioglimento avrebbe violato il loro diritto di questi ultimi al rispetto della vita privata²⁰³.

Forse, tuttavia, lo strumento giuridico più importante in punto di *privacy* adottato nell’ordinamento internazionale, e allo stesso tempo il primo che abbia disciplinato in modo *vincolante* per gli Stati contraenti la materia della *data*

²⁰² L’evocativa ed efficace espressione è tratta dal brillante libro intervista di D. LYON, Z. BAUMANN, *Liquid surveillance*, Polity Press, 2013; con essa, i due autori, fondendo dialogicamente i risultati delle rispettive pluriennali ricerche, identificano quello che ritengono il connotato precipuo dell’individuo del ventunesimo secolo, ossia la costante “visibilità”: l’esposizione di ciascuno di noi, a causa di *smart phones*, *social networks*, piattaforme di *e-commerce*, ecc., alla capacità dell’altro, indifferentemente soggetto pubblico o privato, di invadere l’intimità, ricostruirne la morfologia ed alterare le multiformi proiezioni esterne, per lo più virtuali, della nostra personalità, per mezzo dell’analisi dei dati che ci riguardano, anche *algo-created*.

²⁰³ Cfr. Corte EDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008.

protection, è la Convenzione interamente elaborata ed approvata in seno al Consiglio d'Europa, all'esito di un lungo dibattito circa lo "stato" della legislazione, della giurisprudenza e della dottrina in punto di *privacy* nei singoli Stati membri, nel quadro dell'esponentiale sviluppo della "società dell'informazione" registratosi a partire dagli anni Sessanta: ci riferiamo alla nota Convenzione n. 108 del 1981 sul *trattamento automatizzato* dei dati di carattere personale²⁰⁴. Essa, in realtà, è stata preceduta di un solo anno dalle Linee Guida dell'OCSE in materia di *privacy* e di trasferimenti internazionali di dati personali²⁰⁵, che, come abbiamo ricordato, parte della dottrina soprattutto di oltreoceano ritiene siano state ampiamente influenzate dall'elaborazione delle FIPs da parte dell'HEW in contesto statunitense²⁰⁶. Nonostante il virtuoso obiettivo di armonizzare la disciplina degli Stati membri dell'organizzazione medesima nelle materie in questione, le Linee Guida non hanno efficacia giuridica vincolante per gli stessi; e soprattutto, in conformità dello scopo istituzionale dell'organizzazione, rivolgono un'attenzione marcata al libero trasferimento dei dati quale requisito essenziale per promuovere lo sviluppo economico degli Stati stessi, che un'indebita restrizione dei *personal data transborder flows* potrebbe piuttosto pregiudicare²⁰⁷.

²⁰⁴ CONSIGLIO D'EUROPA, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, n. 108/1981.

²⁰⁵ OCSE, *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data*, 1980, <https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf>.

²⁰⁶ V. *retro*, p. 62.

²⁰⁷ Ricordiamo infatti che l'OCSE, acronimo di *Organisation for European Economic Cooperation* fu istituita il 16 aprile 1948 dalla cosiddetta *Conference of Sixteen o Conference for European Economic Cooperation* allo scopo di gestire gli investimenti finanziari compiuti in Europa in attuazione del Piano Marshall. Sia consentito rinviare, sul punto, alla pagina del sito ufficiale dell'OCSE che inquadra storicamente la nascita dell'organizzazione medesima: <https://www.oecd.org/60-years/timeline/>. Per quanto attiene agli scopi perseguiti dal documento in esame, si veda innanzitutto il memorandum esplicativo: OCSE, *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data - Explanatory Memorandum*, <https://www.oecd.org/digital/explanatory-memoranda-of-the-oecd-privacy-guidelines-ea4e9759-en.htm>; per un commento, cfr. G. SCARCHILLO, «Dal Safe Harbor al

La Convenzione invece, in quanto fonte di diritto internazionale secondario, com'è noto vincola giuridicamente gli Stati contraenti: entrata in vigore per l'Italia nel luglio del 1997, essa è stata ratificata da tutti gli Stati membri del Consiglio d'Europa, ad eccezione della Turchia, e progressivamente da un numero sempre maggiori di Stati terzi, a dimostrazione della sua vocazione a farsi strumento giuridico vincolante a livello universale²⁰⁸. Quest'ultima poi, a differenza delle summenzionate Linee Guida, ha quale preciso obiettivo quello di promuovere la salvaguardia e di massimizzare la tutela dei diritti fondamentali, e segnatamente del diritto al rispetto della vita privata, nel nuovo e insidioso contesto tecnologico globale, come si evince già dal disposto dell'art. 1: «Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, *in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ("protezione dei dati")*»²⁰⁹. Proprio quest'ultimo inciso, sebbene da una parte sottolinei il ruolo pionieristico svolto dal Consiglio d'Europa nel cogliere la dimensione positiva o "informazionale" della *privacy*, rivela però il carattere (almeno formalmente) settoriale della Convenzione, il cui ambito di applicazione risulta appunto circoscritto al fenomeno del trattamento *automatizzato* dei dati riguardanti la persona fisica.

Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems», in *Diritto del Commercio Internazionale*, Anno XXX, Fasc. 4, 2016, p. 901 ss.

²⁰⁸ Per un aggiornato elenco degli Stati che abbiano ratificato la Convenzione, si veda la tabella presente sull'apposita pagina del sito ufficiale del Consiglio d'Europa: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=108>.

²⁰⁹ L'art. 4, consequenzialmente, prescrive poi (secondo la "logica dell'azione positiva" propria di quasi tutti i Trattati internazionali sui diritti umani) che "Ciascuna Parte adotta, nell'ambito del suo diritto interno, le misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati enunciati nel presente capitolo".

Approfondiremo l'analisi di alcuni aspetti di dettaglio dell'atto normativo in questione, nonché delle risoluzioni e dei documenti di natura non vincolante che l'hanno preceduto, nel prossimo paragrafo. Tuttavia occorre qui soffermarsi in breve sulla struttura e sul contenuto della normativa in parola, dal momento che, come è Stato autorevolmente sottolineato, essa contiene la maggior parte dei principi che ancora oggi delineano, quanto meno nell'ordinamento europeo e in quello dei suoi Stati membri, la disciplina della protezione dei dati personali²¹⁰. Principi che hanno dunque rappresentato il modello cui si è successivamente conformata l'allora Comunità Europea per adottare nel 1995 il primo strumento normativo, nella forma della Direttiva, deputato a "ravvicinare le disposizioni nazionali" in materia di trattamento dei dati personali in tutti i suoi Stati membri²¹¹.

Passando velocemente in rassegna tali principi, di carattere evidentemente generale - stante la natura della fonte -, fondamentali appaiono innanzitutto quelli sulla qualità delle informazioni trattate (in particolare, liceità, adeguatezza e pertinenza: art. 5), sul divieto di trattamento automatizzato (*rectius*, di elaborazione automatizzata: "trattamento" è espressione invalsa solo successivamente, con la Direttiva 95/46/CE) di dati sensibili e di dati riguardanti condanne penali *in assenza di appropriate garanzie* (art. 6) e la necessità di disporre idonee misure di sicurezza per la protezione dei dati.

Ancor più importante appare l'articolo 8, di notevole portata innovativa, poiché garantisce agli interessati i diritti di accesso, di rettifica e di cancellazione dei dati, nonché l'obbligo d'informazione a carico dei titolari circa l'identità e i

²¹⁰ Cfr. in particolare F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 60 ss; G BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, Milano, 1997, p. 8 ss.

²¹¹ Il riferimento è ovviamente alla Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

riferimenti del responsabile della raccolta e dell'*elaborazione* dei dati e il diritto ad un effettivo ricorso giurisdizionale in caso di violazione di tali diritti (non contemplando ancora, tuttavia, la possibilità se non l'obbligo di costituire un'Autorità amministrativa indipendente a ciò preposta).

Infine, il Capitolo III della Convenzione, debitore in ciò del lavoro compiuto dall'OCSE con le suddette Linee Guida, ambisce a disciplinare il fenomeno del trasferimento transfrontaliero dei dati personali, sancendo il principio, contrastato tuttavia da rilevanti eccezioni a garanzia dell'integrità della vita privata, della libera circolazione dei dati personali verso altri Stati parte della Convenzione (sull'evidente presupposto implicito che tali Stati, in conformità dei vincoli previsti dalla stessa Convenzione, garantiscano uno standard di tutela analogo a quello dei Paesi di provenienza dei dati ²¹²).

È opportuno concludere l'analisi sul punto ricordando che nel 2018, in occasione dei 40 anni dall'apertura alla firma della Convenzione medesima, il Consiglio d'Europa ha promosso un'opera di profonda modernizzazione della disciplina enucleata dalla stessa, attraverso l'adozione di un Protocollo di Emendamento non entrato ancora in vigore²¹³. Nel report esplicativo, accanto al rilievo posto sull'idoneità della Convenzione, nei suoi decenni di vigenza, a rappresentare « *[the] foundation for international data protection law in over 40*

²¹² Sul requisito rappresentato dall'esistenza, nel Paese di destinazione, di uno "standard di tutela dei dati personali *equivalente*" a quello predisposto nell'ordinamento dello Stato (europeo) di provenienza, molto insisterà negli anni Dieci la Corte di Lussemburgo nel giudicare della validità delle decisioni di adeguatezza degli accordi sui *transborder flows* di dati personali tra USA e UE adottate dalla Commissione Europea: v. *infra*, e già da ora v. C. Giust. UE, 16-07-2020, C-311/18, Data Protection Commissioner/Maximilian Schrems e Facebook Ireland, par. 150 ss., consultabile qui: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11388612>

²¹³ Cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108), 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e#globalcontainer.

European countries», influenzando peraltro le politiche e la legislazione di Stati situati ben oltre le frontiere europee, il Comitato sottolinea come l'esigenza dell'adeguamento della normativa alla nuova realtà sociale derivi dalle nuove sfide (e, insieme, insidie) cui ha esposto l'integrità della sfera privata principalmente lo sviluppo delle ICTs ²¹⁴: su tutte, le nuove tecnologie algoritmiche in punto di elaborazione dei dati, che, come vedremo, nella più moderna economia del GDPR impongono il rispetto del "nuovo" principio di *privacy by design*.²¹⁵

Merita sin d'ora evidenziare la particolare importanza del nuovo articolo 9 della suddetta Convenzione modernizzata (108+): quest'ultimo introduce il diritto di ogni individuo a *non essere soggetto ad una decisione esclusivamente automatizzata* che incida significativamente sulla propria sfera giuridica, senza che gli venga garantita la possibilità di esprimere la propria opinione. Sembrerebbe instaurarsi un virtuoso parallelismo tra la disposizione in esame e l'art 22 GDPR, il cui ambito di applicazione, la cui portata semantica e il cui significato giuridico ci occuperanno nel terzo capitolo. Bisogna tuttavia subito

²¹⁴ Il Consiglio d'Europa sembra in questo modo dare seguito alla Raccomandazione prodotta all'esito del lungo dibattito sugli effetti della profilazione attraverso sistemi automatizzati, adottata nel 2010: cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, CM/Rec(2010)13, 23 novembre 2010, ove a titolo introduttivo si afferma che « il continuo sviluppo di [ICTs] convergenti pone nuove sfide in termini di raccolta e trattamento ulteriore dei dati ».

²¹⁵ Cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – Explanatory Report*, 17-18 maggio 2018, nella cui introduzione si legge: « (...) With new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that the Convention should be modernised in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies (IT), the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism. ». Cfr. sul punto G. DE GREGORIO, R. TORINO, «Privacy, tutela dei dati personali e Big Data», in E. Tosi (a cura di), *Privacy digitale*, Giuffrè Francis Lefebvre, pp. 447-484.

aggiungere che nella già citata Relazione Esplicativa il Comitato *ad hoc* per la protezione dei dati ha specificato che, in virtù del nuovo articolo 9, i soggetti interessati hanno il *diritto di contestare* la decisione automatizzata, esponendo la propria opinione²¹⁶. Tale interpretazione della disposizione potrebbe suscitare il sospetto che, a differenza del GDPR (almeno alla luce dell'interpretazione dell'art. 22 promossa dal Gruppo di Lavoro Articolo 29 e fatta propria da un ampio numero di commentatori), la Convenzione 108+ si sia limitata a riconoscere un diritto attivo di opposizione, evitando di fissare un vero e proprio divieto generale di trattamento unicamente automatizzato dei dati a fini decisionali²¹⁷.

2.2. Vita privata e società dell'informazione: le Costituzioni europee del secondo dopoguerra

Abbandonando ora il piano internazionale, e rinviando ad un secondo momento l'analisi della compiuta positivizzazione nell'ordinamento europeo di un autonomo diritto *fondamentale* alla protezione dei dati personali, distinto tanto dal diritto al rispetto della vita privata e familiare quanto dal diritto alla riservatezza, focalizziamo ora l'attenzione sulle vicende che hanno contrassegnato la lunga gestazione dell'autonomo istituto della *privacy* in seno ai singoli ordinamenti nazionali del continente europeo.

²¹⁶ V. infatti il dettato dell'art. 11, par. 2, di. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, 2018: « 2. The text of Article 8 of the Convention (new Article 9) shall be replaced by the following: “1. Every individual shall have a right: a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration (...)»

²¹⁷ Cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – Explanatory Report*, §75.

Considerata la caratteristica propria dello *stile del sistema giuridico*²¹⁸ di quasi tutti gli Stati del continente europeo, appartenenti alla tradizione di *civil law*, ovvero l'esistenza di Costituzioni *formali e rigide*, adottate nel secondo dopoguerra, che rappresentano la fonte *suprema* di produzione del diritto negli ordinamenti considerati, occorre rivolgere un rapido sguardo alle Costituzioni medesime, per cominciare ad interrogarsi sul dato positivo, vivificato poi dalla giurisprudenza.

È noto, innanzitutto, che la Costituzione italiana, entrata in vigore il primo gennaio del 1948, non contiene alcun esplicito riferimento alla tutela della riservatezza nel testo consegnatoci dall'Assemblea Costituente: essa, pur così attenta al futuro, poca attenzione ha prestato ai potenziali rischi configurati dalla tecnologia rispetto all'integrità dei principi e dei diritti fondamentali limpidamente sanciti nelle sue disposizioni²¹⁹. Tuttavia, dottrina e giurisprudenza di merito e di legittimità (quella costituzionale invece, come più avanti vedremo, è stata per lo più restia a pronunciarsi sull'inquadramento sistematico dell'istituto in esame) hanno nel corso degli anni individuato a livello esegetico, non senza contrasti, una pluralità di principi fondamentali, consacrati nella nostra Carta,

²¹⁸ L'espressione, qui interpretata in senso lato, rinvia alla nota classificazione "sistemologica" propugnata da K. ZWEIGERT, H. KOTZ, *Introduzione al diritto comparato. Vol. I: principi fondamentali*, Giuffrè, Milano 1998.

²¹⁹ Infatti, l'unico mezzo d'informazione che appare direttamente disciplinato in Costituzione (a differenza di altre cronologicamente concomitanti o successive leggi fondamentali, v. *infra*) è la stampa, considerata soprattutto però nella sua veste di strumento di "libera manifestazione del pensiero", come testimonia il disposto dell'art.21: e ciò, nonostante i Costituenti fossero consapevoli della incredibile potenza propagandistica e manipolativa già ai tempi del fascismo svolta da mezzi quali la televisione e la radio. Invece, nel tutelare la "segretezza" delle comunicazioni personali, i costituenti fanno riferimento, al di là della corrispondenza, a "qualsiasi forma di comunicazione": così, per la giurisprudenza è stato e resta più facile adattare la norma ai mutamenti del contesto tecnologico di riferimento, laddove i mezzi per esprimere *in privato* il proprio pensiero diventano sempre maggiori, e si moltiplicano le possibilità di interferenza nella sfera privata (dalle classiche intercettazioni telefoniche ai *Trojans*, fino ai programmi in grado di neutralizzare i sistemi crittografati).

quale potenziale fondamento della tutela costituzionale della riservatezza (e, con maggiori incertezze, della protezione dei dati personali) nel ordinamento italiano. Partendo da una concezione della riservatezza quale “aspetto dei diritti fondamentali”, e dunque quale valore alla luce del quale rimodulare l’estensione del contenuto sostanziale dei diritti di libertà già enunciati dalla Costituzione sulla scorta di un’interpretazione sistematica dei principi di uguaglianza formale e sostanziale consacrati nell’articolo 3²²⁰, il fondamento del relativo diritto è stato individuato nell’art. 13 sulla libertà personale; nell’art.14 sulla inviolabilità del domicilio; nell’art. 15 relativo alla libertà e alla segretezza della corrispondenza; e nell’art. 21, in guisa di profilo negativo della libertà di manifestazione del pensiero (quale pretesa dunque di *non* conoscere e insieme di *non far conoscere* informazioni riguardanti la propria persona)²²¹. Altrettanto invalso in dottrina è tuttavia l’orientamento che individuerebbe il fondamento in questione nell’art. 2 della Costituzione, inteso nella ormai famosa accezione di *norma a fattispecie aperta*, che (secondo un approccio, potremmo dire, di tipo evolutivo) consentirebbe l’ingresso nell’alveo delle situazioni costituzionalmente protette di nuovi interessi inerenti alla persona umana progressivamente emergenti nel corpo sociale, e attraverso la medesima “clausola”, dunque, spontaneamente presidiati da un diritto inviolabile, o della personalità, o di “nuova generazione” che dir si voglia, costituzionalmente fondato ²²². Indipendentemente dall’orientamento

²²⁰ Quest’orientamento, tra i più diffusi nella letteratura costituzionale, trova tra i suoi più autorevoli esponenti F. MODUGNO, *I «nuovi diritti» nella Giurisprudenza Costituzionale*, Giappichelli, Torino, 1995, p. 20 ss, che ivi ne offre un ritratto cristallino ed un’argomentata giustificazione. Per citarne solo un passaggio, opportuno sarebbe reinterpretare i diritti fondamentali «in modo tale da assorbire in essi contenuti di libertà interiore o di consentire esplicazioni di irriducibili esigenze di coscienza», come conseguenza del principio fondamentale di cui all’art. 3, in base al quale «la persona deve essere messa in grado di godere pienamente degli stessi diritti fondamentali».

²²¹ Per una panoramica di tali riferimenti, cfr. L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli 2016, p. 46 ss.

²²² Su tale altrettanto diffuso indirizzo ermeneutico, cfr. sempre *ibidem*; P. GROSSI, «Inviolabilità dei diritti», in *Enc. Dir.*, XXII, Milano, 1972; A. BARBERA, «Art. 2», in

seguito, resta il fatto che nel nostro ordinamento la Costituzione, attraverso l'esegesi compiuta con particolare vigore specialmente dalla dottrina, e dunque nella sua declinazione *concreta*, offre un sistema di garanzie "supreme" per la *privacy* individuale. Quest'ultima affermazione, tuttavia, appare più solida se si offre fondamento costituzionale alla "privatezza" sotto il suo profilo esclusivamente negativo, ossia come libertà di *escludere*, e quindi pretesa di "non intrusione" nella propria sfera privata. Più difficile appare offrire copertura ed anzi vero e proprio *ancoraggio* costituzionale alla sua dimensione positiva, a maggior ragione se intesa come *autonomo* diritto che si sostanzia nella pretesa di svolgere un controllo sulla circolazione delle informazioni che riguardando la propria persona, e dunque come diritto alla protezione dei dati personali, capace di incidere strutturalmente sulla portata di altre libertà fondamentali tutelate in Costituzione, quali la libertà di manifestazione del pensiero e il diritto di iniziativa economica privata (art. 41)²²³. Per questo motivo, sul finire degli anni Ottanta, proprio in concomitanza con il primo boom dei *computers* nel settore privato e

Commentario della Costituzione, G. Branca (a cura di), Bologna 1975; G. GIACOBBE, «Riservatezza (diritto alla)», in *Enc. dir.*, vol. XL, Milano, Giuffrè, 1989. In senso critico, cfr. invece M. LUCIANI, *Il diritto al rispetto della vita privata*, cit., p. 7 ss., che propone piuttosto di interpretare l'art. 2 come una "indicazione di metodo, che affida all'interprete il compito di interpretare i diritti costituzionali *"magis ut valeant"*, così da ampliarne l'ambito di tutela «adeguando la lettura delle norme costituzionali alle esigenze dello sviluppo dei rapporti sociali»; allo stesso modo F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, cit.

²²³ Sui dubbi e sul dibattito circa il fondamento costituzionale implicito, o comunque interpretativo, del diritto alla protezione dei dati personali, cfr. DE SIERVO, «La privacy», in *I diritti fondamentali e le Corti in Europa*, (a cura di) Panunzio, Napoli, 2005, 356-57; PACE-MANETTI, sub «art. 21. La libertà di manifestazione del proprio pensiero», in *Comm. della Cost.*, (a cura di) Branca, Bologna-Roma, 2006, 149 ss. e 159 ss.. Tuttavia, come vedremo meglio in seguito, sul pacifico riconoscimento del carattere fondamentale e del rango costituzionale del diritto alla protezione dei dati personali, a maggior ragione successivamente alla sua cristallizzazione nella Carta dei diritti fondamentali dell'Unione Europea e del valore giuridico pari a quello dei Trattati Istitutivi da essa assunto con il Trattato di Lisbona, cfr. da subito G. FINOCCHIARO, «Identità personale (diritto alla)», in *Digesto/civ.*, Agg., Torino, 2010; AIELLO, «La protezione dei dati personali dopo il Trattato di Lisbona», in *Oss. del dir. civ. e comm.*, n. 2/2015, p. 431 ss.; S. Calzolaio, «Protezione dati personali», in *Dig. disc. pubbl.*, Agg., (a cura di) R. Sacco, Milano, 2017, p. 613 ss.

nella pubblica amministrazione, nonché il rafforzarsi del dibattito sui rischi per la sicurezza delle informazioni personali e sulla *mass surveillance*, sono state avanzate proposte per l'inserimento in Costituzione di apposite disposizioni dedicate alla circolazione e alla protezione dei dati di carattere personale. Emblematica a riguardo è la proposta di introduzione degli articoli 21-bis e 21-ter presentata e discussa in Parlamento il 29 gennaio del 1985, diretta in particolare alla previsione di una riserva di legge in relazione alla disciplina del diritto di *raccogliere* ed elaborare informazioni personali, o piuttosto di un divieto di *utilizzare* le stesse in modo da ledere le libertà fondamentali costituzionalmente sancite²²⁴. La proposta suddetta, come le altre discusse in letteratura o in sede parlamentare, è naufragata senza sostanziale coinvolgimento dell'opinione pubblica. Ma ormai, come vedremo meglio tra poco, a maggior ragione successivamente alla cristallizzazione del diritto fondamentale alla protezione dei dati personali nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea, nonché all'esplicita attribuzione della competenza in materia all'UE in conseguenza delle modifiche introdotte nei Trattati Istitutivi dal Trattato di Lisbona, il rango costituzionale del diritto in questione deve ritenersi altrettanto pacificamente riconosciuto anche nel nostro ordinamento ²²⁵.

²²⁴ V. la relazione presentata ai presidenti della Camere dai senatori Lipari e Buttarelli il 29 gennaio 1985, deputata a discutere, come ricordato, il testo di due potenziali nuovi articoli da introdurre nella Costituzione in materia di protezione dati, il 21 bis e il 21 ter; la discussione è stata verbalizzata in forma sintetica nel Bollettino delle Giunte e delle Commissioni Parlamentari dei lavori che corrono dal 28 gennaio al 5 febbraio, ed è consultabile qui: http://legislature.camera.it/_dati/leg09/lavori/Bollet/19850128_00.pdf. Cfr. sul punto G. BUTTARELLI, *Banche Dati e Tutela della riservatezza*, cit., p. 113 ss.

²²⁵ Sul punto vedi più ampiamente *infra*, ma intanto cfr. già G. FINOCCHIARO, «Identità personale (diritto alla)», in *Digesto/civ.*, Agg., Torino, 2010; AIELLO, «La protezione dei dati personali dopo il Trattato di Lisbona», cit.; S. CALZOLAIO, «Protezione dati personali», in *Dig. disc. pubbl.*, Agg., (a cura di) R. Sacco, Milano, 2017, p. 613 ss.

Al contrario, nelle Carte Costituzionali degli Stati europei che se ne siano più recentemente dotati sono contenuti espliciti riferimenti tanto alla vita privata quanto alla riservatezza in senso proprio, intesa anche nella sua accezione di *information privacy*, o di diritto alla protezione dei dati personali; e ciò, come meglio vedremo, in conseguenza di un processo di adeguamento normativo al mutato contesto tecnologico che già gli stessi o altri Stati del Vecchio Continente andavano intraprendendo in quegli anni²²⁶.

La Costituzione Spagnola, ad esempio, al suo art. 18, oltre a proclamare solennemente il diritto all'onore, all'intimità della propria sfera personale e familiare e alla propria immagine, e in aggiunta all'inviolabilità del domicilio e alla segretezza delle *comunicazioni*, statuisce espressamente che la legge dovrà porre limiti all'uso dell'informatica, al fine esplicito di salvaguardare «l'onore e l'intimità personale e familiare dei cittadini e il pieno esercizio dei loro diritti». Il disposto appena descritto rappresenta il primo fenomeno di costituzionalizzazione espressa, in ambito europeo, del diritto alla protezione della vita privata, e la precipua definizione del suo contenuto, stante l'espressa collocazione nella gerarchia delle situazioni costituzionalmente protette, si deve principalmente al *Tribunal Constitucional*, che del c.d. *derecho a la intimidad* ha determinato l'ampiezza e la portata attraverso una *ponderation de bienes* quando venisse a confliggere con altri diritti costituzionalmente sanciti²²⁷.

²²⁶ Una puntuale rassegna di normative ordinarie e di testi costituzionali che si occupino (anche) di *privacy* come non intrusione e/o come controllo è contenuta in G. RESTA, «Il diritto alla protezione dei dati personali», in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, p. 35 ss.

²²⁷ Per una panoramica sulle pronunce in materia di *intimidad* del *Tribunal Constitucional* spagnolo, cfr. G. FAMIGLIETTI, «Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed *intimidad* sulla scorta della giurisprudenza della Corte costituzionale e del *Tribunal Constitucional*», in *Biotecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, A D'Aloia (a cura di), Giappichelli Editore, Torino 2005, p. 299 ss.

La Costituzione Portoghese del 1976, successivamente alla legge di revisione costituzionale del 1982, offre un catalogo ancora più ricco ed esplicito di situazioni giuridiche soggettive, in cui appaia scomporsi il polimorfico diritto alla vita privata, garantite al vertice della gerarchia delle fonti. L'art. 26 garantisce infatti a ciascuno i diritti «all'identità personale, allo sviluppo della personalità, alla capacità civile, alla cittadinanza, al buon nome e alla reputazione, all'immagine, alla parola, *alla riservatezza dell'intimità della vita privata e familiare*»: posizioni molte delle quali appaiono evidentemente riconducibili alla categoria dei diritti della personalità, la cui tutela costituzionale nel nostro ordinamento, lo si ricorda, viene comunemente ricondotta all'art. 2 della Costituzione²²⁸. L'art. 35 poi appare espressamente dedicato alla dimensione positiva della *privacy*, appunto quale libertà di gestire il proprio fluido *sé informativo*, regolando dettagliatamente l'utilizzo dei dati informatici: esso garantisce in capo a tutti i cittadini «il diritto di *accesso* ai dati informatici che li riguardano, potendone esigere la *rettifica* e l'*aggiornamento*, e il diritto di conoscere la *finalità* cui sono destinati, nei termini della legge»; e con notevole lungimiranza rispetto agli altri legislatori, costituzionali e non, europei, ed importando il modello statunitense delle *authorities*, prevede l'istituzione di autorità amministrative indipendenti per la protezione dei dati personali, seppur circoscrivendo l'obbligo alla fattispecie dei trattamenti automatizzati, ma cogliendo la dimensione collettiva dell'esigenza di protezione dei dati personali, come bene giuridico ascritto tra le «condizioni necessarie per rendere possibili le relazioni con gli altri» e dunque presupposto indefettibile per la libera costruzione

²²⁸ V. *supra* e cfr. comunque sul punto ancora una volta, sull'art. 2 come norma a fattispecie aperta, A. BARBERA, *Articolo 2*, cit.; sull'art. 2 come clausola -solo- interpretativa di tipo estensivo-evolutivo, cit.; M. LUCIANI, «Nuovi diritti fondamentali e nuovi rapporti fra cittadino e pubblica amministrazione», in *Riv. crit. dir. priv.*, 1985; F. MODUGNO, *I nuovi diritti nella giurisprudenza costituzionale*, cit.

della propria *plurale* identità²²⁹. Inoltre, l'art. 35 vieta il trattamento informatico dei c.d. dati sensibili («*relativi a convinzioni filosofiche o politiche, affiliazione a partiti o sindacati, fede religiosa, vita privata e origine etnica*»), prevedendo costituzionalmente come uniche, tassative deroghe il consenso dell'interessato, l'autorizzazione legislativa o l'anonimizzazione degli stessi.

Concludiamo sul punto ricordando che altre Costituzioni recenti contengono riferimenti alla tutela della riservatezza e alla protezione dei dati personali, come la Costituzione albanese del 1998 (art. 35), quella finlandese del 1999 (art. 10, rubricato «Diritto alla riservatezza») e quella svizzera dello stesso anno (art. 13, rubricato «Protezione della sfera privata»).

2.2.1. *Individualrechte, protection de la vie privée*, diritto al riserbo: le origini della “vita privata” in Europa

A questo punto, spostiamo il nostro “carrello” sul piano del diritto ordinario. e dell'agone dottrinale e giurisprudenziale, degli Stati membri dell'Unione europea. A breve, focalizzeremo l'obiettivo soprattutto sull'ordinamento italiano, specialmente a partire dal momento in cui la riflessione sui concetti limitrofi di vita privata e di riservatezza si fanno più maturi.

Prima, però, appare opportuno tracciare un'importante, sebbene certamente non esaustiva, premessa relativa al contesto teorico e culturale in cui si iscrive, a partire dai primi anni del ventesimo secolo, e per motivi analoghi a quelli per

²²⁹ La citazione è di G. BUSIA, «Riservatezza (diritto alla)», in *Dig. disc. pubbl.*, Torino, UTET, 2000, ma il rinvio doveroso è sempre a S. Rodotà, *Il diritto di avere diritti*, cit., p. 312 e seguenti. Sulla dimensione collettiva della privacy, presidiata attraverso l'attribuzione di potestà normative e poteri amministrativi sanzionatori (ruolo misto amministrativo/giurisdizionale) ad Autorità amministrative indipendenti, v. *infra*.

cui si amplifica negli Stati Uniti (su tutti, l'exploit delle moderne ICTs), il discorso filosofico e giuridico sulle categorie *privacy* ²³⁰.

Abbiamo appurato che la vera *fondazione giuridica* dell'istituto si rinviene nell'importante lavoro di Warren e Brandeis del 1890, in quanto modello giuridico poi nel corso del Novecento "importato" nel contesto culturale europeo. Abbiamo però anche detto, parlando a suo tempo delle radici storiche dell'aspirazione alla tutela dell'"illesa intimità", che parte della dottrina le individua nel dibattito, originato in area germanica nel corso del diciannovesimo secolo, circa l'esistenza di una categoria di diritti nota come *Persönlichkeitsrechte* o anche come *Individualrechte* ²³¹. Dobbiamo ora approfondire il punto, poiché tale discorso e le sue articolazioni sono determinanti per lo sviluppo e gli esiti del medesimo nella dottrina italiana, con inevitabili riflessi sulle concezioni di vita privata e di riservatezza che vi fioriscono e che nutrono poi il dibattito più moderno.

Intesi, secondo la tradizionale elaborazione giusnaturalistica post-kantiana, come «signoria sopra una parte della propria sfera di personalità», gli *Individualrechte*, anche dopo l'avvento della Scuola Storica del Diritto (e le mordaci critiche rivolte a tale elaborazione teorica da F. V. Savigny), individuano una categoria ampia ed eterogena di posizioni giuridiche soggettive discendenti dalla nozione di «autonomia morale della persona», soprattutto inerenti alla libertà

²³⁰ Nel compiere l'affresco che seguirà, il debito principale esiste nei confronti del caleidoscopico panorama disegnato da G. RESTA, «I diritti della personalità», in *La Persona Fisica* (a cura di G. Alpa e G. Resta), e dei ricchi spunti bibliografici dal lavoro in questione offerti; si cercherà quindi di riportare puntualmente i diversi riferimenti bibliografici consultati su "suggerimento" dello scritto, sebbene per più puntuali indicazioni si invita caldamente alla consultazione di quest'ultimo.

²³¹ V. *retro*. Cfr. ancora una volta G. MARINI, «Diritto alla privacy», cit., p. 199 ss.; Ferrara, Santamaria, *Il diritto alla illesa intimità privata*, cit., p. 171 ss.; G. RESTA, «I diritti della personalità», cit.

corporea ed intellettuale²³². Tuttavia, nell'epoca della codificazione promossa dai pandettisti, l'interesse per la categoria, stante la sua indeterminatezza, resta confinata alle dispute dottrinali sulla loro struttura dogmatica: i lavori preparatori del *Bürgergerliches Gesetzbuch* (ossia del Codice Civile tedesco, abbreviato BGB) del 1896 rivelano come il discorso sulla tutela della persona umana fosse limitato all'istituto della capacità giuridica²³³. E così il legislatore stenta a riconoscere fondamento positivo a tali posizioni: il BGB offre espressa tutela esclusivamente al diritto al nome (par. 12 del Titolo I, Libro I); mentre il par. 823 comma primo del Titolo II, Libro II, nel configurare l'istituto della responsabilità aquiliana ed enumerare, secondo un principio di tassatività, i beni giuridici la cui lesione colposa e antiggiuridica dà titolo al risarcimento del danno scaturitone, fa riferimento solo al corpo, alla vita, alla salute ed alla libertà, sebbene poi l'elencazione si chiuda dalla formula (come vedremo, importante per l'elaborazione teorica successiva) «ogni altro diritto». Nessuna considerazione è accordata, positivamente, all'onore; meno che mai alla vita privata, o alla riservatezza.

Tuttavia, gradualmente, sul dommatico pensiero romanista comincia a prevalere la più ricca riflessione teorica dei “germanisti”, e in particolare di tre autorevoli autori come Karl von Gareis, Otto von Gierke e Josef Kohler, che impostano la moderna sistemazione scientifica (quanto meno in contesto

²³² Cfr. G. RESTA, «I diritti della personalità», cit., p. 397 ss. L'autore puntualizza utilmente come nella Germania del diciannovesimo secolo il discorso sui diritti della personalità fosse rimasto confinato principalmente alla dottrina, individuandone le ragioni nella tardiva industrializzazione (che si riflette nel fisiologico ritardo nello sviluppo di attività rilevanti per la “sfera privata”, come la commercializzazione del ritratto) e nella frammentazione politica, con la conseguente assenza di un apparato giurisdizionale organizzato su base verticistica e dunque soggetto al controllo di un'unica Corte Suprema. Per approfondimenti sul punto, cfr. ex multis J. WHITMAN, «The Two Western Culture of Privacy: Dignity Versus Liberty», in *The Yale Law Journal*, Vol. 113, No. 6, 2004, pp. 1151-1221.

²³³ Cfr. A. SOMMA, «I diritti della personalità e il diritto generale della personalità nell'ordinamento della Repubblica Federale Tedesca», in *Riv. Trim. Dir. Proc. Civ.*, Anno L, Fasc. 3, 1996, p. 808

continentale) della categoria dei diritti della personalità²³⁴. In particolare, il primo, pur incentrando la riflessione principalmente sui segni distintivi e sui prodotti della personalità creativa, comincia a delineare un quadro unitario dei *Persönlichkeitsrechte*, assumendo come paradigma aggregante l'idea della protezione dell'individualità della persona²³⁵. Si fa strada, dunque, quella teoria monistica che il discorso giuridico tedesco sulla tutela della persona umana domina incontrastata dagli anni Cinquanta: teoria che afferma l'esistenza di un «diritto generale della personalità» (*allgemeines Persoenlichkeitsrecht*), di cui tutte le specifiche posizioni a presidio di attributi fondamentali della persona umana non sarebbero che “aspetti”, declinazioni²³⁶. In questo contesto, non sorprende che Kohler, in alcune sue riflessioni, richiami un «diritto alla segretezza», a protezione dell'individuo dalla pubblicazione non desiderata di rapporti epistolari, ed anche dalla rivelazione di fatti della vita privata²³⁷.

La nuova sistemazione teorica illustrata concorre anzitutto a spronare la giurisprudenza di merito ad accordare tutela risarcitoria anche alla violazione di singoli diritti della personalità non esplicitamente considerati dal BGB²³⁸. Ma soprattutto, con l'avvento molti anni dopo della *Grundgesetz* (abbreviata GG), ossia della Legge Fondamentale della Repubblica federale tedesca del 1949, determina la definitiva consacrazione nell'ordinamento tedesco della teoria monistica: facendo leva sul combinato disposto tra l'art. 1, comma 1 (che afferma stentoreamente: «La dignità dell'uomo è intangibile. È dovere di ogni potere statale proteggerla e rispettarla») e l'art. 2, comma 1 («ognuno ha diritto al libero

²³⁴ G. RESTA, «I diritti della personalità», cit., p. 403 ss.

²³⁵ Cfr. ad esempio, K. GAREIS, «Die privatrechtssphären in modernen Kulturstaate insbesondere in Deutschen Reiche», in *Zeitschrift für Gesetzgebung und Praxis auf dem Gebiete des Deutschen öffentlichen Rechtes*, 1877, p. 137 ss.

²³⁶ Cfr. ad es. K. LAREN, *Allgemeiner Teil des Bürgerlichen Rechts*, C. H. Beck, 8^o edizione, p. 128 ss.

²³⁷ Cfr. KOHLER, «Das Autorrecht», in *Iherings Jahrbucher*, XVIII, nuova serie VI, stampata a parte nel 1880

²³⁸ A. SOMMA, «I diritti della personalità», cit. p. 809 ss.

sviluppo della propria personalità, in quanto non violi i diritti degli altri e non trasgredisca l'ordinamento costituzionale o la legge morale») della GG, si riconosce così l'esistenza del suddetto *diritto generale della personalità*, che raggrupperebbe le singole posizioni (i «diversi aspetti») in cui si articola in un “lato attivo”, come facoltà di agire nel senso più corrispondente ai propri bisogni, e in un “lato passivo”, come diritto a *ritrarsi nella propria sfera privata*, e dunque ad *escludere* le interferenze di terzi: una sorta, questa, di esplicita consacrazione del diritto al rispetto della vita privata. La posizione descritta rileverebbe, allora, per l'ordinamento privatistico proprio in forza del par. 823: chiudendo questo l'elencazione dei beni oggetto di tutela con l'espressione «ogni altro diritto», consentirebbe, alla luce di una rilettura costituzionalmente orientata, di incardinare nell'ordinamento privatistico il diritto generale della personalità (o meglio, i vari aspetti non espressamente codificati in cui si scompone), rendendo così possibile una sorta di *Drittwirkung* indiretta della Legge Fondamentale medesima.

La lettura in questione, conviene anticiparlo, fu definitivamente accolta dal *Bundesgerichtshof* (ossia la Corte di Giustizia federale tedesca, organo di ultima istanza e di sola legittimità) negli anni Cinquanta, in una sentenza del 1954, che qui interessa ulteriormente perché riguarda un caso di divulgazione a mezzo stampa di un testo con tagli ed omissioni incidenti sul significato dello scritto: ebbene, la fattispecie fu sanzionata come ipotesi di responsabilità civile ai sensi del par. 823, sul presupposto che la pubblicazione non autorizzata rappresentasse un'illecita intromissione nella sfera privata; e, dunque, un'alterazione dei tratti caratterizzanti la personalità dell'interessato²³⁹. I rilievi della motivazione appena esposti sono, dunque, fondamentali per individuare il nesso, già in epoca post-bellica avvertito, tra integrità della sfera privata e libertà morale, la prima come

²³⁹ Cfr. BGH, 26.11.1954, in *BGHZ*, vol. 13 (1954), p. 34 ss.

presupposto per la libera costruzione della propria personalità, e, ancor prima, connotato costitutivo della dignità umana. Allo stesso tempo, essa è importante perché ci avverte già del peso assunto dal tema della riservatezza, per motivi noti, sul finire della prima metà dello scorso secolo. Ci torneremo tra poco, con riferimento all'ordinamento italiano.

Concludiamo sul punto evidenziando che a tale sentenza seguirono numerose pronunce della giurisprudenza di legittimità che consolidarono l'orientamento²⁴⁰; e altrettanto pieni furono il recepimento e la consolidazione dello stesso da parte del *Bundesverfassungsgericht*, ossia la Corte Costituzionale Federale tedesca, che in numerose pronunce ha affermato come il diritto generale della personalità rappresenti una «salda e incontestabile acquisizione dell'ordinamento giuridico tedesco»²⁴¹. In ogni caso, il contenuto del diritto generale della personalità è stato dalla giurisprudenza di legittimità e costituzionale definitivamente specificato quale diritto, riconosciuto in ogni forma di rapporto, ad ottenere riguardo per la propria dignità e a *costruire liberamente la propria personalità*.

Il quadro storico fin qui tracciato rileva nella misura in cui il discorso tedesco iniziato nel diciannovesimo secolo travalica ben presto i confini nazionali.

²⁴⁰ Una dettagliata rassegna è contenuta in A. SOMMA, «I diritti della personalità», cit. p. 811 ss. ad es. v. BGH, 26 novembre 1954, in *BGHZ*, vol. 15, (1955), p. 249 ss.; BGH, 20 maggio 1958, ivi, vol. 27, (1958) p. 284, particolarmente importante perché ha a che fare con la registrazione occulta su nastro delle dichiarazioni di una persona, e dunque con un caso simile a quelli già visti nella giurisprudenza americana, seppur soprattutto nel rapporto pubblico-privato: caso che ancora una volta testimonia di come le recent inventions dell'uomo configurino rischi sempre maggiori per la sfera priva dell'individuo, cui il diritto, attraverso i diversi formanti in cui si articola, è chiamato a rispondere in funzione del bilanciamento degli interessi in gioco.

²⁴¹ V. BVerfG, 14 gennaio 1973, in *BVerfGE*, vol. 34, 1973, p. 269 ss.; BVerfG, 31 gennaio 1973, ivi, vol. 34, 1973, p. 238 ss.

Esso trova terreno fertile in Francia, in cui la codificazione napoleonica aveva dimostrato, nel settore dei rapporti tra privati, una sostanziale indifferenza per la dimensione della “personalità umana”: nel *Code Civil* del 1804 mancano infatti disposizioni dirette a tutelare la persona nei suoi attributi materiali e incorporei ²⁴². E questo, è stato rilevato, soprattutto perché, al di là dell’arretratezza del contesto tecnologico, nella concezione prettamente “volontaristica” accolta dal codice tutte le aspirazioni di tutela della personalità promosse dalla Dichiarazione universale dei diritti dell’uomo e del cittadino del 1789 si ritenevano soddisfatte, sotto il profilo privatistico, nella forma della tutela della proprietà (art. 544) e attraverso il riconoscimento dell’autonomia contrattuale e la predisposizione di garanzie in funzione di quest’ultima ²⁴³. Tuttavia, già dalla metà dell’Ottocento la giurisprudenza aveva cominciato ad essere sempre più investita di controversie concernenti la violazione degli attributi costitutivi della persona, quali l’uso indebito del nome, la violazione dell’onore e la pubblicazione non autorizzata del ritratto ²⁴⁴. Tali casi, e la corrispondente

²⁴² Cfr. sul punto G. RESTA, «I diritti della personalità», cit., p. 384, che puntualizza tra l’altro come sotto il profilo della tutela della persona umana nell’ordinamento francese ottocentesco esistesse uno iato profondo tra diritto pubblico e diritto privato: «tanto il primo era ricco di declamazioni solenni [basti pensare alla Dichiarazione universale dei diritti dell’uomo e del cittadino del 1789] circa la primazia dell’uomo e dei suoi diritti innati di fronte allo Stato, quanto il secondo era povero di riferimenti espressi all’individuo, nella concretezza dei suoi *bisogni di natura non strettamente patrimoniale* [cors. nostro]»; per un riscontro nel panorama della dottrina francese, cfr. ex multis G. SAVATIER, «La promotion juridique contemporaine de la personne», in Id., *Les métamorphoses économiques et sociales du droit privé d’aujourd’hui*, in *Revue Internationale de Droit Comparé*, III, 1959, p. 639-642.

²⁴³ Ivi, p. 386; l’autore evidenzia come non possa essere ignorata la disposizione dell’art. 1166 del *Code Civil* relativa alla categoria dei c.d. *droits attachés à la personne*, ma ricorda come quest’ultima avesse assunto autonomia effettività solo sul finire del secolo e al limitato scopo di apprestare tutela alla dimensione morale del soggettivo assoluto *droit d’auteur*. Per una panoramica generale sul formante legale in materia di tutela della persona umana nell’ordinamento francese del periodo storico in esame, cfr. POUSSON PETIT, «Le personne humaine sur la scène d’un théâtre d’ombres», in *Liber Amicorum Marie-Thérèse Meulders-Klein*, Bruxelles, 1998, passim.

²⁴⁴ Ivi, p. 392; LINDON, *La création prétorienne en matière de droits de la personnalité et son incidence sur la notion de famille*, Parigi, 1974, p. 9 ss.

esigenza di tutela, scaturivano (a questo punto della trattazione, non ci sorprenderà) dal processo di liberalizzazione della stampa e dallo sviluppo sempre più marcato dei mezzi di informazione: tra questi ultimi, i fenomeni più prorompenti erano stati l'invenzione del dagherrotipo e, ancor più, l'invenzione della fotografia, con la sostanziale liberalizzazione dell'accesso al ritratto²⁴⁵. Appaiono evidenti le analogie con le trasformazioni che, seppur con modalità e tempi "di reazione" diversi, investirono il contesto socioculturale americano nello stesso periodo storico.

Sebbene, chiamati a pronunciarsi, i tribunali avessero compiuto un'opera di "integrazione" esegetica del testo normativo, cominciando a costruire diritti soggettivi assoluti a presidio dei beni medesimi²⁴⁶, la dottrina era rimasta sostanzialmente silenziosa, e ciò perché essa aveva, di fatto, per lo più ricondotto anche gli attributi della personalità, al pari del *droit d'auteur*, al paradigma giuridicamente dominante nell'Ottocento francese: la proprietà privata²⁴⁷. Concettualizzati in tali termini, la "lesione" di tali attributi rilevava solo nei suoi patrimoniali riflessi pregiudizievoli: alla dimensione spirituale dell'uomo in quanto tale, e alle corrispondenti sofferenze, non era offerta considerazione giuridica.

²⁴⁵ Sullo sviluppo progressivo della tecnologia nella rappresentazione della realtà, per un'analisi di più ampio respiro che intreccia storia dell'arte, estetica e sociologia, cfr. il fondamentale lavoro di W. BENJAMIN, *L'opera d'arte nell'epoca della sua riproducibilità tecnica. Arte e società di massa*, 1^a ed. or. 1936, tr. it, Torino 2000, in part. per l'argomento che qui stiamo trattando p. 57 ss.

²⁴⁶ Per una panoramica cfr. sempre G. RESTA, «I diritti della personalità», cit. p. 392 ss.

²⁴⁷ IVI, p. 396. Cfr. anche A. GAMBARO, voce «Proprietà in diritto comparato», in *Digesto/civ.*, XV, Torino, 1997, pp. 502 ss., 516. Gli autori sottolineano come la circostanza in questione dipenda anche dall'accezione elastica e deformalizzata sostanzialmente accolta a livello sapienziale, e in primis nella tradizione germanistica, che avrebbe consentito alla dottrina di ricondurre anche i nuovi interessi insistenti su beni immateriali suscitati dalla rivoluzione industriale alla tradizionale categoria dominicale, enucleando le molteplici figure delle *propriétés incorporelles*.

E tuttavia proprio sul finire del diciannovesimo secolo le categorie personalistiche elaborate in area tedesca, e in particolare dai suddetti germanisti, cominciarono a circolare in area francese: se tradizionalmente si attribuisce ad un trattato di Boistel il merito di aver affrontato per primo il problema²⁴⁸, la categoria dei diritti della personalità riceve pieno riconoscimento nella dottrina francese grazie all'opera di Perreau²⁴⁹. Grazie al contributo di tale autorevole studioso, che offre una puntuale sistematizzazione dei prodotti del percorso dottrinale tedesco e dell'esperienza delle corti francesi, la stessa giurisprudenza giunge a ritenere meritevole di tutela l'interesse alla *protection de la vie privée*: esso risulta, in tale prospettiva, presidiato da un diritto (di derivazione, dunque, esegetica) soggettivo assoluto che ancora rileva in una prospettiva prevalentemente rimediale, ossia che entrerebbe nell'ordinamento privatistico per effetto della norma di chiusura rappresentata dall'art. 1382 del Code Civil, che configura una fattispecie generale di responsabilità civile, nell'ambito del quale pertanto risulterebbe tutelata, in via risarcitoria, anche la lesione di tale diritto.

Concentriamo finalmente l'attenzione sull'ordinamento italiano. Lo stesso fenomeno che abbiamo denunciato in relazione all'esperienza francese, rappresentato dalla circolazione del modello giuridico enucleato nella tradizione "germanista" tedesca, interessa anche il nostro ordinamento²⁵⁰. Per gran parte del diciannovesimo secolo, la problematica sulla tutela dell'individuo, nella sua dimensione corporea ed intellettuale, era infatti rimasta estranea alle riflessioni dei civilisti, influenzati per lo più dal paradigma volontaristico e proprietario

²⁴⁸ Ci si riferisce qui a A. BOISTEL, *Cours de philosophie du droit*, Parigi, 1899.

²⁴⁹ Cfr. l'importante opera di J. A. PERREAU, «Les droits de la personnalité», in *Rev. Trim. dr. Civ.*, Parigi, 1909.

²⁵⁰ Sull'influenza della pandettistica e sulla circolazione, o il vero e proprio trapianto, dei modelli giuridici nel suo ambito enucleati, cfr. P. GROSSI, *Scienza giuridica italiana. Un profilo storico*, Milano 2002, p. 15 ss.; G. ALPA, *La cultura delle regole. Storia del diritto civile italiano*, Roma-Bari, 150- 199.

francese, diffuso nella penisola attraverso l'instaurazione del Regno d'Italia napoleonico e la sua successiva disgregazione negli Stati successori²⁵¹.

Il percorso seguito dalla dottrina italiana è dunque simile a quello francese; principia a distinguersi solo a partire dall'influenza esercitata, inizialmente, dall'opera della Scuola storica e dei pandettisti; e, successivamente, per quanto attiene alla tematica degli attributi della personalità, dalla riflessione dei germanisti.

Bisogna attendere la fine del diciannovesimo secolo affinché il dibattito in materia assuma connotazioni proprie, e particolare vigore. Se il merito di aver determinato la circolazione degli scritti tedeschi nella dottrina italiana si deve soprattutto alle opere di due tra i più importanti commentatori italiani della pandettistica, ossia Carlo Fadda e Pier Emilio Bensa, il primo sviluppo di un autonomo discorso in materia di diritti della personalità è da ascrivere all'opera di un intellettuale di ampie vedute: Adolfo Ravà²⁵². Sin dal suo primo lavoro monografico sul tema, risalente al 1901²⁵³, l'illustre giurista si pone in aperta polemica con quella parte della civilistica che, specialmente nella voce di Campogrande, intendeva configurare il *jus in se ipsum* sullo schema concettuale proprio del diritto soggettivo assoluto, e segnatamente della categoria degli *jura*

²⁵¹ P. GROSSI, *La cultura del civilista italiano. Un profilo storico*, Milano, 2002, 15 ss.. Cfr. poi sempre G. RESTA, «I diritti della personalità», cit., p. 424 ss.; nelle pagine che seguono, l'autore, in particolare, sottolinea come i principali fattori della rinnovata attenzione per la persona umana nella riflessione della dottrina italiana giuspositivistica di fine diciannovesimo secolo siano stati da una parte la circolazione stessa della dottrina tedesca, romanistica e germanista; e, dall'altra, l'esperienza teorico pratica in tema di contratto di lavoro subordinato. Allo stesso tempo, circolazione del modello germanista degli *Individualrechte* avrebbe seguito, in Italia, due direttrici: da una parte, la traduzione e il commento dell'opera dei Pandettisti, in cui il tema dei diritti della personalità si inseriva nella più ampia discussione sul diritto soggettivo; dall'altra, il confronto critico con le teorie personalistiche sul terreno del diritto commerciale e industriale.

²⁵² Cfr. FADDA, BENSA, *Note al Libro Secondo*, in Windscheid, *Diritto delle Pandette*, a cura di Fadda e Bensa, Vol. 1, I, Torino 1902; in particolare, nota e) ed f); per quanto attiene al pensiero di Ravà, cfr. innanzitutto A. RAVÀ. *I diritti sulla propria persona nella scienza e nella filosofia del diritto*, RISG, 1901, vol. XXXI, pp. 289-378, vol. XXXII, pp. 1-27

²⁵³ V. nota precedente.

in re propria, riducendolo ad una fattispecie di proprietà sulla persona²⁵⁴. Ravà al contrario, stimando alquanto la “meritevolezza” di tutela degli attributi della personalità, sia corporei che immateriali, riteneva che il relativo meccanismo di protezione dovesse ricalcare il modello della *libertà*, sottolineando dunque il legame tra diritto e morale, da cui sarebbe discesa l’esistenza di un «diritto *a* che la propria persona sia rispettata», sottratto all’intransigente pretesa regolatrice del diritto²⁵⁵.

Sebbene la teoria di Ravà non trovi immediato seguito nella cultura giuridica italiana, e il modello dei diritti della personalità venga, in quegli anni, essenzialmente a identificarsi con la figura del “diritto *sulla* propria persona” di stampo proprietario propugnato da una parte della pandettistica²⁵⁶, essa concorre ad emancipare le riflessioni sugli attributi della persona dalla sola dimensione patrimoniale, e segnatamente dalla sola prospettiva della sistematizzazione dei diritti sui segni distintivi e dei diritti di privativa, oggetto delle ricerche di autorevoli cultori del diritto commerciale, quali Franchi e Vivante²⁵⁷. Essa, poi, rappresenta il prodromo del più maturo pensiero dell’autore, che in seguito ai nuovi interventi codificatori del legislatore novecentesco viene ad interrogarsi sull’esistenza e sul fondamento normativo di un autonomo diritto alla riservatezza²⁵⁸.

²⁵⁴ Cfr. V. CAMPOGRANDE, «I diritti sulla propria persona», in *Antologia Giuridica*, 1896, 65 ss. (del fascicolo 2) e 155 ss. (del fascicolo 3)

²⁵⁵ Cfr. A RAVÀ, *I diritti sulla propria persona nella scienza e nella filosofia del diritto*, cit., in particolare p. 85 ss. Particolarmente moderno e meritevole di riflessione appare il passaggio in cui afferma «v. pagina 429 Resta

²⁵⁶ Cfr. G. RESTA, «I diritti della personalità», cit., p. 429 ss.; cfr. anche P. GROSSI, *Tradizioni e modelli nella sistemazione post-unitaria della proprietà*, p. 500 ss.

²⁵⁷ Cfr. FRANCHI, *La protezione del nome commerciale, dell’insegna e del marchio nel diritto italiano*, Mantova, 1896, p. 16 ss.; VIVANTE, *Trattato di diritto commerciale*, vol I, Le persone, 2^a edizione, Torino 1902.

²⁵⁸ Cfr. già da ora A. RAVÀ, *Istituzioni di diritto privato*, Cedam, Padova, 1938, in particolare p. 174 ss.; l’opera di Ravà ispirerà, come vedremo, anche le riflessioni di Carnelutti, tra i primi a proporre una soluzione esegetica sistematica in relazione alle norme della Legge sul Diritto d’Autore del 1941 e del Codice Civile del 1942 a protezione degli attributi

Arrivati a questo punto, occorre allora spostare lo sguardo sullo “stato” della legislazione primo novecentesca, e sull’effettiva sussistenza al suo interno di un riferimento alla vita privata, o alla riservatezza, quali autonomi beni giuridici.

2.2.2. Riservatezza, banche dati, autodeterminazione informativa: la costruzione della *privacy* nella legislazione, nella giurisprudenza e nella dottrina degli ordinamenti nazionali del “Vecchio Continente”. In particolare, uno sguardo all’Italia.

Procedendo ad un sintetico excursus, si può affermare che nella legislazione (e nella normazione regolamentare) italiana di inizio secolo il riferimento alla “vita privata” comparisse con finalità molto diverse da quelle che oggi ci sono familiari e che abbiamo già visto consacrate sul piano delle Convenzioni internazionali sui diritti umani, e con vigore ancora maggiore nella giurisprudenza della CEDU. Facendo solo qualche esempio, l’art. 82 del Regolamento per il Corpo degli agenti di custodia degli Istituti di prevenzione e di pena del 1938, qualificava come infrazione disciplinare, punibile con la riduzione dello stipendio, «il frequentare luoghi, persone o compagnie sconvenienti con evidente offesa alla dignità e alla disciplina del Corpo; l’ubriacarsi in modo scandaloso, il tenere in qualsiasi altro modo contegno riprovevole nella vita privata»²⁵⁹. Allo stesso modo, sul diverso piano delle leggi di pubblica sicurezza, possiamo citare l’art. 70 del testo recante la Riforma delle leggi sul lotto pubblico del 1933, che

immateriali della persona, al fine di ancorarvi positivamente l’esistenza nell’ordinamento italiano di un diritto a presidio dell’integrità della sfera privata dell’individuo: cfr. F. CARNELUTTI, «Diritto alla vita privata», in *Riv. Trim. Dir. Pubbl.*, Giuffrè editore, Milano, 1955, pp. 3-18.

²⁵⁹ V. art. 82, comma 1, n. 19, del r.d. 30 dicembre 1937, n. 2584.

prevedeva delle «note di qualifica» per i ricevitori e gli aiuto ricevitori del giuoco del lotto, che dovevano dare conto anche del «loro comportamento nella vita privata»²⁶⁰.

Se ne potrebbero riportare altri, ma già alla luce di tali esempi appare nitido che il legislatore accogliesse una nozione di vita privata ancora imperniata sul modello della società liberale di fine Ottocento, intesa dunque come paradigma di valutazione dei comportamenti dei soggetti chiamati ad esercitare funzioni pubbliche particolarmente delicate, i quali, in ossequio alla rassicurante immagine del «borghese benpensante», erano tenuti a conformare la loro condotta a un modello di morigeratezza e di buon costume²⁶¹.

Sebbene, come abbiamo detto, sia necessario attendere la Costituzione, ma soprattutto le prime Carte internazionali a tutela dei diritti fondamentali della persona, affinché prenda avvio un vero processo di emancipazione, negli ordinamenti europei e segnatamente in quello italiano, della categoria giuridica della vita privata dal concetto di *respectability* borghese, anche nel nostro ordinamento è possibile individuare, negli anni considerati, alcune eccezioni a tale paradigma.

La più rilevante è certamente rappresentata dall'art. 93 della Legge sul Diritto d'Autore del 1941, che al comma 1 stabiliva (e tutt'ora stabilisce) che «Le corrispondenze epistolari, gli epistolari, le memorie familiari e personali e gli altri scritti della medesima natura, allorché abbiano carattere confidenziale o si riferiscano alla intimità della vita privata, non possono essere pubblicati, riprodotti od in qualunque modo portati alla conoscenza del pubblico senza il consenso dell'autore, e, trattandosi di corrispondenze epistolari e di epistolari,

²⁶⁰ V. art. 70, comma 2, del r.d.l. 19 ottobre 1938, n. 1933.

²⁶¹ Cfr. M. LUCIANI, «Il diritto al rispetto della vita privata», cit., p. 3 ss.; S. RODOTÀ, *Riservatezza*, cit., p. 58 ss.; ID., *Il diritto di avere diritti*, cit., p. 312 ss.

anche del destinatario»²⁶². La norma in questione appare importante per una duplice ragione: non solo essa rappresenta uno dei riferimenti del discorso che la dottrina più avanzata, come tra poco si dirà, svolge nel secondo dopoguerra intorno al riconoscimento nell'ordinamento privatistico di un diritto all'integrità della sfera privata; ma, allo stesso tempo, rappresenta il fulcro del primo indirizzo maturato in seno alla giurisprudenza di legittimità, alla fine degli anni Cinquanta, in materia di riservatezza, formalmente non riconosciuta ancora come specifico *presupposto sostanziale* di un autonomo diritto soggettivo, ma implicitamente ricompresa tra gli aspetti di un più generale «diritto alla libera autodeterminazione nello svolgimento della propria personalità», fondato sull'art. 2 della Costituzione²⁶³.

Occorre poi ricordare che al 1942 risale la promulgazione del Codice Civile, nella cui sistematica potevano (e possono tutt'ora) individuarsi talune norme a tutela di alcuni dei diritti della personalità oggetto della secolare e poco fa brevemente ripercorsa elaborazione della dottrina: su tutte, nel Titolo I («Della persona fisica») del Libro I («Delle persone e della famiglia»), si distinguevano gli artt. 6-9, dedicati alla tutela del diritto al nome, e l'art. 10, sul diritto all'immagine (rubricato, nello specifico, «Abuso dell'immagine altrui»)²⁶⁴. E tuttavia, a dimostrazione dello spiccato impianto *individualistico* del Codice, i diritti in questione erano configurati dogmaticamente come diritti soggettivi assoluti e, secondo lo schema tipico del “diritto reale per eccellenza”, ossia la proprietà, i beni giuridici oggetto dei quali erano considerati, e dunque protetti, alla stregua di *res*: essi rilevavano in quanto segni distintivi *appartenenti* al soggetto, e consequenzialmente le forme di tutela apprestate rispondevano ad una

²⁶² V. art. 93, comma 1, l. 22 aprile 1941, n. 633

²⁶³ Ci si riferisce a Cass. civ., 20.04.63, n. 990 - da cui la citazione è tratta-, in cui la Suprema Corte si pronuncia sull'ormai celebre caso Petacci, v. *amplius* a breve.

²⁶⁴ Art. 6-10, r.d. 16 marzo 1942, n. 262.

logica solo *rimediale*, consistendo essenzialmente nell'azione inibitoria e nell'azione di condanna al risarcimento del danno ingiusto *extracontrattuale*, ex art. 2043²⁶⁵. Tuttavia, anche in quest'ultimo caso, ad ulteriore dimostrazione dell'impronta dominicale del codice, la lesione rilevava solo a fronte della produzione di un danno-conseguenza di natura patrimoniale, dal momento che l'art. 2059 limitava testualmente il risarcimento del danno non patrimoniale ai «soli casi previsti dalla legge»: casi per lungo tempo dalla dottrina dominante identificati esclusivamente nei fatti integranti, contestualmente alla fattispecie di responsabilità civile, reato²⁶⁶.

In tale impianto, alcun diritto alla riservatezza o al rispetto della vita privata aveva trovato posto: questi, secondo l'approccio positivistico seguito dalla più gran parte della dottrina del tempo, diffidente se non ostile ai tentativi di allargare in via interpretativa il catalogo degli attributi della persona tutelati civilisticamente, non avrebbero avuto cittadinanza in quanto autonomi diritti soggettivi nel quadro dell'ordinamento privatistico²⁶⁷.

Tuttavia, come già abbiamo accennato, ciò non ha scoraggiato parte della dottrina in quegli anni a proporre una lettura esegetica che consentisse di riconoscere l'esistenza nell'ordinamento interno di diritti della personalità c.d. *atipici*, e in particolare del diritto alla riservatezza. In una delle sue opere più mature, Adolfo Ravà sosteneva allora che «la qualità di persona richiede ed esige

²⁶⁵ Per tale ricostruzione, cfr. G. RESTA, «Identità personale e identità digitale», cit. p. 518 ss., che sottolinea come dall'impianto del Codice Civile italiano, così come del BGB, possa inferirsi un primo, statico, modello di tutela della persona umana negli ordinamenti giuridici europeo; e A. DI MAJO, *La tutela civile dei diritti*, IV ed., Milano, 2003, 138, che inoltre rileva come si tratta «di forme di tutela che, più che avere riguardo al valore della persona, hanno riguardo alle forme di individuazione, fisica e materiale, di essa (come per il diritto al nome, art. 7) o alla sua riproduzione visiva (come per il diritto all'immagine, art. 10)»

²⁶⁶ Per una ricostruzione del dibattito in materia, cfr. UMBERTAZZI, *Il diritto alla privacy: natura e funzioni giuridiche*, cit., p. 49 ss.

²⁶⁷ Tra le voci più conservatrici, cfr. PUGLIESE, «Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche», in *Foro it.*, 1954, I; ONDEI, «Esiste un diritto alla riservatezza», in *Riv. dir. civ.*, 1955, 166.

che alla persona stessa sia riservata una certa sfera relativa ai dati più gelosi e più intimi di essa e della sua attività»²⁶⁸. Da ciò ne desumeva che, anche in assenza di un esplicito riconoscimento, attraverso un'interpretazione sistematica delle disposizioni esistenti avrebbe potuto essere inferita l'esistenza di un autonomo, fondamentale diritto *generale* alla riservatezza. Negli anni Cinquanta, in aperto contrasto con la dottrina dominante, tali indicazioni sono seguite e sviluppate da Francesco Carnelutti: l'autorevole giurista, ben conoscendo il duplice "binario" del criterio esegetico di tipo analogico consacrato nell'art. 12, comma 2 delle disposizioni preliminari al Codice Civile, proponeva di far ricorso proprio all'analogia *juris*, interpretando le vigenti disposizioni alla luce dei principi generali dell'ordinamento: tra questi, secondo l'Autore, negli ordinamenti democratici necessariamente deve considerarsi annoverato quello che impone la protezione degli attributi fondamentali della personalità, in quanto indefettibile presupposto per una libera esplicazione della persona stessa. Attributi tra i quali ricade, a pieno titolo, la riservatezza stessa, il diritto a presidio del quale risulterebbe protetto *a prescindere* da qualsiasi manifestazione di volontà esplicita del legislatore²⁶⁹. E come disposizioni da assumere ad oggetto di tale procedimento ermeneutico, Carnelutti individua, in campo civilistico, il già ricordato art. 10 del Codice Civile e gli articoli 96 e 97 della Legge sul Diritto d'Autore; mentre nel campo penale attribuisce rilevanza agli articoli dal 616 a 623 del Codice Rocco, che puniscono talune fattispecie di «delitti contro l'inviolabilità dei segreti».

La voce di Carnelutti, nel secondo dopoguerra, non è isolata: altri autorevoli studiosi, quali Adriano De Cupis e Remo Franceschelli, alla luce di diverse ma

²⁶⁸ Cfr. ADOLFO RAVÀ, *Istituzioni di diritto privato*, Cedam, Padova, 1938, pp. 174-175.

²⁶⁹ Cfr. F. CARNELUTTI, «Diritto alla vita privata», in *Riv. Trim. Dir. Pubbl.*, Giuffrè editore, Milano, 1955, pp. 3-18.

collimanti elaborazioni, si schierano a favore dell'esistenza di un diritto "generale" alla riservatezza²⁷⁰. Nessuna di tali proposte teoriche, però, riscuote nell'immediato il favore della cultura giuridica dominante, in cui impera una concezione positivista e dominicale dei diritti della persona²⁷¹. Tuttavia, essa, assieme all'opera di promozione di una concezione della persona umana quale valore *in re ipsa* svolta dai Trattati internazionali sopra richiamati, prepara il terreno affinché la giurisprudenza (ed anche il legislatore, sebbene, fino al recepimento dei primi atti comunitari in materia, settorialmente) riconosca autonoma e fondamentale dignità giuridica all'istituto della *privacy*.

Possiamo, a questo punto, passare a riassumere le tappe in cui si snoda l'iter seguito dalla giurisprudenza italiana per giungere – faticosamente - all'affermazione del diritto in questione (in un primo momento nella sola, limitata accezione negativa in cui lo intendono i suoi padri fondatori d'oltreoceano, come *right to be let alone*).

Nella prima fase post-bellica, complice anche l'arretratezza del contesto tecnologico rispetto alla società già – interamente - massificata della regione nordamericana, la giurisprudenza tende ad escludere un'autonoma cittadinanza nell'ordinamento al diritto alla *privacy*; cosicché, ai fini della tutela del "riserbo", essa ricorre al diritto al nome o al diritto all'onore, adeguatamente tipizzati. Emblematici di tale primo periodo sono due casi, passati alla storia anche per la particolare esposizione mediatica dei loro protagonisti, in cui la Corte di Cassazione ha modo di riaffermare la visione "proprietaria" tipica del modello di

²⁷⁰ Cfr. DE CUPIS, *I diritti della personalità*, Milano, 1959, I, 47; FRANCHESCELLI, *Il diritto alla riservatezza*, Napoli, 1960

²⁷¹ V. *retro*, nota 231.

tutela della persona accolto nel Codice Civile; sebbene nel secondo di questi comincino ad evidenziarsi le prime “rotture” con la tradizione²⁷².

Il primo caso su cui la Corte si pronuncia scaturisce dalla domanda di risarcimento del danno proposta dagli eredi del celebre tenore Enrico Caruso nei confronti della casa produttrice del film (semi)biografico «Leggenda di una voce»: gli attori asserivano che il film ritraesse in modo romanzato e pregiudizievole per il “riserbo” del defunto alcuni fatti riguardanti la vita privata del medesimo, quali le umili origini e le fragilità psicologiche²⁷³. Se il Tribunale di Roma non esita a riconoscere l’esistenza di un autonomo diritto generale alla riservatezza, come posizione a presidio della sfera privata della persona, identificata con tutti quei fatti e comportamenti personali che per natura o per scelta non siano pubblici o pubblicati, e sebbene la Corte d’Appello confermi l’indirizzo, la Cassazione non si mostra dello stesso avviso²⁷⁴. La Suprema Corte afferma infatti che «nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto assoluto all’intimità della vita privata e tanto meno come limite alla libertà dell’arte. Sono soltanto riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona»²⁷⁵. In sostanza, dunque, la Corte rifiuta di riconoscere un diritto generale alla riservatezza in via esegetica desumibile dal sistema delle disposizioni civilistiche sulla tutela della persona fisica e delle sue creazioni intellettuali (come appunto gli artt. 96 e 97 della Legge sul Diritto d’Autore), anche in base all’argomento giuridico secondo le quali queste, ponendo limiti a taluni diritti costituzionalmente sanciti, come la libertà di

²⁷² G. MARINI, «Diritto alla privacy», cit., p. 209 ss.

²⁷³ Cfr. Cass., sez. I, 22.12.1956, n. 4487, in *Foro it.*, 1957, I, 4.

²⁷⁴ T. Roma, 14.9.1953, in *Foro it.*, 1954, I, 115; confermato da App. Roma, 17.5.1955, in *Foro it.*, 1956, I, 793.

²⁷⁵ Cfr. sempre Cass., sez. I, 22.12.1956, n. 4487, in *Foro it.*, 1957, I, 4., che aggiunge: «La varietà della *ratio* di queste e di altre norme, la diversa estensione della tutela da ciascuna di esse accordata ai singoli aspetti della vita privata della persona, impediscono di ricondurle tutte ad una disciplina unitaria e di estendere i divieti posti da ciascuna norma alla materia regolata da un’altra».

espressione ex art. 21, rappresenterebbero *norme eccezionali*, e pertanto soggette al divieto di *analogia legis* previsto dall'art. 14 delle preleggi²⁷⁶.

Nel secondo caso, la Suprema Corte conferma essenzialmente l'orientamento espresso ed il modello delineato nella sentenza appena esaminata²⁷⁷. Oggetto della controversia è, questa volta, un libro che, a sostegno degli attori, ricostruisce la figura di Claretta Petacci (amante, lo si ricorda, di Benito Mussolini) con toni offensivi del pudore e, soprattutto, della riservatezza della famiglia. La Corte di Appello di Milano, nell'accogliere le doglianze dei ricorrenti, ribadisce la convinzione che esista nel nostro ordinamento un diritto alla riservatezza, inteso come «facoltà giuridica di escludere ogni invadenza estranea dalla sfera della propria intimità personale e familiare», diritto che trova soltanto «in ragioni di ordine pubblico o di superiore interesse sociale» una possibile limitazione», e il cui fondamento viene per la prima volta nella storia della giurisprudenza del nostro ordinamento individuato nell'art. 8 della CEDU²⁷⁸. La Cassazione, l'abbiamo detto, continua a negare l'esistenza di un diritto alla riservatezza ed accoglie il ricorso; allo stesso tempo, tuttavia, delinea un «diritto alla libera autodeterminazione nello svolgimento della personalità» che si può espandere nei limiti della solidarietà prevista dall'art. 2 della Costituzione, di cui la pronuncia è tra le prime a promuovere un'interpretazione “aperta”, sebbene ancora vaga: tale esegesi consentirebbe di offrire tutela, di rango costituzionale, anche ad interessi e a relative posizioni non esplicitamente configurate dal legislatore, quale appunto il diritto da essa ricostruito. Diritto che sarebbe consistito proprio in «un *diritto generale della personalità*, distinto dal potere di autonomia inerente ai singoli concreti diritti e alle concrete

²⁷⁶ Cfr. art. 14, r.d. 16 marzo 1942, n. 262, che dispone: «Le leggi penali e quelle che fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati».

²⁷⁷ Cass., 20.4.1963, n. 990, in *Giur. it.*, 1963, I, 1, 961

²⁷⁸ Cfr. App. Milano, 26.8.1960, in *Foro it.*, 1961, I, 43

manifestazioni», di cui le singole norme positive vigenti tutelavano «diversi aspetti»²⁷⁹: quasi un’adesione alla concezione “monistica” propugnata negli anni Cinquanta dalla giurisprudenza tedesca.

In questa pronuncia si intravede, allora, una prima incrinatura nel modello di tutela della “prima generazione” dei diritti della persona. Tuttavia, prima di giungere al definitivo *restatement*, si devono attendere gli anni Settanta; e, soprattutto, alcuni fondamentali interventi del legislatore, sebbene settoriali.

Al pari dell’esperienza nordamericana, anche in contesto europeo comincia infatti ad avvertirsi la crescita esponenziale dei problemi configurati, per l’integrità della sfera privata degli individui, dall’avvento dell’informatica: e se negli Stati Uniti ciò conduce a sviluppare, come abbiamo già rilevato, la nozione di *information privacy* e la predisposizione delle prime *practices* sull’elaborazione elettronica dei dati, in Europa tanto i legislatori nazionali quanto le istituzioni della Comunità europea percepiscono l’emersione di una nuova dimensione della *privacy*, che attiene alla capacità dell’individuo di gestire i *flussi informativi* che lo riguardano. In ciò, guidati dalla dottrina, che accoglie gradualmente la metamorfosi della *privacy* da semplice diritto a *non interferire* a libertà intrinsecamente *positiva*, di «controllare l’uso delle informazioni che [l’individuo] riguardano»²⁸⁰. Il passo che condurrà alla definizione dottrinale,

²⁷⁹ Cfr. nello specifico Cass., 20.4.1963, n. 990, in *Foro it.*, 1963, I, 877, 1298 con nota di A. DE CUPIS, che non a caso si intitola «Riconoscimento sostanziale, ma non verbale, del diritto alla riservatezza».

²⁸⁰ La citazione, precorritrice della successiva “storia” della *privacy*, è tratta da S. RODOTÀ, «La “privacy” tra individuo e collettività», *Pol. dir.*, 1974, pag. 545, che già in *Elaboratori elettronici e controllo sociale*, cit., si era avveduto del problema. Ma tra gli anni Settanta e gli anni Ottanta sono molteplici i contributi sul nesso tra tecnologia e *privacy*, sull’esistenza dell’“omonimo” diritto e sulla trasformazione semantica e giuridica di tale categoria, e la conseguente esigenza di apprestare tutela ad un “nuovo”, dinamico interesse: cfr. tra i molti, AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978, spec.7-1, e alcuni dei fondamentali contributi contenuti in ALPA-BESSONE (a cura di), *Banche dati, telematica e*

prima ancora che positiva, di un autonomo diritto a presidio di tale diversa dimensione della *privacy*, quale appunto diritto alla protezione dei dati personali, non sarà lungo; ma, prima di qualsiasi sistematizzazione dottrinale, sono i legislatori a tentare una regolazione settoriale del fenomeno: e nel farlo essi accolgono la suddetta, “nuova” dimensione della *privacy*, taluni elaborando già concettualmente la categoria dei *dati personali*, ed istituendo forme di protezione non solo civilistiche, bensì di respiro pubblicistico. Più in generale, in ogni caso, questi interventi prendono in considerazione il rapporto tra informatizzazione dei sistemi - pubblici e privati - di “catalogazione” della vita dei consociati e diritti fondamentali della persona²⁸¹.

Tralasciando i processi di costituzionalizzazione, sui quali ci siamo già soffermati, negli anni Settanta l'Europa è disseminata di interventi normativi importanti, la maggior parte dei quali hanno peraltro a che fare proprio con lo strumento delle banche dati e, pertanto, con l'*elaborazione automatizzata* dei dati stessi. La prima si identifica tradizionalmente nella legge promulgata nello Stato federato (*Länder*) dell'Assia, parte dell'allora Repubblica Federale Tedesca, il 7 ottobre del 1970, intitolata proprio alla protezione dei dati (*Datenschutz*) rispetto ai trattamenti automatizzati svolti dal settore pubblico: con notevole lungimiranza, già in questa legge si prevedeva l'istituzione di un'Autorità pubblica a garanzia della sua applicazione: un *Datenschutz beauftragter*, sul modello rappresentato dalle *Authorities* nordamericane.

Guardando al di fuori dei confini italiani, e per citare solo alcuni esempi, a questa legge seguirono la *Datalag* svedese del 1973 e la Legge Federale Tedesca sulla Protezione dei Dati (*Bundesdatenschutzgesetz*) del 1977. È stato poi il turno

diritti della persona, Cedam, Padova 1984, come quello del “padre” dell'informatica giuridica, V. FORSINI, «Diritto alla riservatezza e calcolatori elettronici», p. 29 ss.

²⁸¹ Per una completa analisi, si può consultare l'approfondito lavoro di GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing, 2014, in particolare p. 70 ss.

della Francia, che il 6 ottobre del 1978 ha approvato la *Loi informatique e libertés*, istitutiva tra l'altro di un'Autorità indipendente per garantirne l'effettività, la *Commission Nationale de l'Informatique e des Libertés* (CNIL). Mentre nel 1984 il Regno Unito, in cui la *privacy* era stata fino a quel momento regolamentata in seno al solo *common law*, ha adottato il *Telecommunications and Data Protection Act* del 1984.

Venendo all'Italia, anche il nostro ordinamento conosce negli anni Settanta il primo, capitale intervento del legislatore, che pone per la prima volta un (implicito) fondamento normativo al diritto alla riservatezza. E non è un caso che questo si collochi sul piano della legislazione giuslavoristica. Da una parte, infatti, lo sviluppo delle tecnologie elettroniche rendevano il lavoratore esposto ad un sempre più pervasivo controllo da parte del datore di lavoro, il cui potere risultava accresciuto dal “dominio” sui dati del dipendente. Dall'altra, se il progresso della tecnologia fa emergere la dimensione sociale della *privacy*, bisogna ricordare che in Europa l'affermazione dei diritti sociali passa anche e soprattutto attraverso le lotte dei movimenti operai.

Il primo riferimento normativo che si occupa espressamente della *privacy*, sebbene ancora declinata nella sua dimensione più squisitamente negativa, è dunque, nel nostro ordinamento, da individuarsi in una disposizione del cosiddetto Statuto dei Lavoratori, una delle leggi più garantiste che il continente europeo abbia conosciuto nella disciplina delle relazioni produttive. Si intende l'art. 8, che stabilisce cristallinamente: «È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione

dell'attitudine professionale del lavoratore»²⁸². Norma che, tutt'ora in vigore, per prima offre presidio alla vita privata, sebbene entro i confini dei rapporti di lavoro e segnatamente come diritto del lavoratore; intesa, per la prima volta a livello normativo, come sfera intima, che non tollera intromissioni dall'esterno²⁸³.

Aperta la strada, il legislatore compie un altro importante intervento, che dimostra la sensibilità ai rischi configurati dalla tecnologia per la sfera privata, ed evidenzia ancora una volta il nesso tra evoluzione del diritto e trasformazioni sociali, cui la tecnica risponde e che al contempo la tecnica determina. Poco prima della metà degli anni Settanta, infatti, la l. 8 aprile 1974, n. 98, introduce nel Codice Penale un art. 615-*bis*, intitolato «Interferenze illecite nella vita privata», nel quale, al comma 1, si stabiliva che «Chiunque, mediante l'uso di *strumenti di ripresa visiva o sonora*, si procura indebitamente notizie o immagini attinenti alla *vita privata* svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni» e al comma 2 che «Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo».

L'inedita attività di produzione normativa intrapresa dal legislatore ha un'importante riflesso sullo sviluppo, nel nostro ordinamento, dei successivi orientamenti giurisprudenziali in materia di vita privata e di riservatezza.

²⁸² V. art. 8, l. 20 maggio 1970, n. 300 recante «Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento». Invero, tale norma era stata anticipata da un'altra che, sempre in ambito lavoristico, già declinava in senso moderno la nozione giuridica di vita privata, utilizzando peraltro il termine riservatezza, sebbene intesa come *dovere* del lavoratore: l'art. 6, comma 1, della l. 2 aprile 1958, n. 339 (recante «Norme per la tutela del rapporto di lavoro domestico»), stabiliva infatti che il lavoratore domestico ha, fra i propri doveri, quello di «mantenere la necessaria *riservatezza* per tutto quanto si riferisce alla vita familiare».

²⁸³ Per più approfondite riflessioni, cfr. A. INGRAO, «Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act», in *Riv. It. Dir. Lav.*, 2017.

Innanzitutto, è la Corte Costituzionale a promuovere un primo indirizzo riguardante il fondamento positivo, costituzionale o meno, di tutta una serie di diritti della personalità, tra cui “incidentalmente” viene ascritta anche la riservatezza: nella sentenza n. 38 del 1973 la Corte afferma che le norme nel caso di specie censurate, attinenti alla possibilità di ottenere il sequestro preventivo a tutela dell’immagine, «non contrastano con le norme costituzionali ed anzi mirano a tutelare e a realizzare i fini dell’art. 2 affermati anche negli artt. 3, secondo comma, e 13, primo comma, che riconoscono e garantiscono i diritti inviolabili dell’uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, *riservatezza*, intimità e reputazione, sanciti espressamente *negli artt. 8 e 10 della Convenzione europea sui diritti dell’uomo*, gli artt. 10 del codice civile, 96 e 97 della legge 22 aprile 1941, n. 633». Diritti che, entrando per tali vie nel panorama delle libertà fondamentali, sono suscettibili di bilanciamento con altri diritti di libertà, quali, appunto, la libertà di manifestazione del pensiero ex art. 21, e possono giustificare sue legislative limitazioni²⁸⁴. Da notare che questa è la seconda pronuncia, dopo quella della prima sezione della Cassazione nel caso Petacci, a richiamare direttamente l’art. 8 della CEDU come fondamento normativo di tutta una serie di posizioni considerate come “aspetti” di un più generale, monistico diritto della personalità.

Il precedente in questione influenza tutta la giurisprudenza costituzionale successiva in materia di riservatezza²⁸⁵; e tuttavia, bisogna subito anticipare che fino ad oggi la Corte Costituzionale è stata assai parca nel rendere pronunce relative al fondamento costituzionale, ai limiti, ed invero all’effettiva collocazione nel sistema delle libertà fondamentali di un *autonomo* diritto alla protezione dei dati personali, pur ormai sancito espressamente come tale tanto dalla Carta dei

²⁸⁴ Cfr. C. Cost., 12.4.1973, n. 38, in *Foro it.*, 1973, I, 170.

²⁸⁵ Cfr. tra le altre C. Cost., 139/1990, in *Foro it.*, 1990, I, 2410; C. Cost., 7.08.05, n. 271, in *Foro it.*, 2006, 129, X, p. 2661 ss.

diritti fondamentali dell'Unione europea quanto dai novellati Trattati Istitutivi dell'Unione medesima. Allo stesso modo, bisogna sottolineare che anche nelle decisioni in punto di riservatezza e di vita privata manca un'opportuna e approfondita elaborazione concettuale delle due categorie in termini di autonomi diritti soggettivi²⁸⁶. Elaborazione che, invece, è ben presente nella giurisprudenza di legittimità, a partire dalla metà degli anni Settanta.

Nel 1975, infatti, la Cassazione arriva finalmente alla prima esplicita affermazione dell'esistenza del diritto alla riservatezza nell'ordinamento italiano: stiamo parlando del famoso caso Soraya²⁸⁷. Si tratta di una sentenza particolarmente importante, perché è forse quella che affronta per la prima volta con un approccio sistematico non solo le problematiche giuridiche relative alla *privacy*, bensì anche quel nesso fondamentale esistente tra diritto e sviluppo tecnologico che, come abbiamo ampiamente messo in luce dall'inizio della trattazione, "spiega" la nascita e informa di sé la *ratio* dell'istituto *giuridico* della riservatezza.

Tracciando brevemente il contesto fattuale, negli anni in cui interviene la decisione la giurisprudenza è chiamata numerose volte a pronunciarsi su casi riguardanti la tutela del diritto all'immagine di persone celebri, sempre più vittime della molesta curiosità della stampa scandalistica²⁸⁸.

²⁸⁶ Per alcune considerazioni sinottiche, cfr. S. Calzolaio, «Protezione dati personali», in *Dig. disc. pubbl., Agg.*, (a cura di) R. Sacco, Milano, 2017, p. 616 ss.; per un'analisi più dettagliata, si v. invece il non più recentissimo contributo di Bellocci-Magnanesi-Passa-Glia-Rispoli (a cura di), *Tutela della vita privata e prospettive costituzionali*, 2006, consultabile sul sito istituzionale della Corte: <http://www.cortecostituzionale.it>.

²⁸⁷ Cass., 27.5.1975, n. 2129, in *Giur. it.*, 1976, I, 1, 982.

²⁸⁸ Possiamo rinviare alle considerazioni svolte *illo tempore* sullo *yellow journalism* negli Stati Uniti di fine diciannovesimo secolo, sebbene nei casi con cui si confronta la giurisprudenza italiana dagli anni Sessanta in poi la finalità degli scatti e delle corrispondenti notizie risieda, oltre che nel lucro, nel puro "gossip", o pettegolezzo.

Il caso specifico che interessa la Corte nella controversia di cui parliamo si iscrive in questa sequela, e riguarda un personaggio del tempo assai noto: la principessa Soraya. Quest'ultima agiva davanti al giudice di merito lamentandosi delle indiscrezioni sul suo conto alimentate per mezzo di alcune fotografie "clandestinamente" scattate e pubblicate da un settimanale. Per questo motivo, la questione veniva inizialmente rappresentata come lesione del diritto all'immagine, aggravata dal fatto che la fotografia fosse stata scattata violando il domicilio della principessa: il convenuto, tuttavia, si premurava di eccepire quale scriminante l'esercizio della libertà stampa, rivendicando l'utilità sociale dell'informazione divulgata.

Approdata la lite in Cassazione, quest'ultima si mostra decisa nel riordinare il campo. Le sue argomentazioni dimostrano la spinta impressa alla riflessione medesima proprio, e ancora una volta, dallo sviluppo tecnologico: la Corte comincia dalla constatazione delle dimensioni allarmanti assunte dal fenomeno dell'invasione nella vita privata dei singoli, lucidamente imputata al «*continuo sviluppo della moderna tecnologia*, la quale offre ai poteri pubblici o ai privati smisurate possibilità, mediante perfezionati strumenti di acquisizione conoscitiva, di *penetrante controllo su ogni aspetto di vita* e di rapida divulgazione generale dei dati acquisiti». Conseguentemente, afferma che «questa straordinaria evoluzione, specie per i suoi possibili risvolti negativi (...) non può essere ignorata nemmeno dal diritto privato, ed in particolare in sede giurisprudenziale»²⁸⁹.

Prima di giungere al suddetto *restatement*, in realtà la Corte individua i limiti al diritto di cronaca, il quale risulterebbe giustificato soltanto «se funzionale al perseguimento di uno *scopo informativo* dotato di *particolare rilevanza sociale*», che ovviamente «non può identificarsi nella morbosa curiosità che parte

²⁸⁹ Cfr. Cass., sez. I, 27.5.1975, n. 2129, in *Foro It.*, 1976, I, pp. 2901, 2902

del pubblico ha per le vicende piccanti o scandalose svoltesi nell'intimità della casa della persona assurta a notorietà»²⁹⁰.

A questo punto, la Corte passa a delineare i confini della sfera privata «protetta dal diritto» tra i cui aspetti si staglia limpida anche la riservatezza. Essa gli attribuisce la consistenza di un autonomo diritto soggettivo, individuandone un contenuto composito, sebbene ancora di tipo essenzialmente negativo: innanzitutto ne accoglie la concezione tradizionale quale *right to be let alone*, che identifica la riservatezza con il “riserbo dell'intimità domestica”, collegata al concetto di domicilio in senso materiale; ma poi, con attitudine veramente moderna, ne accoglie una concezione che fa «riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un *domicilio ideale*, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza)»²⁹¹.

In questo modo, la Corte può nella sua massima definire il diritto alla riservatezza «[posizione a] tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti», identificandone il fondamento, oltre che in una pluralità di disposizioni ordinarie, molte già ricordate (*ex multis*, artt. 5-10 cod. civ., art. 623 bis cod. pen., artt. 21 e 24 legge diritto d'autore), non solo nell'art. 2 della Costituzione, bensì anche, altrettanto direttamente, nelle disposizioni degli

²⁹⁰ Ivi, p. 2898.

²⁹¹ Ivi, p. 2903.

artt. 3, 14, 15, 27, 29, 41 della Costituzione e nelle normative internazionali ed europee, come il più volte richiamato art. 8 della CEDU²⁹².

Da quel momento in poi, la giurisprudenza di legittimità ribadirà costantemente l'orientamento espresso in Soraya, peraltro allargandone progressivamente il perimetro applicativo: oltre ad uniformarsi alla “dottrina” del domicilio ideale, essa esplicitamente afferma che, proprio in forza dell'art. 2 della Costituzione, da cui trae il suo principale fondamento giuridico in quanto *norma a fattispecie aperta*²⁹³, esiste un diritto alla riservatezza anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria: confermandone, in modo ancora più solido, la collocazione nel sistema di tutela costituzionale della persona umana²⁹⁴

La sentenza suddetta, e quelle che le seguono a sostegno del principio di diritto sancito, rappresentano un ulteriore stimolo per la dottrina, assai rigogliosa – lo abbiamo detto – negli anni Settanta e Ottanta in punto di esistenza, fondamento (costituzionale o meno), semantica e limiti del diritto alla *privacy*²⁹⁵. Tuttavia, la sentenza, vincolata dai motivi di doglianza svolti dalla ricorrente, nel riconoscere come meritevole di tutela la dimensione -ancora- negativa della *privacy*, e quindi l'interesse all'inviolabilità del proprio «domicilio ideale», sembra “trascurare” le trasformazioni indotte dal crescente processo di informatizzazione della realtà di cui abbiamo parlato sopra, relative tanto alla latitudine della categoria della *privacy* quanto all'aspettativa di tutela della

²⁹² Ivi, pp. 2896 e 2903 ss.

²⁹³ L'indirizzo, già sopra analizzato, che interpreta l'art. 2 come “valvola d'ingresso permanente” di nuovi diritti della personalità nell'ordinamento, con rango costituzionale, è dalla Cassazione già ribadita in Cass., 22.6.1985, n. 3769, in *Nuova giur. comm.*, 1985, 647

²⁹⁴ Cfr. Cass., 9.6.1998, n. 5658, in *Foro it.*, 1998, I, 2387 ed in *Danno e resp.*, 1998, con nota di A. ORESTANO, La riservatezza ancora una volta in Cassazione: fondamento, contenuto e limiti all'indomani dell'entrata in vigore della legge 675/96.

²⁹⁵ V. retro p. 78 ss. e p. 96.

società, che va estendendosi all'interesse a conoscere, controllare, indirizzare, interrompere il flusso di informazioni che la persona riguardano. Abbiamo del pari detto che la dottrina italiana appare sensibile a questa graduale evoluzione in atto nell'allora blocco occidentale, e in particolare al fenomeno della raccolta e dell'elaborazione di informazioni personali²⁹⁶. E tuttavia, il discorso che essa svolge non appare interamente al passo con i tempi.

Se infatti, come si è rilevato, in quegli anni cruciali i diversi legislatori europei cercano, pur in assenza di un preciso inquadramento concettuale del fenomeno, di far fronte a tale mutazione "antropologica" (e ciò rappresenta inevitabilmente un lievito per l'"aggiornamento" della dottrina), l'ordinamento italiano al contrario non appresta (e non appresterà fino alla fine degli anni Novanta, come vedremo) una disciplina nazionale in punto di protezione dei dati personali. Ciò ha, inevitabilmente una ricaduta sul "circolo ermeneutico" alimentato dalla dottrina e dalla giurisprudenza. In assenza di disposizioni che reagiscano ai cambiamenti socioeconomici in atto, esse non riescono infatti ad enucleare, all'interno della composita area semantica della *privacy*, una categoria giuridica *a parte*, che si sostanzi in una specifica posizione giuridica soggettiva a presidio dell'emergente interesse a controllare i propri *dati* come presupposto per il libero compimento delle proprie scelte esistenziali: ossia, in poche parole, in un autonomo diritto alla protezione dei dati personali. Di conseguenza, in Italia per lungo tempo riservatezza e protezione dei dati personali si atteggiavano quali nozioni *giuridicamente* sovrapposte, il secondo concetto essendo inteso non già come bene della vita oggetto di un autonomo diritto, bensì come *estensione*

²⁹⁶ Si possono aggiungere a quelli elencati nella nota 208, ZENO-ZENCOVICH (a cura di), *Le banche dati in Italia*, Napoli, 1985; CAMERA DEI DEPUTATI (a cura di), *Banche dati e tutela della persona*, Roma, 1983.

dell'istituto della riservatezza, a sua volta concepita quale sinonimo di *privacy* in tutte le sue diverse accezioni²⁹⁷.

Prima che la nozione di *data protection* quale autonomo diritto soggettivo invalga nel nostro ordinamento, si dovranno attendere gli atti normativi internazionali e, soprattutto, l'adozione delle prime "olistiche" normative comunitarie di settore, e il conseguente recepimento delle medesime a partire dal 1996. Ma, semplificando un poco l'iter, si può convenzionalmente individuare il momento in cui prende avvio la trasformazione del paradigma epistemologico privacy-riservatezza accolto nella dottrina italiana nel periodo che segue all'adozione di una fondamentale sentenza della Corte Costituzionale Federale tedesca, passata alla storia come «decisione sul censimento»: essa cristallizza a livello giurisprudenziale gli approdi del decennale dibattito fiorito in senso alla dottrina tedesca, particolarmente lungimirante, sull'esistenza di un c.d. diritto all'autodeterminazione informativa (*Recht auf informationelle Selbstbestimmung*), quale aspetto dell' *allgemeines Persoenlichkeitsrecht*²⁹⁸

È necessario, per quanto evidente, premettere che la particolare sensibilità degli operatori del diritto dell'ordinamento tedesco in ordine alle ricadute dell'elaborazione elettronica dei dati sulla libertà personale dei singoli, e dunque

²⁹⁷ Come esempio di una lettura della protezione dati quale bene giuridico "inglobato" nella riservatezza, a sua volta identificata con la nozione angloamericana di *privacy*, cfr. BUSIA, «Riservatezza (diritto alla)», in *Digesto/pubbl.*, Torino, 2000; sulla fisionomia della dottrina e della giurisprudenza italiana degli anni Settanta e Ottanta in punto di privacy, v. l'approfondito lavoro di TIMIANI, «Un contributo allo studio sul diritto alla riservatezza», *SPPC*, 2/2012, 51 ss.

²⁹⁸ Cfr. BVerfG, 15.12.1983, in BVerfGE, 1984, 65, p 1-71. Sul dibattito nella dottrina tedesca che ha condotto alla teorizzazione del diritto alla *Informationelle Selbstbestimmung*, cfr. W. STEINMÜLLER, «Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung», in *NJW*, 1984, p. 398 ss. Per una dettagliata disamina della sentenza, cfr. G. SARTOR, «Tutela della personalità e normativa per la protezione dei dati. La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici della "Datenschutz"», in *Informatica e diritto*, XII Annata, Vol. XII, 1986, n. 3, pp. 95-118.

all'interesse a controllarne il processo, dipende dall'avanzata, quasi precoce in contesto europeo, informatizzazione che caratterizzava la Germania di quegli anni (in particolare la pubblica amministrazione), dalla particolare solerzia con cui tanto i *Landër* quanto la Repubblica Federale aveva risposto al crescente fenomeno del trattamento "informatico" dei dati personali²⁹⁹.

Non stupisce che dunque nell'ordinamento in questione, agli inizi degli anni Ottanta, fosse già esistente ed anzi maturo il dibattito sull'opportunità di riconoscere alla persona fisica un diritto che ne presidiasse l'interesse ad autodeterminarsi nella gestione delle informazioni "in entrata e in uscita" rispetto alla sua persona, sinonimo dunque del concetto di *informational privacy* americano e prodromo del diritto di origine "comunitaria" alla protezione dei dati personali. Penetrate le riflessioni nella giurisprudenza, la Corte costituzionale tedesca, nella sentenza in esame, inaugura un fecondo indirizzo giurisprudenziale che influenza tutto il successivo discorso svoltosi in contesto europeo, nazionale come sovranazionale, sulla protezione giuridica da riconoscere al *soggetto-persona umana* in relazione alle informazioni trattate che lo riguardino. La Corte, investita della questione di legittimità costituzionale avente ad oggetto la legge sul censimento approvata dal parlamento federale nel 1982, la quale prevedeva un'ampia rilevazione dei dati attraverso l'imposizione ai cittadini dell'obbligo, pecuniariamente sanzionato, di rispondere ad una dettagliata serie di domanda, si accorge con lungimiranza delle potenziali ripercussioni di processi così generalizzati di trattamento di dati personali sulle libertà individuali³⁰⁰. Pertanto,

²⁹⁹ Come abbiamo già evidenziato, al 1970 risale la prima legislazione settoriale di livello regionale (Land dell'Assia) e al 1977 quella nazionale, v. retro. Per una sintetica presentazione della normativa tedesca in materia, e del contesto storico-sociale in cui si iscrive, cfr. LOSANO, «La legislazione tedesca sulla protezione dei dati», in CAMERA DEI DEPUTATI (a cura di), *Banche dati e tutela della persona*, cit., pp. 174-188.

³⁰⁰ Cfr. SARTOR, «Tutela della personalità e normativa sulla protezione dei dati», cit. p. 97 ss.; E. BRUGIOTTI «La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico», in *dirittifondamentali.it*, 2/2013, p. 16 ss.

con la sentenza in esame, la Corte attribuisce al bene giuridico rappresentato dall'aspirazione a *proteggere i propri dati*, e dunque a controllarne l'utilizzo, un rilievo costituzionale, individuando un «*Recht auf informationelle Selbstbestimmung*», ossia un *diritto all'autodeterminazione informativa*, ricostruito come una delle specifiche articolazione del diritto generale della personalità (*allgemeines Persoenlichkeitsrecht*), già, come abbiamo detto, pacificamente riconosciuto dalla giurisprudenza costituzionale e di legittimità tedesca, e fondato come sappiamo sugli artt. 1, comma , e 2 comma 1 della *Grundgesetz*³⁰¹. Il suo contenuto è individuato nel «potere di ciascuno di decidere sostanzialmente da sé circa la rivelazione e l'utilizzo dei propri dati personali», dal momento che il libero sviluppo della personalità presuppone la protezione del singolo in relazione alla memorizzazione, all' utilizzazione e al trasferimento incontrollato di dati personali³⁰².

³⁰¹ Cfr. G. SARTOR, «Tutela della personalità e normativa sulla protezione dei dati», cit., p. 100 ss.; E. BRUGIOTTI, «La privacy attraverso le “generazioni dei diritti”», cit.; S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 317 ss.; S. CALZOLAIO, «Protezione dati personali», cit., pp. 616-617.

³⁰² Cfr. il testo del preambolo della sentenza, che ben sintetizza il complesso contenuto del diritto individuato: BVfG, 15.12.1983, cit., pp. 1-2. Assai interessanti sono le considerazioni di S. Rodotà, *Il diritto di avere diritti*, che nel delineare i successivi sviluppi della giurisprudenza costituzionale tedesca, consolidatori di tale orientamento, rileva che «altrettanto importante è la successiva sentenza del 27 febbraio 2008, con la quale il *Bundesverfassungsgericht* ha dichiarato contrario al *Grundgesetz* un emendamento alla legge sui servizi di sicurezza del Land Nord Reno-Westfalia. Questo emendamento aveva attribuito ai servizi il diritto di “controllare segretamente in ogni modo Internet, in particolare intervenendo segretamente sugli strumenti di comunicazione adoperati e accedendo clandestinamente ai sistemi informativi tecnologici con qualsiasi modalità tecnica”. La sentenza del *Bundesverfassungsgericht* è stata considerata una decisione assolutamente innovativa, perché ha creato un nuovo “diritto fondamentale alla riservatezza e all'integrità dei sistemi informativi tecnologici” come parte [anche esso, nell'aggiungersi al già individuato diritto all'autodeterminazione informativa] del diritto generale della personalità riconosciuto [alla luce dell'orientamento consolidatosi dalla metà degli anni Cinquanta in poi] dalla Costituzione tedesca (...)», p. 316

Con la sentenza in questione, la sua successiva consolidazione giurisprudenziale e la penetrazione nella sensibilità giuridica europea dell'idea fatta propria da dottrina e giurisprudenza tedesca, si prepara allora il terreno per il successivo processo di “costituzionalizzazione europea” dell'autonomo diritto alla protezione dei dati personali, che ci apprestiamo ad osservare più da vicino.

2.2.3. Dalla Direttiva 95/46/CE al Trattato di Lisbona: il processo di “costituzionalizzazione europea” del diritto fondamentale alla protezione dei dati personali

Il quadro che abbiamo tracciato ci restituisce un fatto: all'inizio degli anni Novanta, la disciplina della *privacy* e del trattamento delle informazioni personali sul territorio europeo risultava in un mosaico di normative nazionali tra loro assai eterogenee, molte delle quali – lo abbiamo visto – non poco restrittive in relazione all'impiego degli elaboratori elettronici. A questa frammentazione normativa corrisponde, tuttavia, una sempre crescente considerazione dei dati personali quali beni che esprimono un valore patrimoniale, materia prima di una nuova economia che si nutre di informazioni come presupposto assunto dai pubblici decisori per implementare l'efficacia delle proprie politiche, e, soprattutto, dalle imprese per accrescere la propria competitività sul mercato: si parla, non a caso, di *data driven economy*³⁰³.

³⁰³ Illustrano limpidamente il quadro alcuni dei contributi presenti nel volume P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino, 2022: cfr. ad es. S. SICA, V. D'ANTONIO, «La commodification dei dati personali nella data driven society», p. 129 ss.; G. DI FILIPPO, «I dati come beni giuridici. Dati personali e dati non personali: regime di appartenenza e di circolazione», p. 41 ss. Cfr. anche A. MANTELERO, «Big data: i rischi della concentrazione del potere informativo digitale e gli

Per questo motivo, le istituzioni normative comunitarie cominciano ad avvertire prepotentemente l'esigenza di dotare l'ordinamento sovranazionale di una propria disciplina in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali: un atto normativo che armonizzi *all'interno del mercato unico* le differenti discipline vigenti (o meno, come nel caso italiano) negli Stati membri in materia di trattamento dei dati, al fine precipuo di garantire la libera circolazione dei dati personali e, in senso strumentale al primo, di tutelare in modo uniforme la persona sul territorio comunitario³⁰⁴. La risposta ad essa è consistita nell'approvazione della c.d. Direttiva Madre in materia di *data protection*: la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Stante l'assenza di una norma, nel sistema dei Trattati Istitutivi, che attribuisse alla Comunità la competenza normativa in punto di protezione delle informazioni relative alla persona fisica, la Direttiva risultava adottata sul fondamento giuridico degli artt. 7A e 100A del Trattato istitutivo della Comunità Europea (TCE), e dunque come misura di ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri, al fine della instaurazione progressiva di un mercato interno: la prospettiva adottata era, dunque, ancora essenzialmente preordinata a massimizzare le libertà economiche fondamentali quali pilastro dello «spazio senza frontiere [economiche] interne» che l'ordinamento europeo aspira, tra i suoi principali scopi, a realizzare precettivamente³⁰⁵. Al contempo,

strumenti di controllo», in *Dir. Inform.* XXVII, I, 2012, p. 135 ss. Di *data driven society* e di *Big Data* come connotati della nostra epoca se ne parlerà meglio nel prossimo paragrafo.

³⁰⁴ Cfr. ex multis F. DONATI, «sub art. 8. Protezione dei dati di carattere personale», in R. BIFULCO, M. CARTABIA, CELOTTO, *L'Europa dei diritti*, Bologna, 2001; G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati», in *Nuove leggi civ.*, pp. 1-5.

³⁰⁵ Disponeva infatti l'art. 7A, Trattato istitutivo della Comunità Europea: «Il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni del presente trattato»; ricadenti dunque, a seconda delle fattispecie, nell'una o nell'altra delle categorie ivi

come dimostrano i considerando n. 2, 7 e 8, il legislatore intende contemperare tale obiettivo con quello di una più forte ed uniforme tutela dei diritti e delle libertà *fondamentali* della persona, garantendone l'equivalenza in tutti gli Stati membri: e tuttavia la stessa massimizzazione della tutela appare intesa, secondo una prospettiva ancora essenzialmente economica (o anche "mercantilista"), come strumentale a ridurre gli ostacoli alla circolazione stessa dei dati, e conseguentemente al funzionamento del mercato medesimo e sviluppo economico della Comunità che anche (e soprattutto) da essi, nella società dell'informazione, essenzialmente dipende.³⁰⁶ Indice, questo del fatto che in seno alle istituzioni comunitarie non è ancora maturata quella più matura visione, promossa negli anni dall'attività della Corte di giustizia dell'Unione europea su impulso della giurisprudenza della Corte europea dei diritti dell'Uomo e delle «tradizioni costituzionali comuni» e consacrata positivamente, come vedremo, a

previste, il fine al cui perseguimento risultava vincolata la direttiva era proprio la libera circolazione interna dei dati dei cittadini degli Stati membri.

³⁰⁶ Il considerando n. 2 afferma infatti che: «i sistemi di trattamento dei dati sono al servizio dell'uomo (...) debbono rispettare le libertà e i diritti fondamentali (...) [delle persone fisiche], in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui»; l'interpretazione comunitaria della tutela della persona umana con riferimento al trattamento dei suoi dati quale *strumento* per la piena instaurazione del mercato unico traspare nitida dai cons. 7: «considerando che il divario nei livelli di tutela dei diritti e delle libertà personali, in particolare della vita privata, garantiti negli Stati membri relativamente al trattamento di dati personali *può impedire la trasmissione dei dati stessi* fra territori degli Stati membri e che tale divario *può pertanto costituire un ostacolo all'esercizio di una serie di attività economiche* su scala comunitaria, falsare la concorrenza e ostacolare, nell'adempimento dei loro compiti, le amministrazioni»; e dal cons. n. 8, che afferma come «per eliminare gli ostacoli alla circolazione dei dati personali, il livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento di tali dati [debba] essere *equivalente* in tutti gli Stati membri (...) obiettivo, fondamentale per il mercato interno». Sulla strumentalità degli obblighi previsti della direttiva pressoché interamente allo sviluppo del Mercato Interno, cfr. ad es. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino 2016, p. 68 ss.

partire dalla Carta dei diritti fondamentali dell'Unione europea, che interpreta la persona umana come *valore in re ipsa*³⁰⁷.

A prescindere dal fine esplicitamente perseguito, la Direttiva 95/46 riesce a rappresentare uno spartiacque nella concezione e nelle tecniche di protezione della vita privata in contesto europeo: essa promuove un modello di tutela invero statico, di natura essenzialmente rimediale, che con il tempo e l'affermazione di una società sempre più *datificata* risulterà insufficiente; ma, in ogni caso, un primo modello che rispecchi l'obiettivo dell'*integrazione comunitaria* in materia, per almeno un decennio capace di predisporre garanzie uniformi in tutti gli Stati membri³⁰⁸.

La direttiva reca uno schema contenente tutti gli elementi essenziali per approntare una tutela nazionale omogenea dei dati personali, dalle definizioni alle sanzioni, mutuando, come già abbiamo avuto modo di dire, una parte considerevole dei principi enunciati dalla Convenzione 108 del Consiglio d'Europa. E tuttavia, ai fini del presente lavoro occorre mettere in luce tre aspetti fondamentali e innovativi della disciplina introdotta.

Il primo risultato certamente più rilevante, nonché duraturo, consiste nell'aver cristallizzato a livello normativo sovranazionale una precisa concezione di *privacy*, fondata sul legame tra protezione dei dati personali ed esercizio dei diritti fondamentali: l'art. 1 della direttiva, infatti, espressamente lega il trattamento dei dati personali al «diritto alla vita privata» (o - può essere interessante notarlo - *right to privacy*, nell'originale inglese), intendendo questo

³⁰⁷ Sull'impronta «personalista» assunta dal diritto comunitario, specialmente dopo la Carta dei diritti fondamentali e il Trattato di Lisbona, cfr. ad es. AIELLO, «La protezione dei dati personali dopo il Trattato di Lisbona», in *Oss. del dir. civ. e comm.*, n. 2/2015, 431 ss.; S. CALZOLAIO, «Protezione dati personali», cit., p. 618 ss.

³⁰⁸ Sui caratteri del primo modello di tutela *europeo* predisposto dalla dir., cfr. ex multis MACARIO, «La protezione dei dati personali nel diritto privato europeo», in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento di dati personali*, Torino, 1997; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., pp. 73-136.

riferimento fondato sull'art. 8 della CEDU, richiamato dal considerando n. 10³⁰⁹. Come si è già ampiamente sottolineato, sebbene l'articolo in questione tuteli espressamente la vita privata e familiare, la Corte di Strasburgo ha ripetutamente riconosciuto come la protezione dei dati personali ne rappresenti un fondamentale aspetto³¹⁰. Sebbene né l'art. 8 Cedu né l'art. 1 della Direttiva codifichino espressamente alcun *diritto fondamentale* alla protezione dei dati personali, quest'ultima nel riconoscere il legame suddetto dà un fondamentale impulso alla diffusione delle nozioni di dati personali e di *data protection* negli Stati membri dell'allora Comunità Europea, che gradualmente la recepiscono³¹¹. Per quanto attiene nello specifico all'Italia, l'ordinamento provvede all'adeguamento con la legge 31 dicembre 1996, n. 675, recante norme sulla «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali», che rappresenta il primo atto normativo nel nostro Stato interamente dedicato al trattamento dei dati personali: e, a dimostrazione dell'effetto propulsivo della direttiva, esso determina l'introduzione a livello normativo della dimensione *positiva* della *privacy*, attraverso il riferimento ai «dati personali», e il suo fondamentale

³⁰⁹ Cfr. art. 1, comma 1, Dir. 95/46/CE, in forza del quale «Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e *particolarmente del diritto alla vita privata*, con riguardo al trattamento dei dati personali»; il cons. 10, eloquentemente, prevede che «le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario».

³¹⁰ V. *retro*. Un'ampia casistica di sentenze della Corte edu in riferimento alla protezione dei dati personali si trova anche in POLLICINO, BASSINI, «sub art. 8», in *Carta dei diritti fondamentali dell'Unione europea*, a cura di Mastroianni, Pollicino, Allegrezza, Pappalardo, Razzolini, Milano, 2017, 137- 140.

³¹¹ Cfr. sul punto ancora GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, cit., che a p. 156 ss. afferma «as Directive 95/46/EC was progressively transposed into Member States, the notions of personal data, and data protection, spread throughout Europe», per poi sottolineare tuttavia che «national differences persisted, especially in relation to connections between personal data protection and fundamental rights».

rapporto proprio con la riservatezza, quest'ultima finalmente sancita a livello positivo come (oggetto di un) diritto soggettivo³¹². Poco dopo, con la Carta dei diritti fondamentali dell'Unione europea e il Trattato di Lisbona, si realizzerà l'effettivo compimento del processo di affermazione, a livello europeo, del *diritto alla protezione dei dati personali come diritto fondamentale*, autonomo sebbene complementare rispetto al diritto alla riservatezza: l'uno a presidio della dimensione positiva, l'altro della dimensione negativa della *privacy*. Tale affermazione avrà ampi riflessi in tutti gli Stati membri, e specialmente in Italia. Prima, però, concentriamoci sugli altri due aspetti significativi della direttiva.

Il secondo aspetto che merita qui sottolineare è che la direttiva, all'art. 28, obbliga gli Stati ad istituire un'«Autorità di controllo» indipendente, cui siano attribuiti poteri di controllo e di intervento in ordine all'effettiva applicazione della disciplina introdotta³¹³: con ciò, dimostrandosi l'accoglimento di quella prospettiva matura, già fatta propria dalle legislazioni costituzionali ed ordinarie di alcuni Stati membri, che valorizza *la dimensione collettiva della privacy*, e in particolare il rilievo pubblicistico della protezione dei dati personali quale «ineliminabile garanzia contro ogni forma di potere, pubblico o privato che sia»³¹⁴.

³¹² Cfr. infatti art. 1, comma 1, la l. 31 dicembre 1996, n. 675, che recita: «La presente legge garantisce che il *trattamento dei dati personali* si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, *con particolare riferimento alla riservatezza* e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione».

³¹³ Cfr. infatti art. 28, Dir. 95/46 CE, che recita al comma 1: «Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.»

³¹⁴ La citazione è di S. RODOTÀ, «Introduzione», in D. LYON, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano 2003.

Ai fini del presente lavoro, poi, ancora più importante risulta l'art. 15 della Direttiva: quest'ultima disposizione, già circondata nella sua redazione da un acceso dibattito in seno al Parlamento Europeo, introduceva a livello comunitario, sulla scorta di alcune delle legislazioni nazionali già passate in rassegna, un'apposita disciplina dei processi decisionali *interamente* basati su una determinata specie di trattamenti automatizzati, ovverosia quelli essenzialmente consistenti nella *profilazione*. Sulla norma in questione si avrà modo di tornare nel secondo capitolo, in quanto prodromo, con tutti i suoi pregi e le sue criticità, dell'attuale art. 22 del GDPR, il quale rappresenta il fulcro della disciplina oggi vigente nell'ordinamento europeo, e in quello dei suoi Stati membri, in materia di processi decisionali interamente automatizzati³¹⁵. Solo a titolo introduttivo, può già dirsi che l'art. 15, anticipando con lungimiranza le criticità poi esplose nell'attuale "società della spersonalizzazione", imperniata su profilazione e *data mining*, riconosceva ad ogni persona fisica il diritto «a non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti, fondata *esclusivamente* su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità (...)»³¹⁶. Nonostante la virtuosa

³¹⁵ V. cap. 3. Cfr. già sull'art. 15 della direttiva previgente e sul dibattito che l'ha preceduto L.A. BYGRAVE, «Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», 17 *Computer Law & Security Review*, 19 (2001); E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation», in *Nuove leggi civ.*, 2018, pp. 1209-1236

³¹⁶ Cfr., esteso, l'art. 15, Dir. 95/46 CE: «1. Gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc. 2. 2. Gli Stati membri dispongono, salve le altre disposizioni della presente direttiva, che una persona può essere sottoposta a una decisione di cui al paragrafo 1, qualora una tale decisione: a) sia presa nel contesto della conclusione o dell'esecuzione di un contratto, a condizione che la domanda relativa alla conclusione o all'esecuzione del contratto, presentata dalla persona interessata sia stata accolta, oppure che misure adeguate, fra le quali la possibilità di far valere il proprio punto di vista garantiscano la

intenzione di rappresentare una norma generale sulla «distribuzione del potere di decisione nel mondo digitale»³¹⁷, la declinazione della disciplina secondo lo schema del diritto, piuttosto che del divieto generale, e l'ampia possibilità di deroga garantita dal secondo comma dell'art. 15 hanno reso la disposizione soggetta ad interpretazioni restrittive da parte di molte normative nazionali di attuazione, nonché trascurata dalla giurisprudenza europea e nazionale, dimidiandone dunque l'efficacia pratica³¹⁸. Resta comunque la lungimiranza, che ne ha determinato la "reviviscenza" quale modello su cui è stato edificato l'attualmente vigente art. 22 del GDPR.

Riprendendo le fila del percorso di affermazione del diritto alla protezione dei dati personali nel contesto europeo, la vera svolta nel dibattito sull'esistenza e sulla natura di libertà fondamentale del diritto in questione avviene con l'inedita adozione, nel 2000, della Carta dei diritti fondamentali dell'Unione europea (CDFUE), nella prassi denominata Carta di Nizza: quest'ultima, infatti, a differenza dell'art. 8 CEDU per la prima volta distingue da un punto di vista sistematico il diritto al rispetto della vita privata e familiare e il diritto alla protezione dei dati personali, incardinandone la disciplina in due distinti articoli: rispettivamente, l'art. 7 e l'art. 8³¹⁹. E dal momento che alla luce dell'art. 52 della

salvaguardia del suo interesse legittimo, oppure b) sia autorizzata da una legge che precisi i provvedimenti atti a salvaguardare un interesse legittimo della persona interessata.»

³¹⁷ La citazione è di S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 328.

³¹⁸ Cfr. già ora I. MENDOZA, L.A. BYGRAVE, «The Right Not to be Subject to Automated Decisions Based on Profiling», in T.E. Synodinou, P. Jougoux, C. Markou E T. Prastitou (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 77 e 80.

³¹⁹ Cfr. Carta dei diritti fondamentali dell'Unione Europea, Nizza, 2000/C 364/0; art. 7, rubricato «Rispetto della vita privata e familiare»: «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni»; e art. 8, rubricato «Protezione dei dati di carattere personale»: «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati

Carta medesima le sue disposizioni, dove riconoscano diritti corrispondenti a quelli previsti dalle norme della CEDU, devono interpretarsi allo stesso modo in cui lo siano – per interposizione, allora, della Corte di Strasburgo – le seconde, è pacifico che la vita privata di cui all’art. 7 ricomprenda il bene giuridico rappresentato dalla riservatezza³²⁰. Così la Carta finisce per riconoscere la doppia natura della *privacy* e per differenziare positivamente, al suo interno, due autonomi diritti: il primo, che ben conosciamo, radicato nell’art. 7, a presidio della sua dimensione negativa, concretizzantesi dunque nella “tradizionale” libertà di *escludere* gli altri dalla propria sfera privata il secondo, radicato nell’art. 8, a difesa della sua dimensione positiva, dinamica, quale pretesa tutelata di esercitare un controllo consapevole sulla circolazione delle informazioni che la propria persona riguardano³²¹. Stefano Rodotà ha brillantemente osservato che la Carta, nell’operare tale giuridica distinzione, che «non è di facciata», rappresenta sotto tale profilo il «punto di arrivo di una lunga evoluzione del concetto di *privacy*, dal (...) diritto di essere lasciati soli fino al diritto (...) a mantenere il controllo sulle informazioni e di determinare le modalità di costruzione della propria sfera privata»³²².

Ma il rilievo del “sub-sistema normativo” delineato dalla Carta non consiste soltanto nell’aver distinto a livello normativo tra diritto alla riservatezza, quale

raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un’ autorità indipendente.»

³²⁰ Cfr. ad es. v. GROPPI, sub «art. 7. Rispetto della vita privata e della vita familiare», in Bifulco, Cartabia, Celotto, *L’Europa dei diritti*, Bologna, 2001, rispettivamente 76 ss. e 83 ss; F. DONATI, sub «art. 8. Protezione dei dati di carattere personale», in BIFULCO, CARTABIA, CELOTTO, *L’Europa dei diritti*, cit., p. 85 ss.

³²¹ Cfr. per tale lettura, che qui si condivide, S. CALZOLAIO, «Protezione dei dati personali», cit., pp. 614-620.; G. C. FERONI, «I dati personali come oggetto di un diritto fondamentale», cit., pp. 70-72; L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, p. 15 ss.; G. FINOCCHIARO, «Identità personale (diritto alla)», in *Digesto/civ., Agg.*, Torino, 2010.

³²² S. RODOTÀ, «Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della *privacy*», in *Eur. Dir. priv.*, 2004, p. 3.

libertà negativa, e diritto alla protezione dei dati personali, quale *autonoma libertà positiva*, complementari facce del “prisma” rappresentato dall’interesse alla protezione della propria sfera privata. Esso si specifica ulteriormente nell’aver annoverato il diritto alla protezione dei dati personali tra i *diritti fondamentali* riconosciuti in seno all’ordinamento comunitario: rilievo importante, nella misura in cui, lo si ricorda, il diritto in questione pareva non far parte di (almeno) alcune delle tradizioni costituzionali dei suoi Stati membri, tra cui l’Italia³²³.

Allo stesso tempo, nel determinare il nucleo essenziale del suo contenuto, individuando al secondo comma il principio secondo cui «i dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge», e, inciso ancor più importante, affermando il diritto di ogni persona ad «accedere ai dati raccolti che la riguardano e di ottenerne la rettifica», l’art. 8 della Carta di Nizza pare definitivamente accogliere proprio la fisionomia di quel diritto all’autodeterminazione informativa sancito vent’anni prima dalla Corte costituzionale federale tedesca nell’importante «decisione sul censimento» che abbiamo avuto modo di esaminare³²⁴.

Infine, di acuto rilievo è anche in tal caso la previsione, sul piano istituzionale, di un’Autorità amministrativa indipendente preposta a tutela del diritto medesimo, che vigili sull’applicazione della disciplina vigente, prevenendo e sanzionando eventuali violazioni: ulteriore conferma della sensibilità delle istituzioni comunitarie, e più in generale della cultura giuridica europea, alla vocazione sociale dei rischi cui la nuova realtà elettronica, informatica e digitale esponesse la sfera privata dei singoli.

³²³ V. *retro*, e cfr. sempre sul punto GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, cit., 203

³²⁴ V. *retro*, e cfr. BVerfG, 15.12.1983, in BVerfGE, 1984, 65, p 1-71.

Le considerazioni appena svolte in merito alla CDFUE dimostrano che obiettivo dell'ordinamento comunitario, con la proclamazione "solenne" del diritto alla protezione dei dati personali, intendesse spostare sul piano costituzionale, e dunque nell'embrionale sistema europeo dei diritti fondamentali che già ambiva a collocarsi sul piano del diritto dei trattati, i principi essenziali della disciplina introdotta con la Direttiva 95/46, a propria volta ereditati dalla Convenzione 108. Tuttavia, la Carta di Nizza non aveva tale potere: essa, lungi dall'esprimere un autonomo valore giuridico vincolante, era ascrivibile alla categoria delle fonti di ri-cognizione del diritto vigente, o degli atti (internazionali) di *soft law*. Il testo aveva dunque la funzione di *consolidare* i principi generali e i diritti fondamentali già desumibili dalle altre fonti primarie di diritto comunitario, quali i trattati istitutivi e le tradizioni costituzionali comuni agli Stati membri, rappresentando così un'altra "fonte di ispirazione" per la Corte di Giustizia nello svolgimento della propria opera di ricostruzione dei primi; al più, assumeva *valore persuasivo* in ordine a quelle posizioni non altrimenti desumibili dal sistema normativo disegnato dal diritto positivo e della giurisprudenza della CGUE, come nel caso, appunto, dell'art. 8³²⁵. Né, tantomeno, essa poteva introdurre un'apposita base giuridica, che la competenza a disciplinare la protezione dei dati personali quale oggetto di un diritto fondamentale attribuisse alla Comunità europea.

Tuttavia, la prospettiva in questione, stante la carica assiologica di una norma come l'art. 8 della Carta, non poteva che rivelarsi insufficiente. E infatti, poco meno di un decennio dopo, il processo di costituzionalizzazione avviato si

³²⁵ Cfr. E. CANNIZZARO, *Il diritto dell'integrazione europea. L'ordinamento dell'Unione*, Giappichelli Editore, 2017, p. 151 ss.; BIFULCO, CARTABIA, CELOTTO, «Introduzione», in ID., *L'Europa dei diritti*, cit., 12; sull'orientamento già affermato dalla Corte di Giustizia prima del "nuovo" art. 6 TUE che individua i principi generali dell'ordinamento comunitario quali fonti di diritti fondamentali, da ricostruirsi attraverso (in qualità di «fonti d'ispirazione») le tradizioni costituzionali comuni e i Trattati internazionali sui diritti umani (come la CEDU), cfr. C. Giust. UE, 14-05-1974, C-4/73, *Nold*.

conclude con la definitiva sanzione del diritto alla protezione dei dati personali quale diritto fondamentale, di rango dunque primario, nel quadro dell'ordinamento comunitario: il c.d. Trattato di Lisbona, nel modificare i Trattati Istitutivi dell'Unione europea, introduce l'art. 6 dell'attuale TUE, che tra le altre disposizioni attribuisce il medesimo valore giuridico dei Trattati all'intero *corpus* normativo della Carta di Nizza, compreso, pertanto, l'art. 8³²⁶. Contestualmente, il Trattato di Lisbona introduce l'art. 16 del Trattato sul funzionamento dell'Unione europea: norma di capitale importanza, perché si risolve nell'esplicita attribuzione all'Unione della competenza materiale *piena* in materia di «protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale», assurgendo dunque ad apposita base giuridica per l'implementazione di una normativa sul trattamento dei dati personale che persegua lo specifico, primario obiettivo di *tutelare la persona umana*.³²⁷ La norma medesima, nella sua

³²⁶ V. infatti l'art. 6 del Trattato istitutivo dell'unione Europea (TUE), entrato in vigore successivamente alla modifica l'1.12.2009: «1. L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha *lo stesso valore giuridico dei trattati*. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni. 2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati. 3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali». In punto di valore giuridico assunto dalla Carta dopo «Lisbona», cfr. L. TRUCCO, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, Torino, 2013. Sui riflessi del Trattato di Lisbona sull'affermazione del diritto fondamentale alla protezione dei dati personali, cfr. AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona*, cit.

³²⁷ Cfr. art. 16, Trattato sul funzionamento dell'Unione Europea, che recita: «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali

architettura, riproduce e adatta in funzione operativa il disposto dell'art. 8 della CDFUE: essa attribuisce al Parlamento europeo e al Consiglio il potere di stabilire norme relative alla protezione delle persone fisiche in relazione al trattamento dei propri dati personali, nonché sulla libera circolazione di essi; e, ugualmente, affida il controllo sul rispetto di tali norme ad *autorità indipendenti*. Ma, soprattutto, essa proclama ancora una volta, e in qualità di disposizione *materialmente* inserita nel sistema normativo delineato dai Trattati, il diritto di ogni persona alla «protezione dei dati personali che la riguardano».

Il combinato disposto degli art. 16 del TFUE, dell'art. 39 parimenti inserito nel TUE dal Trattato di Lisbona e dell'art. 8 della Carta di Nizza, ormai giuridicamente equivalente ai Trattati, non può che sancire il pieno riconoscimento, nell'ambito dell'ordinamento eurounitario, del diritto alla protezione dei dati personali quale diritto fondamentale³²⁸. Allo stesso tempo, la disciplina così delineata determinata che alla tutela di quest'ultimo diritto, parallelamente ed anzi *prioritariamente* rispetto alla libera circolazione dei dati in funzione dell'instaurazione del Mercato Unico, l'UE risulti vincolata

dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea». Contestualmente, il Trattato di Lisbona introduce l'articolo 39 del TUE, che così recita: «Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».

³²⁸ V. i riferimenti indicati a nota 298, e in più, per un quadro più dettagliato, F. PIZZETTI, *La Privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, Giuffrè, Milano, 2017. Conviene peraltro qui aggiungere scrupolosamente che con Lisbona la stessa "sorte" del diritto alla protezione dei dati personali investe il diritto alla vita privata, e soprattutto, nel suo alveo, l'autonomo e complementare diritto alla riservatezza: il quale, attraverso l'interpretazione «convenzionalmente orientata» dell'art. 7 della Carta, come tutte le disposizioni della stessa ex art. 6 TUE provvisto della *medesima forza giuridica* di una norma dei Trattati, trova anch'esso esplicita e indiscutibile collocazione nel quadro dei diritti fondamentali, di rango «supremo», dell'ordinamento europeo.

nell'esercizio della esplicita competenza normativa ed istituzionale attribuitale. Sul punto, è stato acutamente osservato che i dati «concernenti le persone fisiche, in linea con l'*evoluzione in senso personalista del diritto comunitario* rafforzata dal Trattato di Lisbona, non vengono più trattate esclusivamente come beni provvisti di valore economico, la cui circolazione favorisce la crescita del mercato (...). La tutela delle persone fisiche con riguardo al trattamento dei dati personali diviene, in quanto diritto fondamentale, l'obiettivo primario perseguito dalle istituzioni comunitarie nella regolazione della materia»³²⁹.

Il processo di affermazione della dimensione positiva della *privacy* quale “oggetto” di un autonomo diritto soggettivo, di natura fondamentale proietta riflessi profondi in alcuni Stati membri, sin dall'adozione della Carta; tra questi, spicca certamente l'Italia.

Il faticoso percorso di distinzione concettuale, e conseguentemente giuridica, dell'«autodeterminazione informativa» dalla riservatezza, e delle rispettive pretese di tutela, cominciato con l'attuazione della Direttiva 95/46 ad opera della legge n. 675/1996, riceve un'ulteriore spinta dalla Carta e dall'esigenza di dare completa attuazione anche alla c.d. Direttiva E-Privacy adottata nel 2002³³⁰: il legislatore italiano compie una poderosa opera di

³²⁹ Cfr. ancora AIELLO, *La protezione dei dati personali dopo Lisbona*, cit. che a p. 431. In dottrina invero, non c'è, pacifica convergenza sul punto, e accanto a letture personaliste come quella indicata si collocano piuttosto indirizzi che, pur anche essi orientati verso lo scopo di massimizzare la tutela della persona, suggeriscono di accettare il “dato di realtà” che vorrebbe i dati personali sempre più provvisti di valore economico e negoziale (ad es. come controprestazione nei c.d. *tying arrangements*), oggetto pertanto di un processo di c.d. *commodification*. Cfr. ad es. S. SICA, V. D'ANTONIO, «La commodification dei dati personali nella data driven society», in P. Stanzone (a cura di), *I poteri privati delle piattaforme e le nuove frontiere della privacy*, cit., p. 129 ss.; V. RICCIUTO, «Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali», in *Riv. dir. civ.*, 2020, 3, p. 642 ss. V. amplius cap. 3.

³³⁰ Cfr. Dir. 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche

emendamento, di integrazione e di razionalizzazione della disciplina del trattamento dei dati personali, introdotta attraverso l'attuazione dei diversi strumenti comunitari intervenuti in materia, adottando il decreto legislativo n. 196/2003, denominato «Codice della Privacy»³³¹. Al momento della sua adozione, tale testo unico, come è stato notato, si caratterizza per la vocazione a predisporre un generale ordinamento della protezione dei dati personali in Italia, animato pertanto dalla pretesa di disciplinare in modo organico tutti gli aspetti, sostanziali così come istituzionali, della materia rappresentata dalla protezione, e contestualmente dal trattamento, dei dati personali³³². E tutt'ora, sebbene ampiamente novellato, continua a rappresentare nel nostro sistema il punto di riferimento (quasi un *corpus* normativo in sé conchiuso) in materia di *privacy* e di protezione dei dati personali, per i profili in cui le disposizioni del GDPR risultino “incomplete” e pertanto bisognose di implementazione, nonché di adeguamento del diritto interno³³³.

Ma ai fini del nostro discorso la funzione più importante del d.lgs. n. 196/2003 è quella di introdurre e di sancire *a livello positivo* una situazione giuridica a protezione di quella dimensione positiva e dinamica della *privacy* già avvertita dalla dottrina, ma ancora priva di autonoma concettualizzazione nel nostro ordinamento: l'art. 1 stabilisce infatti a chiare lettere «*chiunque ha diritto alla protezione dei dati personali che lo riguardano*»; e l'art. 2 amplia le finalità

³³¹ Cfr. D.lgs. 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali»; oggi, ampiamente novellato da D.lgs. 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)».

³³² Cfr. S. CALZOLAIO, «Protezione dei dati personali», cit., p. 615; L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 46; tra i numerosi commenti alla disciplina ivi contenuta, e alla sua vocazione «ordinamentale», cfr. ad es. CUFFARO, D'ORAZIO, RICCIUTO, *Il codice del trattamento dei dati personali*, Torino, 2007.

³³³ V. più approfonditamente nel cap. 3.

del codice alla garanzia «che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della *dignità* dell'interessato, con particolare riferimento *alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*».

Perciò l'entrata in vigore del codice formalizza anche nel nostro ordinamento, e definitivamente, l'esistenza di un diritto alla protezione dei dati personali, come diritto insistente su un bene *concettualmente e giuridicamente distinto* dalla riservatezza e dall'identità personale, a loro volta oggetto di autonomi diritti soggettivi. Allo stesso tempo, il codice ne individua comunque un certo carattere di strumentalità, o piuttosto di *indefettibilità*, rispetto alla tutela di altri diritti fondamentali, compresi questi ultimi: a sottolineare, sembra, che il controllo sulle proprie informazioni costituisca il presupposto essenziale per la libera *costruzione* della propria sfera privata e, al contempo, della stessa libertà di scegliere *come e cosa* proiettare di sé all'esterno, e dunque della libertà di determinazione *delle* proprie identità.

Non è questa la sede per analizzare gli ulteriori aspetti fondamentali della disciplina a suo tempo introdotta dal Codice. Ai nostri fini, è sufficiente concludere affermando che, a seguito dell'entrata in vigore della Carta di Nizza, del Codice della Privacy e del Trattato di Lisbona, nella dottrina e nella giurisprudenza italiana sia ormai pacifica la prospettiva (la si riepiloga) che distingue chiaramente il diritto alla riservatezza, come libertà negativa, dal diritto alla protezione dei dati personali, come libertà positiva di autodeterminazione informativa, e dunque di controllare (attraverso la possibilità di accesso, di rettifica, di integrazione ecc.) il flusso di informazioni «in entrata e in uscita»

riguardanti la propria persona³³⁴. Il primo, così come il secondo, così come il diritto all'integrità della propria «proiezione sociale» (c.d. diritto all'identità personale), da intendersi tutti come profili, talvolta complementari, talvolta, inevitabilmente, sovrapposti tra loro, dell'unico, proteiforme «prisma» rappresentato dalla persona umana³³⁵.

2.2.4. L'approdo: il ruolo della Corte di Giustizia come «giudice dei diritti fondamentali», il Pacchetto Protezione Dati e l'EU-U.S. Data Privacy Framework

Concludiamo la nostra analisi, da una prospettiva diacronica, del quadro giuridico europeo in materia di *privacy* e di *data protection* affrontando brevemente le vicende successive al processo di costituzionalizzazione comunitaria del diritto alla protezione dei dati personali appena descritto: in particolare, gettiamo un primo sguardo riassuntivo ai risultati dell'Agenda Digitale Europea 2010-2020, che ha visto l'approvazione del c.d. Pacchetto Protezione Dati³³⁶.

³³⁴ Cfr., ancora e su tutti, G. FINOCCHIARO, «Identità personale (diritto alla)» cit; L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 15; S. CALZOLAIO, «Protezione dei dati personali», cit., p. 614.

³³⁵ Le eleganti espressioni sono di G. FINOCCHIARO G., «Identità personale (diritto alla)», cit., p. 723.

³³⁶ Cfr. da subito RATCLIFF, WOSYKA, MARTINELLO, FRANCO, «L'Agenda Digitale Europea», in Note Tematiche sull'Unione Europea, 2023, <https://www.europarl.europa.eu/factsheets/it/sheet/64/un-agenda-digitale-europea>; sul «Pacchetto Protezione Dati», su cui si tornerà, v. a titolo riassuntivo il documento del Servizio Studi Giustizia della Camera dei Deputati, consultabile sul sito ufficiale alla sezione Aree Tematiche: https://temi.camera.it/leg18/temi/la_protezione_dei_dati_personali.html

Prima, tuttavia, è indispensabile sottolineare il ruolo svolto dalla CGUE nell'affermazione del diritto alla protezione dei dati personali, sancito a partire dalla dir. 95/46, nella comune sensibilità degli ordinamenti giuridici nazionali; nonché dell'esigenza, solo recentemente soddisfatta, di adeguare la disciplina vigente in materia di *data protection* alle trasformazioni intervenute nel contesto sociale e tecnologico di riferimento.

Se nelle prime decisioni successive all'adozione della Carta di Nizza, stante il suo dichiarato valore giuridico non vincolante, la Corte appare trascurare il "sistema" configurato dagli art. 7 e 8, focalizzando l'attenzione sull'esigenza di mantenere un equilibrio fra la libera circolazione dei dati personali e la tutela della vita privata, già sul finire degli anni Dieci essa comincia a mutare indirizzo³³⁷.

Per citare il più noto esempio, nella sentenza *Promusicae* del 2008 la Corte comincia a valorizzare, come prioritaria finalità al cui perseguimento risulti vincolata la disciplina del trattamento dei dati personali, la tutela della persona e dei suoi diritti fondamentali, sebbene in tal caso in un'ottica del bilanciamento tra *privacy* e proprietà intellettuale: in un passaggio della sentenza, richiamando i due articoli suddetti, essa espressamente osserva che l'«art. 8 della Carta proclama espressamente il diritto alla tutela dei dati personali»³³⁸.

Un vero passo decisivo viene però dalla Corte effettivamente compiuto poco dopo l'entrata in vigore del Trattato di Lisbona, e tutte le sue ricadute in materia di *privacy* nel paragrafo precedente analizzate. La CGUE, infatti, nella

³³⁷ Cfr. ad es., per tale prima fase, C. Giust. UE, 20-5-2003, C-465/00, C-138/01 e C-139/01, *Rechnungshof*

³³⁸ Cfr. C. Giust. UE, 29-1-2008, C-275/06, *Promusicae*, in part. par. 64. Il caso, in sintesi, aveva ad oggetto l'interpretazione del diritto comunitario in punto di sussistenza o meno dell'obbligo in capo ai fornitori di «servizi della Società dell'Informazione» di comunicare dati personali di soggetti ritenuti condividere in modo illecito in rete contenuti coperti dal diritto d'autore. Per un'analisi, cfr. A. Del Ninno, «Il caso *Promusicae-Telefonica*: la Corte di Giustizia UE si pronuncia sul rapporto tra tutela della *privacy* e protezione del copyright nell'ordinamento comunitario», in *Diritto e Giustizia*, 2012, <https://www.alessandrodelninno.it/upload/articoli/documenti/00000022.pdf>.

sentenza *Schecke* del 2010, delinea più approfonditamente i caratteri del diritto alla protezione dei dati personali, di cui, in virtù del valore giuridico acquisito della Carta di Nizza, grazie all'art. 6 del TUE, individua la fonte *direttamente* nella medesima, affermando recisamente che «le limitazioni che [alla luce dell'art. 52, commi 1 e 3] possono essere legittimamente apportate [al diritto in questione] corrispondono a quelle tollerate nell'ambito dell'art. 8 della CEDU»³³⁹. I giudici di Lussemburgo, in forza dell'entrata in vigore dei “nuovi” Trattati, mostrano di poter *rileggere* la disciplina introdotta alla dir. 95/46 e dagli altri strumenti normativi in materia alla luce del diritto fondamentale sancito dall'ormai *precettivo* art. 8 della Carta dei diritti fondamentali dell'Unione: in tal modo, cominciando ad elevare la tutela della persona nel trattamento dei dati da *strumento* per la costruzione del Mercato Interno a *valore in sé*, e dunque fine stesso della disciplina³⁴⁰.

Ed è proprio su tale base che la Corte procede negli anni successivi, come vedremo, a sviluppare la sua giurisprudenza sulla qualificazione e sul potenziamento del diritto fondamentale alla protezione dei dati personali: specialmente, lo sottolineiamo, al fine di reagire alla vertiginosa espansione della “società dell'informazione” in “società digitale”.

Per cogliere tuttavia ulteriormente il fondamento concettuale delle decisioni che nel biennio 2014-2015 promuoveranno il profondo aggiornamento della disciplina positivo del trattamento dei dati personali, occorre porre in evidenza due altri principi ribaditi costantemente dalla Corte. In primo luogo, ci

³³⁹ Cfr. C. Giust. UE, 9-11-2010, C-92/09 e C-93/09, *Volker und Markus Schecke GbR*, in part. par. 45-52; merita sottolineare come tale sentenza esprima buona parte dei concetti successivamente sviluppati dalla Corte in punto di estensione e di limiti al diritto *fondamentale* alla protezione dei dati personali: oltre a quanto detto, e alla stretta connessione individuata tra protezione dati e tutela della vita privata, bisogna ricordare l'insistenza sul concetto di «*funzione sociale*» riconosciuta al diritto medesimo.

³⁴⁰ Cfr. S. CALZOLAIO, «Protezione dei dati personali», cit., p. 622; POLLICINO, BASSINI, sub «art. 8», in *Carta dei diritti fondamentali dell'Unione europea*, cit., p.141.

si riferisce alla *dimensione* e insieme alla *funzione sociale* che la stessa riconosce con forza al diritto alla protezione dei dati personali, sottolineando come, alla luce degli art. 8 par. 3 della Carta e 16 comma 2 del TFUE, l'esistenza di una autorità nazionale di controllo indipendente costituisca «un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali»³⁴¹. In secondo luogo, e forse soprattutto, la Corte insiste frequentemente sul nesso di strumentalità che intercorre tra diritto alla protezione dei dati personali e diritto al rispetto della vita privata (e pertanto, nel suo alveo, alla riservatezza): per fare solo un esempio, in una capitale sentenza come *Digital Rights Ireland*, essa afferma come al fine di valutare la legittimità di una deroga (entro i limiti dello stretto necessario consentiti dall'art. 52 della Carta) alla disciplina della protezione dei dati personali in sé considerata, sia necessario analizzarne le ricadute sull'altro diritto in questione, poiché «occorre ricordare che la tutela dei dati personali (...) riveste un'importanza particolare per il diritto al rispetto della vita privata»³⁴². Con ciò, individuando il primo diritto quale sostanziale *arricchimento* del secondo, entrambi a presidio di beni giuridici spesso potenzialmente sovrapponibili, ma non coincidenti.

La Corte, insomma, appare ben conscia di come nell'attuale panorama tecnologico, in cui il dato viene osservato e conseguentemente analizzato dalle macchine, capaci di correlarlo a quantità esorbitanti di altri dati, personali o meno, e di “scoprire” informazioni nuove attraverso processi inferenziali raramente trasparenti, qualsiasi trattamento riguardante le informazioni di una persona fisica

³⁴¹ Cfr. ad es. C. Giust. UE, 9-3-2010, C-518/07, C. Giust. UE, 16-10-2012, C-614/10, *Commissione europea/Germania*, par. 36

³⁴² Cfr. C. Giust. UE, 8-4-2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*, par. 54, su cui v. *infra*.

possa produrre effetti imprevedibili, e spesso gravi, sulla vita privata della persona stessa³⁴³.

Come abbiamo avuto modo di sottolineare nel precedente capitolo, il nuovo millennio, apertosi con gli attacchi terroristici dell'11 settembre, è presto interessato dalla proliferazione in contesto nordamericano di quella che abbiamo chiamato "legislazione dell'emergenza" in funzione della sicurezza nazionale, con la conseguente sospensione, spesso poco circostanziata, delle garanzie apprestate dall'esegesi giurisprudenziale del *Bill of Rights* alla libertà personale: il *USA Patriot Act* ne rappresenta il più limpido esempio³⁴⁴. La marea "reazionaria" investe, lo abbiamo accennato, anche l'Europa, che nell'adozione dell'importante Direttiva 2002/58/CE (dir. *E-Privacy*), accanto alle prescrizioni in punto di sicurezza dei servizi di comunicazione elettronica e di disciplina di *cookies* e *spam*, introduce determinate ipotesi di restrizione alla riservatezza, e in particolare la legittimazione degli Stati membri a predisporre misure legislative che ai fini della sicurezza nazionale o di altri interessi pubblici tassativamente previsti consentano la conservazione dei dati relativi alle comunicazioni medesime per un generico «periodo di tempo limitato» (c.d. *data retention*)³⁴⁵.

³⁴³ Sui temi profondamenti attuali delle inferenze algoritmiche e del correlato fenomeno della c.d. *black box*, nel contesto dei *Big Data analytics* e del *data mining*, ci si soffermerà nel prossimo paragrafo, dedicato ai connotati essenziali dell'attuale contesto tecnologico e della c.d. *data driven society*. Nel frattempo, però, si può già fare riferimento a L. FLORIDI, *The Fourth Revolution: How Infosphere is Reshaping Human Reality*, Oxford University Press, 2014; R. ANGELINI, «Intelligenza artificiale e governance. Alcune riflessioni di sistema», in *Intelligenza artificiale, protezione dei dati personali e regolazione*, F. Pizzetti (a cura di), Torino, 2018, 295; e la fondamentale riflessione di F. PASQUALE, *The black-box society. The secret Algorithms that control money and information*, cit.

³⁴⁴ V. *retro*, par. 1.1.7.

³⁴⁵ Cfr. in part. art. 15 Dir., 2002/58/CE, in forza del quale «Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica; e la prevenzione, ricerca,

Tale approccio è ulteriormente inasprito in seguito agli attacchi di Madrid dell'11 marzo 2004 e di Londra del 7 luglio 2005, entrambi rivendicati dall'organizzazione terroristica di Al-Quaeda: la risposta è la c.d. *Data Retention Directive*, che, emendando la dir. E-Privacy, impone agli Stati membri di implementare norme che obblighino i *service providers* alla conservazione dei dati sulle telecomunicazioni dei cittadini da un minimo di sei mesi fino a un massimo di ventiquattro, consentendo alla polizia e alle agenzie di sicurezza di richiedere l'accesso a dettagli come indirizzo IP e tempo di utilizzo di e-mail, chiamate telefoniche e SMS inviati o ricevuti, seppur dietro legale autorizzazione dell'Autorità giudiziaria³⁴⁶.

Le critiche che le associazioni sui diritti civili e parte della stampa rivolgono in special modo a quest'ultimo strumento normativo si innestano sulle preoccupazioni scaturite dalle rivelazioni, di cui abbiamo parlato, relative ai programmi di sorveglianza di massa implementati dalle amministrazioni statunitensi, in aperta elusione del *Privacy Act*: prima *Carnivore*; poi il c.d. programma *M.A.T.R.I.X*; poi ancora le violazioni alla *privacy* individuale intervenute nel contesto del *Security Fly Program*.

Ma la “goccia che fa (certamente) traboccare il vaso”, e che schiude agli occhi di istituzioni ed opinione pubblica la vulnerabilità dei presidi giuridicamente (e, prima ancora, socialmente) esistenti all'integrità della propria

accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i *dati siano conservati* per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo.

³⁴⁶ Cfr. la ormai annullata Dir.2006/24/CE del Parlamento Europeo e del Consiglio riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE; in particolare, cfr. in particolare art. 3, rubricato «Obbligo di conservazione dei dati», l'art. 4 sull'«accesso ai dati», l'art. 5 sulle «categorie di dati da conservare», l'art. 6 che disciplina i «periodi di conservazione», e l'art. 11, che limita l'applicabilità dell'15 della dir. 2002/58/CE, che prevede limitazioni al diritto alla protezione dei dati personali più tenui, ai casi ricadenti nel perimetro applicativo della presente direttiva.

sfera privata di fronte alla potenza degli algoritmi è lo scandalo *Datagate*, di cui abbiamo precedentemente abbozzato un ritratto: le vere e proprie confessioni di Edward Snowden hanno un respiro che trascende i confini nazionali, e profila l'inquietante scenario della *sorveglianza globale*, che programmi e, più in generale, mezzi cibernetici come *PRISM* renderebbero già, in larga misura, concretizzato³⁴⁷.

Probabilmente, allora, è proprio per far fronte a questo scenario critico e strutturalmente minaccioso per l'integrità del diritto alla vita privata e di quello complementare alla protezione dei dati personali che la Corte di Giustizia decide di intervenire con forza ancora maggiore, adottando, nel biennio 2014-2015, una serie di sentenze che consacrano il principio della rilettura di tutta la disciplina vigente in materia di *privacy*, tanto generale (al tempo, la dir. 95/46) quanto settoriale (al tempo, la dir. *e-privacy* e la dir. *data retention*) alla luce degli art. 7 e 8 della Carta di Nizza e dell'art. 16 del TFUE. Rilettura che deriva dall'individuazione di queste ultime disposizioni quale fondamento primario, gerarchicamente sovraordinato al diritto comunitario derivato, di diritti fondamentali suscettibili di compressione solo negli stretti limiti previsti dal "principio di proporzionalità" codificato dall'art. 52 della Carta, modellato sulla

³⁴⁷ V. retro, par. 1.1.7. Appare qui utile aggiungere che *PRISM* raccoglieva i dati relativi a *stored internet communications* attraverso la collaborazione con i principali service providers, tra cui Google, Yahoo e Facebook, principalmente sulla base della Sezione 702 del FISA Amendments Act del 2008, tutt'ora in vigore, che in quel momento ampliava considerevolmente le ipotesi di *warrantless wiretapping* consentite dal FISA: essa, infatti, in sintesi consentiva e tutt'ora consente all'NSA, su autorizzazione dell'*Attorney General* o del *Director of National Intelligence*, a « *targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information*»; e ciò, pertanto, attraverso l'intercettazione del *contenuto* di email, telefonate e messaggi istantanei. V. H.R. 6304, § 702(a) ss. Cfr. sul tema ad es. BARTON GELLMAN & ASHKAN SOLTANI, «NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say», in *The Washington Post*, 30 ottobre 2013.

stregua dell'art. 51 della CEDU³⁴⁸. Una rilettura che potrebbe dunque definirsi costituzionalmente orientata, stante la matrice evidentemente costituzionale degli articoli della Carta; o, piuttosto, *human rights oriented*; e che, in generale, si iscrive in quel fenomeno da alcuni efficacemente definito come «transizione dall'Europa dei Mercati all'Europa dei Diritti»³⁴⁹.

La prima sentenza cui ci riferiamo, in ordine cronologico, è la già citata *Digital Rights Ireland*, dell'8 aprile 2014: in essa la Corte, facendo applicazione congiunta degli artt. 7, 8, e 52 della Carta di Nizza, dichiara invalida la Direttiva 2006/24/CE sulla conservazione dei dati (c.d. *data retention*), a seguito di rinvio pregiudiziale presentato sia dalla *High Court* irlandese che dalla *Verfassungsgerichtshof* (Corte costituzionale) austriaca in merito proprio alla validità di tale direttiva: e ciò perché il periodo di conservazione di dati previsto per fini di protezione dell'ordine pubblico veniva considerato eccessivo e non proporzionato, e pertanto lesivo del contenuto essenziale del diritto alla vita privata e di quello complementare alla protezione dei dati personali³⁵⁰. L'orientamento in questione, merita sottolinearlo, è stato poi successivamente ribadito nella sentenza *Tele2 Sverige AB* del 2016 con riferimento alle normative

³⁴⁸ Cfr. O. POLLICINO, M. BASSINI, «La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo», in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, 73 ss.; S. CALZOLAIO, «Protezione dei dati personali», 621 ss.

³⁴⁹ L'espressione è di O. POLLICINO, M. BASSINI, «La Corte di Giustizia e una trama ormai nota: la sentenza *Tele2Sverige* sulla conservazione dei dati di traffico per finalità di sicurezza e di ordine pubblico», in *Dir. Pen. Cont.*, 2017, https://archiviodpc.dirittopenaleuomo.org/upload/POLLICINOBASSINI_2017a.pdf. Cfr. anche le riflessioni di G. PITRUZZELLA, «L'Europa del mercato e l'Europa dei diritti», in *federalismi.it*, n.6/2019, consultabile qui: <https://www.sipotra.it/wp-content/uploads/2019/03/L'Europa-del-mercato-e-l'Europa-dei-diritti.pdf>.

³⁵⁰ C. Giust. UE, 8-4-2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd.* Per un commento più approfondito della sentenza, cfr. ex multis L. TRUCCO, «Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali», in *Giur. it.*, 2014, 8-9, 1850 ss.

nazionali preordinate allo stesso fine e fondate sull'art. 15 della dir. E-Privacy: sentenza che ha promosso un'interpretazione restrittiva del medesimo in quanto derogatorio al regime ordinario di *privacy and data protection*, e dunque una complessiva interpretazione della direttiva chiaramente "illuminata" dai suddetti diritti fondamentali sanciti dagli art. 7 e 8 della Carta, stabilendo come lo stesso articolo ostasse ad una normativa nazionale «la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati (...) relativi a tutte le comunicazioni elettroniche»³⁵¹.

La seconda, di importanza altrettanto capitale nel percorso qui tracciato, è la sentenza *Google Spain*, apparsa pochi mesi dopo la decisione appena richiamata e rimasta famosa perché dal dispositivo della medesima parte della dottrina ha desunto il riconoscimento giurisprudenziale, nel quadro del sistema di *data protection* europeo, di un «diritto all'oblio»³⁵². In sintesi, nella sentenza in questione la Corte, applicando evolutivamente la dir. 95/46 alla luce dei diritti di cui agli artt. 7 e 8 della Carta, ha affermato un diritto alla deindicizzazione dei dati personali, riconoscendo che il motore di ricerca è responsabile del trattamento dei dati, individuando in Google Spain uno stabilimento del responsabile Google Inc. e identificandolo, in quanto tale, come destinatario dell'obbligo a sopprimere «dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona»³⁵³.

³⁵¹ C. Giust. UE, 21-12-2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*. Per un commento più approfondito, si rinvia al già citato POLLICINO, BASSINI, «La Corte di Giustizia e una trama ormai nota», cit.

³⁵² C. Giust. UE, 13-5-2014, causa C-131/12, *Google Spain SL*.

³⁵³ Cfr. C. Giust. UE, 13-5-2014, causa C-131/12, *Google Spain SL*., rispettivamente par. 32-41 e par. 88, in cui peraltro la Corte aggiunge che l'obbligo di de-indicizzazione sussiste anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita».

La terza sentenza, forse quella che più interessa ai fini del nostro lavoro, è quella del 6 ottobre 2015, nella causa *Schrems v. Data Protection Officer*, c.d. sentenza *Schrems I*, con cui la Corte ha invalidato la decisione della Commissione 2000/520, adottata ex art. 25 par. 6, della dir. 95/46/CE che dichiarava l'adeguatezza del livello di protezione offerto ai dati personali, oggetto di trasferimenti dal territorio dell'Unione europea agli Stati Uniti, dai c.d. *Safe Harbor Privacy Principles*, e relative FAQ, adottati dal *Department of Commerce* statunitense³⁵⁴. Nel merito del *Sistema Safe Harbor*, ai limitati fini della nostra trattazione (e specialmente per sottolineare la sostanziale indifferenza di tali principi alla predisposizione di un'apposita, rafforzata disciplina in punto di trattamenti *interamente* automatizzati), entreremo nei prossimi capitoli, ma intanto appare opportuno delineare un poco di contesto.

Se già la Commissione europea aveva avuto modo di criticare il sistema scaturito dall'accordo *Safe Harbor*, evidenziando in una prima relazione come molte delle imprese iscritte nella lista dei soggetti aderenti ai principi medesimi, ossia delle c.d. *harborities*, non garantissero la trasparenza delle proprie *privacy policies*, e come queste ultime spesso non rispecchiassero nemmeno i principi *Safe Harbor* (soprattutto sotto il profilo *Notice, Choice and Access*)³⁵⁵, dalle rivelazione di Snowden si era potuto evincere che tutte le imprese soggette al

³⁵⁴ Cfr. C. Giust. UE, C-362/14, *Maximilian Schrems/Data Protection Commissioner*, 6 ottobre 2015, ECLI:EU:C:2015:650. Per un approfondito commento della sentenza e una descrizione dettagliata del Sistema *Safe Harbor*, cfr. G. SCARCHILLO, «Dal *Safe Harbor* al *Privacy Shield*. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza *Schrems*», in *Diritto del Commercio Internazionale*, Anno XXX, Fasc. 4, 2016, p. 901 ss.

³⁵⁵ Cfr. COMMISSIONE EUROPEA, *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, Commission Staff Working Document, SEC(2002) 196, 13 febbraio 2002, http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf.

programma di sorveglianza *PRISM* rientrassero nella lista delle *harborities*: pertanto, era altamente probabile che oggetto di interferenza fossero anche i dati trasferiti dal continente europeo sotto la vigenza dell'accordo Usa-Ue. Su tali basi, lo studente austriaco Maximilian Schrems denunciava davanti all'Autorità Garante della Privacy irlandese la violazione dei diritti fondamentali garantiti dagli art. 7 e 8 della Carta di Nizza a seguito del trasferimento dei propri dati dalla controllata europea Facebook Ireland alla *holding* Facebook Inc., con sede negli Stati Uniti, ritenendo possibile l'indebito accesso ai medesimo da parte delle agenzie federali statunitensi³⁵⁶. Rigettato il ricorso dal Garante irlandese, la *High Court* irlandese, investita del gravame, sospendeva il procedimento sollevando rinvio pregiudiziale ex art. 267 del TFUE, che la CGUE interpretava come inerente alla validità della decisione suddetta³⁵⁷.

Ebbene in sintesi la Corte, aderendo all'interpretazione dell'inciso «livello di protezione adeguato», preteso dallo Stato terzo di destinazione dei dati (nel caso di specie, dunque, gli USA) e contenuto nell'art. 25 della direttiva, in termini di livello «sostanzialmente equivalente», riteneva insoddisfatto tale requisito nell'ordinamento statunitense: e ciò perché, se i diritti fondamentali di cui agli art. 7 e 8 della Carta risultano suscettibili di deroga solo, alla luce dell'art. 52 par.1, nella misura in cui questa sia necessaria e proporzionata, le norme dell'ordinamento statunitense applicabili in materia alla luce dell'accordo intercorso con la Commissione avrebbero contravvenuto a tale principio: tali norme, infatti, consentivano ampiamente alle autorità statunitensi per *ragioni di sicurezza nazionale* di ingerirsi nel trattamento dei dati trasferiti dall'UE alle imprese aderenti ai *Safe Harbor Principles*³⁵⁸. Per questo motivo, come abbiamo

³⁵⁶ C. Giust. UE, C-362/14, *Maximilian Schrems/Data Protection Commissioner*, cit., par. 28

³⁵⁷ *Ivi*, par. 36 ss.

³⁵⁸ *Ivi*, par. 86 ss. La Corte arriva a desumere, in poche parole, come negli Stati Uniti le esigenze di sicurezza nazionale fossero prioritarie rispetto alla tutela del diritto alla protezione

detto, la Corte invalida l'intera decisione di adeguatezza della Commissione, e conseguentemente determina la fine dell'accordo *Safe Harbor*³⁵⁹.

Ora, le sentenze che abbiamo qui brevemente esaminato sono ai nostri fini importanti per due motivi principali.

Innanzitutto esse, come è stato brillantemente notato, colgono «la tutela del diritto fondamentale alla protezione dei dati personali nella sua implicazione rispetto alla architettura della rete internet»³⁶⁰: dalle sentenze traspare infatti la consapevolezza della Corte di come, ai fini della effettiva tutela della sfera privata della persona umana, la regolazione della protezione dei dati non possa prescindere dal considerare il rapporto tra gli ordinamenti sistematicamente interessati da incessanti *transborder flows* di “bit informativi”, e allo stesso tempo l'economia dell'infrastruttura – a cominciare dai dispositivi elettronici - che ospita e condiziona il trattamento dei medesimi (esigenza, questa, cui tentano di rispondere i principi di *privacy by design* e di *privacy by default* introdotti dal GDPR).

Allo stesso tempo, la giurisprudenza in questione ha dato notevole, determinate impulso all'attuazione del c.d. Pacchetto Protezione Dati: un insieme di misure, iscritte nella più generale Agenda Digitale Europea, elaborate in seno alla Commissione in sinergia con le altre istituzioni europee al fine, tra i vari obiettivi, di armonizzare ulteriormente e di unificare *a livello generale* la disciplina delle diverse articolazioni applicative del diritto alla protezione dei dati personali in tutti gli Stati membri dell'Unione europea³⁶¹.

dei dati personali: assetto di interessi non conforme, pertanto, al sistema onnicomprensivo di *data protection* previsto in europa, imperniato come abbiamo visto sui diritti fondamentali alla riservatezza e alla protezione dei dati personali.

³⁵⁹ Ivi, par. 105-106.

³⁶⁰ La citazione è di S. CALZOLAIO, Protezione dei dati personali, cit., p. 622.

³⁶¹ Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo, al Consiglio delle Regioni*.

Dell'Agenda, così come dei principali atti normativi implementati sulla sua base (sulla base di tale strategia), si parlerà a titolo introduttivo nel prossimo capitolo. Qui ci si può limitare a riepilogare sinteticamente i più importanti tra questi.

Al vertice della piramide si colloca sicuramente il Regolamento 2016/679/UE relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la dir. 95/46/CE, abbreviato nella versione inglese GDPR (*General Data Protection Regulation*) e nella versione italiana RGDP (Regolamento Generale sulla Protezione dei Dati), che consolida a livello positivo un largo numero di principi sanciti dalla giurisprudenza della Corte di Giustizia nei vent'anni successivi all'entrata in vigore della direttiva³⁶². Adottato espressamente sulle basi giuridiche rappresentate dall'art. 8 della Carta e dall'art. 16 TFUE, esso, come emerge chiaramente dai considerando, ha lo scopo precipuo di favorire la costruzione di un Mercato Unico Digitale *fondato* sul valore della persona umana, contrastando la frammentazione della disciplina della protezione dei dati personali sul territorio dell'Unione Europea attraverso l'uniformazione del diritto vigente in materia, in quanto strumento direttamente applicabile in tutti gli Stati

Un'agenda digitale europea, COM(2010)245 definitivo, Bruxelles 19 maggio 2010, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52010DC0245>. Cfr. anche il quadro sintetico tracciato da C. RATCLIFF, M. WOSKYA, B. MARTINELLO, D. FRANCO, «L'Agenda Digitale Europea», in *Note Tematiche sull'Unione Europea*, <https://www.europarl.europa.eu/factsheets/it/sheet/64/un-agenda-digitale-europea>, 2023, documento istituzionale che in apertura specifica: «Lanciata nel 2010 per un periodo di 10 anni, l'agenda digitale europea, che fa seguito alla strategia di Lisbona, ha stabilito per la prima volta il ruolo chiave delle TIC per il conseguimento degli obiettivi che l'Europa si è prefissata. Nel 2015 la strategia per il mercato unico digitale ha ulteriormente sviluppato l'agenda digitale, stabilendo disposizioni specifiche basate su tre pilastri volti a garantire un ambiente digitale equo, aperto e sicuro (...)»

³⁶² V. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

membri ai sensi dell'art. 288 TFUE³⁶³. Pertanto, può dirsi che il Regolamento attualmente rappresenta la fonte unitaria della disciplina generale della protezione delle persone fisiche nel trattamento dei dati personali nell'intero contesto ordinamentale dell'Unione europea³⁶⁴.

Sempre il 4 maggio 2016, assieme al GDPR, è stato pubblicato in Gazzetta Ufficiale il testo della Direttiva 2016/680/UE, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Essa, rispetto al GDPR, e al pari ad esempio della (fino ad ora) sopravvissuta dir. 2002/58/CE, rappresenta ovviamente un atto normativo speciale, e in quanto direttiva è un atto di armonizzazione, poiché ai fini della sua applicabilità necessita di essere trasposta dagli Stati nei rispettivi ordinamenti attraverso apposita normativa di attuazione.

Entrato in vigore il 24 maggio 2016, il GDPR è divenuto definitivamente applicabile a partire dal 25 maggio 2018, mentre la Direttiva 2016/680 è entrata in vigore il 5 maggio 2016.

Al di fuori del «pacchetto», merita menzionare il Regolamento 910/2014 UE del Parlamento europeo e del Consiglio del 23 luglio 2014, «in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel

³⁶³ Ivi, in part. cons. nn. 1-15. Molto rilevante l'inciso con cui si apre il cons. n. 4 «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo»; ed anche, ai nostri fini, l'incipit del n. 15 «Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere *neutrale sotto il profilo tecnologico* e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali (...)»

³⁶⁴ Cfr. già per tali rilievi ad es. i commenti di G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati», cit.; E. L. GUASTALLA, «Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori», in *Contr. e Impr.*, 1/2018; M.G. STANZIONE, «Il regolamento europeo sulla privacy: origini e ambito di applicazione», in *Eur. dir. priv.*, 2016, p. 1249 ss

mercato interno e che abroga la direttiva 1999/93/ CE” (c.d. reg *eIDAS*)³⁶⁵, e più di recente il Regolamento (UE) 2018/1807 avente ad oggetto la “generale” categoria dei dati *non* personali.

Altrettanto importante, perché la loro applicazione si intreccia profondamente e non pacificamente a quella del GDPR, sono la Direttiva UE 2019/770 relativa ad alcuni aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. E, ancor più di recente, bisogna citare i due atti normativi deputati a “responsabilizzare”, indipendentemente dallo specifico settore di riferimento, le *piattaforme digitali*, graduandone gli obblighi in ragione della dimensione e del numero degli utenti attivi: stiamo parlando del *Digital Services Act* e del *Digital Markets Act*.

Chiudiamo la carrellata ricordando nel gennaio del 2017 la Commissione europea ha avviato la revisione della disciplina in materia di tutela della riservatezza delle comunicazioni elettroniche, per allinearla agli standard di protezione stabiliti nel Pacchetto Protezione Dati e al contempo aggiornarla alla continua evoluzione delle tecnologie in materia di comunicazione e informazione. Essa è culminata nella presentazione di una proposta di regolamento, COM(2017)10, diretto a sostituire l’ancora vigente dir. 2002/58/CE c.d. *E-Privacy*. La proposta di Regolamento c.d. *E-Privacy* è attualmente in discussione al Parlamento Europeo.

Al fine di concludere il corposo affresco delineato, si intende fare cenno al “momentaneamente definitivo” approdo della giurisprudenza eurounitaria in materia di protezione dei dati personali: il percorso culminato nelle pronunce particolarmente “garantiste” del biennio 2014-2015, accanto alle decisioni che ne hanno consolidato gli orientamenti, si è infatti arricchito dell’ulteriore

³⁶⁵ Il Regolamento è, in sigla, comunemente denominato “eIDAS” perché “e” sta per “electronic”, “ID” per “identification”, “A” per “authentication” e “S” per “signature”.

fondamentale sentenza c.d. *Schrems II*, con cui la Corte ha dichiarato invalida la Decisione 2016/1250 della Commissione, fondata anch'essa sull'art. 25 dir. 95/46/CE sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la *privacy* (c.d. *Privacy Shield*)³⁶⁶.

Per comprenderne il dispositivo, occorre “riavvolgere il nastro” ai giorni successivi alla decisione *Schrems I*, con cui la Corte fondamentalmente smantellava la base giuridica su cui si fondava la liceità del trattamento dei dati “europei” nel porto, giudicato *in-sicuro*, statunitense. Già il 29 febbraio 2016 la Commissione, in un suo comunicato stampa, aveva annunciato di aver finalizzato il testo di quel che è divenuto l'attuale *General Data Protection Regulation* (a dimostrazione ancora una volta della forza propulsiva della sentenza di cui sopra)³⁶⁷; e al contempo di aver negoziato con gli USA tanto un accordo sulla protezione dei dati in ambito penale (c.d. *E.U.- U.S. Data Umbrella Agreement*), quanto, soprattutto, un accordo per i *transborder flows* di dati personali a scopi commerciali che sostituisse gli ormai inefficaci *Safe Harbor Principles*: il c.d. *Privacy Shield*, reso oggetto di apposita decisione di adeguatezza il 12 luglio 2016³⁶⁸. Senza addentrarci nel merito della complessa disciplina, è sufficiente qui dire che, sul piano della tutela dei diritti fondamentali della persona umana e dei meccanismi di ricorso effettivamente previsti a fronte della loro violazione, profilo su cui si concentravano i rilievi critici svolti dalla Corte in *Schrems I*, l'accordo tra le altre novità istituiva il c.d. *Privacy Shield Panel*³⁶⁹ e nell'attribuzione di un concreto ruolo di *law enforcement* alla *Federal Trade*

³⁶⁶ C. Giust UE, C-311/18, *Data Protection Commissioner v. Maximilian Schrems e Facebook Ireland*, 16 luglio 2020.

³⁶⁷ Cfr. COMMISSIONE EUROPEA, «La Commissione europea e gli Stati Uniti concordano un nuovo quadro per i flussi transatlantici di dati: lo scudo UE-USA per la privacy», comunicato stampa del 2 febbraio 2016, IP/16/216, http://europa.eu/rapid/press-release_IP-16-216_i-t.htm.

³⁶⁸ Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (GU 2016, L 207, pag. 1).

³⁶⁹ Ivi, conss. 42 e 56-58.

Commission, legittimata ad intervenire ai sensi della *Section 5* del *Federal Trade Commission Act*³⁷⁰.

Nonostante le virtuose garanzie implementate dal nuovo sistema, il sig. Schrems chiedeva nuovamente all'autorità di controllo irlandese la sospensione o il futuro divieto di trasferimenti dei propri dati dall'UE agli USA, che Facebook effettuava ormai sulla base delle clausole tipo di protezione contenute negli allegati della decisione 2010/87 della Commissione (c.d. clausole contrattuali standard, una tra le diverse e alternative basi giuridiche per il trasferimento transfrontaliero di dati personali contemplate dall'art. 25 della dir. 95/46/CE). Il procedimento interno incardinato dava luogo ad un rinvio pregiudiziale, in cui il giudice a quo in particolare, unitamente alla questione di validità della decisione 2010/87, sollevava anche questione di validità della decisione di adeguatezza dell'accordo *U.S.-E-U Privacy Shield*³⁷¹.

Ebbene, se la Corte, da una parte, dichiara la validità della prima, reputando che in punto di osservanza delle clausole contrattuali standard la stessa predisponga meccanismi efficaci che consentano, in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'Unione, dall'altra essa si convince ancora una volta dell'inadeguatezza del sistema "generale" di protezione previsto dall'accordo USA-UE, anch'esso incentrato sul primato delle esigenze attinenti alla sicurezza nazionale³⁷². In sostanza essa ribadisce la più gran parte dei punti esplicitati nella precedente sentenza, constatando come la normativa interna degli Stati Uniti in materia di accesso e di utilizzo dei dati personali "importati" preveda limitazioni incompatibili con i requisiti oggi previsti dal GDPR, letto alla luce degli art. 7, 8 e 52 della Carta di Nizza, ossia

³⁷⁰ Ivi, cons. 54.

³⁷¹ C. Giust UE, C-311/18, cit., parr. 50-68.

³⁷² Ivi, par. 122-149 su validità decisione 2010/87; parr. 163 ss. su validità decisione 2016/1250.

non necessarie e sproporzionate, giacché i programmi di sorveglianza fondati su suddetta normativa non si limitano a quanto strettamente necessario³⁷³. Ciò conduce inevitabilmente la Corte all'invalidazione della decisione di adeguatezza 2016/1250, e alla conseguente caducazione dell'efficacia del regime dello «scudo per la *privacy*».

Aggiungiamo subito che il vero approdo “momentaneamente definitivo” del nostro percorso risulta l'ulteriore, recentissimo accordo raggiunto dalla Commissione con il governo statunitense, proprio in conseguenza della sentenza *Schrems II*. Con un comunicato stampa del 10 luglio 2023, la Commissione ha annunciato di aver adottato la decisione di adeguatezza di un nuovo accordo negoziato in materia di *transborder flows* di dati personali con gli USA, denominato «quadro UE-USA per la protezione dei dati personali» (c.d. *E.U.-U.S. Data Privacy Framework*)³⁷⁴. Il nuovo accordo e la relativa decisione recepirebbero le preoccupazioni espresse dalla Corte nelle sentenze *Schrems*, implementando ulteriori garanzie quali la limitazione dell'accesso ai dati trasferiti dal territorio dell'Unione da parte dei servizi di intelligence statunitensi a quanto necessario e proporzionato e l'istituzione di un tribunale del riesame in materia di protezione dei dati (*Data Protection Review Court*, DPRC), accessibile ai cittadini dell'UE³⁷⁵.

Le intenzioni delle istituzioni europee risultano chiare dalle dichiarazioni della Presidente Ursula von der Leyen: «Il nuovo quadro UE-USA per la

³⁷³ Ivi, par. 163 ss., in part. par. 171.

³⁷⁴ Cfr. COMMISSIONE EUROPEA, *Protezione dei dati: la Commissione europea adotta una nuova decisione di adeguatezza per la circolazione sicura e affidabile dei flussi di dati UE-USA*, comunicato stampa del 10 luglio 2023, https://ec.europa.eu/commission/presscorner/detail/it/IP_23_3721; cfr. COMMISSIONE EUROPEA, *Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final.

³⁷⁵ Cfr. in part., rispettivamente, conss. 16-28 e 176

protezione dei dati personali garantirà flussi di dati sicuri per i cittadini europei e apporterà certezza giuridica alle imprese su entrambe le sponde dell'Atlantico (...)»³⁷⁶. Solo la prassi svelerà se i risultati corrisponderanno a queste ultime: in ogni caso, torneremo nei prossimi capitoli sul *Data Privacy Framework*, così come sui precedenti accordi negoziati tra USA e UE, per interrogarci sull'esistenza, nel loro quadro, di norme che si occupino strettamente di *automated data processing and decision making*.

Tutta la giurisprudenza che siamo andati ricostruendo dimostra definitivamente il ruolo di “giudice dei diritti fondamentali” assunto dalla Corte di Giustizia dell'UE. Ruolo chiave nella società dei dati “dispersi” nella rete, a maggior ragione a fronte del fenomeno che ci interesserà nello specifico nei prossimi due capitoli: il trattamento automatizzato, ormai algoritmico, dei dati, in cui «scompare la persona del decisore, sostituito appunto da procedure automatizzate, e scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili»³⁷⁷.

Perché il fenomeno dei trattamenti delle informazioni personali «non può essere senza regole» e «il ricorso all'algoritmo non può divenire una forma di deresponsabilizzazione dei soggetti che lo adoperano»³⁷⁸.

Perché la strada per *ri-personalizzare* l'essere umano, irriducibile a qualsiasi classificazione socialmente obbligatoria affidata o meno alle macchine, appare ancora una volta quella dei diritti.

³⁷⁶ Cfr. COMMISSIONE EUROPEA, «Protezione dei dati: la Commissione europea adotta una nuova decisione di adeguatezza per la circolazione sicura e affidabile dei flussi di dati UE-USA», cit.

³⁷⁷ S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 401

³⁷⁸ Ivi, p. 403.

2.3. *Big Data*, trattamenti algoritmici e Intelligenza Artificiale: alcuni concetti fondamentali nel contesto tecnologico della *data driven society*

Prima di addentrarci definitivamente nell'analisi della disciplina dei trattamenti automatizzati, è opportuno completare la definizione della presente cornice introduttiva offrendo alcune importanti indicazioni sull'evoluzione del contesto tecnologico di riferimento. Tale contesto rappresenta infatti il presupposto “naturalistico” e allo stesso tempo il referente oggettivo della disciplina che andremo ad analizzare nel dettaglio. Come già più volte sottolineato, se la tecnologia si modella intorno ai bisogni dell'uomo, al contempo il contesto giuridico in cui siamo immersi “rispecchia” e tenta di governare i conflitti che il progresso medesimo ingenera nella società. Per comprendere quest'ultimo, è fondamentale conoscere il primo, e sapersi orientare nel suo ambito: una “bussola concettuale” può, a tal scopo, essere utile.

Il famoso, già citato report del 1973 del *Secretary's Advisory Committee on Automated Personal Data Systems*, si apriva con alcune considerazioni di stupefacente lungimiranza e attualità³⁷⁹. Si legge infatti nella prefazione, con riferimento ai nuovi mezzi di elaborazione elettronica delle informazioni: «*Computers linked together through high-speed telecommunications networks are destined to become the principal medium for making, storing, and using records about people. Innovations now being discussed throughout government and private industry recognize that the computer-based record keeping system, if properly used, can be a powerful management tool. Its capacity for timely retrieval and analysis of complex bodies of data can be of invaluable assistance to hard-pressed decision makers. Its ability to handle masses of individual*

³⁷⁹ V. *retro*, par. 1.2. Cfr ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens*, Washington D.C., 1973, xx-xxi.

transactions in minutes and hours rather than in weeks or months, as was formerly the case, makes possible programs of service to people that would have been unthinkable in the manual record-keeping era». E ancora, a dimostrazione della complessiva sensibilità dei suoi autori rispetto alla complessità della rivoluzione informatica: «Nonetheless, it is important to be aware, as we embrace this new technology, that the computer, like the automobile, the skyscraper, and the jet airplane, may have some consequences for American society that we would prefer not to have thrust upon us without warning. Not the least of these is the danger that some record-keeping applications of computers will appear in retrospect to have been oversimplified solutions to complex problems, and that their victims will be some of our most disadvantaged citizens»³⁸⁰.

Affermazioni come queste, che richiamano alla nostra memoria quelle dal tono più critico di Arthur Miller nel suo *The Assault on Privacy* dell'anno successivo, sono fino in fondo comprensibili solo se si assume piena consapevolezza dell'impatto travolgente avuto dall'introduzione degli "elaboratori elettronici" nella vita di relazione, e dalla loro ampia diffusione negli anni in cui tali scritti vengono pubblicati.

Come abbiamo già avuto modo di dire, agli anni Cinquanta risale il primo impiego di banche dati elettroniche, intese come insiemi strutturati di informazioni situate in sistemi di *record keeping* elettronici, principalmente da parte delle pubbliche amministrazioni statali, al fine di razionalizzare i propri compiti di gestione della cosa pubblica: lo stesso *excursus* storico tracciato nel suddetto Report dell'HEW suddivideva le tipologie di registri elettronici in *administrative, intelligence and statistical records*³⁸¹.

³⁸⁰ Ivi, pp. v-vii

³⁸¹ Ivi, p. 5 ss. Per maggiori dettagli sullo sviluppo dei sistemi di *record keeping* nella storia americana, lo stesso report rinvia ad ALAN WESTIN in M. Greenberger (a cura di), *Computers, Communications, and the Public Interest* (Baltimore, Md.: The Johns Hopkins Pr.ss), 1971. Aggiungiamo che, sebbene la nascita dell'informatica si ascriva alla pubblicazione

Tuttavia è dagli anni Sessanta che il loro utilizzo subisce un vero exploit, e ciò per via della diffusione dei circuiti integrati e dei microchip, che rendono economicamente più accessibile l'acquisito dei *computers*: tale tecnologia, essenzialmente basta sull'automazione dei processi di raccolta, organizzazione ed utilizzo delle informazioni, comincia a diffondersi nel settore privato, ai precipui scopi di tracciare le operazioni intercorse tra le imprese e i propri clienti e di misurarne statisticamente le fluttuazioni³⁸². Negli anni Settanta, poi, con l'arrivo dei *microcomputers*, caratterizzati dalla presenza di un solo microprocessore e capaci di soddisfare le esigenze di un singolo utente (antesignani, dunque, del *personal computer*), l'implementazione di *automated data processing systems* diviene inarrestabile³⁸³.

Non è dunque un caso che a quegli anni risalgano i contributi di cui si è parlato, le dispute sul concetto di *informational privacy* e le prime legislazioni in materia di elaborazione elettronica delle informazioni personali. Anche dati elettroniche, e *computers* che ne garantivano l'automazione, consentivano infatti per la prima volta all'uomo, in tutta la sua plurimillenaria storia, di reperire,

del famoso articolo in cui Alan Turing teorizza una «macchina computazionale» capace di simulare il processo di calcolo umano (ALAN TURING: «On computable numbers, with an application to the *Entscheidungsproblem*», in *Proc. London Math. Soc.*, 42, 1936, pp. 230–265), è pur vero che in quegli anni le «macchine di Turing multi-nastro» (i c.d. computers) consistevano in calcolatori a valvole di cospicue dimensioni a costi proibitivi: pertanto, solo amministrazioni pubbliche e grandi società potevano, effettivamente, sostenerne la spesa.

³⁸² Ivi, p. 8 ss. Si legge nel report: «*Automated data processing, transplanted from its military origin, quickly blossomed into a powerful industry, feeding on the demands of commerce and government for fast and efficient data handling, and in turn, fueling that demand by significantly changing the philosophy and practice of management itself*». A dimostrazione dell'evoluzione *tecnosociale* intervenuta, è interessante osservare che secondo l'Encyclopaedia Britannica il termine inglese data- base fa per la prima volta la sua comparsa nel 1962: v. la voce «Database», in *Encyclopaedia Britannica*, sez. «Computer Science», 2013, disponibile al sito <http://www.britannica.com>.

³⁸³ Per tali introduttive nozioni su scienza computazionale ed informatica, cfr. M. MELUCCI, «Information Retrieval. Metodi e modelli per i motori di ricerca», Franco Angeli, 2013; G. AUSIELLO, C. BATINI, V. FROSINI, «Informatica» in *Enciclopedia Italiana - Appendice VI*, Roma, Istituto dell'Enciclopedia Italiana, 2000.

raccogliere, archiviare o in qualsiasi modo trattare una quantità illimitata di informazioni, con difficoltà gradualmente decrescenti; e lo scenario si arricchiva di tecniche capaci di realizzare un'interconnessione pressoché costante tra le medesime. Enormi potenzialità di semplificazione per la vita dell'uomo, dunque; ma anche, parallelamente, nel momento in cui ogni aspetto della sua vita diventava velocemente memorizzabile ed accessibile, enormi rischi di dissoluzione della propria sfera riservata, della c.d. *self-determination*.

Non è solo il Dipartimento della Salute americano ad accorgersi dei benefici sociali e dei rischi individuali connessi alla *privacy* determinati dalla allora nuova tecnologia. Già nel 1968 l'Assemblea parlamentare del Consiglio d'Europa, con la Raccomandazione 509, aveva commissionato al Comitato dei Ministri uno studio sull'adeguatezza della CEDU e delle legislazioni nazionali a garantire la protezione del diritto al rispetto della sua vita privata, o « *personal privacy* », di fronte alla « *modern science and technology* », da cui era emersa la sostanziale inidoneità delle medesime a tale scopo, specialmente in relazione al fenomeno delle « *automated data banks* »³⁸⁴. La risposta fu l'adozione di due risoluzioni, rispettivamente la n. 22 e la n. 29, con cui il Consiglio stabiliva una serie di principi relativi alle « *personal information stored in electronic data banks* » che gli Stati membri erano invitati a recepire nell'implementazione di legislazioni *ad hoc*.³⁸⁵

Le risoluzioni in questione ebbero concretamente l'effetto di stimolare l'attività dei legislatori europei, che, come abbiamo visto, negli anni Settanta

³⁸⁴ Cfr. ASSEMBLEA PARLAMENTARE DEL CONSIGLIO D'EUROPA, *Recommendation 509 (1968), Human rights and modern scientific and technological developments*, 22 gennaio 1968, doc. 2326; CONSIGLIO D'EUROPA, *Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data - Explanatory Report*, ETS No. 108, 1981, par. 4. Ss.

³⁸⁵ Cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector*, 26 settembre 1973; e *Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector*, 20 settembre 1974.

principiarono a regolamentare l’“elaborazione” delle informazioni personali, e proprio con specifico, quasi settoriale riferimento alle banche dati automatizzate³⁸⁶. Tuttavia, è stato constatato come la maggior parte di queste coltivassero un approccio spesso restrittivo, che, nell’ offrire garanzie alla persona umana («persona interessata»), dall’altra inibiva l’ utilizzo delle prime; e che allo stesso tempo la frammentazione normativa che da tale pluralità di differenti legislazioni derivava ostacolava il libero trasferimento dei dati medesimi, gradualmente concepito dal settore produttivo e dai governi stessi come volano dello sviluppo economico³⁸⁷.

Per fare un esempio di tale approccio, basti pensare al “divieto categorico” introdotto in punto di «decisioni *unicamente* basate sulla profilazione *automatizzata*» dalla *Loi 78-17*, del 6 gennaio 1978, *relative à l'informatique, aux fichiers et aux libertés* che all’art. 2 secondo comma, nella sua versione originaria, stabiliva «*[a]ucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*»³⁸⁸.

Proprio per far fronte a tale mosaico di legislazioni potenzialmente ostative per lo sviluppo di un’ economia dei dati, nel 1980 interveniva l’OCSE con le sue non vincolanti Linee Guida. Ma ben più rilevante era, come ormai sappiamo,

³⁸⁶ V. *retro*, par. 2.2.2.

³⁸⁷ Cfr. ad es. E. STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Roma, 2008, e lo stesso memorandum esplicativo delle Linee Guida dell’OCSE, che di tale frammentazione normativa offre una panoramica, e che sottolinea l’importanza strategica a livello economico della libera circolazione dei dati, OCSE, *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data - Explanatory Memorandum*, punto 6.

³⁸⁸ Il primo comma, invece, recitava: «*Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*».

l'intervento del Consiglio d'Europa, che preceduto dalle raccomandazioni, dagli studi e dalle risoluzioni suddette, adottava la Convenzione n. 108 *espressamente* dedicata alla fattispecie dei trattamenti automatizzati dei dati personali e, nel loro quadro, teleologicamente orientata a promuovere i diritti fondamentali della persona interessata dal trattamento³⁸⁹. Quest'ultima ancora più dimostra il nesso intercorrente tra sviluppo tecnologico ed evoluzione del diritto, poiché in un atto di tipo *settoriale* quale dichiara di essere si condensano, in realtà, principi lungimiranti in punto di disciplina *generale* dell'elaborazione dei dati relativi alle persone fisiche, poi mutuati dalla stessa dir. 95/46 CE. Nel loro insieme, spiccano alcune delle definizioni generali delineate dall'art. 2, la cui modernità nell'inquadrare i fenomeni regolamentati è testimoniata dal fatto che la terminologia coniata risulta tutt'ora attuale: in particolare, ci si riferisce alla definizione di «dati a carattere personale», che identifica «ogni informazione concernente una persona fisica identificata o identificabile (“persona interessata”)»; e a quella di «trattamenti automatizzati», che «comprende le seguenti operazioni svolte in tutto o in parte tramite procedimenti automatizzati: registrazione dei dati, effettuazione di operazioni logiche e/o aritmetiche su tali dati, loro modificazione, cancellazione, estrazione o diffusione»³⁹⁰.

Lo stesso *Explanatory Report* alla Convenzione 108 poi, nell'individuare le ragioni dell'iniziativa, quasi specularmente al Report del 1973 dell'HEW, sottolineava in apertura come il potere dei dati, l'«*information power*», e insieme la realtà dell'automazione, segnatamente computazionale, affermatasi nella vita dell'uomo implicassero una corrispondente «*social responsibility*» degli utenti e soprattutto dei «gestori» delle informazioni (oggi diremmo titolari e responsabili del trattamento). Si legge infatti: «*In a modern society, many decisions affecting*

³⁸⁹ Per una più puntuale disamina, v. retro

³⁹⁰ Cfr. art. 2, CONSIGLIO D'EUROPA, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, n. 108/1981.

individuals are based on information stored in computerised data files: payroll, social security records, medical files, etc. It is essential that those responsible for these files should make sure that the undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored»³⁹¹. Principio, anche questo, della responsabilità sociale dei titolari, collegato alla *funzione sociale* della protezione dei dati personali così cristallinamente sottolineata dalla giurisprudenza recente della Corte di Giustizia, la cui importanza è quanto mai lievitato nella nostra, contemporanea società *datificata*.

Ora che abbiamo chiaro il contesto sociale e tecnologico in cui *nasce* la disciplina dell'elaborazione automatica, in senso lato, dei dati personali, non possiamo che constatare quanto tutte le analisi, le riflessioni e le raccomandazioni che abbiamo fino ad ora incontrato fossero precorritrici dell'attuale "ecosistema", che ne dilata ulteriormente il senso. Riassumere le caratteristiche principali di quest'ultimo, seppur ai limitati fini della nostra trattazione, è impresa laboriosa, che richiede all'osservatore di confrontarsi con una pluralità di discipline dotate di propri specifici statuti epistemologici, e che tuttavia, sotto il profilo dell'"invadenza" della tecnica nel dominio della "vita privata" interagiscono tra loro: dalla filosofia, anche nelle sue moderne declinazioni "informazionali"³⁹², alla cibernetica, dall'etica all'informatica. Ciononostante, qui si tenterà uno sforzo

³⁹¹ Cfr. CONSIGLIO D'EUROPA, *Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data - Explanatory Report*, ETS No. 108, 1981, par. 2.

³⁹² Il riferimento è chiaramente a quella «nuova disciplina filosofica» applicata alla «tecnologia dell'informazione» elaborata nel corso degli anni Novanta negli ambienti dell'Università di Oxford da Luciano Floridi, cui abbiamo avuto modo di accennare retro; i principi della stessa, utili ad inquadrare la moderna struttura *data driven* della società, sono condensati in alcune opere dell'autorevole studioso quali L. FLORIDI, *The Philosophy of Information*, Oxford University Press, Oxford, 2011 e ID., *The Fourth Revolution. How the infosphere is reshaping human reality*, cit.

(ulteriormente) sinottico, in quanto indispensabile per avere chiaro ambito applicativo ed oggetto della disciplina che analizzeremo.

A partire dagli anni su cui abbiamo poc'anzi “planato dall’alto”, la circolazione, la raccolta e l’archiviazione delle informazioni relative ad ogni aspetto della realtà, oggettiva così come soggettiva, dell’essere umano da parte delle sempre più raffinate tecnologie dell’informazione e della comunicazione (c.d. ICTs, acronimo di *Information and Communication Technologies*) è divenuta connotato costitutivo di qualsiasi contemporanea organizzazione sociale, determinando una «riqualificazione in chiave “informazionale” della realtà circostante»³⁹³. Dalla definizione del protocollo HTTP nel 1991 in senso al CERN di Ginevra, che segnava la nascita del World Wide Web³⁹⁴, fino alla più recente

³⁹³ La citazione è di S. SICA, V. D’ANTONIO, «La commodification dei dati personali nella data driven society», in P. STANZIONE, *I “poteri privati” delle piattaforme*, cit., p. 129.

³⁹⁴ È noto che la nascita della moderna declinazione di Internet, intesa propriamente come «rete di computer» e dunque come struttura, e del Web come servizio, e pertanto come «sistema di interconnessioni tra documenti» che sulla suddetta infrastruttura si fonda, è ricondotto storicamente alle ricerche compiute dall’informatico T. Berners-Lee e dal suo gruppo al CERN di Ginevra, con l’esigenza di disporre di una rete distributiva di materiale scientifico per i fisici delle alte energie. Il 30 aprile 1993 il CERN decise di rendere pubblica la tecnologia alla base del World Wide Web in modo che fosse liberamente disponibile e implementabile da chiunque, rilasciando pertanto il codice sorgente in dominio pubblico: a ciò conseguì la realizzazione del primo browser con caratteristiche simili a quelle attuali, il Mosaic. Da quel momento in poi, la tecnologia in questione si diffuse rapidamente in tutto il mondo: ad esempio, il primo sito web italiano messo on line fu quello del «Centro di ricerca, sviluppo e studi superiori in Sardegna» (CRS4). In ambito informatico, si è soliti suddividere le diverse fasi di sviluppo e di diffusione di Internet e del WWW in Web 1.0, o Web statico, come prima forma implementata e caratterizzata da un’interazione unilatera tra content provider e utente, che non può modificare i contenuti visualizzati; Web 2.0, termine apparso nel 2005, in cui l’interazione tra sito e utente aumenta considerevolmente e si assiste alla nascita e all’affermazione dei motori di ricerca (su tutti, Google), di sistemi di condivisione testuale (blog, chat, forum, wiki), e multimediale (YouTube) da parte degli utenti, dei social network (Facebook, Twitter) e delle piattaforme di e-commerce (Amazon); e Web 3.0, formula plurivoca che individuerrebbe il fenomeno attuale di trasformazione del Web in un database e l’implementazione dell’Intelligenza Artificiale per sfruttarne le potenzialità, compresi sistemi di apprendimento automatico (supervised e, soprattutto, unsupervised Machine Learning). Cfr. per una generale panoramica sui temi in questione A. MARINELLI, «Internet e Web», in *Enciclopedia della Scienza e della Tecnica*, Treccani, 2008,

realtà del c.d. *Metaverso*³⁹⁵, passando per il fenomeno dell'*Internet of Things* che ridefinisce la morfologia delle nostre case e delle nostre città, ormai quasi tutto il globo è interessato dall'inarrestabile fenomeno della digitalizzazione: secondo il report di una nota agenzia globale di *social media management*, nel 2022 si sarebbe raggiunta la vertiginosa cifra di 5,16 miliardi di utenti di internet (il 64% della popolazione mondiale), e di 4,76 miliardi di utenti di social media (pari al 60% della popolazione mondiale)³⁹⁶. Questa crescente, inarrestabile dinamica già evidente all'inizio del nuovo millennio ha indotto acuti "investigatori" del reale a coniare il termine «infosfera» per identificare la dimensione esistenziale della contemporaneità in cui, interpolando la nota sentenza hegeliana, «tutto ciò che è reale è informazionale e tutto ciò che è informazionale è reale»³⁹⁷. Dimensione in

[https://www.treccani.it/enciclopedia/internet-e-web_\(Enciclopedia-della-Scienza-e-della-Tecnica\)/](https://www.treccani.it/enciclopedia/internet-e-web_(Enciclopedia-della-Scienza-e-della-Tecnica)/); S. MELE, M. SPADA, «Internet», in *Enciclopedia Italiana – IX Appendice*, Treccani, 2015, [https://www.treccani.it/enciclopedia/internet_\(Enciclopedia-Italiana\)/](https://www.treccani.it/enciclopedia/internet_(Enciclopedia-Italiana)/); T. BERNERS-LEE, *Weaving the Web. The original design and ultimate destiny of the World Wide Web by its inventor*, San Francisco, Harper, 1999;

³⁹⁵ Termine impiegato per la prima volta nel 1992 da N. Stephenson nel romanzo cyberpunk *Snow crash*, esso individua una zona di convergenza di spazi virtuali interattivi, localizzata nel *cyberspazio* e accessibile dagli utenti attraverso un avatar con funzione di rappresentante dell'identità individuale. Ponendosi come evoluzione dell'*ubiquitous computing*, tale dimensione connette tra loro soggetti, oggetti, informazioni e avatar, e corrisponde sostanzialmente a quella che lo stesso Floridi ha definito *onlife*, espressione che descrive l'erosione della frontiera tradizionalmente esistente tra reale e virtuale. Il termine *Metaverso* ha assunto vasta risonanza mediata quando M. Zuckerberg ha mutato la denominazione della azienda da lui fondata proprio in Meta Platform Inc. Cfr. sul punto soprattutto L. FLORIDI, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer Link, 2015, disponibile in *open acces* qui: <https://link.springer.com/book/10.1007/978-3-319-04093-6>. Sulla possibilità di edificare un sistema coerente di norme disciplinanti il cyberspazio, a cominciare dall'architettura della rete internet (sotto il duplice profilo hardware e software), cfr. L. LESSIG, *Code 2.0*, Basic Books, 2006.

³⁹⁶ Cfr. WE ARE SOCIAL, *Global Digital Report 2023*, consultabile qui: <https://wearesocial.com/it/blog/2023/01/digital-2023-i-dati-globali/>. Il report evidenzia come, stando ai dati divulgati dai rispettivi *Over The Top*, l'insieme delle app e dei social network di Meta (Facebook, Instagram, Whatsapp) avrebbe avuto, nel corso del 2022, 2,958 miliardi di utenti attivi mensili, mentre l'app Tik Tok avrebbe registrato il più alto utilizzo medio mensile per utente, pari alla cifra esorbitante di 23 ore e mezza.

³⁹⁷ Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., 44ss.: «a un livello minimo, l'infosfera indica l'intero ambiente informazionale costituito da tutti gli enti informazionali, le loro proprietà, interazioni, processi e reciproche relazioni

cui le persone si trasformano in utenti “iper-connessi” e gli oggetti, divenuti *smart*, possono scambiare tra loro flussi di informazioni, abbattendo così la tradizionale frontiera tra *reale* e *virtuale* (inteso anche solo limitatamente come *digitale*), in un contesto definito pertanto «*onlife*»³⁹⁸.

Si assiste insomma, per utilizzare altro armamentario concettuale, ad un processo di «datificazione», di cui possono individuarsi tre essenziali profili tra loro complementari³⁹⁹.

Il primo consiste nel fatto che, a partire dalla rapida diffusione degli *smart phones* e degli altri *digitized devices*, ciascun essere umano produce, consapevolmente e inconsapevolmente, una enorme, continua quantità di dati, della più varia specie e natura, che gli strumenti suddetti, costantemente connessi alla *rete*, raccolgono e trasferiscono ad altri *devices*: è la realtà definibile, in prima approssimazione, come *Big Data*. Il secondo consiste nello sviluppo sempre maggiore delle capacità di analizzare i dati informatici osservati, i quali altrimenti,

(...). A un livello massimo, l'infosfera è concetto che può essere utilizzato anche come sinonimo di realtà, laddove interpretiamo quest'ultima in termini informativi. dall'analogico al digitale e la crescita esponenziale di spazi informativi in cui trascorriamo sempre più tempo illustrano con massima evidenza il modo in cui le ICT stanno trasformando il mondo in una infosfera». Cfr. per acute osservazioni sul punto R. MESSINETTI, «La privacy e il controllo dell'identità algoritmica», in *Contr. impr./Eur.*, 1/2021, p. 121 ss.;); E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation», p. 1209 ss.

³⁹⁸ Ivi, p. 47. L'autore sottolinea che «il mondo digitale online trabocca nel mondo analogico offline, con il quale si sta mescolando (...). In misura crescente conduciamo le nostre vite *onlife*».

³⁹⁹ Per la genesi dell'espressione, cfr. MCAFEE-BRYNJOLFSSON, «Big data: the management revolution», in *Harv. Bus. Rev.*, n. 10/2012, 60-68.; per riflessioni dettagliate sul punto, cfr. *ex multis* SCHONBERG, CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2018, p. 1 ss.; NEWELL-MARABELLI, «Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal effects of “datification”», in *Journal of Strategic Information Systems*, 24/2015, 5; per una panoramica generale, cfr. S. CALZOLAIO, «Protezione dei dati personali», cit., p. 594 ss.; ID., «Introduzione. *Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati», in *RIID*, 1, 2021. Per i riferimenti attinenti a ciascuna delle categorie che si introdurranno di seguito, la maggior parte delle quali redatte in corsivo, v. progressivamente *infra*.

allo stato grezzo (*raw data*), non rappresenterebbero che una consecuzione in forma elettronica di bit; e dunque di *estrarre informazioni* (intese come significato) da essi, e trasformarle in *conoscenza* (intesa come risultato dell'acquisizione consapevole, e dunque dell'analisi, di una o più informazioni): processo efficacemente sintetizzato dall'espressione *data mining*. Le capacità in questione, nell'attuale panorama tecno-sociale, sono propriamente "possedute" o, meglio, espresse dalle macchine, intese come elaboratori elettronici (dal più rudimentale computer al più sofisticato *smart watch*), guidati, in prima approssimazione, da formule matematiche codificate denominate *algoritmi*. Questi ultimi, ormai, consentono all'elaboratore stesso di condurre in modo *interamente o parzialmente automatizzato* l'analisi inferenziale dei dati stessi (*automated data processing*, o trattamento automatizzato dei dati), con ciò integrando sistemi di *Intelligenza Artificiale* (AI); e le più recenti declinazioni della tecnologia algoritmica sono in grado di apprendere dalla loro "esperienza" di analisi e, sulla base dei dati accumulati, di procedere ad elaborare e a generare autonomamente nuovi algoritmi in grado di raffinare ed ottimizzare l'analisi dei dati: stiamo parlando della nuova frontiera dell'Intelligenza Artificiale, ossia dei sistemi di *Supervised* e, soprattutto, di *Unsupervised Machine Learning* (ML). Il sempre più avanzato livello di interazione ormai esistente tra macchine e uomini rappresenta il presupposto del terzo e ultimo profilo essenziale del processo che andiamo descrivendo: ci riferiamo alla possibilità e alla capacità di assumere decisioni, per i soggetti pubblici e/o privati che dei suddetti dati e della suddetta tecnologia dispongono, basate sulla conoscenza estratta dai primi attraverso la seconda; ma, soprattutto, di affidarne l'elaborazione (*output*) e finanche l'attuazione concreta (*release*) alle macchine stesse. È il c.d. *alghoritmica* - o, appunto, *automated - decision making*.

Tutto questo complesso fenomeno, qui drasticamente riassunto, implica la nascita di un'economia nuova (*data driven economy*), i cui protagonisti adottando

modelli di business (se privati) e di *policy making* (se pubblici) costruiti sull'immagazzinamento e sullo scambio di dati, che si *patrimonializzano* sempre più (c.d. *commodification*), diventando “materia prima”, preziosa risorsa strategica: economia in cui, dunque, la maggiore o minore efficienza e/o competitività dipende, oltre che dalla disponibilità dei dati suddetti, dal “possesso” della suddetta tecnologia utile a estrarre conoscenza, persino *predittiva*, dai dati. Prima ancora che di fronte ad un'economia nuova, siamo quindi di fronte ad una società nuova, definita tanto dagli studiosi quanto dagli operatori *data driven society*, a sottolineare come ogni aspetto della vita concreta sia, appunto, *datificato*, e dunque tradotto in dato digitale.

Appare chiaro che per capire la portata del fenomeno, e per poterlo regolamentare (o per poter comprendere la regolamentazione vigente), occorre preliminarmente conoscere gli elementi di cui si compone. Dobbiamo quindi soffermarci su alcune delle categorie testé introdotte, seguendo appunto i tre livelli in cui la *datification* si articola: in particolare, *Big Data*, Intelligenza Artificiale ed *Automated Decision-Making* (abb. ADM).

Occupandoci del primo livello, ci occupiamo della materia prima che nutre la nuova economia digitale: il dato, inteso propriamente come *fonte* (e dunque non come sinonimo) di *informazione*, quest'ultima a sua volta *prodotto* dell'elaborazione di un singolo dato o di una pluralità di essi posti in correlazione tra loro⁴⁰⁰. E soprattutto, all'interno di tale composita categoria, della «fluida» materia del *dato personale*⁴⁰¹. Senza addentrarci ora nel merito delle definizioni

⁴⁰⁰ Cfr. le interessanti considerazioni in merito di G. FINOCCHIARO, «Intelligenza artificiale e protezione dati personali», in *Giur. It.*, 07/2019, p. 1673.

⁴⁰¹ Sulla «fluidità» della nozione, cfr. ad es. KORFF, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological*

normative, quanto meno di quelle rilevanti ai fini della presente trattazione, si può affermare che tradizionalmente (e dunque a partire dalla Convenzione n.108, e poi della dir. 95/46/CE che meglio definisce il perimetro della nozione) esso veniva identificato in «qualunque informazione relativa ad una persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale»⁴⁰². E se inizialmente il Gruppo di Lavoro art. 29, in un suo fondamentale parere in materia⁴⁰³, avvertiva che ai fini della qualificazione in termini di dato personale fosse necessario procedere ad una valutazione sulla probabilità e sulla ragionevolezza dell'ipotesi che, in concreto, quell'«altra informazione» fosse associata e associabile dal titolare del trattamento alla persona fisica, oggi questa prospettiva è stata opportunamente abbandonata in favore della più moderna definizione contenuta nel Reg. 2016/679 (GDPR), fino a comprendere esplicitamente tra le «altre informazioni» anche i «dati riferibili all'ubicazione o ad un identificativo online che *possano* rendere identificabile un interessato»⁴⁰⁴.

Questa nuova definizione riflette propriamente l'evoluzione intervenuta nel contesto tecnologico di riferimento, in cui viene meno il presupposto della “raccolta” del dato presso l'interessato e con il suo consenso (c.d. *provided*

Developments, European Commission Directorate-General Justice, Freedom and Security, Working Paper n.2/2010.

⁴⁰² Così disponeva l'originaria versione dell'art.4, lett.b), del d.lg.n.196/2003 (c.d. Codice della Privacy), che trasponessa l'analoga definizione contenuta nell'art. 2, lett a) della dir. 95/46/CE.

⁴⁰³ V. infatti GRUPPO DI LAVORO ARTICOLO 29, *Parere 4/2007 sul concetto di dati personali*, 01248/07/IT, WP 136, 20 giugno 2007, p. 15 ss.

⁴⁰⁴ Ci si tornerà nel terzo cap., ma cfr. già art. 4, par. 1, n. 1), Reg. 2016/679 UE (GDPR), che definisce il «dato personale» come «qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

data)⁴⁰⁵: negli ultimi trent'anni, la produzione specialmente inconsapevole di dati è aumentata raggiungendo quantità che spesso «supera[no] la capacità di un [singolo] database di acquisire, archiviare, gestire e analizzare»⁴⁰⁶; e gli elaboratori, come strumenti utilizzati dall'uomo o come attori totalmente o parzialmente indipendenti, in caso di *automated processing*, sono in grado di creare modelli di correlazione ricorrenti, con indole predittiva, dalle cui inferenze a loro volta discendono nuovi dati, anche detti *algo-created data* (e da parte della dottrina classificati in *observed, derived and inferred data*)⁴⁰⁷.

La realtà appena descritta, e segnatamente il primo “fattore”, viene comunemente identificato con l'espressione *Big Data*⁴⁰⁸. Quest'ultima ha un perimetro semantico tutt'altro che definito, e costituisce oggetto di interpretazione contrastanti, che le riconducono significati eterogenei. Lo stesso Comitato Consultivo istituito dalla Convenzione n. 108 del Consiglio d'Europa, nelle Linee Guida predisposte in materia, sottolinea come «*there are many definitions of Big Data, which differ depending on the specific discipline. Most of them focus on the*

⁴⁰⁵ Dedicando pagine importanti alla centralità del consenso «qualificato» quale base giuridica ordinaria del trattamento dei dati personali, e al requisito della «consapevolezza» M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», in P. STANZIONE, *I “poteri privati” delle piattaforme private*, cit., in part. p. 87 ss.

⁴⁰⁶ La citazione è di J. MANYKA ET AL., *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, maggio 2011, riportata da

⁴⁰⁷ Parla di *algo-created data* R. MESSINETTI, «La privacy e il controllo dell'identità algoritmica», cit., p. 140 ss. Per la tassonomia proposta, che adotta come criterio di classificazione l'origine del dato, cfr. soprattutto ABRAMS, «Origins of Personal Data and its Implications for Governance», in *The Information Accountability Foundation*, marzo 2014, in <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>, che individua le quattro categorie dei *provided, observed, derived and inferred data*, constatando come le ultime tre comportino un basso livello di consapevolezza per l'interessato.

⁴⁰⁸ La letteratura sul tema è vasta; si rinvia, *ex multis*, a M. OREFICE, *I big data e gli effetti su privacy, trasparenza e iniziativa economica*, Roma, 2018, passim; A. MANTELERO, «La privacy all'epoca dei Big Data», in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino 2019, 1181 ss.; G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in E. Tosi (a cura di), *Privacy digitale*, Giuffrè Francis & Taylor, pp. 447-484; S. BAROCCAS, A.D. SELBST, «Big Data's Disparate Impact», 104 *California L.R.*, 673 (2016);

*growing technological ability to collect process and extract new and predictive knowledge from great volume, velocity, and variety of data»*⁴⁰⁹. Stesso approccio segue l'*Information Commisioner's Office* britannico, che tuttavia, nel sottolineare come della categoria siano offerte in letteratura diverse definizioni, allo stesso tempo richiama la nozione fino a questo momento più accreditata e meglio capace di evidenziare le caratteristiche essenziali del fenomeno⁴¹⁰.

Ci si riferisce alla nozione già elaborata dal noto analista Doug Laney con il modello di crescita tridimensionale da questi teorizzato delle «3V: *Volume, Velocity and Variety*»⁴¹¹. Ad essa recentemente si sono aggiunte proposte che aggiungo altre due V: *Veracity* e *Value*⁴¹². Sinotticamente, la complessa definizione è stata recentemente ricostruita in tali termini: «*Big Data is the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value*»⁴¹³. *Big Data*, insomma, come fenomeno caratterizzato dalla disponibilità di una quantità enorme di dati (*volume*), di contenuto e provenienza variegata (*variety*), accurati perché aggiornati in tempo reale (*veracity*), oggetto di tecniche che garantiscono una sempre più alta e rapida capacità di analisi (*velocity*) e perciò

⁴⁰⁹ CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, 23 gennaio 2017, p. 2.

⁴¹⁰ Cfr. INFORMATION COMMISSIONER'S OFFICE (ICO), *Big data, artificial intelligence, machine learning and data protection*, versione 2.0, 3/2017, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>, in part. v. p. 6, in cui viene riportata la definizione riportata dal Gartner IT Glossary e, in conclusione, afferma «we think it is useful to regard it as data which, due to several varying characteristics, is difficult to analyse using traditional data analysis methods»

⁴¹¹ Cfr. D. LANEY, *3D Data Management: Controlling Data Volume, Velocity and Variety*, META Group, febbraio 2001, passim.

⁴¹² Cfr. ad es. Cfr. G. D'ACQUISTO, NALDI, *Big data e privacy by design*, Torino, 2017, passim.; C. TSAI, C. LAI, H. CHAO, A. V. VASILAKOS, «Big Data analytics: a survey», in *Journal of Big Data*, 2015, 2, 2 ss.

⁴¹³ Cfr. A. DE MAURO, M. GRECO, M. GRIMALDI, «A Formal Definition of Big Data Based on its Essential Features», in *Library Review*, 65, 2016, 122.

capaci di estrarre da essi conoscenza, e dunque valore economico (*value*): valore che, appunto, si incardina sulla conoscenza di aspetti della personalità degli interessati, e sulla conseguente possibilità di costruire modelli di preferenze attuali e di *comportamenti futuri* (dunque predittivi). E tale «flusso incessante», accanto alla digitalizzazione di dati strutturati come informazioni sanitarie, patrimoniali ecc., si imputa principalmente alla costante creazione di c.d. *Users Generated Contents* (come le parole chiave digitate sui motori di ricerca o le interazioni sulle piattaforme social) e alla crescente interazione tra «oggetti intelligenti», per lo più ascrivibile alla già citata dimensione dell'*Internet of Things* (IoT)⁴¹⁴.

Ora, si capisce come tale fenomeno connoti i dati, anche quelli personali, di una dimensione sempre più patrimoniale e segnatamente negoziale, in quanto idonei a soddisfare interessi economici e dunque suscettibili di costituire oggetto di transazioni commerciali a tale scopo⁴¹⁵: si parla, sempre più, di

⁴¹⁴ Sul fenomeno dell'*Internet of Things*, vedi innanzitutto INTERNET SOCIETY, *The Internet of Things: An Overview*, October 2015, che definisce lo IoT come la capacità di oggetti dotati di sensori, e diversi dai computers, di connettersi alla rete internet e pertanto di generare, scambiare, e utilizzare dati reciprocamente, richiedendo un intervento umano minimo: tra gli esempi che si possono portare, dispositivi indossabili (come gli *activity tracker* o gli *smart watches*), sistemi domotici (come gli elettrodomestici intelligenti), sistemi per *smart cities* e *connected cars*. Cfr. anche la definizione di Gruppo di Lavoro Articolo 29 si veda WP 29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, adottata il 16 settembre 2014 (WP 223), 4; e cfr. sull'argomento A. MANTELERO, C. VACIAGO, «Internet of Things (IoT)», in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffrè, 2019, 569 ss;

⁴¹⁵ Sull'informazione come «bene giuridico» in generale, cfr. ex multis P. PERLINGIERI, «L'informazione come bene giuridico», in *Rass. Dir. Civ.*, 1990, 326 ss.; ZENO-ZENCOVICH, voce «Informazione (profili civilistici)», in *Dig. disc. Priv.*, sez. civ., IX, Torino, 1993, p. 420 ss.; G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 209 ss.; G. DI FILIPPO, «I dati come beni giuridici», cit., p. 15 ss.; con riferimento specifico al loro «valore negoziale», cfr. A. METZGER, «Data as Counter-Performance: What Rights and Duties do Parties Have?», in *Journal of Intellectual Property*, 8, 2017, p. 1 ss.; G. RESTA, V. ZENO-ZENCOVICH, «Volontà e consenso nella fruizione dei servizi in rete», in *Riv. trim. dir. proc. civ.*, 2018, p. 436 ss.

commodification dei dati personali, e quindi di attribuzione di un valore economico ad essi, quali beni patrimoniali o *tradable commodities*⁴¹⁶.

Appare altrettanto evidente che essi intanto possono nutrire la nuova economia, in cui l'informazione costituisce il principale *input* del sistema produttivo, in quanto sussistano le tecnologie capaci di estrarre il valore in questione: l'attenzione si sposta allora sempre più sul piano del "trattamento" della crescente "mole globale" di dati, e dunque delle tecniche sofisticate indispensabili per implementare tale processo *estrattivo*: una più recente definizione di *Big Data*, non a caso, valorizza il nesso intercorrente tra i due profili, qualificandoli come «*new generation of technologies and architectures, designed to economically separate value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and analysis*»⁴¹⁷. E se il Consiglio d'Europa, nelle linee guida già citate, avvisa che, accanto agli enormi benefici che la loro disponibilità può apportare in termini di innovazione sociale, di produttività del settore privato e di efficienza del settore pubblico, i *Big Data* consentendo di «*collect and analyse large amounts of data to identify attitude patterns and predict behaviours of groups and communities*» schiudono rischi inediti per la collettività⁴¹⁸, è lo stesso Gruppo di Lavoro art. 29 ad affermare che i «*Big Data can be used to identify more general trends and correlations but*

⁴¹⁶ Sulla *commodification*, cfr. V. RICCIUTO, «Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali», in *Riv. dir. civ.*, 2020, 3, p. 642 ss.; intesa come presa di coscienza, da parte del diritto, di un "dato di fatto", ai fini di un effettivo adeguamento (esegetico) alla realtà dei rapporti economici della disciplina a tutela della sfera privata e di autodeterminazione informativa dell'interessato, cfr. S. SICA, V. D'ANTONIO, «La *commodification* dei dati personali nella *data driven society*», cit., in part. P. 136 ss.

⁴¹⁷ La cit. è di P. JAIN, M. GYANCHANDANI, N. KHARE, «Big Data privacy: a Technological Perspective and Review», in *Journal of Big Data*, 2016, 3, 1 ss.; puntualmente riportata da G. DE GREGORIO, R. TORINO, «Privacy, tutela dei dati personali e Big Data», cit.

⁴¹⁸ Cfr. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, cit., p. 1

[...] *big data may also pose significant risks for the protection of personal data and the right to privacy*», in ciò confortato dal Garante europeo della protezione dei dati personali (*European Data Protection Supervisor* - EDPS)⁴¹⁹.

Le moderne tecniche di elaborazione dei dati cui ci stiamo riferendo, che trasformando il trattamento in un *fenomeno produttivo* di rilevanza economica, sono comunemente definite *Big Data analytics*: espressione utilizzata allora per identificare il complesso delle tecnologie computazionali utilizzate per l'analisi di grandi quantità di dati (appunto, Big Data), strutturati o meno, confrontandoli tra loro per scoprire schemi, tendenze e correlazioni altrimenti nascoste; il *processo* stesso di *estrazione* di conoscenza attraverso i suddetti strumenti essendo a sua volta definito, con formula divenuta popolare, *data mining*⁴²⁰. E le tecnologie in questione, impiegate dall'uomo attraverso le macchine o dalle macchine *autonomamente*, si fondano essenzialmente sull'utilizzo degli algoritmi e delle forme di Intelligenza Artificiale che essi implementano, compresi i moderni sistemi di *machine learning*.

⁴¹⁹ Cfr. GRUPPO DI LAVORO ARTICOLO 29, *Opinion 03/2013 on purpose limitation*, aprile 2013; Cfr. anche EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 7/2015, Meeting the challenges of Big Data*, novembre 2015, che sottolinea puntualmente come «*Big data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data*».

⁴²⁰ V. ad es. la definizione adottata dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), secondo cui il termine *Big Data analytics* “*refers to the whole data management lifecycle of collecting, organizing and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours*”; cfr. ex multis G. DE GREGORIO, R. TORINO, «Privacy, tutela dei dati personali e Big Data», cit., G. D'ACQUISTO ET AL., «Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics», ENISA, dicembre 2015.; sul concetto di *data mining*, v. in part. U.M. FAYYAD, G. PIATETSKY-SHAPIRO, P. SMYTH, G. PIATETSKY-SHAPIRO, P. SMYTH, «From data mining to knowledge discovery: an overview», in U. Fayyad, (ed.) *Advances in Knowledge Discovery and Data Mining*. AAAI Press, Menlo Park, CA (1996).

In questo modo, tuttavia, ci siamo spostati al “secondo livello” del suddetto processo di *datification*, che attiene alla capacità di *analisi* dei dati: occorre analizzare separatamente le relative categorie.

Il *paper* dell’ICO già citato ha ben evidenziato la relazione reciproca che intercorre tra *Big Data*, tecnologie utilizzate per estrarne valore e “struttura” intima delle medesime (e, pertanto, tra i primi due livelli della datificazione): premettendo che, *Big Data*, Intelligenza Artificiale e *Machine Learning* sono concetti spesso impropriamente sovrapposti, vi si afferma limpidamente «(...) *Big Data can be thought of as an asset that is difficult to exploit. AI can be seen as a key to unlocking the value of big data; and machine learning is one of the technical mechanisms that underpins and facilitates AI. The combination of all three concepts can be called ‘big data analytics’*»⁴²¹.

Senza coltivare la pretesa di analizzare nel dettaglio, sotto il profilo scientifico, le tecnologie computazionali in parola, è tuttavia essenziale ai fini della trattazione tracciare un quadro riassuntivo.

È stato efficacemente affermato che tutto il processo fino ad ora descritto (ed anche il terzo livello dell’*output* e della sua *azione*) è governato dagli algoritmi⁴²². Al netto dell’uso disinvolto che oggi spesso si fa di tale termine, il quale ne svisceri tutta la densità semantica, ai fini della materia che qui ci occupa possiamo isolare nel suo composito alveo il significato attribuitogli in ambito informatico. Possiamo definire, allora, l’algoritmo come un *sequenza finita di operazioni elementari*, eseguibili facilmente da un elaboratore che, a partire da un insieme di dati (*input*), produce in un *tempo ragionevole* un altro insieme di dati (*output*) i quali soddisfano un preassegnato insieme di requisiti: un complesso

⁴²¹ ICO, *Big Data*, cit., p. 8.

⁴²² Cfr. STEINER, *Automate this. How algorithms came to rule our world*, Penguin, 2012, passim.

di istruzioni matematiche impartite ad un elaboratore, dunque; o, se si vuole, un modello matematico applicato *attraverso* una macchina alla risoluzione di uno o più problemi specifici⁴²³. L'avvento dell'informatica ha dunque consentito lo sviluppo delle prime forme di *automazione* (parziale o totale) nella soluzione di problemi attraverso l'elaborazione di dati da parte delle macchine, ancora interamente "di supporto" alla razionale (e manuale) attività dell'uomo. Tuttavia, dalla metà degli anni Ottanta le tecniche algoritmiche hanno subito notevoli evoluzioni sotto diversi aspetti, quali una migliore utilizzazione delle crescenti possibilità offerte dai moderni mezzi di elaborazione e, soprattutto, l'uso di strutture di dati sempre più sofisticate. E dunque, con la crescente capacità computazionale delle macchine, si è provveduto a configurare i primi sistemi algoritmici capaci di "far riprodurre" alle prime alcuni procedimenti logici tipici dell'intelletto umano, al fine di dare ai computers «(...) *behaviours which would be thought intelligent in human beings*» (e dunque, in prospettiva, di "sostituire" potenzialmente gli umani in numerose operazioni). In questo modo, entriamo tuttavia nel "dominio" dell'Intelligenza Artificiale⁴²⁴.

⁴²³ Cfr. il fortunato e fondamentale manuale di T. H. CORMEN, CH. E. LEISERSON, R. L. RIEVEST., C. STEIN, *Introduction to Algorithms*, The MIT Press, 2022, p. 5 ss, usando le parole degli autori «*informally, an algorithm is any well-defined computational procedure that takes some value, or set of values, as input and produces some value, or set of values, as output in a finite amount of time*»; AA.V.V., «Algoritmo» (voce), in *Enciclopedia on line*, Treccani, disponibile qui: <https://www.treccani.it/enciclopedia/algoritmo/> ; A. PANCONESI, «Programmazione (algoritmi di)», in Treccani, *Enciclopedia della scienza e della tecnica*, 2008, [https://www.treccani.it/enciclopedia/algoritmi-di-programmazione_\(Enciclopedia-della-Scienza-e-della-Tecnica\)/](https://www.treccani.it/enciclopedia/algoritmi-di-programmazione_(Enciclopedia-della-Scienza-e-della-Tecnica)/); WITTEN, FRANK, HALL, PAL, *Data Mining. Practical Machine Learning Tools and Techniques*, Morgan Kaufmann-Elsevier, 2017, pp. 4 ss. Aggiungiamo, alla luce di tali riferimenti, che strutturalmente altri elementi fondamentali dell'algoritmo consistono nella complessità computazionale, relativa al numero di operazioni elementari necessarie per produrre l'output (direttamente legato al tempo di calcolo necessario per eseguire l'a.), e nell'approssimazione, relativa a quanto vengono soddisfatti gli obiettivi secondo il criterio specificato.

⁴²⁴ Cfr. A. CAROBENE, «Intelligenza artificiale (voce)», in *Enciclopedia online*, Treccani <https://www.treccani.it/enciclopedia/intelligenza-artificiale/>; F. AMIGONI, V. SCHIAFFONATI E MARCO SOMALVICO, «Intelligenza artificiale (voce)», in *Enciclopedia della Scienza e della Tecnica*, Treccani, 2008, <https://www.treccani.it/enciclopedia/intelligenza->

Intelligenza Artificiale (d'ora in poi IA; o, abbreviando il corrispettivo inglese *Artificial Intelligence*, AI) è concetto, anche questo, altrettanto plurivoco. Esso conosce definizioni che ne accentuano la dimensione di *disciplina autonoma*, crocevia fecondo di numerose scienze quali la filosofia, la matematica, la psicologia, la cibernetica, le scienze cognitive. Ad esempio, in ambito istituzionale, il Consiglio d'Europa definisce l'IA come quel «complesso di scienze, teorie e tecniche finalizzate a riprodurre le abilità cognitive di un essere umano per mezzo di una macchina, al fine ultimo di affidargli compiti finora delegati ad operatori umani»⁴²⁵. Al contempo, e sempre in contesto europeo, il concetto conosce altre definizioni che l'IA identificano come qualsiasi insieme di «sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato»⁴²⁶.

[artificiale \(Enciclopedia-della-Scienza-e-della-Tecnica\)/](#) ; R. CORDESCI, «L'intelligenza artificiale», in L. Geymonat, *Storia del pensiero filosofico e scientifico. Il Novecento*, a cura di Enrico Bellone, Corrado Mangione, Milano, Garzanti, 1996, VIII, pp. 145-200; la citazione, invece, è di THE SOCIETY FOR THE STUDY OF ARTIFICIAL INTELLIGENCE AND SIMULATION OF BEHAVIOUR, «What is Artificial Intelligence», AISB Website. <http://www.aisb.org.uk/public-engagement/what-is-ai>.

⁴²⁵ Cfr. PORTALE DEL CONSIGLIO D'EUROPA, *Glossario, Intelligenza Artificiale (voce)*, disponibile all'indirizzo www.coe.int/en/web/artificial-intelligence/glossary.

⁴²⁶ Sono le parole del Gruppo Indipendente di esperti ad alto livello sull'Intelligenza Artificiale, istituito dalla Commissione Europea nel giugno 2018, nei recenti *Orientamenti Etici per un'AI affidabile*, B-1049 Bruxelles, 4 aprile 2018, p. 45, che prosegue sottolineando come: «I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando gli effetti che le loro azioni precedenti hanno avuto sull'ambiente». È importante rilevare che la definizione in questione pare essere stata recepita anche dalla Commissione Europea nella predisposizione della proposta di Regolamento sull'Intelligenza Artificiale attualmente in discussione al Consiglio e al Parlamento Europeo. V. infatti. Art. 3, Par. 1, n. 1), *Proposta di Regolamento del Parlamento*

Tralasciando il nodo terminologico, è importante sottolineare come il funzionamento delle reti neurali umane, e la loro potenziale applicazione alle macchine, in epoca moderna rappresenti oggetto di indagine multidisciplinare sin dagli anni Quaranta del secolo scorso, il cui primo compiuto approdo consiste nel capitale saggio pubblicato nel 1950 da Alan Turing e intitolato «Macchine calcolatrici e intelligenza»⁴²⁷. E la nascita in senso istituzionale dell'Intelligenza Artificiale come «campo del sapere» si fa comunemente risalire alla Conferenza di Dartmouth (Hanover, New Hampshire) del 1956⁴²⁸.

Tuttavia, l'IA come scienza o come oggetto di indagine ha vissuto fasi di instabile interesse proprio fino agli anni Novanta, in cui essa ha cominciato a ricevere un'attenzione esponenzialmente maggiore, fino alla predisposizione della vigente disciplina dei processi decisionali interamente automatizzati configurata dall'art. 22 del GDPR: disciplina che proprio i sistemi di IA assume quale principale elemento (se non addirittura in qualità di *soggetti*) della fattispecie considerata, e che più in generale si confronta con l'uso sistematico

Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, OM(2021) 206 final, 21.4.2021, che definisce un «sistema di Intelligenza Artificiale» come «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I [es. Machine Learning, Deep Learning, approcci basati su logica e conoscenza, approcci statistici], che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

⁴²⁷ A. M. TURING, «Computing Machinery and Intelligence», in *Mind*, 49, 1950, p.v433ss, in cui il celebre matematico inglese propone il test, passato alla storia come *imitation game*, strumentale a stabilire se una macchina sia in grado di esibire un comportamento intelligente (l'esito positivo riscontrandosi laddove la macchina riesca ad “ingannare”, nell'esecuzione delle istruzioni impartitegli, un essere umano circa la propria natura artificiale); attendibilità del test confutata solo negli anni Ottanta a livello filosofico da J.R. SEARLE, *Minds, Brains and Science*, 3, *Behavioral and Brain Sciences*, 1980, 3, 417 ss, che ivi propone il famoso esperimento mentale noto come «Chinese Room».

⁴²⁸ V. il testo della proposta con cui gli organizzatori della conferenza (nonché “padri fondatori” di questa tecnologia) affrontarono i temi principali del campo di ricerca, tra cui le reti neurali, la teoria della computabilità: la creatività, l'elaborazione e il riconoscimento del linguaggio naturale: MCCARTHY-MINSKY-ROCHESTER-SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, <https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802>.

dell'automazione nei trattamenti dei dati personali⁴²⁹. Ad aver determinato tale mutamento di paradigma e pertanto lo sviluppo delle potenzialità già insite nell'IA è stato, proprio in conseguenza del potente sviluppo della microelettronica (e dunque dell'evoluzione incrementale dei processori dei *computers* secondo la c.d. «legge di Moore»⁴³⁰), il denunciato exploit del fenomeno *Big Data*. La possibilità di analizzare una mole di dati anche non strutturati, attinti da ogni aspetto del reale, e di individuare le correlazioni tra gli stessi per produrre conoscenza suscettibile di sfruttamento per i più disparati scopi, dalla *public policy* al marketing personalizzato, ha infatti rappresentato il motore dello sviluppo di forme sempre più avanzate di IA⁴³¹. Nuovi sistemi, pertanto, sempre più capaci di emulare il funzionamento del cervello umano, e quindi non solo di analizzare linearmente i dati, bensì finanche di *imparare* dai dati analizzati per rispondere intelligentemente ai nuovi dati da trattare e *adattare* di conseguenza il proprio *output*⁴³². Quanto sottolineato sarebbe già idoneo a condurci nel terzo e ultimo livello della *datification*, ovvero quello delle decisioni interamente o parzialmente automatizzate (algoritmiche, appunto). Prima, tuttavia, conviene dedicare alcuni

⁴²⁹ Cfr. per alcune note generali G.F. ITALIANO, «Intelligenza Artificiale: passato, presente, futuro», in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018, 209ss.

⁴³⁰ Cfr. per alcune info. generali B. RICCÒ, «Legge di Moore», in *Enciclopedia della Scienza e della Tecnica*, Treccani, 2008, [https://www.treccani.it/enciclopedia/legge-di-moore_\(Enciclopedia-della-Scienza-e-della-Tecnica\)/](https://www.treccani.it/enciclopedia/legge-di-moore_(Enciclopedia-della-Scienza-e-della-Tecnica)/)

⁴³¹ Cfr. ad es. M. HILDEBRANDT, *Smart Technologies and the End(s) of Law Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Northampton, 31 ss.; U. M. FAYYAD, G. PIATETSKY-SHAPIO, P. SMYTH, «From Data Mining to Knowledge Discovery in Databases», 17, *AI Magazine*, 3, 1996, 37, 39ss; per alcune riflessioni sull'evoluzione dell'AI, e sulle sue ragioni, cfr. Per una riflessione di più ampio respiro sulle caratteristiche dell'intelligenza artificiale cfr. M. IASELLI, «Intelligenza artificiale e robotica», in G. CASSANO, V. COLAROCCHIO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè, 2018, 281 ss.

⁴³² Cfr. ad es. sul punto The Outlook for Big Data and Artificial Intelligence (AI). IDG Research, 11 November 2016 <https://idgresearch.com/the-outlook-for-big-data-and-artificial-intelligence-ai/> Accessed 7 December 2016.

cenni a quelle più avanzate declinazioni di IA cui abbiamo appena fatto riferimento: intendiamo il *Machine Learning* e, nel suo ambito, il *Deep Learning*.

Il *Machine Learning* (d'ora in poi, ML) è considerato una sottocategoria dell'Intelligenza Artificiale, un "livello più profondo"; o anche un più sofisticato mezzo di utilizzo della medesima⁴³³. In particolare, essa viene definita come quella branca dell'IA che studia in funzione applicativa l'utilizzo dei dati e degli algoritmi per imitare i sistemi e le modalità attraverso cui il cervello umano impara, gradualmente implementando l'accuratezza dei propri procedimenti intellettivi e, conseguentemente, delle informazioni (selezionate ed anche "inferite"): per questo si dice che gli algoritmi di ML sono "capaci di apprendere"⁴³⁴. La categoria in questione, a sua volta, si distinguerebbe in *supervised* e *unsupervised* ML: se nel primo caso gli algoritmi che compongono "l'anima razionale" del sistema di IA sono stati programmati in modo da raggiungere determinati risultati, nel secondo il sistema non viene provvisto dal programmatore delle categorie utili ad analizzare il flusso di dati considerato, cosicché sono gli algoritmi stessi a "scoprire" le correlazioni tra i dati senza alcuna istruzione sui risultati da raggiungere⁴³⁵.

⁴³³ Per un'analisi più approfondita sui temi dell'AI e del ML, cfr. da subito E. ALPAYDIN, *Introduction to machine learning*, MIT press, 2014, passim; M. IASELLI, «Intelligenza artificiale e robotica», in G. Cassano, V. Colarocco, G. Battista Gallus, F.P. Micozzi (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018*, n. 101 cit.

⁴³⁴ Cfr. la definizione dell'International Business Machine Corporation (IBM), la più antica azienda statunitense nel settore informatico e tra le più grandi al mondo, reperibile qui: <https://www.ibm.com/topics/machine-learning>. La pagina, e le altre dedicate al *topic* in questione, offrono anche un'intelligibile descrizione del funzionamento e dei principali impieghi di tale tecnologia. Cfr. anche

⁴³⁵ Cfr. in particolare C. KUNER, D. J. B. SVANTESSON, F.H. CATE, O. LYNKEY, C. MILLARD, «Machine learning with personal data: is data protection law smart enough to meet the challenge?», in *7 International Data Privacy Law*, 1 (2017); R. ANGELINI, «Intelligenza Artificiale e governance. Alcune riflessioni di sistema», in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 295 ss.; per una disamina dal taglio più divulgativo ma estremamente utile per comprendere la materia, D. CASTELVECCHI, «Can we open the black-box of AI?», in *Nature*, n. 538/2016, <http://www.natu->

A propria volta, l'*unsupervised* ML conosce una sottocategoria, o declinazione, ancora più avanzata, alla base di tutte le più recenti applicazioni della cibernetica, dell'informatica e, in definitiva, dell'IA preposti allo svolgimento di compiti analitici e fisici *senza* l'intervento umano: il *Deep Learning* (d'ora in poi, DL), così denominato per la circostanza di essere strutturato su più livelli di c.d. *Artificial Neural Networks* (ANN) o reti neurali artificiali, ovvero un insieme di livelli di nodi ognuno dei quali produce uno o più *output* che opereranno come *input* nel livello successivo, la cui configurazione è pertanto ispirata al modo in cui i neuroni biologici si inviano gli impulsi nervosi⁴³⁶. Questa configurazione rende la capacità computazionale di tali sistemi *incrementale*: essendo in grado di acquisire e di organizzare in formato strutturato *anche* set di dati non strutturati, essi sono capaci di migliorare le proprie prestazioni, compresa l'accuratezza della propria attitudine *predittiva*, all'aumentare dei dati disponibili⁴³⁷. Ciò ne spiega il poderoso sviluppo successivamente all'esplosione del fenomeno *Big Data*⁴³⁸.

re.com/news/can-we-open-the-black-box-of-ai-1.2073; ed anche MARR, «What Is The Difference Between Deep Learning, Machine Learning and AI?», in *Forbes*, 8-12-2016, ma v. anche <http://www.forbes.com/sites/bernardmarr/2016/12/08/what-is-the-difference-between-deep-learning-machine-learning-and-ai/#f7b7b5a6457f>.

⁴³⁶ Cfr. ad es N. BOLDRINI, *AI. Artificial Intelligence*, Milano Finanzia S.p.a., Milano, 2018; M. HODNETT, J.F. WILEY, *Deep Learning Essentials*, Packt Publishing, Birmingham, 2018, 9ss.; G. CERULLI, *Fundamentals of Supervised Machine Learning*, SpringerLink, 2023, pp. 1-17 e 269ss.; E. ALPAYDIN, *Introduction to Machine Learning*, cit.

⁴³⁷ V. nota precedente; Per una spiegazione dal taglio meno specialistico, e di pregevole chiarezza, cfr. il già citato D. CASTELVECCHI, Can we open the black-box of AI?, *Nature*, n. 538/2016, <http://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731>. Consulta poi la pagina dell'IBM dedicata al *deep learning*, che ne traccia un esaustivo quadro, descrivendo anche i tipi di apprendimento somministrabile al sistema e le classi di reti neurali oggi esistenti (convoluzionali, o CNN, e ricorrenti, o RNN): <https://www.ibm.com/it-it/topics/deep-learning>.

⁴³⁸ Per portare solo alcuni esempi prodotti e dei servizi d'uso quotidiano sempre più basate su applicazioni guidate dal Deep Learning, questi comprendono il riconoscimento vocale e facciale, la computer vision, la guida autonoma, la traduzione in tempo reale, il video captioning, i chatbot, gli assistenti virtuali (Siri, Alexa ecc.), il marketing targettizzato, il dynamic pricing, l'high frequency trading, e le più recenti applicazioni di IA generativa, come ChatGPT (chatbot basato sull'apprendimento automatico). V. <https://www.ibm.com/it-it/topics/deep-learning>.

L'attitudine all'autoapprendimento della rete neurale dei sistemi di DL, quindi, colloca quest'ultimo nella categoria della c.d. *strong AI*, poiché, piuttosto che limitarsi a coadiuvare l'uomo nell'utilizzo delle sue facoltà intellettive, si propongono come autonomo sistema razionale, dotato di un proprio *status* cognitivo⁴³⁹.

Alla luce di tutta l'analisi che abbiamo svolto, si capisce come tali sviluppi senza precedenti della tecnologia abbiano incentivato, e allo stesso tempo consentito, l'implementazione di sistemi *non solo* di trattamento, ma anche di *decision making* automatizzato.

È centrale evidenziare uno dei principali e più ampiamente denunciati limiti della tecnologia in parola, che riflessi profondi ha sulla materia degli *algorithmic data processing and decision making*. Stiamo parlando del fenomeno efficacemente descritto dagli studiosi con l'espressione *black box*, che identifica l'opacità del percorso logico di tipo *inferenziale* seguito dalla macchina nell'elaborazione del dato, nella conseguente produzione dell'output e ancora più nel processo di autoapprendimento ed implementazione di "perfezionati" algoritmi⁴⁴⁰. In sostanza, mentre aumenta la capacità delle macchine di correlare i dati e di scoprirne (alias produrne) per inferenza di nuovi, persiste (se non

[it/topics/deep-learning; https://www.bnova.it/intelligenza-artificiale/deep-learning-cose-e-quali-le-applicazioni/#:~:text=Oggi%20il%20deep%20learning%20è,generativa%20\(creazione%20testi%2C%20immagini%2C](https://www.bnova.it/intelligenza-artificiale/deep-learning-cose-e-quali-le-applicazioni/#:~:text=Oggi%20il%20deep%20learning%20è,generativa%20(creazione%20testi%2C%20immagini%2C)

⁴³⁹ Cfr. per l'origine di tale proposta classificatoria J.R. SEARLE, «Minds, Brains and Science», 3, in *Behavioral and Brain Sciences*, 1980, 3, 417 ss

⁴⁴⁰ La letteratura è vasta; cfr. ex multis, Cfr. T. CERQUITELLI-D. QUERCIA-F. PASQUALE (a cura di), *Transparent Data Mining for Big and Small Data*, Springer International, New York, 2017; J. BURRELL, «How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms», in *Big Data & Soc'y*, Jan.–June 2016, 1ss; J. A. KROLL, J. HUEY, S. BAROCAS, E. W. FELTEN, J. R. REIDENBERG, D. G. ROBINSON, H. YU, *Accountable Algorithms*, 165 Un. Pennsylvania L. R., 633ss. (2017); per le sue implicazioni giuridiche e più specificamente nella materia delle ADM, v. *amplius* cap. 3.

aumenta) l'incapacità dell'uomo di spiegare le cause di tali correlazioni, e dunque di decifrare, o ricostruire, i processi attraverso cui i sistemi algoritmici "arrivano a tali conclusioni"⁴⁴¹.

Tali rilievi hanno un impatto determinante sul profilo dell'"accuratezza" dell'analisi compiuta dalle macchine e, conseguentemente, sulla qualità della decisione finale, quando interamente o prevalentemente delegata alle macchine: l'attendibilità della decisione dipende strutturalmente, oltre che dalla qualità dei dati, dalla trasparenza dei processi che vi presiedono⁴⁴². Ed oggi, la decisione di una macchina, sempre più *opaca*, riguarda una persona umana, al contrario, sempre più *trasparente*⁴⁴³.

Questo tema ci introduce al terzo livello della *datification*: a tale ampia disponibilità dei dati, ed alla sempre più potente tecnologia che abbiamo descritto, corrisponde non solo l'automazione nel trattamento dei primi, bensì anche, incrementalmente, l'automazione delle decisioni che su tale trattamento si basano.

Premettendo che svolgeremo ampiamente le considerazioni sul contesto antropologico in cui si colloca l'attuale disciplina dei processi decisionali automatizzati nei prossimi capitoli, occorre già in questa sede individuare i principali attori coinvolti nel processo sin qui descritto, dotati di un "effettivo"

⁴⁴¹ V. ancora una volta D. Castlevecchi, «Can we open the black-box of AI?», cit., che spiega in modo chiaro in cosa consista l'opacità di cui stiamo parlando.

⁴⁴² Per le implicazioni giuridiche del fenomeno della *black box*, e più specificamente per i suoi riflessi sulla materia dei trattamenti automatizzati e delle decisioni basate su di essi, v. *amplius* cap. 3. Ma cfr. già da ora i fondamentali contributi di B.W. SCHERMER, «The limits of privacy in automated profiling and data mining», 27 *Computer law & security review*, 52 (2011); G. D'ACQUISTO, «Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati», in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., 285.; G. MALGIERI-G.COMANDÈ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», in *International Data Privacy Law*, vol. 7, Issue 4, 2017; E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black box society», cit.; R. MESSINETTI, «La privacy e il controllo dell'identità algoritmica», cit.

⁴⁴³ Cfr. S. RODOTÀ, «Il diritto di avere diritti», cit., p. 336

potere sui dati, perché di quei dati, insieme alle tecnologie suddette utili ad estrarvi valore, dispongono. Approssimando, si possono individuare due macro-tipologie di attori, che si confrontano nel dominio del campo in esame⁴⁴⁴.

Da una parte, come è emerso più volte nel corso della trattazione, campeggiano gli Stati sovrani, percorsi dalla crescente attitudine a piegare l'analisi dei dati al perseguimento degli interessi pubblici ad essi tradizionalmente affidati: su tutti, la tutela della sicurezza e dell'ordine pubblico, la prevenzione e repressione dei reati e, più di recente, la salute pubblica⁴⁴⁵. I fenomeni nel presente paragrafo descritti hanno infatti esponenzialmente aumentato la capacità di controllo (dei dati) dei cittadini e dei residenti da parte dei pubblici poteri nazionali. E se ciò rappresenta da una parte un prezioso strumento per implementare la razionalità delle politiche pubbliche, dall'altro rischia di sclerotizzare le tradizionali pretese di controllo sociale, fino alle frontiere della *mass surveillance*, per gli scopi suddetti (come hanno dimostrato gli scandali sui programmi di sorveglianza di massa sui quali ci siamo soffermati *retro*): il rapporto tra *privacy* individuale ed interessi pubblici si complica ulteriormente⁴⁴⁶.

⁴⁴⁴ Si v., a scopo introduttivo, il suggestivo quadro offerto da S. CALZOLAIO, «Protezione dei dati personali», cit., p. 602 ss.

⁴⁴⁵ Cfr. *ex multis* SIMONCINI, «Sovranità e potere nell'era digitale», in FROSINI, POLLICINO, APA, BASSINI, *Diritti e libertà in internet*, Milano, 2017, 19 ss., Cfr. F. FOCARELLI, *Privacy. Proteggere i dati personali oggi*, Bologna, 2015, che dedica il secondo capitolo del saggio proprio al tema dei “dati personali e sicurezza nazionale”; RUBECHI, «Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)», in *federalismi.it*, 23/2016; nello specifico campo della prevenzione e della repressione dei reati, DI NICOLA, ESPA, BRESSAN, DICKSON, NICOLAMARINO, *Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictive policing e moduli di data mining*, e-Crime Working papers, n. 2/2014; in punti di salute collettiva, anche in relazione alla recente pandemia globale da Covid-19, M. CIANCIMINO, *Protezione e controllo dei dati in ambito sanitario e Intelligenza Artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, Edizioni Scientifiche Italiane, Napoli, 2020, p. 7ss

⁴⁴⁶ Cfr. anche, come contributo ricco di riferimenti, BONINI, «Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti “violabili” in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea», *Rivista AIC*, n. 3/2016.

Ancor più rilevante, tuttavia, perché qualificante tutto il dibattito filosofico prima ancora che giuridico sull'attuale assetto dei poteri cui è soggetto l'individuo⁴⁴⁷, è l'altra grande tipologia di attori, i quali inverno appaiono come i maggiori protagonisti della *datification*: il settore privato, e nel suo ambito le imprese che operano nel settore delle ICTs⁴⁴⁸. Tra questi, accanto agli *internet service providers* (o ISP, anche denominati *gatekeepers* della rete internet), che arricchiscono progressivamente l'infrastruttura della rete⁴⁴⁹, si collocano ormai pressoché tutte le aziende che sviluppano strategia di analisi dei dati per finalità di miglioramento del prodotto e dei servizi e di marketing aziendale e commerciale, anche per conto di terze aziende⁴⁵⁰. Soggetti che possono accedere (e crescere grazie) all'enorme mole di dati "ceduti", consapevolmente o meno, dai propri clienti o scambiati con terze parti; e i più importanti tra i quali, data la propria consistenza patrimoniale, l'eterogeneità dei servizi e la dimensione

⁴⁴⁷ Cfr. le note di P. STANZIONE, «Introduzione», in ID., *I poteri privati delle piattaforme*, cit., p. 1 ss.

⁴⁴⁸ La letteratura è amplissima. Molti contributi sono già stati citati, ma si v. anche ex multis, a titolo introduttivo e in quanto densi di riferimenti, VANNUCCHI, «Internet e le dinamiche dei ruoli degli OTT (Over The Top) e Telco nel panorama ICT», in *Mondi digitale*, n. 5/ 2015, consultabile qui: <http://mondodigitale.aicanet.net/>; V. MAYER SCHONBERG - K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Garzanti, Milano, 2013, 103 ss.; F. PASQUALE, *The black-box society. The secret Algorithms that control money and information*, cit.; S. ZUBOFF, *Il capitalismo della sorveglianza*, cit.; P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme*, cit.;

⁴⁴⁹ TADDEO-FLORIDI, «New civic responsibilities for online service providers», in *The Responsibilities of Online Service Providers*, (a cura di) TADDEO-FLORIDI, Springer, 2017, spec. 1-5; cfr. anche E. Garzonio, «Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social», in *Media Laws*, 2019, p. 190 ss., https://iris.uniroma1.it/retrieve/handle/11573/1275266/1239197/Garzonio_responsabilità-degli-ISP_2019.pdf

⁴⁵⁰ MCAFEE, BRYNJOLFSSON, *Big data: the management revolution*, cit., 60; Cfr. F. DI PORTO (a cura di), «Big data e concorrenza», in *CeM*, n. spec. 23/2016, 5 ss.; A. G. PARISI, «Dati, proliferazione e social network: l'emersione di un nuovo modello giuseconomico», in *I "poteri privati" delle piattaforme*, (a cura di) P. Stanzone, cit., p. 173 ss.

transnazionale dell'offerta, sono riconducibili alla composita categoria degli *Over The Top* (OTT: ad es. Google, Meta, X, Amazon, Microsoft, Netflix ecc.)⁴⁵¹.

Ebbene, tanto i pubblici poteri, per ragioni di interesse pubblico e di razionalizzazione delle proprie politiche, quanto i privati, per ragioni o in occasione della propria attività economica, *raccolgono, conservano e trattano* l'enorme mole dei dati di cui abbiamo parlato *ricorrendo* alle discusse tecnologie: e, pertanto, all'automazione e (ormai) all'apprendimento automatico della macchina sia sotto il profilo del trattamento che, sempre più, di quello decisionale (*algorithmic decision making*)⁴⁵². Come avremo modo di evidenziare nei prossimi capitoli, pressoché tutti i processi di *decision making*, interamente algoritmici o meno, implementati da tali soggetti si basano oggi prevalentemente sulla *profilazione*⁴⁵³: operazione che, riprendendo solo a titolo introduttivo la puntuale definizione fornita dal GDPR, consiste in « qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità,

⁴⁵¹ Per una definizione, cfr. VANNUCCHI, «Internet e le dinamiche dei ruoli degli OTT (Over The Top) e Telco nel panorama ICT», in *Mondi Digitali*, cit.; Il termine OTT è utilizzato «per evidenziare che i molteplici servizi da essi forniti sono “disgiunti” dal trasporto dei dati e si “appoggiano” alle reti IP degli operatori di telecomunicazioni (“Telco”). Essi operano pertanto «al di sopra» delle Reti ed il modello di business che li caratterizza permette loro di mantenere la completa esclusività dei contenuti inviati e dei relativi copyright».

⁴⁵² Cfr. R. MESSINETTI, «La privacy e il controllo dell'identità algoritmica», cit., p. 125 ss.; S. CALZOLAIO, «Protezione dei dati personali», cit., p. 599; MALGIERI, G. COMANDÈ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», in *International Data Privacy Law*, vol. 7, Issue 4, 2017; cfr. poi ancora le fondamentali riflessioni di S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 323 ss.

⁴⁵³ Cfr. E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black-box society», cit., p. 1032 ss.; F. KALTHEUNER, E. BIETTI, «Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR», in *Journal of Information Rights Policy and Practice*, 2018, p. 1 ss.; A. G. PARISI, «Dati, proliferazione e social network: l'emersione di un nuovo modello giuseconomico», cit., p. 181 ss.

il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»⁴⁵⁴. Avremo modo di soffermarci sulla definizione più avanti, ma occorre sin d'ora sottolineare che tale operazione, anche dove non interamente automatizzata, si “nutre” delle informazioni che si riferiscono alla singola persona, poiché costituiscono la base per generare un profilo dell'individuo, della famiglia (in senso economico) cui appartiene, del gruppo di suoi simili, e di molto altro; e, così, per *personalizzare* la decisione (provvedimento amministrativo o annuncio pubblicitario che sia) rispetto al singolo soggetto destinatario⁴⁵⁵. Per ciò stesso, tale operazione non può che fondarsi sul *data mining* e sulla tecnica, al suo interno implementata, di *Knowledge Discovery Database*⁴⁵⁶.

A questo punto della nostra analisi, apparirà sufficientemente chiaro che, se da una parte la fonte del dato non è attendibile, e se dall'altra l'analisi algoritmica, e pertanto il trattamento del dato, risulta *opaco*, non decifrabile, allora anche il *profilo comportamentale* che ne scaturisce risulta potenzialmente viziato:

⁴⁵⁴ V. art. 4, par. 1, n. 4, Regolamento (UE) 2016/679 (GDPR); a dimostrazione dell'importanza di tale *species* di trattamento, il Regolamento, al fine di meglio specificarne l'ambito di applicazione materiale, rubrica il fondamentale art. 22 «processi decisionali interamente automatizzati *compresa* la profilazione».

⁴⁵⁵ Cfr. già da ora le importanti pagine dedicate a questa *species* di trattamento dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI nelle fondamentali *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679*, 3 ottobre 2017, p. 7 ss., su cui avremo modo di soffermarci ampiamente nel prossimo capitolo. Cfr. anche, ex multis F. LA GIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *federalismi.it*, n. 11/2020, p. 11 ss.; D.K. CITRON, F. PASQUALE, «The Scored Society: Due Process for Automated Predictions», in *Washington Law Review*, 2014, 89, 1 ss.; T. ZARSKY, «Understanding Discrimination in the Scored Society», in *Washington Law Review*, 2014, 89, 1375 ss;

⁴⁵⁶ Cfr. J. BURREL, «How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms», in *Big Data & Soc’y*, Jan.–June 2016, 1ss.; CALO, «Artificial Intelligence Policy: a Primer and Roadmap», in 51 *Univ. California D. L. Rev.*, 421 (2017); ma cfr. soprattutto WITTEN, FRANK, HALL, PAL, *Data Mining. Practical Machine Learning Tools and Techniques*, Morgan Kaufmann-Elsevier, 2017, 6, in cui tra l'altro si chiarisce che l'attività di “estrazione” di dati (*data mining*) attraverso un sistema di machine learning può svilupparsi in due modi: come in una *black-box*, in cui le correlazioni fra dati non sono comprensibili, e come in una *transparent box* ove il procedimento di correlazione fra i dati analizzati è osservabile.

e se su di esso si basa una decisione *altrettanto* automatizzata, anche l'attendibilità di quest'ultima risulterà consequenzialmente compromessa. Peraltro, proprio per denunciare la dimensione problematica del fenomeno in questione è stata coniata la suggestiva espressione *black-box society*, che individua tra i connotati caratterizzanti della nostra contemporaneità proprio il rapporto critico tra crescente utilizzo delle informazioni personali e persistente ignoranza dei processi che vi presiedono: «*we can observe [their] inputs and outputs, but we cannot tell how one becomes the other*»⁴⁵⁷.

Il tema risulta, pertanto, di stringente attualità e fondamentale intrecciato a quello della “sovranità su di sé”, che (l'abbiamo ampiamente sottolineato fino ad ora) individua come presupposti proprio l'immunità della propria sfera privata e la libertà di autodeterminazione informativa: la profilazione, infatti, svelando le attitudini e “scommettendo” *predittivamente* sulle preferenze, sui comportamenti e sulle performance dell'individuo, condiziona (avendo a mente il dettato dell'art. 2 della nostra Costituzione) lo svolgimento della sua personalità «sia come singolo, sia nelle formazioni sociali». Essa pretende di ridurre l'irriducibile: e così, le decisioni adottate sulla sua base, a maggior ragione quando non “filtrate” razionalmente dall'uomo, possono incidere profondamente sulle libertà e sui diritti dell'interessato. Solo per citare alcuni dei rischi esistenti, tali decisioni possono infatti segregare le persone in specifiche categorie riducendo la loro possibilità di scelta, o consolidare stereotipi⁴⁵⁸.

⁴⁵⁷ La fortuna espressione e la citazione sono di F. PASQUALE, *The Black-Box Society. The Secret Algorithms that Control Money and Information*, cit., p. 3.

⁴⁵⁸ Si rinvia subito, ancora una volta, alle lucide considerazioni svolte dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato*, cit., p. 5 ss., su cui avremo modo di soffermarci ampiamente nel prossimo capitolo. Cfr. già sul punto B. MITTLESTADT, «From Individual to Group Privacy in Big Data Analytics», in *Philosophy & Technology*, 2017, 30, 4, 475 ss.; 90 B. GOODMAN, S. FLAXMAN,

Emerge quindi la centralità, ed anzi la vocazione sociale, della regolazione giuridica del trattamento dei dati personali nella società dell'informazione, o della "sorveglianza liquida", o della *black-box*, che dir si voglia. E, nel suo ambito, l'implementazione della specifica disciplina dell'impiego dell'automazione (nel suo trionfo macchine-algoritmi-IA) nel trattamento stesso; e, ancora più nello specifico, nei processi di *decision making* che sull'*output* del trattamento si basano.

La disciplina in questione illumina, ancora una volta, il nesso che intercorre tra *privacy*, società e tecnologia. E, soprattutto, la funzione sociale dei diritti che la dimensione più intima dell'uomo, e la sua capacità di autodeterminarsi nelle proprie scelte esistenziali, presidiano. Per dirla, ancora una volta, con Stefano Rodotà: «Senza una forte tutela delle informazioni che le riguardano, le persone rischiano sempre di più d'essere discriminate per le loro opinioni, credenze religiose, condizioni di salute: la *privacy* si presenta così come un *elemento fondamentale della società dell'eguaglianza* (...) Senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo. Diventa così evidente che: la *privacy* è uno *strumento necessario per difendere la società della libertà*, e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale (...) la *privacy* si specifica così come una *componente ineliminabile della società della dignità*: parola, questa, scritta all'inizio della Costituzione tedesca proprio come reazione alla logica nazista e che, oggi, apre la Carta dei diritti fondamentali dell'Unione europea»⁴⁵⁹.

«EU regulations on algorithmic decision-making and a "right to explanation"», in *AI magazine*, 83, 3 ss.; G. DE GREGORIO, R. TORINO, «Privacy, tutela dei dati personali e Big Data», cit., p. 475 ss.

⁴⁵⁹ S. RODOTÀ, *Privacy, libertà, dignità*, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati del 16 settembre 2004, Wroclaw, Polonia, 14, 15, 16

Oggi, la difesa dignità della persona umana risulta in primo luogo affidata alla tutela del diritto alla protezione dei dati personali *rispetto* ai trattamenti e ai processi decisionali algoritmici. Per questo motivo bisogna occuparsene, a maggior ragione nei due ordinamenti sociali che costituiscono, rispettivamente, uno dei più grandi consumatori di ICTs e al contempo produttore di dati (l'Europa) e uno dei principali ideatori e produttori di *devices* e delle stesse ICTs (gli U.S.A.) del mondo. E per questo motivo bisogna interrogarsi sull'effettiva idoneità della disciplina vigente a salvaguardare la dignità della persona umana, e la libertà di autodeterminazione che ne rappresenta il presupposto. Sarà il nostro obiettivo nei prossimi due capitoli.

settembre 2004, consultabile qui: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293> .

CAPITOLO TERZO

IL TRATTAMENTO AUTOMATIZZATO DEI DATI PERSONALI: LA DISCIPLINA EUROPEA

SOMMARIO: 3.1. Contesto giuridico: il GDPR nel quadro dell'Agenda Digitale Europea – 3.1.1. Il Regolamento Generale sulla Protezione dei Dati, tra tutela della persona fisica e sviluppo del Mercato Unico Digitale. Le motivazioni giuridiche – 3.1.2. Ambito di applicazione, definizioni generali e principi di protezione dei dati: risk-based approach e autodeterminazione informativa – 3.1.3. Accountability, privacy by design e privacy by default. I nuovi istituti del GDPR nella società delle ICTs – 3.2. Il trattamento automatizzato dei dati personali: la disciplina del GDPR alla luce delle linee guida del Gruppo di Lavoro 29 – 3.2.1. Trattamento automatizzato, profilazione e processi decisionali automatizzati: definizioni essenziali – 3.2.2. Le disposizioni generali: principi, basi giuridiche e diritti dell'interessato – 3.2.3. Processi decisionali interamente automatizzati, compresa la profilazione: l'art. 22, par. 1 e i nodi interpretativi – 3.2.4. Le eccezioni al divieto generale e le "misure appropriate" per tutelare i diritti dell'interessato. Right to explanation: essere o non essere? – 3.2.5. La sentenza del 7 dicembre 2023 della Corte di Giustizia nel caso SCHUFA (e i suoi precedenti nazionali): il leading case europeo in materia di processi decisionali interamente automatizzati – 3.3. Uno sguardo all'Italia. La trasparenza algoritmica nella giurisprudenza della Corte di Cassazione e del Consiglio di Stato – 3.3.1. Orientamenti fondamentali del Garante per la Protezione dei Dati Personali in materia di trattamenti algoritmici: dal caso Mevaluate al provvedimento del 7 luglio 2022 in materia di pubblicità personalizzata nei confronti di Tik Tok

3.1. Contesto giuridico: il GDPR nel quadro dell'Agenda Digitale Europa

Nel presente capitolo si scandaglierà nel merito la disciplina dettata dal legislatore europeo in punto di trattamenti automatizzati dei dati personali, sia in generale sia in relazione ai c.d. processi decisionali interamente automatizzati, fattispecie attualmente oggetto di specifica regolamentazione, di cui si affronteranno i principali nodi interpretativi. Dopo aver delineato, in chiave comparatistica, un sintetico quadro delle normative di adeguamento adottate da alcuni singoli Stati membri al fine di implementare, nei limiti in cui consentito, la disciplina di derivazione eurounitaria, ci si soffermerà su alcune applicazioni di quest'ultima nella giurisprudenza: in tale contesto, accanto alla doverosa attenzione rivolta all'attività della Corte di Giustizia si adotterà un punto di vista più squisitamente "interno", indagando i più recenti approdi della giurisprudenza di legittimità e analizzando alcune importanti decisioni dell'Autorità Garante nell'ambito dell'ordinamento italiano.

La fonte della disciplina attualmente vigente nella materia che qui ci occupa si rintraccia, come già anticipato, nel più volte citato Regolamento UE 2016/679 (GDPR). Si anticipa già che, nell'analisi della disciplina medesima, si seguirà la struttura argomentativa fatta propria dal Gruppo di Lavoro Articolo 29 (c.d. WP29), oggi sostituito dall'*European Data Protection Board* (c.d. EDPB) nelle fondamentali Linee Guida in materia di processi decisionali automatizzati relativi alle persone fisiche, adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018, alle quali si farà riferimento costante⁴⁶⁰. Queste ultime, nel contesto del GDPR,

⁴⁶⁰ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del*

limpidamente individuano un *corpus* di disposizioni generali, applicabile a qualsiasi trattamento ricadente nell’ambito di applicazione, *rationae personae* e *ratione materiae*, del regolamento (compresi, dunque, i trattamenti parzialmente o totalmente automatizzati); e, in parallelo, un sub-sistema di norme specificamente riguardante la cruciale categoria dei processi decisionali *interamente* automatizzati *compresa la profilazione*, in una certa misura derogatorio del primo⁴⁶¹.

A breve, considereremo l’articolato sistema in questione nel dettaglio. Prima, tuttavia, appare necessario aggiungere alcune indicazioni sul contesto culturale, politico e giuridico in cui è venuto germogliando lo stesso GDPR, poiché di esso risente l’“anima” della disciplina che andremo ad esaminare. Al contempo, si individueranno i principi che informano l’articolato normativo in questione, e si ricostruiranno i caratteri essenziali di quest’ultimo (segnatamente, evidenziando il binomio tra tutela della dimensione dinamica della *privacy* e approccio *risk-based*).

Come già ricordato nel capitolo precedente, il *General Data Protection Regulation* rappresenta una delle principali misure implementate dalle istituzioni normative dell’Unione Europea ai fini dell’attuazione del Pacchetto Protezione Dati, compreso nella c.d. “Agenda Digitale Europea”, strategia promossa dall’Unione con un’apposita comunicazione successivamente all’entrata in vigore del Trattato di Lisbona⁴⁶². Essa rappresenta, a propria volta, una delle sette

regolamento 2016/679, WP 251 rev.01, adottate il 3 ottobre 2017 (versione emendata e adottata in data 6 febbraio 2018). V. ampiamente *infra*.

⁴⁶¹ Ivi, p. 9.

⁴⁶² V. *retro*, cap. 2, par. 2.2.4. Ci si riferisce alla già citata COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo, al Consiglio delle Regioni. Un’agenda digitale europea*, COM(2010)245 definitivo, Bruxelles 19 maggio 2010, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52010DC0245>. Per le considerazioni che seguiranno, cfr.

“iniziative faro” nel quadro della più ampia, olistica strategia “Europa 2020”, lanciata dall’Unione nel marzo 2010 per un periodo di dieci anni con l’intento di uscire dalla crisi conseguita al crollo finanziario del biennio 2007-2008 e di trasformare l’economia europea in un’«economia intelligente, sostenibile e inclusiva caratterizzata da alti livelli di occupazione, produttività e coesione sociale»: in poche parole, in un’economia di mercato sociale nella prospettiva dell’integrazione europea⁴⁶³.

In questo quadro, l’Agenda mirava a stabilire il ruolo chiave delle tecnologie dell’informazione e della comunicazione (ICTs, o anche TIC in italiano), e in special modo di internet, nel perseguimento degli obiettivi prefissati dall’Unione, massimizzando il potenziale economico e sociale insito nelle medesime⁴⁶⁴. Le intenzioni dell’Unione erano chiare sin dall’incipit del documento: «Lo scopo generale dell'agenda digitale europea è ottenere vantaggi socioeconomici sostenibili grazie a un mercato digitale unico basato su internet veloce e superveloce e su applicazioni interoperabili»⁴⁶⁵. Dunque, costruire un mercato unico digitale, rimuovendo tuttavia i molteplici ostacoli disseminati

principalmente C. RATCLIFF, M. WOSKYA, B. MARTINELLO, D. FRANCO, «L’Agenda Digitale Europea», cit.

⁴⁶³ Cfr. COMMISSIONE EUROPEA, *Europa 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM(2010) 2020, marzo 2010 p. 3 ss. <https://ec.europa.eu/eu2020/pdf/COMPLET%20IT%20BARROSO%20-%20Europe%202020%20-%20IT%20version.pdf>

⁴⁶⁴ Ricordiamo che l'agenda del digitale si basa sui risultati di estese consultazioni, in particolare sui contributi della Relazione sulla competitività digitale in Europa 2009, COM(2009)390, sulla consultazione pubblica della Commissione sulle priorità future nel settore delle TIC (2009); inoltre, essa trova un precedente negli studi e nelle comunicazioni della Commissione Europea degli anni Novanta in materia di commercio elettronico, in cui già si sottolineava la centralità delle comunicazioni e delle transazioni elettroniche e la necessità di rafforzare la fiducia del consumatore, anche attraverso la protezione dei dati personali, per favorire lo sviluppo del mercato: cfr. ad es. COMMISSIONE EUROPEA, *Comunicazione della Commissione delle Comunità europee al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, Un’iniziativa europea in materia di commercio elettronico*, COM(97) 157, 15 aprile 1997.

⁴⁶⁵ Cfr. COMMISSIONE EUROPEA, *Un’agenda digitale europea*, cit., p. 3.

lungo il percorso. Tra questi, come si legge chiaramente nell'atto, accanto alla mancanza di interoperabilità tra le amministrazioni pubbliche, alla mancanza di investimenti nelle reti ed alla carente alfabetizzazione digitale dei "cittadini europei", si stagliava la già denunciata «frammentazione dei mercati digitali», e segnatamente del quadro normativo di riferimento vigente in ciascuno degli Stati membri⁴⁶⁶. Come abbiamo già avuto modo di sottolineare, all'esito dell'iter di "costituzionalizzazione europea" del diritto alla protezione dei dati personali, si mostrava salda la certezza di dover declinare nell'ambito dell'economia digitale, e in modo *uniforme* nei diversi Stati membri, i principi consacrati nella Carta di Nizza, e dunque di dover tutelare la persona fisica nel godimento dei suoi diritti fondamentali. Tale visione antropocentrica pare emergere chiaramente dal bilanciamento tra interesse all'autodeterminazione informativa, non più strumentale bensì primario, ed interesse alla libera circolazione dei dati personali che informa il GDPR e la contestuale Direttiva 2016/680.

Nel 2015 interveniva poi la c.d. "strategia per il mercato unico digitale" che sviluppava ulteriormente l'Agenda, stabilendo disposizioni specifiche strumentali ad edificare un ambiente digitale equo, aperto e sicuro, migliorando l'accesso dei consumatori e delle imprese ai beni e ai servizi digitali in tutta l'Europa e creando un contesto favorevole affinché internet, reti e servizi digitali potessero svilupparsi, esprimendo a pieno le proprie potenzialità⁴⁶⁷.

⁴⁶⁶ Ivi, p. 6, dove a chiare lettere la Commissione afferma che «L'Europa è tuttora un mosaico di mercati online nazionali e alcuni problemi, seppur risolvibili, impediscono ai cittadini di beneficiare dei vantaggi di un mercato digitale unico. I contenuti e i servizi commerciali e culturali devono poter superare i confini, cosa possibile eliminando le barriere normative (...) rafforzando la fiducia dei consumatori. Si può e si deve fare di più nell'ambito del quadro normativo vigente per creare un mercato unico nel settore delle telecomunicazioni».

⁴⁶⁷ Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, 6 maggio 2015, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015DC0192>.

Il sistema normativo che è scaturito dalla strategia decennale in questione, tutt'ora per la maggior parte vigente, ha pertanto perseguito l'obiettivo di massimizzare la libertà di circolazione di beni e servizi di natura digitale, e ancor prima dell'informazione che della nuova *data driven economy* rappresenta il "petrolio", dotando al contempo l'UE di un sistema avanzato in materia di diritti degli utenti e protezione dei consumatori e delle imprese. Avendo già nel capitolo precedente richiamato i principali atti normativi di cui si compone, sottolineando la centralità del GDPR, della dir. 2016/680 e del reg. eIDAS, ci limitiamo qui ad individuare solo alcune delle altre sue articolazioni. Certamente, è necessario ricordare la normativa che reca modifica alle previgenti legislazioni in materia di comunicazioni elettroniche per massimizzare la tutela dei consumatori-interessati, ossia la Direttiva 2009/136/CE ⁴⁶⁸ ; il Regolamento UE 2018/881 sulla cbersicurezza, che rafforza l'Agenzia dell'Unione europea per la cbersicurezza (ENISA) e istituisce un quadro per la certificazione della *cybersecurity* di prodotti e servizi⁴⁶⁹; l'importante normativa sull'apertura dei dati (c.d. *Open Data*) nella disponibilità del settore pubblico, ossia la Direttiva UE 2019/1024, che stabilisce norme comuni per un mercato europeo dei dati in possesso dei governi⁴⁷⁰; e infine

⁴⁶⁸ Cfr. Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori; OJ L 337, 18.12.2009, p. 11–36; <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009L0136>

⁴⁶⁹ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cbersicurezza, e alla certificazione della cbersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cbersicurezza»), GU L 151 del 7.6.2019, pagg. 15–69; <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881> .

⁴⁷⁰ Cfr. Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, GU L 172 del 26.6.2019, pagg. 56–83, <https://eur-lex.europa.eu/legal->

il fondamentale Regolamento UE 2018/1807 sulla libera circolazione dei dati non personali, che consente alle imprese e alle amministrazioni pubbliche di archiviare e trattare i dati non personali ovunque scelgano di farlo nell'UE⁴⁷¹.

Attualmente, il quadro sopra descritto è stato integrato dalla nuova, o seconda, Agenda Digitale Europea, predisposta per il decennio 2020-2030 e incentrata sui profondi cambiamenti introdotti dalle tecnologie digitali, sul ruolo essenziale svolto dai servizi e dai mercati digitali e sulle nuove ambizioni dell'UE in campo tecnologico e geopolitico ⁴⁷². Essa è stata inizialmente delineata attraverso la comunicazione strategica della Commissione Europea, intitolata «Plasmare il futuro digitale dell'Europa» ⁴⁷³, e il più generale programma

[content/IT/TXT/PDF/?uri=CELEX:32019L1024](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L1024); secondo una comune definizione, accreditata in ambito internazionale, gli Open Data consisterebbero in quei dati resi disponibili (da soggetti pubblici o da privati) con le caratteristiche tecniche e legali necessarie per essere liberamente utilizzati, riutilizzati e ridistribuiti da chiunque, in qualsiasi momento e ovunque: cfr. ad es. il sito istituzionale dell'International Data Character, <https://opendatacharter.net>. Per un approfondimento in materia, legato alla tematica dei Big Data cfr. F. FAINI, «Dati, algoritmi e Regolamento europeo 2016/679», in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, A. Mantelero, D. Poletti (a cura di), Pisa University Press, 2018, pp. 333-348; in part. v. p. 345 in cui l'autrice afferma: «L'apertura dei Big Data potrebbe contribuire a sanare, insieme alla trasparenza, le asimmetrie informative, mettendo a disposizione della collettività i dati, anche se inevitabilmente provocherebbe una perdita di potere per i titolari degli stessi».

⁴⁷¹ Cfr. Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, GU L 303 del 28.11.2018, pagg. 59-68, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1807>. Per un'analisi circa la crescente rilevanza dei dati non personali, quali dati anonimizzati e dati industriali o *a-personali*, delle ragioni e della struttura della normativa in questione e del suo rapporto con la disciplina del GDPR, cfr. G. Di Filippo, «I dati come beni giuridici», cit., p. 46 ss.

⁴⁷² Cfr. C. RATCLIFF, M. WOSKYA, B. MARTINELLO, D. FRANCO, «L'Agenda Digitale Europea», cit., p. 3 ss.

⁴⁷³ Cfr. COMMISSIONE EUROPEA, *Communication: Shaping Europe's digital future*, Febbraio 2020, https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future-feb2020_en.pdf&prefLang=it.

strategico intitolato «Il decennio digitale europeo»⁴⁷⁴. In esse, la Commissione ha definito le azioni specifiche che intende intraprendere per contribuire alla creazione di mercati e servizi digitali sicuri e per rafforzare ulteriormente l'esistente sistema di protezione dei dati: tra le priorità per l'attuale decennio, figurano inoltre lo sviluppo della computazione quantistica, l'implementazione di una politica commerciale basata sulla *blockchain*, lo sviluppo di sistemi di intelligenza artificiale antropocentrici e affidabili, il 5G e il 6G e la *cybersecurity*⁴⁷⁵.

Inoltre, il 9 marzo 2021 la Commissione ha ulteriormente integrato la strategia presentando la decennale c.d. «Bussola per il digitale 2030: il modello europeo per il decennio digitale»: comunicazione che, tra i nuovi e più precisi obiettivi digitali posti dall'Unione, individua l'alfabetizzazione e la professionalizzazione digitale della più gran parte della popolazione adulta europea, l'ampia diffusione di ICTs, e segnatamente dei sistemi di *cloud computing*, *Big Data analytics* e Intelligenza Artificiale, tra le imprese, la costruzione di infrastrutture Gigabit e di una copertura 5G che raggiungano tutte

⁴⁷⁴ Cfr. COMMISSIONE EUROPEA, *Decennio digitale europeo: obiettivi digitali per il 2030*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it.

⁴⁷⁵ Cfr. in particolare la pagina tematica del sito istituzionale della Commissione Europea dedicata alla c.d. strategia *blockchain*, <https://digital-strategy.ec.europa.eu/it/policies/blockchain-strategy>, in cui si legge tra l'altro che: «La Commissione riconosce l'importanza della certezza del diritto e di un regime normativo chiaro nei settori relativi alle applicazioni basate su blockchain. Attualmente sta sviluppando un quadro giuridico favorevole all'innovazione nei settori delle risorse digitali (tokenizzazione) e dei contratti intelligenti (*smart contracts*), che tuteli i consumatori e fornisca certezza giuridica alle imprese». Sinteticamente, con l'espressione *blockchain* ci si riferisce a quella tecnologia basata su un registro di contabilità condiviso e immutabile che facilita il processo di registrazione delle transazioni e la tracciabilità degli asset in una rete commerciale: asset che può essere indifferentemente tangibile (qualsiasi bene mobile o immobile, compreso ovviamente il denaro) o intangibile (proprietà intellettuale, brevetti, copyright, branding ecc.). Cfr. la definizione reperibile sulla pagina dedicata del sito internet di IBM, <https://www.ibm.com/it-it/topics/blockchain>. Per un approfondimento, cfr. P. CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in NGCC, 2017, 107ss.

le famiglie europee, nonché la disponibilità online della più gran parte dei servizi pubblici (resi accessibili attraverso l'utilizzo dell'identità elettronica) ⁴⁷⁶.

Per finanziare nel suo complesso la seconda Agenda Digitale, l'Europa ha istituito con il Regolamento UE 2021/694 il c.d. Programma Europa Digitale, programma di finanziamento con una dotazione complessiva pari a 7,5 miliardi di euro per il periodo 2021-2027, destinato ad essere integrato da altri programmi, tra i quali particolare rilievo assume il c.d. Dispositivo per la Ripresa e la Resilienza (istituito dal Regolamento UE 2021/241) implementato dall'Unione nel quadro dell'ampio *economic recovery package* approntato in conseguenza della pandemia da SARS-CoV-2, denominato Next Generation EU ⁴⁷⁷. Ciò, pertanto, a dimostrazione della centralità assunta dall'Agenda, in risposta al processo di *datificazione* della realtà socioeconomica contemporanea sopra ampiamente descritto, nell'ambito delle politiche economiche e commerciali dell'Unione.

⁴⁷⁶ Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM/2021/118 final, 9 marzo 2021, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021DC0118>.

⁴⁷⁷ Cfr. Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240, GU L 166 dell' 11.5.2021, pagg. 1–34, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021R0694>. Sull'istituzione del fondo, pari in valore a 750 miliardi, per la ripresa dell'Unione post pandemia, strumento noto come *Next Generation EU* o come *Recovery Plan*, cfr. gli atti normativi (non legislativi) con cui sono stati adottato il quadro finanziario pluriennale 2021-2027 e lo strumento in questione: Regolamento (UE, Euratom) 2020/2093 del Consiglio del 17 dicembre 2020 che stabilisce il quadro finanziario pluriennale per il periodo 2021-2027; Regolamento (UE) 2020/2094 del Consiglio del 14 dicembre 2020 che istituisce uno strumento dell'Unione europea per la ripresa, a sostegno alla ripresa dell'economia dopo la crisi COVID-19. Sull'istituzione, più nello specifico, del “Dispositivo per la ripresa e per la resilienza”, cfr. poi Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, GU L 57 del 18.2.2021, pagg. 17–75, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021R0241>

Concludiamo sottolineando come l'attuale strategia decennale si fondi su tre pilastri portanti, tra loro profondamente interconnessi, a ciascuno dei quali corrisponde l'adozione di taluni degli strumenti normativi cui abbiamo sinteticamente fatto cenno.

Da una parte si colloca l'Intelligenza Artificiale, disciplina e insieme fenomeno che l'Unione ritiene capace di svolgere nei prossimi anni un ruolo centrale nel processo di crescita dell'economia digitale, e del relativo mercato unico, apportando numerosi benefici sociali ed economici tanto nel settore pubblico quanto nel settore privato, a fronte tuttavia della già denunciata serie di rischi riguardanti la vita privata, l'autodeterminazione informativa e più in generale gli attributi fondamentali della persona umana: a questo proposito, la Commissione ha adottato nel febbraio 2020 il c.d. Libro Bianco sull'Intelligenza Artificiale (atto, al pari delle suddette comunicazioni, di *soft law*), in cui si afferma a chiare lettere: «Dato l'impatto significativo che l'intelligenza artificiale può avere sulla nostra società e la necessità di creare maggiore fiducia, è essenziale che l'IA europea sia fondata sui nostri valori e diritti fondamentali quali la dignità umana e la tutela della privacy»⁴⁷⁸. Su tale base, successivamente a talune importanti risoluzioni del Parlamento Europeo sull'IA riguardanti l'etica, la responsabilità civile e la proprietà intellettuale, in cui veniva sottolineata l'importanza di un quadro giuridico europeo comune in materia ⁴⁷⁹, la

⁴⁷⁸ Cfr. COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final, 19 febbraio 2020, p. 2, <https://op.europa.eu/it/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1>; molte delle considerazioni ivi svolte dalla Commissione erano già contenute in alcune precedenti comunicazioni, come ad es. COMMISSIONE EUROPEA, *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa*, COM(2018) 237, 25 aprile 2018, 1.

⁴⁷⁹ Cfr. ad es. Parlamento Europeo, Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici

Commissione Europea ha presentato ad aprile 2021 la fondamentale, già citata proposta di Regolamento UE in materia di Intelligenza Artificiale, che per la prima volta sancisce nel diritto europeo una definizione di sistemi di IA neutra dal punto di vista tecnologico e predispone un corpus normativo fondato sul principio di precauzione (c.d. *risk-based approach*)⁴⁸⁰.

Inoltre, nel settembre 2022 la Commissione ha pubblicato una proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'Intelligenza Artificiale, per assicurare alle persone danneggiate da un sistema di IA un livello di protezione equivalente a quello riconosciuto dall'UE a fronte di danni cagionati dall'impiego di altre tecnologie⁴⁸¹; nonché una proposta relativa a una nuova Direttiva sulla responsabilità per danno da prodotti difettosi che, modificando la direttiva del 1985 in materia, è preordinata ad includere nel novero i nuovi prodotti digitali (come l'IA) e i prodotti dell'economia circolare⁴⁸².

L'altro pilastro consiste, ancora una volta, nella creazione di un mercato unico digitale più sicuro e aperto, che tuteli i diritti fondamentali degli utenti e crei condizioni di parità per le imprese. Il pacchetto comprende due iniziative

dell'intelligenza artificiale, della robotica e delle tecnologie correlate, Bruxelles, 20 ottobre 2020, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html#title1

⁴⁸⁰ COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*, COM/2021/206 final, 21 aprile 2021, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206>; il progetto di relazione alla proposta è stato pubblicato il 20 aprile 2022, ed è disponibile qui: https://www.europarl.europa.eu/doceo/document/CJ40-PR-731563_IT.pdf.

⁴⁸¹ Cfr. COMMISSIONE EUROPEA, *Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)*, COM/2022/496 final, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0496>.

⁴⁸² Cfr. COMMISSIONE EUROPEA, *Proposta di Direttiva del Parlamento Europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi*, COM/2022/495 final, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0495>.

legislative, di cui già abbiamo discusso e sulle quali torneremo talvolta a fare riferimento nel corso della trattazione, che mirano ad aggiornare le norme dell'UE in materia di servizi digitali: da una parte, il Regolamento sui Servizi Digitali, c.d. *Digital Services Act*, adottato il 19 ottobre 2022, che introduce norme uniformi in materia di responsabilità dei prestatori di servizi intermediari (denominati *gatekeepers*) e, in particolare, delle piattaforme online, quali i social media e i mercati online; e il Regolamento sui Mercati Digitali, c.d. *Digital Markets Act*, adottato il 14 settembre 2022 e deputato a garantire un più elevato livello di competitività per le imprese sui mercati (digitali europei) prevenendo (e reprimendo) eventuali abusi nell'esercizio della propria posizione economicamente dominante da parte degli OTT e più in generale delle grandi imprese del digitale⁴⁸³.

Infine, altro fondamentale asse portante della strategia è la condivisione dei dati, obiettivo ai fini del quale la Commissione nel febbraio 2020, unitamente al Libro Bianco sull'IA, ha lanciato la c.d. Strategia Europea dei Dati: concependo i dati quale imprescindibile volano per l'innovazione e per lo sviluppo economico, l'UE mira da una parte a implementare strategie di "liberalizzazione" dei dati non personali al fine di sviluppare nuove tecnologie e nuovi modelli imprenditoriali redditizi; e, dall'altra, a massimizzare ulteriormente l'equilibrio tra libera circolazione dei dati (segnatamente, personali) e tutela dei diritti e delle libertà fondamentali delle persone fisiche, già perseguito con il GDPR⁴⁸⁴. Ricade

⁴⁸³ Cfr. rispettivamente Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), GU L 277 del 27.10.2022, pagg. 1–102, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R2065>; e il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), GU L 265 del 12.10.2022, pagg. 1–66, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R1925>.

⁴⁸⁴ Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni*.

certamente sotto il primo profilo della strategia il Regolamento sulla governance dei dati - Regolamento (UE) 2022/868 - entrato in vigore a giugno 2023, che mira ad aumentare la disponibilità e la riutilizzabilità dei dati e la fiducia collettiva in tale processo⁴⁸⁵; mentre al secondo profilo è riconducibile la proposta della Commissione Europea, datata 26 gennaio 2022, di adozione di una dichiarazione solenne congiunta (a firma della Commissione stessa, del Parlamento Europeo e del Consiglio) denominata “Dichiarazione europea sui diritti e sui principi digitali”, preordinata a promuovere a livello politico una transizione digitale *antropocentrica* basata sui valori europei, specialmente su quelli consacrati in guisa di principi e di diritti fondamentali nella Carta fondamentale dei diritti dell’Unione Europea⁴⁸⁶.

Dopo aver finalmente tracciato l’essenziale fisionomia del contesto politico, economico e giuridico in cui si colloca, possiamo passare alla sintetica

Una strategia europea per i dati, COM(2020) 66 final, 19 febbraio 2020, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0066>.

⁴⁸⁵ Cfr. Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), GU L 152 del 3.6.2022, pagg. 1–44, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R0868>.

⁴⁸⁶ Cfr. Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, COM(2022) 27 final, 26 gennaio 2022, in cui (attestata la natura esclusivamente *politica* del documento) si legge tra l’altro a p.3: «(...) inoltre la crescente disponibilità di nuove tecnologie e dati digitali comporta anche rischi indesiderati che possono avere conseguenze di vasta portata per i cittadini, per i nostri valori democratici, per la nostra sicurezza o per le fondamenta delle nostre società. Tali rischi sono aumentati in modo significativo, anche per quanto riguarda le violazioni della vita privata e dei dati personali, la diffusione di contenuti illeciti e nocivi e di prodotti non sicuri, nonché (...) la sorveglianza di massa, le distorsioni algoritmiche che ostacolano l’accesso equo e non discriminatorio alle informazioni e al dibattito democratico e persino la censura vera e propria. Tali problemi colpiscono l’essenza dei diritti fondamentali e intaccano i progressi faticosamente conquistati in questo settore, sia nell’Unione europea, sia a livello internazionale» e ancora a p. 4 «in tale contesto la dichiarazione propone principi digitali al servizio di tutti gli europei, con particolare riguardo ai seguenti elementi: una trasformazione digitale che mette al centro le persone; solidarietà e inclusione; libertà di scelta; partecipazione allo spazio pubblico digitale; sicurezza, protezione e conferimento di maggiore autonomia e responsabilità; e sostenibilità».

analisi dei principi che ispirano l'atto normativo che ospita la disciplina dei processi decisionali automatizzato, e che per primo quel bilanciamento tra diritti fondamentali e libertà economiche, in chiave tuttavia autenticamente *antropocentrica*⁴⁸⁷, altrettanto centrale nell'attuale strategia europea dei dati, è riuscito a perseguire in materia di protezione dei dati relativi alle persone fisiche: il *General Data Protection Regulation*.

3.1.1. Il Regolamento Generale sulla Protezione dei Dati, tra tutela della persona fisica e sviluppo del Mercato Unico Digitale. Le motivazioni giuridiche

Come abbiamo avuto modo di rilevare ampiamente nel capitolo precedente, la *protezione dei dati personali*, successivamente all'adozione della Carta dei diritti fondamentali dell'Unione Europea (art. 8), all'entrata in vigore del Trattato di Lisbona che ad essa ha riconosciuto lo stesso valore giuridico dei Trattati Istitutivi (nuovo art. 6 TUE) ed ha introdotto una nuova, precisa base giuridica in materia all'art. 16 del TFUE, costituisce ormai pacificamente l'oggetto di un *diritto fondamentale della persona* codificato nell'ambito della dimensione ordinamentale europea.

Tale prospettiva è oggi ulteriormente rafforzata dal GDPR, ovvero dal Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei

⁴⁸⁷ Almeno per alcuni commentatori. V. subito *infra*.

dati)⁴⁸⁸. Quest'ultimo edifica un vero e proprio *ordinamento generale* sulla protezione dei dati personali nel contesto giuridico dell'Unione europea, sostituendo alla fonte di semplice *armonizzazione* della disciplina vigente nei singoli Stati membri, rappresentata per un ventennio dalla dir. 95/46/CE, una fonte di *unificazione* del diritto vigente in materia, consistendo la fonte regolamentare, ex art. 288 TFUE, in un atto recante norme *direttamente applicabili*, in tutti gli Stati membri dell'Unione Europea (necessitanti di attuazione, ai fini della loro efficacia interna, *solo* laddove incompiute nel loro contenuto dispositivo: e tutto ciò, in prima approssimazione, al fine di assicurare una maggiore tutela di un diritto fondamentale *non solo* per i cittadini europei, bensì per *tutti* gli individui che si trovano sul territorio dell'Unione, traducendo in disciplina positiva molti dei principi negli anni enunciati dalla vitale giurisprudenza della Corte di Giustizia, già in precedenza analizzata⁴⁸⁹.

A titolo introduttivo, si può subito osservare come sia stato sottolineato che il GDPR affianchi, ed anzi anteponga, all'approccio essenzialmente riparatorio

⁴⁸⁸ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GU L 119 del 4.5.2016, pagg. 1-88, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679>.

⁴⁸⁹ La letteratura specialistica che si è occupata del Regolamento UE 2016/679, e della ricostruzione sistematica della disciplina che ne scaturisce, è vastissima. Ai fini della presente trattazione, l'analisi e le riflessioni che seguiranno sono principalmente il distillato dei seguenti contributi; G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati», cit.; C. COLAPIETRO, «I principi ispiratori del Regolamento UE 2016/679 e la loro incidenza sul contesto normativo nazionale», in *federalismi.it*, n. 22/2018, 21 novembre 2018; S. CALZOLAIO, «Privacy by design. Principi, dinamiche, ambizioni del nuovo Re. Ue. 2016/679», in *federalismi.it*, n. 24/2017, 20 dicembre 2017; M. G. STANZIONE, «Il Regolamento europeo sulla privacy: origini e ambito di applicazione», in *Europa e Dir. Priv.*, IV/2016, 1249-1264; E. LUCCHINI GUASTALLA, «Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori», in *Contr. e impr.*, n. 1/2018, pp. 106-125. Per un'analisi complessiva e approfondita, cfr. i due volumi di F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, I (Dalla dir. 95/46 al nuovo regolamento europeo) e II (Il regolamento europeo 2016/679), Torino, 2016; e AA.VV., *La nuova disciplina europea della privacy*, (a cura di) S. Sica, V. D'Antonio e G.M. Riccio, Milano, 2016.

proprio della dir. 95/46/CE un modello di tutela *preventiva* (o anche *risk-based approach*) fondata sulla responsabilizzazione di tutti i soggetti coinvolti nel trattamento dei dati riguardanti la persona fisica, e pertanto sui “nuovi” principi fondamentali di *accountability*, di *privacy by design* e di *privacy by default*⁴⁹⁰. In questo senso, il Regolamento rovescerebbe l’approccio del precedente strumento normativo, adottandone uno basato sui (potenziati) doveri di informazione, di controllo e di *gestione del rischio* in capo al Titolare e al Responsabile del trattamento⁴⁹¹.

Prima di addentrarci nell’analisi di dettaglio, nei limiti in cui lo consente l’oggetto della presente trattazione, delle norme del Regolamento, occorre tentare di illuminare le ragioni che hanno condotto all’adozione della presente normativa, rivolgendoci a tal fine ai *considerando* che, come ampiamente sottolineato in dottrina, svolgono una fondamentale funzione di indirizzo interpretativo delle disposizioni del Regolamento custodendo i principi che ispirano il sistema normativo configurato dall’atto e dunque la *motivazione giuridica*⁴⁹²: e tale ruolo è stato più volte ribadito dalla Corte di Giustizia che, nel sottolineare più in generale l’indissolubilità del legame sussistente tra atti dell’Unione e loro preambolo, ha affermato: «Il dispositivo di un atto dell’Unione è indissociabile dalla sua motivazione e deve essere interpretato, se necessario, tenendo conto dei motivi che hanno portato alla sua adozione»⁴⁹³.

⁴⁹⁰ Cfr. M.G. STANZIONE, «Genesi e ambito di applicazione», in S. Sica, V.D’Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, p. 21; S. CALZOLAIO, «Protezione dei dati personali», cit., p. 626 ss.

⁴⁹¹ Cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 153 ss

⁴⁹² Cfr. in particolare Cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., 8 s.; e M.G. STANZIONE, «Genesi e ambito di applicazione», in S. Sica, V.D’Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., p. 24, nota 29.

⁴⁹³ Cfr. C. Giust. Ue, procedimenti riuniti C-509/09 (*eDate Advertising GmbH c. X*) e C-161/10, (*Martinez c. MGN Limited*), del 25 ottobre 2011, parr. 54-55.

Se, come abbiamo già avuto modo di sottolineare, da una parte in dottrina, proprio alla luce dei *considerando* (in particolare il primo, il secondo e il dodicesimo), è ampiamente invalso l'indirizzo che identifica la base giuridica del GDPR negli art. 8 della Carta di Nizza e nell'art. 16 TFUE, dall'altra più controversa appare l'individuazione dello scopo precipuo cui sarebbe preordinata la normativa (che sull'interpretazione più o meno garantistica delle sue disposizioni si riflette)⁴⁹⁴. Accanto ad un orientamento che sottolinea come «*evidente*» appaia il fine del Regolamento di garantire il suddetto diritto fondamentale alla protezione dei dati personali con riguardo al loro trattamento, sancito dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e ribadito dall'art. 16 TFUE⁴⁹⁵, se ne collocano altri che, per lo più in senso critico rispetto alla denunciata persistenza di un approccio “mercantilista”, pur mitigato rispetto al passato, individuano il fine medesimo nel *bilanciamento* tra il diritto in questione e la contrapposta esigenza di garantire l'esercizio delle libertà economiche fondamentali su cui il Mercato Interno si fonda (declinate nella specie della libertà di circolazione dei dati personali quali ineludibile presupposto per implementare un'efficiente Mercato Unico Digitale europeo)⁴⁹⁶. Senza

⁴⁹⁴ Per l'interpretazione suddetta, cfr. su tutti F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, cit., p. 8 ss. e S. CALZOLAIO, «Protezione dei dati personali», cit., p. 626 ss.

⁴⁹⁵ Cfr. su tutti F. DONATI, «Art. 8. Protezione dei dati di carattere personale», in R. BIFULCO, M. CARTABIA, A. CELOTTO (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione europea*, Bologna, 2001, p. 83 ss.; S. CALZOLAIO, «Privacy by design», cit., p. 3 ss.

⁴⁹⁶ Cfr. in primis G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati», cit., p. 1672 ss., che nel sottolineare la «tensione» tra i due suddetti interessi che informerebbe la disciplina del GDPR, nonché la centralità del passaggio dalla fonte direttiva alla fonte regolamentare quale unico strumento per eliminare gli ostacoli giuridici al pieno funzionamento del Mercato Interno, afferma chiaramente come: «l'intento del legislatore europeo [sia quello] di disegnare un mercato unico digitale, rimuovendo gli ostacoli giuridici costituiti dalla disomogeneità delle norme applicabili». V. poi F. PIRAINO, «Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato», in *Nuove Leggi civ. comm.*, II, 2017, 369 s, che pur evidenziando le innovazioni introdotte in punto di

esplicitamente aderire all'una o all'altra lettura, che pur condividono l'essenziale rilievo che nella disciplina del trattamento dei dati personali dovrebbe assumere la protezione della dimensione positiva della *privacy* quale oggetto di un diritto fondamentale consacrato a livello *primario*, conviene procedere alla lettura e all'interpretazione congiunta dei *considerando*.

Sin dall'incipit del preambolo, si ha la netta sensazione che l'intervento riformatore adottato in materia dal legislatore europeo sia dipeso dalla crescente digitalizzazione, o datificazione, della società e dell'economia europea e globale. Rinviano, per più approfondite considerazioni, ai rilievi svolti nell'ultimo paragrafo del precedente capitolo, è sufficiente qui riportare le parole stesse del *considerando* 6, in cui si afferma che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. [...] La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività». Tale affermazione sembra rivelare la profonda consapevolezza maturata intorno all'esponenziale importanza che vanno assumendo i dati personali, quali oggetto di un flusso voluminoso e incessante, nell'era digitale contemporanea. In essa quasi riecheggiano le parole pronunciate nel 2009 dall'allora Commissario europeo per la tutela dei consumatori Meglena Kuneva: «*[p]ersonal data is the new oil of the internet and the new currency of the digital world*»⁴⁹⁷.

responsabilizzazione dei soggetti coinvolti nel trattamento dei dati denuncia come il sistema normativo disegnato dal Regolamento paia presentarsi piuttosto come disciplina della circolazione dei dati personali che quale disciplina diretta a massimizzare la protezione della persona.

⁴⁹⁷ Parole pronunciate il 31 marzo 2009 a Bruxelles, nell'ambito di una *Roundtable on Online Data Collection, Targeting and Profiling* (testo leggibile nel sito www.istitutoitaliano-privacy.it). In quell'occasione la Kuneva ebbe anche a sottolineare che «the development of marketing based on profiling and personal data is what makes it go round. (...) We accept this

Globalizzazione, digitalizzazione, *Big Data* e sviluppo vertiginoso delle tecnologie capaci di estrarre da essi informazioni non potevano che condurre il legislatore a ripensare il paradigma di tutela configurato con la c.d. Direttiva Madre, implementandone una declinazione non più (soltanto) *statica*, incentrata dunque sul momento dell'esclusione dei terzi da interferenze nella sfera privata dell'interessato (*privacy* come *seclusion*), bensì *dinamica*, che recependo la "nuova" dimensione della *privacy* quale interesse - presidiato da un autonomo diritto fondamentale - ad autodeterminarsi nelle scelte relative al flusso di informazioni in entrata e in uscita rispetto alla propria persona (*privacy* come *control*) "seguisse" i dati nella loro circolazione⁴⁹⁸. E l'attenzione prioritaria per il tale profilo è evidenziata proprio dalla disposizione che apre in senso proprio l'articolato normativo, ossia l'art. 1 (rubricato «Oggetto e finalità»), che, al paragrafo 1, prevede: «il presente Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla *libera circolazione* di tali dati»; sebbene al par. 3 contenga un inciso che sfida la visione antropocentrica cui parrebbe altrimenti ispirato il Regolamento: «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

È certo che il sistema di protezione configurato accolga una logica di bilanciamento tra diritti fondamentali: se da una parte «il trattamento dei dati

reality because it is one chosen by users. Internet users have massively opted for free services offered in exchange for acceptance of advertisement».

⁴⁹⁸ Cfr. sul punto S. RODOTÀ, *Il diritto di avere diritti*, cit., 397 s. Lo stesso illuminato autore, qualche pagina indietro (p. 395), avverte sulle potenziali conseguenze, in termini di *reificazione*, della riduzione della persona a (mero) complesso di informazioni "circolanti": «[dalla persona] vengono continuamente estratte, con le tecniche più diverse, tutte le possibili informazioni, non solo per le tradizionali, anche se sempre più dilatate, forme di controllo, ma sempre più intensamente per costruire profili e identità, per stabilire nessi e relazioni, di cui ci si serve soprattutto per finalità economiche, per ritagliare dalla persona quel che interessa il mercato».

personali dovrebbe essere al servizio dell'uomo», cosicché «il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta» (cons. 4), dall'altra «l'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali» (cons. 5)⁴⁹⁹. Appare chiara la concezione secondo cui la circolazione di tale massa crescente di dati sia un valore da custodire e promuovere, sia all'interno dell'Unione europea, sia nei rapporti con i paesi terzi. E tuttavia, ancora più chiara sembra essere la priorità rappresentata dall'esigenza di *garantire* il diritto individuale alla protezione dei dati personali, se è vero che quasi tutti i *considerando* sottolineano, in apertura, l'intenzione di predisporre un'efficace tutela della sfera privata della persona fisica, anzitutto presidiandone la “capacità” di *autodeterminazione informativa*: oltre a quelli già ricordati, eloquente in tal senso è già il *considerando* 1, che afferma: «la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale», richiamando poi l'art. 8 della Carta di Nizza e l'art. 16 TFUE; e poi il *considerando* 2, che ancor più chiaramente sottolinea come «i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale (“dati personali”) dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali»; e poi ancora al *considerando* 6 «la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più

⁴⁹⁹ È importante sottolineare che il *considerando* 4, nell'elencare i “più importanti diritti” con cui quello alla protezione dei dati personali dovrebbe necessariamente costituire oggetto di bilanciamento, ricomprende anche la libertà d'impresa, a dimostrazione della persistenza di una prospettiva mercantilista latente nella pur virtuosa concezione antropocentrica promossa dal legislatore: si legge infatti: «Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.»

la libera circolazione dei dati personali (...) garantendo al tempo stesso un elevato livello di protezione dei dati personali.»⁵⁰⁰. In questo senso, può certamente parlarsi di *visione antropocentrica*⁵⁰¹.

Altrettanto evidente è, però, la prospettiva economica che continua latente a guidare il legislatore europeo: pare, infatti, che in fin dei conti la stessa massimizzazione della tutela apprestata alla dimensione dinamica della *privacy* delle persone fisiche rappresenti, oltre che (certamente) un *valore in re ipsa*, anche (o ancora) uno *strumento* per implementare il funzionamento del Mercato Interno, e segnatamente per edificarlo anche in ambiente digitale, sul presupposto rappresentato dalla fiducia degli utenti-consumatori. Eloquente in tal senso è il *considerando 7*: ivi si afferma che le nuove regole europee intendono instaurare quel «clima di fiducia» e di certezza giuridica – fondato sulla consapevolezza delle persone fisiche di avere il controllo sui propri dati personali – necessario per lo «sviluppo dell'economia digitale in tutto il mercato interno».

Arriviamo, così, all'ultimo degli obiettivi perseguiti dal Regolamento, a sua volta strumentale rispetto a ciascuno di quelli appena enunciati (protezione delle persone fisiche nella società digitale, certezza giuridica, sviluppo del mercato unico digitale): il superamento della frammentazione giuridica delle norme e delle prassi applicative in tema di protezione dei dati personali sul suolo dell'Unione europea⁵⁰². Il *considerando 9* afferma nitidamente: «Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio

⁵⁰⁰ Altrettanto rilevante in tal senso appare il *considerando 11*, laddove osserva che «un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali».

⁵⁰¹ Cfr. ancora una volta S. CALZOLAIO, «Privacy by design», cit., p. 4; e F. DONATI, «Art. 8. Protezione dei dati di carattere personale», cit., p. 83 ss.

⁵⁰² Cfr. sul punto nitidamente G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati», cit., p. 1670 ss.,

dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà (...) può ostacolare la libera circolazione dei dati personali all'interno dell'Unione»⁵⁰³. Ecco, allora, che l'obiettivo strumentale del superamento delle disomogeneità normative tra gli Stati membri si collega proprio al bilanciamento tra protezione (del *sé informativo*) della persona fisica e libertà di circolazione del dato nella sua dimensione patrimoniale: «Al fine di assicurare un *livello coerente ed elevato di protezione* delle persone fisiche e *rimuovere gli ostacoli alla circolazione dei dati personali* all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri» (cons. 10). La sostituzione della fonte regolamentare, direttamente applicabile, alla direttiva (che agli Stati membri lascia margine di operatività circa i mezzi attraverso cui attuare i principi dalla medesima stabiliti) risulta allora, per il legislatore europeo, l'unica strada idonea ad assicurare un livello elevato di protezione delle persone fisiche e a prevenire le disparità di ordine normativo tra gli Stati membri che altrimenti ostacolerebbero la libera circolazione dei dati nel Mercato Interno: un regolamento, nello specifico, che, con le parole del *considerando* 13, «garantisca la certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e

⁵⁰³ Il *considerando* continua con affermazione altrettanto importanti: «Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. *Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE.*»

assicuri un controllo coerente del trattamento dei dati personali». Per usare una formula divenuta celebre, insomma, «*one continent, one law*»⁵⁰⁴.

A tali complessive esigenze sembra, in modo più o meno adeguato a seconda dei settori disciplinati, rispondere il Regolamento UE 2016/679.

3.1.2. Ambito di applicazione, definizioni generali e principi di protezione dei dati: *risk-based approach* e autodeterminazione informativa

Veniamo, ora, alla disciplina di dettaglio contenuta nel GDPR. Si premette che si analizzeranno qui soli i principi che sostanziano l'impalcatura normativa del Regolamento, concentrandosi poi sull'esame di alcuni istituti di nuova introduzione: altri aspetti di dettaglio, segnatamente in punto di principi sulla protezione dei dati e di basi giuridiche del trattamento (rispettivamente, artt. 6, 7 e 9 del Reg.) saranno analizzati nei paragrafi dedicati alla disciplina (generale) dei trattamenti automatizzati, seguendo gli spunti offerti dalle Linee Guida già citate del Gruppo di Lavoro Articolo 29.

Occorre innanzitutto soffermarsi sull'ambito di applicazione territoriale del GDPR, principiando da un importante rilievo: la scelta della fonte regolamentare, che uniforma la disciplina applicabile al trattamento vigente nei diversi Stati membri, consente di superare la questione (di diritto internazionale privato, diremmo), cruciale in punto di applicazione della previgente Dir. 95/46/CE, circa l'individuazione del diritto nazionale (materiale) applicabile. Quanto meno, intanto, laddove i soggetti coinvolti siano domiciliati o residenti (se persone fisiche) o stabiliti (se persone giuridiche) in diversi Stati membri: come è stato

⁵⁰⁴ Per il noto motto che ha accompagnato l'iter di approvazione del GDPR, cfr. L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 70 ss.

autorevolmente affermato, il problema diventa ora semmai l'individuazione del diritto applicabile allorché il titolare del trattamento sia stabilito in un *Paese terzo*⁵⁰⁵.

E tuttavia, il Regolamento pare superare anche questo annoso problema: l'art. 3 par. 1, infatti, stabilisce che il Regolamento «si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare di trattamento o di un responsabile del trattamento nell'Unione, *indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*». Con ciò, si evidenzia la centralità della nozione di stabilimento, che va interpretata a sua volta alla luce del *considerando* 22, il quale stabilisce che «lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica». In tal modo, l'art. 3 (assurgendo a norma di diritto internazionale privato *uniforme*) allarga notevolmente l'ambito di applicazione territoriale del Regolamento, in linea con alcune determinanti decisioni della Corte di Giustizia dell'Unione europea, che hanno anticipato questo mutamento legislativo attraverso l'interpretazione estensiva dell'art. 4 (rubricato «Diritto nazionale applicabile») dell'allora vigente dir. 95/46/CE: le più note sono certamente le già ricordate *Google Spain* e *Schrems I*⁵⁰⁶.

⁵⁰⁵ Cfr. M.G.STANZIONE, «Il Regolamento europeo sulla privacy: origini e ambito di applicazione», in *Europa e dir. priv.*, 2016, p. 1251

⁵⁰⁶ Cfr. sul punto specialmente G. FINOCCHIARO, «La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems», in G. Resta –V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe harbour principles" al "Privacy shield"*, Roma 2016, 116, che sottolinea come la corte statuisca in tal modo il più elevato livello di tutela garantito rispetto in contesto europeo rispetto ad altri paesi nel mondo, e a p. 122 ss., riferendosi alla sentenza Google Spain, afferma «la Corte osserva che Google Spain (con sede legale a Madrid) costituisce una filiale di Google Inc.(con sede legale negli Stati Uniti) nel territorio spagnolo e, per tanto, uno "stabilimento" ai sensi della direttiva». Cfr. ancora una volta C. Giust. UE, causa C-131/12, *Google Spain SL*, 13 maggio 2014 e C. Giust UE, C-311/18, *Data Protection Commissioner v. Maximilian Schrems e Facebook*

Il Regolamento, tuttavia, non si ferma al recepimento di tale indirizzo della giurisprudenza eurounitaria: il secondo paragrafo dell'art. 3, dispone infatti che «il presente Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione». In questo modo, il legislatore europeo ha voluto garantire la generale applicabilità del Regolamento a qualunque trattamento di dati, connesso alla fornitura di servizi agli interessati o finalizzato a monitorare il loro comportamento, che avvenga all'interno dell'Unione, *anche qualora lo stabilimento sia collocato fuori dal suo territorio*.⁵⁰⁷

Il Regolamento procede al contempo ad individuare l'ambito di applicazione materiale della disciplina: art. 2, paragrafo 1, dispone infatti che «il presente Regolamento si applica al *trattamento interamente o parzialmente automatizzato* di dati personali e al *trattamento non automatizzato* di dati personali contenuti in un archivio o destinati a figurarvi». Se la disposizione in

Ireland, 16 luglio 2020. Per la sentenza *Scherms* e le sue ripercussioni sulla tutela dei dati personali nell'Unione europea, si vedano, in particolare, R. BIFULCO, «La sentenza Scherms e la costruzione del diritto europeo della privacy», cit.; G SCARCHILLO, «Dal Safe Harbor al Privacy Shield», cit..

⁵⁰⁷ Cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., 160 s., il quale osserva che in questo modo si supera «nettamente il principio di stabilimento quale unico parametro, previsto dall'art. 4 della Direttiva, per individuare la legge applicabile». Occorre aggiungere che le previsioni del secondo paragrafo dell'art. 3 devono interpretarsi alla luce di quanto previsto dai *considerando* 23 e 24 dello stesso Regolamento. Si deve, poi, anche ricordare il par. 3 dell'art. suddetto, il quale stabilisce che il reg. «si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico», quali, ad esempio, consolati e/o ambasciate.

questione ricalca il tenore dell'art. 3 della dir. 95/46/CE, dall'altro il perimetro applicativo *ratione materiae* del Regolamento nel suo complesso non può dirsi coincidente con quello della previgente Direttiva Madre, dal momento che molti dei termini – o, piuttosto, elementi normativi – che compongono la fattispecie assumono nell'economia del Regolamento, sia alla luce dell'articolato stesso (e dei suoi *considerando*) sia per effetto dell'evoluzione della giurisprudenza della CGUE in materia, un significato giuridico diverso: un significato quasi sempre, lo si anticipa, più ampio, idoneo ad estendere la protezione offerta alla sfera privata della persona fisica, per mezzo dell'esplicita tutela della dimensione dinamica della *privacy*, al novero più ampio possibile di fattispecie che coinvolgano l'elaborazione delle informazioni riconducibili alla medesima, e dunque a rendere la relativa disciplina *onnicomprendensiva*⁵⁰⁸.

Soffermandoci ancora un momento sul punto, bisogna aggiungere che l'art. 2 medesimo, al par. 2, pone positivamente dei limiti “in negativo” all'ambito materiale di applicazione disegnato dal par. 1, introducendo alcune importanti deroghe alla nuova disciplina. In particolare, il legislatore europeo ha escluso che esso debba applicarsi al trattamento di dati personali: «a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del Titolo V, Capo 2, TUE; c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la

⁵⁰⁸ Cfr. S. SICA, «Verso l'unificazione del diritto europeo alla protezione dei dati personali?», in S.Sica, V.D'Antonio, G.M.Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 5.; C. COLAPIETRO, «I principi ispiratori del Regolamento UE 2016/679 e la loro incidenza sul contesto normativo nazionale», p. 13 ss.

salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse».

Le previsioni che pongono maggiori problemi interpretativi sono certamente quelle di cui alla lett. c) e alla lett. d).

Per quanto attiene alla prima (che riproduce la clausola, già prevista all'art. 3 della dir., della c.d. *household exemption*), risulta particolarmente difficile individuare il criterio attraverso cui stabilire il confine tra attività qualificabili o meno come *personali o domestiche*. Al riguardo, viene in soccorso quanto previsto dal *considerando* 18 del Regolamento, in base al quale l'*household exemption* deve escludersi ogni qual volta l'attività posta in essere abbia una connessione con un'attività commerciale o professionale. Lo stesso considerando aggiunge poi che «le attività a carattere personale potrebbero comprendere (...) l'uso di social network e attività online comprese nell'ambito di tali attività». Non è mancato, allora, chi abbia fatto notare con acume che il Regolamento avrebbe potuto predisporre una tutela più incisiva rispetto a tutte quelle operazioni *sui* dati che, pur svolgendosi, in senso generico, in ambito domestico, implicino l'utilizzo dei social (come *mezzo*), stante la loro capillare diffusione nel tessuto sociale globale e i rischi di nocimento cui espongono la vita privata e l'identità personale dei singoli: dal combinato disposto tra l'art. 2 par. 2 e il considerando in questione, parrebbe infatti che l'ascrivibilità o meno di attività siffatte entro il perimetro applicativo del Regolamento dipenda quasi da una logica «caso per caso»⁵⁰⁹.

La seconda previsione rinvia invece alla complessa questione, di cui già ci siamo occupati a livello generale nei precedenti capitoli, concernente il rapporto tra diritti a presidio di attributi fondamentali della persona umana e interessi

⁵⁰⁹ Cfr. ad es. Cfr. P. PASSAGLIA, «Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità», in *Consulta Online*, Fascicolo 3, 2016, p. 335 s..

superindividuali, quali appunto la sicurezza pubblica. Si tratta di un territorio in cui logiche securitarie, alimentate dalle numerose opportunità offerte dalle ICTs sotto il profilo del controllo sociale (anche con riguardo alle attività di prevenzione e di repressione dei reati, nonché allo svolgimento delle indagini). e prospettive liberali e umanitarie, consacrate nel denunciato processo di “costituzionalizzazione” dell’Unione europea vengono a confliggere, alla ricerca di quel difficile equilibrio che oggi trova il suo ineludibile (ed imperativo) faro nel principio di proporzionalità sancito dall’art. 52 della Carta di Nizza⁵¹⁰. Occorre però ricordare che la materia in questione risulta espunta dall’ambito di applicazione del Regolamento, poiché ricadente nell’ambito applicativo della citata Direttiva 2016/680, relativa alla protezione delle persone fisiche nel trattamento dei dati da parte dell’Autorità giudiziaria e dell’Autorità di pubblica sicurezza in materia di prevenzione e di repressione dei reati. Tale strumento normativo, tuttavia, non già uniforme, bensì armonizza il diritto vigenti nei singoli Stati membri in materia, necessitando di trasposizione ai fini della sua concreta applicazione⁵¹¹.

Veniamo ora ad esaminare nello specifico alcuni dei principali elementi normativi delle fattispecie considerate, dalla cui definizione dipende l’applicabilità o meno della disciplina prevista dal Regolamento. Dobbiamo

⁵¹⁰ Tale disposizione, lo si ricorda, prescrive che nessuna misura legislativa che incida in senso restrittivo sui diritti fondamentali possa lederne il contenuto essenziale V. *retro*, cap. 1 par. 2 e cap. 2, par. 2.3. Cfr. sul punto anche M. RUBECHI, «Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)», in *Federalismi.it*, n. 23/2016, 24 s.

⁵¹¹ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 119 del 4.5.2016, pagg. 89–131; <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L0680>

rivolgerci all'art. 4 del Regolamento (rubricato «Definizioni»); e, nel suo ambito, necessariamente soffermarci sulla nozione, o più in generale sulla categoria di *dato personale*. Nozione e categoria che, nei vent'anni intercorsi tra l'adozione della Direttiva Madre e l'elaborazione del Regolamento, ha subito in via positiva un'*estensione* semantica, strumentale ad adeguarla al mutato contesto storico sociale e tecnologico in cui ICTs, tecniche di *Big Data analytics* e i sistemi algoritmici e di IA preposti ad implementarle producono il risultato di *frantumare la personalità umana* in una pluralità di proiezioni virtuali, che definiscono un «corpo elettronico» in cerca di sintesi⁵¹².

La nozione fatta propria dal Regolamento, allora, pare ispirata al già descritto mutamento di prospettiva, che recependo la realtà di una persona fisica immersa in un flusso costante di informazioni *in uscita e in entrata* accoglie e ambisce a proteggere una declinazione positiva di *privacy*, in termini di *autodeterminazione informativa*: in termini, dunque, di autonomo diritto fondamentale alla protezione dei dati personali, “costituzionalizzato” in sede europea, quale libertà di «mantenere attivamente il controllo sui propri dati», e di intervenire per ripristinarne l'integrità⁵¹³.

Ecco allora che l'art. 4 del Regolamento, al n. 1) del par. 1, introduce una definizione molto ampia di dato personale, secondo cui costituisce dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile una persona fisica che può essere identificata, direttamente o indirettamente», aggiungendo poi un vasto novero (non esaustivo) di situazioni tipicizzate, ossia «con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati

⁵¹² Cfr., tra i molti citati, ancora una volta i contributi di S. RODOTÀ, *Tecnopolitica*, cit., p. 134 ss, e G. RESTA, «Identità personale e identità digitale», cit., spec. 522 ss.

⁵¹³ S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 396 ss; cfr. poi ancora una volta F. DONATI, «Art. 8. Protezione dei dati di carattere personale»

relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

La definizione appare di centrale rilievo per un duplice ordine di ragioni. Da una parte, infatti, emerge «la scelta di una nozione di dato personale al limite della genericità, ma in realtà, *con funzione onnicomprensiva*, per un verso, e con capacità di attrazione di nuove situazioni non previste né prevedibili *ex ante* dal legislatore»⁵¹⁴. Dall'altra, è necessario constatare un incremento delle ipotesi tipizzate già a livello normativo, dal momento che la disposizione fa riferimento ad un'ampia serie di “nuovi” identificativi, compresi quelli *online*, con ciò manifestando l'intenzione di abbracciare nell'alveo della nozione il numero più ampio possibile di elementi caratteristici dell'identità *a tutto tondo*⁵¹⁵. L'ampio aggiornamento della nozione, aggiungiamo, pare testimoniato anche dalle definizioni di dettaglio che fanno riferimento alle “innovative” nozioni di dato genetico (art. 4, par. 1, n. 13) e di dato biometrico (art. 4, par. 1, n. 14)⁵¹⁶.

Diversi commentatori fanno notare come la definizione medesima recepisca molti dei felici approdi raggiunti in punto di esegesi della nozione di dato personale coniata dalla previgente Direttiva Madre dal Gruppo di Lavoro

⁵¹⁴ Cfr. S. SICA, Verso l'unificazione del diritto europeo alla protezione dei dati personali?, cit., p. 5 ss.

⁵¹⁵ Cfr. sul punto M.G. STANZIONE, Genesi e ambito di applicazione, cit., 23. Bisogna ricordare che l'art. 2 della previgente dir. 95/46/CE faceva riferimento in modo specifico (solo) ai tratti «caratteristici della (...) identità fisica, fisiologica, psichica, economica, culturale e sociale».

⁵¹⁶ Ex art. 4 par. 1, n. 13 per dato genetico si intende «i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione»; ex n. 14, i dati biometrici sono «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

Articolo 29 (oltre che dai Garanti nazionali) ⁵¹⁷. In primo luogo, esso pare accordarsi agli insegnamenti contenuti nel Parere 4/2007 del Gruppo, il quale aveva accolto una nozione -già allora- onnicomprensiva di dato personale, avvertendo l'esigenza di evitare indebite restrizioni della nozione medesima anche alla luce dell'(ancora non vincolante) art. 8 della Carta di Nizza: nozione onnicomprensiva «tanto sotto il profilo della *natura* (potendo includere informazioni soggettive e oggettive nonché vere o false) quanto con riferimento al suo *contenuto* (ricomprendendo sia i dati generali sia i dati sensibili), nonché avendo riguardo al *formato* (non rilevando la forma cartacea, alfabetica, numerica, grafica, fotografica, acustica ovvero l'eventuale conservazione mediante codice binario)»⁵¹⁸. Ad esso ha poi fatto seguito il Parere n. 13/2011 del medesimo Gruppo, secondo cui la nozione di dato personale sarebbe talmente ampia da potersi ricomprendere all'interno di essa anche il c.d. *MAC Address* (*Media Access Control Address*), ossia una sequenza numerica che identifica il produttore, il dispositivo e da cui è possibile desumere, finanche, l'acquirente o l'utilizzatore dell'apparto.

E tuttavia, il Regolamento fa un ulteriore, fondamentale passo avanti, che pare ispirato dalla consapevolezza dell'inarrestabile avvento del fenomeno dei *Big Data*, delle loro caratteristiche sintetizzate nelle 4V, e della capacità delle tecnologie esistenti di estrarre da tale mole di dati - che comprende *anche e soprattutto* dati non personali, perché tali già in origine o altrimenti in seguito ad

⁵¹⁷ Cfr. L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., p. 48 ss.; S. CALZOLAIO, «Protezione dei dati personali», cit. p. 606 ss.; C. COLAPIETRO, «I principi ispiratori del Regolamento UE 2016/679 e la loro incidenza sul contesto normativo nazionale», p. 18 ss.

⁵¹⁸ La ricognizione sistematica è di C. COLAPIETRO, «I principi ispiratori del Regolamento UE 2016/679», cit., p. 18, che chiaramente rinvia a Gruppo di Lavoro Articolo 29 sulla protezione dei dati personali, Parere 4/2007 sul concetto di dati personali, 20 giugno 2007, p. 6 ss.

anonimizzazione - informazioni analitiche relative ad una determinata persona fisica⁵¹⁹.

Ci riferiamo da una parte all'accoglimento, *a contrario*, di una nozione solo relativa di dato anonimo, peraltro non contenuta nell'articolato, bensì nel *considerando* 26, in cui si legge che la disciplina del Regolamento *non* dovrebbe risultare applicabile a quelle «informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi *sufficientemente anonimi* da impedire o da non consentire più l'identificazione dell'interessato». L'elemento chiave, che segna la distinzione tra dato personale e dato anonimo, è allora la “collegabilità” tra le suddette informazioni, la quale a propria volta dipende da numerosi fattori, tra i quali, oltre alla natura e ai mezzi a disposizione del soggetto che opera il collegamento, rientra certamente la “generale” disponibilità sul mercato di tecnologie a ciò preposte. L'anonimato, dunque, si specifica in relazione alla singola situazione concreta; e qualsiasi informazione potrebbe, dacché in principio qualificata anonima, successivamente ricadere nella categoria di dato personale, e dunque nell'ambito di applicazione del Regolamento.⁵²⁰ Al contempo, in conseguenza dell'approccio *risk-based* fatto proprio dalla normativa, per far fronte in modo sistematico ai rischi configurati soprattutto dalle moderne tecnologie nell'ambito dei trattamenti, anche automatizzati, dei dati personali, il Regolamento introduce l'istituto della

⁵¹⁹ Oltre alle considerazioni già svolte *retro*, cfr. M.M. WINKLER, J. MOSCA, «Cloud computing e protezione dei dati personali», in M. Fumagalli Meraviglia (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Napoli, Editoriale Scientifica, 2015, pp. 121 ss. e G. D'ACQUISTO, J. DOMINGO-FERRER, P. KIKIRAS, V. TORRA, Y. A. DE MONTJOYE, A. BOURKA, «Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics», European Union Agency for network and information security, dicembre 2015, in <http://www.enisa.europa.eu>.

⁵²⁰ Cfr. gli importanti rilievi svolti sul punto da G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati», cit., p. 1673; e di R. DUCATO, «La crisi della definizione di dato personale nell'era web 3.0», in F. Cortese -M. Tomasi (a cura di), *Il diritto e le definizioni*, Editoriale Scientifica Italiana, Napoli 2016, 164 ss., che parla di «fallimento dell'anonimizzazione» a fronte delle sempre maggiori «reali possibilità di re-identificazione».

«pseudonimizzazione», che all'art. 4, par. 1, n. 5 definisce come «trattamento dei dati personali in modo tale che i dati personali *non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive*, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Essa appare, insieme, una misura tecnica ed una misura organizzativa in cui si specifica il principio di *accountability*, di cui parleremo a breve, che investe il titolare del trattamento. I *considerando* 28 e 29, peraltro, sembrano fortemente incentivare l'impiego di tale misura, poiché considerata in grado di minimizzare il rischio per gli interessati coinvolti nel trattamento⁵²¹. Di assoluto rilievo appare poi, alla luce di un'interpretazione dell'art. 4 orientata dal *considerando* 26, l'assoggettamento dello stesso dato pseudonimo alla disciplina del Regolamento, poiché esso continua ad essere considerato come «informazion[e] su una persona fisica identificabile»⁵²².

Tuttavia, il profilo più rilevante consiste proprio nelle indicazioni, aventi insostituibile funzione interpretativa (di tipo teleologico e sistematico), contenute nei *considerando* 26 e 30, che risolvono alcuni dei margini di ambiguità altrimenti profilati dalla definizione di dato personale delineata dall'art. 1. Tali indicazioni, *asl contempo*, consentono di superare la prospettiva, inadatta a far fronte alla datificazione e al fenomeno degli *algo-created data*, fatta propria dal Gruppo di Lavoro Articolo 29 nel già ricordato Parere del 2007, e di implementarne una che ricomprenda nella categoria del dato personale qualsiasi informazione che renda

⁵²¹ Cfr. per più puntuali rilievi G. Finocchiaro, «Introduzione al regolamento europeo sulla protezione dei dati», cit., p. 1673; S. Calzolaio, «Protezione dei dati personali», cit., p. 628 ss.

⁵²² V. cons. 26, che nello specifico afferma: «I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile». Cfr. anche sul punto D'ACQUISTO-NALDI, *Big data*, cit., p. 39 ss.

potenzialmente identificabile un interessato, anche quando non sia ragionevole attendersi che il titolare del trattamento sia in concreto in grado di identificare quest'ultimo⁵²³.

Il *considerando* 26 afferma infatti che per definire se una persona sia identificabile è necessario valutare «tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona direttamente o indirettamente». E il *considerando* 30 aggiunge che «le persone fisiche possono essere associate ad identificativi on line prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies), o identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone e identificarle». In questo modo il dettato normativo sembra persino anticipare alcuni approdi giurisprudenziali sul tema: emblematico è, infatti, il caso in cui la Corte di Giustizia dell'Unione europea, nelle more del procedimento di approvazione ed entrata in vigore del nuovo Regolamento, ha affermato che costituisce dato personale (ai sensi dell'allora vigente art. 2, lett. a), della Dir. n. 95/46/CE) l'indirizzo IP dinamico (ossia quello provvisorio che viene assegnato a ogni connessione internet e che cambia alle eventuali connessioni successive); aggiungendo tuttavia la Corte, in questo caso, che ciò dipende essenzialmente dal fatto che il fornitore di servizi media online disponga di mezzi che possano essere ragionevolmente utilizzati per identificare, anche con l'aiuto di altri soggetti (ad

⁵²³ Cfr. ancora una volta GRUPPO DI LAVORO ARTICOLO 29 SULLA PROTEZIONE DEI DATI PERSONALI, Parere 4/2007 sul concetto di dati personali, 20 giugno 2007, che subordinava la qualificazione di un'informazione in termini di dato personale ad una valutazione sulla probabilità e ragionevolezza dell'ipotesi che, in concreto, quella informazione fosse associata e associabile dal titolare del trattamento alla persona fisica, sulla base di una valutazione che tenga conto dei costi di questa operazione, della capacità e della evoluzione tecnologica, del contesto e delle finalità del trattamento.

esempio, l'autorità competente ed il fornitore di accesso a internet), la persona interessata⁵²⁴.

Appare insomma chiaro che, allo stato attuale della disciplina, la nozione di dato personale risulta essenzialmente *onnicomprendiva*: espressione, in particolare, della volontà del legislatore europeo di ampliare le fattispecie di trattamento ricadenti nell'alveo della tutela accordata alla sfera privata della persona fisica dal Regolamento medesimo.

Altra definizione assai rilevante è, nel quadro dell'art. 4, quella di «trattamento», che ai sensi del n. 2 si identifica in «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»⁵²⁵. E poi quella di «titolare del trattamento», che ex n. 7 individua «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali»; e di «responsabile del trattamento», che ex n. 8 identifica «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

Su altre nozioni di capitale importanza, anche e soprattutto ai fini della nostra trattazione (come quella di consenso dell'interessato, di profilazione ed

⁵²⁴ Cfr. CGUE, 19 ottobre 2016, C-582/2014, *P. Breyer c. Bundesrepublik Deutschland*, spec. paragrafo 49.

⁵²⁵ Cfr. ampiamente F. PIZZETTI, *Privacy*, cit., I, p. 193 ss.

anche di «categorie particolari di dati personali» ex art. 9), torneremo nel prossimo paragrafo.

Abbandonando il piano delle definizioni, procediamo ora ad analizzare i più importanti principi sulla protezione dei dati personali che informano il GDPR: in particolare, qui si intende tracciare un quadro sintetico ma puntuale della “architettura normativa” da tali principi disegnata, riservandoci di approfondirne successivamente le implicazioni nella specifica materia dei trattamenti automatizzati e, soprattutto, i principali profili di frizione con il fenomeno (rapporto tra *Big Data analytics*, sistemi algoritmici ed elaborazione dei dati) che la disciplina di dettaglio di tale *species* di trattamenti intende governare.

Anticipiamo che particolare rilievo assumono gli innovativi principi di *accountabilty* del titolare e/o del responsabile del trattamento, di *privacy by design* e di *privacy by default* in cui questo prevalentemente si specifica (principi, nel loro complesso, i cui riferimenti normativi si individuano negli artt. 24, 25 e 32 del Regolamento), nonché gli istituti altrettanto innovativi che della *privacy by design* costituiscono articolazione (in particolare, il c.d. *Privacy Impact Assesment* ex art. 35 e la figura del *Data Protection Officer* ex art. 37). Pur esulando dagli scopi della presente trattazione, anche essi costituiranno oggetto di succinta analisi, nei limiti in cui rilevino nell’economia generale del nostro discorso sugli *automated data processing*.

È necessario, preliminarmente, ricordare ancora una volta che l’intero impianto del Regolamento ruota intorno a due cardini: la protezione dei dati personali come tutela dell’autodeterminazione informativa e un approccio sensibile al rischio espresso da qualsiasi operazione (*rectius*: trattamento) svolto in relazione alle informazioni oggetto di tale diritto (c.d. *risk-based approach*)

È stato autorevolmente sottolineato come tale impostazione discenda dal “classico” modello di protezione dei dati personali in ambito comunitario che «si realizza attraverso la rigida imposizione di obblighi nei confronti dei soggetti che vogliano (o si trovano ad) entrare in contatto con specifiche tipologie di informazioni (titolare/responsabile del trattamento) e, d’altra parte, riconosce una libertà positiva di controllo ed intervento (diritto all’autodeterminazione informativa o *recht auf Informationelle selbstbestimmung*) in favore del soggetto a cui l’informazione è riferita»⁵²⁶.

Altrettanto brillantemente è stato detto che, se il GDPR si concentra sull’imposizione di un’articolata trama di obblighi (espressione del principio di *accountabilty* ex art. 32) in capo al titolare e/o al responsabile del trattamento, allargando la strategia normativa della precedente Direttiva, ciò deriva dalla maturata consapevolezza che «la produzione di un dato in ambiente digitale coincide di norma con l’accettazione di un rischio da parte del soggetto interessato, un rischio che abbraccia il trattamento nel cui ambito quel dato è richiesto e tutti i potenziali trattamenti cosiddetti secondari», cosicché « l’insieme delle disposizioni del reg. europeo appare trovare le sue fondamenta concettuali su questa osservazione del rischio e della rischiosità della circolazione in rete di dati (e di dati personali)»⁵²⁷. Dall’accoglimento di una prospettiva che vede nel rischio, e nel corrispondente principio di precauzione, il “baricentro” della disciplina a presidio dell’autodeterminazione informativa (e, strumentalmente, della riservatezza e dell’identità personale), discende che altro elemento caratteristico del Regolamento. consiste nella strutturale necessità di una

⁵²⁶ G. GIANNONE CODIGLIONE, «Risk-based approach e trattamento dei dati personali», in S. Sica, V.D’Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 58, spec. nota 8

⁵²⁷ S. CALZOLAIO, «Protezione dei dati personali», cit., p. 627, che fa notare come il termine rischio ricorra più di cento volte nel testo del Regolamento. Cfr. anche gli importanti rilievi di A. MANTELERO, «Responsabilità e rischio nel Reg. UE 2016/679», in NLCC, 1/2017, 144 ss. e di M. G. STANZIONE, «Genesi ed ambito di applicazione», cit., p. 21 ss.

valutazione sistematica da parte del Titolare dei rischi attuali e potenziali del trattamento, sia in riferimento alla protezione dei diritti dell'interessato sia in riferimento specifico alla sicurezza dei dati (e ciò si lega saldamente al nuovo istituto della c.d. «Valutazione Preventiva d'Impatto», su cui v. *infra*).

In punto di c.d. «principi sulla protezione dei dati» (rubrica dell'art. 5), il Regolamento ad una prima lettura sembra riprodurre pedissequamente quelli enunciati dall'art. 6 della previgente Direttiva, a propria volta mutuati dalla Convenzione n.108 del 1981. Tuttavia, non solo si deve constatare che molti di essi sono assurti ad un rango supremo, o anche costituzionale, in seguito alla loro cristallizzazione nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea e al descritto processo di “uniformazione” della sua efficacia giuridica a quella dei Trattati Istitutivi subito per effetto del Trattato di Lisbona, segnatamente laddove prevede che i «dati devono essere trattati secondo il principio di lealtà, per finalità determinate ed in base al consenso della persona interessata o a un altro fondamento legittimo posto dalla legge». Soprattutto, è necessario ricordare come il Regolamento cristallizzi a livello normativo molti dei principi elaborati specialmente a partire dal nuovo millennio dalla giurisprudenza della Corte di Giustizia dell'Unione europea, e sia il prodotto di quel processo, promosso dalla stessa Corte, che ha condotto le istituzioni normative dell'Unione ad abbandonare una prospettiva esclusivamente *market driven* e ad adottarne una *fundamental rights-oriented*⁵²⁸.

⁵²⁸ G.FINOCCHIARO, «Introduzione al Regolamento europeo sulla protezione dei dati personali», cit., p. 2; O. POLLICINO, «Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale», in *Federalismi.it*, in Comunicazione, media e nuove tecnologie, n. 3/2014; e soprattutto M. BASSINI, «La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali», in *Quad. cost.*, 2016, 588, che, come già ampiamente sottolineato *retro*, rileva il passaggio da una normativa europea sulla libera circolazione dei dati personali di impronta sostanzialmente “mercantilistica”, ad una diversa prospettiva legata principalmente alla tutela dei diritti fondamentali.

Sempre a titolo preliminare, è necessario ricordare che il Regolamento distingue tra disciplina applicabile a qualsiasi tipo di trattamento e disciplina applicabile o ai trattamenti aventi ad oggetto «categorie particolari di dati» (art. 9), o a determinate specie di trattamento (emblematica è la fattispecie che ci occuperà nei prossimi paragrafi: ossia i processi decisionali interamente automatizzati compresa la profilazione, ex art. 22).

I primi principi rilevanti sono enunciati nella lettera a) dell'art. 5, che specifica come i dati siano (ovvero: *debbono essere*) «trattati in modo lecito, corretto e trasparente». Primo viene allora il principio di liceità del trattamento, la cui osservanza è vincolata alla (necessaria) sussistenza di *una* (almeno una) delle basi giuridiche, o fondamenti di liceità, previsti (dove non derogati da altre norme) dall'art. 6. Basi giuridiche che possono essere a loro volta raggruppate in due *species*, di natura tra loro alternativa: da una parte, campeggia il *consenso (qualificato) dell'interessato*, fondamento generale di liceità del trattamento i cui requisiti sono identificati dall'art. 4 n. 4 nella libertà, specificità, consapevolezza ed inequivocabilità della manifestazione di volontà in cui consiste; dall'altra l'art. 6 identifica tassativamente una serie di *fondamenti normativi*, che derogano all'ipotesi generale prevista dalla lettera a) e il cui comune denominatore può essere, sinteticamente, rintracciato nella *necessità* del trattamento medesimo⁵²⁹. È

⁵²⁹ Per comodità espositiva, si riporta qui il dettato del menzionato articolo: «Art. 6 – Liceità del trattamento. 1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità ;b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di poteri pubblici di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti o le libertà fondamentali dell'interessato che richiedono la protezione dei dati

necessario subito aggiungere che, sebbene temperato da una nutrita serie di eccezioni previste dal par. 2, l'art. 9 prevede il generale divieto di trattamento di quelle informazioni dalla Direttiva 95/46/CE qualificate come «dati sensibili», ed oggi con diversa espressione identificati come «categorie particolari di dati personali»: stabilisce infatti il primo paragrafo che «è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»⁵³⁰.

La stessa previsione della lettera a) continua identificando due altri pilastri dell'integrità dell'*informational privacy*, ossia il principio di correttezza ed il principio di trasparenza, i quali si traducono a livello di dettaglio nella disciplina che impone al titolare del trattamento un'adeguata informativa da rivolgere all'interessato (delineata dagli artt. 12, 13 e 14 del reg.), la quale, come è stato osservato, risulta «funzionale alla formazione e all'espressione di un consenso al trattamento autenticamente libero e consapevole, nonché all'eventuale esercizio di tutti i diritti dell'interessato»⁵³¹. E il legislatore valorizza ulteriormente gli obiettivi in questione, laddove al *considerando* 39 esplicita il

personali, in particolare se l'interessato è un minore. (...)). Le diverse condizioni che rendono lecito il trattamento dei dati sono ulteriormente esplicitate nei *considerando* dal 42 al 50 quali prioritari strumenti, o criteri, di indirizzo esegetico in relazione alla disposizione in esame.

⁵³⁰ Sulla disposizione ci soffermeremo più ampiamente *infra* quando individueremo i principali limiti di ordine generale alla liceità dei trattamenti anche solo parzialmente automatizzati dei dati personali.

⁵³¹ L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., 63; cfr. anche M.G.Cubeddu, «Commento art. 13», in C.M.BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali*, in Le Nuove Leggi civ. comm., 2007, 295, che ivi afferma come l'informativa assurga a «premessa logica non solo di un consenso informato, ma altresì della delimitazione dei diritti dei soggetti interessati e della definizione dell'ambito di tutela connesso al trattamento».

«rapporto tra consenso dell'interessato e l'obbligo d'informazione posto in capo al titolare, avente come oggetto in primo luogo le finalità del trattamento».

Avendo poi riguardo al nuovo contesto della *società digitale*, è stato più volte affermato in seno al Gruppo di Lavoro Articolo 29 (cui ha fatto eco il Garante Privacy italiano in diverse pronunce aventi ad oggetto i *cookies*) il c.d. *principio di lealtà del trattamento* (o *fairly manner* del titolare del trattamento), in forza del quale l'informativa a carico del titolare deve consentire all'interessato di comprendere in modo adeguato non solo le modalità del trattamento, bensì anche gli effetti che da questo potrebbero ulteriormente derivare a suo carico⁵³².

Centrale, soprattutto, nella materia che ci riguarda nello specifico è il terzo termine della triade suddetta, ossia il *principio di trasparenza*, che impone un trattamento le cui condizioni, le cui modalità e i cui effetti siano, appunto, agevolmente *conoscibili* dall'interessato: in questo senso, il principio in parola rappresenta un'ulteriore declinazione del principio, o dovere, di *lealtà* dei titolari, e in relazione ai trattamenti interamente automatizzati, come avremo modo di vedere, trova specificazione nelle disposizioni che prescrivono l'obbligo per il titolare di fornire, e il corrispondente diritto dell'interessato di ricevere, informazioni *chiare sulla logica del trattamento algoritmico*.⁵³³ Sul punto,

⁵³² V., rispettivamente, GRUPPO DI LAVORO ARTICOLO 29 SULLA PROTEZIONE DEI DATI PERSONALI, *Working Document providing guidance on obtaining consent for cookies*, Documenti n. 2/2013, 2° October 2013 (WP n. 208); Garante per la protezione dei dati personali, "Individuazione delle modalità semplificate per l'informatica e l'acquisizione del consenso per l'uso di cookies", 8 maggio 2014, in cui il Garante che il leale comportamento del titolare dovrebbe concretizzarsi (anche) in un duplice grado d'informativa, in forma breve ed in forma estesa, che consenta «agli utenti di esprimere scelte realmente consapevoli sull'installazione dei cookie mediante la manifestazione di un consenso espresso e specifico». Cfr. sul punto F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., 268

⁵³³ V. sin d'ora art. 13, par. 2, let g), art. 14 par. 2, let f), art. 15, par. 1, let. h), e, ovviamente, art. 22 del Reg. UE 2016/679; cfr. sul punto, a titolo introduttivo, i rilievi di A. MANTELERO, «Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo», in *Dir. Inf.*, XXVIII, 1, 2012, pp. 135-144; F. FAINI, «Dati, algoritmi e Regolamento europeo 2016/679», cit., p. 344 ss.

merita sin da ora evidenziare quanto proprio nel contemporaneo contesto dei *Big Data* e in relazione al diffuso utilizzo di “sistemi intelligenti” nell’elaborazione dei dati emergano i profili di maggior frizione tra realtà e principio in questione: realtà connotata dall’indiscriminata acquisizione e dal sistematico utilizzo di dati personali (originari o inferiti) per mezzo di algoritmi complessi i cui processi decisionali sono spesso, come già abbiamo sottolineato, opachi⁵³⁴. È il fenomeno cui già ci siamo riferiti con il termine *black box*, anche definito “*transparency paradox*”, che rende, appunto, la trasparenza al centro del dibattito sugli algoritmi, come lo stesso Gruppo di Lavoro nelle Linee Guida che andremo ad esaminare ha ripetutamente sottolineato⁵³⁵.

La lettera b) codifica poi il *principio di finalità* (o di limitazione delle finalità, come si esprime la norma), stabilendo che i dati personali debbano essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità»; principio che risulta dunque intrinsecamente collegato al principio di liceità, come dimostra il richiamo ad esso operato dall’art. 6 lett. a) («l’interessato ha espresso il consenso per specifiche finalità»). Particolarmente importante risulta l’inciso «esplicite», che sottolinea come queste debbano figurare espressamente nell’informativa: da che si inferisce, come è stato notato, che i dati personali, ai fini della liceità del trattamento stesso, debbano essere ««trattati esclusivamente nell’ambito delle finalità che si intendono perseguire e delle quali gli interessati *devono* essere puntualmente

⁵³⁴ Oltre ai riferimenti già riportati *retro*, in part. al cap. 2, par. 3, cfr. sul punto M. TURILLI, L. FLORIDI, «The ethics of information transparency, in *Ethics and Information Technology*», 2009, 11, 2, 105; T. ZARSKY, «Transparent predictions», in *University of Illinois Law Review*, 2013, 4, 1507 ss.

⁵³⁵ V. *retro*, cap. 2 par. 3, e v. amplius nel prossimo paragrafo. Sul “transparency paradox”, cfr. subito l’importante contributo di N. M. RICHARDS, J. H. KING, «Three Paradoxes of Big Data», in *Stanford Law Review Online*, 2013, 66, 41 ss.

edotti tramite l'informativa»⁵³⁶. Il legislatore europeo pare allora consapevole dell'insufficienza della (mera) logica del consenso di fronte all'inarrestabile progresso tecnologico e alle declinazioni della tecnica sempre più "invasive" della sfera privata, statuendo che condizione indefettibile di liceità sia la strumentalità del trattamento alle sole finalità dichiarate (qualunque sia la base giuridica, anche diversa dal consenso dell'interessato, su cui il trattamento si fondi)⁵³⁷.

A testimoniare il fatto che il legislatore, avveduto soprattutto della natura dei più moderni servizi offerti sul *Web*, intenda anche far fronte al crescente fenomeno dei c.d. trattamenti secondari, ossia svolti per finalità diverse da quelle originariamente dichiarate, emerge dal combinato disposto tra l'art. 6 e il *considerando* 50 che il trattamento successivo *non potrà avvenire con finalità incompatibili rispetto alle originarie*, la valutazione in concreto (e quindi caso per caso) di conformità essendo posta in capo al titolare del trattamento: il *considerando* in questione prosegue con la puntuale indicazione degli elementi sulla base dei quali il titolare *dovrebbe* svolgere la valutazione medesima ⁵³⁸.

⁵³⁶ Cfr. L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., 55., la quale sottolinea pertanto come il principio di finalità si ponga come «limite intrinseco al trattamento lecito dei dati personali».

⁵³⁷ Cfr. M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», in *I poteri privati delle piattaforme*, (a cura di) P. STANZIONE, cit., p. 77 ss.

⁵³⁸ Cfr. infatti l'art. 6 par. 4, letto alla luce del *considerando* 50, che afferma: «Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;» Cfr. sul punto C. COLAPIETRO, «I principi ispiratori del Regolamento UE 2016/679 e la loro incidenza sul contesto normativo nazionale», cit., p. 23 ss; e si veda anche nello specifico GRUPPO DI LAVORO ARTICOLO 29 SULLA PROTEZIONE DEI DATI PERSONALI, *Opinion 03/2013 on purpose limitation*,

Successivamente l'art. 5, alla lett. c), enuncia il fondamentale principio di necessità, o, mutuando la terminologia del Regolamento, di *minimizzazione dei dati*: principio che, a sua volta, sembra “inglobare” quello di esattezza (*ex lett. d*) e quello di limitazione della conservazione (*ex lett. e*)⁵³⁹.

Se, in primo luogo, il principio di necessità- minimizzazione richiede che i dati siano caratterizzati da un *nesso di pertinenza ed adeguatezza rispetto alle finalità*, che impedisca strutturalmente la raccolta di dati eccedenti rispetto a quelle dichiarate (o compatibili con le prime), dall'altra esso pare imporre chiaramente che i sistemi di trattamento dei dati riducano *al minimo* l'utilizzazione dei dati personali⁵⁴⁰. La previsione pare allora tenere in debito conto tanto la dimensione dei c.d. “dati inferiti” cui già abbiamo fatto cenno, e quindi la capacità della tecnologia esistente di estrarre informazioni personali da masse non strutturate di dati anche non personali (o da semplici megadati), quanto l'insufficienza delle tecniche di *anonimizzazione* a tal scopo. Al contrario, la previsione sembrerebbe trovare una possibile specificazione di dettaglio nella misura tecnica e insieme organizzativa della *pseudonimizzazione* (che il dato non sottrae alla disciplina del GDPR ma che del dato minimizza, se non neutralizza, l'utilizzo medesimo)⁵⁴¹. In questo modo, allora, il principio di minimizzazione dei

2 aprile 2013 (in inglese). http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion_recommendation/files/2013/wp203_en.pdf.

⁵³⁹ Cfr. C. COLAPIETRO, «I principi ispiratori del Regolamento UE 2016/679», cit., p. 24 ss. L'art. 5, alle corrispondenti lettere, così recita: «(...) c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (...)»

⁵⁴⁰ Cfr., per un'analisi più approfondita, Cfr. R.D'ORAZIO, «Il principio di necessità nel trattamento dei dati», in V.CUFFARO, R.D'ORAZIO, V. RICCIUTO (a cura di), *Il Codice del trattamento dei dati personali*, cit., 20 ss; e L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, cit., 56

⁵⁴¹ Sul punto torneremo, ma cfr. da subito G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017, 34 ss.;

dati appare il risultato della trasposizione sul piano del diritto derivato in materia di *data protection* di quel *principio di precauzione* che permea il tessuto normativo del diritto primario dell'Unione: in questo senso, il principio in esame impone al titolare del trattamento una valutazione *ex ante* di pertinenza del dato rispetto al fine. Al contempo, il principio di minimizzazione pare rappresentare una declinazione settoriale del principio di proporzionalità, stentoreamente sancito dall'art. 52 della Carta di Nizza e, con riferimento al nostro ordinamento, ricompreso nel principio di ragionevolezza pacificamente desunto dall'art 3 della Costituzione, il quale assurge pertanto a «canone ermeneutico» privilegiato dell'intera disciplina sulla *privacy*⁵⁴².

Il principio di minimizzazione, infine, ha trovato espresso riconoscimento in alcuni pareri del Gruppo di Lavoro Articolo 29 , come il n. 2/2017 sul trattamento dei dati sul posto di lavoro, in cui si afferma a chiare lettere che «*The information registered from the on going monitoring, as well as the information that is shown to the employer, should be minimized as much as possible. Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances (...) Employers must take the principle of data minimization into account when deciding on the deployment of new*

e ancora F. FAINI, «Dati, algoritmi e Regolamento europeo 2016/679», cit., che afferma: «Il rischio si annida nelle inferenze che possono essere tratte su gruppi o individui da dati anonimi, grazie anche alla disponibilità di dati ausiliari riferibili alla persona».

⁵⁴² I riferimenti sono molti ed eterogeni; sul principio di proporzionalità, numerosi contributi sono già stati citati *retro*, per cui qui ci si limita a rinviare a M. CARTABIA, «I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana-Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta 24-26 ottobre 2013», in www.cortecostituzionale.it, 4 ss; per alcune riflessioni che il principio in questione legano alla specifica materia della *privacy* e della protezione dei dati personali, cfr. V. FIORILLO, «Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia», in *Federalismi.it*, n. 15/2017, 22 s, il quale ivi afferma che: «sia che la si legga come proporzionalità del trattamento strictu sensu, che come proporzionalità dell'intervento pubblico a limitazione della *privacy* individuale (...) si conferma protagonista anche all'interno del nuovo Regolamento europeo»

technologies (...) Whenever information is no longer needed it should be deleted»⁵⁴³.

3.1.3. Accountability, privacy by design e privacy by default. I nuovi istituti del GDPR nella società delle ICTs

Nel quadro dei principi delineato dal Regolamento, menzione a parte merita appunto quel nuovo approccio al rischio imperniato sul c.d. *principio di accountability*. È opportuno premettere che il significato giuridico riconducibile al lessema “*accountability*” risulta solo in parte espresso dal vocabolo comunemente utilizzato per tradurlo nella lingua italiana, ovvero “responsabilità”. A tal proposito, lo stesso Gruppo di Lavoro Articolo 29, nel suo parere n. 3 del 2010, propone un ampio ventaglio di traduzioni idoneo a non svilirne la portata semantica: accanto a, “responsabilità”, il parere individua quali traducenti possibili i vocaboli “affidabilità”, “assicurazione”, e le perifrasi “obbligo di rendicontare” e “attuazione dei principi concernenti il trattamento dei dati personali”⁵⁴⁴. Appare in ogni caso evidente che, comunque lo si intenda, il principio in questione si confronta con il problema rappresentato dalle misure di sicurezza che dovrebbero essere adottate a protezione dei dati personali al fine di

⁵⁴³ Cfr. Gruppo di Lavoro Articolo 29 sulla protezione dei dati personali, Opinion 2/2017 on data processing at work, WP 249, 8 giugno 2017.

⁵⁴⁴ Cfr. GRUPPO DI LAVORO ARTICOLO 29 SULLA PROTEZIONE DEI DATI PERSONALI, Opinion 3/2010 on the principle of accountability, WP 173, 13 luglio 2010, p. 4 ss. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf; è opportuno sottolineare che Il concetto di accountability è già presente nelle famose, già citate Linee Guida dell’OCSE del 1980 in base alle quali: “A data controller should be accountable for complying with measures which give effect to the [mate- rial] principles stated above”, cfr. OCSE, *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data*, 1980, <https://www.oecd-ilibrary.org/docserver/9789264196391-en.pdf>.

evitare o ridurre i rischi di accesso, di divulgazione e di distruzione dei dati (e più in generale tutti i c.d. *data breaches*), promuovendo – qui sta la novità – una autentica, concreta *responsabilizzazione* del titolare del trattamento⁵⁴⁵.

Quest'ultimo risulta innanzitutto sancito dal secondo paragrafo dell'articolo 5, il quale stabilisce che «il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo (“responsabilizzazione”)»: inciso chiarito attraverso la preziosa lente esegetica fornita dal *considerando* 74, che afferma come sia «opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto» aggiungendo poi che «il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.».

Ebbene, appare chiaro che il legislatore europeo intenda abbracciare una prospettiva che, come è stato da più parti osservato, individua nel titolare del trattamento (e, a cascata, nei suoi *preposti*, ossia nel/i responsabile/i del trattamento) il soggetto cui addebitare l'intera responsabilità (intesa tanto come responsabilità giuridica quanto come “cura amministrativa e organizzativa”) della complessa filiera del trattamento dei dati; articolando, alla luce di ciò, una serie di *doveri specifici* che, in prima approssimazione, consistono nell'adozione *sin dall'inizio* di misure (tecniche ed organizzative) sulla base delle valutazioni dei

⁵⁴⁵ Sul punto la letteratura è altrettanto vasta, ma per approfondire cfr. in modo particolare G. FINOCCHIARO, «Introduzione al regolamento europeo sulla protezione dei dati personali», cit., p. 10 ss.; ID., Privacy e protezione dei dati personali. Disciplina e strumenti operativi, Zanichelli Editore, 2012, cit., p. 289 ss.; A. Mantelero, «Responsabilità e rischio nel Reg. UE 2016/679», in *NLCC*, 1/2017, 144 ss.

rischi connessi al trattamento dei dati personali in termini di *impatto negativo sui diritti e le libertà degli interessati*⁵⁴⁶.

Le norme che specificano a livello applicativo il principio di *accountability* sono, innanzitutto, l'art. 24 e l'art. 32 del Regolamento.

La seconda in particolare, come è stato notato, sembra precipuamente preordinata a tradurre il suddetto principio generale in politiche e procedure concrete definite a livello dei soggetti di volta in volta responsabili nella filiera del trattamento, in conformità della disciplina vigente⁵⁴⁷. L'articolo 32 stabilisce in particolare che, tenendo conto specialmente dello «stato dell'arte e dei costi di attuazione», il titolare del trattamento di dati personali debba valutare le misure tecniche e organizzative da adottare sulla base della natura dei dati, dell'oggetto, delle finalità di trattamento; e, al contempo, debba metterle in atto. Misure che, a titolo non esaustivo, la norma stessa individua in particolare nella «pseudonimizzazione», nella «cifatura dei dati personali» nonché nella «capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento»⁵⁴⁸.

⁵⁴⁶ Cfr. L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, cit., p. 35 ss.; S. CALZOLAIO, «Protezione dei dati personali», cit., p. 630 ss.; ID., «Privacy by design», cit.

⁵⁴⁷ G. FINOCCHIARO, «Introduzione al Regolamento europeo sulla protezione dei dati personali», cit., p. 4.

⁵⁴⁸ V. art. 32, Regolamento UE 2016/679 (General Data Protection Regulation): «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifatura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla

È necessario subito aggiungere che il Regolamento non si limita a imporre al titolare di individuare e di attuare le misure in questione nella fase prodromica, o comunque iniziale, del trattamento, bensì prescrive al medesimo di svolgere una continua attività di monitoraggio per verificare che esse siano proporzionate e adeguate ai rischi, anch'essi in continuo mutamento. Tuttavia, tale aspetto dell'*accountability* del titolare emerge segnatamente dall'art. 24, che pare piuttosto definire l'intera architettura del sistema dei doveri gravanti sul medesimo soggetto, e dunque, più nello specifico, della sua attività di *valutazione, di prevenzione e di rendicontazione del rischio*⁵⁴⁹. Ebbene, in forza della disposizione medesima il titolare del trattamento è tenuto innanzitutto a delineare puntualmente i caratteri del trattamento, alla luce della natura, dell'ambito di applicazione e delle finalità opportunamente considerate; sulla base di tale prima valutazione, è tenuto a ponderare i rischi del trattamento sia sul versante della probabilità del verificarsi dei medesimi, sia sul versante della gravità della lesione dei diritti e delle libertà delle persone fisiche che possa conseguirne; solo allora il titolare del trattamento decide quali misure tecniche e organizzative sono adeguate per garantire che il trattamento sia effettuato conformemente alle disposizioni del regolamento e procede a metterle in atto⁵⁵⁰. Il paragrafo 2 è

perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".»

⁵⁴⁹ V. subito il testo della disposizione in esame, rubricato «Responsabilità del titolare del trattamento»: «1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.»

⁵⁵⁰ Cfr. sul punto ancora una volta G. Finocchiaro, Introduzione al Regolamento europeo sulla protezione dei dati personali, cit., p. 9 ss.; A. MANTELERO, «Responsabilità e rischio nel Reg. UE 2016/679», cit.; R. D'ORAZIO, Protezione dei dati by default e by design, in S. Sica,

cristallino nell'affermare che in capo al titolare grava poi non solo l'onere di dimostrare che le misure in questione siano state poste in essere e che fossero idonee alla luce del Regolamento medesimo; ma anche che queste siano «riesaminate e aggiornate qualora necessario», con ciò evidenziandosi l'importanza delle attività *monitoraggio* che al titolare compete.

Il Regolamento non si ferma qui, e accoglie nel proprio impianto assiologico, prima ancora che normativo, due principi che del principio di minimizzazione e di *accountability* sono forse le più analitiche espressioni: ci riferiamo ai principi di *privacy by design* e di *privacy by default*, il primo dei quali già traspare dall'art. 24, ma entrambi compiutamente sanciti dall'art. 25 (rubricato, proprio per questo «Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita»), rispettivamente al primo e al secondo comma. Principi che, in estrema approssimazione, impongono al titolare di «implementare misure in grado di proteggere efficacemente i dati personali *al momento della progettazione* di processi e modelli di trattamento, e di *garantire il rispetto del principio di necessità* nel corso dell'esecuzione dei trattamenti»⁵⁵¹.

V.D'Antonio, G.M.Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., 87 s. Opportuno appare anche rilevare come il combinato disposto tra art. 32 e *considerando* 78 indirizzino il Titolare verso determinate specie concrete di misure, ex ante ritenute dal legislatore generalmente idonee allo scopo; e come l'ultimo paragrafo sottolinei come l'osservanza dei c.d. codici di condotta e dei meccanismi di certificazione agevoli il Titolare nell'assolvimento del suddetto onere della prova, rappresentando elemento utile, se non *preponderante*, a tale scopo.

⁵⁵¹ La citazione è di L. CALIFANO, Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali, cit., 34 ss, ma la letteratura su tali concetti, declinati nello specifico ambito del Regolamento, è vasta. Cfr. D'ORAZIO, Protezione dei dati by default e by design, in Sica, D'Antonio, Riccio, *La nuova*, cit., 79 ss.; S. Calzolaio, «Privacy by design», cit., p. 12 ss.; CALZOLAIO, PAGANELLI, «From data protection to privacy by research. Food for thoughts in the light of the new General data Protection Regulation», in *Law and Administration XXI Century*, n. 4(41)/2016, 80 ss.; Cfr. G. D'ACQUISTO, M. NALDI, *Big data e privacy by design*, cit. Nel presente lavoro, viene prevalentemente seguito l'approccio di S. Calzolaio e di U. Pagallo nelle diverse opere rispettivamente citate nel corso della trattazione

Se è stato Lawrence Lessig nella sua opera capitale, “*Code 2.0*” ad «aver attirato l’attenzione dei giuristi sui modi in cui il design determini e/o condizioni il comportamento dei soggetti, sia nel mondo reale sia nel mondo virtuale di internet»⁵⁵², la nozione di *privacy by design* deve tuttavia farsi risalire al lungo lavoro speculativo, filosofico prima ancora che giuridico, di Anne Cavoukian, che tale espressione ha coniato per riferirsi all’opportunità di garantire la protezione dei dati personali fin dal momento della progettazione (architettura) dei sistemi hardware e software attraverso i quali, successivamente, si svolgerà il trattamento dei dati personali⁵⁵³.

Il Regolamento accoglie il concetto in esame; e tuttavia, distanziandosi dalle intenzioni dei suoi teorici, che individuavano come suo primario termine di riferimento la progettazione di applicazioni, servizi, e prodotti nel contesto delle ICTs, e dunque come principali destinatari i produttori dei medesimi, esso lo declina in capo al titolare del trattamento (e, solo per suo tramite, nei confronti di chi definisce l’architettura hardware e software dei sistemi informatici), ovvero sia in termini di *protezione sin dalla progettazione del trattamento*⁵⁵⁴. Sebbene tale

⁵⁵² La citazione è di U. PAGALLO, «Privacy e design», in ID, n. 1/2009, e si riferisce all’opera di L. LESSIG, *Code 2.0*, cit.; lo stesso autore indica come utile al fine di introdursi alla teoria generale del design la lettura di YEUNG, «Towards an understanding of regulation by design, in *Regulating technologies. Legal futures, regulatory frames and technological fixes*», (a cura di) Brownsword, Yeung, London, Hart publishing, 2008, 79 ss.

⁵⁵³ Per la genesi storica, e insieme per un approfondimento, del concetto in esame, nel contesto teorico in cui è nato, cfr. A. CAVOUKIAN, *7 foundational principles of privacy by design*, Office of the Information & Privacy Commissioner of Ontario, 2010.; ID., «Patience, Persistence, and Faith: Evolving the Gold Standard in Privacy and Data Protection», in *Future Challenges in Security and Privacy for Academia and Industry*, (a cura di) Camenisch, Fischer Hubner, Murayama, Portmann, Rieder, Springer, 2011, 1 ss., spec. 7 ss..

⁵⁵⁴ Per la ricostruzione del dibattito sul punto, cfr. S. CALZOLAIO, «Protezione dei dati personali», p. 633. A rimarcare la discrasia in questione si aggiunge anche la lettera del considerando 78, che, in riferimento alle misure tecniche ed organizzative, rivolge l’attenzione non esclusivamente al Titolare del trattamento, bensì anche ai «produttori dei prodotti, dei servizi e delle applicazioni», i quali «in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni (...) dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppino e progettano tali prodotti, servizi e

positivizzata prospettiva “riduttiva” abbia prestato il fianco a critiche, nondimeno la disciplina in esame presenta ampi tratti di novità e garantisce ulteriori presidi ai diritti fondamentali degli interessati nel contesto dei *data processing*, specialmente se automatizzati: in particolare, vincolando i titolari, si sostiene che possa riverberarsi (come istanza dai primi rivolta ai secondi) sugli stessi produttori di ICTs, spingendo questi ultimi a integrare orientamenti di *privacy by design* già nei prodotti e nei sistemi informatici che “ospitano” il trattamento⁵⁵⁵.

Il comma primo dell’art. 25, riepilogando anche in parte le fasi del processo di “responsabilizzazione” del titolare del trattamento ed arricchendo (nonché specificando) i principi di “progettazione del trattamento” già enunciati dall’art. 24, stabilisce allora che «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, *sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate*», a titolo esemplificativo essendo citata la pseudonimizzazione; misure a loro volta dirette «*ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*».

applicazioni e, tenuto debito conto dello stato dell’arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati».

⁵⁵⁵ Esprime entrambe le suddette prospettive (quella critica e quella fiduciosa in ordine a tale “*butterfly effect*”) lo stesso EDPS: in THE EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7-3-2012, il Garante Europeo afferma infatti che «*The principles of data protection by design and by default are not presently addressed to advisers, developers and producers of hardware or software. However, they will be relevant for them from the start, as controllers are bound by them and accountable for compliance. In other words, obligations for controllers (and for processors, as mentioned above) are likely to create some incentives for the market of relevant goods and services*».

Centrali appaiono ancora una volta i principi di proporzionalità e di ragionevolezza: nella prospettiva del legislatore, quanto più il trattamento appare suscettibile di comportare il rischio di una circolazione di dati personali in ambiente digitale, tanto più si fanno stringenti le esigenze strutturali di minimizzazione e di pseudonimizzazione dei dati trattati fin dalla progettazione del trattamento⁵⁵⁶.

A completare l'articolata disciplina interviene allora il principio di *privacy by default*, o protezione dei dati per impostazione predefinita, enunciato dal paragrafo successivo, che, come è stato notato, appare una più che opportuna specificazione del principio generale di minimizzazione dei dati *ex art. 5 par. 1 lett. c)*⁵⁵⁷.

Esso, in poche parole, stabilisce che il titolare del trattamento *deve* garantire, in primo luogo, che l'infrastruttura tecnica di cui si avvale consenta di svolgere il trattamento utilizzando «solo i dati personali necessari per ogni specifica finalità del trattamento», ribadendosi contestualmente lo scopo cui tale strategia (vincolante) di progettazione risulta normativamente preordinata, ossia evitare, attraverso i *default settings*, che «siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica»⁵⁵⁸.

⁵⁵⁶ S. CALZOLAIO, «Protezione dei dati personali», cit. p. 632.

⁵⁵⁷ Cfr. R. D'ORAZIO, Protezione dei dati by default e by design, in Sica, D'Antonio, Riccio, *La nuova*, cit., 79 ss.

⁵⁵⁸ V. il par. 2 dell'art. 25, che recita: « Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.». Occorre aggiungere che anche il paragrafo 3 del presente articolo afferma come un “elemento” che possa essere utilizzato dal Titolare per dimostrare la conformità ai requisiti della *privacy by design* e *by default* si identifica in un meccanismo di certificazione riconosciuto ai sensi dell'art. 42».

Concludiamo la nostra disamina dei principi fondamentali del GDPR evidenziando che l'intento, espresso dal principio di *accountability* e nella sua più specifica declinazione rappresentata dalla *privacy by design*, di valorizzare in capo ai *data controller* l'adozione di comportamenti proattivi e di misure idonee ad assicurare e a dimostrare la corretta applicazione della disciplina europea, in una prospettiva di tutela preventiva, viene ulteriormente perseguito dal legislatore introducendo determinati istituti che si inscrivono a pieno titolo nella suddetta ottica di responsabilizzazione, e che potrebbero anzi dirsi vere e proprie proiezioni applicative del concetto di *privacy by design*: ci riferiamo, soprattutto, alla c.d. *Privacy Impact Assessment* e alla nuova figura del *Data Protection Officer*.

In breve, il primo istituto trova il proprio fondamento normativo nell'art. 35 (rubricato «Valutazione preventiva d'impatto sulla protezione dei dati»), il quale al paragrafo primo impone al titolare del trattamento, a fronte di situazioni che alla luce di una ponderazione compiuta nell'osservanza dei richiamati principi evocano la possibile configurazione di gravi rischi per i diritti e le libertà dell'interessato, di effettuare, prima di procedere al trattamento, una «*valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali*»⁵⁵⁹.

Dopo aver enucleato tale ipotesi generale, la norma stessa al paragrafo 3 individua, sebbene in modo abbastanza generico, tre fattispecie di trattamento al ricorrere delle quali il titolare ha l'*obbligo* di svolgere la valutazione d'impatto. Tutte e tre risultano particolarmente rilevanti nella materia che occupa la presente trattazione, e specialmente quella prevista dalla lettera a), che si riferisce a qualsiasi trattamento consistente in una «valutazione sistematica e globale di

⁵⁵⁹ Art. 35, par. 1: «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.»

aspetti personali relativi a persone fisiche, basata su un *trattamento automatizzato*, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche»: il legame con la fattispecie disciplina dall'art. 22 del Regolamento appare da subito evidente. Ci si tornerà più avanti.

Completano la previsione del terzo comma le lettere b) e c), che individuano quali trattamenti rispetto ai quali sussiste l'obbligo suddetto di *Privacy Impact Assessment* quei «trattament[i], su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10» e quelle operazione che si risolvano nella «sorveglianza sistematica su larga scala di una zona accessibile al pubblico».

Solo se dalla valutazione d'impatto emerge l'esistenza di un rischio elevato in assenza di misure di attenuazione del rischio il titolare del trattamento, *ex art. 36*, è tenuto a consultare preventivamente l'autorità di controllo⁵⁶⁰: come è stato sottolineato, l'introduzione dell'istituto di cui all'art. 35 ha pertanto consentito ragionevolmente al legislatore europeo di superare la previsione, contenuta nella previgente direttiva, dell'obbligo generale, in riferimento ad alcuni trattamenti, di notifica alla autorità di controllo⁵⁶¹.

⁵⁶⁰ Cfr. il primo par. dell'art. 36 (rubricato «Consultazione preventiva»): Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

⁵⁶¹ G. GIANNONE CODIGLIONE, «Risk-based approach e trattamento dei dati personali», cit., p. 68 ss., in cui viene svolta una più approfondita analisi dell'istituto della Valutazione preventiva d'impatto. L'opportunità del superamento di tale obbligo generale, con la previsione della Valutazione d'impatto e il collegato istituto della (meno frequente) Consultazione preventiva, viene sottolineato dal legislatore stesso al considerando 89, che recita: «La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali (...)».

L'ultimo istituto di cui ci occupiamo è il *Data Protection Officer* (DPO, nella traduzione italiana «responsabile della protezione dei dati»), cui lo stesso art. 35 al par. 2 fa riferimento stabilendo che «il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno»⁵⁶².

La figura in questione viene puntualmente enucleata e disciplinata dall'art. 37 che al primo paragrafo individua *inderogabilmente* le fattispecie in cui il titolare del trattamento e il responsabile del trattamento sono tenuti a designare il DPO. In primo luogo, ai sensi della lettera a), pare che i soggetti pubblici («autorità pubblica», «organismo pubblico») debbano sistematicamente nominare un DPO, ad eccezione delle autorità giurisdizionali quando esercitino le loro funzioni giurisdizionali; per quanto attiene a tutti gli altri soggetti, invece, l'articolo obbliga alla designazione del DPO quando le «attività principali del titolare», considerati i caratteri del trattamento, «richiedono il monitoraggio regolare e sistematico degli interessati su larga scala» (lettera b)), o quando consistono nel trattamento, su larga scala, di categorie particolari di dati, di cui all'art. 9 o di dati relativi a condanne penali e reati di cui all'art. 10 (lettera c))⁵⁶³.

⁵⁶² Per una più puntuale analisi dell'istituto, cfr. subito V. RICCIO, «Data protection officer e altre figure», in Sica, D'Antonio, Riccio, cit., 33 ss., spec. 49 ss.

⁵⁶³ V. il primo paragrafo della disposizione in esame (rubricato «Designazione del responsabile della protezione dei dati»), che recita: «1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniquale volta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure; c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10».

Passando brevemente in rassegna il dettato delle disposizioni a tale figura dedicate, dal quarto paragrafo del medesimo articolo emerge che il DPO deve essere designato in funzione delle qualità professionali ed è tenuto ad una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di «assolvere ai compiti di cui all'art. 39» (tra i quali, facendo un solo esempio, si annoverano l'informazione e la consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento medesimo).

Alla luce degli artt. 38 e 39, i compiti del DPO si dipanano essenzialmente su due fronti: nei confronti del titolare/responsabile del trattamento, poiché spetta al DPO fornire consulenza e sorvegliare la corretta applicazione della normativa in materia di protezione dei dati; e nei confronti dell'Autorità di controllo, con cui il DPO è chiamato a collaborare e a fungere da «punto di contatto» (in particolare in caso di comunicazione preventiva). Non si può tuttavia escludere (come emerge dall'art. 38, par. 4) che il DPO possa avere una funzione anche nei confronti dei soggetti interessati dal trattamento, i quali hanno diritto di ottenerne i dati di contatto da parte del titolare (cfr. gli artt. 13 e 14).

Prima di concludere il quadro generale che stiamo delineando, occorre soffermarsi su un altro profilo di assoluto rilievo nell'ambito della *data driven society*, e della stessa automazione della filiera del trattamento dei dati personali.

Ci si riferisce al generale potenziamento degli strumenti che la normativa europea offre ai singoli individui ai fini della *tutela collettiva* del proprio diritto, a completa dimostrazione della maturata consapevolezza, in senso alle istituzioni UE, della *dimensione sociale* dell'interesse alla protezione dei dati personali, e della fragilità della persona umana e della sua capacità di autodeterminarsi laddove lasciata “sola” (e dunque, anche, laddove tenuta a difendersi

singularmente) di fronte alle possibili manipolazioni ed alle eventuali discriminazioni che la *società gli algoritmi* appare capace di realizzare⁵⁶⁴.

A tal riguardo, spicca nella sistematica del Regolamento l'art. 80: disposizione che, se al primo paragrafo prevede il diritto dell'interessato di «dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro (...) i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti (...) nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento (...)», al par. 2 in modo autenticamente innovativo afferma che «gli Stati membri possono prevedere che un organismo, organizzazione o associazione [...], indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79 [es. diritto ad un ricorso giurisdizionale effettivo] (...) qualora ritenga che i diritti dell'interessato (...) siano stati violati in seguito al trattamento». In questo modo, come è stato notato, «la protezione del singolo “si sgancia” dalla necessità di azione da parte dell'individuo stesso e può essere attivata da organizzazioni e associazioni nel momento in cui siano violati quei valori collettivi protetti dalla disciplina»⁵⁶⁵.

All'esito della “carrellata” che abbiamo compiuto, appare chiaro come il GDPR. introduca molteplici novità, ma con una chiara coscienza della necessità di una attuazione progressiva dei nuovi principi e dei nuovi istituti: ne sono un segno evidente non solo i diversi rinvii alla integrazione da parte degli Stati

⁵⁶⁴ Cfr. in particolare Cfr. A. MANTELERO, «I Big Data nel quadro della disciplina europea della tutela dei dati personali», in *Il Corriere giuridico*, ed. speciale, 2018, 54 ss.

⁵⁶⁵ F. FAINI, «Dati, algoritmi e Regolamento europeo 2016/679», cit., pp. 345-346

membri (es. cons. 8) contenuti nell'articolato, ma anche il ruolo riconosciuto alla cosiddetta *soft law* (codici di condotta, linee guida, elenchi, ecc.) e agli atti delegati della Commissione europea (cfr. art. 92).

È tuttavia altrettanto chiaro che se lo stesso principio di *privacy by design*, nato in territorio americano, si è fatto ampiamente strada proprio nell'Unione europea, ciò è da imputarsi al fatto che l'ordinamento europeo, in quanto realtà ascrivibile all'elenco dei principali *consumatori* di ICTs, e conseguentemente dei principali *bacini* di provenienza dei dati, avverte in modo particolare l'esigenza di tutelare l'autodeterminazione tanto dei singoli quanto dei gruppi⁵⁶⁶: come è stato notato in questo senso allora il fine più "alto" del Regolamento è quello di rappresentare uno «standard globale» di tutela, capace di diffondersi "viralmente" grazie alla ragionevolezza ed alla utilità dell'approccio di tutela in esso contenuto⁵⁶⁷.

Resta, tuttavia, da osservare nello specifico se, nella contemporanea società datificata, caratterizzata dai *Big Data*, dall'Intelligenza Artificiale e dal pericolo della sorveglianza di massa, la disciplina predisposta (principalmente) dal GDPR sia *effettivamente* idonea a garantire la libertà della persona fisica di autodeterminarsi nelle proprie scelte esistenziali: presupposto per l'esercizio di qualsiasi altra libertà fondamentale, e, in definitiva, per la libera costruzione della propria personalità secondo il dettato dell'art. 2 della Costituzione.

È il momento, insomma, di concentrarci sulla disciplina dei trattamenti automatizzati dei dati personali.

⁵⁶⁶ Cfr. A. CAVOUKIAN, «Privacy by Design: Leadership, Methods, and Results», in *European Data Protection: Coming of Age*, (a cura di) Gutwirth Leenes de Hert Poullet, Springer, 2013, 175

⁵⁶⁷ Cfr. G. BUTTARELLI, «The EU GDPR as a clarion call for a new global digital gold standard», in *International Data Privacy Law*, 2/2016, 77-78; S. CALZOLAIO, «Protezione dei dati personali», cit., p. 635.

3.2. Il trattamento automatizzato dei dati personali: la disciplina del GDPR alla luce delle linee guida del Gruppo di Lavoro Articolo 29

Come abbiamo già avuto modo di anticipare all'inizio del presente capitolo, la fonte della disciplina attualmente vigente nella specifica materia che ci occuperà d'ora in poi si rintraccia nel GDPR, che abbiamo poc'anzi esaminato nei suoi lineamenti essenziali.

Ai fini dell'analisi della disciplina dei trattamenti automatizzati, nel prosieguo si farà riferimento costante alle fondamentali Linee Guida in materia di processi decisionali automatizzati relativi alle persone fisiche, adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018, che costituiscono opera del Gruppo di Lavoro Articolo 29 per la protezione dei dati (in inglese *Article 29 Working Party*, abbreviato WP29), oggi sostituito dall'*European Data Protection Board* (abbreviato EDPB), già più volte citate nel corso della trattazione⁵⁶⁸. Si seguirà, pertanto, la struttura argomentativa delle Linee Guida in parola, le quali, nel contesto del GDPR, limpidamente individuano un *corpus* di disposizioni generali, applicabile a qualsiasi trattamento ricadente nell'ambito di applicazione, *rationae personae* e *ratione materiae*, del Regolamento (compresi, dunque, i trattamenti parzialmente o totalmente automatizzati); e, in parallelo, un sub-sistema di norme specificamente riguardanti la cruciale categoria dei processi decisionali *interamente* automatizzati compresa la profilazione: regime, pertanto, speciale e derogatorio rispetto a quello previsto dal suddetto *corpus* generale.

⁵⁶⁸ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, WP 251 rev.01, adottate il 3 ottobre 2017 (versione emendata e adottata in data 6 febbraio 2018)

È necessario preliminarmente ricordare che il Gruppo di Lavoro Articolo 29 per la Protezione dei Dati (nella versione originale inglese *Article 29 Working Party*, abbreviato WP 29) costituiva l'organo consultivo indipendente dell'Unione europea per la protezione dei dati personali e della vita privata, istituito in forza dell'art. 29 della previgente Direttiva 95/46/CE, rubricato «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali»: in forza di tale disposizione, tale organo risultava «composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante della o delle autorità create per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione». Lo stesso organo, in forza dell'articolo 30, risultava investito di un nutrito insieme di funzioni, prevalentemente consultive o di indirizzo, tra le quali, oltre al compito di esaminare «ogni questione attinente all'applicazione delle norme nazionali di attuazione» della direttiva e di «formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi», rilevava la formulazione «*di propria iniziativa* [di] raccomandazioni su qualsiasi questione riguardante la tutela delle persone nei confronti del trattamento di dati personali nella Comunità»: previsione sulla cui base, tradizionalmente, esso ha fondato la ripetuta adozione di linee guida in ordine ai più importanti settori della *data protection*, specialmente quelli oggetto di contrasti interpretativi, tra le quali ricadono dunque anche quelle in esame nel presente paragrafo e in quelli a seguire⁵⁶⁹.

⁵⁶⁹ Cfr. Può essere utile, per sottolineare l'importante ruolo svolto dal Gruppo nel quadro del sistema europeo della *data protection*, riportare qui l'intero disposto dell'articolo 30 della dir. 95/46/CE: « 1. Il gruppo ha i seguenti compiti: a) esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente direttiva per contribuire alla loro applicazione omogenea; b) formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi; c) consigliare la Commissione in merito a ogni progetto di modifica della presente direttiva, ogni progetto di misure aggiuntive o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano

Oggi, l'organo in questione è stato sostituito dal c.d. Comitato Europeo per la protezione dei dati (in inglese, *European Data Protection Board*, abbreviato in EDPB), istituito ai sensi degli articoli 68 e seguenti del Regolamento UE 2016/679, che ricalcano, implementandole (stante la diversa natura della fonte di diritto in questione), le previsioni della previgente direttiva, tanto in termini di struttura, di composizione e di organigramma, quanto in punto di funzioni imputate al Comitato medesimo: di particolare rilievo risulta l'art. 70, che nell'attribuire ad esso il compito di adottare linee guida in ordine ad una nutrita schiera fattispecie, esplicitamente alla lettera c) del par. 1 ricomprende «linee guida, raccomandazioni e migliori pratiche conformemente alla lettera e) del presente paragrafo, [al fine di] specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione ai sensi dell'articolo 22, paragrafo 2»; lettera e) che più in generale stabilisce come il Comitato « esamin[i], di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblic[hi] linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento»⁵⁷⁰.

su tali diritti e libertà; d) formulare un parere sui codici di condotta elaborati a livello comunitario. 2. Il gruppo, qualora constati che tra le legislazioni o prassi degli Stati membri si manifestano divergenze che possano pregiudicare l'equivalenza della tutela delle persone in materia di trattamento dei dati personali nella Comunità, ne informa la Commissione. 3. Il gruppo può formulare di propria iniziativa raccomandazioni su qualsiasi questione riguardante la tutela delle persone nei confronti del trattamento di dati personali nella Comunità. 4. I pareri e le raccomandazioni del gruppo vengono trasmessi alla Commissione e al comitato di cui all'articolo 31. 5. La Commissione informa il gruppo del seguito da essa dato ai pareri e alle raccomandazioni. A tal fine redige una relazione che viene trasmessa anche al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione. 6. Il gruppo redige una relazione annuale sullo stato della tutela delle persone fisiche con riguardo al trattamento dei dati personali nella Comunità e nei paesi terzi e la trasmette alla Commissione, al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione».

⁵⁷⁰ V. art. 70 del Regolamento UE 2016/679. Cfr. anche le informazioni presenti sito istituzionale dell'EDPB, consultabili qui: https://web.archive.org/web/20180614122818/https://edpb.europa.eu/news/news/2018/europe-s-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en.

Ora, sebbene le linee guida del Gruppo di Lavoro (prima) e del Comitato che lo sostituisce (oggi) rappresentino atti di *soft law*, e dunque, secondo le considerazioni già svolte, giuridicamente non vincolanti né per le istituzioni europee, né per gli Stati membri e per i suoi cittadini, esse rappresentano un fondamentale e soprattutto autorevole *ausilio interpretativo* in relazione alle disposizioni recate dagli atti normativi dell'Unione: ciò, anche in punto di trattamenti automatizzati nel contesto del diritto comunitario, è ampiamente dimostrato dal fatto che pressoché tutta la letteratura esistente, indifferentemente aderendo o piuttosto respingendo le proposte esegetiche promosse dal Comitato, si confronta con il suddetto strumento⁵⁷¹. Per questo, nell'analizzare le disposizioni rilevanti in materia, si è deciso di tenerlo in elevata considerazione.

Le Linee Guida in materia di processi decisionali relativi alle persone fisiche (d'ora in poi, soltanto Linee Guida) si aprono subito sottolineando come il GDPR si occupi in maniera specifica della profilazione, evidentemente considerata la più rilevante declinazione della categoria dei sistemi parzialmente o totalmente automatizzati di trattamento (lo vedremo), e dei processi decisionali automatizzati *compresa* la profilazione: con ciò ponendosi le premesse per la distinzione concettuale tra le due espressioni che verrà svolta alcune pagine

⁵⁷¹ Per fare solo dei primi, introduttivi esempi, cfr. I. MENDOZA, L.A. BYGRAVE, «The Right Not to be Subject to Automated Decisions Based on Profiling», cit.; S. WACHTER, B. MITTELSTADT, L. FLORIDI, «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», in *International Data Privacy Law*, Volume 7, Issue 2, May 2017, 76-99, <https://doi.org/10.1093/idpl/ix005>; G. MALGIERI, G.. COMANDÈ, «Why a Right to Legibility of Automated Decision- Making Exists in the General Data Protection Regulation», cit.; S. WACHTER, B. MITTELSTADT, C. RUSSELL, «Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR», in *Harvard Journal of Law & Technology*, 31 (2), 2018, disponibile su SSRN: <https://ssrn.com/abstract=3063289> or <http://dx.doi.org/10.2139/ssrn.3063289> R. MESSINETTI, Privacy e controllo dell'identità algoritmica, cit.;

avanti⁵⁷². Il Gruppo tuttavia offre subito una precisazione: i rilievi concernenti la disciplina dei trattamenti automatizzati relativi alle persone fisiche *in generale*, che trova il suo fondamento normativo nelle disposizioni del GDPR, valgono anche, *in quanto compatibili*, per la disciplina della profilazione e dei processi decisionali automatizzati configurate dalle analoghe disposizioni previste dalla Direttiva UE 2016/680 sul trattamento dei dati personali da parte dell'Autorità Giudiziaria e dell'Autorità di Pubblica Sicurezza (come già abbiamo detto, *lex specialis* rispetto al GDPR); aggiungendo poi che «le caratteristiche specifiche della profilazione e del processo decisionale automatizzato relativo alle persone fisiche ai sensi della direttiva 2016/680 sono analizzate nel parere del Gruppo di Lavoro Articolo 29 intitolato «Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)»⁵⁷³. Pertanto, anche noi tralasceremo l'analisi specifica delle pertinenti disposizioni recate dalla normativa speciale in questione, riservandoci di evidenziarne, laddove necessario, solo gli aspetti in cui maggiormente si distinguono da quelle del GDPR⁵⁷⁴.

Il Gruppo di Lavoro svolge alcune considerazioni preliminari sull'importanza strategica e insieme sul ruolo problematico assunti tanto dalla profilazione quanto dai sistemi (e dai relativi processi) automatizzati di *decision*

⁵⁷² GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 5.

⁵⁷³ *Ibidem*, nota 1. Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere su alcune questioni chiave della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie*, adottato il 29 novembre 2017, che tratta tali aspetti alle pagine 11-14. Tale parere è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178.

⁵⁷⁴ Torneremo essenzialmente sul punto nel prossimo paragrafo, in cui analizzeremo la disciplina dell'art. 22: in tale contesto, faremo un fugace riferimento all'art. 11 della Direttiva 2016/680, che della medesima fattispecie si occupa. Cfr. già sul punto I. MENDOZA, L.A. BYGRAVE, «The Right Not to be Subject to Automated Decisions Based on Profiling», cit., p. 6, in part. Nota 22.

making. Forti delle osservazioni svolte nel paragrafo conclusivo del secondo capitolo, ed accontentandoci per ora delle “generalì” definizioni ivi ricostruite dei due concetti in esame, possiamo focalizzarci sulla prospettiva adottata dal Gruppo.

Subito, viene rilevato come i fenomeni in esame trovino sempre maggiore diffusione tanto nel settore pubblico quanto nel settore privato: «Banche e finanza, assistenza sanitaria, fiscalità, assicurazioni, marketing e pubblicità sono soltanto alcuni esempi dei settori nei quali la profilazione viene effettuata con maggiore regolarità a sostegno del processo decisionale.». Segnatamente, si sottolinea come «i progressi tecnologici e le capacità in materia di analisi dei megadati (big data), intelligenza artificiale e apprendimento automatico hanno reso più facile la creazione di profili e l’adozione di decisioni automatizzate»: tutti profili su cui ci siamo già, a livello tecnologico e di implicazioni filosofiche, prima ancora che giuridiche, soffermati nelle pagine addietro. Conseguimenti di tale specie possono, allora, offrire significativi vantaggi per le persone fisiche e per le «organizzazioni» offrendo loro vantaggi quali «miglioramento dell’efficienza» e «risparmi di risorse». Essi presentano poi numerose applicazioni commerciali, potendo essere utilizzati per «segmentare meglio i mercati e personalizzare i servizi e i prodotti allineandoli alle singole esigenze»; a beneficiarne potrebbero poi essere «la medicina, l’istruzione, l’assistenza sanitaria e i trasporti»⁵⁷⁵.

Tuttavia, e qui si rinviene il baricentro dell’intera premessa, quegli stessi progressi così potenzialmente vantaggiosi per i singoli consociati e per lo sviluppo della collettività in termini di *benessere* (non solo economico) possono avere ripercussioni significative di ordine *negativo* sui diritti e sulle libertà delle persone fisiche, le quali a fronte di tali «rischi significativi», richiedono «garanzie

⁵⁷⁵ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit. p. 6.

adeguate». Gli aspetti potenzialmente più perniciosi per l'integrità degli attributi fondamentali della persona umana sono dallo stesso organo individuati in quei fenomeni che possono essere sintetizzati nei concetti di "reinvestimento del surplus comportamentale" e di *black-box*⁵⁷⁶: il Gruppo sottolinea infatti come «la diffusa disponibilità di dati personali su Internet e di quelli ricavabili dai dispositivi di Internet delle cose, associata alla *capacità di trovare correlazioni e creare collegamenti*, può consentire la determinazione, l'analisi e la previsione di aspetti della personalità, del comportamento, degli interessi e delle abitudini di una persona»; e, al contempo, che «questi processi possono essere poco trasparenti. Le persone fisiche potrebbero non sapere di essere profilate o non comprenderne le conseguenze»⁵⁷⁷. Sul tema della trasparenza algoritmica le Linee Guida si soffermano più avanti, e dunque vi torneremo anche noi: quello che qui conta è sottolineare come la premessa riconosca che la profilazione e i processi decisionali automatizzati, e più in generale tutto l'universo dell'elaborazione dei dati per mezzo dell'automazione, si fondino oggi, come già ampiamente rilevato, sugli algoritmi⁵⁷⁸.

Il Gruppo fa poi immediatamente riferimento, sebbene ancora sintetico, nello specifico ai rischi configurati dalla profilazione, a testimonianza dell'impatto che *soprattutto* tale tipologia di trattamento automatizzato possa

⁵⁷⁶ Sul primo fondamentale concetto nel contesto della "società sorvegliata", cfr. S. ZUBOFF, *Il Capitalismo della Sorveglianza*, cit., p. 74 ss., in cui l'autrice si sofferma sull'epocale implementazione di tecnologie (impiegate, come primo tra gli OTT, da Google) capaci di tradurre le «interazioni con gli utenti che avvengono fuori dal mercato in un surplus grezzo da usare come materia prima per costruire prodotti diretti a vere transazioni economiche con i [propri] veri clienti: gli inserzionisti» (p. 104), e in cui introduce e spiega i concetti di «ciclo del reinvestimento del surplus comportamentale» e di «mercato dei comportamenti futuri»; sul secondo, v. *retro* e ancora una volta F. PASQUALE, *The Black-Box Society*, cit.

⁵⁷⁷ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 6.

⁵⁷⁸ V. *retro*, cap. 2 par. 3; e cfr. ancora una volta STEINER, *Automate this. How algorithms came to rule our world*, Penguin, 2012, passim; e WITTEN, FRANK, HALL, PAL, *Data Mining. Practical Machine Learning Tools and Techniques*, cit., passim.

avere sulla libertà di autodeterminazione delle persone fisiche: «La profilazione può *perpetuare stereotipi e la segregazione sociale*. Può anche *confinare una persona in una categoria specifica* e limitarla alle preferenze suggerite per tale categoria. Ciò può minare la libertà delle persone di scegliere, ad esempio, determinati prodotti o servizi (...) in taluni casi, la profilazione può portare a previsioni imprecise, in altri al diniego di servizi e beni e a discriminazioni ingiustificate»⁵⁷⁹. Tali rilievi preliminari sono utili ad evidenziare ulteriormente il potenziale discriminatorio insito nelle tecnologie che sfruttano i dati con finalità *estrattiva*: basti pensare, per portare un esempio, a quel fenomeno che alcuni studiosi definiscono «bolla di filtraggio nei motori di ricerca», o *filter bubble*, e che si identificherebbe nella tendenza dell'algoritmo medesimo ad utilizzare informazioni sull'utente (come posizione, click precedenti, ricerche passate) per scegliere selettivamente, tra tutte le risposte, quelle all'utente più gradite (perché ideologicamente conformi), con il risultato di isolare il soggetto da informazioni che siano in contrasto con il suo punto di vista⁵⁸⁰. Fenomeno, e intrinseci rischi, a cui nell'inciso sopra riportato il Gruppo sembra fare implicito riferimento.

La premessa teorica, o sarebbe meglio dire la “*Weltanschauung*”, fatta propria dal Gruppo di Lavoro nelle Linee Guida in esame non è isolata nel panorama istituzionale (altre organizzazioni internazionali, organi consultivi, comitati promotori dei diritti civili istituiti in seno alle prime ed Autorità Garanti per la protezione dei dati personali) europeo (e non solo, come vedremo nel prossimo capitolo).

⁵⁷⁹ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 7.

⁵⁸⁰ Cfr. sul tema E. PARISER, *The Filter Bubble: What The Internet Is Hiding From You*, Paperback, 2012, passim. Più in generale, sulla potenziale segregazione determinate dagli “algoritmi di profilazione”, cfr. B.W. SCHERMER, *The Limits of Privacy in Automated Profiling and Data Mining*, cit.

Le considerazioni in analisi trovano un loro precedente “internazionale” nella Raccomandazione n. 13 del Comitato dei Ministri del Consiglio d’Europa agli Stati Membri, non a caso in materia di protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali «nel contesto di attività di profilazione»⁵⁸¹. In esse il Comitato, soffermandosi in prima battuta sulla capacità delle ICTs di consentire la raccolta ed il trattamento su larga scala di dati, anche personali, in ambito pubblico e privato, ai fini della loro utilizzazione «per servizi che godono di vasto consenso e riconoscimento da parte della società, dei consumatori e dei soggetti economici», rileva come tale raccolta si estenda a «diverse tipologie di dati, quali dati di traffico e ricerche effettuate dagli utenti su Internet, abitudini di consumo, informazioni su attività, stili di vita e comportamenti di utenti di dispositivi di telecomunicazioni»: dati, a loro volta, «trattati, in particolare, attraverso software di calcolo, raffronto e correlazione statistica al fine di generare profili che potrebbero essere utilizzati in molti modi per una pluralità di scopi»⁵⁸². Di seguito, si evidenzia allora come «le tecniche di profilazione [siano] in grado di produrre effetti sulle persone interessate collocandole in categorie predefinite, molto spesso a loro insaputa», e che gli stessi profili algoritmicamente delineati consentono di «generare nuovi dati personali che non sono quelli comunicati dall’interessato stesso al titolare né quelli che l’interessato può ragionevolmente ipotizzare siano noti al titolare»: chiosandosi con l’acuta osservazione secondo cui «la mancanza di trasparenza, o addirittura l’invisibilità, della profilazione e *l’inesattezza potenzialmente conseguente all’applicazione automatica di regole inferenziali predefinite*

⁵⁸¹ COMITATO DEI MINISTRI DEL CONSIGLIO D’EUROPA, *Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, CM/Rec(2010)13, 23 novembre 2010.

⁵⁸² Ivi, p. 1.

possono comportare rischi significativi per i diritti e le libertà individuali», e che dunque su tale base «la profilazione di una persona fisica può comportare che quest'ultima sia ingiustamente privata dell'accesso a determinati beni o servizi, e quindi può violare il principio di non discriminazione»⁵⁸³.

Seguendo poi sempre un ordine cronologico, tornano alla mente le parole dell'*Information Commissioner's Office* nel già citato Report dedicato proprio al legame tra *Big Data*, *AI*, *Machine Learning* e *data protection*: se, infatti, nel comparare costi e benefici sociali delle tecniche di *Big Data Analytics* (come sappiamo, fondamentalmente algoritmiche), l'Autorità Garante britannica non può non constatare che «*there are obvious commercial benefits to companies, for example in being able to understand their customers at a granular level and hence making their marketing more targeted and effective (...) Big data analytics is also helping the public sector to deliver more effective and efficient services, and produce positive outcomes that improve the quality of people's lives*»; dall'altra l'Autorità stessa afferma chiaramente che le tecniche in questione «*involve repurposing data in unexpected ways, using complex algorithms, and drawing conclusions about individuals with unexpected and sometimes unwelcome effects*»⁵⁸⁴. La questione centrale diventa allora – prosegue l'ICO- per le imprese

⁵⁸³ Ivi, p. 1 e 2.

⁵⁸⁴ INFORMATION COMMISSIONER'S OFFICE (ICO), *Big data, artificial intelligence, machine learning and data protection*, versione 2.0, 3/2017, p. 15 ss. Può essere interessante evidenziare come, per sottolineare i benefici apportati dalla tecnologia in parola in materia di sanità, l'ICO riporti come esempio il «*Big Data Project*» implementato nel 2009 che, al fine di indagare le ragioni del più basso coefficiente di sopravvivenza dei pazienti oncologici britannici rispetto al resto di Europa, attraverso l'utilizzo di sofisticati algoritmi ha analizzato 118 milioni di cartelle relative a più di 2 milioni di pazienti. Grazie a tale sistema, la ragione è stata individuata nel fatto che la maggior parte delle diagnosi fosse avvenuta in casi di emergenza; tale scoperta, come sottolinea l'ICO, ha dunque permesso al sistema sanitario britannico di porre in essere iniziative mirate per aumentare le diagnosi precoci di cancro, e i più recenti studi (datati 2015) dimostrerebbero che dal 2013 solo il 20 % dei casi di cancro sarebbe stato diagnosticato in situazioni di emergenza, come in caso di ricovero in pronto soccorso. Cfr. sul

che intendano sfruttare i dati per tali scopi «*whether the processing is fair*»; e la *fairness* implica innanzitutto «*transparency*», ma anche il fondamentale interrogativo circa gli effetti che il trattamento (automatizzato) avrà sugli individui, così come «*[the individuals] expectations as to how their data will be used*»: e a tal proposito il Garante britannico limpidamente afferma che «*Big data analytics (...) may use personal data to make decisions affecting individuals. Some of those decisions will obviously affect individuals more than others. Displaying a particular advert on the internet to an individual based on their social media 'likes', purchases and browsing history may not be perceived as intrusive or unfair, and may be welcomed if it is timely and relevant to their interests. However, in some circumstances even displaying different advertisements can mean that the users of that service are being profiled in a way that perpetuates discrimination (...)*»⁵⁸⁵.

Tornando alla dimensione comunitaria, può essere utile riportare alcune delle considerazioni introduttive condensate nelle c.d. *European Recommendations on Machine-Learned Automated Decision Making*, promosse da alcuni importanti organismi operanti in ambito informatico a livello europeo: *Informatics Europe*, l'*ACM Europe Council* e l'*ACM Europe Policy Committee* (EUACM). Il documento, risalente al 2018 e intitolato emblematicamente «*When Computers Decides*», ambisce a ritrarre «*[th]e principal implications of the coming widespread adoption of ML- driven automated decision making with a particular emphasis on its technical, ethical, legal, economic, societal and educational ramifications*», e, al contempo, ad elaborare «*a number of*

punto Elliss-Brookes, Lucy. Big data in action: the story behind Routes to Diagnosis. Public health matters blog, 10 November 2015.

⁵⁸⁵ Ivi, p. 19 ss.

recommendations that policy makers might wish to consider»⁵⁸⁶. Si legge, infatti, nell'Executive Summary, che «substantial advances over the past decade in machine learning (ML) techniques (...) have produced systems that sometimes rival or even exceed human ability at challenging ambiguous and highly skilled tasks such as image and speech recognition, radiological image analysis, game play, and others», a cui si aggiunge l'attuale stato dell'arte, per cui «today, due to very recent breakthroughs in deep neural network (DNN) technology, these ML-powered automated decision-making (ADM) systems can both augment human decision making or, in some cases, replace it with a fully autonomous system»: integrazione o sostituzione della manodopera umana che può condurre a «potentially massive loss of jobs and de-skilling of the humans who hold them». Segue un rilievo forse ancora più importante: «Concerns about ML also extend beyond physical systems, as other potential delegations of human judgment to machines—such as aiding judges in making sentencing and incarceration decisions in criminal actions—present serious issues about the equity and fairness of an opaque, inexplicable, and potentially biased process making life-changing decisions». E una delle prime questioni che gli autori del Report esplicitano attiene proprio ai già richiamati problemi della discriminazione algoritmica: «can we train systems to produce results untainted by gender, race, class, and other bias when the training data used to “educate” these systems is produced by humans who share these biases to a greater or lesser degree?»⁵⁸⁷. Di fronte a questo e ad altri dilemmi etici (pieni di riflessi giuridici), secondo gli autori del documento «social and moral values thus should no longer be seen simply as

⁵⁸⁶ Cfr. INFORMATICS EUROPE & EUACM, *When Computers Decide: European Recommendations on Machine-Learned Automated Decision Making*, 2018, p. 2.

⁵⁸⁷ Ivi, p. 3. Di estremo interesse, anche le altre questioni etiche e filosofiche che gli autori sollevano, in sintesi, nella stessa pagina, tra cui la seguente: «Is it acceptable to permit machines to autonomously decide to kill humans, even if this decision is made in the context of a war?».

“risk factors” or constraints, but as primary drivers and shapers of innovation»⁵⁸⁸.

Concludiamo tale comparazione citando alcuni estratti dell'introduzione della più recente Raccomandazione rivolta dal Comitato dei Ministri del Consiglio d'Europa agli Stati membri, relativa proprio all'impatto dei sistemi algoritmici sui diritti umani: dopo aver anch'esso riconosciuto l'utilizzo crescente, oramai pressoché assoluto, delle «*digital applications*», in qualità di essenziali strumenti nella vita di tutti i giorni, che include settori come l'educazione, la salute e più in generale le attività economiche di ogni sorta, sottolineando dunque il loro enorme potenziale benefico per la collettività, il Comitato ribadisce la consapevolezza dell'impatto -anche, potenzialmente, assai negativo- che l'impegno di «*algorithmic systems with automated data collection, analytics, decision making, optimisation or machine learning capacities has on the exercise, enjoyment and protection of all human rights and fundamental freedoms*». E anche'esso ammonisce rispetto alla circostanza che «*racial, gender and other societal and labour force imbalances that have not yet been eliminated from our societies are not deliberately or accidentally perpetuated through algorithmic systems*».⁵⁸⁹

Tutte le riflessioni e gli avvertimenti “istituzionali” che abbiamo qui riportato, e più in generale le relative raccomandazione e linee guida in cui sono incorporate, partono da simili presupposti teorici. Essi chiamano tutti in causa, oltre al tema della trasparenza dei processi algoritmici che reggono la filiera del

⁵⁸⁸ Ivi, p. 3 e 4.

⁵⁸⁹ Cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, CM/Rec(2020)1, 18 aprile 2020, p. 1 ss.

trattamento e, sempre più spesso, dell'*automated decision making*, quello dell'attendibilità delle fonti e della qualità dei dati utilizzati come *input*: lo si è anticipato, ma qui occorre ribadire con forza che, secondo il noto principio *garbage-in, garbage out*, la scadente qualità dei dati in ingresso implica oggi non solo la "produzione" di un modello (o profilo) comportamentale, basato sulle relazioni statistiche individuate tra i *data set* disponibili, *viziato* o comunque *inaffidabile*; ma, nel mondo dell'Intelligenza Artificiale e dei sistemi di apprendimento automatico (ML e DL), anche la compromissione della capacità stessa del sistema algoritmico di apprendere, così da trasformare l'errore occasionale in *errore sistemico*⁵⁹⁰. Se *data mining*, profilazione che ne consegue e raccomandazione operativa che ne scaturisce (nonché, potenzialmente, attuazione della decisione medesima), interamente o parzialmente automatizzati, si fondano su un siffatto *bias* iniziale, a risultare viziato e potenzialmente discriminatorio risulta l'intero processo decisionale in tal modo implementato.

Contestualmente, le riflessioni in questione ammoniscono rispetto alla stessa natura di discriminazione statistica che strutturalmente connoterebbe le tecniche di *data mining*, e più in generale di *Big Data analytics*, quale base di tutti quei trattamenti automatizzati che consistano in una profilazione, poiché preordinate a fornire una base razionale su cui fondare la distinzione, o meglio la riduzione a *categorie*, di individui, a partire dalle loro (presunte) qualità⁵⁹¹. Allo stesso modo, esse avvertono circa le capacità insite nei sistemi di IA di generare, in virtù dei *Big Data*, nuove informazioni personali (c.d. *observed, derived* e

⁵⁹⁰ Cfr. G. D'ACQUISTO, «Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati», cit., p. 285 ss; E. PELLECCIA, «Profilazione e decisioni automatizzate», cit. p. 6 ss.; l'autrice si esprime eloquentemente nei suddetti termini: «dati di addestramento distorti portano a modelli discriminatori».

⁵⁹¹ Cfr. sul punto LIPPERT, RASMUSSEN, «We Are All Different: Statistical Discrimination and the Right to Be Treated as an Individual», in *J. Ethics*, 15, 2011, p.54 ss.

inferred data) a partite da dati che personali non sono, nonché quella di derivare dati sensibili da dati che non lo sono e persino da dati che sono anonimi⁵⁹².

Temi, insomma, che rendono assolutamente evidente l'attualità, la centralità e insieme la potenziale pericolosità dei fenomeni che costituiscono oggetto della disciplina di cui si occupano le Linee Guida in esame.

Tornando alle Linee Guida del WP 29, queste precisano nell'introduzione come, di fronte allo scenario così delineato, il GDPR introduca nuove disposizioni per far fronte ai rischi derivanti dalla profilazione e dal processo decisionale automatizzato, «in particolare, ma non solo, in relazione alla tutela della vita privata»: scopo del documento in esame è, appunto, quello di chiarirne il significato normativo.

Prima di procedere all'analisi delle disposizioni generali in materia di profilazione e di ADM, e successivamente delle disposizioni specifiche sui processi decisionali *interamente* automatizzati, le Linee Guida, opportunamente, si soffermano sulla delimitazione dell'ambito di applicazione delle disposizioni in esame: e, dunque, sulle definizioni di profilazione e di processo decisionale automatizzato e sull'«approccio del regolamento a tali aspetti in generale».

Spostiamoci, dunque, al primo livello di tale struttura argomentativa.

3.2.1. Trattamento automatizzato, profilazione e processi decisionali automatizzati: definizioni essenziali

⁵⁹² Cfr. ex multis BAROCAS, SELBST, «Big-data's Disparate Impact», cit., p. 671 ss.; e, ancora una volta la classificazione fatta propria da ABRAMS, «Origins of Personal Data and its Implications for Governance», in *The Information Accountability Foundation*, marzo 2014, in <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>

Il Gruppo di Lavoro sottolinea come il Regolamento introduca le disposizioni generali e specifiche suddette al fine precipuo di garantire che i trattamenti automatizzati, e in particolar modo la profilazione e i processi decisionali automatizzati non siano utilizzati in modo da avere un impatto ingiustificato sui diritti delle persone fisiche: con ciò esplicitando la propria adesione a quell'indirizzo che interpreta l'impianto del regolamento alla luce di una prospettiva *fundamental-rights oriented*⁵⁹³. Le declinazioni di questo obiettivo vengono individuate in molte delle previsioni già commentate del Regolamento, preordinate a rafforzare, appunto, i presidi alla sfera privata e più nello specifico all'autodeterminazione informativa della persona fisica: il Gruppo fa riferimento, allora, tra le altre, alla previsione di «requisiti specifici di trasparenza e correttezza», che abbiamo ricondotto al dettato dell'art. 5, par. 1 lett a); di « maggiori obblighi in termini di responsabilizzazione», ascrivibili al sistema disegnato dagli art. 5 secondo paragrafo, 24, 25 e 32 del GDPR; di «basi giuridiche specifiche per il trattamento», puntualmente descritte nell'art. 6; di un «diritto delle persone fisiche di opporsi alla profilazione, segnatamente alla profilazione per finalità di marketing», con ciò riferendosi al diritto di opposizione sancito dall'art. 21, su cui ci soffermeremo a breve; e, non ultima, di effettuare, laddove ne ricorrano le condizioni ex. art. 35, «una valutazione d'impatto sulla protezione dei dati»⁵⁹⁴. Ciascuno dei “gruppi” di previsioni in questione trova puntuale analisi nel prosieguo delle Linee Guida.

⁵⁹³ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 6. Sulla prospettiva in questione cfr. ancora M.BASSINI, La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali, in *Quad. cost.*, 2016, 588; S. Calzolaio, «Protezione dei dati personali», p. 628 ss.

⁵⁹⁴ *Ibidem*. Per una panoramica generale, v. retro par. 3.1.1.

Solo a questo punto il documento si occupa della definizione dei termini che circoscrivono l'ambito di applicazione delle disposizioni che verranno esaminate: il primo oggetto preso in considerazione è la profilazione.

Occorre fare una precisazione. Il Gruppo, pur essendo consapevole del fatto che questa operazione sia una *species* del più ampio *genus* rappresentato dal trattamento automatizzato dei dati personali, assume quale privilegiato oggetto di indagine la *profilazione* medesima. Ciò perché, da una parte, il Regolamento si astiene dall'offrire una definizione precipua della "fattispecie" del trattamento automatizzato, o *automated data processing*; anzi, sarebbe meglio dire, perché esso, consapevole dello stato della tecnologia di cui abbiamo ampiamente discusso, individua l'elaborazione dei dati svolta *con* mezzi automatizzati come la *regola*, e piuttosto il trattamento manuale come *eccezione*, pur assoggettando chiaramente entrambi alla propria disciplina. È quanto si evince dall'art. 2 del Regolamento stesso, che nel delimitare il proprio ambito di applicazione materiale ha riguardo innanzitutto al «trattamento interamente o parzialmente automatizzato di dati personali»; e solo in seconda battuta (come testimonia la congiunzione coordinante copulativa "e") fa riferimento al «trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi», quasi l'evenienza in questione rappresentasse un'eventualità, se non remota, comunque *poco incidente* sulla sfera di libertà della persona fisica⁵⁹⁵. In estrema approssimazione, si può comunque identificare una nozione minima di trattamento automatizzato nell'art. 4, par. 1, n. 2, che definisce in termini generale il «trattamento» come

⁵⁹⁵ L'interpretazione in questione è chiaramente confortata dal *considerando* 15, che richiama il principio di "neutralità tecnologica" del Regolamento: in esso il legislatore osserva che «al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate», e a ciò fa conseguire che «la protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio». A non dover rientrare nel perimetro applicativo del Regolamento dovrebbero essere solo «i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine».

«qualsiasi operazione o insieme di operazioni, compiute *con o senza l'ausilio di processi automatizzati* e applicate a dati personali o insiemi di dati personali»: per trattamento automatizzato potendoci limitare ad intendere dunque quell'operazione sui dati svolta attraverso qualsiasi mezzo automatizzato, interamente o parzialmente, dunque anche dove coinvolga in una certa misura il comportamento umano; mezzi che oggi per lo più consistono nei software algoritmici integrati o ospitati nei dispositivi di ICTs (hardware) digitali⁵⁹⁶.

La seconda ragione pare, tuttavia, di ordine teleologico piuttosto che “terminologico”. Abbiamo infatti già esaminato l'approccio *risk-based* cui pare evidentemente improntato l'intero Regolamento: aggiungiamo ora che dal combinato disposto di determinate disposizioni il legislatore europeo pare aver coltivato una presunzione di elevata “rischiosità” per i trattamenti che comportano l'utilizzo di nuove tecnologie⁵⁹⁷. Orbene, tra le tipologie di trattamento che più ampiamente coinvolgono le ICTs, e che agli occhi stessi del Regolamento sembrano integrare tutti gli estremi di una elevata e persistente rischio, tale da imporre garanzie “rafforzate” a presidio dei diritti fondamentali dell'individuo a cominciare dalla protezione dei suoi dati personali, figura ed anzi spicca senza dubbio la profilazione. Lo dimostra il fatto stesso che la prima fattispecie per cui l'art. 35, par. 3 prescrive l'obbligo in capo al titolare della valutazione preventiva

⁵⁹⁶ Si rinvia all'analisi del contesto tecnologico svolta retro, capitolo 2 par. 3. Cfr. poi art. 4, par. 1, n. 2, Regolamento UE 2016/679: «“trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (...)»

⁵⁹⁷ In particolare essa sembra scaturire dal combinato disposto tra l'art. 35 primo comma e il considerando 89, che nell'indicare le specie di trattamento per cui dovrebbe ritenersi sussistente l'obbligo della valutazione preventiva d'impatto, in quanto idonei a configurare un rischio elevato per i diritti fondamentali degli interessati, esplicitamente afferma che «tali trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie (...)». Per tale lettura cfr. S. CALZOLAIO, «Protezione dei dati personali», cit., p. 628 ss.

d'impatto consiste proprio nella sussistenza di una «*valutazione sistematica e globale di aspetti personali relativi a persone fisiche*, basata su un trattamento automatizzato, *compresa la profilazione*, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche»; e che il Regolamento risulta disseminato di riferimenti alla specie di trattamento (interamente o parzialmente) automatizzato in questione⁵⁹⁸.

A questo punto, possiamo dunque passare ad interrogarci (assieme alle Linee Guida) sulla definizione di *profilazione* fatta propria dal Regolamento.

Essa si rinviene, come alcune pagine indietro già ricordato, nell'art. 4, par. 1, n. 4 dell'articolato normativo, in cui il legislatore europeo concepisce il fenomeno in esame come «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica*, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione

⁵⁹⁸ Depongono nel senso di riconoscere un'elevata rischiosità al fenomeno in questione anche i diversi considerando che se ne occupano: il cons. 24 ad esempio, nell'indicare i criteri utili a discernere quando il comportamento degli interessati sia soggetto a monitoraggio svolto nel territorio dell'Unione da soggetto stabilito fuori da esso, prevede che « Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a *tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica*, in particolare per (...) analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali»; o il cons. 30, che, nel rilevare la diffusione degli identificativi online come informazioni che rendono *identificabile* l'interessato, osserva – con preoccupazione – come « Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle». Procedendo poi ad una veloce e non esaustiva carrellata, vedi poi i cons. nn. 60, 63, 70 e artt. 13, c. 2, lett. f), 14, c. 2, lett. g), 15, 1o co., lett. h), 21, c. 1 e 2 (in merito ai diritti dell'interessato rispetto alla *profilazione*); cons. n. 71 e art. 22 (in merito al trattamento -unicamente- automatizzato); cons. 91 e art. 35 (in merito alla valutazione di impatto). Cfr. sul tema BOSCO, CREEMERS, FERRARIS, GUAGNIN, KOOPS, «Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities», in Gutwirth, Leenes, De Hert (a cura di), *Reforming European Data Protection Law*, cit., 3 ss.

economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

Dalla lettera della disposizione risulta subito chiaro che tale fattispecie, agli effetti del GDPR, costituisce una sottocategoria di trattamento automatizzato⁵⁹⁹, la quale si compone *necessariamente* di tre elementi: innanzitutto, essa deve costituire una forma di trattamento automatizzato (l'aggettivo indefinito *qualsiasi* indica che essa include anche i trattamenti *parzialmente* automatizzati, ovvero caratterizzati da un certo coefficiente di *effettivo coinvolgimento umano*); deve essere effettuata, in quanto trattamento rilevante agli effetti del GDPR medesimo, su *dati personali*; e il suo obiettivo deve essere quello di *valutare aspetti personali* relativi alla persona fisica (valutazione che, precisa la norma stessa, può consistere nell'analizzare o nel prevedere gli aspetti medesimi)⁶⁰⁰. Come è stato notato, allora, si può affermare già preliminarmente che nel Regolamento la profilazione è concepita come mezzo funzionale alla assunzione di una decisione rilevante per l'individuo o per il gruppo profilato, proprio in quanto adeguato a valutare analiticamente il comportamento presente, ed anche eventualmente a *prevedere* il comportamento futuro del soggetto cui i dati (individuali o di gruppo) si riferiscono: da qui, l'enfasi sull' "attitudine al pregiudizio" insita nella tipologia di operazioni in questione⁶⁰¹.

⁵⁹⁹ Per l'interpretazione medesima, che fa leva sulle caratteristiche peculiari che assume la profilazione quale forma (v. subito *infra* il testo del reg.) di trattamento automatizzato, e quindi tanto interamente quanto parzialmente tale, cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli Editore, Torino, 2016, 193 ss.

⁶⁰⁰ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 7.

⁶⁰¹ Sul tema cfr. ampiamente BOSCO, CREEMERS, FERRARIS, GUAGNIN, KOOPS, «Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities», in Gutwirth, Leenes, De Hert (a cura di), *Reforming European Data Protection Law*, cit., 3 ss.; E. PELLECCIA, *Profilazione e decisioni automatizzate al tempo della black-box society*, cit., p. 1032 ss.; F. KALTHEUNER, E. BIETTI, «Data is power: Towards additional guidance on profiling and automated decision-

Aggiungiamo che, come le stesse Linee Guida sottolineano, la definizione è ampiamente debitrice rispetto a quella contenuta nella già citata Raccomandazione n. 13 del 2010 del Comitato dei Ministri del Consiglio d'Europa agli Stati Membri: essa infatti all'art. 1, par. 1, lett e), intendeva la profilazione come «una tecnica di trattamento automatico consistente nell'applicazione di un “profilo” ad una persona fisica determinata, in particolare al fine di prendere decisioni relative a tale persona oppure ai fini dell'analisi o della previsione delle sue preferenze, dei suoi comportamenti e delle sue propensioni personali»⁶⁰². Sebbene lo stesso Gruppo aggiunga che la definizione in questione risultasse maggiormente riduttiva, in quanto non contemplante l'attività di *deduzione* del profilo medesimo a partire dai dati elaborati, l'organo afferma che la Raccomandazione stessa risulta utile ad evidenziare le tre distinte fasi in cui può articolarsi la profilazione medesima: la *raccolta* dei dati; l'analisi (parzialmente o interamente) *automatizzata* dei dati medesimi per individuare correlazioni tra gli stessi; e l'applicazione delle correlazioni stesse, o dei *pattern* così identificati ad una persona fisica per individuare *caratteristiche di comportamento presenti o future*, e dunque in definitiva per analizzare o per *prevedere* la capacità di eseguire un compito, gli interessi e i gusti della persona stessa o la probabilità di adottare o meno un determinato comportamento⁶⁰³.

making in the GDPR», in *Journal of Information Rights Policy and Practice*, 2018, p. 1 ss.; A. G. PARISI, «Dati, proliferazione e social network: l'emersione di un nuovo modello giuseconomico», cit., p. 181 ss..

⁶⁰² COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, CM/Rec(2010)13, 23 novembre 2010. La lettera d) del medesimo articolo definisce poi il «profilo» come quell' «insieme di dati caratterizzanti una categoria di persone fisiche che si intende applicare ad una persona fisica determinata».

⁶⁰³ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 7 e 8.

È lo stesso Gruppo a sottolineare come a distinguere la profilazione dalla semplice classificazione in base a «caratteristiche note quali età, altezza o peso», sia proprio la finalità, valorizzata dal dato normativo, di *valutare* aspetti e qualità di una persona fisica o di un gruppo: proprio per questo, la profilazione è una procedura che può implicare (ed anzi quasi sempre implica) una «serie di deduzioni statistiche», poiché laddove impiegata per fare previsioni essa si avvale di quantità di dati provenienti da varie fonti per «dedurre qualcosa su una persona in base alle qualità di altre persone che sembrano statisticamente simili»⁶⁰⁴.

Tale considerazione immediatamente ci riporta alla questione poc'anzi evocata dell'attitudine alla discriminazione statistica insita nella profilazione (per lo più) algoritmica, amplificata dagli strumenti di *Big Data analytics*. La peculiarità del *data mining*, e del principio di *Knowledge Discovery in Databases* su cui si fonda, è quella di individuare relazioni statistiche in un set anche non strutturato (oltre che *big*) di dati, e di condurre tale processo di scoperta attraverso processi *automatizzati*⁶⁰⁵. Al contempo, gli algoritmi più impiegati sono oggi quelli di ML, che come sappiamo sono caratterizzati dalla capacità di “apprendere” (supervisionati o meno) quali regolarità causali e quali correlazione tra i dati siano utili al fine di “estrarre” il modello o profilo su cui basare le successive decisioni: tuttavia, lo si ricorda nuovamente, se i dati che funzionano come esempio sono distorti, altrettanto viziati, e pertanto discriminatori, saranno i modelli che ne discendono⁶⁰⁶. E questo può accadere non solo perché sono stati usati come esempi casi che esprimevano o riflettevano un pregiudizio, ma anche

⁶⁰⁴ *Ibidem*.

⁶⁰⁵ Cfr. ancora una volta J. BURRELL, «How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithm», cit.; R. CALO, «Artificial Intelligence Policy: a Primer and Roadmap», cit.; E. PELLECCIA, «Profilazione e decisioni automatizzate nella black-box society», cit.

⁶⁰⁶ V. amplius retro, cap. 2 par. 3. Per il noto principio *garbage in-garbage out* v. ancora G. D’ACQUISTO, «Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati», cit.

soltanto perché il campione della popolazione è parziale: da ciò discende chiaramente il pericolo che siano sistematicamente svantaggiati coloro che sono sottorappresentati o sovrarappresentati nel set di dati⁶⁰⁷. L'attendibilità del modello, e della decisione che vi si basa, dipende essenzialmente dalla fonte e dalla qualità del dato di partenza, oltre che dalla coerenza del processo inferenziale (algoritmico) che presiede alla sua produzione: nella *data driven society*, si tratta di una questione, prima ancora che giuridica, esistenziale.

In tema profilazione, una questione altrettanto importante, e intimamente collegata a quella della discriminazione statistica, è quella inerente agli *algo-created data*. Come abbiamo già accennato, caratteristica principale del trattamento algoritmico, e in particolare della profilazione - specialmente se condotta attraverso sistemi di ML e di DL -, è la capacità di desumere, e quindi inferire, dati personali *anche* da dati che tali non sono⁶⁰⁸. Ad occuparsi del problematico profilo in questione è lo stesso Gruppo di Lavoro, laddove nelle Linee Guida afferma che «la profilazione può creare dati appartenenti a categorie particolari desumendoli [*by inference*] da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati. Ad esempio, può essere possibile desumere lo stato di salute di una persona associando le registrazioni dei suoi acquisti di alimenti a dati sulla qualità e sul contenuto energetico di tali alimenti»⁶⁰⁹. E se ne è occupato anche il Consiglio d'Europa, nella dichiarazione del 13 febbraio 2019 dedicata alle “capacità manipolative” dei

⁶⁰⁷ Cfr. soprattutto S. BAROCA & A.D. SELBST, *Big Data's Disparate Impact*, 104 California L.R., 673 (2016): “Big Data is the buzzword of the decade”.

⁶⁰⁸ Oltre al riferimento costante a R. MESSINETTI, «Privacy e controllo dell'identità algoritmica», cit., p. 131 ss., cfr. S. WACHTER, «Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR», in *Computer L. & Security Rev.*, 2018, p. 436 ss.; ed ancora S. BAROCAS & A.D. SELBST, «Big Data's Disparate Impact», cit. p. 671 ss.

⁶⁰⁹ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 15 ss.

processi algoritmici, sottolineando l'idoneità dei dati derivati ad influenzare nel suo complesso la capacità di autodeterminazione, e dunque la vita, delle persone fisiche⁶¹⁰.

Ciò che appare messo in crisi dal fenomeno fin qui descritto diventano in questo modo le stesse categorie fondamentali della disciplina della *data protection*: quella di *dato personale* e, in quest'ambito, la stessa distinzione tra *dati ordinari* e *dati sensibili*.

Se non fosse che, come abbiamo analizzato, la definizione ampia, “onnicomprensiva” di dato personale accolta dal GDPR, anche alla luce della corrispondente nozione “relativa” di anonimizzazione che traspare dall'articolato e dai considerando, nonché l'enfasi posta sulle tecniche di pseudonimizzazione, sembrano reagire, se non in modo risolutivo, almeno in via iniziale al fenomeno descritto⁶¹¹. E a ciò potrebbe concorrere anche una lettura ulteriormente estensiva della nozione di dato personale agli effetti del GDPR, alla luce di alcune alternative proposte classificatorie che valorizzano il criterio dell'*origine* del dato medesimo: ci riferiamo in particolare a quella di Abrams, che sulla sua base distingue innanzitutto i dati forniti dall'interessato (*provided data*), e poi altre tre categorie che nella società datificata hanno assunto un rilievo assoluto, ovvero i dati osservati (*observed data*), attraverso le tracce digitali lasciate dagli utenti; i dati derivati tanto dai primi quanto dai secondi, ossia veri e propri nuovi set di

⁶¹⁰ Cfr. COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*; 13 febbraio 2019. Al par. 6, il Comitato afferma in modo cristallino che «*computational means make it possible to infer intimate and detailed information about individuals from readily available data. This supports the sorting of individuals into categories, thereby reinforcing different forms of social, cultural, religious, legal and economic segregation and discrimination. It also facilitates the micro-targeting of individuals based on profiles in ways that may profoundly affect their lives*». È utile rilevare che al par. 4 il Comitato premette significativamente: «*These data are used to train machine-learning technologies to prioritise search results, to predict and shape personal preferences, to alter information flows, and, sometimes, to subject individuals to behavioural experimentation*».

⁶¹¹ V. retro, par. 3.1.1.

dati tratti da quelli raccolti o osservati in origine (*derived data*); e, ancora più critiche, le informazioni dedotte, pur sempre a partire dai primi due, attraverso un procedimento di analisi fondato sulle probabilità ed automaticamente implementato da un sistema algoritmico (*inferred data*)⁶¹².

In ogni caso, resta il fatto che nel nostro tempo, in cui l'analisi è sviluppata «dalla macchina e non dall'uomo con le sue sole forze di analisi», la distinzione fra dato personale e dato non personale finisce per dissiparsi, poiché la macchina può trarre informazioni personali anche da dati insignificanti per le capacità di indagine dell'uomo (basti pensare ai dati anonimi, appunto, o anche agli stessi dati a-personali)⁶¹³. Diventa quindi fondamentale, per garantire l'effettiva tutela della capacità dell'interessato di autodeterminarsi, concentrare l'attenzione sul funzionamento dei «processi neurali» seguiti dalla macchina nel trattamento: per l'interessato, insomma, può essere rilevante conoscere come la macchina relazioni i suoi dati con altri dati, poiché tali informazioni possono consentirgli di assumere autonomamente decisioni migliori (o di potersi difendere dalle decisioni altrui che lo riguardano)⁶¹⁴. Centrale diventa quindi quella questione, assai controversa, che nell'ambito dei processi decisionali interamente automatizzati attiene alla configurabilità o meno di un *diritto alla spiegazione*, o comunque a *conoscere la logica* utilizzata nel singolo trattamento algoritmico e in relazione alla *specifica* decisione adottata (dalla macchina stessa) sulla base di esso⁶¹⁵. Affronteremo il tema più avanti.

⁶¹² Cfr. ABRAMS, «The Origin of Personal Data», cit. Appare importante sottolineare come le categorie più rilevanti di dati – osservati, derivati, dedotti – comportano strutturalmente un basso livello di consapevolezza dell'interessato in ordine alla loro stessa esistenza: vengono creati a distanza e senza il coinvolgimento della persona interessata.

⁶¹³ Già abbiamo citato retro molta letteratura sul punto, ma cfr. anche IGUAL, SEGUÌ, *Introduction to data science*, Springer, 2017, passim.

⁶¹⁴ Cfr. s. Calzolaio, «Protezione dei dati personali», cit., p. 607.

⁶¹⁵ V. più avanti, par. 3.2.3, ma cfr. da subito, per una ricostruzione del dibattito in materia, B. GODDMAN, S. FLAXMAN, «European Union Regulations on Algorithmic Decision Making and a “Right to Explanation”», in *AI Magazine*, 2017, pp.50-57; L. FLORIDI L., S.

Appariranno a questo punto chiari tanto i problemi quanto i rischi evocati dalla fattispecie della profilazione, e il motivo della grande attenzione riservatagli dal legislatore europeo, e dallo stesso Gruppo nella sua attività esegetica.

Nel prosieguo delle Linee Guida, il Gruppo di Lavoro passa ad occuparsi della definizione di «processo decisionale automatizzato»: fattispecie che, come lo stesso organo puntualmente afferma, «ha una portata diversa da quella della profilazione, a cui può sovrapporsi parzialmente o da cui può derivare»⁶¹⁶. Il Gruppo si concentra nello specifico sulla definizione di «processo decisionale *esclusivamente* automatizzato», poiché, come vedremo, particolarmente rilevante al fine di determinare il perimetro applicativo dell'art. 22 del GDPR (che, appunto, alle sole «decisioni basate unicamente [*solely*] su trattamenti automatizzati» si riferisce): in particolare, nel documento l'organo individua il *proprium* di tale categoria nella «capacità di prendere decisioni impiegando mezzi tecnologici *senza* il coinvolgimento umano»; e specifica più avanti che il

WACHTER, B. MITTLESTADT, «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», in *International Data Privacy Law*, 2017, pp. 76-99.; S. WACHTER, B. MITTELSTADT, C. RUSSELL, «Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR», in *Harvard Journal of Law & Technology*, 31 (2), 2018; G. MALGIERI, G. COMANDÈ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», in *International Data Privacy Law*, vol. 7, Issue 3, 2017, p. 256ss; G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», in *Computer Law & Security Review*, 2019; E. BIETTI, F. KALTHEUNER, «Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR», in *Journal of Information Rights, Policy and Practice*, 2018, 2 ss.; S. WACHTER, B. MITTLESTADT, «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI», in *Colum. Bus. L. Rev.*, 2019, pp. 2-78.

⁶¹⁶ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 8.

coinvolgimento umano, ai fini dell'integrazione della fattispecie, deve essere *effettivo*, ossia in grado di influire *effettivamente* sulla decisione finale, con ciò avallando l'orientamento espresso da una consistente parte della dottrina nel dibattito intorno alla portata semantica del concetto in parola, in particolare agli effetti del suddetto art. 22⁶¹⁷.

Da tale interpretazione si desume tuttavia, da una parte, che sussistono processi decisionali solo parzialmente automatizzati, e che tali sono i processi connotati appunto da un maggiore o minore - purché effettivo - coinvolgimento o comunque contributo umano; e, allo stesso tempo, che il trattamento automatizzato su cui la decisione si fonda, e dunque il primo momento del processo decisionale (interamente o parzialmente) automatizzato può anche *non* consistere nella profilazione. Con le parole del Gruppo: «Le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate». Processo decisionale automatizzato e profilazione, insomma, possono andare congiunti o disgiunti a seconda dei casi concreti⁶¹⁸.

⁶¹⁷ Ivi, p. 8 e p. 21 ss.; in part. p. 23, in cui il Gruppo afferma che la disposizione in esame, nel limitare il proprio ambito di applicazione alle decisioni basate unicamente sul trattamento automatizzato non può essere elusa «*by fabricating human involvement*», ossia «creando coinvolgimenti umani fittizi»: v. più ampiamente *infra*. Cfr. anche G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation cit., p. 243 ss.; G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit.; cfr. anche la corrispondente interpretazione adottata a livello istituzionale da ICO, *Feedback request- profiling and automated decision-making*, 2017, 1

⁶¹⁸ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 8. In punto di *non sovrapposibilità tra processo decisionale interamente automatizzato e profilazione*, le Linee Guida portano come esempio la fattispecie in cui una multa per eccesso di velocità sia inflitta esclusivamente in base alle prove fornite da un autovelox: esso rappresenta certamente un processo decisionale (interamente) automatizzato, ma il trattamento su cui la decisione si basa, sebbene automatizzato, *non* consiste in una profilazione. Diverso sarebbe il discorso - e pertanto la decisione di infliggere la multa sarebbe da considerarsi basata sulla profilazione - se «le abitudini di guida della persona in

Parallelamente, il Gruppo dedica un'attenzione specifica alla tipologia di dati su cui le decisioni automatizzate possono essere prese, con ciò dimostrando la sensibilità maturata in ambito istituzionale rispetto al tema poc'anzi affrontato degli *algo-created data*. Questi ultimi, infatti, possono consistere in: «dati forniti direttamente dall'interessato (come le risposte a un questionario); dati osservati riguardo a una persona (come i dati relativi all'ubicazione raccolti tramite un'applicazione) [quelli che nella classificazione di Abrams sono chiamati *observed data*]; dati derivati o desunti, come un profilo della persona che è già stato creato (ad esempio un punteggio sull'affidabilità creditizia) [c.d. *inferred e/o derived data*]]»⁶¹⁹.

Il Gruppo conclude il capitolo dedicato alle definizioni specificando l'«approccio» del GDPR ai concetti medesimi: e ciò a dimostrazione dell'importanza delle distinzioni appena esaminate allo scopo di circoscrivere l'ambito di applicazione della disciplina prevista dall'art. 22, ben più rigorosa rispetto alla disciplina generale, desumibile dall'impianto normativo del Regolamento, applicabile a *tutti* i trattamenti automatizzati (profilazione

questione fossero state monitorate nel tempo e, ad esempio, l'ammontare della multa fosse il risultato di una valutazione che coinvolge altri fattori quali l'eventuale recidiva di eccesso di velocità (...)).»

⁶¹⁹ *Ibidem*. Il Gruppo, a p. 9, porta un esempio anche per dimostrare che una *decisione non unicamente automatizzata* possa basarsi sulla *profilazione*: esso considera la fattispecie in cui un istituto di credito adotti una decisione su una richiesta di mutuo basandosi sul punteggio di affidabilità creditizia generato da un algoritmo (punteggio e relativo profilo derivante, dunque, da un trattamento automatizzato di profilazione), e tuttavia facendo precedere la decisione da *ulteriori interventi significativi svolti da esseri umani*. La fattispecie in questione, astratta dal contesto teorico delle Linee Guida, rappresenta anche il principale ambito in cui sono insorte controversie decise dalle Corti nazionali in punto di diritto a non essere sottoposti a (o piuttosto divieto generale di) decisioni basate unicamente su trattamenti automatizzati, e quello che ha fatto da sfondo alle uniche due pronunce della Corte di Giustizia -per ora- intervenute in ordine all'interpretazione dell'art. 22: ci riferiamo alle due sentenze c.d. SCHUFA, su cui v. *amplius infra*.

compresa) e conseguentemente ai processi decisionali non interamente automatizzati⁶²⁰.

Seguendo le indicazioni del documento, può constatarsi che esistono tre possibili modalità d'uso della profilazione, intesa come ormai sappiamo quale declinazione *specificata e particolare* della categoria dei trattamenti automatizzati: accanto alla profilazione «generale», ossia intesa come trattamento in sé e per sé, le altre ipotesi sono quelle di un processo decisionale *basato* sulla profilazione e quella di una «decisione basata *unicamente* su un trattamento automatizzato *compresa* la profilazione [nel contesto in esame, sarebbe meglio dire *consistente* nella profilazione], che produce effetti giuridici o incide in modo analogo significativamente sull'interessato».

È chiaro che la terza rappresenta un'ipotesi molto specifica: le Linee Guida, in questo modo, fanno preciso riferimento (tant'è che al capitolo del documento in materia rinviano) alla fattispecie disciplinata dall'art. 22 del Regolamento, mutuando peraltro l'insieme di proposizioni con cui il paragrafo 1 ne identifica *tutti* i presupposti applicativi. Sull'analisi della disposizione in questione, e del suo ambito di applicazione, ci soffermeremo in un paragrafo *ad hoc*, tuttavia qui merita sottolineare che la classificazione articolata dal Gruppo va, più in generale, interpretata nel senso che tutti i processi decisionali (nel discorso svolto dalle Linee Guida, «basati» sulla profilazione) che non rispondano ai requisiti di cui alla terza ipotesi sono da ricondursi nell'alveo della seconda: in prima approssimazione, si può dunque affermare che questi ultimi processi decisionali esulino dall'ambito di applicazione dell'art. 22⁶²¹.

⁶²⁰ Ivi, p. 9.

⁶²¹ Cfr. E PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black-box society», cit.; ; F. KALTHEUNER, E. BIETTI, «Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR», cit., p. 13.

La distinzione è talmente importante per il Gruppo da esigere un ulteriore esempio, che chiarisce quando si versi nella seconda o nella terza ipotesi: riferendosi alla richiesta di un prestito online, ricorre un processo decisionale del secondo tipo laddove «un essere umano decide se accordare il prestito sulla base di un profilo prodotto con mezzi unicamente automatizzati»; si ricade invece nella terza ipotesi, coincidente con l'ambito di applicazione dell'art. 22, laddove «un algoritmo decide se il prestito viene accordato e la decisione viene trasmessa automaticamente alla persona, senza alcuna previa valutazione significativa da parte di un essere umano»⁶²².

Le Linee Guida concludono sul punto affermando come da tale distinzione derivi l'applicazione del diverso regime previsto dalle disposizioni generali o, piuttosto, dall'art. 22 del GDPR.

Nell'ipotesi di processi decisionali automatizzati - per così dire - *semplici*, i quali dunque prevedano un coinvolgimento umano (non meramente formale) sotto il profilo del trattamento (sia esso o meno una profilazione) e/o della decisione che vi si basi, il titolare può svolgere i relativi trattamenti purché «sia in grado di soddisfare tutti i principi e disponga di una base legittima per il trattamento»: applicabili risultano, appunto, le disposizioni del Regolamento relative a tutti i trattamenti e i processi decisionali automatizzati riguardanti le persone fisiche, *compresi* dunque quelli non interamente automatizzati.

Laddove, invece, ricorra l'ipotesi di una decisione basata unicamente sul trattamento automatizzato, *compresa* la profilazione, e siano soddisfatti gli altri requisiti di cui all'art. 22, par. 1, il titolare risulta soggetto a «garanzie

⁶²² GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 9. Bisogna tuttavia aggiungere che, affinché tutti i requisiti della fattispecie di cui all'art. 22 siano soddisfatti, la decisione dovrebbe inoltre produrre effetti giuridici o incidere in modo analogo significativamente sull'interessato. V. *amplius infra*.

supplementari e limitazioni»: applicabili sono le disposizioni specifiche previste dal Regolamento in materia, inquadrabili in un sub-sistema imperniato sull'art. 22, la cui disciplina, è bene evidenziarlo subito, è ricostruita dal Gruppo (che già sinteticamente lo esplicita), anche alla luce dei *considerando* pertinenti, in termini di «divieto generale relativamente a questo tipo di trattamento al fine di riflettere i potenziali rischi per i diritti e le libertà delle persone fisiche»⁶²³.

È ora di occuparci delle disposizioni generali.

3.2.2. Le disposizioni generali: principi, basi giuridiche e diritti dell'interessato

Prima di addentrarci nell'analisi delle disposizioni applicabili a *tutti* i trattamenti automatizzati, e ai processi decisionali che li implicano, laddove appunto non operante il più rigoroso regime di cui all'art. 22, occorre premettere che, stante la vastità della materia, approfondiremo nel presente paragrafo soltanto

⁶²³ *Ibidem*. Si riporta di seguito, per familizzarvi subito, il testo dell'art. 22, rubricato «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione»: «1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.». Occorre subito aggiungere che il sub-sistema a cui abbiamo fatto riferimento comprende anche, come vedremo, l'art. 13, par. 2, lett. f); l'art. 14, par. 2, lett. g); l'art. 15, par. 1, lett. h); e l'art. 35, par. 3, lett a) ».

alcuni degli elementi in cui si articola la platea dei principi sulla protezione dei dati, delle basi giuridiche e dei diritti dell'interessato rilevanti in tale specifico settore. Molti di essi, invero, li abbiamo già osservati in precedenza da una prospettiva generale, nell'esaminare l'impianto del GDPR. Il criterio sarà, ancora una volta, quello di selezionare le dimensioni del fenomeno dell'elaborazione automatica (*rectius* algoritmica) dei dati che paiono più attuali e, soprattutto, maggiormente capaci di esporre la sfera privata a gravi rischi di pregiudizio, e di indagare così l'esistenza nel quadro del GDPR di strumenti giuridici preordinati a farvi fronte, e la loro idoneità (astratta e, nei limiti della presente trattazione, concreta) a tale scopo⁶²⁴.

Continuando a seguire la struttura argomentativa fatta propria dalle Linee Guida in esame, occorre partire dai principi in materia di protezione dei dati. Il Gruppo richiama opportunamente il *considerando* 72, nella parte in cui afferma che «la profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati», e sottolinea che il titolare del trattamento, per adempiere ai propri obblighi da cui dipende la liceità del trattamento medesimo, dovrebbe innanzitutto osservare i principi in questione, tenendo conto delle seguenti indicazioni esegetiche fondamentali⁶²⁵.

Il primo principio che si intende richiamare (insieme al Gruppo) è quello di trasparenza, sancito assieme a quelli di liceità e di correttezza dall'art. 5, par. 1

⁶²⁴ L'analisi che seguirà farà costante riferimento, come ormai sappiamo, a GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 10 ss. È bene ancora una volta sottolineare come il Gruppo affermi chiaramente che «Qualora il trattamento soddisfi la definizione di cui all'articolo 22, paragrafo 1, si applicano le disposizioni specifiche supplementari».

⁶²⁵ *Ibidem*.

lett. a) e ad essi inscindibilmente legato. Tralasciando gli argomenti generali e di sistema, già *retro* scandagliati, occorre qui unirsi all'enfasi che il Gruppo pone sul principio in questione quale «prescrizione fondamentale» sancita dal Regolamento: discorso che vale a maggior ragione in punto di trattamenti algoritmici, per le ragioni che abbiamo già esplicitato nella parte in cui ci siamo occupati dei limiti intrinseci ai sistemi algoritmici, e segnatamente del fenomeno critico della *black box*⁶²⁶. Occorre ora riprendere brevemente tali considerazioni ed aggiungere alcuni elementi, che sottolineano la centralità nel contesto della società datificata, governata dai sistemi automatizzati, della trasparenza algoritmica.

Si è già detto che il profilo più problematico nell'implementazione di sistemi algoritmici nel trattamento dei dati, sintetizzato appunto dall'espressione *black box*, consiste nell'opacità del percorso logico di tipo inferenziale seguito dalla macchina nell'elaborazione del dato, nella conseguente produzione dell'*output* e ancora più, nel caso dei sistemi di ML e DL, nel processo di autoapprendimento ed implementazione di “perfezionati” algoritmi: le logiche in questione sono spesso ignote agli stessi sviluppatori, cosicché all'aumentare delle prestazioni della macchina si riduce la capacità dell'uomo di comprenderne il funzionamento⁶²⁷.

Ebbene, se nemmeno gli sviluppatori sono in grado di “aprire la *black box*” del sistema utilizzato, l'interessato (anche il più dotato di conoscenze specialistiche) si trova in una posizione di totale vulnerabilità: l'opacità comincia

⁶²⁶ Rinviamo al cap. 2, par. 3, e in particolare alla nota 440 in cui si indicano importanti riferimenti bibliografici. È opportuno comunque anche qui rinviare al fondamentale contributo di J. BURRELL, «How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms», cit., p. 1ss; ed anche, anzi soprattutto, al fine di approcciarsi alla tematica nonostante la carenza di nozioni altamente specialistiche, D. CASTELVECCHI, «Can we open the black-box of AI?», cit., <http://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731>.

⁶²⁷ Cfr. ancora J. BURRELL, *How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms*, cit.

dall'esistenza stessa del trattamento, di cui spesso l'interessato non è avveduto; coinvolge la materia prima "estratta" da quest'ultimo, poiché spesso il trattamento ha ad oggetto dati altrettanto personali che abbiamo definito inferiti o derivati, ossia scaturiti dal processo stesso di profilazione, non provenienti (mediante prestazione del *consenso*) dall'interessato e dunque non conosciuti da quest'ultimo; e si estende, per la più gran parte della collettività, alla comprensione delle «complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati»⁶²⁸. Sotto ogni profilo, il trattamento automatizzato esige a gran voce un maggior grado di trasparenza come presidio indispensabile per l'autodeterminazione dell'interessato.

Ecco allora che, come contromisura, il Regolamento inverte a livello di dettaglio il principio di trasparenza all'art. 12, par. 1, che nel delineare in via generale la fisionomia dei doveri di informazione gravanti a carico del titolare del trattamento, obbliga quest'ultimo a fornire all'interessato (precipuamente al fine dell'esercizio dei diritti attribuitigli dagli artt. 15-22) le informazioni sul trattamento dei loro dati personali «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro»⁶²⁹. Le informazioni

⁶²⁸ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 10

⁶²⁹ *Ibidem*. V. il par. 1 dell'art. 12, Reg. UE 2016/679: «Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato». Il Gruppo porta come esempio eloquente il caso in cui una società di assicurazioni offra tariffe e servizi differenziati in base al comportamento di guida delle persone, monitorati per mezzo di sistemi algoritmici e dunque raccolti per finalità di profilazione, ad esempio per individuare comportamenti di guida errati, da cui dipenderebbe un incremento del massimale di polizza: ai sensi delle norme richiamate, il Titolare è pertanto tenuto a fornire le informazioni sui dati utilizzati, nonché sulle finalità della raccolta e sugli altri aspetti contemplati dagli artt. 13 ss.

in questione, comunicate in tali termini, devono pervenire all'interessato al momento della raccolta laddove avvenga presso il medesimo, o entro i termini stabiliti dall'art. 14 par. 3 laddove raccolte presso terzi.

Può essere interessante evidenziare come il Gruppo richiami in nota un inciso delle Linee Guida in materia di *Big Data* adottate dal Garante australiano, in cui si afferma perspicacemente che «la stessa tecnologia che porta a una maggiore raccolta di informazioni personali offre anche l'opportunità di realizzare informative sulla protezione dei dati più dinamiche, a più livelli e incentrate sull'utente»⁶³⁰.

Possiamo concludere sul punto evidenziando (non senza qualche preoccupazione) che, sebbene autorevole dottrina ritenga la trasparenza il naturale, nonché migliore, antidoto all'opacità (quasi tautologicamente), altra parte della letteratura specialistica avverte circa l'insufficienza della stessa *dimensione* della trasparenza a tale scopo⁶³¹. E ciò, innanzitutto, perché non è chiara quale forma dovrebbe assumere la trasparenza, dal momento che la stessa esplorazione del codice sorgente (o *source code*) è idonea a rivelare solo il metodo di apprendimento automatico utilizzato, e non piuttosto la regola che abbia presieduto alla specifica decisione prodotta all'esito di un processo automatizzato e basata sui dati⁶³²; né a migliori risultati conduce l'*auditing*, ovvero la revisione dei record digitali che descrivono ciò che un computer ha fatto in risposta agli

⁶³⁰ UFFICIO DEL COMMISSARIO AUSTRALIANO PER L'INFORMAZIONE, *Bozza di consultazione: Guide to big data and the Australian Privacy Principles* [Guida ai megadati e ai principi australiani in materia di tutela della vita privata], 05/2016.

⁶³¹ Si comparino, come esempio di tale dialettica, F. Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, in *Nw. U. L. Rev.*, 104, p. 160ss. (2010); KROLL J.A., J. HUEY, BAROCAS S., FELTEN E.W., REIDENBERG J.R., ROBINSON D.G. YU H., «Accountable Algorithms», in *Un. Pennsylvania L. R.*, 165, 2017, p. 633ss.

⁶³² Cfr. KROLL J.A., J. HUEY, BAROCAS S., FELTEN E.W., REIDENBERG J.R., ROBINSON D.G. YU H., *op. cit.*, p. 639.

input ricevuti, dal momento che esaminare le risposte alla luce delle variazioni degli *input* non risolve la questione dell'individuazione della causa di tali cambiamenti, né consente di stabilire se o perché un cambiamento è significativo⁶³³. E poi perché la trasparenza al più può incidere sulla revisione delle basi delle decisioni generali, ma assai meno incisiva risulta per la revisione individualizzata di decisioni specifiche: si può ad esempio pensare al caso dei sistemi di apprendimento automatico online (come quelli per estrarre dati dai *post* sui *social network*), i quali possono aggiornare il loro modello per le previsioni dopo ogni decisione, incorporando ogni nuova osservazione come parte dei dati di addestramento. Anche conoscere il codice sorgente e i dati, per quanto attiene a tali sistemi, non è sufficiente per replicare o prevedere il loro comportamento⁶³⁴. La trasparenza, a fronte degli aggiornamenti compiuti indifferentemente da umani o (continuamente) dal sistema in autonomia, da sola non spiega perché sia stata presa una decisione particolare o quanto il sistema funzioni *in modo equo*.

Trasparenza, insomma, non è ancora sinonimo di sicurezza.

Altrettanto rilevante appare il principio di correttezza, legato a doppio filo a quello di trasparenza nella misura in cui, come abbiamo ampiamente evidenziato, il trattamento automatizzato, e segnatamente la profilazione, può essere iniquo e può creare discriminazioni fortemente incidenti sulla libertà di autodeterminazione dell'interessato- In proposito, si può pensare all'emblematico esempio riportato in un noto Report del Comitato per il commercio, la scienza e i trasporti del Senato degli Stati Uniti, che contempla la fattispecie in cui un intermediario di dati venda profili di consumatori a società finanziarie senza il consenso dei consumatori o senza che essi conoscano i dati sottostanti: tali profili classificano gli stessi consumatori in categorie con diciture quali "popolazione

⁶³³ Ivi, p. 660.

⁶³⁴ Ivi, p. 640.

rurale e che ce la fa a malapena” o “membro di una minoranza etnica”, oppure assegnano loro dei punteggi, basati sulla rispettiva vulnerabilità finanziaria dei consumatori, così da determinare la società finanziaria ad offrire ai consumatori medesimi prodotti finanziari rischiosi⁶³⁵.

Le Linee Guida si soffermano poi sul principio di limitazione delle finalità nel caso assai diffuso degli ulteriori trattamenti (o trattamenti secondari), sancito come sappiamo dall’art. 5 lett. b), rilevando come la profilazione possa ampiamente comportare l’utilizzo di dati raccolti per finalità diverse da quelle originarie, senza che le prime siano esplicitamente dichiarate all’interessato al pari di quanto accaduto originariamente con le seconde: esempio emblematico è quello in cui un’applicazione da *smart phone* che fornisce servizi di localizzazione utili all’utente per trovare ristoranti nelle vicinanze utilizzi i dati raccolti anche per creare un profilo dell’interessato per finalità di marketing personalizzato, ossia per individuare le sue preferenze alimentari o il suo stile di vita in generale allo scopo di proporgli annunci pubblicitari personalizzati; e ciò senza che l’interessato sia stato informato del trattamento secondario in questione, e dunque della relativa estensione delle finalità⁶³⁶.

In ipotesi, infatti, la finalità in questione potrebbe non essere compatibile con quelle originariamente dichiarate nell’informativa: come sappiamo, il Regolamento impone che un trattamento per finalità diverse da quelle originarie sia lecito solo allorché le prime siano compatibili con quelle dichiarate in origine,

⁶³⁵ Cfr. SENATO DEGLI STATI UNITI, COMITATO PER IL COMMERCIO, LA SCIENZA E I TRASPORTI, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* [Rassegna del settore degli intermediari: raccolta, utilizzo e vendita di dati sui consumatori per finalità di marketing], rapporto informativo per il presidente Rockefeller, 18 dicembre 2013 (in inglese), p. 12 ss.

⁶³⁶ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 12.

necessitando altrimenti il medesimo di un'autonoma base giuridica (ovvero, in linea di principio, necessitando del *consenso dell'interessato*, in quanto fondamento ordinario di liceità nell'architettura del GDPR)⁶³⁷.

Ebbene, il Regolamento, alla luce del suddetto principio invero nella disciplina di cui all'art. 6, in particolare nel suo paragrafo 4, letto alla luce del considerando 50, subordina la compatibilità in questione al modo in cui si declinino, nel caso di specie, determinati fattori, che la disposizione medesima elenca in modo non esaustivo, ma che il Gruppo ricostruisce a livello esegetico ed identifica innanzitutto nel «rapporto tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento», nonché nel «contesto in cui i dati personali sono stati raccolti e le ragionevoli aspettative dell'interessato in merito al loro uso futuro»; e poi, oltre alla natura dei dati e all'impatto del nuovo trattamento sull'interessato, valorizzando le *specifiche* «garanzie applicate dal titolare del trattamento per assicurare un trattamento corretto e prevenire qualsiasi impatto indebito sull'interessato»⁶³⁸.

Dopo un inciso dedicato al principio di minimizzazione dei dati, che nel contesto dei *Big Data analytics* importa la fondamentale esigenza, che il titolare è tenuto a soddisfare, di non «raccolgere più dati personali di quelli di cui [il titolare abbia] effettivamente bisogno» per il trattamento in essere, con il relativo obbligo *ex art. 12* di spiegare in maniera chiara e di giustificare la necessità della raccolta, il Gruppo si concentra su quella sua “articolazione” fondamentale rappresentata dal *principio di esattezza*, sancito dall'art. 5, par. 1, lett. d) del Regolamento, il quale puntualmente prescrive che i dati personali debbano essere «esatti e, se necessario, aggiornati», e che debbano essere adottate «tutte le misure

⁶³⁷ V. infatti, in combinato disposto, l'art. 6, in part. il par. 4, e il *considerando* 50. V. più ampiamente *retro*, par. 3.1.1.

⁶³⁸ *Ivi*, p. 12. V. art. 6 par. 4 e cons. 50 Reg. UE 2016/679.

ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati».

Abbiamo già più volte rilevato quanto decisivo sia, ai fini dell'attendibilità dell'output algoritmico, e più in generale della decisione, tanto la qualità dei dati "di partenza" e delle loro fonti quanto la qualità dell'intera filiera del trattamento. È stato limpidamente notato come spesso, nell'ambito delle ICTs, si dimentichi che non sempre la *qualità* dell'analisi è direttamente proporzionale alla *quantità* dei dati disponibili, e, soprattutto, che i costi sociali di quel fenomeno cui è stato dato il nome di *Bad Data* possono essere molto alti e «generare una vera e propria economia digitale dell'inefficienza, nella quale vengono sistematicamente ripetuti errori»⁶³⁹. Anche per questo, in letteratura si fa sempre più spesso richiamo ad una dimensione di *ecologia dei dati*, espressione che starebbe ad indicare la necessità di un nuovo modo di pensare ai dati e la promozione di maggiore consapevolezza e maggiore responsabilizzazione nel loro uso⁶⁴⁰.

Il Gruppo di Lavoro sembra aderire proprio a quest'ultimo indirizzo, nella misura in cui nelle Linee Guida sottolinea con forza come «il titolare del trattamento dovrebbe esaminare l'esattezza in tutte le fasi del processo di profilazione», facendo specifico riferimento alla raccolta e all'analisi dei dati, alla creazione del profilo di una persona fisica o all'applicazione di un profilo alla medesima per prendere una decisione⁶⁴¹. L'enfasi posta su tale profilo dei doveri del titolare pare motivato dalla consapevolezza dei problemi che abbiamo sopra evidenziato, e in particolar modo del fenomeno descritto come *garbage in-*

⁶³⁹ La citazione è di E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black-box society», cit. Cfr. più ampiamente sul punto D. BENDETTI, «IA e (in)sicurezza informatica», in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 241.

⁶⁴⁰ G. D'ACQUISTO, *Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati*, cit., p. 289.

⁶⁴¹ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 13.

garbage out: consapevolezza che traspare dall'inciso in cui efficacemente si constata che «se i dati utilizzati nel contesto di un processo decisionale automatizzato o di profilazione non sono esatti, qualsiasi decisione o profilo che ne deriverà sarà viziato», e ancora che «anche qualora i dati grezzi siano registrati in maniera esatta, l'insieme dei dati potrebbe non essere pienamente rappresentativo oppure l'analisi potrebbe contenere distorsioni nascoste». A ciò consegue che «il titolare del trattamento deve introdurre misure efficaci per verificare e assicurare su base continuativa che i dati riutilizzati od ottenuti indirettamente siano esatti e aggiornati», e ancora una volta si sottolinea l'importanza dell'obbligo gravante in capo al medesimo di fornire informazioni chiare, anche e soprattutto ai fini dell'esercizio del diritto, in cui il principio di esattezza più precipuamente si specifica, di rettifica (e di integrazione) di cui all'art. 16⁶⁴².

Conclude la panoramica sui principi il riferimento al principio di limitazione della conservazione, *ex art. 5 par. 1 lett. e*). Esso, anche nella prospettiva adottata dal Gruppo, assurge a declinazione del principio di minimizzazione dei dati: ciò traspare dal fatto che le Linee Guida, dopo aver preso atto che gli algoritmi di apprendimento automatico, implementandosi attraverso il trattamento di grandi quantità di informazioni, possono beneficiare della conservazione dei dati, a maggior ragione in caso di profilazione, subito specifica che il titolare del trattamento «deve rispettare il principio di minimizzazione dei dati all'atto della raccolta e assicurare che i dati non siano conservati per un periodo superiore a quello necessario e proporzionato alle finalità per le quali i

⁶⁴² *Ibidem*. V. poi l'art. 16 del Reg. UE 2016/679, in forza del quale: «L'interessato ha il diritto di ottenere dal titolare del trattamento la *rettifica* dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa».

dati vengono trattati»⁶⁴³. Al principio in questione fanno dunque specularmente riscontro, oltre all'obbligo che dall'art. 5 lettera f) sul principio di integrità si desume, ossia quello di garantire che i dati siano «aggiornati durante il periodo di conservazione in maniera da ridurre il rischio di inesattezze», e dunque al corrispondente diritto di rettifica cui abbiamo già fatto riferimento, anche e soprattutto il diritto alla cancellazione sancito dall'art.17, disposizione che la più gran parte della dottrina ha ritenuto codificasse allora quel *diritto all'oblio* che la Corte di Giustizia dell'Unione europea avrebbe definitivamente sancito in contesto “telematico” (e in particolare con riferimento alla cancellazione dei dati personali da banche dati informatiche) nella già più volte citata sentenza *Google Spain*, desumendolo da un'interpretazione evolutiva, *fundamental rights oriented* della dir. 95/46/CE (e in particolare del suo art. 12)⁶⁴⁴: il collegamento con il principio di limitazione della conservazione, cui facevamo cenno, in particolar modo troverebbe il proprio riferimento normativo nella lettera a) del par. 1, che prescrive l'obbligo in capo al titolare, laddove l'interessato ne faccia richiesta e

⁶⁴³ *Ibidem*.

⁶⁴⁴ Sul tema la letteratura è vasta, e al suo interno si confrontano voci più favorevoli ed altre più critiche, le quali segnatamente sottolineano l'eccessiva genericità della disposizione a fronte dell'orientamento al contrario assai puntuale esplicitato dalla Corte nella sentenza, che ivi ha riconosciuto esistenti in capo all'interessato, quale specifica articolazione del diritto fondamentale alla protezione dei dati personali, un vero e proprio *diritto all'oblio*, azionabile nei confronti dei motori di ricerca in quanto titolari secondari del trattamento, comunque sempre bilanciabile caso per caso, secondo il principio di proporzionalità, con altri diritti fondamentali, tra cui il diritto di cronaca. Cfr. *ex multis* G. FINOCCHIARO, «La memoria della rete e il diritto all'oblio», in *Dir. inf.*, 2010, p. 391 ss.; MESSINA, «Le prospettive del diritto all'oblio nella società dell'informazione e della comunicazione», in *Inform. dir.*, 2009, p. 93 ss.; M. LUCIANI, *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, cit., p. 20 ss.; VIGLIANISI FERRARO, «La sentenza Google Spain ed il diritto all'oblio nello spazio giuridico europeo», in *Contr. impr./Eur.*, 2015, p. 159 ss.; O. POLLICINO, «Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain», in *Dir. dell'Informazione e dell'Informatica*, 2014, 569 sgg; C. COLPAIETRO, A. IANNUZZI, «I principi generali del trattamento dei dati personali e i diritti dell'interessato», in AA. VV., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, (a cura di) L. CALIFANO, C. COLAPIETRO, Milano, ES, 2017, 85 sgg.

non prevalga uno degli altri diritti fondamentali oggetto di ponderazione positivamente imposta dal par. 3, di cancellare i dati quando essi «non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati»⁶⁴⁵.

Successivamente, le Linee Guida passano ad occuparsi delle basi giuridiche, e quindi delle situazioni tipicizzate dal Regolamento dalla cui sussistenza dipende la liceità del trattamento: per i trattamenti, compresa la profilazione ed i processi decisionali automatizzati diversi da quelli ricadenti nell'alveo dell'art. 22, risultando adeguati pressoché tutti i fondamenti di liceità individuati dall'art. 6 del Regolamento. Ci limiteremo qui ad analizzare più nel dettaglio soltanto le due basi il riferimento alle quali, oltre che ad essere più frequente, solleva nella nostra contemporaneità diversi problemi esegetici, prima ancora che applicativi. Si tratta del *consenso dell'interessato* e del *legittimo interesse* del titolare del trattamento.

La prima, fondamentale base giuridica oggetto di analisi non può che essere quella che apre la “piramide” di cui all'art. 6: il consenso dell'interessato, nel quadro della disciplina europea della protezione dei dati personali, rappresenta la

⁶⁴⁵ Cfr. art. 17, par. 1, Reg. UE 2016/679: «1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.»

regola, e dunque il *fondamento giuridico* del trattamento ogniqualvolta non sussista l'elemento della *necessità*, nelle differenti declinazioni previste dal medesimo art. 6 del GDPR⁶⁴⁶. Sin dal primo intervento armonizzatore in materia, il consenso - quale elemento legittimante il trattamento - è sempre stato posto dal legislatore europeo al centro della disciplina a protezione dei dati personali, e ciò allo scopo di dare attuazione al diritto all'autodeterminazione informativa della persona fisica, che autorizzando l'altrui ingerenza nella propria sfera privata innesca così un meccanismo di «circolazione controllata delle informazioni»⁶⁴⁷. Il consenso, peraltro, veniva ritenuto tradizionalmente lo strumento più idoneo a garantire un soddisfacente equilibrio tra sviluppo della personalità e costruzione del mercato⁶⁴⁸.

Tuttavia, come abbiamo già rilevato, nella contemporanea società datificata, in cui la sfera privata della persona «si riscopre fragile – stretta tra pretese di controllo di matrice pubblicistica e logiche di mercato»⁶⁴⁹, particolarmente esposta alle pratiche commerciali di aziende che occupano posizioni dominanti sul mercato ed offrono servizi difficilmente rinunciabili se non a pena di “emarginazione” sociale, il consenso rischia di tradursi in una trappola che garantisce una «tutela meramente formale» della persona e la riduce a consumatore: ciò vale in particolare nel contesto delle c.d. Condizioni Generali di Contratto, riconducibili al più ampio fenomeno della contrattazione standardizzata, unilateralmente predisposte dagli operatori commerciali (nel

⁶⁴⁶ Cfr. F. Bravo, Il consenso e le altre condizioni di liceità del trattamento di dati personali, in G. Finocchiaro (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 101 ss.

⁶⁴⁷ La citazione è di G. M. RICCIO, «Commento artt. 23-27», in S. SICA, P. STANZIONE (a cura di), *La nuova disciplina della privacy*, Bologna, 2003. Cfr. sul punto M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», cit., p. 82 ss.

⁶⁴⁸ Cfr. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema di fonti multilivello*, Napoli, 2018, passim.

⁶⁴⁹ Cfr. S. RODOTÀ, *Riservatezza*, cit., p. 72, e M. G. STANZIONE, *Consenso e trattamento di dati personali nella dimensione europea*, cit., p. 80.

nostro campo, anche, titolari del trattamento) in virtù del loro asimmetrico potere negoziale⁶⁵⁰. A tale realtà oggi, come più volte evidenziato, si aggiunge l'utilizzo delle tecnologie computazionali e dei sistemi algoritmici ai fini del c.d. *tracciamento* delle attività compiute online, e dunque la stessa raccolta ed elaborazione per scopi di profilazione delle informazioni consistenti nelle “tracce” lasciate dall'utente durante la navigazione attraverso l'invio (o piuttosto, l'applicazione) di quei marcatori temporanei denominati *cookies*⁶⁵¹. In questo opaco contesto, tra gli ISP e i fornitori di contenuti online era invalsa la consuetudine di ottenere il consenso per mezzo di caselle preselezionate, secondo la logica dell'*opting out*: la liceità di tale condotta, tuttavia, pare oggi essere definitivamente esclusa dalla recente sentenza *Planet 49* della Corte di Giustizia⁶⁵².

Oggi, insomma, assai attuale appare la questione relativa all'idoneità del consenso dell'interessato a costituire ancora il mezzo più adeguato nel garantire l'esercizio del diritto all'autodeterminazione informativa: a tal proposito,

⁶⁵⁰ Sul punto cfr. le importanti riflessioni di S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 400 ss. e V. D'ANTONIO, «Il consenso al trattamento dei dati personali tra autodeterminazione informativa e dinamiche remuneratorie», in *I “poteri privati” delle piattaforme*, cit., p. 163 ss.

⁶⁵¹ L'Autorità garante per la protezione dei dati personali italiana nelle recenti Linee Guida su cookie ed altri strumenti di tracciamento del 10 giugno 2021 definisce i cookies nel modo seguente: «i cookie sono di regola stringhe di testo che i siti web (cd. Publisher, o “prime parti”) visitati dall'utente ovvero siti o web server diversi (cd. “terze parti”) posizionano ed archiviano – direttamente, nel caso dei publisher e indirettamente, cioè per il tramite di questi ultimi, nel caso delle “terze parti” - all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo». Aggiunge l'Autorità che «i terminali cui ci si riferisce sono, ad esempio, un computer, un tablet, uno smartphone, ovvero ogni altro dispositivo in grado di archiviare informazioni. Già oggi, e ancor più in futuro, tra essi occorre annoverare anche i cd. dispositivi IoT (Internet of Things, o Internet delle cose), i quali sono progettati per connettersi alla rete e tra loro per fornire servizi di varia natura, non necessariamente limitati alla mera comunicazione». Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPD), *Linee guida cookie e altri strumenti di tracciamento* - 10 giugno 2021 [9677876], par. 2.

⁶⁵² Cfr. C. Giust. UE, 1 ottobre 2019, C-673/17. Occorre sottolineare che, sempre in ambito eurounitario, le recenti Linee guida sul consenso 5/2020 dell'EDPB escludono la liceità dei c.d. *cookie wall*, che costituiscono vere e proprie barriere dirette a impedire l'accesso ai siti internet nei confronti degli utenti che non prestino il proprio consenso alla profilazione.

riecheggiano forti le parole con cui il Garante italiano ha avuto modo di sottolineare, in tempi non ancora (del tutto) sospetti, che il consenso possa dirsi libero solo allorché si presenti «come manifestazione del diritto all'autodeterminazione informativa, e dunque al riparo da qualsiasi pressione, e se non viene condizionato all'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto»⁶⁵³.

Il Gruppo di Lavoro, nel contesto delle Linee Guida e con specifico riferimento all'attività di profilazione, non resta certo indifferente, e afferma che «la profilazione può non essere trasparente. Spesso si basa su dati derivati o desunti da altri dati, anziché su dati forniti direttamente dall'interessato». Tuttavia, esso rinvia alle pertinenti Linee Guida 5/2020 sul consenso ai fini di una disamina nel merito della disciplina della base giuridica in parola, limitandosi ad affermare che «il titolare del trattamento che intende fare affidamento sul consenso come base per la profilazione dovrà dimostrare che gli interessati comprendono esattamente a cosa stanno acconsentendo e dovrà ricordare che il consenso non è sempre una base appropriata per il trattamento»; e, al contempo, a specificare che, nei casi dei processi decisionali di cui all'art. 22, una delle tre deroghe al divieto generale che il Gruppo ritiene configuri la norma medesima consiste proprio nel consenso, tuttavia *espresso*⁶⁵⁴. Ci si soffermerà a tempo debito sul significato di quest'ultimo termine: in questa sede, nei limiti in cui la presente trattazione lo consente, è necessario passare in rassegna quali siano i requisiti cui il Regolamento, alla luce dei più consolidati indirizzi esegetici (dottrinali e giurisprudenziali), subordini l'integrazione della fattispecie del

⁶⁵³ Cfr. Garante per la protezione dei dati personali, Prov. 28 maggio 1997, doc. web. 40425.

⁶⁵⁴ Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 14. Cfr. poi Comitato europeo per la protezione dei dati, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 14 maggio 2020.

consenso dell'interessato agli effetti della normativa medesima, e dunque quale *fondamento di liceità del trattamento dei dati dell'interessato*.

La prima considerazione da cui occorre partire è che, se in ordine alla natura (per lo più identificata come dispositiva-negoziale⁶⁵⁵ o piuttosto autorizzativa-procedimentale⁶⁵⁶) del consenso come base giuridica del trattamento si sono succedute negli anni molteplici e contrastanti opinioni, con l'avvento della disciplina generale in materia di protezione dei dati personali introdotta dal GDPR il problema in questione sembra essere superato. Si concorda qui, insomma, con quella parte della dottrina che ritiene il *consenso qualificato*, ossia utile a fondare la liceità del trattamento ex art. 6 par. 1, in combinato disposto con l'art. 4 par. 1 n. 11 che della fattispecie medesima individua i presupposti costitutivi, un *istituto di autonoma configurazione*, risultante dal sistema predisposto dal Regolamento al fine di tutelare il diritto fondamentale della persona alla protezione dei dati che la riguardano, garantendo il bilanciamento con gli altri diritti e interessi meritevoli di tutela, di pari rango, con cui possa entrare in conflitto⁶⁵⁷. Così, ai fini della ricostruzione della sua natura, delle sue funzioni e dei suoi limiti, le disposizioni che vi si riferiscono andrebbero lette in modo sistematico, alla luce dell'intero *corpus* regolamentare, e dunque - primo fra tutti - alla luce del nuovo, centrale principio di responsabilizzazione del titolare.

Le caratteristiche essenziali del consenso sono elencate nella definizione di cui all'art. 4, n. 11 del GDPR, che identifica il consenso dell'interessato in «qualsiasi manifestazione di volontà *libera, specifica, informata e inequivocabile* dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante

⁶⁵⁵ Cfr. ad es. G. OPPO, «Sul consenso dell'interessato», in V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 124 ss.

⁶⁵⁶ Cfr. ad es. A. FICI, E. PELLECCIA, «Il consenso al trattamento», in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, I, p. 485 ss.

⁶⁵⁷ Così in particolare M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», cit., p. 82 ss.

dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

Al primo posto viene, allora, posta tra le condizioni essenziali per la validità del consenso (ai fini dell'integrazione della relativa base giuridica del trattamento) la sua *libertà*, intesa quale assenza di condizionamenti tanto nella formazione quanto nella espressione della volontà medesima: l'attenzione è posta dal Regolamento, in particolare, sulle conseguenze dell'eventuale dissenso, laddove alla luce del *considerando* 42 pare richiedere che l'interessato sia posto nella condizione di poter scegliere se accettare o meno il trattamento dei propri dati senza che da tale scelta possa derivare un pregiudizio nei suoi confronti⁶⁵⁸.

Nella realtà attuale, l'interrogativo sulla sussistenza di una manifestazione di volontà effettivamente libera si pone soprattutto in quelle situazioni in cui il perfezionamento del contratto sia subordinato alla prestazione del consenso al trattamento dei dati personali dell'interessato, laddove quest'ultimo non possa ritenersi necessario all'esecuzione del contratto medesimo (poiché in tal caso ricorrerebbe l'ipotesi tipicizzata dall'art. 6, par. 1 lett. b), consistente nella funzionalità a fini negoziali del trattamento, e risulterebbe dunque integrata la base giuridica della *necessità ai fini dell'esecuzione di un contratto*), quanto piuttosto preordinato al perseguimento di finalità ulteriori, come quelle pubblicitarie o di marketing. Le operazioni in questione, denominati anche *tying arrangements*, hanno scaturito da tempo un intenso dibattito dottrinale che ha condotto a discorrere di "mercato dei dati personali" e ha posto l'attenzione sul fenomeno, già descritto, della patrimonializzazione del dato personale stesso, con

⁶⁵⁸ V. il *considerando* 42 nella parte in cui afferma: «Il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio».

i conseguenti interrogativi sull'ammissibilità di una qualificazione del consenso al trattamento quale controprestazione nello schema contrattuale ⁶⁵⁹.

Ebbene, se è vero in punto di liceità del trattamento effettuato su tali basi nel quadro delle suddette operazioni il Garante italiano ha sempre manifestato un atteggiamento di chiusura, ribadendo che «non può definirsi libero, ma necessitato, il consenso al trattamento dei dati personali che l'interessato "deve" prestare (aderendo a un testo predisposto unilateralmente dalla controparte contrattuale), quale condizione per il conseguimento della prestazione richiesta»⁶⁶⁰; e se è vero che lo stesso *European Data Protection Supervisor* ha affermato a gran voce che «i diritti fondamentali, come il diritto alla protezione dei dati personali, non possono essere ridotti a semplici interessi dei consumatori e (...) non possono essere considerati una mera merce»⁶⁶¹; tuttavia il quadro pare essersi complicato con l'entrata in vigore della Direttiva (UE) 2019/770 relativa a determinati aspetti del contratto di fornitura di contenuto digitale e di servizi digitali⁶⁶². Quest'ultima, infatti, all'art. 3 stabilisce l'applicabilità della direttiva medesima anche al «caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico» per finalità diverse dalla fornitura del contenuto o dei servizi medesimi: con ciò trovando

⁶⁵⁹ Cfr. sul punto G. RESTA, V. ZENCOVICH, «Volontà e consenso nella fruizione dei servizi in rete», in *Rivista trimestrale di diritto e procedura civile*, 2018, p. 441 ss.; C. PERLINGIERI, «Data as the Object of a Contract and Contract Epistemology», in *The Italian Law Journal*, 2019, 5, 2, p. 613 ss.; S. THOBANI, «Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente», in *Media Laws*, 2018, p. 131 ss.

⁶⁶⁰ V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Prov. 14 luglio 2013, n. 330, doc. web n. 2542348.

⁶⁶¹ V. EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, n. 4/2017.

⁶⁶² Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, OJ L 136, 22.5.2019, p. 1–27, <https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32019L0770>.

riscontro normativo una fattispecie negoziale in cui il consenso al trattamento pare, effettivamente, assurgere a controprestazione.

Tuttavia, nella Direttiva stessa sussiste una clausola che rende la disciplina medesima *espressamente residuale* rispetto all'applicazione del GDPR: l'art. 3, par. 8 dispone infatti che in caso di conflitto tra le disposizioni della direttiva medesima e del diritto dell'UE in materia di protezione dei dati personali, a prevalere è quest'ultimo, in ciò supportato dal *considerando* 38 che, nell'inciso che a noi qui più interessa così afferma: «quando il trattamento dei dati personali si basa su un consenso, segnatamente a norma dell'articolo 6, paragrafo 1, lettera a), del regolamento (UE) 2016/679, si applicano le disposizioni specifiche di tale regolamento, comprese quelle relative alle condizioni per valutare se il consenso sia stato o meno liberamente prestato»⁶⁶³.

Ora, nel quadro del Regolamento assume rilevanza centrale il disposto dell'art. 7, par. 4, che espressamente dispone: «Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto». Secondo l'interpretazione fatta

⁶⁶³ Può essere utile leggere per intero il *considerando* in parola: «La presente direttiva non dovrebbe disciplinare le condizioni per il trattamento lecito dei dati personali, dal momento che tale questione è specificamente disciplinata dal regolamento (UE) 2016/679. Di conseguenza, qualsiasi trattamento di dati personali in relazione a contratti rientranti nell'ambito di applicazione della presente direttiva è lecito solo se è conforme alle disposizioni del regolamento (UE) 2016/679 relativo ai fondamenti giuridici per il trattamento dei dati personali. Quando il trattamento dei dati personali si basa su un consenso, segnatamente a norma dell'articolo 6, paragrafo 1, lettera a), del regolamento (UE) 2016/679, si applicano le disposizioni specifiche di tale regolamento, comprese quelle relative alle condizioni per valutare se il consenso sia stato o meno liberamente prestato. La presente direttiva non dovrebbe disciplinare la validità del consenso prestato. Il regolamento (UE) 2016/679 include inoltre diritti esaustivi in materia di cancellazione e portabilità dei dati. La presente direttiva non dovrebbe pregiudicare tali diritti, che si applicano ai dati personali forniti dal consumatore all'operatore economico o raccolti dall'operatore economico in relazione a qualsiasi contratto rientrante nell'ambito di applicazione della presente direttiva, e in caso di risoluzione del contratto da parte del consumatore in conformità della presente direttiva».

propria dalle Linee Guida dell'EDPB in materia di consenso, e condivisa da autorevole dottrina, la disposizione in esame subordinerebbe il carattere libero del consenso all'effettiva sussistenza per l'interessato della possibilità di scelta effettiva e di controllo sui propri dati: cosicché essa, in siffatta prospettiva, sancirebbe una presunzione legale *relativa* di invalidità del consenso fondato sul difetto del requisito di libertà ogniqualvolta la conclusione del contratto sia condizionata alla prestazione del consenso al trattamento per finalità *non necessarie* all'esecuzione del contratto medesimo⁶⁶⁴. Le stesse Linee Guida aggiungono che, se l'effettività della scelta dipende dalla possibilità per l'interessato di accedere al servizio anche senza prestare il consenso al trattamento, chi subordina un servizio al medesimo dovrebbe pertanto offrire all'utente anche una *versione «generalmente equivalente»* del servizio medesimo⁶⁶⁵: e a tale indirizzo si è conformato il Garante europeo, che ha dichiarato come il fornitore del servizio debba provvedere a porre in essere tale alternativa senza alcun detrimento nei confronti dell'utente o almeno prevedendo in alternativa un *servizio a pagamento a prezzo ragionevole*, introducendo dunque il requisito dell'equivalenza⁶⁶⁶.

A fronte di tale felice approdo, bisogna tuttavia qui sinteticamente considerare che la Corte di Cassazione italiana in una recente sentenza ha accolto un'interpretazione della nozione in esame in senso oggettivo, ritenendo

⁶⁶⁴ Cfr. Comitato europeo per la protezione dei dati personali, Linee Guida 5/2020 sul consenso, cit. Da aggiungersi che secondo il parere 06/2014 del WP 29 il termine «necessario per l'esecuzione di un contratto» deve essere interpretato in senso stretto, cosicché il trattamento deve essere necessario per il vero e proprio adempimento delle obbligazioni derivanti dal singolo contratto in concreto stipulato con ciascun interessato. Per la dottrina concorde, cfr. in particolare M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», cit., p. 103 ss.; S. THOBANI, «Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente», cit. p. 140 ss.

⁶⁶⁵ Ivi, punto 37.

⁶⁶⁶ Cfr. EDPS, *Opinion in the review of the ePrivacy Directive (2002/58/CE)*, 22 luglio 2016, 15-16.

sufficiente la reperibilità sul mercato di un servizio, appunto, provvisto delle medesime caratteristiche, e dunque la sussistenza di un'equivalente alternativa messa a disposizione sul mercato *anche solo* da altri operatori economici⁶⁶⁷. Ci riferiamo al noto caso *ADSpray*, avente ad oggetto la situazione in cui una società offriva l'accesso ad una newsletter su tematiche inerenti a fisco, finanza e diritto subordinandone l'iscrizione alla prestazione del consenso al trattamento dei dati personali da parte dell'utente tramite spunta attiva ad una casella. In breve, per i profili che qui interessano, la Suprema Corte, pur accogliendo il ricorso in virtù della riscontrata assenza del requisito della specificità, afferma l'ammissibilità di tali operazioni, e conseguentemente la liceità del trattamento sotto il profilo della sussistenza del requisito indefettibile della libertà, laddove, oltre ad un consenso «non coartato» nelle sue tradizionali accezioni, sussistano i due requisiti della «*fungibilità*» e della «*rinunciabilità*» della prestazione medesima: numerose criticità sollevando soprattutto l'interpretazione del secondo requisito, dacché difficile risulta l'individuazione di un univoco criterio attraverso cui stabilire quando un servizio o contenuto sia irrinunciabile, e dunque *essenziale*, per l'utente-interessato⁶⁶⁸.

Venendo agli altri requisiti indefettibili del consenso individuati dall'art. 4 n. 11, il secondo consiste nella *specificità*, cui il primo si lega saldamente: dal momento che un servizio può includere molteplici operazioni diverse (anche di trattamento, e specialmente automatizzato), risulta essenziale per la persona

⁶⁶⁷ Cfr. sul punto S. THOBANI, «La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità», in *Europa e Diritto Privato*, 2016, 2, p. 547 ss.; M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», cit. p. 106 ss.

⁶⁶⁸ Cass. civ., Sez. I, 2 luglio 2018, n. 17278, in *Giur. It.*, 2019, 3, p. 530 ss., con nota di S. THOBANI, «Operazioni di tying e libertà del consenso».

interessata la libertà di scegliere a quale specifico trattamento acconsentire e per quali finalità⁶⁶⁹.

Il principio in virtù del quale il consenso al trattamento risulta validamente prestato, e dunque idoneo a fondare la liceità del primo, solo se manifestato liberamente e specificamente in relazione ad un trattamento chiaramente individuato, si arricchisce poi del requisito della *consapevolezza* dell'interessato in ordine ai termini, alle modalità, ai limiti, alle finalità e a tutti gli elementi di cui si compone il trattamento specifico: principio cui fa da corollario, appunto, il dovere del titolare di predisporre (*ex art. 12*) un'adeguata informativa, affinché appunto l'interessato possa autodeterminarsi. Il consenso libero e specifico, attraverso il requisito in questione, diviene dunque (se vuole essere qualificato, e di conseguenza valido) anche informato⁶⁷⁰.

Infine, il GDPR introduce il requisito dell'*inequivocabilità* della manifestazione del consenso da parte dell'interessato, che tuttavia si lega saldamente al principio di *libertà di forma*, in virtù del quale non è richiesta *ad substantiam* la dichiarazione espressa, bensì risulta sufficiente qualsiasi azione positiva inequivocabile: scelta che assume particolare rilevanza nel contesto online, ove può ritenersi valida ai fini della manifestazione del consenso, anche alla luce del *considerando 32*, qualsiasi comportamento che indichi senza dubbio l'accettazione del trattamento, tra cui la selezione positiva di caselle⁶⁷¹. Ciò,

⁶⁶⁹ Cfr. M. G. STANZIONE, «Consenso e trattamento di dati personali nella dimensione europea», cit., p. 88.

⁶⁷⁰ Ivi, pp. 88-89.

⁶⁷¹ Il *considerando 32*, tra le altre importanti indicazioni, promuove il superamento della logica dell'*opting-out*, affermando che non dovrebbe considerarsi validamente prestato, ed anzi non configurerebbe proprio manifestazione di volontà integrante la base giuridica rappresentata dal consenso dell'interessato, il silenzio, l'inattività e, soprattutto, la preselezione di caselle. Recita infatti, integralmente, il *considerando* in parola: «Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di

ovviamente salve le eccezioni espressamente previste dal legislatore, in cui ai fini della validità del consenso sia richiesta la sua sola *espressione mediante dichiarazione*: eccezioni tra le quali emblematicamente ricadono il trattamento di dati sensibili *ex art. 9* e, per quel che qui più interessa, la prima deroga al divieto generale di processi decisionali interamente automatizzati prevista dall' *art. 22, par. 2, lett. c)*, sulla quale ci soffermeremo a breve. Strettamente legata a tali prescrizioni è quella dell' *art. 7 par. 2* che impone al titolare, qualora la richiesta di consenso sia predisposta per iscritto, nel contesto di una dichiarazione riguardante più trattamenti, di proporla in modo chiaramente distinguibile.

Il principio di libertà di forme poi, letto alla luce del principio fondamentale di responsabilizzazione del titolare, parrebbe implicare come corollario il principio di *libertà di prova*, che troverebbe allora il proprio fondamento nell' *art. 7 par. 1*: perciò il titolare del trattamento dovrebbe risultare libero di provare con qualsiasi mezzo tanto l'accettazione intervenuta da parte dell'interessato quanto degli adempimenti da questi posti in essere per garantire il soddisfacimento dei requisiti di validità del consenso (tra cui la predisposizione di adeguata informativa).

Chiudiamo la nostra analisi sugli elementi essenziali della base giuridica in esame aggiungendo che il diritto a prestare un consenso libero, specifico, consapevole e inequivocabile, quale principale declinazione del diritto fondamentale di autodeterminazione informativa, si completa di - e trova ulteriore garanzia nel - *diritto di revoca* sancito dall' *art. 7 par. 3*, che legittima l'interessato

impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. *Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle*. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

a revocare il consenso medesimo non solo in qualsiasi momento e senza motivazione, ma anche con la stessa facilità con cui lo abbia inizialmente prestato, a dimostrazione della corrispondenza biunivoca tra i due termini⁶⁷².

Abbandonando la principale, generale base giuridica del consenso dell'interessato, possiamo limitarci a fare un cenno alla prima tra le basi individuate dal legislatore come manifestazione del presupposto della *necessità* del trattamento: quella, cui già abbiamo fatto riferimento, consistente nella *necessità di esecuzione di un contratto* di cui l'interessato sia parte (o, anche, di misure precontrattuali adottate su richiesta dello stesso), prevista dalla lett. b) dell'art. 6 par. 1.

Lucidamente, il Gruppo di Lavoro osserva come i titolari del trattamento potrebbero avere interesse ad impiegare trattamenti o più articolati processi decisionali automatizzati nell'alveo di un rapporto contrattuale poiché essi riducono potenzialmente le possibilità di errore umano nella maturazione e nella esecuzione della decisione, riducono potenzialmente il rischio che i clienti non riescano a soddisfare i pagamenti di beni e servizi e in generale «consentono di prendere decisioni in tempi più brevi e di migliorare l'efficienza»⁶⁷³. In ogni caso, tuttavia il Gruppo efficacemente sottolinea come nessuna di queste condizioni sia da sola sufficiente a dimostrare che il trattamento sia necessario ai fini dell'esecuzione del contratto ai sensi dell'art. 6, par. 1 lett. b): come è stato affermato a livello esegetico dallo stesso Gruppo nel suo Parere n. 06/2014 in

⁶⁷² V. art. 7, par. 3: «L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato». Cfr. F. Resta, Art. 7 Condizioni per il consenso, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), GDPR e normativa privacy, cit., p. 83 ss.

⁶⁷³ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 14.

punto di legittimo interesse, infatti, la nozione di necessità deve essere interpretata in maniera *restrittiva*⁶⁷⁴.

Veniamo a questo punto all'altra importante base giuridica che, lo anticipiamo, non ricade tra i fondamenti eccezionali di liceità individuati dall'art. 22 par. 2 in materia di processi decisionali interamente automatizzati: ci riferiamo all'ipotesi prevista dall'art. 6, par. 1, lett. f), ovvero la circostanza in cui il trattamento sia «necessario per il perseguimento del *legittimo interesse* del titolare del trattamento o di terzi»⁶⁷⁵.

La base giuridica in questione assume rilievo centrale perché essa, tra le situazioni tipicizzate di necessità, alternative dunque al fondamento del consenso, figura tra le più addotte dai titolari, specialmente laddove questi siano operatori economici. Ciò si spiega anche in virtù del fatto che il GDPR, al *considerando* 47, risulta abbastanza generico nell'individuare - in funzione esegetica - le situazioni potenzialmente qualificabili come *legittimo interesse*. Il *considerando* in parola si limita ad affermare che «potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento». E ancora, sempre a titolo di esempio, individua quale legittimo interesse quello del titolare del trattamento «interessato a trattare dati personali strettamente necessari a fini di prevenzione delle frodi». Aggiunge poi che possa

⁶⁷⁴ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf . V. in part. *retro*, nota 662.

⁶⁷⁵ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit, p. 16.

essere considerato tale anche l'«interesse a trattare dati personali per finalità di marketing diretto»⁶⁷⁶.

Tuttavia, il Gruppo in base al dettato letterale del medesimo articolo 6, par. 1, lett. f) sottolinea opportunamente come la base in questione non sia automaticamente integrata per il solo fatto che sussista un interesse siffatto, dal momento che la norma prescrive esplicitamente che «il titolare del trattamento *deve procedere a una ponderazione* per valutare se gli interessi o i diritti e le libertà fondamentali dell'interessato non prevalgano sui propri interessi»⁶⁷⁷. Lo stesso *considerando* 42 offre sul punto dei chiarimenti importanti a livello interpretativo, in particolare là dove afferma che, nel valutare la prevalenza o meno dei diritti e delle libertà dell'interessato, in massima considerazione vanno tenute le «ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento»; e, ancora che «l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine».

Nel quadro di tale ponderazione, qualora il trattamento consista nella profilazione, le Linee Guida individuano poi talune circostanze essenziali per stabilire la prevalenza o meno dei diritti e delle libertà fondamentali dell'interessato sull'asserito legittimo interesse del titolare: si ha riguardo, principalmente, al livello di dettaglio del profilo, ossia se questo risulti inserito in un gruppo ampio o piuttosto segmentato; la completezza del profilo medesimo;

⁶⁷⁶ Da notare che il *considerando* 49 aggiunge: «Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione (...)».

⁶⁷⁷ Risulta fondamentale la lettura dell'art. 6 par. 1 lett. f): «il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

l'impatto di quest'ultimo, in termini di effetti, sull'interessato; e, non ultime, «le garanzie destinate ad assicurare la correttezza, la non discriminazione e l'esattezza nel processo di profilazione»⁶⁷⁸.

Ebbene, a questo punto il Gruppo opera un fondamentale rinvio al proprio precedente Parere sui legittimi interessi, poc'anzi citato: documento che, sebbene ancora fondato sull'art. 7 della Dir. 95/46/CE, comunque contiene esempi «utili e pertinenti» per i titolari al fine di valutare la sussistenza di un interesse idoneo ad integrare la base giuridica in esame e, soprattutto, a soddisfare il requisito della *non prevalenza* di interessi e diritti fondamentali dell'interessato⁶⁷⁹. Assai importante, nel Parere, risulta anzitutto l'analisi del concetto di interesse rilevante ai fini della previgente Direttiva Madre (considerazioni che oggi valgono pressoché immutate anche per il GDPR) e soprattutto del suo connotato di «legittimità». Il Gruppo, in sintesi, ivi afferma che per essere pertinente ai sensi delle disposizioni menzionate, e dunque per soddisfare la soglia della «legittimità» e risultare «ammesso dalla legge», l'interesse dedotto dal titolare o dal responsabile del trattamento debba essere: «concreto ed effettivo», «lecito», e pertanto conforme al diritto europeo o nazionale applicabile; nonché «articolato in maniera sufficientemente chiara da consentire di eseguire il test comparativo valutando l'interesse legittimo del responsabile del trattamento rispetto agli interessi e ai diritti fondamentali dell'interessato»⁶⁸⁰.

⁶⁷⁸ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit, p. 16.

⁶⁷⁹ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, Commissione europea, 9 aprile 2014., cit., in part. p. 70 e 71.

⁶⁸⁰ Ivi, p. 30. Fondamentale sottolineare come il Gruppo preliminarmente a p. 28, se da una parte premetta che il concetto di interesse è strettamente collegato a quello di finalità, dall'altro nel contesto della disciplina europea della protezione dei dati personali esso se ne distingue poiché, in senso proprio, coincide piuttosto con «l'interesse più ampio che un responsabile può avere nel trattamento oppure il beneficio che il responsabile trae (o che potrebbe trarre la società) dal trattamento».

Sempre nel contesto delle Parere sul legittimo interesse richiamato, merita particolare attenzione il passaggio in cui il Gruppo si occupa della possibilità di ricorrere alla base del legittimo interesse a fronte di «pratiche intrusive di profilazione» e, più in generale, per qualsiasi trattamento, compresa l'attività di tracciamento, *per finalità di marketing o di pubblicità*, come ad esempio quelle che comportano il «tracciamento di persone fisiche su più siti web, ubicazioni, dispositivi, servizi o l'intermediazione tra dati». Se da una parte l'organo *non esclude* a priori che le finalità suddette possano integrare la base giuridica del legittimo interesse quale legale fondamento di liceità dei trattamenti in parola (allo stesso modo in cui, come abbiamo visto, non lo esclude, con riferimento esemplificativo al marketing diretto, il *considerando* 47), esso specifica che sarebbe *assai difficile* per il titolare giustificare il ricorso al medesimo⁶⁸¹.

Può essere utile aggiungere, in tale contesto, ricordare che l'art. 5 par. 3 della Direttiva 2002/58/CE, relativa alla vita privata ed alle comunicazioni elettroniche, prevede l'obbligo del consenso per tutte quelle attività consistenti nell'invio di pubblicità comportamentale basata su tecniche di tracciamento come i cookies (specialmente, dunque, di profilazione), che archiviano informazioni nel terminale dell'utente⁶⁸².

⁶⁸¹ Assai importante appare il passaggio, a p. 54 del suddetto parere, in cui il Gruppo, prendendo atto dell'evoluzione intervenuta nelle tecniche di tracciamento e di invio di materiale pubblicitario, afferma che «l'oggetto del test comparativo è cambiato: non si tratta più di valutare il diritto alla libertà di espressione commerciale, ma sostanzialmente gli interessi economici delle organizzazioni imprenditoriali di conoscere i loro clienti tracciandone e controllandone le attività online and offline, che devono essere bilanciati con i diritti (fondamentali) alla vita privata e alla tutela dei dati personali di tali persone e il loro interesse a non essere indebitamente controllate.».

⁶⁸² V. art. 5, par. 3 della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche: «Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la

Prima di passare ad una rapida analisi dei più importanti diritti garantiti all'interessato dalle disposizioni disciplinanti *tutti* i trattamenti automatizzati, è opportuno soffermare un momento l'attenzione su quella fattispecie che il GDPR all'art. 9 definisce «categorie particolari di dati», formula con cui lo stesso identifica le informazioni nella previgente disciplina qualificate in termini di «dati sensibili»: l'art. 9 prescrive infatti il divieto generale di «trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Tuttavia, come già sappiamo, al par. 2 la disposizione prevede una nutrita serie di eccezioni al divieto, che richiamano e integrano di ulteriori requisiti (a garanzia dell'interessato) alcune delle basi giuridiche previste dall'art. 6 par. 1: tra queste, lo ricordiamo, sia annovera *ex par. 2 lett. a)* anche il «consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1». L'esigenza del consenso *esplicito* ai fini della liceità del trattamento di tale tipologia di dati (peraltro solo allorché il divieto di cui al par. 1 non sia, per così dire, “rafforzato” dal diritto eurounitario o nazionale) rappresenta certo una delle più importanti deroghe al poc'anzi ricordato principio di libertà di forme.

Opportunamente, allora, le Linee Guida in esame affermano che la disciplina di cui all'articolo 9 si applica anche alla profilazione ed ai processi

trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio». Sul punto, cfr. anche Gruppo di Lavoro Articolo 29 per la protezione dei dati, parere 2/2010 sulla pubblicità comportamentale online, (WP 171).

decisionali automatizzati: e ciò non solo con riguardo ai dati raccolti presso l'interessato (*provided data*), bensì, e qui sta tutto il rilievo dell'inciso, anche ai «dati appartenenti a categorie particolari *derivati o desunti* da attività di profilazione»⁶⁸³. Con ciò, appunto, dimostrandosi ancora una volta la consapevolezza del fenomeno degli *algo-created data*, e segnatamente della scoperta di dati sensibili *by inference* anche a partire da altri set di dati, personali o meno⁶⁸⁴.

Il Gruppo insiste sul punto ricordando come «la profilazione può creare dati appartenenti a categorie particolari desumendoli da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati». Come esempio ipotetico, viene portata la circostanza per cui può essere possibile desumere lo stato di salute di una persona associando «le registrazioni dei suoi acquisti di alimenti a dati sulla qualità e sul contenuto energetico di tali alimenti». Altrettanto emblematico risulta, ad esempio, il caso tratto dalla realtà di uno studio che ha combinato i “Mi Piace” di Facebook con informazioni limitate tratte da sondaggi e ha rilevato che i ricercatori hanno predetto con precisione l'orientamento sessuale di un utente maschile nell'88 % dei casi, l'origine etnica di un utente nel 95 % dei casi e se un utente era cristiano o musulmano nell'82 % dei casi⁶⁸⁵.

Passando allora ad individuare, alla luce dell'esegesi sistematica delle disposizioni del Regolamento, le contromisure che il titolare sarebbe chiamato ad adottare, il Gruppo sostiene che laddove dalla profilazione siano dedotte

⁶⁸³ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 16.

⁶⁸⁴ V. *retro*, e cfr. ancora una volta per un riepilogo R. MESSINETTI, «Privacy e controllo dell'identità algoritmica», cit.

⁶⁸⁵ M. KOSINSKI, D. STILWELL, T. GRAEPEL, «Private traits and attributes are predictable from digital records of human behaviour», in *Atti della National Academy of Sciences degli Stati Uniti d'America*, <http://www.pnas.org/content/110/15/5802.full.pdf>.

preferenze e caratteristiche sensibili, il titolare del trattamento dovrebbe assicurarsi innanzitutto «che il trattamento non sia incompatibile con la finalità originaria», in forza dell'art. 6 par. 4; in seconda battuta «di aver individuato una base legittima per il trattamento di dati appartenenti a categorie particolari», ex art. 9 par. 2; e infine «di informare l'interessato sul trattamento», in conformità degli obblighi di informativa gravanti a suo carico ai sensi dell'art. 12⁶⁸⁶.

Requisiti più stringenti sono previsti ai fini della liceità di processi decisionali interamente automatizzati aventi ad oggetto categorie particolare di dati, sempre ai sensi dell'art. 22: verremo ad esaminarli in sede di commento della disposizione in questione.

Come ultimo punto della sua analisi delle disposizioni generali, il Gruppo dedica un paragrafo ai diritti dell'interessato, sottolineando come il Regolamento abbia ampliato questi ultimi e i corrispondenti doveri insistenti in capo ai titolari⁶⁸⁷. Il Gruppo specifica come essi, nel contesto della profilazione e più in generale dei trattamenti automatizzati (non ricadenti nella fattispecie di cui all'art. 22, rispetto alla quale come ormai sappiamo vige un regime diverso, che approfondiremo a breve), «questi diritti possono essere esercitati nei confronti del titolare del trattamento che crea il profilo e del titolare del trattamento che prende una decisione automatizzata su un interessato (con o senza intervento umano)».

Qui, ci soffermeremo brevemente solo su alcuni di essi, e segnatamente sul diritto di informazione (desumibile dagli artt. 13 e 14 del Reg.), sul diritto di accesso (ex art. 15) e sul fondamentale diritto di opposizione (ex art 21).

⁶⁸⁶ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 17.

⁶⁸⁷ Ivi, p. 17 ss.

Il Gruppo, nell'interpretare gli art. 13 e 14 che rispettivamente prescrivono gli obblighi di informazione gravanti sul titolare quando i dati personali siano raccolti presso l'interessato e quelli insistenti sul medesimo quando gli stessi siano raccolti presso terzi, li legge alla luce del principio di trasparenza poc'anzi descritto, rilevando come «il titolare del trattamento de[bba] spiegare in maniera chiara e semplice alle persone interessate come funziona la profilazione o il processo decisionale automatizzato». In particolare, a fronte della sussistenza di un trattamento che implichi un processo decisionale basato sulla profilazione, e indipendentemente dalla sussistenza di un'ipotesi ricadente nell'art. 22 (per la quale tali articoli, come vedremo, prevedono degli ulteriori e specifici obblighi), dagli art. 13 par. 1 lett. c) e dall'art. 14 par. 1 lett. c) sarebbe desumibile l'obbligo per il titolare di spiegare chiaramente all'interessato «il fatto che il trattamento avviene per finalità di profilazione e di adozione di decisioni basate sul profilo generato»⁶⁸⁸. La lettura in questione risulta corroborata dal *considerando* 60, che afferma come «fornire informazioni sulla profilazione fa parte degli obblighi di trasparenza del titolare del trattamento ai sensi dell'articolo 5, paragrafo 1, lettera a)».

Da tali elementi il gruppo inferisce l'esistenza, a fronte delle predette ipotesi, del corrispondente diritto per gli interessati di essere informati, ossia di ricevere le informazioni appena menzionate, *indipendentemente* dall'esistenza di un processo decisionale interamente automatizzato di cui all'art. 22 (che rappresenta, come meglio vedremo, l'unica fattispecie in relazione alla quale *esplicitamente* il legislatore, agli art. 13 par. 2 lett. f) e art. 14 par. 2 lett. g), ha

⁶⁸⁸ Ivi, p. 18. Sia l'art. 13 che l'art. 14, alle rispettive lettere c) del paragrafo 1, prevedono infatti che il titolare fornisca all'interessato «le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento». Per la lettura in questione, cfr. anche GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679* (WP 260), 28 novembre 2017 (in inglese) http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, Accesso effettuato il 18 dicembre 2017.

impone al titolare di informare l'interessato dell'esistenza del processo medesimo).

Il Gruppo passa allora ad esaminare il disposto dell'art. 15, fondamento normativo del c.d. diritto di accesso: nel contesto in esame (trattamenti automatizzati, profilazione e processi decisionali automatizzati di qualsiasi specie), esso si declina ad opinione del Gruppo nella pretesa giuridicamente tutelata in capo all'interessato ad «ottenere informazioni dettagliate sui dati personali utilizzati per la profilazione, ivi comprese le categorie di dati impiegati per creare un profilo»⁶⁸⁹. Inoltre, ai sensi del par. 3, il titolare a fronte della richiesta dell'interessato parrebbe dover, oltre alle informazioni generali, «rendere disponibili i *dati utilizzati come input per creare il profilo*, e consentire l'accesso alle informazioni sul profilo e ai dettagli dei segmenti nei quali l'interessato è stato inserito»: tale contenuto del diritto parrebbe distinguersi dall'innovativo diritto alla portabilità dei dati previsto dall'art. 20, che nel contesto in esame, e segnatamente in forza della lett. b) del par. 1, si declinerebbe nella pretesa dell'interessato ad ottenere dal titolare (e pertanto nel corrispondente obbligo in capo a quest'ultimo a fornire) la comunicazione dei dati forniti dall'interessato o osservati dal titolare del trattamento, e non già del profilo stesso⁶⁹⁰.

Aggiunge poi il Gruppo un rilievo importante con riguardo alla profilazione, ovverosia che il *considerando* 63 parrebbe offrire una certa

⁶⁸⁹ Ivi, p. 19.

⁶⁹⁰ V. il testo dell'art. 20, par. 1, Reg. UE 2016/679: «L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati».

protezione al titolare del trattamento nei confronti della divulgazione di segreti aziendali e della proprietà intellettuale: questo, infatti, afferma che il diritto di accesso «non dovrebbe ledere i diritti e le libertà altrui, *compreso il segreto industriale e aziendale e la proprietà intellettuale*, segnatamente i diritti d'autore che tutelano il software». Tuttavia, il *considerando* stesso si premura di specificare che tali considerazioni «non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni», non potendo dunque il titolare far affidamento sulla disciplina a protezione dei segreti industriali per ostacolare l'esercizio del diritto in parola⁶⁹¹.

Concludiamo la disamina delle disposizioni generali in materia di trattamenti automatizzati analizzando i rilievi svolti dal Gruppo intorno all'art. 21, base giuridica del *diritto di opposizione*, una delle situazioni giuridiche soggettive - in cui il diritto alla protezione dei dati personali si specifica agli artt. 15- 22 del GDPR - più rilevanti nella materia che qui ci occupa⁶⁹².

⁶⁹¹ Il *considerando* 63 specifica inoltre che «ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali». Ricordiamo che oggi l'atto normativo di riferimento in contesto europeo deputato ad armonizzare la disciplina degli Stati membri in materia di segreti industriali è la Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, OJ L 157, 15.6.2016, p. 1–18.

⁶⁹² Occorre subito riportare qui un estratto del testo della disposizione in esame, rubricata appunto «diritto di opposizione», comprensivo dei paragrafi più importanti ai nostri fini: «L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri *l'esistenza di motivi legittimi cogenti* per procedere al trattamento *che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato* oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. 2. *Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.* 3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento

Il Gruppo principia ricordando che ai sensi del par. 4 il titolare del trattamento deve portare *espressamente* all'attenzione dell'interessato informazioni dettagliate in merito al diritto di opposizione di cui all'articolo 21, paragrafi 1 e 2, e presentare tale diritto chiaramente e separatamente da qualsiasi altra informazione.

A questo punto, in prima battuta il Gruppo si sofferma sul contenuto del diritto configurato dai par. 1: questo sussiste in relazione ai trattamenti effettuati sulla base della lettera e) o f) del par. 1 dell'art. 6, e dunque laddove la base giuridica consista nella *necessità* del trattamento ai fini dell'*esecuzione di un compito di interesse pubblico* (o dell'esercizio di pubblici poteri di cui sia investito il titolare) o piuttosto *nel legittimo interesse* del titolare medesimo; e consiste appunto nella libertà riconosciuta all'interessato di opporsi ai trattamenti fondati su tali basi, *compresa naturalmente la profilazione*, «per motivi connessi alla sua situazione particolare»⁶⁹³.

Ebbene, conseguentemente all'esercizio da parte dell'interessato del diritto di opposizione, ai sensi dell'art. 18 par. 1 lett. d) il titolare dovrebbe allora interrompere, o evitare di iniziare, il trattamento medesimo (compreso dunque l'eventuale processo di profilazione), ed *ex art.* 17 par. 1 lett. c), se richiesto dall'interessato, dovrebbe cancellare i dati medesimi: ciò, tuttavia, come statuito dal medesimo par. 1 dell'articolo 21, a meno che il titolare non possa (e non riesca) a dimostrare *l'esistenza di motivi legittimi cogenti che prevalgono sugli*

per tali finalità. 4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.(...)».

⁶⁹³ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 20. Merita sottolineare che tra le ipotesi in cui il diritto in questione risulta riconosciuto all'interessato non figura il trattamento fondato sul consenso per il semplice fatto che in quest'ultimo caso lo stesso, come abbiamo visto, gode del sostanziale e ben più ampio diritto di revoca *ad libitum*, ex art. 7 par. 3 del GDPR.

interessi, sui diritti e sulle libertà dell'interessato (oppure, aggiunge il legislatore, «per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria»).

Il Regolamento, come sappiamo, non fornisce alcuna spiegazione dei motivi che potrebbero essere considerati «legittimi» e insieme «cogenti»: per entrambe le definizioni il rinvio è fatto al già citato Parere sui legittimi interessi, cui già abbiamo fatto poco fa riferimento⁶⁹⁴. Un esempio di motivo legittimo cogente portato dal Gruppo nelle Linee Guida in esame è il caso in cui la profilazione effettuata sia utile per la società in senso lato e non in funzione dei soli interessi economici o aziendali del soggetto anche privato che la compia, come nel caso del trattamento in questione condotto per individuare in anticipo la diffusione di malattie contagiose⁶⁹⁵.

In ogni caso, un'attenzione specifica è posta ancora una volta sulla ponderazione tra i concorrenti interessi (legittimi e cogenti) del titolare (a proseguire nel trattamento) e piuttosto la base dell'opposizione dell'interessato, che il Gruppo riconosce possa identificarsi in un motivo di natura tanto personale quanto professionale o sociale⁶⁹⁶. Se da una parte l'onere di dimostrare l'esistenza di diritti legittimi cogenti ricade (come si evince valorizzando il termine «dimostri» utilizzato al paragrafo 1 dell'articolo 21) sul titolare medesimo, dall'altra appare evidente che la ponderazione qui richiesta differisce da quella

⁶⁹⁴ Cfr. ancora una volta la spiegazione di «legittimità» in GRUPPO DI LAVORO ARTICOLO 29, *Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014. Pagine 28-31. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

⁶⁹⁵ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 20.

⁶⁹⁶ Ivi, p. 21, in cui il Gruppo innanzitutto specifica come il titolare, prima e allo stesso tempo ai fini della ponderazione in esame, debba «considerare l'importanza della profilazione per il proprio particolare obiettivo» e «considerare l'impatto della profilazione sugli interessi, sui diritti e sulle libertà dell'interessato, che *dovrebbe essere limitato al minimo necessario per conseguire l'obiettivo*».

che inizialmente, soprattutto ai sensi dell'art. 6 par. 1 lettera f), il titolare fosse tenuto a svolgere, poiché in tal caso ai fini della lecita prosecuzione del trattamento la norma richiede che il legittimo interesse addotto sia *cogente*, implicitamente prescrivendo che sia soddisfatta una soglia maggiore affinché tale interesse prevalga sulle opposizioni dell'interessato⁶⁹⁷.

A questo punto, Il Gruppo di Lavoro passa a considerare il par. 2 dell'articolo 21, che configura una garanzia ancora maggiore per l'interessato: esso, secondo l'interpretazione del Gruppo - sebbene tuttavia il dato letterale sembreri già esplicitarlo sufficientemente da sé - riconosce all'interessato un *diritto incondizionato* ad opporsi al trattamento dei suoi dati personali per finalità di *marketing diretto*, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto: e ciò dunque, verrebbe da aggiungere, indipendentemente dalla base giuridica su cui il trattamento si fondi (e dunque a prescindere dal fatto che la finalità in questione sia o meno assunta dal titolare quale legittimo interesse)⁶⁹⁸. Il Gruppo prosegue affermando che tale disposizione implichi come, a differenza della declinazione del (medesimo) diritto prevista al paragrafo 1, a fronte della fattispecie descritta «non sia necessario effettuare alcun bilanciamento degli interessi; *il titolare del trattamento deve rispettare le volontà dell'interessato senza mettere in discussione i motivi dell'opposizione*». A corroborare tale interpretazione interviene il *considerando* 70, che nel fornire ulteriore contesto a questo diritto afferma come lo stesso possa essere esercitato

⁶⁹⁷ *Ibidem*. V. anche il *considerando* 69, più netto nell'affermare come l'onere della prova circa la prevalenza degli interessi legittimi cogenti a fronte dell'opposizione dell'interessato, nel periodo in cui afferma che «è opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato».

⁶⁹⁸ *Ibidem*.

*in qualsiasi momento e gratuitamente*⁶⁹⁹. Bisogna rilevare, a titolo conclusivo, come il Gruppo stesso ritenga che dalla lettura in combinato disposto del *considerando* in questione e dell'art. 12 par. 2, che impone al titolare di agevolare l'esercizio dei diritti dell'interessato di cui all'art. 15-22, parrebbe desumibile l'opportunità che il titolare del trattamento (il quale raccolga dati personali dalle persone fisiche allo scopo di utilizzarli per finalità di marketing diretto), offra agli interessati *direttamente al momento della raccolta* un modo semplice per indicare che non desiderano che i loro dati personali siano utilizzati per finalità di marketing diretto (piuttosto che, dunque, attendere l'esercizio successivo del loro diritto di opposizione)⁷⁰⁰.

Terminato l'esame dei diritti configurati dagli artt. 15-21, e rilevanti in punto di trattamenti automatizzati di *qualsiasi specie*, il Gruppo passa, al capitolo IV delle Linee Guida, a trattare delle *disposizioni specifiche* in materia di processi decisionali interamente automatizzati, compresa la profilazione. Forti delle definizioni appena ripercorse, dei concetti appena richiamati, e di tutto quanto esaminato in precedenza, addentriamoci nell'analisi (in particolare) dell'art. 22, quale disposizione complessa e tuttavia centrale non solo nell'economia del Regolamento, bensì della stessa contemporanea società datificata.

⁶⁹⁹ Il *considerando* 70 recita infatti: «Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, *in qualsiasi momento e gratuitamente*, di opporsi a tale trattamento, con riguardo sia a quello iniziale che a quello ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere *esplicitamente portato all'attenzione dell'interessato* e presentato chiaramente e separatamente da qualsiasi altra informazione».

⁷⁰⁰ *Ibidem*, nota 31. V. art. 12, par. 2: «Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato».

3.2.3. Processi decisionali interamente automatizzati, compresa la profilazione: l'art. 22, par. 1 e i nodi interpretativi

Per cominciare, può essere utile riportare qui il testo dell'intera disposizione, che, lo si anticipa, analizzeremo paragrafo per paragrafo, ciascuno di essi introducendo una diversa "tessera" di quel mosaico che, come si ambisce a dimostrare, si articola in un divieto generale (par. 1), in parallelo al quale corre una serie circoscritta di eccezioni, tutte assai rilevanti (par. 2), ai fini della liceità delle quali il legislatore stesso pretende l'implementazione di determinate garanzie che si aggiungono agli obblighi previsti per il titolare e agli speculari diritti attribuiti all'interessato in relazione a tale fattispecie (par. 3; art. 13 par. 2 lett. f); art. 14 par. 2 lett. g); art. 15 par. 1 lett. e); art. 35 parr. 1 e 3 lett. a)); l'ultima tessera consistendo poi in una deroga parziale alla disciplina speciale così articolato, attraverso la configurazione di un diverso e ancor più garantista regime in relazione a quei processi decisionali che abbiano ad oggetto categorie particolari di dati (par. 4). L'intera disciplina dovrà essere letta alla luce dei *considerando* 71 e 72, che contengono alcune specificazioni dalla letteratura specialistica e dallo stesso Gruppo di Lavoro ritenute fondamentali in chiave esegetica⁷⁰¹.

⁷⁰¹ Per l'analisi che si condurrà nel presente paragrafo, si anticipa che fondamentali sono risultati, tra i molteplici rilevanti in materia e meritevoli di menzione e di consultazione (e oltre alle linee guida che continueremo ad esaminare e che rappresentano forse il più importante strumento esegetico fin ora a disposizione), i contributi seguenti: L. A. BYGRAVE, «Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making», in K. Yeung, M. Lodge (a cura di), *Algorithmic Regulation*, Oxford University Press, 2019; ID., I. MENDOZA, «The Right not to be Subject to Automated Decisions based on Profiling», in Tatiani Synodinou, Philippe Jougoux, Christiana Markou, Thalia Prastitou (eds.), *EU Internet Law: Regulation and Enforcement*, Springer, 2017; E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black-box society», cit.; R. MESSINETTI, «Privacy e controllo dell'identità algoritmica», cit.; F. KALTHEUNER, E. BIETTI, «Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR»; G. MALGIERI,

L'Articolo 22, rubricato «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione», così recita:

«1. L'interessato ha il *diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato*, compresa la profilazione, che *produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona* (corsivo nostro).

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul *consenso esplicito* dell'interessato [corsivo nostro].

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato».

Innanzitutto, è bene introdurre il discorso in materia principiando dai “fondamentali”, ovvero da alcuni dei prodromi normativi che già abbiamo

«Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit.

incontrato nel ripercorrere l'emersione del fenomeno dell'elaborazione automatica dei dati e l'evoluzione della relativa disciplina.

La prima norma che può rintracciarsi in contesto europeo, specificamente relativa alla fattispecie dei processi decisionali interamente automatizzati e portatrice di un *approccio restrittivo* interviene nell'ambito dell'ordinamento francese alla fine degli anni 70: l'ormai abrogato art. 2 della *Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, stabiliva infatti: «*Aucune décision de justice impliquant une appréciation sur en comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*»; e, in modo ancor più rilevante ai nostri fini, che «*Aucune décision administrative ou privée impliquant une appréciation sur en comportement humain ne peut avoir seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*». L'art. 3, poi, sanciva espressamente un diritto ad esprimere la propria opinione sulla decisione così adottata e conseguentemente a contestarla, segnatamente con riguardo al «*raisonnements utilisés*»: lungimirante assai, dunque, nel configurare alcune delle garanzie in termini di posizione giuridica soggettiva oggi parimenti consacrate nelle disposizioni del GDPR, sebbene in modo tanto generico da aver scaturito quel già accennato dibattito sulla sussistenza o meno di un *diritto alla spiegazione* della logica della *specifica* decisione adottata⁷⁰².

E tuttavia, come abbiamo già rilevato, la prima, autentica norma di carattere “paneuropeo”, in quanto adottata nel contesto di un atto comunitario, esplicitamente preordinata ad uniformare la disciplina vigente negli Stati membri

⁷⁰² V. infatti art. 3 *Loi n. 78-87*: «*Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés* ».

(e in alcuni casi, come l'Italia, ad introdurla proprio) in materia di decisioni *unicamente* basate su un trattamento automatizzato, dunque svolto interamente da una macchina, senza (o comunque, come vedremo meglio commentando l'art. 22, al più con un *non significativo*) coinvolgimento umano, si identifica nell'art. 15 della previgente Direttiva 95/46/CE ⁷⁰³. Nel virtuoso intento di rispondere in anticipo al poderoso sviluppo delle ICTs che veniva profilandosi, la norma in questione, rubricata «decisioni individuali automatizzate», prescriveva che ogni persona fisica godesse del *diritto* di «non essere sottoposta ad *una decisione che produca effetti* giuridici o abbia effetti *significativi* nei suoi confronti *fondata esclusivamente su un trattamento automatizzato* di dati destinati a *valutare taluni aspetti della sua personalità*, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.»⁷⁰⁴. Essa allora, come è evidente, limitava la sua portata applicativa a quelle sole decisioni *unicamente basate su una sola specie* di trattamento interamente automatizzato, ossia la profilazione: ma, come è stato notato, essa presentava la peculiarità di rivolgersi piuttosto al profilo decisionale che a quello del semplice *data processing*, ed affermava un principio inedito rispetto alle comuni *fair information practices* codificate dalla stessa Convenzione 108 del 1981: quello in forza del quale le valutazioni interamente

⁷⁰³ Cfr. L.A. BYGRAVE, «Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», cit.; L. A. BYGRAVE, I. MENDOZA, «The Right not to be Subject to Automated Decisions based on Profiling», cit., 77 e 78.

⁷⁰⁴ Cfr., esteso, l'art. 15, Dir. 95/46 CE: «1. Gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc. 2. Gli Stati membri dispongono, salve le altre disposizioni della presente direttiva, che una persona può essere sottoposta a una decisione di cui al paragrafo 1, qualora una tale decisione: a) sia presa nel contesto della conclusione o dell'esecuzione di un contratto, a condizione che la domanda relativa alla conclusione o all'esecuzione del contratto, presentata dalla persona interessata sia stata accolta, oppure che misure adeguate, fra le quali la possibilità di far valere il proprio punto di vista garantiscano la salvaguardia del suo interesse legittimo, oppure b) sia autorizzata da una legge che precisi i provvedimenti atti a salvaguardare un interesse legittimo della persona interessata.»

automatizzate del comportamento di una persona fisica non potessero costituire la sola base di decisioni destinate a “impingere” significativamente sulla sfera giuridica e ancor prima sulla sfera privata, e sugli attributi fondamentali, della persona medesima⁷⁰⁵.

E tuttavia, come già abbiamo notato, nonostante le felici peculiarità della norma e la virtuosa intenzione di rappresentare una norma generale sulla «distribuzione del potere di decisione nel mondo digitale»⁷⁰⁶, alcune sue caratteristiche hanno concorso a renderla, nella prassi dei rapporti giuridici, sostanzialmente *ineffettiva*; su tutti, la declinazione della disciplina secondo lo schema del diritto, piuttosto che del divieto generale, e l’ampia possibilità di deroga garantita dal secondo comma dell’art. 15. Com’è stato notato da attenta dottrina, infatti, escluso il doveroso recepimento ad opera delle legislazioni nazionali⁷⁰⁷, in punto di applicazione della disposizione pressoché marginale è stato il contenzioso davanti alle Corti e ai Garanti nazionali, se si esclude un emblematico caso deciso dal *Bundesgerichtshof* (Corte Suprema Federale tedesca)⁷⁰⁸; e non migliore sorte essa ha conosciuto in ambito comunitario, non

⁷⁰⁵ Cfr. L. A. BYGRAVE, I. MENDOZA, «The Right not to be Subject to Automated Decisions based on Profiling», cit; Id., *Data protection law: approaching its rationale, logic and limits*. Alphen aan den Rijn, Kluwer Law International, 2002, passim.

⁷⁰⁶ La citazione è di S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 328.

⁷⁰⁷ Cfr. ad esempio, per quanto attiene all’ordinamento italiano, il previgente art. 11 del D.lgs. 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali», oggi abrogato dal D.lgs. 10 agosto 2018, n. 101, recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” (in G.U. 4 settembre 2018 n.205).

⁷⁰⁸ Ci si riferisce al noto caso *SCHUFA*, deciso dal BGH, 28.1.2014, VI ZR 156/13, consultabile sul sito internet istituzionale del *Bundesgerichtshof* <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=66910&pos=0&anz=1>. La sentenza costituirà oggetto di sintetico commento nella parte in cui ci occuperemo della (esigua, ma fondamentale) giurisprudenza della CGUE maturata in ordine all’interpretazione e all’applicazione dell’attualmente vigente art. 22. Cfr. ancora L. A. BYGRAVE, «Minding the

essendo note pronunce della Corte di Giustizia dell'Unione europea che abbiano affrontato nello specifico la materia dei processi decisionali interamente automatizzati, occupandosi dell'interpretazione o della validità della disposizione medesima. La disposizione poi, oltre ad aver costituito oggetto d'interesse limitato da parte della dottrina, tanto da essere stata definita costitutiva di un «*second-classa data protection right*»⁷⁰⁹, è stata ignorata anche nel quadro degli *International Safe Harbor Privacy Principles*, elaborati fra il 1998 e il 2000, e poi confluiti in quel *Safe Harbour Agreement* tra Unione europea e Stati Uniti d'America che, come già abbiamo avuto modo di rilevare ampiamente in precedenza, è stato invalidato dalla Corte di Giustizia con la nota sentenza *Schrems I*; stessa sorta essa ha peraltro ricevuto (parimenti al *condendum* art. 22, nelle more dell'approvazione del GDPR) nel quadro del successivo *UE-EU Privacy Shield*, a sua volta invalidato nel 2020 con la sentenza *Schrems II*⁷¹⁰.

Il contesto tecnosociale, come ampiamente riferito, è tuttavia notevolmente mutato dall'entrata in vigore della Direttiva Madre ad oggi: lo sviluppo dell'ecosistema *Big Data*, accompagnato dai rapidi avanzamenti delle applicazioni di IA, ha infatti notevolmente contribuito a innalzare il livello di «vigilanza sugli algoritmi», espressione coniata per sottolineare l'opportunità di intensificare il controllo sulle conseguenze che i sistemi di IA sono in grado di

Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making», cit.

⁷⁰⁹ L. A. BYGRAVE, I. MENDOZA, «The Right not to be Subject to Automated Decisions based on Profiling», cit., p. 78.

⁷¹⁰ V. retro, par. 2.2.4, ma per un'analisi più approfondita cfr. ex multis M.D. SCOTT, Scott on Multimedia Law, IV ed., Wolters Kluwer, New York, 2019, 93 ss; S. SICA, V. D'ANTONIO, «Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles», in V. Zeno Zencovich e G. Resta (a cura di), *La protezione transnazionale dei dati personali: dai Safe Harbour Principles al "Privacy Shield"*, Roma Tre E-Press, Roma, 2016, 137 ss. Sul punto si tornerà in apertura del prossimo capitolo

produrre nella sfera giuridica dei soggetti interessati⁷¹¹. Tutto ciò ha condotto ad una riscrittura, e prima ancora ad un'implementazione, del sistema di garanzie apprestato a fronte della fattispecie di decisioni *unicamente* basate sul trattamento – puramente - automatizzato, e quindi sostanzialmente algoritmico, dei dati relativi alla persona fisica. Ed è da questo maturato contesto di preoccupazioni e di riflessioni che origina la lettera dell'art. 22 del GDPR.

È opportuno sottolineare che il cuore della disposizione previgente, e dunque il principio di cui abbiamo poc'anzi parlato, resta saldo nell'art. 22, sebbene appunto declinato in senso più ampio e circondato di ulteriori garanzie. Allo stesso tempo bisogna ricordare che una norma speculare a quella in questione è stata dal legislatore europeo inserita all'art. 11 della Direttiva 2016/680 sul *Data Protection and Law Enforcement*, a dimostrazione dell'ulteriore problematicità della questione delle decisioni interamente automatizzate nell'ambito dell'esercizio dei pubblici poteri, segnatamente per finalità di repressione dei reati (tale, appunto, da richiedere una disciplina derogatoria e più stringente rispetto a quella generale)⁷¹².

⁷¹¹ Cfr. sul punto le importanti riflessioni di due istituzioni cardine in materia di data protection: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Privacy e intelligenza artificiale: vigilare sugli algoritmi. Il contributo del Garante italiano nel Comitato consultivo della Convenzione 108*, Notiziario n. 451 del 25 marzo 2019, disponibile in <www.garanteprivacy.it> ; COMITATO CONSULTIVO DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108), *Guidelines on Artificial Intelligence and Data Protection*, (Starsburgo, 25 gennaio 2019, T-Pd(2019)01), 3.

⁷¹² V. art. 11 della già citata Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio; esso, prevedendo essenzialmente un divieto di decisioni simili e un più ristretto novero di deroghe, così recita: «1. Gli Stati membri dispongono che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato sia vietata salvo che sia autorizzata dal diritto

Venendo al merito dell'articolo 22 del GDPR, bisogna subito riscontrare che, dietro allo schema apparentemente semplice della norma, si cela un realtà un groviglio di questioni interpretative che corrono dal suo ambito di applicazione sino alla natura degli effetti prodotti dalla medesima: cominciando dal primo paragrafo (che il nucleo essenziale della disciplina contiene) e seguendo, ancora una volta, la struttura argomentativa fatta propria dal Gruppo di Lavoro nelle Linee Guida in esame, la cui interpretazione della disposizione in questione brilla per chiarezza ed esaustività (pur non essendo, come vedremo, pacificamente avallata dalla dottrina), ci soffermeremo nello specifico sul significato da attribuire all'espressione «diritto a non essere sottoposto» ad una decisione totalmente automatizzata; sul concetto stesso di «decisione basata *unicamente* su un trattamento automatizzato», e in particolare sulla soglia di coinvolgimento umano da raggiungersi o superarsi affinché la decisione *non* ricada nel perimetro applicativo della norma; e sul significato di «effetti giuridici» o di altri effetti che comunque «incidano in modo significativo» sulla persona fisica, scaturenti dalla decisione medesima.

A titolo ulteriormente preliminare, occorre considerare che, sebbene i lavori preparatori al GDPR contengano pochi riferimenti specifici alla disposizione medesima, è il *considerando* 71 a riservare un'attenzione privilegiata alla fattispecie in questione, in modo da riflettere le preoccupazioni che animavano le istituzioni europee nell'atto di predisporla. Tale *considerando*, quale prezioso ausilio interpretativo, è dunque più volte richiamato dallo stesso Gruppo nelle

dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento. 2. Le decisioni di cui al paragrafo 1 del presente articolo non si basano sulle categorie particolari di dati personali di cui all'articolo 10, a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato. 3. La profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 è vietata, conformemente al diritto dell'Unione».

linee Guida. In proposito, è opportuno evidenziare da subito come il suo dettato si soffermi in via principale sulla potenziale carenza di qualità di un processo decisionale interamente delegato alle macchine: il considerando, nello specifico, sottolinea a chiare lettere la speculare necessità per il titolare di adottare «misure statistiche e matematiche appropriate», nonché «misure tecniche e organizzative» strumentali al fine di «garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e [che] sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti».

Il preambolo, per mezzo del *considerando* in questione, sembra allora esprimere le stesse preoccupazioni della Commissione cristallizzate nei lavori preparatori della Direttiva 95/46/CE, che condussero appunto all'adozione del richiamato art. 15. In tali lavori traspariva innanzitutto la consapevolezza dell'indebolimento progressivo della capacità umana di esercitare una qualche influenza sui processi decisionali che la riguardassero, a fronte della crescente informatizzazione, e dunque automazione dei medesimi⁷¹³. E, in seconda battuta, emergeva anche l'ineludibile apprensione circa la potenziale deriva delle capacità

⁷¹³ Cfr. COMMISSIONE EUROPEA, *Explanatory text for Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*, COM (90) 314 final – SYN 287, p. 29. In essa lucidamente si legge: « *This provision is designed to protect the interest of the data subject in participating in the making of decisions which are of importance to him. The use of extensive data profiles of individuals by powerful public and private institutions deprives the individual of the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'.* »

di giudizio dell'essere umano, che, a fronte dell'automazione dei suddetti processi, potesse “dare per scontata” la validità (innanzitutto logica) della decisione medesima: con le parole della Commissione, «*the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities*»⁷¹⁴.

Bisogna, ancora, notare due aspetti. Anzitutto, come sottolineeremo anche più avanti, nonostante l'orientamento *dignty-oriented* espresso dal *considerando* 71, sulla scorta delle richiamate riflessioni, il testo finale dell'art. 22 non sembra tuttavia rispecchiare esattamente alcuna delle proposte avanzate dalla Commissione, dal Parlamento e dal Consiglio. Merita poi considerare che il rilievo assegnato alla profilazione - oltre che nell'impianto generale del Regolamento - nello stesso art. 22 (lo abbiamo già anticipato), in cui essa rappresenta l'unica *subspecie* di trattamento automatizzato esplicitamente citata, trova ulteriore conforto nel fatto che la Commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento Europeo avesse inizialmente avanzato la proposta (poi caduta in sede di emendamenti) di attribuire alla persona fisica il diritto di opporsi (o, piuttosto, di non essere proprio sottoposto) a *qualsiasi* trattamento di profilazione: e non solo dunque, come la norma oggi prevede, con riferimento esclusivo ad alcune specifiche tipologie di decisioni – distinte, in sintesi, sulla base dei loro *effetti* - basate *unicamente* su un trattamento automatizzato, *compresa* la profilazione⁷¹⁵. Tutte queste considerazioni vanno

⁷¹⁴ Cfr. COMMISSIONE EUROPEA, *Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (COM (92) 422 final – SYN 287).

⁷¹⁵ Cfr. PARLAMENTO EUROPEO, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))(A7- 0402/2013;

tenute bene a mente, ora che ci addentriamo nell'analisi della disciplina di cui all'art. 22.

La prima questione interpretativa di cui ci occupiamo, unitamente al Gruppo di Lavoro, è l'individuazione del significato dell'espressione «diritto di non essere sottoposto» ad una decisione basata unicamente su un trattamento – solo - automatizzato. Le Linee Guida, in proposito, manifestano pochi dubbi. Secondo l'organo consultivo, il termine “diritto” non significa che l'art. 22 par. 1 si applichi solo se invocato attivamente dall'interessato: la norma in parola, infatti, stabilisce un *divieto generale* in relazione ai processi decisionali interamente automatizzati (attenendoci, per ora, alla definizione in via generale delineata qualche pagina indietro), che opera *ex ante* ed *ipso iure*, «indipendentemente dal fatto che l'interessato intraprenda un'azione in merito al trattamento dei propri dati personali»; e, pertanto deve essere rispettato “di *default*” dai titolari del trattamento⁷¹⁶.

Il Gruppo prosegue sostenendo che tale interpretazione sia quella che meglio esprime i già analizzati principi che informano il Regolamento: su tutti, quello in cui si sintetizza la visione personalistica o *fundamental rights-oriented* che rappresenta una delle due anime del Regolamento (e forse, come abbiamo visto, la più forte) e che mira a preordinare l'intera disciplina della *data protection* alla massimizzazione del diritto fondamentale della persona fisica a mantenere il controllo sui propri dati, e dunque a conservare la propria *autodeterminazione*

PE501.927v05-00), 2013, p. 93. Cfr. anche, per tutta la ricognizione qui svolta, L. A. BYGRAVE, I. MENDOZA, «The Right not to be Subject to Automated Decisions based on Profiling», cit.

⁷¹⁶ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 21. Cfr. anche, per tale ricostruzione, E. Pellicchia, «Profilazione e decisioni automatizzate al tempo della black-box society», cit.

*informativa*⁷¹⁷. A suffragare tale lettura, vi sarebbe, innanzitutto, la “morfologia” complessiva della disposizione: in primis, laddove si interpretasse la disposizione medesima come fonte di un diritto di opposizione *ex post*, questo renderebbe superfluo il dettato del par. 2 lett. a), il quale ascrive tra i fondamenti di liceità del processo decisionale interamente automatizzato lo stesso *consenso esplicito* dell’interessato (non si può, infatti, contemporaneamente acconsentire e opporsi al trattamento: e il consenso trova già il suo contraltare nel diritto generale di revoca *ex art. 7 par. 3*; inoltre, esso finirebbe per configurarsi come *diritto all’intervento-coinvolgimento umano* nella decisione, con ciò rendendosi ridondante la stessa garanzia in questione imposta dal par. 3 a fronte delle eccezionali basi giuridiche di cui al par. 2 lett a) e lett. c)⁷¹⁸. In secondo luogo, a tale lettura concorre il fondamentale *considerando 71* nella parte in cui afferma che «tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell’Unione o degli Stati membri (...), o se è necessario per la conclusione o l’esecuzione di un contratto (...), o se l’interessato ha espresso il proprio consenso esplicito»: ciò, pertanto, implicando che il trattamento di cui all’art. 22 *non* sia consentito in generale.

⁷¹⁷ Cfr. per tale lettura anche MENDOZA-BYGRAVE, «The right non to be subjected», cit., che suffragando la ricostruzione della situazione in parole come divieto generale, affermano che « Such a result conforms better than the former result to the overarching aim of Art. 22 – and, indeed, of the Regulation more generally – to safeguard privacy and data protection as fundamental human rights in the face of technological and other developments».

⁷¹⁸ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 39, in cui l’organo svolge approfondimenti rispetto alla lettura offerta nel capitolo apposito del documento. Cfr. sempre Mendoza-Bygrave, «The right non to be subjected», cit. p. 87 che sottolineano come l’interpretazione della disposizione in termini di divieto inoltre preserva «l’operatività funzionale» della garanzia dello «human involvement» che costituisce un prerequisito per l’applicazione tanto dell’eccezione sub a) -consenso espresso dell’interessato- quanto per l’eccezione sub c) – necessità del trattamento per l’esecuzione di un contratto o di una misura precontrattuale, di cui al par. 3 art. 22.

Come abbiamo detto, tale lettura non trova pacifico riscontro in dottrina: è stato notato come un'interpretazione della situazione in esame in termini di diritto da esercitarsi *ex post* ad opera dell'interessato sia più aderente al dato letterale della disposizione, nonché alla circostanza che le norme che precedono, nel fare riferimento al novero dei diritti dell'interessato, indichino le disposizioni che corrono dall'art. 15 all'art. 22 medesimo⁷¹⁹; ed è stato anche evidenziato come la norma si adeguerebbe meglio alla realtà dei rapporti economici e giuridici, contrassegnata già ampiamente dall'uso di sistemi decisionali automatizzati tanto nel settore pubblico quanto nel settore privato, stante l'ormai avanzata digitalizzazione di entrambi (l'interpretazione in termini di divieto, insomma, vanificherebbe in partenza l'efficacia precettiva della norma)⁷²⁰. Tuttavia, alla luce delle considerazioni di cui sopra, soltanto un'interpretazione dell'articolo in termini di divieto *ex ante* pare concordare *interamente* tanto con i principi che informano l'impianto del Regolamento quanto con la struttura e il disposto *generali* della norma, orientati a massimizzare la tutela del diritto alla protezione dei dati personali dell'individuo. È, pertanto, a tale tesi che pare preferibile aderire.

Il divieto generale, in ogni caso, si applica solo nelle circostanze specifiche evidenziate dalla norma, e trova puntuali – e tassative - deroghe, e dunque fondamenti eccezionali di liceità, nelle situazioni tipicizzate al par. 2: cosicché il Gruppo può in prima istanza concludere affermando che l'art. 22, nel suo complesso, prevede un *divieto generale* all'adozione di decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che

⁷¹⁹ Cfr. ad es. L. A. BYGRAVE, «Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making», cit.

⁷²⁰ Cfr. In particolare EDWARDS, VEALE, «Slave to the Algorithm: Why a “Right to an Explanation” is Probably not the Remedy You are Looking for», 16 (1), in *Duke Law & Technology Review*, 2017, 18-84.

riguardino una persona fisica; ma tali decisioni sono *solo e soltanto* quelle che « hanno un effetto giuridico o che incidono in modo analogo significativamente» sulla persona medesima; la disposizione prevede, al contempo, determinate eccezioni alla regola (par. 2); e prescrive che, laddove ricorra una delle eccezioni medesime, siano « adottate misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato»⁷²¹. In prima approssimazione, le garanzie in questione comprendono il dovere a carico dei titolari di fornire, e il corrispondente diritto degli interessati ad ottenere, informazioni specifiche e significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste per l'interessato, ai sensi degli art. 13 par. 2 lett. f), art. 14 par. 2 lett. g), art. 15 par. 1 lett. e), e il diritto a contestare la decisione e ad ottenere l'intervento umano di cui al par. 3 dello stesso art. 22; inoltre, l'art. 35 impone al titolare di svolgere la già esaminata valutazione d'impatto sulla protezione dei dati laddove ritenga che il trattamento stesso configuri rischi elevati per i diritti e le libertà fondamentali dell'interessato, nonché nelle situazioni tipicizzate dal par. 3. Sulle garanzie in parola ci soffermeremo più avanti.

Ora, è necessario concentrarci sugli altri nodi interpretativi che abbiamo accennato, dai quali essenzialmente dipende la portata applicativa del divieto che, aderendo alla lettura proposta dal Gruppo, il par. 1 sembra senza dubbio configurare.

La seconda questione interpretativa che abbiamo introdotto appare forse, ai fini della delimitazione dell'ambito applicativo della disposizione, la più essenziale: ci riferiamo alla determinazione del concetto di «decisione basata

⁷²¹ Ulteriore supporto esegetico è fornito dal *considerando* 71 nella parte in cui afferma che afferma che tale trattamento dovrebbe essere «subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione».

unicamente sul trattamento automatizzato», che ampio ed aspro dibattito ha scaturito in dottrina. Come è stato notato, «è infatti su tale nozione che si plasma l'estensione del divieto, che è poi – a cascata – anche il terreno nel quale operano le eccezioni (subordinate a precisi presupposti) e le conseguenti salvaguardie che rafforzano comunque la protezione dell'interessato, anche quando l'operatività del divieto generale è inibita»⁷²².

È bene introdurci all'argomento ricordando che sull'estensione del concetto medesimo il dibattito ha interessato le stesse istituzioni europee in sede di discussione della proposta di Regolamento: in particolare, il Parlamento Europeo aveva emendato, in prima lettura, il testo del Regolamento proposto dalla Commissione europea, prevedendo all'art. 20 (rubricato in origine «Misure basate sulla profilazione»), che la profilazione idonea a produrre effetti giuridici sull'interessato o a incidere sui suoi interessi, diritti e libertà *non* potesse essere basata «unicamente o in modo predominante» sul trattamento automatizzato, bensì che dovesse includere obbligatoriamente «una valutazione umana, compresa una *spiegazione della decisione* conseguita dopo tale valutazione»⁷²³.

⁷²² Cfr. E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black box society», cit.

⁷²³ Cfr. PARLAMENTO EUROPEO, *Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)); in particolare, v. art. 20, par. 5, che in seguito agli emendamenti apportati recitava: «La profilazione avente come conseguenza misure che producono effetti giuridici sull'interessato o che, parimenti, incide significativamente sugli interessi, sui diritti o sulle libertà dello stesso non si basa unicamente o in modo predominante sul trattamento automatizzato e include una valutazione umana, compresa una spiegazione della decisione conseguita dopo tale valutazione. Le misure adeguate a salvaguardia dei legittimi interessi dell'interessato di cui al paragrafo 2 includono il diritto di ottenere una valutazione umana e una spiegazione della decisione conseguita dopo tale valutazione». In generale, bisogna ulteriormente ribadire che lo stesso art. 20 nella sua interezza risulta eloquentemente sintomatico di quella originaria tendenza, già ricordata, della Commissione sulle libertà civili del Parlamento Europeo a focalizzare l'attenzione sulla profilazione, quale *species* di trattamento automatizzato potenzialmente più incidente in senso pregiudizievole sulla libertà di autodeterminazione della persona fisica.

Risulta dunque evidente come nella versione non definitiva del Regolamento, e in particolare secondo l'indirizzo politico al tempo dominante in senso al Parlamento Europeo, ad essere vietata risultasse non solo la decisione basata *unicamente* sul trattamento automatizzato, come oggi recita l'art. 22, bensì qualsiasi decisione in cui l'apporto umano risultasse comunque *minore* rispetto all'impiego dei sistemi automatizzati. Inoltre (ma sul punto si tornerà più avanti), era esplicitamente accordato agli interessati uno specifico «diritto di ottenere una valutazione umana e una spiegazione della decisione conseguita *dopo*» il trattamento automatizzato: diritto che – nel testo poi approvato del Regolamento e oggi vigente – è stato limitato al «diritto di ottenere l'intervento umano» (art. 22 par. 3) e al diritto di accedere ad «informazioni significative sulla logica utilizzata» nell'ambito di un processo decisionale automatizzato (art. 15, 1o comma, lett h))⁷²⁴.

A fronte della definitiva lettera dell'art. 22, il dilemma principale attiene pertanto al significato - agli effetti della norma - dell'espressione «basate unicamente». Compito non facile per l'interprete, ma che appare necessario assolvere.

Parte della dottrina, pur con lo scopo di evidenziare in senso critico le carenze che il Regolamento europeo manifesterebbe in termini di tutela dell'interesse fondamentale alla protezione dei dati personali e più in generale della sfera privata, ha ritenuto che l'avverbio «unicamente» potrebbe consentire di sottrarre all'ambito di applicazione del divieto tutte quelle decisioni in cui l'intervento umano fosse presente anche solo in misura minima,

⁷²⁴ Cfr. sul G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit.; G. FINOCCHIARO, «Intelligenza artificiale e protezione dei dati personali», cit. p. 1675 ss.

indipendentemente dalla fase del processo decisionale in cui si iscriva⁷²⁵. Ed altra parte della dottrina, pur senza giungere a tali drastiche conclusioni, pone il dubbio se per soddisfare il requisito predetto sia necessariamente richiesto che anche la raccolta delle informazioni utilizzata nel quadro del processo decisionale sia automatizzata (ad esempio perché compiuta da c.d. *data sensors*)⁷²⁶.

L'interpretazione in questione, fortemente limitativa dei diritti e delle libertà fondamentali dell'interessato nel contesto della *data protection*, è stata invece respinta da altra parte della dottrina, che ha proposto di accogliere una nozione *relativa* dell'avverbio in parola, la quale impone, ai fini dell'esclusione dell'operatività del divieto in esame e dunque affinché la decisione non sia qualificabile come totalmente automatizzata, che il coinvolgimento umano nell'ambito del processo decisionale risulti *significativo*, ossia tale da incidere *effettivamente* sul contenuto della decisione finale e da non limitarsi pertanto al passivo recepimento (e contestualmente all'acritica esecuzione) delle *raccomandazioni* che costituiscono l'*output* del prodromico trattamento algoritmico⁷²⁷. A tale scopo, l'opzione interpretativa fa leva sulla formulazione

⁷²⁵ Cfr. In particolare S. WACHTER, B. MITTELSTADT, L. FLORIDI; «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», cit., p. 17, in cui gli autori affermano « While the required level of human involvement is not clear in practice, the phrase ‘solely’ suggests even some nominal human involvement may be sufficient»; e ancora « Decisions based predominantly on automated processes, but with nominal human involvement, would thus not invoke Article 15(1)h (right of access) or Article 22(3) (safeguards against automated decision-making) (...)». Cfr. anche MIREILLE HILDEBRANDT, “The Dawn of a Critical Transparency Right for the Profiling Era” (2012), *Digital Enlightenment Yearbook*, (IOS Press 2012), 41-56, 50

⁷²⁶ Cfr. a: D.W. SCHATUM, «Personvernforordningen og helt automatiserte avgjørelser innen forvaltningsretten», 134(2) *Lov&Data* (2018) 4–7.

⁷²⁷ Cfr. in particolare G. MALGIERI, G. COMANDÈ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 13 ss., in cui gli stessi autori rinviando al contributo di Lee A. Bygrave, «Automated Profiling – Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», cit. Essi affermano infatti che « According to Bygrave, decisions “formally attributed to humans”, but originating ‘from an automated data-processing operation the result of which is not actively assessed by either that person or other persons before being formalized as a decision,’ would be included in the scope of ‘automated decision-making’ ».

letterale della disposizione in esame, valorizzando la dizione «decisioni *basate* unicamente» («*based solely*») sul trattamento automatizzato: l'inciso in questione implicherebbe che a ricadere nell'ambito di operatività del divieto siano non solo i processi in cui il sistema algoritmico assolva tanto al *data processing* quanto al *decision making*; ma *anche* tutte quelle decisioni la cui fase preparatoria risulti completamente automatizzata e in cui il contributo umano intervenga soltanto nella fase finale e quale *mero strumento di attuazione* della prima, il cui contenuto risulti algebricamente prestabilito⁷²⁸. La lettura in questione è incardinata, insomma, sulla prospettiva per cui, per potersi qualificare come *effettivamente umano*, il contributo di una persona fisica dovrebbe determinare l'impiego di *sensibilità critica* e di *capacità di giudizio*: solo così potrebbe prevenirsi una irragionevole discriminazione tra sistemi decisionali in cui l'intera filiera risulti automatizzata ed altri in cui l'intervento umano si limiti a tradurre un punteggio in una risposta, applicando (soltanto) la regola algebricamente prodotta⁷²⁹.

Ebbene, quest'ultima interpretazione è proprio quella fatta propria dal Gruppo di Lavoro nelle sue Linee Guida. L'organo consultivo, infatti, limpidamente afferma come il titolare del trattamento non possa eludere le disposizioni dell'art. 22 «creando coinvolgimenti umani fittizi» («*by fabricating*

⁷²⁸ Ivi, p. 14. Con le parole degli autori: « *even from a literal interpretation of Article 22(1), we observe that the scope is not limited to 'solely automated decision-making' but it mentions (human or machine) decisions that are 'based' solely on automated decision-making. We argue that the expression 'based solely on automated processing' refers to all decision-making where preparatory evidence and discretionary judgements (e.g. scoring) are fully based on automated means*». Quindi, concludono gli autori: « *even though a nominal human intervention formally 'takes' the decision, Article 22(1) still applies*».

⁷²⁹ Ivi, p. 15. Gli autori aggiungono che «At the same time, only this more systemic interpretation would be able to cover the full scope of Article 22 as described at recital 71: 'in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements'. These are all fields where scoring techniques are generally employed and where human intervention often occurs but is usually only nominal». Cfr. anche sul punto DANIELLE KEATS CITRON, AND FRANK A. PASQUALE, 'The Scored Society: Due Process for Automated Predictions' (2014), *Washington Law Review*, Vol. 89, 2014, p. 1.

human involvement» è l'espressione adottata nell'originale inglese): per aversi un coinvolgimento realmente qualificabile come umano, il titolare del trattamento «deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico», e che questo sia svolto da una persona che «dispone dell'autorità e della competenza per modificare la decisione»⁷³⁰. Non formale attribuzione della decisione ad un essere umano; piuttosto, contributo che effettivamente influisca sul contenuto della decisione, e risulti dall'impiego delle umane facoltà razionali⁷³¹.

Pertanto, secondo l'esempio portato dallo stesso Gruppo, risulta chiaramente qualificabile come decisione basata unicamente sul trattamento automatizzato - ricadendo dunque nel perimetro applicativo del divieto di cui all'art. 22 par. 1 - la fattispecie in cui « qualcuno applic[chi] abitualmente profili generati automaticamente a persone fisiche senza avere alcuna influenza effettiva sul risultato ».⁷³² È il caso, ad esempio, assai attuale dei c.d. *scoring mechanisms*, diffusamente impiegati da banche, istituti finanziari ed assicurazioni e basati su un sistema algoritmico che effettua valutazioni automatizzate in relazione ai loro potenziali clienti assegnandogli un punteggio in termini di affidabilità, solvibilità e qualità simili: punteggi che i suddetti soggetti, nella quasi totalità dei casi, si limitano poi ad applicare passivamente ai rapporti con i clienti medesimi, ad esempio definendo su tale base i termini dei contratti standard (essenzialmente

⁷³⁰ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 23. Il Gruppo sottolinea che, a tale scopo, opportuno risulterebbe che nel quadro della valutazione d'impatto di cui all'art. 35 il titolare del trattamento individui e registri «il grado di coinvolgimento umano nel processo decisionale e la fase nella quale quest'ultimo ha luogo».

⁷³¹ Cfr. sul punto anche T. Zarsky, «Transparent predictions», cit., che fa riferimento al concetto di «*human discretion*».

⁷³² GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 23

“B2C”) predisposti per questi ultimi⁷³³. Sul tema, e in particolare sul fenomeno dell’*credit scoring* algoritmico, torneremo più avanti, in sede di commento della fondamentale, assai recente sentenza della Corte di Giustizia sul caso *SCHUFA*.

La terza ed ultima questione interpretativa in relazione al divieto generale di cui al par. 1 attiene all’espressione «[decisione] che produca effetti giuridici che lo [ovvero, l’interessato] riguardano o incida in modo analogo significativamente sulla sua persona [ovvero, sulla persona dell’interessato]»: questione oltremodo rilevante, poiché precisa in via ulteriore l’ambito di applicazione del divieto in esame. Come puntualmente rilevato dalle Linee Guida, il Regolamento, pur riconoscendo che il processo decisionale interamente automatizzato può avere «gravi conseguenze per le persone fisiche», non reca una precisa definizione né dei concetti evocati dalla prima proposizione subordinata relativa, «[decisione] che produca effetti giuridici che lo riguardano»; né dei concetti posti dalla subordinata relativa coordinata alla prima, «o [che] incida in modo analogo significativamente sulla sua persona». E tuttavia, la formulazione dell’art. 22 pare chiarire che rientrano nel proprio alveo applicativo «*soltanto gli effetti che hanno un impatto grave*»⁷³⁴. Questa, secondo il Gruppo, dovrebbe essere la bussola che orienti l’interprete nella ricostruzione dei medesimi

⁷³³ Ne parlano ancora una volta G. MALGIERI, G. COMANDÈ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 13; rilevante assai il seguente periodo: «*After a score is assigned, companies usually take a passive ‘human’ decision, applying specific conditions (or denying services) for each specific score, according to pre-set guidelines*». Sul più specifico tema degli scoring systems, cfr. ex multis BRENDA REDDIX-SMALLS, «Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market», (2011) 12 U.C. Davis Bus. L.J. 87, 117-18; e, ancora una volta, FRANK PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, cit., in part. Pp. 98 and 196.

⁷³⁴ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 23. Nell’originale inglese le espressioni utilizzate sono “*legal effects*” e “*similarly significant effects*”.

significati. E però, come vedremo subito, l'interpretazione delle formule in questione non è affatto pacifica in letteratura.

Cominciamo dalla prima delle due formule. Già l'art. 15 della dir. 95/46/CE, come abbiamo visto, faceva riferimento ai c.d. «*legal effects*», e a fronte dei numerosi contrasti esegetici sul punto la lettura più convincente deve forse identificarsi in quella che ravvisava effetti di tal sorta, dunque in senso proprio *giuridici*, in ogni conseguenza (riconducibile causalmente alla decisione) incidente sui diritti e sui doveri dell'interessato⁷³⁵. Le Linee Guida in esame sembrano accogliere proprio l'interpretazione in parola, laddove si afferma che «un effetto giuridico richiede che la decisione, basata unicamente su un trattamento automatico, incida sui diritti giuridici di una persona», come ad esempio la libertà di associarsi ad altre persone o di votare nel contesto di un'elezione: il riferimento parrebbe dunque essere ai diritti soggettivi assoluti, e in primo luogo a quelli costituzionalmente fondati. Ma lo stesso documento subito aggiunge che «un effetto giuridico può altresì essere qualcosa che influisce sullo status giuridico di una persona o sui suoi diritti ai sensi di un contratto»: così ricomprendendosi nell'alveo semantico della formula un ampio ventaglio di posizioni giuridiche, che corrono appunto dallo status sino al diritto soggettivo relativo. Gli esempi portati, a tale ultimo scopo, sono dei più vari: annullamento di un contratto, concessione o rifiuto di una particolare prestazione sociale

⁷³⁵ Cfr. L.A. BYGRAVE, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, cit.; con le parole dell'autore, «These are effects that are able to alter or determine (in part or in full) a person's legal rights or duties». V. anche S. WACHTER, B. MITTELSTADT, L. FLORIDI; 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', cit., p. 34, che nel novero espressamente ricomprendono «civil procedural rights and administrative law rights».

prevista dalla legge (come, ad esempio, contributi familiari o assegnazione di un alloggio), rifiuto dell'ammissione in un paese, diniego di cittadinanza⁷³⁶.

La dottrina più recente specifica e rafforza ulteriormente la lettura promossa dal Gruppo, nella misura in cui afferma che la previsione ambirebbe a qualificare come effetto giuridico « *any influence on human rights or constitutional rights of individuals* », così da coprire ogni potenziale limitazione a diritti fondamentali quali il diritto alla salute, il diritto di libertà di manifestazione del pensiero, e in definitiva la libertà personale. A tal proposito, si fa richiamo a quella visione sistematica che identifica una violazione dei diritti umani, in senso lato, in qualsiasi prevedibile minaccia a quegli attributi fondamentali della personalità più vulnerabili (*human vulnerabilities*): tale visione consentirebbe allora di estendere il perimetro dell'art. 22 fino ad ascrivervi « *a larger set of vulnerability than those already provided for by specific statutory provisions* »⁷³⁷.

A questo punto, ci si può occupare della formula che pare svolgere la funzione di allargare, già a partire dalla sua lettera, il margine di operatività del divieto generale di *solely automated decision making* disegnato dal par. 1 dell'art. 22: l'espressione « [decisione che] incida in modo analogo significativamente » sulla persona dell'interessato. A tal proposito, le Linee Guida specificano che un processo decisionale interamente automatizzato, nel senso sopra descritto, può comunque rientrare nell'ambito di applicazione dell'art. 22 se produce un « effetto *equivalente* o in modo analogo significativo *in termini di impatto* »: aggiungendo immediatamente che, affinché una decisione soddisfi il requisito menzionato, le

⁷³⁶ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 23.

⁷³⁷ G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 252 ss., che rinviano, per quanto attiene ai più recenti contributi inerenti al più specifico ambito dei diritti di “ultima generazione”, a MARCELLO IENCA AND ROBERTO ADORNO, «Towards new human rights in the age of neuroscience and neurotechnology», (2017) in *Life Sciences, Society and Policy*, vol. 13, issue n. 5, 8-9.

conseguenze che ne scaturiscono, anche laddove non producano «alcun cambiamento nei suoi [ovvero dell'interessato] diritti od obblighi giuridici [rectius *legali*]», comunque producano in capo all'interessato «*ripercussioni sufficienti* da richiedere le protezioni previste da questa disposizione»⁷³⁸. A suffragio della lettura, che sottolinea l'importanza dell'*equivalenza* in termini di effetti prodotti dal processo decisionale automatizzato, il cui riflesso pregiudizievole insista tanto nella sfera materiale quanto nella sfera immateriale del soggetto⁷³⁹, il Gruppo sottolinea come il Regolamento introduca l'espressione «in modo analogo», che va ad aggiungersi alla formula «incida significativamente» già presente nella lettera dell'art. 15 della dir. 95/46/CE. Ciò, secondo l'organo consultivo, vuol dire che il legislatore ha inteso *restringere* le aperture consentite dal concetto in parola, cosicché «la soglia per l'*importanza* deve essere *analogo* a quella di una decisione che produce un effetto giuridico». Inoltre, il *considerando* 71 offre alcuni esempi tipici che sembrerebbero evidenziare i contorni di tale soglia di importanza: sarebbero decisioni che incidono in modo analogo significativamente sulla persona «il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». La dottrina, poi, sottolinea come lo stesso *considerando* già provveda ad individuare un ampio elenco, chiaramente non esaustivo, degli interessi la potenziale compromissione dei quali renda la decisione che su di essi incide soggetta al divieto di cui all'art. 22: e ciò laddove, individuando la finalità della profilazione – unica specie di trattamento automatizzato esplicitamente considerata dall'articolo 22 – nella valutazione (analisi o previsione) di aspetti

⁷³⁸ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 24

⁷³⁹ Per la qualificazione dei suddetti come both *material and immaterial effects*, cfr. già per quanto atteneva alla lettera dell' Art. 15 della dir. 95/46/CE L.A. BYGRAVE, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, cit.

personali concernenti la persona fisica, specifica che tali aspetti possono riguardare «il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato»⁷⁴⁰.

Merita tuttavia sottolineare che le Linee Guida si spingono oltre, nella misura in cui tentano di individuare già astrattamente – ma al contempo con una chiara proiezione applicativa - le categorie di processo decisionale che soddisfino il requisito in parola, ovvero quello di incidere in modo significativo sulla (*rectius*, sugli interessi della) persona dell'interessato: processi accomunati dal fatto che, o per la tipologia di elaborazione dei dati, o per gli *output* decisionali che ne scaturiscono, anche alla luce delle indicazioni fornite dal *considerando* suddetto, producano effetti «*sufficientemente rilevanti o importanti da meritare attenzione*». La decisione, allora, deve essere in grado, alternativamente, di influenzare significativamente le circostanze, il comportamento o le scelte delle persone interessate; avere un impatto prolungato o permanente sull'interessato; o, nella sua forma più estrema, portare all'esclusione o alla discriminazione delle persone⁷⁴¹.

⁷⁴⁰ Cfr., G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 253, in particolare laddove, nel commentare il considerando in parola, notano che « '*performance at work*', '*economic situation*' and '*reliability*' reflect the two most relevant cases, i.e. refusal of a credit application or recruiting practices », e allo stesso tempo che « *the reference to 'personal preferences or interests (...) or behaviour' seems to lead to behavioural advertisements, neuromarketing and price discrimination* ».

⁷⁴¹ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 24, che tra gli esempi attinti dalla realtà dei rapporti socioeconomici più idonei a soddisfare la soglia in questione individua le decisioni che influenzino la situazione finanziaria dei soggetti, come la loro idoneità al credito; quelle da cui dipenda l'accesso ai servizi sanitari o ad un'opportunità di impiego; e, non ultime, quelle che si ripercuotano sull'accesso all'istruzione, ad esempio l'assegnazione di alloggi universitari. Cfr. anche S. WACHTER, B. MITTELSTADT, L. FLORIDI; «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», cit., che a p. 34 si soffermano proprio sull'esempio del job recruitment, sottolineando che, sebbene alcun

Il Gruppo non nasconde la difficoltà di individuare in concreto *quali* decisioni automatizzate (o, più specificamente, quali sistemi decisionali automatizzati) siano idonee a soddisfare la soglia d'importanza richiesta dall'art. 22 con tale residuale formula, alla luce dell'interpretazione promossa dall'organo medesimo. Tra gli esempi riportati, una certa attenzione sembra riservata ai processi decisionali automatizzati che si traducono in una tariffazione differenziata basata su dati personali o caratteristiche personali, come accade ad esempio nel *dynamic pricing*: operazioni di questo tipo, infatti, potrebbero avere un «effetto similmente significativo» se, ad esempio, prezzi proibitivi elevati impediscano l'accesso a determinati beni o servizi⁷⁴².

Occorre tuttavia rilevare che le Linee Guida dedicano un'attenzione privilegiata al settore della pubblicità online, che sempre più appare basarsi su strumenti automatizzati e implicare dunque decisioni basate *unicamente* sul trattamento automatizzato (nel senso sopra descritto), e specialmente, come ormai ben sappiamo, sulla profilazione. Il Gruppo di Lavoro in primo luogo sottolinea come, data la trasversalità del fenomeno, rilevanti in materia potrebbero essere, oltre alle disposizioni generale del GDPR e alle prescrizioni più specifiche dedicate al rapporto tra minori e profilazione⁷⁴³, le disposizioni recate dalla

ordinamento garantisca un generico “diritto ad essere assunti”, tuttavia « *there is a legitimate interest to be assessed loyally, fairly and not to be discriminated during recruitment*».

⁷⁴² Ivi, p. 25. Sul fenomeno del *dynamic pricing*, cfr. ex multis R.M. WEISS & A.K. MEHROTRA, *Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce*, 6 *Va. J.L. & Tech.*, 11 (2011), passim.

⁷⁴³ A queste ultime il Gruppo di Lavoro dedica una sezione conclusiva delle Linee Guida che stiamo esaminando, ivi riscontrando che, pur non sussistendo nell'articolato alcuna disposizione rilevante sul tema, dal combinato disposto tra l'articolo 22 (e le altre disposizioni del subsistema normativo in esame) e alcuni *considerando* possono desumersi attraverso un'esegesi teleologica norme che dettano requisiti più stringenti. In proposito, sono rilevanti gli incisi in cui il Gruppo «raccomanda al titolare del trattamento di *non* fare affidamento, di norma, sulle eccezioni di cui all'articolo 22, paragrafo 2, per giustificare» il processo decisionale interamente automatizzato, che la profilazione (ma non solo) coinvolga nella fase dell'elaborazione dei dati; e quello in cui afferma che «dato che i minori rappresentano un gruppo più vulnerabile della società, le organizzazioni dovrebbero, in generale, astenersi dal profilarli per finalità di marketing», aggiungendo che «i minori possono essere particolarmente

proposta di regolamento sulla vita privata e le comunicazioni elettroniche attualmente in discussione in seno alle istituzioni europee. Poi, nonostante l'organo consultivo resti cauto e osservi che in numerosi casi tipici la decisione di proporre pubblicità mirata basata sulla profilazione «*non* inciderà in modo analogo significativamente sulle persone» (l'esempio portato è quello di una pubblicità per un outlet di moda online basato su un semplice profilo demografico), esso non si esime dal constatare come il fenomeno in questione, e segnatamente la pubblicità mirata, possa avere un impatto significativo sugli interessi e sugli *attributi materiali o immateriali* della persona, così da integrare i requisiti della decisione che «incida in modo analogo significativamente» sul soggetto. A rilevare sono le caratteristiche del caso di specie, tra le quali il Gruppo di Lavoro lucidamente annovera, ad esempio, l'invadenza del processo di profilazione (compreso il tracciamento delle persone su diversi siti Web, dispositivi e servizi), il condizionamento delle aspettative e dei desideri delle persone interessate, il modo in cui l'annuncio viene inviato e la consapevolezza (e lo sfruttamento) delle vulnerabilità dei soggetti interessati⁷⁴⁴.

A tal proposito, la dottrina risulta ancor più netta nel riconoscere che il *cybermarketing*, e in particolare il fenomeno dell'*online behavioural advertising*, ricada tra i processi idonei a produrre un impatto – altamente - significativo (e dunque equivalente ad un effetto giuridico nel senso sopra precisato) sulla sfera

vulnerabili nell'ambiente online e più facilmente influenzabili dalla pubblicità comportamentale». Oltre al *considerando* 71, sul punto a rilevare è soprattutto il *considerando* 38, laddove recita: «i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere *meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate* nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore». GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 31 ss.

⁷⁴⁴ Ivi, p. 24 ss.

d'interessi della persona fisica, poiché questa sfrutterebbe i «*consumers' biases*»⁷⁴⁵. Secondo tale orientamento, seppur non sia giuridicamente riconosciuto all'individuo un diritto in senso stretto a non ricevere in assoluto annunci pubblicitari personalizzati (*personalized advertisements*), nondimeno sussiste, e risulta meritevole di protezione, un legittimo interesse della persona fisica a non essere vittima di pratiche commerciali scorrette, quali ad esempio quelle di *weblining* o di *brand differentiation* che si risolvano in una discriminazione algoritmica, o di qualsiasi tipo di «*cognitive manipulation*»⁷⁴⁶. Di conseguenza, l'ambito di applicazione dell'art. 22, par. 1 non includerebbe solo decisioni (della specie di cui ci stiamo occupando) relative all'assunzione e al “mansionamento” in ambito lavorativo, all'accesso al credito, alla stipulazione di polizze assicurative, o alla fornitura dei più disparati servizi; bensì anche potenzialmente, nei limiti che

⁷⁴⁵ Sul punto, cfr. nello specifico, G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», p. 253 ss., che puntualmente affaermano come «In general terms, scholars have argued that 'cybermarketing process could be plausibly said to have a significant (significantly adverse) effect on the persons concerned if it involves unfair discrimination in one or other form of 'weblining', e a tal proposito rinviando *ex multis* a FREDERIK ZUIDERVEEN BORGESIJUS, «Online Price Discrimination and Data Protection Law», in *Amsterdam Law School Research Paper* No. 2015-32, 2015; e a T. ZARSKY, «Understanding Discrimination in the Scored Society», cit.

⁷⁴⁶ Cfr. sempre, in particolare, G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 254. Gli stessi autori sottolineano come anche al di fuori del GDPR in realtà l'interesse “legittimo” della persona fisica a non costituire oggetto di *pervasive marketing manipulation*, di natura essenzialmente algoritmica, trovi tutela nel quadro di altri strumenti quali la Direttiva sulle pratiche commerciali sleali, la quale al *considerando* 6, se da una parte chiarisce che «pratiche pubblicitarie e di marketing generalmente ammesse, quali il product placement consentito, la differenziazione del marchio o l'offerta di incentivi in grado di incidere legittimamente sulla percezione dei prodotti da parte dei consumatori e di influenzarne il comportamento», dall'altra sottolinea precisamente come requisito essenziale della loro liceità si individui nel fatto che le pratiche medesime non limitino «la capacità di prendere una decisione consapevole» (nella versione originale inglese, «*the consumer's ability to make an informed decision*»). V. cons. 6 e anche cons. 18 della Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali»), GU L 149 dell' 11.6.2005, pagg. 22–39.

abbiamo descritto, le pratiche di *behavioural advertisement* e di *neuromarketing*, come ambito in cui i *profiling algorithms* sono massicciamente impiegati, e in cui dunque risulta ancor più importante vigilare sul raggiungimento di quella “soglia d’importanza” di cui poc’anzi ci siamo occupati⁷⁴⁷.

Per concludere sul punto della terza questione interpretativa che abbiamo introdotto ed esaminato, il Gruppo di Lavoro dedica alcuni cenni anche a quei processi decisionali interamente automatizzati (ormai, sarebbe sufficiente dire, algoritmici) *di gruppo*: esso infatti sottolinea come «effetti significativi possono risultare anche da azioni di persone *diverse* dalla persona alla quale fa riferimento la decisione automatizzata»: l’esempio portato dal Gruppo è quello di una società che fornisce carte di credito, la quale potrebbe ridurre il limite della carta di un cliente «*non* sulla base dello storico dei rimborsi di quel cliente, bensì su criteri di credito non tradizionali, quali un’analisi di altri clienti che vivono nella medesima area e acquistano presso i medesimi negozi». ⁷⁴⁸ Ciò, rileva opportunamente il Gruppo, «potrebbe comportare la limitazione delle opportunità di una persona sulla base di azioni di terzi»⁷⁴⁹. Dall’inciso in questione si inferisce, allora, che la natura collettiva della profilazione, e dunque del trattamento automatizzato su cui si fonda la successiva decisione riguardante una persona fisica, non escluda affatto a priori l’applicabilità del divieto generale previsto dall’art. 22, e la conseguente disciplina specifica⁷⁵⁰.

⁷⁴⁷ Ivi, p. 254 ss.

⁷⁴⁸ ». GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit, p. 25.

⁷⁴⁹ *Ibidem*.

⁷⁵⁰ Cfr. più diffusamente sul punto Mantelero, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of Data Protection, 32 Computer Law & Security Review, 238 (2016), passim.

3.2.4. Le eccezioni al divieto generale e le “misure appropriate” per tutelare i diritti dell’interessato. *Right to explanation*: essere o non essere?

Alla luce dei rilievi svolti nel paragrafo precedente, e allo scopo di operare un sintetico riepilogo della vasta gamma di concetti introdotti, possiamo affermare che l’art. 22 par. 1 stabilisce un *divieto generale* all’adozione di un processo decisionale unicamente automatizzato relativo alle persone fisiche con effetti giuridici riguardanti l’interessato o che incidano in modo analogo significativamente sulla sua persona: ciò significa che il titolare, di regola, *non dovrebbe intraprendere il trattamento*, e più in generale l’intero processo decisionale, appena descritto nei suoi elementi essenziali.

Possiamo dunque ora passare al secondo livello del sub-sistema normativo che, come abbiamo detto, l’art. 22 edifica: il par. 2, infatti, individua *tassativamente* una serie di eccezioni al ricorrere dei quali, nei limiti che subito tenteremo di precisare, *legittimano* (*rectius*: rendono lecito, al contestuale ricorrere dei presupposti previsti dalle disposizioni generali del Regolamento) il trattamento interamente automatizzato e la conseguente decisione presa *unicamente* sulla sua base; decisione che, altrimenti, risulterebbe soggetta al divieto di cui al par. 1. La lettera del par. 2 *consente*, pertanto, le decisioni basate unicamente su trattamenti automatizzati quando «sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento» (ipotesi sub a)); oppure quando «sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che *precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato*» (ipotesi sub b)); o altrimenti quando «si basi sul *consenso esplicito* dell'interessato» (ipotesi sub c)). Tanto nell’ipotesi sub a) quanto nell’ipotesi sub c) il par. 3 subordina poi esplicitamente la derogabilità del divieto di cui al par. 1

all'adozione da parte del titolare del trattamento di «misure appropriate» a favore dell'interessato, su cui ci soffermeremo in seconda battuta.

Occorre allora innanzitutto procedere a precisare il perimetro applicativo delle suddette ipotesi, seguendo ancora una volta le indicazioni delle Linee Guida in esame.

Per quanto attiene all'ipotesi di cui al par. 2 lett. a), bisogna innanzitutto ricordare come il Gruppo di Lavoro, nel già ricordato parere 06/2014, abbia precisato che il termine «necessario per l'esecuzione di un contratto» debba essere interpretato in senso stretto, cosicché il trattamento deve essere necessario per il vero e proprio adempimento delle obbligazioni derivanti dal singolo contratto in concreto stipulato con ciascun interessato⁷⁵¹. Premesso ciò, nelle Linee Guida in esame il Gruppo specifica che talvolta il coinvolgimento umano ai fini dell'esecuzione del contratto può essere impraticabile o impossibile in ragione della notevole quantità di dati che vengono trattati: tuttavia, conformemente all'interpretazione accolta nell'opinione appena citata, subito aggiunge che il titolare del trattamento «deve essere in grado di dimostrare che questo tipo di trattamento è *necessario*, tenendo conto della possibilità di adottare un metodo più rispettoso della vita privata»⁷⁵². Se esistono altri mezzi efficaci e meno

⁷⁵¹ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 06/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*. Commissione europea, 9 aprile 2014. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf. Cfr. S. THOBANI, «Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente», cit. p. 140 ss.

⁷⁵² GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 26. Sul punto, cfr. anche Buttarelli, Giovanni. Assessing the necessity of measures that limit the fundamental right to the protection of personal data. A Toolkit [Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali. Uno strumentario]. Garante europeo della protezione dei dati, 11 aprile 2017, (in inglese) https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf. Aggiungiamo solo che il Gruppo di lavoro nota poi che Il Gruppo ricorda come il processo interamente automatizzato potrebbe essere (effettivamente)

invasivi per conseguire il medesimo obiettivo, allora il requisito della «necessità» non sarà integrato.

Attenta dottrina ha sottolineato come la previsione in esame si distingua, in senso per lo più positivo, dalla precedente formulazione della deroga nel contesto dell'art. 15 della Direttiva 95/46/CE *non solo* per l'opportuna introduzione (tanto per tale ipotesi quanto per quella sub c)), ai sensi del par. 3, dell'ulteriore requisito rappresentato dall'adozione, da parte del titolare, delle misure adeguate di protezione di cui parleremo a breve; ma anche per aver aggiunto esplicitamente il criterio stesso della *necessaria strumentalità* del processo in questione all'esecuzione del contratto (o del rapporto precontrattuale), nonché per l'espunzione del requisito precedentemente rappresentato dal fatto che il contratto esistente fosse stato “richiesto” dall'interessato medesimo⁷⁵³.

La seconda deroga, prevista dalla lettera b) del par. 2, consente i processi medesimi laddove lo Stato membro ne autorizzi l'uso. Tuttavia, lo Stato è tenuto a stabilire misure adeguate a garanzia dei diritti, delle libertà e degli interessi legittimi dell'interessato, che in prima approssimazione si può dire coincidano semanticamente con le «misure appropriate» dal par. successivo imposte ai fini della effettiva integrazione dei fondamenti eccezionali di liceità sub a) e sub c): si potrebbe dunque, nella specie, ritenere che nel loro contenuto minimo *anche* esse debbano quanto meno includere «la possibilità per l'interessato di ottenere l'intervento umano, di esprimere il proprio punto di vista e di contestare la

necessario anche per l'esecuzione di un rapporto precontrattuale, portando il caso di un'azienda che, dopo aver pubblicizzato un posto di lavoro vacante, si trovi a dover valutare un elevato numero di candidature.

⁷⁵³ Cfr. L. A. BYGRAVE, I. MENDOZA, «The Right not to be Subject to Automated Decisions based on Profiling», cit.

decisione»⁷⁵⁴. Ci soffermeremo sulla questione del contenuto delle misure adeguate, di cui parla il par. 3, a breve.

Il Gruppo, sinteticamente, si limita a ricordare sul punto che il *considerando* 71 afferma che un processo decisionale interamente automatizzato idoneo ad integrare, al ricorrere dei suddetti presupposti, la fattispecie derogatoria articolata dal par. 2 lett. b) potrebbe essere quello adottato per «fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale o a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento»⁷⁵⁵.

L'ultima eccezione al divieto generale di cui al par. 1 consiste, come sappiamo, nel «consenso esplicito» dell'interessato. Tralasciando le considerazioni di ordine generale, per cui si rinvia all'analisi svolta al par. 3.2.2., è necessario qui brevemente soffermarsi sul termine «esplicito», interrogandosi sulla nozione accolta dal Regolamento. A tal proposito, le Linee Guida in esame rinviano alle rispettive linee guida adottate dal Comitato Europeo per la protezione dei dati (EDPB: organo, come sappiamo, subentrato al Gruppo a partire dal 2018) dedicate proprio alla base giuridica del consenso ai fini del GDPR, ed è nel loro contesto che alcune preziose indicazioni esegetiche sul significato *normativo* della formula «consenso esplicito» possono opportunamente rintracciarsi⁷⁵⁶.

Tenendo a mente che tale disposizione rappresenta, al pari ad esempio del trattamento di «categorie particolari di dati», una delle eccezioni previste dal Regolamento al nuovo principio di libertà delle forme sancito dal GDPR in punto

⁷⁵⁴ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 26 e 30 ss.

⁷⁵⁵ Ivi, p. 26.

⁷⁵⁶ Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 14 maggio 2020.

di consenso (qualificato) ai fini del lecito trattamento di dati personali, le linee guida 5/2020 affermano lucidamente come il consenso esplicito, quale rafforzamento della base giuridica del consenso, sia richiesto «in talune circostanze nelle quali emergono gravi rischi per la protezione dei dati e in cui si ritiene quindi appropriato un livello elevato di controllo individuale sui dati personali»: circostanze tra le quali quella dei processi decisionali interamente automatizzati, compresa la profilazione, ricade a pieno titolo⁷⁵⁷. Subito, il Comitato passa allora ad offrirne una definizione, rilevando come «il termine esplicito si riferisce al modo in cui il consenso è espresso dall'interessato e significa che l'interessato deve fornire una dichiarazione esplicita di consenso»⁷⁵⁸. L'organo precisa poi che, sebbene la dichiarazione scritta e – inoltre – firmata dall'interessato appaia il mezzo più ovvio per soddisfare senza margine di dubbio il requisito medesimo, esso non deve considerarsi affatto l'unico mezzo a tal scopo idoneo, e soprattutto, dato il sempre più digitalizzato contesto sociale, «non si può affermare che il regolamento prescriva dichiarazioni scritte e firmate in tutte le circostanze che richiedono un consenso esplicito valido». Il Comitato porta allora alcuni esempi di stretta attualità, osservando come, nel contesto digitale, o comunque online, l'interessato possa emettere la dichiarazione richiesta «compilando un modulo elettronico, inviando un'e-mail, caricando un documento scansionato con la propria firma oppure utilizzando una firma elettronica»⁷⁵⁹.

⁷⁵⁷ Ivi, punto, 91.

⁷⁵⁸ Ivi, punto 93.

⁷⁵⁹ Ivi, punto 94. È importante aggiungere come il Comitato ritenga che anche «l'uso di *dichiarazioni verbali* può essere sufficientemente specifico per ottenere un consenso esplicito valido», sottolineando come tuttavia possa essere difficile per il titolare del trattamento «dimostrare che tutte le condizioni per la validità del consenso esplicito siano state soddisfatte quando la dichiarazione è stata registrata». Conseguentemente, al punto 95 afferma che «Un'organizzazione può anche ottenere il consenso esplicito tramite una conversazione telefonica, a condizione che le informazioni sulla scelta siano corrette, intelligibili e chiare e

Prima di passare all'analisi del par. 3 dell'articolo 22, occorre evidenziare come il par. 4 configuri un regime derogatorio connotato da più rigorosi requisiti a fronte di quei processi decisionali automatizzati *ex par. 1* che abbiano ad oggetto le *categorie particolari di dati* di cui all'art. 9, sulla cui individuazione ci siamo già soffermati in precedenza. Il dato letterale della disposizione, come traspare dalle poche indicazioni offerte dal Gruppo di Lavoro, è già sufficientemente chiaro nell'esigere, ai fini della liceità del processo in questione, che lo stesso si fondi su di una situazione tipicizzata dal Regolamento: le apposite basi giuridiche, tuttavia, in tale contesto sono individuate dalla norma *solo* in quelle codificate dall'art. 9 par. 2, lett a), ossia ancora una volta nel consenso esplicito dell'interessato; e dall'art. 9, par. 2, lettera lett. g), ossia nella necessità del trattamento automatizzato (su cui la decisione *esclusivamente* si fondi) «per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»⁷⁶⁰. A differenza delle ipotesi ricadenti nell'alveo del par. 2, non sono dunque ammessi a derogare al divieto di cui al par. 1 i sistemi di *automated data processing and decision making* che elaborino dati sensibili agli stretti fini dell'esecuzione di un contratto tra interessato e titolare. Per entrambe le eccezioni, poi, la norma aggiunge (al pari del par. 2 lett. b) e del par. 3) come requisito ulteriore l'obbligo per il titolare di adottare misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

che venga richiesta una conferma specifica da parte dell'interessato (ad esempio premendo un pulsante o fornendo una conferma verbale)».

⁷⁶⁰ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 27.

A questo punto, appare necessario chiarire, ai fini ed agli effetti tanto del par. 2 quanto del par. 4, la natura e la portata delle «misure adeguate di tutela» che il par. 2 lett. b), il par. 3 e il par. 4 individuano quale *requisito cumulativo* al cui soddisfacimento risulta subordinata l'integrazione dei fondamenti eccezionali di liceità dei processi decisionali interamente automatizzati compresa la profilazione (e dunque la legittimità delle deroghe al divieto generale di cui al par. 1).

Il par. 3 appare il riferimento normativo precipuo per ricostruire l'estensione del concetto in esame: esso, infatti, con riguardo alle basi individuate dal par. 2 lett. a) e lett. c), stabilisce che «tali misure dovrebbero includere *quanto meno* la possibilità per l'interessato di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare la decisione». Il Gruppo, sul punto, individua il baricentro della disciplina in analisi principio secondo cui *l'intervento umano* rappresenta l'*elemento chiave* ai fini dell'eccezionale deroga al divieto di cui al par. 1: a ciò consegue che «qualsiasi revisione dovrebbe essere eseguita da qualcuno che dispon[ga] dell'autorità appropriata e delle competenze adeguate per modificare la decisione»; e, inoltre, la conseguente opportunità che il responsabile della revisione effettui «una valutazione approfondita di tutti i dati pertinenti, comprese eventuali informazioni aggiuntive fornite dall'interessato»⁷⁶¹. Riteniamo che tale lettura, stante l'identico dettato letterale, valga automaticamente anche per le basi giuridiche eccezionali di cui al par. 2 lett. b), e quindi per il tipo di «misure adeguate» che il diritto rispettivamente dell'UE o dello Stato membro è tenuto a precisare; nonché per le basi di cui al par. 4, e dunque con riferimento alle misure imposte ai titolari a fronte di decisioni basate esclusivamente sul trattamento automatizzato di dati sensibili.

⁷⁶¹ Ivi, p. 30.

In tema, l'organo consultivo fornisce indicazioni ermeneutiche ancor più importanti laddove valorizza la lettera del *considerando* 71 nella parte in cui osserva che in ogni caso le garanzie in parola, accanto al diritto ad una *specific information*, alla possibilità per l'interessato di *manifestare la propria opinione* in ordine alla decisione cui risulta soggetto e di ottenere un *coinvolgimento umano effettivo*, dovrebbero comprendere anche il «diritto (...) di ottenere una *spiegazione della decisione* conseguita *dopo* tale valutazione e di contestare la decisione»⁷⁶². L'inciso in questione ovviamente rafforza l'interpretazione secondo cui le *safeguards* cui il Regolamento fa esplicito riferimento al paragrafo 3 rappresentino solo il *contenuto minimo* del sistema di protezione che a favore dell'individuo *deve* essere predisposto affinché il divieto di cui al par. 1 sia derogabile. Conduce inoltre a ritenere che lo stesso breve (ma efficace) elenco di «misure appropriate» articolato dal par. 3 sia, chiaramente, *non esaustivo*: ciò appare desumibile, d'altra parte, dallo stesso dato letterale, che nel riferirsi a tali misure utilizza la locuzione avverbiale «almeno» («*at least*», nell'originale inglese)⁷⁶³. L'inciso in parola, infine, rappresenta il principale aggancio con l'analisi fondamentale dei diritti più specificamente configurati dalle altre disposizioni del Regolamento che compongono il sub-sistema normativo incardinato sull'art. 22, in ordine all'interpretazione della quale è germogliato

⁷⁶² *Ibidem*. Sul punto cfr. anche : L. A. BYGRAVE, «Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making», laddove sottolinea che «it is important to highlight that aspects of Article 22(3) offer a higher level of protection than under the DPD. Unlike the latter, a data subject will always have the right to demand human review of a fully automated decision, except where the decision is pursuant to statute. Even if statutory authority kicks in, this might well also allow for a right of review – as part of the requisite 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests' (Article 22(2)(b))».

⁷⁶³ Cfr. sempre L.A. BYGRAVE, op. cit., *ibidem*, che di seguito afferma «The list of rights laid down by Article 22(3) is the bare minimum required, and accordingly not exhaustive. Which other rights it encompasses is contested».

forse il più “infuocato” dibattito che la materia di cui ci stiamo occupando abbia fin ora conosciuto.

Svolgeremo l’esame di tali diritti a conclusione del presente paragrafo. Prima, tuttavia, occorre soffermarsi sul fatto che il Gruppo di Lavoro richiami, in sede di commento del par. 3, il *considerando* 71 non solo per precisare che il titolare del trattamento, come imposto dallo stesso art. 12 par. 2, «deve mettere a disposizione dell’interessato un modo semplice per esercitare tali diritti»; ma anche e soprattutto per evidenziare quella che più volte abbiamo identificato come una delle questioni centrali in punto di trattamento algoritmico dei dati, e consequenziali *solely automated decisions*: ciò che il Regolamento ambisce (o, alla luce di una sua interpretazione *fundamental rights-oriented*, risulta preordinato) a garantire, attraverso la prescrizione delle misure in questione e la costruzione di alcuni puntuali diritti dell’interessato, è la «*necessità di trasparenza del trattamento*»: l’interessato, infatti, sarà in grado di contestare una decisione o di esprimere il proprio parere «*soltanto se comprende pienamente come è stata presa la decisione e su quali basi*»⁷⁶⁴. Parole che ancora una volta fanno leva sulla centralità del principio di trasparenza sancito dall’art. 5, par. 1 lett. a), e che richiamano le considerazioni di quella parte della dottrina che ritiene come a propria volta, per comprendere le basi e la logica su cui la decisione algoritmica si fonda, risulti necessario comprendere e riconoscere le *inferenze* che la giustificano⁷⁶⁵. Concludendo sul tema delle misure adeguate di tutela che *in generale* (e nel minimo appena visto) il titolare risulta tenuto a predisporre, il Gruppo di Lavoro fornisce alcuni esempi utili a specificare le misure in questione, per garantire inoltre l’effettiva possibilità di esercizio dei diritti menzionati: tra

⁷⁶⁴ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 31.

⁷⁶⁵ Cfr. su tutti S. WATCHER, B. MITTELSTADT, «A Right to Reasonable Inferences», cit., p. 1 ss.

questi si ascrive l'opportunità per il titolare di effettuare «valutazioni frequenti degli insiemi di dati che tratta, in maniera da rilevare eventuali distorsioni», nonché lo sviluppo di «metodi per affrontare eventuali elementi pregiudizievoli, compreso un eccessivo affidamento sulle correlazioni»; ed anche la predisposizione di «sistemi che verific[hino] gli algoritmi» e lo svolgimento di «riesami periodici dell'esattezza e della pertinenza del processo decisionale automatizzato, compresa la profilazione», con particolare riguardo a tutte quelle «procedure e misure adeguate per prevenire errori, inesattezze o discriminazioni sulla base di categorie particolari di dati»⁷⁶⁶. Senza dimenticare l'esigenza, corollario dei principi di *privacy by design* e di *privacy by default*, di attuare ciclicamente tali misure, «non soltanto in fase di progettazione, ma anche in continuativamente, durante l'applicazione della profilazione alle persone fisiche»⁷⁶⁷.

Veniamo a questo punto ad occuparci della problematica questione concernente l'individuazione di alcuni puntuali diritti che, in materia di processi decisionali interamente automatizzati - laddove consentiti, al ricorrere delle fattispecie derogatorie che abbiamo analizzato - il legislatore europeo sembrerebbe (o meno, a seconda delle tesi di riferimento) configurare in capo all'interessato. La discussione, lo si considera a titolo preliminare, coinvolge necessariamente anche le altre norme che paiono comporre il sub-sistema normativo in esame: ci si riferisce nello specifico, come già ricordato più volte nelle pagine addietro, al disposto degli art. 13, par. 2 lett. f), 14 par. 2 lett. g e 15,

⁷⁶⁶ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 31.

⁷⁶⁷ *Ibidem*. Cfr. ancora, per una puntuale disamina in ordine alla trasparenza algoritmica, M. TURILLI, L. FLORIDI, «The ethics of information transparency, in *Ethics and Information Technology*, 2009, 11, 2, 105; T. ZARSKY, «Transparent predictions», in *University of Illinois Law Review*, 2013, 4, 1507 ss.

par. 1 lett. h). Tutte e tre le disposizioni prevedono, con formula identica, per il caso di processo decisionale automatizzato ai sensi dell'art. 22 (dove eccezionalmente lecito), il diritto dell'interessato di ricevere «informazioni significative sulla logica utilizzata, nonché [sull'] importanza e le conseguenze previste di tale trattamento per l'interessato»: informazioni, rispettivamente, declinate come oggetto di un obbligo in capo al titolare dall'art. 13 (laddove la raccolta dei dati avvenga presso l'interessato) e dall'art. 14 (laddove la suddetta raccolta avvenga presso un soggetto diverso), e piuttosto come uno dei molteplici oggetti del diritto di accesso dell'interessato *ex art.* 15.

Ebbene, l'oggetto che più vivamente ha acceso ed alimentato il dibattito in dottrina attiene alla configurabilità o meno di un vero e proprio *right to explanation* che originerebbe dal complesso delle disposizioni cui abbiamo fatto riferimento: e dunque, da una parte, il par. 3 dell'art. 22, che genericamente individua quelle «misure adeguate di tutela» sulle quali ci siamo poc'anzi soffermati: e, dall'altra, le disposizioni appena menzionate, che più puntualmente riconoscono all'interessato una posizione giuridica soggettiva qualificabile, in prima approssimazione, come *diritto ad informazioni significative* sulla logica della decisione e sulle conseguenze della medesima che lo riguardano. La domanda, nel dibattito, viene posta anche nei suddetti termini: è il diritto che risulta dai rispettivi par. degli art. 13, 14 e 15, corroborato dalle *appropriate safeguards* di cui al par. 3 dell'art. 22, qualificabile, alla luce di una sistematica interpretazione del Regolamento e dei pertinenti *considerando*, come *diritto alla spiegazione* della decisione medesima? Ed è, questo, un diritto che attiene alla spiegazione della sola logica che presiede all'*astratto funzionamento* dell'algoritmo utilizzato (diritto di spiegazione *ex ante* rispetto alla singola decisione); o che tutela la pretesa a conoscere la logica che informa lo *specifico procedimento* dal sistema algoritmico implementato per generare la *particolare*

decisione incidente sull'interessato (diritto ad una spiegazione *ex post* rispetto alla singola decisione)?⁷⁶⁸

Il dibattito in parola, lo si premette, è assai denso, ricco di contributi le cui riflessioni più propriamente giuridiche risultano spesso incardinate su dei presupposti teorici, e segnatamente filosofici, anche molto diversi tra loro (il che giustifica, stante l'eterogeneità delle premesse anche epistemologiche dei rispettivi discorsi, la forte dialettica esistente tra le conclusioni dei medesimi). Qui, umilmente, si cercherà soltanto di tracciare le linee essenziali del dibattito e alcune dei suoi principali sbocchi, nei limiti in cui lo consentano il tema specifico della trattazione, i tempi di redazione e (non da ultimo) la preparazione specialistica di chi scrive. Soprattutto, data la rotta che abbiamo deciso di seguire, ci si soffermerà sull'interpretazione accolta (sulla scorta dei contributi di vasta dottrina) dal Gruppo di Lavoro nelle Linee Guida in esame, per poi fare cenno ad alcune delle più recenti (e convincenti) ricostruzioni dottrinali che cercano di uscire dalla dicotomia esistenza/inesistenza di un *right to explanation* (e, pertanto, di valorizzare alcuni connotati del pacificamente esistente *right to meaningful information* di cui agli art. 13 par. 2 lett. g) e seguenti).

La questione scaturisce, innanzitutto, dalla non perfetta sovrapponibilità tra il disposto delle norme cui abbiamo fatto riferimento e le «garanzie adeguate» che, come abbiamo visto, vengono menzionate dal par. 3 dell'articolo 22 e le quali, si riporta nuovamente il testo, «dovrebbero comprendere la specifica

⁷⁶⁸ Per una ricostruzione dei termini in cui viene posta la questione, nonché dello stesso dibattito in materia cfr. G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit.; I. MENDOZA, L.A. BYGRAVE, «The Right Not to be Subject to Automated Decisions Based on Profiling», cit.; A.D. SELBST, J. POWELS, «Meaningful information and the right to explanation», in *7 International Data Privacy Law*, 233 (2017).

informazione all'interessato e *il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione*». È quest'ultimo inciso a rappresentare la più marcata differenza tra articolato normativo e preambolo del GDPR, nella questione di cui ci stiamo occupando. A complicare il quadro certamente concorre la complessa "trama" che in punto di configurabilità o meno di un vero e proprio diritto alla spiegazione della singola decisione algoritmica ha contrassegnato l'iter di approvazione delle disposizioni del GDPR in materia di processi decisionali interamente automatizzati, cui già in precedenza abbiamo fatto riferimento. In sintesi, dall'esame dei lavori preparatori al GDPR emerge come, sebbene inizialmente le istituzioni coinvolte, e segnatamente il Parlamento Europeo nelle sue proposte di emendamento, avessero previsto esplicitamente nel testo delle disposizioni dedicate alla materia più stringenti misure di protezione, e in particolare un «*legally binding right to explanation of specific decisions*», queste ultime nel testo definitivamente approvato furono espunte e incorporate solo nel quadro del preambolo⁷⁶⁹. In particolare, dal report del novembre 2013 ad opera del Parlamento Europeo si evince come il testo in prima lettura emendato prevedesse espressamente al paragrafo 5 dell'art. 20, allora rubricato «Misure basate sulla profilazione», che «le misure adeguate a salvaguardia dei legittimi interessi dell'interessato di cui al paragrafo 2 *includono il diritto di ottenere una valutazione umana e una spiegazione della decisione conseguita dopo tale valutazione*»⁷⁷⁰. Tuttavia, dopo

⁷⁶⁹ Cfr. in particolare S. WACHTER, B. MITTELSTADT, L. FLORIDI; 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', cit., p. 6; G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit., nota. 29.

⁷⁷⁰ Cfr. EUROPEAN PARLIAMENT COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, 'Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and

anni di negoziazione, la versione finale risultò più simile alle originarie proposte della Commissione e del Consiglio, e un riferimento al diritto in parola fu situato esclusivamente nel *considerando* 71 già più volte richiamato, mentre nell'articolato normativo si scelse di includere, in termini espliciti, soltanto: il diritto all'intervento umano, ad esprimere la propria opinione e a contestare la decisione, di cui al par. 3 dell'art. 22; ed il diritto di accedere a (con i corrispondenti obblighi per il titolare di notificare/fornire) informazioni significative sulla logica utilizzata, previsto dall'art. 15 par. 1 lett. h) e dalle altre disposizioni già menzionate ⁷⁷¹.

Ora, il dibattito che andiamo considerando non può non principiarsi proprio e soprattutto dal valore riconosciuto ai *considerando* - e quindi al preambolo degli atti normativi europei - dalla dottrina che in punto di *right to explanation* è venuta a confrontarsi, con particolare riguardo alla loro (contrastata) rilevanza nell'interpretazione sistematica delle singole disposizioni del Regolamento. Abbiamo tuttavia già precedentemente sottolineato come, stante la loro natura non vincolante, pacifica giurisprudenza della Corte di Giustizia riconosca ai *considerando* un'essenziale *funzione di indirizzo interpretativo* con riferimento alle disposizioni precettive delle fonti di diritto comunitario, sottolineando come questi siano principalmente preordinati a dissolvere le ambiguità che connoti la lettera delle disposizioni medesime ⁷⁷².

on the Free Movement of Such Data (General Data Protection Regulation) - A7-0402/2013' (European Parliament 2013) A7-0402/2013.

⁷⁷¹ Per la proposta originaria, "ripristinata" poi nella versione finale del Regolamento, cfr. COMMISSIONE EUROPEA, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, Bruxelles, 2012, COM(2012) 11 fin.

⁷⁷² Per tale interpretazione, cfr. F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679, cit., p. 8 ss; per una dettagliata ricostruzione della giurisprudenza della CGUE in materia, cfr. R. Baratta, *Complexity of EU Law in the Domestic Implementing Process*, 2 *The Theory and Practice of Legislation*, 293 (2014).

Tuttavia, sul riconoscimento di un valore più o meno *forte* ai *considerando* medesimi la dottrina resta divisa. Ed anche da tale divisione dipende il diverso esito cui le disparate “scuole” sono giunte in punto di qualificazione del suddetto *diritto ad informazioni significative*, in seguito all’interpretazione sistematica delle disposizioni del GDPR. La dottrina, almeno inizialmente, si è recisamente divisa tra coloro che hanno ritenuto discendente dal GDPR un nuovo *right to (algorithmic) explanation*, segnatamente *ex post*, come originariamente previsto da una parte delle proposte di legge in seno alle istituzioni comunitarie⁷⁷³; e coloro che, coltivando un approccio più scettico e teso ad evidenziare -in senso critico- i limiti disegnati dalle previsioni del Regolamento agli interessi fondamentali dell’interessato, in funzione dell’anima ancora “mercantilista” della normativa, hanno concluso che l’atto, accanto ai semplici diritti d’informazione e di accesso di cui agli art. 13 e seguenti, non configurerebbe un più ampio (né, tantomeno, autonomo) diritto alla spiegazione *ex post*⁷⁷⁴.

Approfondendo brevemente le due tesi *radicali*, si può affermare che la prima fu anche quella da cui prese origine il dibattito, ed emerse negli ambienti dell’Università di Oxford ad opera di alcuni studiosi convinti che «[t]he GDPR’s policy on the right of citizens to receive an explanation for algorithmic decisions

⁷⁷³ Cfr. in particolare B. GOODMAN, S. FLAXMANN, «European Union regulations on algorithmic decision-making and a "right to explanation"», 38, AI Magazine, 3, 2017, <http://arxiv.org/abs/1606.08813>; cfr. per un’interpretazione simile I. MENDOZA, L.A. BYGRAVE, «The Right Not to be Subject to Automated Decisions Based on Profiling», cit.; per una netta ricostruzione del *right to explanation* come *ulteriore* rispetto a quello ad ottenere informazioni significative sulla logica utilizzata di cui agli art. 13 e seguenti, cfr. invece .D. Selbst and J. Powels, *Meaningful information and the right to explanation*, in 7 *International Data Privacy Law*, 233 (2017).

⁷⁷⁴ Su tutti, cfr. S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, cit.; ma v. anche, nel criticare l’impianto poco garantista del regolamento, Lilian Edwards and Michael Veale, ‘Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For’, 16 *Duke Law & Technology Review* 18 (2017). Available at SSRN: <https://ssrn.com/abstract=2972855>.

*highlights the pressing importance of human interpretability in algorithm design»*⁷⁷⁵.

Essi, convinti dell'esigenza di prevenire e di contrastare la discriminazione algoritmica, ritengono infatti che il fondamento normativo del diritto ad una spiegazione della decisione si individui non soltanto nelle «misure adeguate» di cui all'articolo 22 GDPR, ma anche e soprattutto nelle concrete modalità attuative dei doveri informativi di cui agli articoli 13, 14 e 15 GDPR: a tal riguardo, essi valorizzano appunto il dettato del *considerando* 71, pur riconoscendone la non vincolatività giuridica in sé e per sé, ritenendo tuttavia che dal sistema così delineato origini una fondamentale questione: «*what does it mean, and what is required, to explain an algorithm's decision?*»⁷⁷⁶. La risposta può essere varia, ma ciò non toglie che, nello scaturirla, il Regolamento implicitamente configuri il diritto che della risposta costituisce il cuore: «*The law will also effectively create a "right to explanation," whereby a user can ask for an explanation of an algorithmic decision that was made about them*»⁷⁷⁷.

A tale interpretazione altri autori, sempre negli ambienti di Oxford, reagirono immediatamente e in modo altrettanto radicale, sostenendo quella tesi che abbiamo già definito come diametralmente opposta: il GDPR nella sua attuale formulazione non riconoscerebbe il diritto ad una spiegazione *ex post* delle specifiche decisioni assunte, ma un più limitato diritto ad essere *ex ante* informati sulle caratteristiche generali di funzionamento del sistema di IA utilizzato⁷⁷⁸. E tale tesi, è importante sottolinearlo, oltre che sull'iter di approvazione del

⁷⁷⁵ Cfr. B. GOODMAN, S. FLAXMAN, European Union regulations on algorithmic decision-making and a "right to explanation", 38, AI Magazine, 3, 2017, 1.

⁷⁷⁶ Ivi, pp. 1-6.

⁷⁷⁷ Ivi, p. 1.

⁷⁷⁸ S. WACHTER, B. MITTELSTADT, L. FLORIDI, «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», cit.

Regolamento in punto di processi decisionali interamente automatizzati, si basa essenzialmente sul dato letterale sopra ricordato, secondo cui il diritto alla “spiegazione” viene espressamente menzionato *solo* a livello dei *considerando* del GDPR, e in particolare nell’ormai noto *considerando* 71 al quale, notano gli Autori, non può che attribuirsi un valore meramente interpretativo (o piuttosto, verrebbe da dire, *interpretativo debole*), non inidoneo ad integrare, in senso stretto, il contenuto dispositivo dei precetti normativi⁷⁷⁹.

Bisogna tuttavia concordare, anche alla luce delle premesse teoriche accolte (che, in accordo con la giurisprudenza della CGUE, riconoscono ai *considerando* un ruolo determinante nell’interpretazione in chiave teleologica, oltre che sistematica, delle disposizioni degli atti normativi europei⁷⁸⁰), con quelle voci che hanno sottolineato come quest’ultima ricostruzione, per quanto testualmente fedele, minimizzi in modo forse eccessivo il ruolo dei *considerando* stessi: ruolo che, per quanto meramente persuasivo o interpretativo, trova una sua forte ragion d’essere laddove chiarisce, ad esempio, la portata dell’espressione «misure adeguate» utilizzata dal legislatore nell’articolo 22 par. 3⁷⁸¹. A tale rilievo, deve aggiungersi il carattere particolarmente delicato della questione in esame: come è stato lucidamente notato, infatti, «la massima trasparenza garantita da *standards*

⁷⁷⁹ Ivi, p. 4 ss. A suffragio della loro lettura essi richiamano le considerazioni della CGUE nel caso Case 215/88 Casa Fleischhandels [1989] ECR-2789, para 31; nonché tra le altre le tesi di K.-J. VAICIUCAITE, «The Law of Recitals in European Community Legislation», 15 *Journal of International & Comparative Law* 32 (2008);

⁷⁸⁰ Cfr. quanto esplicitato dalla Corte di Giustizia ad esempio in C. Giust. Ue, procedimenti riuniti C-509/09 (*eDate Advertising GmbH c. X*); e C-161/10, (*Martinez c. MGN Limited*), del 25 ottobre 2011, parr. 54-55.

⁷⁸¹ Cfr. in particolare G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», 243, 254-255, spec. nt. 85.

pur elevati di informazione potrebbe essere insufficiente, se le informazioni non sono comprese dal destinatario»⁷⁸².

Sono questi allora, tra gli altri, i rilievi che hanno condotto il Gruppo di Lavoro, nelle Linee Guida in esame, ad accogliere un'interpretazione che, pur non esplicitando mai l'adesione alla tesi della configurabilità *incondizionata* di un diritto alla *spiegazione ex post*, sembra comunque propendere per quest'ultima, beninteso entro certi limiti: e ciò cominciando proprio dalla valorizzazione del *considerando* 71, a dimostrazione di come lo stesso organo consultivo riconosca ad esso, e all'intero preambolo, quella fondamentale idoneità a guidare l'interpretazione teleologica delle disposizioni del Regolamento⁷⁸³.

Abbiamo già denunciato l'enfasi posta dal Gruppo sull'esigenza (e sul relativo principio) di trasparenza delle decisioni algoritmiche: essa viene ulteriormente specificata laddove si afferma che il titolare del trattamento dovrebbe «prestare particolare attenzione agli obblighi in materia di trasparenza» proprio «in considerazione dei potenziali rischi e delle interferenze che la profilazione [e non solo] di cui all'articolo 22 [dove ammessa ai sensi del par. 2 o del par. 4] pone in relazione ai diritti degli interessati». Obblighi che, giova ripeterlo, scaturiscono dall'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g), ai quali corrisponde la relativa declinazione del diritto di accesso di cui all'art. 15 par. 1 lett. h), e che consistono essenzialmente nel comunicare all'interessato «l'esistenza di processi decisionali automatizzati, compresa la profilazione», e di fornirgli «informazioni significative sulla logica

⁷⁸² Cfr. E. Pellicchia, *Profilazione e decisioni algoritmiche al tempo della black-box society*, cit.

⁷⁸³ Ancora più forte è, poi, la funzione riconosciuta ai *considerando* da alcuni autori che come U. Pagallo ritengono questi ultimi idonei a fondare un'interpretazione (veramente) integrativa del disposto degli articoli del Regolamento: cfr. U. Pagallo, «Three Lessons Learned for Intelligent Transport Systems That Abide by the Law», in Jusletter IT RZ 13, 2016.

utilizzata nonché sull'importanza e le conseguenze previste del trattamento per l'interessato»⁷⁸⁴.

Il Gruppo, innanzitutto, sottolinea che tali norme impongono al titolare di fornire informazioni, sui “punti” in questione e più in generale sul processo decisionale interamente automatizzato di cui all'art. 22, che siano «specifiche e facilmente accessibili»⁷⁸⁵. Di seguito, esso provvede esplicitamente a chiarire il perimetro delle espressioni e dei concetti di «informazioni significative sulla logica utilizzata», di «importanza» e di «conseguenze previste»: dalle riflessioni che qui riassumeremo emerge chiaramente la preferenza del Gruppo per una lettura in combinato disposto delle suddette disposizioni che garantisca l'interesse (fondamentale) della persona fisica *quanto meno* a conoscere e a comprendere completamente il procedimento logico-inferenziale che ha condotto alla decisione che lo riguarda, le sue basi e i suoi motivi⁷⁸⁶.

Le Linee Guida partono dal presupposto che la crescita e la complessità dell'apprendimento automatico (che oggi come sappiamo si spinge sino agli “imponderabili” sistemi di *Deep Learning* basati sulle reti neurali artificiali) possono «rendere difficile comprendere come funzionano un processo decisionale automatizzato o la creazione di profili»: di conseguenza, il titolare del trattamento che si avvalga di essi (segnatamente, verrebbe da dire, nel contesto della profilazione), deve trovare «*metodi semplici per comunicare all'interessato le motivazioni alla base o i criteri invocati per raggiungere la decisione*». L'inciso in questione va posto in evidenza: nel riferirsi alle motivazioni alla base e nei

⁷⁸⁴ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 27 ss.

⁷⁸⁵ Ivi, pp. 27-28

⁷⁸⁶ Cfr. G. MALGIERI, G. COMANDÉ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 255 ss.; S. Watcher, B. Mittelstadt, A Right to Reasonable Inferences, cit., p. 1 ss.; R. Messinetti, Privacy e controllo dell'identità algoritmica, cit., p. 134 ss.

criteri invocati, il Gruppo sta di fatto riconoscendo l'opportunità di accogliere un'interpretazione che riconosca in capo all'interessato un diritto ad ottenere una spiegazione che attiene al singolo processo decisionale implementato; dunque, di necessità, una spiegazione *successiva* all'adozione della decisione medesima⁷⁸⁷.

Tuttavia, il Gruppo si affretta (opportunamente) a precisare che il Regolamento, nell'imporre al titolare di fornire informazioni significative (a maggior ragione dove richiesto *ex art. 15*) sulla logica e sulle conseguenze della *singola* decisione, non impone necessariamente una «spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo»; ma senza dubbio impone *in qualsiasi caso* che siano fornite informazioni «*sufficientemente complete*» - in particolare, sui fattori presi in considerazione e sul loro peso aggregato- affinché l'interessato possa comprendere le ragioni della decisione, presupposto indispensabile affinché lo stesso possa *contestarla* nel merito⁷⁸⁸. La

⁷⁸⁷ Cfr. anche, a suffragio della lettura che pare accolta dal Gruppo, le interessanti note di I. MENDOZA, L.A. BYGRAVE, «The Right Not to be Subject to Automated Decisions Based on Profiling», cit., che, nel criticare la tesi radicalmente negativa di WACHTER MITTELDSTAT FLORIDI affermano che «*First, the wording of Art. 15 does not necessarily exclude the possibility that it embraces a right of ex post explanation of an Art. 22 type decision. The fact that one has a right to information about the 'existence' of automated decision making suggests that such decisions already take place. Further, the reference in Art. 15 to supply of information regarding the 'significance and envisaged consequences' of such decision making could point to the practical consequences of an already taken decision which are viewed by the controller as likely to follow from that decision*».

⁷⁸⁸ GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 28. È interessante sottolineare come venga portato dal Gruppo un esempio che ricalca in modo simile quello oggetto del *leading case* della Corte di Giustizia in materia di processi decisionali interamente automatizzati, recentemente intervenuto e che sarà a breve oggetto di analisi, ossia il caso SCHUFA: l'esempio è appunto quello in cui un titolare del trattamento utilizza il punteggio di affidabilità creditizia (*credit scoring*) per valutare e respingere una domanda di prestito di una persona. Tale punteggio può essere stato fornito da un'agenzia di referenze per il credito oppure calcolato direttamente sulla base delle informazioni detenute dal titolare del trattamento. Ebbene, il Gruppo chiaramente afferma che, che se il titolare del trattamento si basa su tale punteggio, esso deve essere in grado di spiegarlo e di illustrarne la logica all'interessato.

complessità, infatti, «non è una scusa per non fornire informazioni all'interessato»⁷⁸⁹.

Nel riferirsi, poi ai concetti di «importanza» della decisione e di «conseguenze previste», centrale è il fatto che secondo il Gruppo, tra i modi per fornire informazioni in modo semplice e chiaro, particolarmente efficace risulterebbe la predisposizione di «*esempi reali e tangibili del tipo di possibili effetti*» cui si troverà esposto l'interessato, messi a disposizione (e dunque, resi conoscibili) a quest'ultimo. A tal proposito, le Linee Guida portano un esempio chiaro: laddove una compagnia assicurativa utilizzi un processo decisionale automatizzato per impostare i premi dell'assicurazione auto in base al monitoraggio del comportamento di guida dei clienti, per illustrare il significato e le conseguenze previste del trattamento occorrerà spiegare che una guida pericolosa può comportare pagamenti assicurativi più elevati, e a tal scopo si potranno utilizzare, ad esempio, un'applicazione o elementi grafici per dare consigli su come migliorare queste abitudini e di conseguenza come ridurre i premi assicurativi⁷⁹⁰.

Ricordiamo, a titolo conclusivo, che sempre secondo il Gruppo un ruolo centrale per la riduzione dell'impatto sui diritti e sulle libertà dell'interessato del potenziale discriminatorio insito nella tecnologia algoritmica, e pertanto nei *solely automated systems* attraverso cui siano elaborati i dati e consequenzialmente adottate le decisioni che la sua persona riguardano, risulta svolto dalla valutazione d'impatto *ex art. 35*, la quale, lo ricordiamo, ai sensi del par. 3 è *obbligatoria*

⁷⁸⁹ *Ibidem*, nota 40, in cui il Gruppo richiama il considerando 58, che emblematicamente afferma come il principio di trasparenza sia “particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online”».

⁷⁹⁰ Ivi, p. 29.

quando il processo consista in una «valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche»⁷⁹¹. E altrettanto importante è ricordare che il par. 11 del medesimo articolo impone una revisione costante della valutazione in relazione alle modifiche dei trattamenti o all'attivazione di nuovi.

In chiusura della nostra analisi delle Linee Guida del Gruppo di Lavoro, sulla quale ci siamo ampiamente intrattenuti, ci sembra di poter constatare che le sezioni da ultimo esaminate, pur aprendo significativamente alla necessità di motivare e spiegare la decisione automatizzata, non risultino altrettanto chiare (contraddittoriamente, viene da dire) nel riconoscere in modo esplicito l'esistenza di un vero e proprio diritto alla spiegazione della singola decisione, deducibile dalla sistematica del GDPR⁷⁹².

Tuttavia, proprio per superare la ferrea dicotomia tra esistenza e inesistenza del diritto in parola, in dottrina sono emerse alcune proposte ricostruttive (alcune delle quali, peraltro, valorizzano anche le aperture insite nelle Linee Guida). Tutte le proposte in questione sono dirette a massimizzare, nei limiti ammessi dalla lettera delle disposizioni del Regolamento (pur interpretate estensivamente alla luce del preambolo), i presidi a salvaguardia dell'autodeterminazione

⁷⁹¹ Ivi, p. 33 ss.

⁷⁹² Da sottolineare come non tutti gli autori apprezzino lo sforzo esegetico condotto dal Gruppo di Lavoro, ed anzi ne criticino o la genericità o l'eccessiva forzatura del dato letterale. Cfr. ad esempio Per critica dell'attività interpretativa del WP art. 29, VEALE, EDWARDS, «Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling», in *Computer Law & Security Review*, 2018, p. 398 ss. Gli autori rilevano non soltanto mancanza di chiarezza nel discorso interpretativo del WP ma ampi sconfinamenti nell'attività creativa di diritto.

informativa dei *data subjects* rispetto alle eccezionali in cui i processi decisionali interamente automatizzati risultino consentiti in deroga al par. 1 dell'art. 22⁷⁹³.

Nella variopinta moltitudine di tali proposte, alcune più orientate sul versante teorico ed altre piuttosto su quello pratico-applicativo, particolarmente interessanti appaiono quella incentrata su di un modello di c.d. «spiegazione controfattuale» (*counterfactual explanations*), alla luce della quale l'interpretazione sistematica delle disposizioni del Regolamento parrebbe imporre al titolare di fornire agli interessati su cui ricadano gli effetti di decisioni unicamente basate su trattamenti automatizzati informazioni di ordine *pratico*, in particolare relative a cosa sarebbe necessario modificare (nell'input, ma non solo) affinché lo stesso possa ottenere un più desiderabile risultato, sulla base del modello di *algorithmic decision making* di cui attualmente disponga il titolare⁷⁹⁴; o anche quella fondata sull'assunto che dall'impianto generale del Regolamento discenda un nuovo diritto della personalità, in cui si specifica il diritto all'autodeterminazione informativa, ossia il diritto ad inferenze ragionevoli (*right to reasonable inferences*): un diritto che, alla luce di una concezione olistica della *privacy*, dovrebbe presidiare l'interesse ad essere “correttamente visti e rappresentati” dal sistema algoritmico e ancor più dall'IA, da garantirsi con particolare e ulteriore forza nel contesto, chiaramente, dei processi decisionali interamente algoritmici di cui all'art. 22⁷⁹⁵.

⁷⁹³ Per una efficace panoramica generale sulle medesime e sui loro scopi, cfr. G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit.

⁷⁹⁴ Cfr. SANDRA WACHTER, BRENT MITTELSTADT, CHRIS RUSSELL, «Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR», in *Harvard Journal of Law & Technology*, 31 (2), 2018. Disponibile su SSRN: <https://ssrn.com/abstract=3063289> or <http://dx.doi.org/10.2139/ssrn.3063289>, 4.

⁷⁹⁵ Cfr. WACHTER, MITTELSTADT, «A Right to Reasonable Inferences», cit., p. 1 ss. . Osserva R. MESSINETTI, «Privacy e controllo dell'identità digitale», cit., p. 159 ss. che «il significato attribuito all'espressione “ragionevole” identifica lo standard di controllo dell'accuratezza giuridica delle inferenze: un giudizio di “accettabilità normativa”, rilevanza e

In particolare, però, riteniamo opportuno soffermarci con maggiore attenzione sulla proposta, sempre avanzata in dottrina, di introdurre in contesto giuridico, e nel settore che qui ci occupa, il concetto di *legibility*: concetto comunemente impiegato nell’ambito della *computer science*, che identifica «*the capability of individuals to autonomously understand data and analytics algorithms, with a concrete comprehension of methods and data used*»⁷⁹⁶. La “leggibilità”, in altre parole, combinerebbe la *readability*, ossia la capacità di comprendere in autonomia il funzionamento dell’algoritmo, con la *comprehensibility*, e dunque la trasparenza rispetto alla sua utilizzazione, e dunque rispetto all’importanza e alle conseguenze della decisione automatizzata medesima⁷⁹⁷. Tale soluzione, come è stato notato, consentirebbe di «fornire agli individui la capacità di comprendere autonomamente il funzionamento, l’impatto, le conseguenze, la ratio del processo decisionale automatizzato», così da rappresentare «la soluzione più desiderabile (e) radicata nelle previsioni del Regolamento europeo»⁷⁹⁸.

L’interpretazione in questione fa essenzialmente leva – al pari delle Linee Guida – sull’obbligo a carico dei titolari di fornire informazioni significative sulla logica utilizzata e sull’importanza e sulle conseguenze del processo decisionale *ex art. 22 par. 1*, di cui agli artt. 13 par. 2 lett f) e ss.: secondo la proposta, l’espressione «*meaningful*» della versione inglese del Regolamento verrebbe

affidabilità alla stregua di regole giuridiche, etiche e scientifiche che sono richiamate dal GDPR».

⁷⁹⁶ Cfr. RICHARD MORTIER et al., «Human Data Interaction: The Human Face of the Data-Driven Society», *MIT Technology Review*, 2014 <<https://www.technologyreview.com/s/533901/the-emerging-science-of-human-data-interaction/>>

⁷⁹⁷ Per la proposta dottrinale che ora ci occupa, cfr. diffusamente G. MALGIERI, G. COMANDÈ, «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», cit., p. 248 ss.

⁷⁹⁸ Cfr. E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black-box society», cit.

assunta in tutta la sua ricchezza di significanti, ovvero sia come «*significant, serious*», sia come «*intended to show the meaning*». Il primo significato è evocativo della trasparenza (o *readability*), il secondo della comprensibilità, e tali risultano essere le due anime del concetto di leggibilità⁷⁹⁹.

Pertanto, “leggibilità” è concetto che, secondo gli autori, supererebbe il dilemma – e la dialettica – informazione/spiegazione, perché rappresenterebbe un approccio «*more “proactive”, tailored to individual understanding and concrete comprehensibility of the logic and consequences disclose*»⁸⁰⁰.

Accenniamo, infine, solo al fatto che la stessa dottrina da ultimo richiamata, assieme ad altre voci, ha elaborato un *legibility test* (fondato su un complesso ed analitico questionario), strutturato in due parti, l’una relativa al funzionamento dell’algoritmo (per illuminare la logica utilizzata), e l’altra per rivelarne la concreta incidenza sul processo decisionali. Obiettivo di tale ulteriore proposta sarebbe quella di promuovere un approccio *legibility by design*, che, secondo gli autori, avrebbe ricadute positive anche per i titolari dei trattamenti, grazie all’innalzamento della qualità e dell’accuratezza dei processi decisionali automatizzati⁸⁰¹.

3.2.5. La sentenza del 7 dicembre 2023 della Corte di Giustizia nel caso *SCHUFA* (e i suoi precedenti nazionali): il *leading case* europeo in materia di processi decisionali interamente automatizzati

⁷⁹⁹ Ivi, p. 256 ss.

⁸⁰⁰ Ivi, p. 250.

⁸⁰¹ Ivi, p. 259. Cfr., tra gli altri studiosi che si sono diffusi nella teorizzazione e nella concreta elaborazione del test in questione, Julie E. Cohen, *Configuring The Networked Self: Law, Code, And The Play Of Everyday Practice*, (Yale University Press, 2012), 167–69, 256; Tal Zarsky, «Transparent Predictions», cit. pp. 1563–1567.

Abbiamo già avuto modo di constatare come, successivamente all'entrata in vigore della Direttiva 95/46/CE, l'art. 15 in materia di decisioni unicamente basate su un trattamento automatizzato (essenzialmente, secondo il suo dettato, di profilazione), nonostante gli Stati membri avessero provveduto alla sua trasposizione nei singoli ordinamenti nazionali, fosse stato raramente oggetto di contenzioso davanti alle corti e di *litigation* davanti ai garanti nazionali. Parimenti, abbiamo già detto di come non sia possibile riscontrare alcuna decisione della CGUE in punto di interpretazione o di validità della disposizione medesima in tutti i vent'anni di vigenza della suddetta normativa⁸⁰².

Le eccezioni in ambito nazionale, stando ai risultati della ricerca sin qui condotta, sono assai poche, ed appaiono essenzialmente concentrati in Germania e in Francia.

Ci si riferisce, innanzitutto, alla decisione resa nel 2014 dalla Corte Federale Suprema tedesca (*Bundesgerichtshof*) nel cosiddetto caso *SCHUFA* (nome di una società privata d'informazione sul merito creditizio), riguardante l'impiego di sistemi automatizzati di *credit scoring*. Investita del gravame, nella sentenza - in sintesi - la Corte, interpretando il §6a della normativa federale tedesca sulla protezione dei dati personali (*Bundesdatenschutzgesetz*, abbreviato BDSG), che l'art. 15 della Direttiva Madre trasponeva nell'ambito dell'ordinamento federale tedesco, statuiva che il suddetto sistema interamente automatizzato di *scoring* creditizio esulasse dall'ambito di applicazione della norma in questione: e ciò perché, ad opinione della Corte, gli elementi "automatizzati" del processo decisionale avrebbero riguardato solo il momento dell'elaborazione dei dati e della conseguente preparazione dell'evidenza (ovvero del punteggio assegnato al singolo creditore), laddove invece l'attuale decisione di erogare (nella specie,

⁸⁰² V. retro, e cfr. ancora L. A. BYGRAVE, L. A. BYGRAVE, «Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making», cit.

negare) il credito sarebbe stata adottata da un essere umano⁸⁰³. Risulta ancora, nel contesto della decisione, non interamente matura la riflessione svolta dai giudici intorno al funzionamento dei sistemi di trattamento algoritmici, in particolare sotto il delicato e problematico profilo del coinvolgimento umano effettivo, che secondo la più gran parte della dottrina e le stesse Linee Guida europee *non può dirsi sussistente* in caso di mero recepimento passivo della raccomandazione algoritmica (ad esempio, nella specie, quella implicita in un basso punteggio circa il merito del potenziale creditore).

Altrettanto rilevante appare poi un caso più risalente, deciso dalla Corte di Cassazione francese (*Cour de Cassation*). Tra le diverse articolazioni del complesso oggetto del giudizio in questione, infatti, ricadeva anche l'utilizzo da parte dei giudici, nell'ambito di un procedimento penale, di tecniche (automatizzate) di analisi statistica dell'attività di professionisti (quali, nella specie, fisioterapisti-massaggiatori) per mezzo di *computer systems*⁸⁰⁴. Pur non riguardando la disposizione preordinata alla trasposizione interna della direttiva 95/46/CE, tale giudizio concerne comunque il principale antecedente normativo dell'articolo 15 della direttiva medesima, ovvero il già richiamato art. 2 della *Loi 78-17*: anche in questo caso, la Suprema Corte, pur nei limiti delle proprie funzioni di giudice di legittimità, escluse che l'utilizzo di sistemi computerizzati

⁸⁰³ V. diffusamente BGH, 28.1.2014, VI ZR 156/13, consultabile sul sito internet istituzionale del Bundesgerichtshof <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=66910&pos=0&anz=1>. Con le parole della Corte, che qui traduciamo (si perdonino, nel caso, le approssimazioni terminologiche): « Nel caso del punteggio [rating creditizio], si può presumere che la decisione individuale sia effettivamente automatizzata *solo se* l'organo responsabile della decisione assume una decisione, la quale abbia conseguenze giuridiche per la persona interessata o un impatto negativo significativo su di lui, *esclusivamente* sulla base del risultato del punteggio senza ulteriore esame del contenuto, ma non se la *conoscenza acquisita attraverso l'elaborazione automatizzata* dei dati è *solo la base per una decisione finale* che deve ancora essere presa da un essere umano», par. 34.

⁸⁰⁴ Cfr. Cour de Cassation, Chambre criminelle, du 24 septembre 1998, 97-81.748, Bulletin criminel 1998 N° 236 p. 686.

di valutazione statistica, come avvenuto nella fattispecie *de qua*, ricadesse nell'ambito di applicazione del divieto di decisioni giudiziarie (interamente) automatizzate prescritto dal par. 1 dell'art. 2, dal momento che le statistiche non sarebbero state generate e usate in modo tale da definire il profilo o la personalità del soggetto coinvolto⁸⁰⁵.

Per quanto attiene, invece, al contenzioso davanti alle Autorità Garanti nazionali, l'unica pronuncia riscontrata sotto la vigenza dell'art. 15 è quella adottata nel 2017 (nelle more, dunque, dell'entrata in vigore e del conseguente adeguamento dell'ordinamento interno alla disciplina del già approvato GDPR) dal Garante francese (*Commission Nationale de l'Informatique et des Libertés*, abbreviato CNIL), in cui si è riscontrato che i sistemi automatizzati impiegati dalla pubblica amministrazione per valutare e decidere sulle domande di ammissione degli studenti alle Università francesi - senza che tra l'altro agli stessi studenti in caso di rifiuto fosse garantita la possibilità di integrare la domanda con altre modalità (ottenendo, in definitiva, l'intervento umano) - fosse in contrasto con l'art. 10 della *Loi 78-17*, che l'art. 15 della Direttiva Madre trasponeva nell'ordinamento francese⁸⁰⁶.

Tutto ciò, prima dell'entrata in vigore del GDPR e, conseguentemente, dell'art. 22. Successivamente, lo scenario ha subito alcune sostanziali modifiche.

⁸⁰⁵ Merita notare che il disposto dell'art. 2 sarebbe stato poi modificato e spostato nell'art. 10 della medesima normativa al fine di meglio allinearli al recepimento art. 15 della Direttiva Madre.

⁸⁰⁶ Cfr. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), Décision MED-2017-053 du 30 août 2017; particolarmente importante il passaggio in cui l'Autorità constata che «*Un étudiant dont la candidature n'est pas retenue pour une formation non sélective de son choix, du fait de la position qui lui a été attribuée par l'algorithme dans le classement, ne pourra intégrer celle-ci par un autre moyen. Il en résulte qu'une décision produisant des effets juridiques à l'égard des candidats est prise sur le seul fondement du traitement [...] dès lors que celui-ci détermine les formations post-baccalauréat auxquelles ils peuvent s'inscrire.*».

Di fatti l'accresciuta consapevolezza, in ambito informatico, filosofico, giuridico e istituzionale dei rischi esistenti nella “civiltà degli algoritmi” per la libertà di autodeterminazione informativa del singolo; le maggiori garanzie predisposte a favore degli interessati attraverso il sub-sistema edificato sul perno dell'art. 22; e l'intenso dibattito dottrinale intervenuto sull'esegesi e sull'operatività di quest'ultima disposizione hanno innescato un processo di sensibilizzazione della collettività all'impatto delle decisioni algoritmiche sui propri interessi fondamentali, e alimentato un primo “bagliore” di contenzioso in relazione alla fattispecie dei processi decisionali interamente automatizzati, e dunque all'interpretazione e all'applicazione dello stesso art. 22. Nel prossimo paragrafo, a tal proposito, ci focalizzeremo sull'ordinamento italiano, soffermandoci su alcune delle più recenti pronunce della giurisprudenza ed esaminando talune delle più rilevanti decisioni del Garante in materia.

Come si suol dire, insomma, il *trend* è in crescita. Tuttavia, la tendenza è ancora ben lontana dall'eguagliare il numero di ricorsi, amministrativi o piuttosto effettivamente giurisdizionali, pendenti in relazione agli altri fondamentali profili della disciplina della *data protection*. Merita poi rilevare che, in ambito comunitario, fino a pochi mesi fa continuava a mancare un qualsiasi intervento della Corte di Giustizia *nello specifico* dedicato alla fattispecie, ed alla relativa disciplina, in esame.

Non è il caso di addentrarsi troppo diffusamente nei motivi che presiedono a tale ingiustificata lacuna: se da una parte la “verginità” giurisprudenziale della materia stimola l'interprete a formulare le più caleidoscopiche ipotesi, e, come abbiamo constatato esaminando le numerose diatribe dottrinali in ordine all'art. 22, ne “liberano la fantasia”, dall'altra i tempi che si impongono a questa ricerca e gli strumenti d'indagine a disposizione di chi scrive non ci consentono di elaborare una convincente proposta teorica. Tuttavia, alcune considerazioni sono comunque possibili.

In parte, bisogna rilevare che stante la natura di “strumento”, oltre che di vero e proprio “agente operativo”, espressa dai sistemi algoritmici e di IA, numerose sono state nella storia della giurisprudenza – nazionale ed anche comunitaria - le controversie solo incidentalmente riguardanti l’utilizzo dei sistemi in questione, laddove il *thema decidendum* atteneva piuttosto alla sussistenza o meno dei requisiti di liceità del trattamento medesimo. Caso emblematico è quello deciso con la nota sentenza *Planet 49*, che ha definitivamente sancito l’invalidità, per difetto del requisito della libertà, del consenso ai *cookie* di profilazione prestato per mezzo di caselle preselezionate⁸⁰⁷. È utile in proposito ricordare che le operazioni svolte *ex cookies* per definizione, stante la totale matrice algoritmica dei sistemi su cui si fondano tali marcatori temporanei, risulta qualificabile come trattamento automatizzato (e di certo *interamente* automatizzato è il profilo della *raccolta* dei dati).

Al contempo, è evidente che, essendo i mezzi di ricorso individuale interamente assorbiti, in sede europea, dall’istituto del rinvio pregiudiziale configurato dall’art. 267 del TFUE, in assenza di contenzioso nazionale non ci si poteva ragionevolmente attendere alcuna consequenziale pronuncia della Corte (mancando, appunto, una questione pregiudiziale sollevata da un giudice nazionale). Con l’infoltirsi della giurisprudenza nazionale in punto di applicabilità dell’art. 22 (e delle relative disposizioni interne di adeguamento), c’è da attendersi che si moltiplicheranno gradualmente anche le pronunce in sede di rinvio pregiudiziale della CGUE.

A testimonianza di ciò, risale al 7 dicembre 2023 la prima sentenza fino ad ora conosciuta con cui la Corte di Giustizia abbia risposto ad una domanda di rinvio pregiudiziale relativa all’interpretazione dell’art. 22 del GDPR, facendo luce su alcuni dei nodi interpretativi che abbiamo avuto modo di analizzare nelle

⁸⁰⁷ Cfr. C. Giust. UE, 1° ottobre 2019, C-673/17, cit.

pagine addietro: ci riferiamo alla decisione resa nel caso *OQ contro il Land Hessen*, noto piuttosto come caso *SCHUFA*, con cui, lo si anticipa, la Prima Sezione della Corte ha stabilito che l'art. 22 par. 1 del GDPR deve essere interpretato nel senso che il calcolo algoritmico di natura probabilistica di un punteggio relativo al merito creditizio di una persona fisica basato sul trattamento dei dati personali della medesima da parte di un'agenzia di valutazione del credito costituisce di per sé un «processo decisionale automatizzato relativo alle persone fisiche» qualora da tale punteggio «dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo», al quale il punteggio sia comunicato⁸⁰⁸.

La sentenza in parola può essere definita senza troppe esitazioni un *leading case* in materia. Essa, infatti, si occupa *per la prima volta* nella storia della Corte dell'art. 22 *nello specifico*, ma soprattutto appare animata, come ben vedremo, dall'evidente proposito (parzialmente soddisfatto, a parere di chi scrive) di svolgere una ricostruzione sistematica della disciplina in punto di processi decisionali interamente automatizzati, consacrando nel panorama dei precedenti alcuni dei *principi cardine* già enucleati dalla più sensibile dottrina e destinati a svolgere un ruolo fondamentale a presidio della personalità umana nel contesto tecnosociale contemporaneo.

Inoltre, come è stato rilevato, tale sentenza risultava grandemente attesa per due fondamentali ragioni. La prima consiste certamente nel fatto che essa interviene in uno dei settori nei quali, come abbiamo constatato, l'impiego di sistemi (interamente) algoritmici risulta più diffuso e potenzialmente più pregiudizievole per l'individuo, ossia il *credit scoring* o *rating* creditizio. Ricordiamo, in sintesi, che tale pratica consiste nell'attività di calcolo di un punteggio di c.d. merito creditizio, fondato su un tasso di probabilità, derivante

⁸⁰⁸ C. Giust. UE 7.12.2023, causa C-634/21, *OQ contro Land Hessen*. Cfr. già, per le considerazioni qui svolte, il dispositivo della sentenza.

dal trattamento dei dati personali della persona fisica che richieda l'accesso ad una linea di credito, relativo alla capacità attuale e futura del soggetto medesimo di onorare l'impegno finanziario assunto (e circa la sua solvibilità)⁸⁰⁹.

La seconda ragione attiene al fatto che la decisione si iscrive in modo “prepotente” nel dibattito in corso all'interno delle istituzioni comunitarie sul c.d. *Artificial Intelligence Act*, ossia sulla proposta di Regolamento in materia di IA cui già *retro* abbiamo fatto riferimento⁸¹⁰.

Stante l'importanza della pronuncia *SCHUFA*, occorre procedere al suo esame, premettendo che, data la sua recentissima sopravvenienza, non sono ancora apparsi in dottrina rilevanti contributi con i quali confrontarsi. Tuttavia, nel corso del commento faremo ampiamente riferimento (come del resto fa la stessa Corte) alle Conclusioni dell'Avvocato Generale del 16 marzo 2023, cui la Corte si è quasi interamente uniformata nell'articolare il proprio ragionamento. Le importanti riflessioni condensate nelle predette Conclusioni, e richiamate dalla Corte nelle motivazioni della pronuncia, sembrano ampiamente nutrirsi del dibattito dottrinale fiorito intorno all'art. 22, e in particolar modo degli indirizzi

⁸⁰⁹ Cfr. E. PELINO, «IA, storica sentenza UE su mutui: nuovi obblighi per le aziende», in *Network Digital 360*, consultabile qui: <https://www.agendadigitale.eu/sicurezza/sentenza-schufa-che-guaio-per-lai-quel-mutuo-negato-dallalgoritmo-ecco-limpatto/>. Sullo specifico tema del credit scoring, cfr. BRENDA REDDIX-SMALLS, «Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market», (2011) 12 *U.C. Davis Bus. L.J.* 87, 117-18.

⁸¹⁰ Cfr. F. SARZANA, La Corte di Giustizia UE tra GDPR e Artificial Intelligence Act; in *Il Sole 24 Ore*, 8 dicembre 2023, consultabile qui: <https://fulviosarzana.nova100.ilsole24ore.com/2023/12/08/corte-di-giustizia-ue-gdpr/>. V. COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*, COM/2021/206 final, 21 aprile 2021, COM/2021/206 final, consultabile qui: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206>. Dobbiamo sottolineare che, pochi giorni dopo la sentenza, l'UE ha annunciato il raggiungimento di un accordo provvisorio tra i negoziatori del Parlamento Europeo e del Consiglio sul testo della proposta di Regolamento medesimo: cfr. il comunicato stampa pubblicato sul sito istituzionale dell'ente, <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>.

fundamental rights-oriented di cui abbiamo dato conto: ciò, anche a dimostrazione della centralità del *formante dottrinale* nella materia che ci occupa⁸¹¹. Non si può poi tacere del fatto che tanto le Conclusioni quanto le motivazioni della pronuncia, per gli stessi motivi, dimostrano un debito con la visione altrettanto *antropocentrica* espressa dal Gruppo di Lavoro Articolo 29 nelle Linee Guida sul processo decisionale automatizzato da noi ampiamente esaminate.

La pronuncia *SCHUFA* ha sullo sfondo una controversia di merito scaturita in Germania. Anche tale sentenza, al pari della precedente pronuncia della Corte Federale Suprema tedesca poc'anzi richiamata, riguarda i risultati dell'attività della SCHUFA Holding AG, società di diritto privato tedesco che, come sintetizza la Corte nel ritenuto in fatto, «fornisce ai suoi partner contrattuali informazioni sul merito creditizio di terzi, in particolare di consumatori», stabilendo a tale scopo «un pronostico sulla probabilità di un comportamento futuro di una persona («score»), come il rimborso di un prestito, a partire da talune caratteristiche di tale persona, sulla base di procedure matematiche e statistiche»⁸¹².

Più nello specifico, la pronuncia ha ad oggetto, in senso stretto, la domanda di pronuncia pregiudiziale vertente sull'interpretazione dell'articolo 6, paragrafo 1, e dell'articolo 22 del GDPR, presentata nell'ambito di una controversia tra OQ e il *Land Hessen* (il Land dell'Assia tedesco) in merito al rifiuto dello *Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (Commissario per la protezione dei dati e la libertà di informazione per il Land Assia, Germania, in prosieguito lo «HBDI») di ingiungere alla SCHUFA Holding AG (in prosieguito, la

⁸¹¹ Cfr. sin d'ora le Conclusioni dell'Avvocato Generale Priit Piikmäe, causa C-634/21, *OQ contro Land Hessen*, con l'intervento di SCHUFA Holding AG, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62021CC0634&qid=1707426086567>.

⁸¹² Cfr. C. Giust. UE 7.12.2023, causa C-634/21, *OQ contro Land Hessen*, punto 14.

«SCHUFA») di accogliere una domanda presentata da OQ diretta ad *ottenere e a cancellare dati personali che la riguardano*.

Venendo brevemente ai fatti, il caso riguardava una persona fisica – OQ - a cui era stato negato un prestito da parte di un terzo, a causa di informazioni negative erogate dalla SCHUFA. A fronte della richiesta di OQ a quest’ultima società di comunicargli informazioni sui propri dati personali registrati e di cancellare quelli erronei, la società si era limitata ad informare OQ del livello del suo punteggio di “merito creditizio” e aveva esposto, a grandi linee, le modalità di calcolo dei punteggi; tuttavia, si era rifiutata, *invocando il segreto commerciale*, di divulgare le diverse informazioni prese in considerazione ai fini di tale calcolo, nonché la loro ponderazione. La SCHUFA aveva peraltro evidenziato come essa si limitasse a far pervenire le informazioni elaborate alle sue controparti contrattuali (banche, istituti di credito, società finanziarie), e di come fossero in seconda istanza solo queste ad adottare le decisioni di concessione o diniego del credito⁸¹³.

Di fronte a tale risposta, OQ aveva allora presentato un reclamo amministrativo, respinto tuttavia dall’autorità di controllo competente (HBDI), la quale affermava che la SCHUFA avrebbe rispettato i requisiti di legge⁸¹⁴.

Sulla scorta di queste premesse, veniva proposto ricorso dinanzi al Tribunale amministrativo di Wiesbaden (*Verwaltungsgericht Wiesbaden*; da ora in avanti, «giudice del rinvio»), il quale riteneva che al fine di statuire sulla controversia di cui fosse investito, occorresse determinare se il calcolo di un tasso di probabilità come quello oggetto del procedimento principale (e dunque del

⁸¹³ Ivi, punti 15-18. Cfr, anche le Conclusioni dell’Avvocato Generale Priit Piakmäe, causa C-634/21, cit., punto 11, laddove ricostruisce nei suddetti termini la risposta della SCHUFA: «La SCHUFA ritiene di non essere tenuta a divulgare i suoi metodi di calcolo, poiché essi rientrano nel segreto professionale e nel segreto industriale e aziendale. Inoltre, a suo dire, essa si limiterebbe a fornire informazioni ai clienti, i quali adotterebbero poi le decisioni vere e proprie in merito ai contratti di credito».

⁸¹⁴ Ivi, punto 19.

punteggio di *credit scoring*) costituisse un processo decisionale automatizzato relativo alle persone fisiche, ai sensi dell'articolo 22, paragrafo 1, del GDPR: infatti, in caso affermativo, la liceità di tale attività sarebbe stata subordinata, conformemente all'articolo 22, paragrafo 2, lettera b) del GDPR medesimo, alla condizione che tale decisione fosse autorizzata dal diritto dell'Unione o dal diritto dello Stato membro cui fosse soggetto il titolare del trattamento⁸¹⁵.

Ancora, si legge nella sentenza come il giudice del rinvio nutrisse dubbi quanto alla tesi secondo cui l'articolo 22, paragrafo 1, del GDPR *non* fosse applicabile all'attività di società quali la SCHUFA, segnatamente alla luce dell'importanza di un tasso di probabilità come quello oggetto della controversia *de qua* per la prassi decisionale dei terzi ai quali tale tasso di probabilità fosse trasmesso, nonché all'obiettivo perseguito dall'art. 22 di «proteggere le persone dai rischi connessi alle decisioni puramente basate su automatismi». In particolare, il giudice del rinvio sottolineava come in generale sia il tasso di probabilità in parola a determinare *se e come* il terzo contratterà con l'interessato. E, conseguentemente, evidenziava come un'interpretazione dell'art. 22 par. 1 tale da riconoscere la qualificazione in termini di «processo decisionale relativo alle persone fisiche» (o, sarebbe meglio dire, di *decisione basata unicamente sul trattamento automatizzato* relativo alle stesse) alla sola decisione adottata dal terzo, e non anche all'attività di *scoring* automatizzato sui risultati della quale la decisione si basa, determinerebbe una intollerabile lacuna nella tutela giuridica dell'interessato: a quel punto, infatti si verserebbe *de facto* nell'insussistenza di alcun obbligo di fornire informazione supplementari (ai sensi, come sappiamo, degli art. 13 par. 2 lett f), o 14 par. 2 lett g)) in capo alla società di *credit scoring*, e parimenti del corrispondente diritto di accesso alle informazioni medesime, declinato ai sensi dell'art. 15 par. 1 lett. h), esercitabile dall'interessato nei

⁸¹⁵ Ivi, punti 20-21

confronti della società⁸¹⁶. Peraltro, notava ancora il giudice *a quo*, il terzo al quale viene comunicato il tasso di probabilità del rimborso non potrebbe allo stesso modo fornire le informazioni supplementari richieste, in quanto non ne disporrebbe: alla luce di questo e degli alti rilievi condotti, il giudice del rinvio riteneva che il calcolo di un tasso di probabilità come quello di cui trattasi nel procedimento principale ricadesse nell'ambito di applicazione dell'articolo 22, paragrafo 1, del GDPR⁸¹⁷.

Allo scopo di chiarire in via definitiva la portata applicativa dell'art. 22, par. 1, precisamente in relazione alla fattispecie oggetto del procedimento principale, il Tribunale amministrativo di Wiesbaden sospendeva il procedimento principale sollevando davanti alla CGUE questione pregiudiziale inerente all'interpretazione della suddetta disposizione: e dunque, in sostanza chiedeva se il «calcolo automatizzato di un tasso di probabilità relativo alla capacità di un interessato di saldare in futuro un debito» costituisca *già* una decisione basata unicamente sul trattamento automatizzato di cui all'art. 22 par. 1 (relativo alle persone fisiche, dunque, ed avente *legal* o *similarly relevantly effects* sull'interessato medesimo), «qualora tale tasso di probabilità, calcolato sulla base di dati personali relativi all'interessato, sia trasmesso dal titolare del trattamento ad un terzo titolare del trattamento, e quest'ultimo basi prevalentemente su di esso la decisione sulla stipulazione, sull'esecuzione o sulla cessazione di un contratto con l'interessato»⁸¹⁸.

⁸¹⁶ Ivi, punto 21 ss.

⁸¹⁷ Ivi, punto 24.

⁸¹⁸ Ivi, punto. 27. Merita sottolineare che il giudice *a quo*, in subordine, aveva sottoposto alla Corte un'altra questione pregiudiziale "dipendente", subordinandone la soluzione all'adozione di una risposta negativa sulla prima; questione così formulata: « se l'articolo 6, paragrafo 1, e l'articolo 22 del [RGPD] debbano essere interpretati nel senso che ostano a una normativa nazionale ai sensi della quale il ricorso a un tasso di probabilità – nella fattispecie relativo alla solvibilità e alla disponibilità a pagare di una persona fisica, che includa informazioni sui crediti – di un certo comportamento futuro di una persona fisica, allo scopo di decidere sulla stipulazione, sull'attuazione o sulla cessazione di un contratto con tale persona

La decisione di rinvio della questione alla Corte perveniva in data 21 ottobre 2021 presso la cancelleria della Corte di Giustizia, e successivamente la SCHUFA decideva di intervenire nel giudizio di rinvio pregiudiziale pendente.

Risolte le questioni procedurali, sulle quali soprassedere, la Corte viene ad occuparsi nel merito della questione pregiudiziale in esame. L'intero impianto della pronuncia, come abbiamo già accennato, risente sin dall'incipit del contributo teorico dell'Avvocato Generale: quest'ultimo, già a partire dalle proprie osservazioni preliminari, sembra accogliere quella prospettiva *umanitaria* (o antropocentrica, o personalista, o *fundamental rights-oriented* che dir si voglia) che valorizza l'anima del Regolamento orientata a massimizzare la tutela dei diritti fondamentali della persona fisica, compreso dunque il diritto all'autodeterminazione informativa quale presupposto per la *libera costruzione della propria personalità*. Nelle Conclusioni, infatti, sin da subito si legge che, nel contesto della profilazione «vanno evidenziate le restrizioni previste all'articolo 22 del RGPD, pertinenti nella presente causa, che mirano a *tutelare la dignità umana*», e poco più avanti che «l'intervento umano richiesto nell'ambito di questo tipo di trattamento automatizzato dei dati garantisce che l'interessato abbia la possibilità di esprimere il suo punto di vista, ottenere una spiegazione in

(“scoring”), [sia] consentito solo se sono soddisfatte determinate ulteriori condizioni, meglio specificate nella motivazione della domanda di pronuncia pregiudiziale». Le disposizioni della legislazione interna pertinente in materia di *credit scoring*, alla luce dei rilievi svolti nella motivazione della domanda di pronuncia pregiudiziale ad opera del giudice *a quo*, venivano identificate essenzialmente nell'art. 31 del *Bundesdatenschutzgesetz* (legge federale sulla protezione dei dati), del 30 giugno 2017, come modificato dalla legge del 20 novembre 2019⁴ (in prosieguo: il «BDSG»), rubricato «Protezione delle transazioni commerciali in caso di *scoring* [determinazione di punteggi di *scoring*] e di informazioni sulla solvibilità». Nonostante l'approfondita disamina della questione da parte dell'Avvocato Generale, di cui comunque proponeva una soluzione in senso negativo, si anticipa che la Corte, risolvendo positivamente la prima, ha consequenzialmente ritenuto non opportuno rispondere a quest'ultima. Cfr, per un approfondimento Conclusioni dell'Avvocato Generale Priit Piikmäe, causa C-634/21, cit., par. 60 e ss.

merito alla decisione adottata al termine di detta tipologia di valutazione e contestarla qualora non la condivida»⁸¹⁹.

Peraltro, l'accoglimento generale di una prospettiva *fundamental rights-oriented* appare ancora più evidente se a questi rilievi si uniscono i passaggi in cui, nell'esaminare la portata dei concetti che compongono la fattispecie di cui all'art. 22 par. 1, l'Avvocato Generale valorizza la centralità del *considerando* 71 come ausilio interpretativo privilegiato della disposizione medesima, alla luce del quale non si possa concludere in altro modo se non riconoscendo che «la disposizione de qua prevede un *divieto generale* delle decisioni» basate unicamente sul trattamento automatizzato compresa la profilazione⁸²⁰.

La Corte a sua volta, lo abbiamo detto, mutua quasi interamente la struttura argomentativa seguita dall'Avvocato Generale nelle proprie Conclusioni. Preliminarmente, tuttavia, essa principia dalla considerazione secondo cui l'interpretazione di una disposizione del diritto dell'Unione richieda di tener conto *non soltanto* della sua formulazione, ma anche del *contesto in cui essa si inserisce*

⁸¹⁹ Cfr. Conclusioni dell'Avvocato Generale Priit Piakmäe, causa C-634/21, cit., par. 18 ss. Pare interessante soffermarsi brevemente sulle considerazioni che l'Avvocato dedica al contesto in cui la vicenda si iscrive: esso rileva come in un'economia di mercato, rappresentando la fiducia reciproca il fondamento di ogni vincolo contrattuale, «è, in linea di principio, comprensibile (...) che i fornitori di servizi e di beni desiderino conoscere i propri clienti e i rischi connessi» al primo, di modo che «le agenzie di valutazione del credito possono contribuire a rafforzare detta fiducia reciproca attraverso metodi statistici che consentono alle imprese di stabilire se determinati criteri pertinenti, compresa la solvibilità dei loro clienti, siano nella specie soddisfatti». Tuttavia, «taluni dei metodi impiegati possono fondarsi su dati personali dei clienti, raccolti e trattati in modo automatizzato grazie alla tecnologia informatica». All'interesse imprenditoriale dunque «si contrappone quello vantato dai soggetti interessati a sapere *in che modo i dati di cui trattasi sono gestiti e registrati e i metodi seguiti dalle imprese per adottare decisioni nei confronti dei propri clienti*». E l'Avvocato, qui sta il punto, sembra riconoscere, nel ponderare i due interessi, prevalenza (in quanto valore *fondamentale* della persona umana), proprio a quest'ultimo, laddove più avanti (par. 43) assume tale netta posizione: «Posto che un punteggio di *scoring* negativo [interamente automatizzato, s'intende] può avere, da solo, ripercussioni negative sull'interessato, vale a dire limitarlo sensibilmente nell'esercizio delle sue libertà, o stigmatizzarlo nella società, sembra giustificato qualificarlo come «decisione» ai sensi della disposizione succitata [art. 22, par. 1] quando un istituto finanziario gli attribuisce un'importanza fondamentale nel processo decisionale».

⁸²⁰ Ivi, par. 31.

nonché degli *obiettivi e della finalità* che persegue l'atto di cui essa fa parte⁸²¹. Contesto, obiettivi e finalità che, in relazione all'art. 22, anche la Corte sembra ritenere illuminati proprio dal *considerando* 71.

La Corte pertanto ritiene che, ai fini della soluzione della questione, essenziale sia innanzitutto definire quelle che - conformemente alla proposta dell'Avvocato, in proposito a propria volta debitrice delle Linee Guida del Gruppo di Lavoro a noi ben note - rappresentano le *tre condizioni essenziali* cumulative cui pare subordinata l'applicabilità dell'art. 22 par. 1: vale a dire, come ormai sappiamo, il concetto di «decisione»; in secondo luogo, quello di decisione «basata unicamente sul trattamento automatizzato, compresa la profilazione»; e infine quello di «effetti giuridici che [l'interessato] riguardano» e quello di «incida in modo analogo significativamente sulla sua persona»⁸²². Anche la definizione di tali concetti risulta profondamente aderente al dettato delle Linee Guida, alla cui analisi condotta nei paragrafi precedenti pertanto si rinvia. Qui possiamo limitarci ad evidenziare in special modo come la Corte ritenga che dalla disposizione in esame emerga una *nozione ampia* di «decisione», e che questa sia confermata a livello interpretativo proprio dal *considerando* 71, che tra l'altro, a titolo esemplificativo, ascrive al concetto di decisione «il rifiuto automatico di una domanda di credito online», pertinente nel caso di specie. Ma il passaggio certamente più rilevante sul concetto di «decisione» si rinviene al punto 46 della sentenza, in cui la Corte, aderendo alla lettura dell'Avvocato Generale di cui al par. 38 delle sue Conclusioni, afferma che la nozione medesima appare «sufficientemente ampia da ricomprendere il risultato del calcolo della solvibilità

⁸²¹ C. Giust. UE 7.12.2023, causa C-634/21, *OQ c. Land Hessen* punto 41, cit., che rinvia a sentenza del 22 giugno 2023, *Pankki S*, C-579/2, punto 38 e giur. citata.

⁸²² Ivi, punti 43 ss.

di una persona sotto forma di tasso di probabilità relativo alla capacità di tale persona di onorare impegni di pagamento in futuro»⁸²³.

La Corte ritiene parimenti soddisfatte le altre due condizioni, e segnatamente la qualificazione del (calcolo del) tasso di probabilità medesimo in termini di «decisione *basata unicamente* su un trattamento automatizzato compresa la profilazione», poiché pacifica appare la qualificazione dell'attività dello SCHUFA in termini di «profilazione»⁸²⁴; e, allo stesso tempo, quella di decisione che produca «effetti giuridici» nei confronti dell'interessato, svolgendo tale tasso un ruolo decisivo nella decisione di una terza parte di concedere il credito a quest'ultimo⁸²⁵.

La Corte può allora, su tali basi, affermare già che «in circostanze come quelle di cui al procedimento principale, nelle quali il tasso di probabilità stabilito da una società che fornisce informazioni commerciali e comunicato a una banca svolge un ruolo decisivo nella concessione di un credito, il *calcolo di tale tasso* deve essere *qualificato di per sé* come decisione che produce nei confronti di un interessato «effetti giuridici che lo riguardano o che incid[e] in modo analogo significativamente sulla sua persona», ai sensi dell'articolo 22, paragrafo 1, del GDPR⁸²⁶.

⁸²³ Ivi, punto 46. Cfr. ancora una volta il par. 31 delle Conclusioni dell'Avvocato Generale Priit Piakmäe, causa C-634/21, cit

⁸²⁴ Ivi, punto 47. Cfr. par. 33 delle Conclusioni dell'Avvocato Generale, cit., dove si afferma che « lo scoring compiuto dalla SCHUFA ricade nella definizione legale contenuta nell'articolo 4, punto 4, del RGPD, posto che detta procedura utilizza dati personali per valutare determinati aspetti relativi alle persone fisiche per analizzare o prevedere aspetti riguardanti la situazione economica, l'affidabilità e il probabile comportamento di dette persone».

⁸²⁵ Ivi, punto 48. Anche dove non producesse effetti giuridici in senso stretto, lo stesso sarebbe comunque più che idoneo a produrre effetti significativi incidenti in modo analogo sull'interessato, se come rileva l'Avvocato al par. 35 delle sue Conclusioni « un siffatto rifiuto [conseguenziale alla comunicazione al terzo del tasso di probabilità] può incidere anche sulla situazione finanziaria dell'interessato», cosicché risulta «logico concludere che la disposizione di cui trattasi inciderà, in ogni caso, «in modo analogo» su detta persona».

⁸²⁶ Ivi., punto 50.

La Corte, tuttavia, non si ferma qui. Il collegio coglie l'opportunità offerta dalla domanda di rinvio pregiudiziale per addentrarsi in una ricostruzione "olistica" del sistema di protezione rafforzato che, a fronte di processi decisionali interamente automatizzati riguardanti la persona fisica (quale, secondo la felice interpretazione accolta dalla Corte, risulta essere la fattispecie oggetto del procedimento principale), l'art. 22 configurerebbe. Tale edificio discenderebbe per l'appunto da un'interpretazione sistematica dell'art. 22, condotta alla luce (con le parole della Corte) del «contesto in cui si inserisce l'articolo 22, paragrafo 1, del RGPD nonché [degli] obiettivi e dalla finalità perseguiti da tale regolamento»⁸²⁷.

La ricostruzione in questione, ancora una volta, si adegua pressoché interamente alla lettura promossa dal Gruppo di Lavoro nelle analizzate Linee Guida e alla Corte restituita dalla sensibilità e dalla penna dell'Avvocato Generale. Di seguito, ci soffermiamo esclusivamente su quei passaggi che testimoniano del generale accoglimento, ad opera della Corte, della predetta prospettiva personalista, tale da massimizzare le garanzie predisposte a favore della persona fisica dall'art. 22.

Primo e più rilevante elemento della ricostruzione è certamente l'accoglimento, in seno dunque alla giurisprudenza della Corte, della tesi che interpreta l'articolo 22 par. 1 come fondamento di un divieto generale *ex ante*⁸²⁸. Nell'argomentare a difesa di tale tesi in modo pressoché speculare alle Conclusioni dell'Avvocato Generale ed alle stesse Linee Guida del WP29, rileva senza dubbio ancora una volta il peso attribuito al *considerando* 71: con le parole della Corte, «*come risulta dal combinato disposto dell'articolo 22, paragrafo 2,*

⁸²⁷ Ivi punto 51.

⁸²⁸ Ivi, punto 52, in cui si afferma: «come osservato dall'Avvocato Generale al par. 31 di tali conclusioni (...) tale disposizione sancisce un *divieto di principio* la cui violazione non necessita di essere fatta valere individualmente da una tale persona».

*del RGPD e del considerando 71 di tale regolamento, l'adozione di una decisione basata esclusivamente su un trattamento automatizzato è autorizzata solo nei casi di cui a tale articolo 22, paragrafo 2 (...)).*⁸²⁹ All'esito di una ricognizione della struttura della disposizione stessa, guidata dal *considerando 71*, la Corte non può che riscontrare come «[i] requisiti più rigorosi per quanto riguarda la liceità di un processo decisionale automatizzato nonché gli obblighi di informazione supplementari del titolare del trattamento e i relativi diritti di accesso supplementari dell'interessato *si spiegano con la finalità perseguita dall'articolo 22 del RGPD, che consiste nel proteggere le persone contro i rischi specifici per i loro diritti e le loro libertà derivanti dal trattamento automatizzato di dati personali, compresa la profilazione*»⁸³⁰.

La Corte si avvia verso le conclusioni: forte della ricostruzione sistematica appena svolta, essa evidenzia che in una fattispecie come quella *de qua* «nelle quali sono coinvolti tre attori, sussisterebbe un rischio di elusione dell'articolo 22 dell'RGPD e, di conseguenza, una *lacuna nella protezione giuridica* qualora fosse accolta un'interpretazione restrittiva di tale disposizione, secondo la quale il calcolo del tasso di probabilità deve essere considerato *soltanto un atto preparatorio* e solo l'atto adottato dal terzo può, se del caso, essere qualificato

⁸²⁹ Ivi, punto 53.

⁸³⁰ Ivi, punto 57. La Corte attribuisce intende poi sottolineare ulteriormente il motivo per cui, tra le diverse specie di trattamento automatizzato, la disposizione menzioni proprio la profilazione: e, sempre dunque svolgendo considerazioni simili a quelle del Gruppo, cui lo stesso Avvocato si attiene, evidenzia nuovamente come l'idoneità della specie di trattamento medesimo a «compromettere i legittimi interessi e i diritti dell'interessato, in particolare tenendo conto dei potenziali effetti discriminatori» dalla medesima derivanti risulti valorizzato dallo stesso *considerando 71*, che individua in particolare il *proprium* e insieme i rischi configurati dalla medesima, ampiamente analizzati retro (ossia, in sintesi, il suo stesso identificarsi in una valutazione a fini di *analisi o di previsione* di aspetti personali relativi al rendimento professionale, la situazione economica, la salute ecc.)

come “decisione”, ai sensi dell’articolo 22, paragrafo 1, di tale regolamento»⁸³¹. Rilievo centrale è attribuito, ancora una volta sulla scorta delle riflessioni dell’Avvocato Generale, al fatto che accogliendosi un’interpretazione restrittiva «la persona interessata non potrebbe far valere, presso la società che fornisce informazioni commerciali che calcola il tasso di probabilità che la riguarda, il suo diritto di accesso alle informazioni specifiche di cui all’articolo 15, paragrafo 1, lettera h), del RGPD, in assenza di adozione di un processo decisionale automatizzato da parte di tale agenzia»; né tantomeno il terzo che adotta la decisione sulla richiesta di credito, anche qualora questa ricadesse nell’ambito di applicazione dell’art. 22, sarebbe in grado di fornire alcuna informazione supplementare⁸³².

Ultima questione da risolvere attiene allora alla potenziale ricorrenza di uno dei fondamenti di liceità eccezionali individuati dal par. 2, in concorso con il soddisfacimento del requisito delle «misure adeguate di tutela» di cui al par. 3. A tal proposito, ai presenti fini è sufficiente ricordare come il giudice del rinvio, se da una parte indicasse che l’articolo 31 del BDSG (rubricato «Protezione delle transazioni commerciali in caso di scoring [determinazione di punteggi di scoring] e di informazioni sulla solvibilità») avrebbe potuto costituire una «base giuridica nazionale» ai sensi dell’articolo 22, paragrafo 2, lettera b), dall’altra nutrisse «seri

⁸³¹ Ivi, punto 61. Cfr. il par. 47 delle Conclusioni dell’Avvocato Generale, in cui si legge: «(...) le considerazioni svolte *supra* mi sembrano indicare che il punteggio di scoring calcolato da un’agenzia di valutazione del credito e comunicato a un istituto finanziario *tende generalmente a predeterminare* la decisione di quest’ultimo quanto alla concessione o al diniego del credito all’interessato, cosicché si deve ritenere che detta presa di posizione rivesta un carattere puramente formale nel quadro del processo²⁰. Ne consegue che occorre riconoscere al punteggio di scoring stesso la natura di «decisione» ai sensi dell’articolo 22, paragrafo 1, del RGPD». E ancora, all’inizio del par. seguente «Una siffatta conclusione mi sembra ragionevole perché qualsiasi altra interpretazione rimetterebbe in discussione l’obiettivo che il legislatore dell’Unione persegue con la disposizione di cui trattasi, volta a proteggere i diritti degli interessati».

⁸³² Ivi, punto 63. Cfr. sul tema il par. 48 delle Conclusioni dell’Avvocato Generale.

dubbi quanto alla compatibilità di tale articolo 31 con il diritto dell'Unione».⁸³³ A tal riguardo, la Corte di Giustizia si limita a stabilire che «spetta al giudice del rinvio verificare se l'articolo 31 del BDSG possa essere qualificato come base giuridica che autorizza, ai sensi dell'articolo 22, paragrafo 2, lettera b), del RGPD, l'adozione di una decisione fondata esclusivamente su un trattamento automatizzato»; aggiungendo poi opportunamente che «qualora tale giudice dovesse giungere alla conclusione che detto articolo 31 costituisce una siffatta base giuridica, esso dovrebbe ancora verificare se le condizioni poste dall'articolo 22, paragrafi 2, lettera b), e 4, del RGPD e quelle di cui agli articoli 5 e 6 di tale regolamento siano soddisfatte nel caso di specie»⁸³⁴.

Pertanto, alla luce di tutto quanto rilevato e argomentato nelle motivazioni, la Corte risponde (soltanto) alla prima questione pregiudiziale, dichiarando che l'art. 22 par. 1 del GDPR debba essere interpretato nel senso che « il calcolo automatizzato, da parte di una società che fornisce informazioni commerciali, di un tasso di probabilità basato su dati personali relativi a una persona e riguardanti la capacità di quest'ultima di onorare in futuro gli impegni di pagamento costituisce un «processo decisionale automatizzato relativo alle persone fisiche», ai sensi di tale disposizione, qualora da tale tasso di probabilità dipenda in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale con tale persona da parte di un terzo, al quale è comunicato tale tasso di probabilità»⁸³⁵.

⁸³³ Ivi, punto p. 64 ss. in ordine all'intera ricognizione delle basi giuridiche eccezionali di cui al par. 2; in part., per il richiamo alla posizione prospettata dal giudice nazionale, p. 71.

⁸³⁴ Ivi, p. 72.

⁸³⁵ Ivi, p. 73 e dispositivo.

Svolgendo alcuni nostri rilievi conclusivi, possiamo innanzitutto affermare che, sul piano squisitamente tecnico, la decisione commentata esplicitamente rovescia la precedente ricostruzione fatta propria dalla Corte Suprema Federale tedesca nell'omonimo caso (solo nazionale) SCHUFA del 2014, secondo la quale il soggetto finale che utilizzi il punteggio di credito per decidere su una domanda di concessione del credito avrebbe garantito un coinvolgimento umano effettivo nell'adozione della decisione medesima⁸³⁶.

Appare poi ragionevolmente prevedibile che l'orientamento promosso dalla CGUE inciderà notevolmente sul modo in cui i giudici e i Garanti nazionali interpreteranno negli anni a venire l'intero subsistema normativo di cui all'art. 22, indipendentemente dalla singola tipologia di ADM rilevante nel caso di specie. Valicando i confini della decisione sul caso concreto, la pronuncia ambisce infatti a sancire un quadro di principi fondamentali, i quali concorrano a dipanare la matassa interpretativa che l'edificio in esame *storicamente* circonda. E nel farlo, la CGUE – occorre ribadirlo – sostanzialmente aderisce a quella corrente della dottrina che coltiva un approccio generale alla *data protection* di tipo *antropocentrico*, e che dunque l'autodeterminazione informativa valorizza quale *oggetto di un diritto fondamentale*⁸³⁷.

La sentenza non esprime, allora, solo una maggior consapevolezza della delicata realtà del *credit scoring* automatizzato. Essa, facendo propria la visione predetta, si pone come pietra angolare per la costruzione *anche* giurisprudenziale

⁸³⁶ V. *retro*, anche nota 801.

⁸³⁷ V. ampiamente *retro*, ma cfr. ancora una volta in generale sulla prospettiva “costituzionale” penetrata progressivamente nel panorama giurisprudenziale e istituzionale eurounitario, O. POLLICINO, «Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale», in *Federalismi.it*, in Comunicazione, media e nuove tecnologie, n. 3/2014; e soprattutto M. BASSINI, «La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali», in *Quad. cost.*, 2016, 588, che, come già ampiamente sottolineato *retro*, rileva il passaggio da una normativa europea sulla libera circolazione dei dati personali di impronta sostanzialmente “mercantilistica”, ad una diversa prospettiva legata principalmente alla tutela dei diritti fondamentali.

(attraverso l'autorità che di fatto connota il precedente interpretativo della Corte di Giustizia) di un sistema rafforzato di protezione dei diritti e delle libertà fondamentali della persona umana, rispetto al fenomeno oggi tra i più capaci di compromettere la *dignità* della persona umana, di cui la libertà di determinarsi nelle proprie scelte esistenziali senza indebite (e imperscrutabili) interferenze costituisce indefettibile presupposto: la tecnologia algoritmica, e segnatamente i sistemi di *automated data processing & decision making*, quali espressioni tra le più *privacy-invading* della prima. A dimostrazione, ancora una volta, del nesso indissolubile che corre tra progresso tecnologico, vulnerabilità – crescente - della sfera privata ed attitudine evolutiva del diritto. Diritto (positivo) che tuttavia, finché non penetra nella prassi giudiziaria, resta muto e in-effettivo. La pronuncia in questione, finalmente, potrebbe innescare quel circolo virtuoso che *veramente* consenta alle disposizioni in precedenza esaminate di raggiungere i propri scopi: ovvero, con le stesse parole della Corte, di «proteggere le persone contro i rischi specifici per i loro diritti e le loro libertà derivanti dal trattamento automatizzato di dati personali, compresa la profilazione»⁸³⁸. E di conservare (il più possibile) in capo all'umano il controllo, e la costruzione, della propria identità⁸³⁹.

Certo la sentenza non scioglie tutti i dubbi interpretativi. Non si esprime, ad esempio, chiaramente sulla configurabilità o meno di un *right to expalantion* ai sensi del sub-sistema normativo di cui all'art. 22 e alle altre disposizioni coinvolte. Ma, verrebbe da dire, ciò esulava dal perimetro del *petitum*. La sentenza in parola, d'altronde, ha solo sciolto gli ormezzi: l'esperienza giurisprudenziale in materia di sistemi decisionali algoritmici è appena cominciata.

⁸³⁸ C. Giust. UE 7.12.2023, causa C-634/21, *OQ contro Land Hessen*, punto 57.

⁸³⁹ Cfr. ancora una volta S. RODOTÀ, *Il diritto di avere diritti*, cit., in particolare p. 318 ss; e R. MESSINETTI, «Privacy e controllo dell'identità algoritmica», p. 125 ss.

3.3. Uno sguardo all'Italia. La trasparenza algoritmica nella giurisprudenza della Corte di Cassazione e del Consiglio di Stato

A conclusione del presente capitolo, in ottica comparatistica, rivolgiamo lo sguardo alla disciplina dei trattamenti automatizzati nell'ambito dell'ordinamento giuridico italiano. Cercheremo, in particolar modo, di indagare il livello di “penetrazione” dell'impianto normativo in materia di sistemi interamente algoritmici edificato dalle disposizioni comunitarie di cui ci siamo occupati nei precedenti paragrafi in primo luogo nella giurisprudenza di legittimità; e, in secondo luogo, negli orientamenti e nelle decisioni del Garante nazionale per la protezione dei dati personali.

Preliminarmente, è doveroso ricordare che il legislatore nazionale, al fine di provvedere all'adeguamento del quadro normativo interno al Regolamento 2016/679 UE, ha adottato la legge n. 163 del 2017, il cui art. 13 ha delegato il Governo ad adottare uno o più decreti legislativi volti ad abrogare espressamente le disposizioni del c.d. Codice della Privacy incompatibili con quelle del GDPR, a modificare il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni *non direttamente applicabili* contenute nel regolamento e a coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni adottate in sede europea. Parallelamente, la delega contemplava l'adeguamento del sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento con previsione di sanzioni penali e amministrative

efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse⁸⁴⁰.

In attuazione della delega in parola, il Governo ha dunque emanato il già citato decreto legislativo n. 101 del 2018⁸⁴¹: cosicché la nuova normativa sulla protezione dei dati personali vigente in Italia risulta dalle norme del GDPR, direttamente applicabili (ed efficaci), nonché dalle residue disposizioni del Codice della Privacy così come riformato dal d.lgs. n. 101/2018, le quali integrano la disciplina prevista dalle disposizioni del Regolamento il cui contenuto dispositivo risulti incompleto e, in presenza di *clausole di apertura*, dettano una disciplina derogatoria o altrimenti più stringente rispetto a quella articolata dalle prime⁸⁴².

Ulteriori modifiche al previgente Codice della Privacy ed altre disposizioni in materia di *data protection* sono state apportate dall'articolo 9 del decreto-legge n. 139 del 2021, poi convertito con modificazioni dalla L. 3 dicembre 2021, n. 205.

Si ricorda anche che il decreto legislativo n. 51 del 2018, attuativo della delega contenuta negli artt. 1 e 11 della già citata legge n. 163 del 2017, ha contestualmente attuato la già più volte citata Direttiva 2016/680 sulla *Data Protection and Law Enforcement*.

⁸⁴⁰ V. l. 25 ottobre 2017, n. 163, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017». (17G00177) (GU Serie Generale n.259 del 06-11-2017)

⁸⁴¹ V. D.lgs., 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)», cit.

⁸⁴² Un esempio di quest'ultima può essere individuato nel disposto del nuovo articolo 2-sexies del Codice, che attuando la clausola di cui all'art. 9, par. 2 lett. g) del Reg., disciplina il trattamento delle categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante, consentendolo (in sintesi) solo in presenza di un fondamento legislativo o regolamentare che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante.

Gli interventi sinteticamente ripercorsi hanno letteralmente rivoluzionato l'originaria architettura del sistema normativo in materia di protezione dei dati personali vigente nel nostro paese, e prima ancora, ovviamente, quella del Codice che, come ricordato nel corso della trattazione, al momento della sua introduzione edificava l'«ordinamento della protezione dei dati personali in Italia». Oggi, stante l'intervento della fonte regolamentare, quanto meno la disciplina generale del trattamento dei dati personali scaturisce essenzialmente dal diritto comunitario direttamente applicabile (nonché, per lo più, direttamente efficace), in tutti gli Stati membri.

Come abbiamo notato, tuttavia, lo stesso GDPR prevede alcune disposizioni che offrono la possibilità agli Stati membri di prevedere *norme nazionali supplementari*, più rigorose ovvero a carattere derogatorio, che lasciano a questi ultimi un margine di discrezionalità circa il modo in cui tali disposizioni possono essere attuate («clausole di apertura»), a condizione (come la giurisprudenza ha sottolineato) che dette norme non pregiudichino il contenuto e gli obiettivi del GDPR.

Ebbene, l'art. 22, la cui analisi ha ampiamente occupato i paragrafi che precedono, come sappiamo prevede, al par. 2 lett. b), che i processi decisionali altrimenti vietati *ex par. 1* possano eccezionalmente svolgersi laddove autorizzati dal diritto dell'Unione o dello Stato membro cui il titolare appartenga, *a condizione* che il diritto medesimo «precis[i] altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato». Pertanto, in punto di *suitable safeguards*, gli Stati membri godono del relativo margine di discrezionalità cui abbiamo fatto cenno. Nonostante ciò, è importante sottolineare come l'Italia ricada tra i paesi che sul punto *non* si sono avvalsi della clausola di

apertura in parola, non introducendo a livello legislativo alcun caso di «*permitted decision making*» automatizzato di cui all'art. 22, par. 2 lett. b)⁸⁴³.

Da ciò non può che derivare come la (ancora esigua) giurisprudenza che nel nostro ordinamento si sia espressamente confrontata con il fenomeno dei processi decisionali interamente automatizzati abbia potuto (e dovuto) fare riferimento solo ed esclusivamente alla disciplina dettata dall'art. 22 e dalle altre disposizioni del GDPR comprese nel *sub-sistema normativo* di cui abbiamo parlato. Allo stesso tempo, occorre premettere che nel vigore della precedente disciplina la disposizione del Codice della Privacy che provvedeva al recepimento e all'attuazione dei principi di cui all'art. 15 della Direttiva 95/46/CE, prodromo dell'attuale articolo 22 del GDPR (con tutte le fondamentali differenze di cui abbiamo ampiamente discusso), fosse l'art. 14, rubricato «Definizione di profili e della personalità dell'interessato», ed oggi chiaramente abrogato⁸⁴⁴.

Spostandoci effettivamente sul piano della giurisprudenza, ribadiamo che le pronunce, innanzitutto di merito, che si occupino in senso stretto della liceità dell'impiego di sistemi decisionali interamente automatizzati non sono ancora molte. Ci sembra che tale scenario dipenda da un duplice ordine di ragioni. Da una parte, rileva la circostanza che la norma di cui all'art. 22 – lo ribadiamo – sia relativamente “giovane” (il Regolamento è entrato in vigore solo nel maggio del

⁸⁴³ Cfr. chiaramente sul punto G. MALGIERI, «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», cit.

⁸⁴⁴ V. l'originario art. 14 del d.lgs. 196/2003, cit., che così recitava: «1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato. 2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17».

2018). Dall'altra, si deve sottolineare come la maggior parte delle controversie in materia di *data protection* e di *data breach*, pur confrontandosi necessariamente con il trattamento algoritmico dei dati personali, abbiano piuttosto ad oggetto la sussistenza di uno dei fondamento di liceità del trattamento legalmente previsti. L'attenzione degli operatori del diritto (ancora non del tutto provvisti in linea generale, sia consentito dirlo, di un'appropriata *educazione digitale*), insomma, raramente si concentra sulla natura, o sulla qualità che dir si voglia, del trattamento medesimo. Altrimenti, più spesso di quanto attualmente accada, gli operatori riscontrerebbero nella fattispecie con cui si confrontino un processo decisionale di cui all'art. 22; e conseguentemente, con più frequenza, invocherebbero l'esercizio della funzione giurisdizionale per censurare l'illiceità del processo medesimo per violazione del divieto di cui al par. 1, in virtù del difetto delle *rigorose eccezioni* contemplate dal par. 2 del medesimo articolo.

Detto ciò, nel panorama giurisprudenziale italiano è possibile riscontrare alcuni importanti approdi della giurisprudenza civile ed amministrativa in materia di processi decisionali automatizzati, particolarmente rilevanti nella misura in cui tutti si occupano del delicato profilo relativo alla *inconoscibilità degli schemi essenziali del sistema algoritmico* (o, anche, *black box*). Pronunce le quali, di conseguenza, si interrogano e contestualmente sanciscono importanti principi in punto di trasparenza del processo di trattamento dei dati personali e di *decision making* algoritmico.

Principiamo dalla fondamentale, nonché recente ordinanza n. 14381/2021 con cui la I Sezione civile della Suprema Corte di Cassazione ha statuito sulla validità del consenso reso dall'utente che non sia venuto preventivamente a

conoscenza dello schema esecutivo di un algoritmo⁸⁴⁵. Assai rilevante, lo si sottolinea già, appare come i fatti di causa sottostanti al ricorso proposto dal Garante per la Protezione dei Dati Personali avverso la sentenza resa dal Tribunale di Roma concernessero l'impiego da parte del resistente di un sistema automatizzato preordinato all'elaborazione di profili reputazionali degli utenti.

Nel cassare la sentenza, la Corte afferma il fondamentale principio di diritto in forza del quale «in tema di trattamento di dati personali, il consenso è validamente prestato *solo se* espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati»⁸⁴⁶.

Prima di addentrarci nell'analisi dei fatti da cui prende origine la sentenza, e del suo contenuto essenziale, occorre sottolineare come la causa, pur inscrivendosi nell'attuale dibattito che anima le istituzioni europee e che ha determinato la configurazione dell'art. 22, è insorta nel vigore della precedente disciplina (la causa ha, difatti, avuto inizio nel 2016, quando il GDPR non era ancora in vigore). Pertanto, ai fini della soluzione della controversia la Corte ha dovuto applicare, in combinato disposto tra loro, le disposizioni (per lo più interne) che la dir. 95/46/CE attuavano. Tuttavia - e qui sta tutta l'importanza della decisione -, come alcuni commentatori hanno osservato la Cassazione, pur applicando la disciplina previgente, ha ivi chiaramente affermato e sancito alcuni

⁸⁴⁵ V. Cass. Civ., sez. I, ordinanza n. 14381/21, depositata il 25 maggio 2021.

⁸⁴⁶ Ivi, punto VIII, p. 8.

dei principi fondamentali che informano le nuove disposizioni europee in materia di protezione dei dati personali e di *governance* dell'intelligenza artificiale, compreso l'art. 22: in ciò anticipando alcuni profili dello stesso *leading case* in ambito europeo, ovvero il caso *SCHUFA*, approfonditamente commentato nel paragrafo precedente⁸⁴⁷.

Venendo all'analisi dei fatti di causa, la vicenda prendeva avvio dal Provvedimento n. 488 del 24 novembre 2016 con cui l'Autorità Garante per la Protezione di Dati Personali aveva considerato illecita la piattaforma predisposta dall'Associazione Mevaluate Onlus a causa della forte incidenza del servizio sulla dignità dei soggetti interessati⁸⁴⁸. Dalla documentazione offerta in comunicazione a suo tempo dall'Associazione, titolare del trattamento, risultava che la piattaforma fosse preordinata ad erogare un servizio di “qualificazione reputazionale”, e pertanto constasse in un sistema di raccolta, verifica, ed elaborazione di dati personali con una successiva fase di assegnazione di «indicatori alfanumerici asseritamente in grado di misurare l'affidabilità reputazionale dei soggetti censiti (persone fisiche e giuridiche)»⁸⁴⁹. L'Autorità si soffermava pertanto sulle ripercussioni potenzialmente pregiudizievoli di un trattamento siffatto sulla vita non solo professionale, bensì soprattutto privata dei soggetti i cui dati fossero oggetto di elaborazione algoritmica, fossero essi clienti, dipendenti o candidati di varia specie, «in considerazione del fatto che la “reputazione” che si vorrebbe qui misurare, in quanto strettamente correlata alla considerazione delle persone e alla loro stessa “proiezione” sociale, risulta

⁸⁴⁷ G. SCORZA, «L'algoritmo deve essere trasparente, la Cassazione rilancia il GDPR», in *Agenda Digitale*, 26 maggio 2021.

⁸⁴⁸ V. Provv. n. 488 del 24 novembre 2016, Autorità Garante per la Protezione dei Dati Personali, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5796783>.

⁸⁴⁹ Ivi, punto 1.8 e 2.1.

intimamente connessa con la loro dignità, elemento cardine della disciplina di protezione dei dati personali»⁸⁵⁰. L’Autorità, alla luce di queste considerazioni, aveva disposto, ex art. 154 co. 1 lett. d) del citato d.lgs. n. 196 del 2003, il divieto di qualunque operazione di trattamento dei dati personali (presente e futura) effettuata dall’Associazione nell’ambito della piattaforma medesima.

L’Associazione adiva il Tribunale di Roma chiedendo l’annullamento del provvedimento. Con parziale accoglimento del ricorso, il giudice di merito accoglieva l’istanza di parte ricorrente facendo salva la portata del provvedimento solamente per un particolare ambito del servizio: il c.d. “Profilo Contro”, ovvero soggetti terzi non associati a Mevaluate Onlus. Il Garante, allora, impugnava la sentenza con ricorso diretto davanti alla Suprema Corte.

Il supremo giudice di legittimità, nella sentenza, articola una sintetica e tuttavia lucida ed efficace motivazione a suffragio della decisione di cassare la sentenza, accogliendo i principali motivi del gravame.

La Corte riscontra nella motivazione del giudice di merito un cortocircuito logico-giuridico rappresentato dal fatto che, nel sostenere la liceità parziale del trattamento, esso valorizzasse in maniera preponderante il diritto d’iniziativa economica privata, in cui ricadrebbe la libertà di predisporre e di utilizzare sistemi di accreditamento “reputazionale” di soggetti, mancando di valutare la condizione necessaria cui risulta subordinata l’erogabilità di un servizio siffatto: la validità del consenso e la conseguente liceità del trattamento su cui esso si basa⁸⁵¹. Il rilievo oggi, come sappiamo, troverebbe fondamento normativo nell’art. 6 par. 1 lett. A) del GDPR. Ma già al tempo in cui insorse la controversia tale fondamento si identificava nell’ancora vigente art. 23 del Codice della Privacy, che sulla base della dir. 95/46/CE individuava anch’esso il consenso quale fondamento generale di liceità del trattamento dei dati personali, specificando come esso dovesse essere

⁸⁵⁰ Ivi, punto 2.2.

⁸⁵¹ Cass. Civ., sez. I, ordinanza n. 14381/21, p. 5 ss.

valido: validità che, in particolare, il terzo comma subordinava al fatto che esso fosse «espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato» nonché «documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13»⁸⁵². L'interpretazione fornita dalla Corte, come vediamo subito, risulta profondamente innervata della consapevolezza dei rischi configurati in punto di autodeterminazione individuale dall'attuale *società degli algoritmi*, e dunque consonante con i principi sanciti dalla nuova normativa ed illuminati dalle stesse indicazioni del Gruppo di Lavoro delle linee guida 5/2020 sul consenso, cui abbiamo già fatto riferimento.

Il menzionato terzo comma, in particolare con l'espressione «chiaramente individuato», presuppone che «il consenso debba essere previamente informato in relazione ad un trattamento ben definito nei suoi elementi essenziali», affinché possa dirsi che sia stato espresso, in quella prospettiva, *liberamente e specificamente*: la consapevolezza, insomma, risulta coesistente ai primi due requisiti menzionati. È poi, aggiunge la Corte, «onere del titolare del trattamento fornire la prova l'accesso e il trattamento contestati siano riconducibili alle finalità» per le quali il consenso (valido) sia stato richiesto ed ottenuto⁸⁵³. Ebbene, nel contesto in esame, tra i principali elementi suscettibili di incidere sulla consapevolezza, e conseguentemente sulla specificità e dunque sulla libertà della manifestazione di volontà positiva, ricadono necessariamente gli «elementi implicati e considerati dall'algoritmo» su cui il trattamento profilazione

⁸⁵² V. art. 23, oggi abrogato, del d.lgs. n. 196/2003 cit. Rubricato «consenso», recitava: «1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. 2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. 3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13. 4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.» Cfr. Anche la giurisprudenza richiamata sul punto dalla Corte, ossia ex multis, Cass. n. 17278-18, Cass. n. 16358-18.

⁸⁵³ Cass. Civ., sez. I, ordinanza n. 14381/21, punto IV, p. 6.

“reputazionale” si fonda: centrale è quindi, secondo la Corte, la trasparenza dell’algoritmo medesimo, non sufficientemente considerata dal giudice di merito che, assegnando al mercato -in senso metaforico inteso come luogo di libero scambio- la funzione di determinare la bontà o meno dei risulti del suo impiego, ha ritenuto la validità della formula subordinata al solo «momento valutativo del procedimento»⁸⁵⁴. È invece proprio la «scarsa trasparenza» dell’algoritmo impiegato, con tutti i dubbi relativi al «sistema automatizzato di calcolo per la definizione del *rating* reputazionale» a risultare, per la Corte, decisiva ai fini della validità del consenso, e conseguentemente della liceità del trattamento stesso: se l’interessato ignora l’esistenza di tale sistema, l’*input* di cui si nutre e il modello essenziale di funzionamento (nell’elaborare i dati medesimi ai fini della creazione del profilo), il consenso non può dirsi affatto informato⁸⁵⁵. Con le parole della Corte, «non può logicamente affermarsi che l’adesione [s’intende, generica] ad una piattaforma da parte dei consociati comprenda *anche* l’accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano reso conoscibili lo schema esecutivo dell’algoritmo e gli elementi all’uopo necessari»⁸⁵⁶.

Conseguenzialmente, la Corte cassa la sentenza con rinvio al giudice di primo grado, prescrivendone l’uniformazione al principio che abbiamo enunciato in apertura del nostro commento, e di cui merita ancora sottolineare questo passaggio: in una fattispecie come quella che sostanzia i fatti di causa, «il requisito di consapevolezza [da cui dipende la validità del consenso al trattamento] non può considerarsi soddisfatto ove lo schema esecutivo dell’algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati»⁸⁵⁷.

⁸⁵⁴ Ivi, punto VII, p. 7.

⁸⁵⁵ *Ibidem*.

⁸⁵⁶ Ivi, punto VII, p. 7-8.

⁸⁵⁷ Ivi, punto VIII, p. 8.

La sentenza nel suo complesso, tanto sotto il profilo della motivazione quanto sotto il profilo del principio di diritto che la Corte ivi enuclea, appare importante per diverse ragioni, che non attengono soltanto alla portata “innovativa” nel contesto della disciplina previgente, e dunque all’indubbia idoneità a preparare il terreno ai fini di una chiara applicazione dell’impianto normativo del GDPR.

In primo luogo, la pronuncia si sofferma sulle criticità in sé e per sé legate all’impiego di strumenti algoritmici per la definizione di un *rating* di persone fisiche e giuridiche. Di più, essa, nello specifico, si focalizza sul requisito della consapevolezza nella prestazione del consenso - da cui dipendono essenzialmente la sua stessa libertà e specificità - che appare necessariamente *rafforzato* a fronte di trattamenti *anche solo parzialmente algoritmici*: oggetto dell’indagine della Corte risulta infatti precipuamente quell’opacità, o «scarsa trasparenza», che inevitabilmente condiziona il presupposto in parola nel momento in cui ci si avvalga di un algoritmo per la valutazione di dati personali; e, conseguentemente, l’effettiva conoscibilità dello schema esecutivo dell’algoritmo impiegato⁸⁵⁸.

Volendo calare il principio nell’attuale sistema normativo predisposto dal GDPR, dalle motivazioni articolate dalla Corte sembra si possa dedurre che all’integrazione del requisito della consapevolezza presieda indefettibilmente la

⁸⁵⁸ Profilo che, a dimostrazione della sua contemporanea rilevanza, costituisce anche oggetto della Direttiva (UE) 2019/2161 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell’Unione relative alla protezione dei consumatori. Tuttavia, a dimostrazione della prospettiva piuttosto mercantilista, preordinata a massimizzare l’esercizio delle libertà fondamentali su cui si fonda il Mercato Interno, il considerando 23 osserva che: «(...) I professionisti non dovrebbero essere obbligati a comunicare il funzionamento dettagliato dei loro meccanismi di classificazione, compresi gli algoritmi. Essi dovrebbero fornire una descrizione generale dei principali parametri di classificazione che determini i principali parametri predefiniti da essi utilizzati e l’importanza relativa di tali parametri rispetto ad altri parametri, ma tale descrizione non deve necessariamente essere fornita individualmente per ogni ricerca effettuata».

chiara indicazione, nell'informativa dettagliata che il titolare ha l'obbligo di redigere e di sottoporre al -potenziale- interessato, dell'impiego dell'algoritmo medesimo e dei suoi elementi essenziali, *indipendentemente* dal fatto che l'algoritmo governi l'intera elaborazione e che la decisione conseguente si basi esclusivamente su di esso. E laddove si intendesse coraggiosamente estenderne la portata in funzione applicativa, valorizzandone la componente "personalistica", dal principio in parola potrebbe quasi inferirsi un obbligo per il titolare - e uno speculare diritto dell'interessato -, a fronte di qualsiasi tipo di trattamento algoritmo, a ricevere informazioni significative *ex ante*, non solo relative all'utilizzo del sistema siffatto, ma anche riguardanti la logica generale (lo schema essenziale che presiede al procedimento logico-inferenziale svolto dalla macchina per suo tramite) che ne caratterizza il funzionamento⁸⁵⁹.

La Corte, insomma, si confronta con il tema dell'effettiva sussistenza di quei requisiti indefettibili ai fini di un consenso qualificabile come *fondamento di liceità* di un trattamento, e a maggior ragione algoritmico, di dati personali: libertà, specificità e consapevolezza. Requisiti, ormai lo sappiamo, che debbono connotare la formazione della volontà dell'interessato affinché sia garantita effettivamente l'autodeterminazione informativa della persona medesima. Ebbene, com'è stato acutamente notato, le riflessioni di ordine etico, filosofico e giuridico che circondano questo tema conducono a interrogarsi in modo più approfondito sulle condizioni di validità del consenso quando raccolto «per sottoporre i dati personali dell'interessato a un *ranking* reputazionale tramite un

⁸⁵⁹ Informazioni significative sulla logica utilizzata, sulle conseguenze e sull'importanza che il Regolamento esplicitamente, come abbiamo visto apporofonditamente (sottolinenando tutti i nodi interpretativi che tali concetti circondano e dividono la dottrina), per ora individua come contenuto dell'obbligo di informazione e del relativo diritto di accesso solo in materia di processi decisionali interamente automatizzati di cui all'art. 22.

sistema automatizzato», e dunque sui «necessari *quid pluris* per la formazione di un consenso reso consapevolmente» in tali circostanze⁸⁶⁰.

Tutti le considerazioni qui svolte devono, tuttavia, confrontarsi con alcune domande fondamentali: la generalità dei consociati è in grado di comprendere, anche se menzionati nell'informativa, gli elementi essenziali che caratterizzano lo schema esecutivo dell'algoritmo? Gli operatori del diritto, avvocati o giudici che siano, sono in grado di ricondurre ad un coerente sistema di categorie giuridiche, di principi normativi e di regole di dettaglio - attraverso l'interpretazione della lettera (talvolta *anacronistica*) della legge guidata dagli sforzi ermeneutici degli studiosi - la complessa realtà tecnologica (l'«autonomo ordine sociale e giuridico delle macchine») con cui la personalità umana ogni giorno dialoga? L'introduzione degli algoritmi nell'agire individuale e sociale, non ancora sostenuto da un'adeguata educazione tecnologica dei suoi attori, privati o pubbliche amministrazioni che siano, non rischia di rendere i primi, piuttosto che lo strumento, la *mente* dell'agire medesimo?⁸⁶¹

Sul punto, possiamo richiamare alcune riflessioni già svolte alcune pagine indietro: senza l'integrazione dei principi a protezione dei dati personali già nella *progettazione* dell'architettura informatica, hardware e software, che “ospita” i

⁸⁶⁰ F. PAOLUCCI, «Consenso, intelligenza artificiale e privacy». Commento a: Corte di Cassazione, sez. I Civ. – 25/05/2021, n. 14381, in *Media Laws*, 16 giugno 2021, https://www.medialaws.eu/consenso-intelligenza-artificiale-e-privacy-commento-a-corte-di-cassazione-sez-i-civ-25-05-2021-n-14381/#_ftn3.

⁸⁶¹ A tal riguardo, eloquente risulta il rapporto annuale europeo sul c.d. *digital divide* del 2022, che, nell'occuparsi dell'Italia, pur evidenziando come «la maggior parte delle piccole e medie imprese italiane (il 60%) ha raggiunto almeno un livello base di intensità digitale; l'utilizzo di servizi *cloud*, in particolare, ha registrato una considerevole crescita», dall'altra sottolinea in modo preoccupante come «ancora oggi oltre la metà dei cittadini italiani non dispone neppure di competenze digitali di base. La percentuale degli specialisti digitali nella forza lavoro italiana è inferiore alla media dell'UE e le prospettive per il futuro sono indebolite dai modesti tassi d'iscrizione e laurea nel settore delle TIC». Cfr. COMMISSIONE EUROPEA, *Digital Economy and Society Index (DESI) 2022*, disponibile qui: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>.

trattamenti algoritmici, e dunque senza lo sfruttamento di tutte le potenzialità intrinseche nell'applicazione del principio di *privacy by design*, la trasparenza (con tutti i problemi semantici che tale concetto, inoltre, dischiude) non è in grado, da sola, di presidiare la libertà di autodeterminazione dell'individuo, e dunque la capacità di quest'ultimo di costruire senza indebite interferenze la propria personalità. La trasparenza non è una panacea⁸⁶².

Le domande che ci siamo poc'anzi posti rendono opportuna una sintetica indagine sulle posizioni della giurisprudenza amministrativa in punto di trattamenti algoritmici (e, segnatamente, di trasparenza algoritmica).

Nel processo di ampio sviluppo della digitalizzazione all'interno della Pubblica Amministrazione, che dal 2005 ha visto il legislatore impegnato nell'introdurvi l'uso delle tecnologie informatiche come strumento privilegiato nella gestione dell'attività amministrativa⁸⁶³, recentemente si è assistito all'ulteriore implementazione degli stessi sistemi algoritmici, e in definitiva dell'IA, nell'ambito dei procedimenti amministrativi medesimi⁸⁶⁴.

La tecnologia dell'algoritmo trasforma la fisionomia della Pubblica Amministrazione, laddove da mero supporto nella fase istruttoria di raccolta e organizzazione dei dati questi sono utilizzati talora anche in sostituzione del

⁸⁶² Per questi rilievi v. *retro*, par. 3.2., dove si analizza più nello specifico l'applicazione del principio di trasparenza in materia di processi decisionali interamente automatizzati. Cfr. poi ancora una volta L. EDWARDS E M. VEALE, «Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For», in *Duke Law & Technology Review*, 16, 2017, 18-84.

⁸⁶³ Cfr. gli obiettivi delineati dall'Art 3-bis comma 1 della Legge n.241/1990 così come introdotto dall'art. 12, comma 1, lettera a) della Legge n. 120 del 2020.

⁸⁶⁴ Cfr. per alcuni importanti rilievi sul punto CATERINA BO, «La carente disciplina sull'uso degli algoritmi nella PA: come interviene il giudice amministrativo?», in *Media Laws*, 7 ottobre 2021, <https://www.google.com/search?client=safari&rls=en&q=La+carente+disciplina+sull%E2%80%99uso+degli+algoritmi+nella+PA%3A+come+interviene+il+giudice+amministrativo%3F&ie=UTF-8&oe=UTF-8>; A. G. PARISI, «Illiceità del trattamento dei dati personali e rimedi», in P. Stanzione (a cura di), *I “poteri privati” delle piattaforme*, cit., p. 272 ss;

pubblico funzionario al momento dell'assunzione del definitivo provvedimento: tant'è che gli interpreti discorrono già da qualche anno di «Amministrazione 4.0»⁸⁶⁵.

Tale circostanza ha fatto prepotentemente emergere come attuale la questione circa la compatibilità dell'utilizzo dei sistemi algoritmici e di IA medesimi con numerosi principi di diritto amministrativo, e segnatamente di quelli consacrati nell'art. 97 della Costituzione (imparzialità e buon andamento della Pubblica Amministrazione), e declinati con precipuo riferimento al procedimento amministrativo dalla legge n. 241/1990, come negli anni interpretati in funzione applicativa dalla giurisprudenza di merito e di legittimità⁸⁶⁶.

La tematica è complessa e non potrà qui chiaramente costituire oggetto di analisi diffusa. Ai nostri fini, tuttavia, si intende evidenziare le tre linee fondamentali emerse in seno alla giurisprudenza (ciascuna supportata da diversi indirizzi dottrinali).

Le prime due appaiono (verrebbe da dire) “radicali” nello stigmatizzare o piuttosto nel celebrare il ricorso all'*Algorithmic Decision Making* nell'esercizio dell'attività amministrativa (vincolata, ma anche discrezionale). La terza, invece, lo si anticipa, sembra orientata a superare la dicotomia predetta, con un approccio di “moderata apertura” (che pare, in effetti, il più ragionevole): orientamento che, lo si anticipa, pare oggi prevalente, nonché consacrato in una fondamentale sentenza del Consiglio di Stato che ha sancito un “quadro” di principi di

⁸⁶⁵ Cfr. D. U. GALETTA, J. C. CORVOLAN, «Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto», in *Federalismi.it*, 2019.

⁸⁶⁶ Oltre ai contributi suddetti, per alcune considerazioni di sistema cfr. la trascrizione integrale dell'intervento al corso di formazione per Magistrati organizzato dall'Ufficio studi, massimario e formazione della Giustizia amministrativa, M. CORRADINO, *Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future*, 10 settembre 2021.

riferimento in relazione all'utilizzo della tecnologia algoritmica nel rapporto procedimentalizzato tra potere pubblico e individuo, e pertanto alla cui osservanza risulterebbe subordinata la legittimità del provvedimento conclusivo del procedimento così svolto⁸⁶⁷.

Da una parte, si riscontra nella giurisprudenza amministrativa una frangia sostanzialmente diffidente all'integrazione dell'Intelligenza Artificiale nel quadro dell'attività procedimentalizzata della P.A., il cui indirizzo trova ad esempio espressione in quella pronuncia del T.A.R. del Lazio in cui si evidenzia come tra le preoccupazioni principali campeggi «l'abdicazione da parte del responsabile del procedimento del suo ruolo di timoniere ed anche di correttore» del procedimento amministrativo⁸⁶⁸. Sulla stessa linea si colloca un'altra, di poco più risalente decisione del medesimo organo, che interviene in una vicenda riguardante una procedura di mobilità avviata dal MIUR, la quale disponeva i trasferimenti dei docenti immessi in ruolo in fascia C senza tener conto delle loro preferenze espresse nelle domande inoltrate. Nel quadro della sentenza, il T.A.R. del Lazio ammette che la procedura automatizzata, *non prevedendo la motivazione dei provvedimenti adottati*, non garantisce la partecipazione del cittadino al procedimento amministrativo, cosicché la decisione adottata attraverso l'uso di algoritmi non sarebbe conforme alla disciplina dettata dalla l. n. 241/1990, stante (oltre alla carenza di motivazione) la sua inidoneità a soddisfare i principi di trasparenza e di partecipazione al procedimento; e ciò *indipendentemente* dalla circostanza che il procedimento sia connotato da una

⁸⁶⁷ Si fa già riferimento a Cons. Stato Sez. VI, Sent., 13-12-2019, n. 8472 in www.giustizia-amministrativa.it

⁸⁶⁸ T.A.R. Lazio-Roma, sez. III, sentenza n. 4409 del 15 aprile 2021.

forte standardizzazione, e pertanto costituisca esercizio di poteri amministrativi interamente vincolati ⁸⁶⁹.

Dall'altra, si individua invece quell'orientamento che guarda con favore la scelta metodologica della digitalizzazione e del ricorso all'ADM *anche* nella redazione dell'atto finale, in quanto pienamente conforme ai principi di ragionevolezza e logicità ed apprezzabile non solo in termini di efficacia e di efficienza, ma anche per il surplus di certezza che consente di perseguire la parità di trattamento⁸⁷⁰. Esso trova sbocco in alcune affermazioni dello stesso Consiglio di Stato secondo cui, almeno nei procedimenti seriali e standardizzati, in cui si articola l'esercizio di poteri amministrativi strettamente vincolati e che implicano l'elaborazione di grandi quantità di dati, «la regola tecnica che governa ciascun algoritmo resta pur sempre una regola amministrativa generale, costruita dall'uomo (...) per essere poi (solo) applicata [dalla macchina] anche se ciò avviene in via esclusiva», di modo che, in tali contesti, la decisione automatizzata andrebbe incoraggiata comportando «la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità» e «l'esclusione di interferenze dovute a negligenza [o peggio dolo] del funzionario [essere umano]». ⁸⁷¹

⁸⁶⁹ T.A.R., Lazio – Roma, Sezione III Bis, Sentenza 10-13 settembre 2019, n. 10964.

⁸⁷⁰ Cfr. ad es. T.A.R. Lazio, Roma, Sez. III-bis, 22 marzo 2017, n. 3769.

⁸⁷¹ Cons. Stato, Sez. VI., 8 aprile 2019, n. 2270. Per quanto nella suddetta sentenza si considera la regola algoritmica un mero atto informatico, la pronuncia limita le aperture ai soli casi, come abbiamo detto, di attività strettamente vincolata e standardizzata, e fissa comunque gli importanti principi secondo cui la P.A., ai fini del rispetto dei principi di imparzialità e di buon andamento costituzionalmente sanciti, deve costantemente perfezionare l'algoritmo utilizzato e renderlo pienamente conoscibile in sé. Tant'è che la sentenza in esame statuisce in realtà l'annullamento dell'atto impugnato, in quel caso concreto, per violazione dei principi di imparzialità, pubblicità e trasparenza. Così, di fatto, la sentenza medesima getta le basi per la sentenza “decalogo” n. 8472, che andremo ad esaminare, che stabilisce principi precisi alla cui osservanza è subordinata la legittimità di qualsiasi tipologia di procedimento amministrativo che coinvolga l'impiego di algoritmi nelle sue diverse fasi, anche dunque di quelli discrezionali.

La terza (e forse, più ragionevole) tendenza che si riscontra nella giurisprudenza amministrativa degli ultimi anni è quella che accetta l'esistenza degli algoritmi, ne ammette l'utilizzazione nell'azione amministrativa e prova, piuttosto, a contenerne l'operato a tutela dei diritti degli individui che possano esserne investiti.

Tale orientamento si rinviene ad esempio nella sentenza del 4 febbraio 2020 n. 881 cui la Sezione VI del Consiglio di Stato⁸⁷². L'organo di ultima istanza della Giustizia Amministrativa considera preliminarmente che «non vi sono ragioni di principio, ovvero concrete, per limitare l'utilizzo [dell'algoritmo] all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse». Nel decidere sul gravame, il collegio valorizza precipuamente la dimensione della tutela dei diritti -specialmente, fondamentali- dei cittadini in quanto destinatari del provvedimento, affermando che «ai fini dell'ammissibilità del ricorso ad algoritmi informatici nel procedimento di formazione della decisione amministrativa, assumono rilievo fondamentale, anche alla luce della disciplina di origine sovranazionale, due aspetti preminenti, quali elementi di minima garanzia per ogni ipotesi di utilizzo di algoritmi in sede decisoria pubblica: a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati; b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo»⁸⁷³.

⁸⁷² Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881. Per una nota di commento alla sentenza, cfr. A. VALSECCHI, «Algoritmo, discrezionalità amministrativa e discrezionalità del giudice» (nota a Cons. Stato, sez. VI, sent. del 4 febbraio 2020, n. 881), in *Ius in itinere*, 14 settembre 2020, <https://www.iusinitinere.it/algoritmo-discrezionalità-amministrativa-e-discrezionalità-del-giudice-nota-a-cons-stato-sez-vi-sent-del-4-febbraio-2020-n-881-30630>.

⁸⁷³ *Ibidem*.

Tuttavia, la più emblematica pronuncia del Consiglio di Stato in cui l'orientamento in esame si cristallizza, e che offre una “guida” in punto di *algorithmic decision making* nell'attività della Pubblica Amministrazione (che si ritiene sarà seguita e ulteriormente specificata), è la rilevante sentenza n. 8472/2019⁸⁷⁴.

Parimenti allo “sfondo” di una delle sentenze poc'anzi citate, nel caso in esame era insorta una controversia promossa da docenti immessi in ruolo nella c.d. fase C del piano straordinario assunzionale di cui alla l. n. 107 del 2015, per mezzo di ricorsi avverso gli esiti della procedura nazionale di mobilità attuata con Ord. MIUR n. 241 del 2016 in attuazione dell'art. 1, comma 108, della citata legge. In particolare, la contestazione riguardava l'esito della procedura la quale, svolta sulla base di un «*algoritmo tuttora sconosciuto*», avrebbe disposto i trasferimenti senza tener conto delle preferenze espresse, pur in presenza di posti disponibili nelle province indicate, «in evidente contrasto con il fondamentale principio della strumentalità del ricorso all'informatica nelle procedure amministrative»⁸⁷⁵.

Il giudice del gravame, dopo aver ribadito il principio per cui la «formula tecnica», che di fatto rappresenta l'algoritmo, deve essere corredata da spiegazioni che la traducano nella «regola giuridica» ad essa sottesa e che la rendano *leggibile e comprensibile*, afferma che in senso contrario «non può assumere rilievo l'invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati le quali, ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria

⁸⁷⁴ Cons. Stato Sez. VI, Sent., 13-12-2019, n. 8472 in www.giustizia-amministrativa.it. Per un commento, cfr. già da ora G. Pesce, Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale, 16 gennaio 2020, reperibile sul sito istituzionale del Consiglio di Stato, nella sezione Giustizia Amministrativa: <https://www.giustizia-amministrativa.it/-/pesce-il-consiglio-di-stato-ed-il-vizio-della-opacita-dell-algoritmo-tra-diritto-interno-e-diritto-sovranoazionale>.

⁸⁷⁵ Cfr. per un riscontro T.A.R. Lazio-Roma, Sez. III bis, sentenza n. 3742/2017.

trasparenza»⁸⁷⁶. Cosicché come nella precedente sentenza n. 2270 dello stesso anno, l'esito del contenzioso è sfavorevole alla P.A. resistente, poiché la stessa impossibilità di comprendere le modalità con le quali, attraverso l'algoritmo, sono stati assegnati i posti disponibili di docente, costituisce di per sé un vizio tale da inficiare la procedura e più radicalmente «*il metodo in quanto tale per il difetto di trasparenza dello stesso*».

La sentenza in esame tuttavia, parallelamente al suo esito, rileva ancora più per le considerazioni logico-giuridiche che del primo costituiscono il substrato e, segnatamente, per la ricostruzione sistematica della disciplina applicabile al rapporto tra Intelligenza Artificiale e procedimento amministrativo, per la gran parte riconducibile al diritto sovranazionale: nello specifico, al GDPR; alla (non vincolante) Carta sulla Robotica; ed alla Convenzione europea sui diritti umani⁸⁷⁷.

Possiamo qui limitarci a richiamare quei principi che puntualmente il Consiglio di Stato afferma come condizionanti la legittimità del procedimento (e conseguentemente del suo provvedimento conclusivo) che sia connotato dall'impiego dell'algoritmo nelle sue diverse fasi, e in particolare in quella decisoria: principi che molto risentono della disciplina dettata proprio dal subsystema normativo che abbiamo detto edificato *sull'*art. 22 del GDPR, in materia di processi decisionali interamente automatizzati.

In primo luogo, viene sancito il *principio di conoscibilità*, per cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino (specialmente, lo sappiamo, quando soddisfino i presupposti di cui al par. 1 dell'art. 22 del GDPR), ed in tal caso a ricevere informazioni significative sulla logica utilizzata.

⁸⁷⁶ Cons. Stato Sez. VI, Sent., 13-12-2019, n. 8472, capo 13.1. della motivazione.

⁸⁷⁷ Ivi, capi 14 ss. Cfr. sul tema anche S. CIVITARESE MATTEUCCI, «“Umano troppo umano”. Decisioni amministrative automatizzate e principio di legalità», in *Dir. pubbl.* 1/2019, p. 23.

Il secondo principio è definibile come il *principio di non esclusività della decisione algoritmica*. Nel caso in cui una decisione automatizzata «produca effetti giuridici che riguardano o che incidano significativamente su una persona», questa ha *diritto a che tale decisione non sia basata unicamente su tale processo automatizzato*: e dunque, segnatamente, ad ottenere l'intervento umano

Il terzo principio è quello della *non discriminazione algoritmica*, secondo cui è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori.

Come è facile constatare, il vademecum approntato nella sentenza n. 8472/2019 resa dalla sezione VI del Consiglio di Stato risulta fortemente debitore al dibattito fiorito intorno all'ambito di applicazione e alla portata della disciplina prevista dall'art. 22 del GDPR; e, in particolar modo, agli orientamenti accolti dalle Linee Guida sul processo decisionale automatizzato del Gruppo di Lavoro Art. 29 ampiamente esaminate: orientamenti – sappiamo ormai anche questo - recentissimamente consacrati anche nella giurisprudenza della Corte di Giustizia dell'Unione europea con l'“epocale” sentenza *SCHUFA*.

In chiusura, si possono allora riportare le parole di quanti hanno affermato come in materia di trattamenti algoritmici il Consiglio di Stato, alla luce della “sentenza guida” citata, «da una parte ribadisce la natura servente dell'algoritmo per la p.a. (secondo il canone “la macchina per l'uomo, non viceversa”); dall'altro lato, pone le premesse per un esplicito superamento anche dei limiti di utilizzo dell'algoritmo e della stessa IA nei diversi ambiti dell'attività amministrativa», e ciò in particolare nel contesto dell'attività amministrativa discrezionale, pur entro

la cornice di precisi principi che rappresentano la moderna declinazione dei principi già sanciti nella legge generale sul procedimento amministrativo⁸⁷⁸.

3.3.1. Orientamenti fondamentali del Garante per la Protezione dei Dati Personali in materia di trattamenti algoritmici: dal caso *Mevaluate* al provvedimento del 7 luglio 2022 in materia di pubblicità personalizzata nei confronti di *TikTok*

Abbiamo già avuto modo di sottolineare ampiamente nel corso della trattazione il ruolo svolto tanto dalle Autorità Garanti dei singoli Stati membri quanto dall'*European Data Protection Supervisor* (EDPS) nel massimizzare, sul piano della concreta osservanza ed applicazione delle norme sulla protezione dei dati personali, il diritto all'autodeterminazione informativa. In proposito, basterà ricordare l'intervento dell'EDPS, a commento dell'allora proposta di Direttiva su alcuni aspetti dei contratti di fornitura di servizi e contenuti digitali, in punto di condizioni di validità dei c.d. *tying agreements*, laddove l'Autorità ha affermato che «i diritti fondamentali, come il diritto alla protezione dei dati personali, non possono essere ridotti a semplici interessi dei consumatori e i dati personali non possono essere ridotti a mera merce»⁸⁷⁹.

Altrettanto eloquente è stata l'interpretazione di tale ruolo da parte del Garante per la Protezione dei Dati Personali italiano, sin dalla sua istituzione con la legge n. del 1996 che per prima attuava la direttiva 95/46/CE, nei più disparati

⁸⁷⁸ Cfr. G. PESCE, «Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale», 16 gennaio 2020, cit.

⁸⁷⁹ EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion in the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, n. 4/2017.

settori in cui le norme in materia di *data protection* estendessero il loro raggio d'azione (fondamenti di liceità del trattamento, obblighi d'informativa, puntuale definizione dei diritti degli interessati, ecc.), nell'ambito dei procedimenti instaurati mediante reclamo o ricorso proposto dagli interessati attraverso l'applicazione degli eterogenei rimedi previsti dalle norme della parte III del Codice della Privacy⁸⁸⁰. La concezione personalistica accolta dal Garante è stata espressa ripetutamente dal medesimo nel corso della sua storia: basterà qui riproporre le lucide considerazioni con cui, affrontando il delicato e sempre più massiccio fenomeno della profilazione algoritmica online, esso puntualmente osserva come «deve essere tenuta in considerazione l'evoluzione comportamentale degli stessi utenti della rete, sempre più orientati alla moltiplicazione delle proprie identità digitali come risultanti dall'accesso a plurimi servizi e funzioni disponibili e, in primo luogo, ai social network. (...) Si impone, di conseguenza, la necessità di un quadro rafforzato di tutele maggiormente orientate a favorire e a rendere effettivo il controllo sulle informazioni personali oggetto di trattamento e, in definitiva, la capacità di autodeterminazione del singolo»⁸⁸¹.

A dimostrazione della profonda sensibilità giuridica, e prima ancora sociale, che contraddistingue il Garante, con l'approfondirsi della *datification* e il dilagare della tecnologia algoritmica e dei sistemi di IA in pressoché tutti i settori della vita sociale, è progressivamente aumentata l'attenzione rivolta all'individuazione stessa dei trattamenti svolti mediante l'impiego dei suddetti

⁸⁸⁰ Sul quadro normativo ancora una volta ha inciso il Regolamento UE 2016/679, che ha previsto un regime uniforme di rimedi inibitori, ablativi, satisfattivi e sanzionatori: il d.lgs. n. 101/2018, adeguando l'ordinamento alla disciplina del Reg., ha di conseguenza abrogato, in particolare, l'intera Sezione III rubricata «Tutela alternativa a quella giurisdizionale» e gli artt. 161-171 del capo I del Titolo III della Parte III, rubricato «Sanzioni».

⁸⁸¹ Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPDP), *Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021* [9677876], p. 4.

automated systems, al precipuo scopo di rafforzare le garanzie previste a favore degli interessati in punto di liceità, trasparenza e corretta del trattamento⁸⁸². In un suo recente intervento deputato a indagare il ruolo e le prospettive dell'Autorità in relazione al rapporto sempre crescente tra Intelligenza Artificiale ed elaborazione dei dati personali (e conseguentemente crescenti istanze di protezione dei medesimi), il Vice Presidente del Garante per la Protezione dei Dati Personali Ginevra Cerrina Feroni ha puntualmente affermato come «con il passaggio dalla *società digitale* alla *società algoritmica*, l'intelligenza artificiale è divenuto uno strumento sempre più utilizzato a supporto della funzione gestoria, della definizione degli indirizzi strategici privati e pubblici e del controllo sull'attività amministrativa», ricordando poi opportunamente che, nel contesto in parola, «il ruolo del Garante privacy nella tutela dei diritti digitali a fronte di trattamenti automatizzati dei dati personali è stato sempre di primo piano, anche quando il tema non era ancora diventato, per così dire, da grande pubblico»⁸⁸³.

Di seguito, pertanto, passeremo in rassegna taluni dei più importanti interventi provvedimentali o consultivi del Garante in materia di trattamenti - interamente o parzialmente – algoritmici; per poi focalizzare l'attenzione, a conclusione del paragrafo, su uno dei più recenti provvedimenti dell'Autorità in materia, che ancora una volta si confronta con il problematico tema della profilazione online e della pubblicità comportamentale (sui social network).

⁸⁸² V. *retro*, anche cap. 2, par. 3 per l'approfondita riflessione svolta sul contesto tecnologico contemporaneo e sulle insidie che configura per l'integrità della sfera privata della persona umana. Per ulteriori recenti contributi sul rapporto tra IA e protezione dei dati personali, cfr. anche A. SIMONCINI, A. ADINOLFI (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, ESI, 2022.

⁸⁸³ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Intelligenza artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerrina Feroni*, Intervento di Ginevra Cerrina Feroni, Vice Presidente del Garante per la protezione dei dati personali, 14 febbraio 2023, p. 1.

Sin dalle prime pronunce del Garante in punto di applicazione delle tecnologie di IA ai trattamenti di dati personali, dimostrando la propria vocazione «a presidio dei diritti fondamentali in settori svariati»⁸⁸⁴, emerge una sufficiente consapevolezza dei rischi rappresentati dall'esposizione delle persone fisiche e della loro vita privata a processi decisionali automatizzati, basati tanto sui dati personali quanto, semplicemente, su *metadati*.

Il primo rilevante caso che citiamo è quello di cui già ci siamo occupati nel paragrafo precedente, dacché successivamente oggetto dell'importante ordinanza n. 14381/2021 della I Sezione della Suprema Corte. Ci riferiamo al c.d. caso *Mevaluate*, in cui il Garante ha emesso un provvedimento inibitorio censurando l'illiceità di una piattaforma deputata a costruire, attraverso un sistema di raccolta e di elaborazione dei dati a scopo di profilazione interamente algoritmico, profili reputazionali dei soggetti censiti (persone fisiche o giuridiche), a causa della violazione di una molteplicità di norme a garanzia degli interessati: violazione tra cui figuravano in particolare il difetto dei presupposti della libertà e della specificità del consenso, richiesti dal previgente art. 23 del Codice della Privacy e l'inosservanza del principio di qualità dei dati di cui all'art. 11, comma 1, lett. c), stante la carente documentazione circa l'affidabilità del sistema descritto⁸⁸⁵.

Sempre nella vigenza della disciplina antecedente al GDPR, e alla novella apportata al Codice dal D.lgs. n. 101/2018, esprimendosi su trattamenti di analisi comportamentale degli utenti di siti commerciali in base alle loro modalità di navigazione online, il Garante ha vietato un sistema di lettura biometrica che, montato su totem pubblicitari, registrava sesso, range di età, distanza dal monitor e tempo di permanenza dinanzi ad esso dei passanti che s'imbattevano o

⁸⁸⁴ *Ibidem*.

⁸⁸⁵ V. ancora Provv. n. 488 del 24 novembre 2016, doc. web n. 5796783. Le norme violate risultavano gli artt. 2, 3, 11, 13, 23, 24 e 26 del Codice nella sua versione ante-riforma del 2018.

s'intrattenevano a guardare uno degli spot proiettati, in modo da calcolare la fascia d'età, il sesso, il grado di attenzione e persino la stima dell'espressione facciale mostrata da differenti target commerciali rispetto ai vari prodotti pubblicizzati⁸⁸⁶.

Il Garante, nei casi in questione, pare aver anticipato allora alcuni dei principi poi consacrati nella disciplina di cui all'art. 22 di cui ci siamo ampiamente occupati.

Ugualmente importanti risultano i casi in cui il Garante abbia vigilato sulla tutela dei diritti e delle libertà dei cittadini laddove il titolare del trattamento che ricorre all'utilizzo dell'IA fosse un soggetto pubblico.

Un emblematico esempio della funzione di “guardiano dei diritti” svolta dal Garante in tale settore si identifica nel caso che ha coinvolto il c.d. Redditometro, strumento di controllo che si fondava sul trattamento automatizzato di dati personali presenti nell'anagrafe tributaria: nel 2013 l'Autorità ha espresso parere favorevole sulla richiesta dell'Agenzia delle Entrate, definendo però le garanzie necessarie per il rispetto dei diritti degli interessati⁸⁸⁷. In ambito tributario, parimenti, si segnalano i provvedimenti del Garante in relazione alla sperimentazione, progettata dall'Agenzia dell'Entrate, di procedure per l'individuazione di profili di evasione attraverso l'analisi dei dati finalizzata: in tali occasioni, il Garante ha individuato le misure di sicurezza e organizzative idonee per fare in modo che il controllo tramite algoritmo fosse conforme alla protezione dei dati personali ma, al contempo, efficace, ad esempio prevedendo

⁸⁸⁶ Prov. Doc. web. N. 7496252 del 21 dicembre 2017, «Installazione di apparati promozionali del tipo 'digital signage' (definiti anche Totem) presso una stazione ferroviaria».

⁸⁸⁷ Cfr. Prov. n. 515 del 21 novembre 2013, [doc. web n. 2765110], «Redditometro: le garanzie dell'Autorità a seguito della verifica preliminare sul trattamento di dati personali effettuato dall'Agenzia delle entrate». In esso il Garante, tra l'altro, in relazione alla circolare n. 24/E del 31 luglio 2013 dell'Agenzia dell'Entrate che introduceva modifiche (in senso garantistico) al disegno originario, rileva che «con riferimento alla protezione dei dati personali, tali correttivi sono da valutarsi favorevolmente anche in relazione alla correttezza del trattamento dei dati personali dei contribuenti in quanto riducono nella fase di selezione gli effetti determinati dal trattamento automatizzato di dati presunti, e quindi non esatti».

che « il protocollo FTP utilizzato per l'interscambio dei dati sia cifrato, anche attraverso i meccanismi di protezione già presenti nella gran parte dei prodotti disponibili (anche open source)»; e che, conseguentemente, «nel caso in cui i file di esito dell'invio contengano dati personali, siano adottate idonee modalità di cifratura, con riferimento ad entrambe le modalità di interscambio (FTP e PEC)»⁸⁸⁸.

Ma forse ancora più rilevante risulta l'impegno almeno relativamente profuso dal Garante a partire dalla pandemia da Sars Cov-2 nel contenere il rischio di proliferazione senza criterio di sistemi di analisi intelligente dei dati sanitari dei cittadini, adottati da parte di enti locali e nazionali senza un coordinamento centralizzato. L'esempio più rilevante in tal senso può individuarsi nel parere del 5 marzo 2020 al Consiglio di Stato in merito ai criteri di ripartizione del Fondo Sanitario Nazionale che prevedevano il trattamento di dati personali, anche sulla salute, di tutti i cittadini assistiti dal Servizio Sanitario Nazionale, così da rimodulare il sistema di distribuzione delle risorse economiche sulla base dello stato di salute di ogni singolo assistito: nel suo quadro, il Garante ha rilevato che il progetto ministeriale risultasse privo di una base normativa necessaria per raggiungere gli obiettivi prefissati e che invece l'uso di algoritmi avrebbe suddiviso tutta la popolazione in gruppi per omogeneità patologiche e reddituali, sottolineando con forza che «la *profilazione dell'utente del servizio sanitario*, sia questo regionale o nazionale, determinando un *trattamento automatizzato di dati*

⁸⁸⁸ V. Provv. n. 861 del 15 novembre 2012, [doc. web n. 2099774], «Comunicazioni all'anagrafe tributaria da parte di banche e operatori finanziari: parere sulle modalità di trasmissione e di conservazione dei dati»; cfr. anche il successivo Provv. n. 321 del 20 luglio 2017, [doc. web n. 6843736], «Sperimentazione di una procedura basata sull'utilizzo di informazioni fornite dall'Archivio dei rapporti finanziari e degli elementi presenti nell'Anagrafe tributaria per l'individuazione di profili di evasione rilevanti», in cui il Garante giudicava idonee, in funzione della tutela dei diritti degli interessati, le modifiche introdotte allo schema di Provvedimento iniziale dall'Agenzia.

personali volto ad analizzare e prevedere l'evoluzione della situazione sanitaria del singolo assistito e l'eventuale correlazione con altri elementi di rischio clinico (nel caso di specie l'infezione da Sars Cov-2), può essere effettuata solo nel rispetto di requisiti specifici e *garanzie adeguate per i diritti e le libertà degli interessati*»⁸⁸⁹. Si può ragionevolmente presumere che l'attività del Garante sul punto proseguirà, in particolare attraverso la vigilanza in ordine agli impatti sul diritto alla protezione dei dati personali di quella che è considerata la nuova frontiera della medicina, ovvero l'impiego dell'IA a scopi di medicina preventiva o d'iniziativa da parte delle amministrazioni sanitarie⁸⁹⁰.

Tornando sul piano dei rapporti interprivati, deve sottolinearsi la funzione di contrasto svolta dal Garante, attraverso l'irrogazione di provvedimenti insieme inibitori e sanzionatori, in relazione all'utilizzo dell'IA nell'ambito dei rapporti di lavoro a domicilio, in particolare con riguardo al profilo della prenotazione e dell'assegnazione dei turni di lavoro, censurate in quanto foriere di discriminazioni algoritmiche a carico dei dipendenti (c.d. *riders*). Ci si riferisce alle due ordinanze di ingiunzione adottate, rispettivamente il 10 giugno e il 22 luglio 2021, nei confronti di Foodinho s.r.l., controllata italiana di GlovoApp23, e di Deliveroo Italy s.r.l., condannate rispettivamente al pagamento di una sanzione amministrativa pari a 2,6 e a 2,5 milioni di euro. Interventi di particolare peso, se si considera che essi costituiscono l'esito del primo ciclo ispettivo

⁸⁸⁹ V. Prov. n. 43 del 5 marzo 2020, [doc. web n. 9304455], Parere al Consiglio di Stato sulle nuove modalità di ripartizione del fondo sanitario tra le regioni proposte dal Ministero della salute e basate sulla stratificazione della popolazione.

⁸⁹⁰ Cfr. per alcuni approfondimenti sul tema, i recenti contributi raccolti nel volume di M. GABBRIELLI, U. RUFFO (a cura di), *Intelligenza Artificiale, dispositivi medici e diritto. Un dialogo fra saperi: giuristi, medici e informatici a confronto*, Giappichelli, Torino 2023.

condotto nell'ordinamento italiano sulle modalità di gestione dei lavoratori di alcune delle principali società di *food delivery* operanti anche nel nostro paese⁸⁹¹.

In special modo nel primo procedimento (il secondo ne ricalca essenzialmente il contenuto, sia in punto di contestazione che in punto di conseguenze sanzionatorie), l'attività istruttoria ha evidenziato numerose violazioni del Regolamento 2016/679 e della l. n. 300/1970, c.d. Statuto dei Lavoratori. Tra queste, per quel che più rileva ai fini del tema che ci occupa, la società non aveva adeguatamente informato i lavoratori sul funzionamento del sistema e non assicurava garanzie sull'esattezza e la correttezza dei risultati dei sistemi algoritmici utilizzati per la valutazione dei *riders*. Dall'attività istruttoria, era infatti emerso che la società effettuasse, attraverso il sistema complessivamente utilizzato per l'operatività della piattaforma, «trattamenti automatizzati, compresa la profilazione, nell'ambito del c.d. “sistema d'eccellenza” che attribuisce a ciascun rider, attraverso l'operatività di specifici e predeterminati parametri, un punteggio che consente di accedere prioritariamente al “sistema di selezione delle fasce orarie (slots)” stabilite dalla società all'interno delle quali sono distribuiti giornalmente gli ordini ricevuti»; sistema la cui formula algoritmica – aggiunge il provvedimento - penalizza i *riders* che non accettano tempestivamente l'ordine o lo rifiutano favorendo invece i *riders* che accettano nei termini stabiliti o consegnano il maggior numero di ordini⁸⁹². Secondo il Garante, diversamente dalla lettura prospettata dalla società nelle sue memorie, il trattamento, il calcolo del punteggio personalizzato e la successiva assegnazione degli ordini attraverso l'altrettanto algoritmico sistema *Jarvis* integrerebbero un processo decisionale puntualmente ricadente nell'ambito di

⁸⁹¹ Cfr., rispettivamente, Provv. N. 234 del 10 giugno 2021, [doc. web n. 9675440], «Ordinanza ingiunzione nei confronti di Foodinho s.r.l. »; Provv. N. 285 del 22 luglio 2021, [doc. web n. 9685994], «Ordinanza ingiunzione nei confronti di Deliveroo Italy s.r.l.».

⁸⁹² Provv. N. 234 del 10 giugno 2021, [doc. web n. 9675440], par. 3.3.6.

applicazione dell'art. 22: l'Autorità, in proposito, rileva che «la necessaria impostazione dei parametri in base ai quali opera il funzionamento dell'algoritmo non fa venir meno, in sé, l'assunzione di decisioni basate unicamente su un trattamento automatizzato», e che «la stessa società in sede di accertamenti ispettivi ha dichiarato che “l'assegnazione del punteggio è generalmente automatizzata”»⁸⁹³. A partire da tale premesse, tuttavia, e in estrema sintesi, l'Autorità rileva proprio l'inosservanza delle garanzie rafforzate previste dall'ampiamente analizzato subsistema normativo edificato sull'art. 22: pur a fronte dell'integrazione della base giuridica eccezionale rappresentata dalla necessità del processo siffatto *ai fini dell'esecuzione del contratto* intercorrente con l'interessato, *ex par. 2 lett a)*, la piattaforma non avrebbe predisposto le adeguate misure di tutela imposte dal par. 3, non garantendo procedure per tutelare il diritto di ottenere l'intervento umano, esprimere la propria opinione e contestare le decisioni adottate mediante l'utilizzo degli algoritmi in questione, compresa quella rappresentata dall'esclusione di una parte dei *riders* dalle occasioni di lavoro⁸⁹⁴.

Il Garante, dunque, oltre ad irrogare la non irrilevante sanzione di cui sopra, con il provvedimento in parola (il secondo, lo ripetiamo, ne ricalca la struttura e i contenuti) ha prescritto alla società di *food delivery* implicata di individuare misure per tutelare i diritti e le libertà dei *riders* a fronte di decisioni automatizzate; di verificare l'esattezza e la pertinenza dei dati utilizzati dal sistema (chat, email e telefonate intercorse tra i *riders* e il *customer care*, geolocalizzazione ogni 15 secondi e visualizzazione su mappa del percorso ecc.); e di adottare, inoltre, misure che impediscano utilizzi impropri o discriminatori

⁸⁹³ *Ibidem.*

⁸⁹⁴ *Ibidem.*

dei meccanismi reputazionali basati sul feedback dei clienti e dei partner commerciali⁸⁹⁵.

Ma ancora più rilevante, considerate le potenziali ripercussioni sulla libertà dell'individuo di autodeterminarsi, consiste l'impegno del Garante in relazione alle pratiche che configurano in capo ai consociati il rischio di soggiacere a sistemi di sorveglianza di massa. E tali pratiche, per la maggior parte, consistono proprio nei trattamenti di profilazione, che sempre più spesso rappresentano la fase iniziale, o prodromica, di sistemi di *solely automated decision making*. In questa sede, ci soffermeremo più nello specifico sul versante della profilazione effettuata allo scopo di implementare strategie di pubblicità comportamentale, specialmente sulle ormai capillarmente diffuse piattaforme dei *social media*: per questo motivo, faremo cenno alla problematica questione del marketing diretto in ambito elettorale, prepotentemente emersa con il già citato caso *Facebook-Cambridge Analytica*.

Prima, tuttavia, può essere utile citare un emblematico caso generale risalente al 2022, di cui si sono interessate per qualche tempo le cronache nazionali, in cui il Garante è dovuto intervenire per censurare la condotta della nota società americana Clearview, rea di aver posto in essere un vero e proprio sistema di monitoraggio biometrico coinvolgente anche persone che si trovassero nel territorio italiano, irrogando la pesante sanzione di 20 milioni di euro⁸⁹⁶.

Come forse sarà noto, Clearview è una società che offre tecnologie algoritmiche di sorveglianza, e in particolare di riconoscimento facciale, tanto a

⁸⁹⁵ Cfr. anche le note di sintesi contenute nel comunicato stampa del Garante per la Protezione dei Dati Personali, «Rider: Garante privacy, no a discriminazioni basate sugli algoritmi. Sanzione di 2,6 milioni di euro a una piattaforma del gruppo Glovo», 5 luglio 2021, Doc-Web 9677377.

⁸⁹⁶ Provv. N. 50 del 10 febbraio 2022, [doc. web n. 9751362], «Ordinanza ingiunzione nei confronti di Clearview AI».

soggetti pubblici quanto, attualmente, ad aziende private. Essa, in particolare, avvalendosi di un database di oltre 10 miliardi di immagini di volti di persone di tutto il mondo, estratte da fonti web pubbliche tramite *web scraping* (come siti di informazione, social media e video online), offre un servizio di ricerca altamente qualificata che, grazie a sistemi di intelligenza artificiale, consente la *creazione di profili basati sui dati biometrici* estratti dalle immagini, eventualmente arricchiti da altre informazioni ad esse correlate, come titolo e geolocalizzazione della foto, pagina web di pubblicazione⁸⁹⁷.

L'interesse internazionale per i suoi prodotti, in particolare, è emerso quando nel 2019 ne hanno promosso, con esiti positivi, l'impiego nell'ambito di indagini sulla pornografia infantile. Da quel momento, la società ha stipulato contratti ai fini dell'apertura di account di prova con alcuni clienti europei, in particolare agenzie intergovernative, pur sempre al fine (secondo le memorie difensive presentata dalla società nel procedimento instaurato presso il Garante italiano) di migliorare la sicurezza pubblica, riducendo i tempi delle indagini e adjuvando le forze dell'ordine nell'identificazione dei criminali.

Tuttavia, gli account di prova in questione sono stati chiusi a seguito di recami pervenuti a Garanti di singoli Stati membri nel marzo 2020, e lo stesso Garante italiano ha avviato d'ufficio l'istruttoria - conclusa poi dal provvedimento in esame - a seguito di notizie stampa concernenti alcune criticità in punto di *privacy* individuale derivanti dai prodotti della società: istruttoria in cui si iscrivevano una serie di reclami presentati da persone fisiche e associazioni a tutela dei diritti civili nel corso del 2021⁸⁹⁸.

⁸⁹⁷ Cfr. per alcune più specifiche informazioni in ordine alle attività svolte dalla società, oltre ai parr. 2 e ss. del suddetto provv., l'articolo di L. ZORLONI, «Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto», in *Wired*, 23 marzo 2021, <https://www.wired.it/attualita/tech/2021/03/23/clearview-ai-riconoscimento-facciale-foto/>; nonché il sito ufficiale della società medesima, <https://www.clearview.ai>.

⁸⁹⁸ Cfr. Provv. N. 50 del 10 febbraio 2022, [doc. web n. 9751362], par. 2.

Ebbene, in sintesi, dall'istruttoria medesima è emerso che la società americana consentiva anche il tracciamento di cittadini italiani e di persone collocate in Italia: le risultanze avrebbero rivelato che i dati personali detenuti dalla società, inclusi quelli biometrici e di geolocalizzazione, venivano trattati illecitamente, senza un'adeguata base giuridica, che non poteva certamente consistere nel legittimo interesse della società americana⁸⁹⁹. La società, secondo il Garante, ha inoltre violato, tra gli altri, i principi del GDPR che impongono obblighi di trasparenza, non avendo adeguatamente informato gli utenti (art. 5, par. 1, lett. a); di limitazione delle finalità del trattamento, avendo utilizzato i dati degli utenti per scopi diversi rispetto a quelli per i quali erano stati pubblicati online (lett. b); e di limitazione della conservazione, non avendo stabilito tempi di conservazione dei dati (lett. e)⁹⁰⁰. Tuttavia, nel caso di specie, il Garante non ha ritenuto sussistessero sufficienti elementi per riscontrare *anche* la violazione, nello specifico, dell'art. 22, pur contestata da taluni dei reclamanti⁹⁰¹.

Alla luce delle violazioni riscontrate, oltre alla esosa sanzione pecuniaria predetta, il Garante ha ordinato alla società di cancellare i dati relativi a persone che si trovino in Italia e ne ha vietato l'ulteriore raccolta e trattamento attraverso il suddetto sistema di riconoscimento facciale⁹⁰².

⁸⁹⁹ Cfr. in proposito il rilevante passaggio contenuto al par. 3.4., laddove il Garante osserva attentamente che «pare innanzitutto doveroso ricordare come la pubblica disponibilità di dati in Internet non implica, per il solo fatto del loro pubblico stato, la legittimità della loro raccolta da parte di soggetti terzi. Infatti, ogni dato che viene pubblicato on-line subisce tale operazione di trattamento (segnatamente, la diffusione), sulla scorta di una base giuridica e per finalità determinate e legittime stabilite e perseguite dal titolare del trattamento che ne ha disposto la pubblicazione». Per le motivazioni in punto di accertamento positivo della violazione dell'art. 22, cfr. par. 3.6.6.

⁹⁰⁰ Ivi, par. 3.6 ss.

⁹⁰¹ Ivi, par. 3.6.6., dove il Garante afferma tra l'altro che Si rileva ancora che «l'art. 22 prevede il diritto a non subire una decisione basata unicamente su di un trattamento automatizzato ma, da quanto emerso in fase istruttoria, tale decisione pare al più poter essere assunta dei clienti del servizio offerto da Clearview e non dalla Società, la quale ha implementato e reso disponibile a terzi il suo sistema di riconoscimento facciale».

⁹⁰² Ivi, Conclusioni.

Se tale caso risulta particolarmente delicato, stante il coinvolgimento esplicito di dati biometrici, non meno incidenti sulla sfera privata e sul diritto di autodeterminazione informativa risultano tutte le fattispecie contraddistinte dallo svolgimento di un'*attività di profilazione*, tanto interamente quanto solo parzialmente algoritmica.

Nel contesto in esame risulta particolarmente rilevante quello che è stato definito, con formula generale, il c.d. *Behavioral targeting advertising system*, o “Sistema pubblicitario di targeting comportamentale”, già incontrato nel corso della trattazione: giova ricordare che si tratta di un modello generale di marketing diretto ormai largamente implementato nel settore privato, basato su un meccanismo di profilazione globale realizzato per mezzo di *web beacons*, ovvero immagini elettroniche (chiamate anche *web bugs* o *pixel tags*) che assieme ai *cookies* tracciano il profilo virtuale del potenziale utente-interessato-consumatore⁹⁰³.

Sappiamo già, in proposito, come tanto la giurisprudenza della Corte di Giustizia quanto l'EDPB siano intervenuti nel merito della questione dei *cookies* e dei rispettivi *cookie wall*, sancendone sostanzialmente l'illiceità laddove basati su logiche di *opting out*⁹⁰⁴. A tale indirizzo si è parimenti conformato il Garante italiano nelle sue Linee Guida sull'utilizzo dei cookies, esprimendosi in detti termini: «Tale meccanismo [il *cookie wall*], non consentendo di qualificare l'eventuale consenso così ottenuto come conforme alle caratteristiche imposte dal Regolamento, e segnatamente al suo art. 4, punto 11 con particolare riferimento

⁹⁰³ Per più approfonditi rilievi sul tema, cfr. A. G. PARISI, *Privacy e mercato*, Pacini giuridica, Pisa 2020; V. GUGGINO, B. BANORRI, «L'advertising ai tempi dell'Intelligenza Artificiale: algoritmi e marketing personalizzato», in P. Stanzone (a cura di), *I “poteri privati” delle piattaforme*, cit., p. 625.

⁹⁰⁴ V. *retro* e cfr. ancora una volta C. Giust. UE, 1 ottobre 2019, C-673/17, in cui la Corte, lo si ricorda, ha ritenuto non potersi considerare validamente espresso il consenso all'utilizzo di cookie mediante una casella di spunta preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso; cfr. ancora poi Comitato Europeo per la Protezione dei Dati, Linee Guida 5/2020 sul consenso, cit.

al requisito della “libertà” del consenso, è da ritenersi illecito, salva l’ipotesi da verificare caso per caso nella quale il titolare del sito offra all’interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all’installazione e all’uso di cookie o altri strumenti di tracciamento» (unica fattispecie, secondo l’indirizzo del Garante - come sappiamo oggi *non* condiviso interamente dalla Cassazione -, per vincere la presunzione legale relativa di invalidità di cui all’art. 7 par. 4, su cui già ci siamo soffermati)⁹⁰⁵.

Allo stesso modo, l’*Autoreit Persoonsgegevens* (l’Autorità olandese per la protezione dei dati), nella sua «Guida sull’utilizzo dei cookies nei siti web» pubblicata il 7 marzo 2019, ha ritenuto che i *cookie wall banner* che informano l’utente dell’utilizzo dei *cookies*, consentendogli di accedere al contenuto del sito solo a seguito dell’accettazione di tale utilizzo, non soddisfino il requisito essenziale della libertà del consenso: similmente a quanto espresso dal Garante italiano, e come già rilevato dall’Autorità austriaca, il *cookie wall* pregiudicherebbe tale libertà nella misura in cui, in difetto del consenso, risulterebbe negato all’utente l’accesso al sito in caso di rifiuto dell’installazione dei *cookies* di profilazione, senza prevedere alternative sostanzialmente equivalenti⁹⁰⁶.

La sensibilità delle istituzioni preposte a garanzia della protezione dei dati personali, della dottrina e della stessa giurisprudenza (nazionale ed europea), non ha tuttavia impedito e tutt’ora non impedisce che della profilazione, soprattutto per scopi di pubblicità comportamentale - strumentale a sua volta ai più disparati

⁹⁰⁵ V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida cookie ed altri strumenti di tracciamento*, cit., par. 6.1.

⁹⁰⁶ V. AUTOREIT PERSOONSgegevens, *Websites moeten toegankelijk blijven bij weigeren tracking cookies*, 7 marzo 2019, <https://autoriteitpersoonsgegevens.nl/actueel/websites-moeten-toegankelijk-blijven-bij-weigeren-tracking-cookies>.

fini -, si faccia ampio utilizzo, spesso in spregio alle opportune garanzie e ai limiti previsti dal GDPR. E che ciò, in particolar modo, avvenga sui *social network*, come ha riscontrato lo stesso Garante italiano, tentando di reagire al fenomeno (come vedremo a breve). Il che risulta particolarmente grave se, come sempre più accade, tali trattamenti si uniscono all'impiego delle più recenti acquisizioni nel campo della psicomетria e del c.d. *neuromarketing*⁹⁰⁷.

Anche in relazione al fenomeno della profilazione per scopi di pubblicità comportamentale, il Garante ha interpretato assiduamente il proprio ruolo di guardiano dei diritti fondamentali degli utenti-interessati.

A tal proposito, è d'obbligo principiare dall'intervento dell'istituzione italiana in quella vicenda che ha rappresentato la ricaduta interna del caso *Facebook-Cambridge Analytica* (sulla quale, lo si ricorderà, ci siamo soffermati nel primo capitolo, per quanto attiene alla sua dimensione americana e transnazionale)⁹⁰⁸. Vicenda che pur non attenendo nello specifico al tema dei presupposti (rafforzati) di liceità dei trattamenti algoritmici, ma più in generale al difetto di una qualsiasi delle base giuridiche previste dal GDPR al fine di giustificare *qualsiasi* tipo di trattamento, automatizzato o meno, dei dati personali, pur sempre coinvolge il profilo dell'elaborazione dei dati in termini di profilazione, per la predisposizione (anch'essa, verosimilmente, secondo sistemi di *decision making* anche solo parzialmente algoritmici) di annunci pubblicitari personalizzati, in tal caso soprattutto per scopi di propaganda politica.

⁹⁰⁷ Con tale espressione si identifica «la disciplina di recente introduzione che si sostanzia, in linea generale, nell'applicazione al campo del marketing di strumenti che derivano dalle neuroscienze al fine di ricavarne informazioni da utilizzare per determinate scelte di marketing: attraverso l'analisi di alcuni meccanismi cerebrali si registra l'impatto che su soggetti monitorati ha l'esposizione ad un determinato prodotto, ad una pubblicità o ad una modalità di vendita». Cfr. sul punto ancora V. GUGGINO, B. BANORRI, «L'advertising ai tempi dell'Intelligenza Artificiale: algoritmi e marketing personalizzato», cit., p. 633 ss.; e per una prospettiva più generali, cfr. gli interessanti spunti offerti da NOCI, *Biomarketing*, Milano, 2018.

⁹⁰⁸ V. *retro*, cap. 1, par. 1.2.

La vicenda scaturisce dal *whistleblowing* dell'ex dipendente Christopher Wylie, che aveva portato alla pubblicazione nel marzo 2018 di alcuni articoli di stampa nazionale e internazionale i quali mettevano in luce come la Società Cambridge Analytica avesse indebitamente raccolto e utilizzato i dati di 87 milioni di utenti di Facebook a scopo di profilazione, a propria volta strumentale a veicolare tramite lo stesso social campagne pubblicitarie personalizzate per influenzare le elezioni presidenziali USA dell'8 novembre 2016. Successivamente a tali rivelazioni, il 10 gennaio 2019 il Garante italiano adottava un Provvedimento che avviava formale istruttoria, trasmettendo in data 21 marzo 2018 a Facebook Italy e a Facebook Ireland Limited un «prima richiesta d'informazione in merito all'utilizzo di dati personali di cittadini italiani fruitori dei servizi della piattaforma Facebook, da parte di Cambridge Analytica»; e se, contestualmente, tali dati fosse stati resi accessibili anche ad altri soggetti per attività di profilazione a fini politici e/o elettorali⁹⁰⁹.

Dall'istruttoria, in sintesi, emergeva che da una parte i fatti fossero avvenuti ancora nel vigore della Direttiva 95/46/CE; e, dall'altra, che in occasione delle elezioni politiche svoltesi in Italia il 4 marzo 2018, Facebook avrebbe fornito agli utenti italiani un prodotto ("*Ballot*") per ottenere informazioni sui candidati nella propria circoscrizione elettorale, sospettato di aver registrato informazioni sulle preferenze di voti degli utenti. Il Garante rilevava inoltre come, in ogni caso, Facebook medesimo avesse comunicato i dati degli utenti ubicati in Italia all'app *Thisisyourdigitallife* al momento del login, in violazione degli allora vigenti artt. 13 e 23 del Codice della Privacy, poiché la comunicazione sarebbe avvenuta in difetto di un'informativa idonea e dello stesso requisito essenziale di validità del consenso rappresentato dalla sua libertà, non essendo stata offerta agli utenti

⁹⁰⁹ Cfr. Provv. N. 5 del 10 gennaio 2019, [doc.web n. 9080914], «Istruttoria Cambridge Analytica».

alcuna alternativa tra l'integrale trasferimento del profilo *compresi* i dati degli amici e l'impossibilità della sottoscrizione⁹¹⁰.

Pertanto, in data 14 giugno 2019 il Garante con ordinanza ingiunzione ha disposto l'applicazione nei confronti di Facebook Ireland Ltd e di Facebook Italy s.r.l. di una sanzione amministrativa pecuniaria di 1 milione di euro, «relativamente alle violazioni perpetrate dalle due società nell'ambito di un non corretto trattamento dei dati personali degli utenti di cui ai fatti afferenti al caso *Cambridge Analytica*»: nel provvedimento medesimo, nel riepilogare i già sinteticamente riportati esiti dell'istruttoria, si legge come il Garante abbia rilevato che il trasferimento dei dati in questione fosse avvenuto «sulla base di un'informativa, fornita agli utenti al momento dell'iscrizione a Facebook, dal contenuto onnicomprensivo, generico e di difficile ricostruzione» e che inoltre «il consenso non può ritenersi espressamente, specificamente e liberamente espresso, posto che, nel momento in cui si attivava l'app attraverso la funzione "Facebook login", agli utenti non veniva lasciata alcuna alternativa rispetto al trasferimento integrale dei dati a suo tempo conferiti a Facebook (Versione.1 della suddetta funzione), ovvero veniva consentito di effettuare solo parziali variazioni, con modalità *opt-out*, rispetto a scelte già "*pre-flaggate*" (Versione.2)»⁹¹¹.

L'emblematico caso in questione ci consente di approfondire ulteriormente il problematico tema della profilazione nell'ambito dei social network, a scopo, essenzialmente, di marketing personalizzato; ma, più in generale, dei problemi

⁹¹⁰ Cfr. Provv. n. 134 del 14 giugno 2019, «Ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l.», [doc. web n. 9121486]. Da notare come il Garante rilevi che, secondo quanto noto a Facebook Ireland Ltd, a fronte dell'installazione della *web app* da parte di soli 57 utenti italiani, fossero in realtà stati condivisi con l'app i dati di altri utenti italiani fino ad un numero massimo di addirittura 214.077, e ciò per mezzo di utenti "Amici", anche ubicati fuori dal territorio italiano, che avessero a propria volta installato l'app.

⁹¹¹ *Ibidem*. Con l'espressione «flaggare», in ambito informatico e digitale, si intende segnare con un *flag*, ossia con un segno di spunta.

configurati dai sistemi di *algorithmic data processign and decision making* che per la maggior parte presiedono al funzionamento delle piattaforme, specialmente in relazione all'integrità della sfera privata (e, prima ancora, psicofisica) evidentemente più fragile dei minori.

Già nel dicembre 2020 il presidente del Garante italiano, il Prof. Pasquale Stanzone, ha avviato il primo “*Hackaton*”, iniziativa diretta a sensibilizzare esperti di diverse discipline, tra cui informatici, sviluppatori di software e grafici, sull'ottimale utilizzo di strumenti di *legal design* (in conformità del principio fortemente penetrato nella sensibilità dell'informatica giuridica e, con il GDPR, nella dimensione normativa europea) per la semplificazione delle informative connesse alla *privacy* specialmente nell'ambito dei social media e con particolare riguardo a quelle destinate ai minori⁹¹².

Il Garante osservava già allora come l'informativa rilasciata agli utenti dai gestori dei social network sia predefinita e, soprattutto, non prenda in considerazione specifica la situazione dei minori, laddove sarebbe invece necessario creare un'apposita sezione loro dedicata, scritta con linguaggio più semplice e con meccanismi di *alert* che segnalino a quali rischi si espongono⁹¹³. In particolare, sotto osservazione risulta il famoso social TikTok, nato nel settembre 2016 in Cina come Douyin e successivamente oggetto di fusione con la piattaforma americana Musical.ly, che già tra 2020 e 2021 contava 2 miliardi di utenti a livello globale, tra cui soprattutto giovanissimi⁹¹⁴: ebbene, la principale

⁹¹² V. sul punto l'intervento di GUIDO SCORZA, Componente dell'Autorità Garante per la protezione dei dati personali, su *Wired*, del 2 dicembre 2020, *Un hackathon per rendere le privacy policy qualcosa che tutti possano leggere* (e capire), disponibile sul sito del Garante: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9495622>.

⁹¹³ Cfr. anche sul punto A. G. PARISI, «Illiceità del trattamento dei dati personali e rimedi», cit., p. 266 ss.

⁹¹⁴ Per alcune più approfondite riflessioni, informatiche e anche giuridiche, sul “fenomeno” TikTok, sulla distinzione formale tra tale persona giuridica e Douyin (attualmente, il corrispettivo cinese), e sulle sfide in punto di *privacy* lanciate dalla piattaforma, cfr. l'interessante analisi di PELLAEON LIN, «TikTok vs Douyin. A Security and Privacy Analysis»,

criticità consisteva a suo tempo nel preimpostare il profilo dell'utente come pubblico, in contrasto con i principi del GDPR che impongono misure organizzative e tecniche idonee a garantire, *by default*, la scelta se rendere conoscibile o meno a terzi il medesimo; gli stessi tempi di conservazione dei dati risultavano indefiniti rispetto agli scopi per cui fossero raccolti, e la medesima mancanza di chiarezza riguardava anche il trasferimento all'estero dei medesimi⁹¹⁵.

Con riferimento alle criticità cui risulta esposta la *privacy* dei minori, appare fondamentale ricordare che il GDPR all'art. 8, rubricato «Condizioni applicabili al consenso dei minori in relazioni ai servizi della società dell'informazione», prevede al par. 1 che l'età minima ai fini della liceità del trattamento *nell'ambito dell'offerta diretta di servizi della società dell'informazione* sia di 16 anni, per i soggetti di età inferiore la liceità essendo invece subordinata alla prestazione o all'autorizzazione del consenso da parte di chi esercita la responsabilità genitoriale⁹¹⁶. Il par. 2 tuttavia prevede che gli Stati

in *The Citizen Lab*, 22 Marzo 2021, <https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/>

⁹¹⁵ V. a tal proposito il comunicato stampa con cui il garante annuncia l'apertura di formale procedimento amministrativo contro TikTok nel dicembre 2020, cui faremo cenno *infra*: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *TikTok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network*, 22 dicembre 2020, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923>.

⁹¹⁶ La disposizione in parola va letta alla luce, in particolare, del *considerando* 38, che recita: « I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali». Passaggio che merita particolare attenzione è il successivo periodo, che afferma: «Tale *specifica protezione* dovrebbe, in particolare, riguardare *l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente* e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore». E ancora, per ciò che più nello specifico attiene al perimetro applicativo dell'art. 8 «Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore». Ricordiamo anche l'importante proposizione conclusiva dell'art. 71, che nel riferirsi alla profilazione osserva puntualmente come «Tale misura non dovrebbe riguardare un minore».

membri possano derogare a tale norma stabilendo un'età inferiore, purché entro i limiti dei 13 anni: e di tale clausola di apertura si è avvalso il legislatore italiano, che all'art. 1 dell'art. 2-*quiquies* del novellato Codice della Privacy modificato dal d.lgs. n. 101/2018, ha previsto come in relazione alla medesima fattispecie possa esprimere consenso valido il minore che abbia compiuto 14 anni - per i soggetti di età inferiore il trattamento essendo lecito a condizione che il consenso sia prestato da chi esercita la responsabilità genitoriale.

Tuttavia, è facile constatare come tali garantistiche norme siano agevolmente eludibili attraverso la creazione da parte del minore di falsi profili. E tale vicenda ha interessato in particolar modo TikTok, nei confronti del quale il Garante italiano ha aperto nel mese di dicembre un formale procedimento contestandogli, oltre alla violazione degli obblighi di trasparenza, di chiarezza e di completezza dell'informativa, la facile "eludibilità" del divieto di iscriversi alla piattaforma per i minori di 13 anni⁹¹⁷.

Tuttavia, ciò non è bastato ad evitare il terribile fatto di cronaca, legato alle c.d. *Challenge* settimanalmente proposte dal social ai suoi utenti, che ha tragicamente coinvolto una bambina di Palermo di dieci anni, morta di soffocamento per prendere parte ad una di queste, la "*Blackout Challenge*". A seguito di tale fatto, che ha sconvolto l'opinione pubblica, il Garante ha adottato il Provvedimento del 22 gennaio 2021, con cui in forza degli artt. 58 par. 2 lett. f) e 66 del Regolamento UE 2016/679 adottava un rimedio insieme inibitorio e limitativo, disponendo il blocco immediato del trattamento dei dati degli utenti per i quali non fosse stata accertata con sicurezza l'età anagrafica, e ciò fino al 15 febbraio dello stesso anno, poi prorogato tanto con due successivi provvedimenti

⁹¹⁷ V. nota n. 47853 del 15 dicembre 2020; e cfr. ancora una volta GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, «Tik Tok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network», 22 dicembre 2020, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9508923>.

del mese di febbraio e di marzo⁹¹⁸. Solo successivamente a tale dura risposta del Garante, TikTok ha dato attuazione alle richieste/ingiunzioni del Garante, provvedendo a disattivare tutti gli account degli utenti italiani ed invitandoli ad inserire nuovamente la data di nascita.

È in tale contesto che si inserisce il recente e rilevante provvedimento in punto di profilazione online sui *social network*, riguardante proprio TikTok, che si intende esaminare a titolo conclusivo. Il rilievo di tale caso è amplificato dal fatto che, nel contesto del procedimento e del conseguente provvedimento, esplicitamente il Garante si occupa del tema dei processi decisionali interamente automatizzati di cui all'art. 22 del GDPR, e segnatamente di quelli in cui il trattamento a monte della decisione consista nella profilazione.

Ci riferiamo al Provvedimento adottato d'urgenza il 7 luglio 2022 per avvertire la piattaforma TikTok circa l'illiceità dell'utilizzo di dati personali archiviati nei dispositivi degli utenti allo scopo di profilarli in funzione del conseguente invio ai suddetti di pubblicità personalizzata in assenza di un esplicito consenso. Secondo il Garante, infatti, il legittimo interesse, che TikTok stesso modificando la propria *privacy policy* (e quindi l'informativa sul trattamento) indicava come base giuridica per alcune tipologie di futuri trattamenti a tali scopi, non rappresentava affatto un idoneo fondamento di liceità, a fronte della violazione della Direttiva *e-Privacy* (e stante, tra l'altro, la sussistenza di elementi sufficienti a qualificare l'attività predetta come processo decisionale interamente automatizzato ex art. 22 del GDPR)⁹¹⁹. Vediamo di scendere un poco più nel dettaglio della pronuncia.

⁹¹⁸ Cfr. rispettivamente Provv. n. 20 del 22 gennaio 2021, [doc. web n. 9524194]; Provv. n. 61 dell'11 febbraio 2021, [doc. web n. 9554603]; Provv. n. 126 del 25 marzo 2021, [doc. web n. 9574709].

⁹¹⁹ V. Provv. n. 248 del 7 luglio 2022, [doc. web n. 9788429], disponibile qui: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9788429> ;

A partire dal mese di giugno 2022, TikTok annunciava la modifica della propria *privacy policy*, comunicando agli utenti, anche mediante specifici messaggi, l'intenzione di avviare, a far data dal successivo 13 luglio 2022, un'attività di fornitura di «pubblicità personalizzata (...) agli utenti dai 18 anni in su» consistente nel mostrare a questi «annunci personalizzati in base alla [rispettiva] attività sull'app di TikTok». Il trattamento si sarebbe basato su «Informazioni che ci fornisci, Informazioni raccolte *automaticamente* e Informazioni da altre fonti», allo scopo di mostrare ai propri utenti «annunci che possano essere di loro interesse e per collegare gli inserzionisti con gli utenti che possano essere interessati ai loro prodotti o servizi»⁹²⁰: ma ancora più rilevante è la circostanza che tali trattamenti di dati personali avrebbero trovato, ad avviso della piattaforma, «la propria base giuridica nel “legittimo interesse” di cui all'art. 6, par. 1, lett. f) del Regolamento, anziché nel consenso degli interessati»⁹²¹.

Nel corso dell'istruttoria avviata dal Garante, la società, nel rispondere alle richieste dell'Autorità, nelle sue memorie affermava in particolare che a partire dal 13 luglio 2022 i trattamenti finalizzati a mostrare annunci personalizzati basati sui soli dati tratti dall'«Attività su TikTok» (che, come la stessa sottolineava, comprendono «dati ricavabili da attività su TikTok: informazioni raccolte direttamente dalle azioni dell'utente sulla piattaforma»), e per i soli utenti di età superiore ai 18 anni, avrebbero trovato la base giuridica nei «legittimi interessi perseguiti da TikTok», dai suoi partner pubblicitari e dai suoi utenti ai sensi dell'art. 6, paragrafo 1, lettera f), del GDPR. Imponendo quest'ultima

cfr. anche il relativo comunicato stampa, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, «Tik Tok: Altolà del Garante Privacy alla pubblicità “personalizzata” basata sul legittimo interesse. Base giuridica inadeguata e rischi che la pubblicità arrivi anche ai minori», 11 luglio 2022, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9788342>.

⁹²⁰ Così, come puntualmente riportato dal Garante, si esprime la modificata *privacy policy* della piattaforma, nel suo complesso precedentemente disponibile qui: <https://www.tiktok.com/legal/new-privacy-policy?lang=it-IT>).

⁹²¹ Prov. n. 248 del 7 luglio 2022, [doc. web n. 9788429], par. 1.

disposizione un attento bilanciamento, come sappiamo, tra l'interesse medesimo e i diritti, le libertà e i legittimi interessi dell'interessato medesimo, TikTok affermava (in modo, all'evidenza, generico), di aver effettuato tutte le valutazioni pertinenti ai sensi del GDPR, e che queste ultime avessero dato esito positivo. La società aggiungeva poi che in punto di base giuridica per le c.d. «Attività fuori da TikTok», non vi sarebbe stata alcuna modifica, per cui il social avrebbe continuato a basarsi sul consenso dell'utente ai sensi dell'art. 6, par. 1 lett. a), del GDPR⁹²².

A fronte di tali deduzione difensive, il Garante rileva in via preliminare come «non [possa] non evidenziarsi un *approccio della piattaforma al tema della base giuridica piuttosto ondivago e piegato alle varie esigenze di volta in volta emergenti*», richiamando la stessa vicenda appena analizzata dell'illecito trattamento dei dati dei minori dei 13 anni sfociata nel blocco dell'utilizzo dei dati degli utenti, avendo TikTok stesso ivi insistito sull'opportunità della base giuridica del consenso per gli utenti dai 16 anni in su. Il Garante riprova con fermezza, insomma, un approccio che sembra degradare la scelta della base giuridica a «disinvolto utilizzo della migliore opzione di volta in volta selezionabile da parte del titolare»⁹²³.

Di seguito, il Garante evidenzia allora una nutrita serie di criticità, riscontrando come «non [sia] stata sufficientemente rappresentata la modalità di svolgimento delle attività di pubblicità personalizzata basate sulla raccolta diretta dei dati relativi alle azioni dell'utente sulla piattaforma né il fondamento giuridico legittimante il trattamento dei dati in questione». Non solo non è stato esplicitato agli utenti quale sia il legittimo interesse perseguito dal titolare e da terzi (partner pubblicitari), nonché (addirittura) dagli stessi utenti, né tantomeno è stato specificato se il trattamento riguardi categorie particolari di dati di cui all'art. 9 e

⁹²² Ivi, par. 2.

⁹²³ Ivi, par. 3.1.

se sussista una delle eccezioni che, parallelamente al legittimo interesse (per tale trattamento inadeguato), giustificano ex par.2 il trattamento medesimo; ma soprattutto «il test di bilanciamento è indicato in modo generico e insufficiente a consentire una adeguata valutazione della sua correttezza alla luce dei criteri forniti dalla giurisprudenza della Corte di Giustizia dell'Unione europea» nella sentenza *Rīgas satiksme*⁹²⁴. Il Garante ritiene conseguentemente che il bilanciamento, nella specie, non sarebbe stato soddisfatto, richiamando le importanti considerazioni, sotto il profilo esegetico, svolte dall'EDPB nelle Linee Guida sul *targeting* sui social media: «il mero adempimento dei doveri di informazione a norma dell'art. 13 del GDPR - menzionato al primo punto del test di bilanciamento - non costituisce una misura di trasparenza da prendere in considerazione per la ponderazione degli interessi conformemente all'art. 6, paragrafo 1, lett. f) del GDPR»⁹²⁵.

Il Garante prosegue con altri rilievi fondamentali. Dall'informativa, infatti, risulta che «vengono con alto grado di probabilità effettuate operazioni a fini di “personalizzazione” della pubblicità che comportano verosimilmente l'uso di cookie o di altre tecniche di tracciamento (anche di terze parti)». Inoltre, e ciò rileva ancor più ai nostri fini, dalla stessa informativa si evince che, con un grado

⁹²⁴ V. C. Giust. UE, 4 maggio 2017, C-13/16, *Rīgas satiksme*; ivi la CGUE, pur nella vigenza della Dir. 95/46/CE e dunque, in relazione alla base giuridica del legittimo interesse, dell'art. 7 lett.f) della direttiva, individua un test articolato in tre fasi ai fini della valutazione circa l'esito positivo del bilanciamento imposto dal legislatore europeo ai fini della sussistenza della base giuridica del legittimo interesse, parimenti valido in relazione al disposto dell'attuale art. 6, par. 1, lett. f) del GDPR. Al par. 28, infatti, la Corte afferma che: «l'articolo 7, lettera f), della direttiva 95/46 prevede tre condizioni cumulative affinché un trattamento di dati personali [fondato sul c.d. legittimo interesse del titolare e/o del responsabile del trattamento] sia lecito, vale a dire, in primo luogo, il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi [titolare e/o responsabile del trattamento “secondario”] cui vengono comunicati i dati; in secondo luogo, la necessità del trattamento dei dati personali per il perseguimento dell'interesse legittimo; e, in terzo luogo, la condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata dalla tutela dei dati.

⁹²⁵ Cfr. COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 8/2020 sul targeting degli utenti dei social media*, il 13 aprile 2021, pag. 22, punto 66.

altrettanto alto di probabilità, le operazioni di profilazione compiute nel contesto dei predetti trattamenti, che la società ritiene di fondare da quel momento in poi sulla base giuridica del legittimo interesse, *«comportano anche processi di decisione automatizzata ai sensi dell'art. 22 del Regolamento in assenza delle previste garanzie»*. Infine, nella stessa informativa «il diritto di opposizione non è posto in adeguata evidenza»⁹²⁶.

Tali profili presentano, per il Garante, evidenti fronti di contrasto con buona parte della disciplina sulla cui analisi già ci siamo intrattenuti.

Ai sensi dell'informativa, infatti, TikTok intendeva tra l'altro utilizzare sulla base del legittimo interesse «informazioni raccolte automaticamente» ovvero, sempre ai sensi di quanto previsto nella medesima informativa, «informazioni sul dispositivo (...) che includono il modello del tuo dispositivo, il sistema operativo, i pattern o i ritmi di digitazione, l'indirizzo IP e la lingua del sistema (...)», nonché informazioni sulla posizione dell'utente e simili. Nella stessa informativa si riferiva inoltre che TikTok raccoglie e utilizza «cookie e simili tecnologie di tracciamento per gestire e fornir[ti]e i nostri servizi», e che tali tecnologie sono utilizzate «anche per finalità di marketing»⁹²⁷.

Ebbene, le operazioni in parola contrasterebbe con la tutt'ora vigente Direttiva direttiva 2002/58/CE (*e-Privacy*), in particolare con l'art. 5 par. 3, trasposto nell'ordinamento italiano dall'art. 122 del Codice della Privacy, ancora vigente, che stabilisce al comma 1: « L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato

⁹²⁶ Provv. n. 248 del 7 luglio 2022, [doc. web n. 9788429], par. 3.1.

⁹²⁷ Ivi, par. 3.2.

informato con modalità semplificate». La dizione è sufficientemente ampia da ricomprendere, chiaramente, anche l'utilizzo dei *cookies* di profilazione⁹²⁸.

Il descritto quadro normativo è già in sé e per sé sufficiente a consentire al Garante di «escludere che il legittimo interesse possa rappresentare una idonea base giuridica almeno per il trattamento, ai fini dell'invio di pubblicità personalizzata, di tutti quei dati personali che nell'informativa di TikTok vengono definite "informazioni raccolte automaticamente" e, pertanto, di ritenere illecito, almeno parzialmente, a prescindere da ogni ulteriore e successivo approfondimento, il trattamento dei dati personali degli utenti che Tik Tok intende intraprendere a far data dal prossimo 13 luglio»⁹²⁹.

E tuttavia, il Garante si sofferma anche sul secondo profilo di contrasto, emergente dall'informativa, tra la fattispecie di cui si sta occupando e le disposizioni tanto generali quanto speciali in relazione ai *processi decisionali ricadenti nell'alveo dell'art. 22 del GDPR* in materia di trattamenti algoritmici, specialmente laddove qualificabili come operazioni di profilazione.

A tal riguardo, l'Autorità richiama le Linee Guida sul processo decisionale automatizzato, osservando come esse, in punto di profilazione, e già nell'analisi delle disposizioni applicabili a *tutti* i trattamenti automatizzati, con o senza coinvolgimento umano effettivo, «indicano una serie di elementi di cui occorre tener conto, nell'ambito del necessario *balancing test* (grado di dettaglio e granularità del profilo, esaustività dello stesso, impatto sull'interessato, presenza di garanzie finalizzate ad assicurare la correttezza e a mantenere l'esattezza del trattamento nonché a prevenire discriminazioni)», ricordando opportunamente come già il «precedente parere del WP29 sul concetto di legittimo interesse (Parere 06/2014), seppure basato sull'art. 7 dell'abrogata direttiva 95/46/CE, riteneva difficile per il titolare del trattamento giustificare il ricorso al legittimo

⁹²⁸ *Ibidem.*

⁹²⁹ *Ibidem.*

interesse come base legittima per pratiche intrusive di profilazione e tracciamento per finalità di marketing o pubblicità»⁹³⁰. Il rilievo conclusivo, sul punto, appare ancora più importante: «Dirimente deve poi ritenersi quanto già chiarito dal WP29, ovvero che il legittimo interesse del titolare del trattamento non può rendere lecita la profilazione se il trattamento, *come parrebbe essere quello effettuato da Tik Tok nella fattispecie in esame*, rientra nella definizione di cui all'art. 22, par. 1 del Regolamento»: laddove ci si trovasse di fronte ad una serie di operazioni che insieme compongano una fattispecie di processo decisionale - interamente- automatizzato relativo alle persone fisiche, che soddisfi gli ulteriori requisiti di cui al par. 1 dell'art. 22 e dunque ricada nell'ambito di applicazione del relativo divieto generale, il legittimo interesse sarebbe *a priori* escluso, non rappresentando quest'ultimo una delle basi giuridiche che in via eccezionale, *ex* par. 2 al ricorrere delle misure adeguate di tutela obbligatorie di cui al par. 3, sono idonee a fondare la liceità del processo medesimo, in deroga al suddetto divieto generale⁹³¹.

Infine, a sottolineare ancora una volta l'attenzione riservata all'età degli utenti dopo i tragici fatti del 2021, il Garante manifesta la preoccupazione secondo cui: «in assenza di elementi certi per l'identificazione della persona maggiore di età, alla luce anche delle negative prove sin qui susseguites in ordine alla capacità di TikTok (al pari di altri social network) di effettuare tale valutazione, [la piattaforma] rischia di coinvolgere nella suddetta attività anche le persone minori di 18 anni, ma anche di anni 14, per i quali sarebbe necessario un consenso degli

⁹³⁰ Ivi, par. 3.3.. V. assai ampiamento *retro*, cap. 3, par. 2 ss., e cfr. ancora una volta GRUPPO DI LAVORO ARTICOLO 29 SULLA PROTEZIONE DEI DATI PERSONALI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit,

⁹³¹ *Ibidem*. Vi ampiamente cap. 3, par. 2.3.

esercenti la responsabilità genitoriale e, in ipotesi anche dei minori di anni 13, per i quali l'accesso alla piattaforma sarebbe del tutto interdetto»⁹³².

Tutte le considerazioni su esposte conducono il Garante, nella specie (stante l'evidenza della violazione in questione rispetto a quella, probabile ma non accertata, dell'art. 22 del GDPR), a concludere che «l'attività di somministrazione di pubblicità commerciale “personalizzata”, da parte di TikTok agli utenti maggiorenni, attraverso attività di profilazione dei loro comportamenti all'interno del social network, almeno nella misura in cui risulti basata, come espressamente riferito dalla società, sulle c.d. “informazioni raccolte automaticamente” e archiviate sul dispositivo degli utenti non possa basarsi giuridicamente sull'interesse legittimo ponendosi tale attività in contrasto con l'art. 5, par. 3 della Direttiva e-privacy e l'art. 122 del Codice». A ciò consegue, nelle conclusioni del Garante, che «nelle more dell'acquisizione di eventuali maggiori elementi informativi, in considerazione delle violazioni rilevate e della competenza del Garante, si ritiene necessario rivolgere, ai sensi del combinato disposto di cui all'art. 58, par. 2, lett. a), del Regolamento e all'art. 154, comma 1, lett. f), del Codice *un avvertimento a TikTok*, evidenziando che il trattamento previsto può verosimilmente configurare una violazione della disciplina vigente con le connesse responsabilità di un trattamento basato su una base giuridica non corretta».⁹³³

La vicenda esaminata, successivamente al provvedimento in esame, ha trovato positiva conclusione pochissimi giorni dopo: a seguito dell'avvertimento del Garante Privacy, TikTok ha infatti prontamente sospeso il passaggio al legittimo interesse come base giuridica per la pubblicità personalizzata per le persone maggiori di 18 anni, e dunque fondata sulla profilazione dei

⁹³² *Ibidem.*

⁹³³ Ivi, Conclusioni.

comportamenti tenuti nella navigazione sulla piattaforma. Nel comunicato stampa del 12 luglio (il giorno dopo aver annunciato il provvedimento adottato d'urgenza il 7 luglio), il Garante scrive che l'istituzione «prende atto della decisione “responsabile” del social network e si dichiara aperta a un dialogo finalizzato alla ricerca del bilanciamento tra interessi economici e diritti degli utenti»⁹³⁴.

La vicenda, e l'epilogo in questione, rappresentano un ulteriore dimostrazione del ruolo indispensabile svolto dalle Autorità Garanti quali imprescindibile presidio per l'effettività delle norme a tutela dei fondamentali interessi all'integrità della vita privata, della riservatezza e dell'autodeterminazione informativa, colti nella loro dimensione sociale, e dunque quali interessi da cui dipende l'edificazione stessa di una società della dignità. Tale ruolo, di fronte alla proliferazione dei sistemi algoritmici, e vieppiù di IA, applicati al trattamento dei dati personali, appare coesistente alla sopravvivenza dell'irrinunciabile diritto di costruire liberamente la propria personalità, come singoli e nelle formazioni sociali in cui andrà a svolgersi, secondo la luminosa lettera dell'art. 2 della nostra Costituzione, ed oggi anche dell'art. 1 della Carta dei diritti fondamentali dell'Unione Europea, che (lo si recita nuovamente) afferma: «La dignità umana è inviolabile. Essa deve essere rispettata e tutelata».

Assumendo, ancora una volta, come bussola il nesso tra tecnica, società e diritto, e i suoi riflessi sulla costruzione della disciplina preordinata alla protezione della sfera privata, aspetto fondamentale e indefettibile della dignità umana, facciamo nuovamente rotta verso le sponde dell'ordinamento in cui,

⁹³⁴ V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, «Tik Tok rinvia la pubblicità basata sul legittimo interesse. Per il Garante privacy “una decisione responsabile”», comunicato stampa del 12 luglio 2022, <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9789143>.

convenzionalmente, ha avuto origine la storia giuridica della *privacy*. È ora di interrogarci sull'esistenza e sulla latitudine della disciplina del trattamento automatizzato dei dati personali negli Stati Uniti d'America.

CAPITOLO QUARTO

DATA PRIVACY E AUTOMATED DECISION-MAKING SYSTEMS: LA DISCIPLINA STATUNITENSE

SOMMARIO: 4.1. Il modello settoriale di data privacy and protection law statunitense, tra technology dependence e flusso transfrontaliero di dati. L'assenza di una legislazione federale unitaria – 4.1.1. Automated decision making systems: sulle tracce di una disciplina frammentaria. I rilievi della Commissione Europea nelle decisioni di adeguatezza del Privacy Shield e del Data Privacy Framework – 4.2. Automated data processing nei rapporti tra Government e Citizen: la giurisprudenza della Supreme Court sul Quarto Emendamento nella società degli algoritmi. “Is there any reasonable expectation of privacy in there”? – 4.2.1. Electronic Communication Privacy Act: le proposte della dottrina circa un divieto di monitoraggio automatizzato delle comunicazioni elettroniche – 4.3. La disciplina federale degli automated decision making systems nei rapporti tra privati: sector specific statutes e consumer protection – 4.3.1. ADM e consumer credit system: i regimi di consumer disclosure e di adverse action notice nel Fair Credit Reporting Act e nell'Equal Credit Opportunity Act – 4.3.2. Discriminazione algoritmica ed Equal Protection Laws: in particolare, il Titolo VII del Civil Rights Act e il Fair Housing Act – 4.3.3. La Sezione 5 del Federal Trade Commission Act: unfairness, deception e processi decisionali automatizzati – 4.4. California Consumer Privacy Act: il modello giuridico di riferimento della legislazione statale in materia di data privacy. Un passo avanti: il recente Draft for Automated Decisionmaking Technology Regulations

4.1. Il modello settoriale di *data privacy and protection law* statunitense, tra *technology dependence* e flusso transfrontaliero di dati. L'assenza di una legislazione federale unitaria

Siamo tornati nel cuore dell'ordinamento statunitense, dove come ormai ben sappiamo più di centoventi anni fa, nell'ambito di un saggio di poco più di trenta pagine, è stata posta la prima pietra del complesso, moderno edificio giuridico della *privacy*, e consequenzialmente della *data protection*⁹³⁵.

Dando per assunte la ricognizione storica e l'analisi delle categorie giuridiche fondamentali del diritto statunitense in materia, che abbiamo puntualmente introdotto nel primo capitolo (cui si fa sin d'ora rinvio, poiché indispensabile per approcciarsi senza "bias" all'oggetto del discorso che seguirà), nel presente capitolo focalizzeremo lo sguardo sulla disciplina dei trattamenti e insieme dei processi decisionali automatizzati: fenomeni che, adottando la

⁹³⁵ Si anticipa subito che fondamentali, ai fini della ricerca e dello studio sugli argomenti trattati nel presente capitolo, nonché della sua redazione, sono stati lo studio, cui ampiamente si farà riferimento nel prosieguo, della Commissione Europea, ai fini del monitoraggio sull'E.U.-US. Privacy Shield, sull'esistenza e la conformazione di un regime normativo in punto di *automated decision making* negli Stati Uniti, G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (Commissione Europea, 2018); la ricerca, ricca di spunti accademici e bibliografici importanti, di C. TABARRINI, *La trasparenza algoritmica nel trattamento dei dati personali. Prospettive eurounitarie e statunitensi*, Università Ca' Foscari, Venezia, 2022, p. 161 ss.; il già ampiamente citato lavoro di U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit.; gli interessati contributi raccolti in N.S. LIND, E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 400; l'ampia panoramica disegnata da D.J. SOLOVE, M. ROTENBERG, P.M. SCHWARZ, *Privacy, Information and Technology*, Aspen Law & Business, 2006; da P.P. SWIRE, K. AHMAD, *Foundations of Information Privacy And Data Protection*, International Association of Privacy Professionals, Portsmouth, 2012; e da D. J. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, George Washington University of Law School, 2004; il sintetico ma efficace affresco generale di S. H. BOYNE, «Data Protection in the United States», in *The American Journal of Comparative Law*, vol. 66, 2018. A tali contributi, anche laddove non puntualmente seguiti e citati, il rinvio s'intende implicito.

terminologia propriamente utilizzata nel contesto ordinamentale statunitense, sono identificati rispettivamente dalle espressioni *automated data processing* (ADP) e *automated decision making* (ADM)⁹³⁶. O meglio, ciò che faremo sarà andare *alla ricerca* delle fonti, positive e giurisprudenziali, in cui sia dato ravvisare le *tracce* della disciplina medesima, specialmente in relazione al secondo fenomeno. Come meglio spiegheremo a breve, la premessa da cui occorre partire, le cui ragioni (in prima approssimazione) devono pur sempre ascriversi al diverso modularsi del rapporto tra tecnologia e diritto nell'ambito dell'esperienza giuridica statunitense, è che gli Stati Uniti difettino non solo di un quadro unitario, bensì anche di una trama di sub-sistemi normativi settoriali, informati ad un *corpus* di coerenti principi desumibili dalla giurisprudenza costituzionale, in punto di disciplina della *data privacy* rispetto ai fenomeni di (*solely o human involved*) *automated decision making*⁹³⁷. Nel prosieguo, andremo pertanto alla ricerca di una disciplina specialistica lacunosa (così come lo è, a livello positivo, la più generale disciplina della *data privacy* in cui si iscrive), la costruzione della

⁹³⁶ V. ampiamente *retro*, cap. 1. Ulteriore premessa terminologica, su cui già ci siamo soffermati ma che appare importante ribadire, è che negli Stati Uniti la nozione eurounitaria di protezione dei dati personali, nella sua sostanziale identità con la dimensione dell'autodeterminazione informativa, risulta generalmente sintetizzata nel concetto di *informational privacy* (sottocategoria della *proprietary privacy*), più comunemente nota come *data privacy*. Sul punto, oltre che alle più approfondite riflessioni svolte nei par. 1.2 e 2 del cap. 1, cfr. P.P. SWIRE E K. AHMAD, *Foundations of Information Privacy And Data Protection*, International Association of Privacy Professionals, Portsmouth, 2012, 4; S. COBB, «Data Privacy and Data Protection: U.S. Law and Legislation», in *WeLiveSecurity*, 2016; S. H. BOYNE, «Data Protection in the United States», in *The American Journal of Comparative Law*, vol. 66, 2018

⁹³⁷ Cfr. già da ora uno dei documenti, già citati, che è risultato fondamentale ai fini della ricognizione normativa, giurisprudenziale e dottrinale che delinearemo nel corso del presente capitolo, ossia G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (Commissione Europea, 2018), 33. Ad avvalersene ampiamente per la sua ricognizione sulla disciplina degli automated decision making systems in America è la stessa C. TABARRINI, *La trasparenza algoritmica nel trattamento dei dati personali*, cit., p. 161 ss.

quale sta ricevendo tuttavia negli ultimi anni un rilevante impulso dagli sforzi concettuali della dottrina, dalla sensibilità dei legislatori statali e dalle criticità che hanno contrassegnato il rapporto tra U.S.A ed Unione europea in punto di trasferimenti transcontinentali di dati personali. A volte esplicitamente, a volte tra le righe, si porranno a confronto gli apparati di garanzie attualmente disponibili in materia nell'ordinamento statunitense e in quello europeo (quest'ultimo ampiamente analizzato nel capitolo precedente), con particolare riguardo alla decisiva fattispecie dei processi decisionali *interamente* automatizzati: ciò, allo scopo di interrogarci sull'esistenza, nei diversi formanti del sistema giuridico statunitense, di un'attenzione analoga a quella dedicatagli dal legislatore europeo con la predisposizione del sub-sistema di cui all'art. 22 del GDPR.

Per compiere tale ricerca nel quadro di un ordinamento di *common law* caratterizzato da una vivacità culturale, da una dialettica valoriale, insomma da un'ontologica (verrebbe da dire) attitudine genetico-evolutiva, opportuna sarà l'adozione di quella prospettiva che (lo si ripete ancora una volta), rifacendoci ad un'importante opera del secolo scorso, abbiamo definito *Law in the Making*, la quale valorizza la dimensione del *diritto come processo*, invitando pertanto a studiare tale fenomeno socio-istituzionale così come esso *concretamente* evolve e si sviluppa nel corso del tempo⁹³⁸. Solo così riusciremo a cogliere, sotto le spoglie di un quadro giuridico disomogeneo, le *tendenze fondamentali* che, a fronte dell'inarrestabile progresso della tecnica, e dunque dell'inevitabile diffondersi degli strumenti algoritmici nel trattamento dei dati personali, emergono in seno alla società civile e alla comunità degli operatori del diritto e

⁹³⁸ V. *retro*, cap. 1 par. 1.2; cfr. ancora una volta C. K. ALLEN, *Law in the Making*, Clarendon Press, Oxford 1955.

guidano il *processo* di edificazione di un apparato normativo che governi il rapporto tra contesto digitale, Intelligenza Artificiale ed *informational privacy*⁹³⁹.

Prima di addentrarci nel merito, occorre tuttavia svolgere un'ultima panoramica sul contesto, culturale e giuridico, in cui si collocano tanto l'attenzione contemporanea per la materia degli *ADM systems* quanto frammentario sistema normativo di cui andremo ad occuparci, concentrandoci su due profili essenziali.

Il primo è di carattere “sistemologico”, e attiene ad una di quelle problematiche che si colloca al confine tra micro e macrocomparazione⁹⁴⁰: ci si riferisce all'individuazione, attraverso una lettura sistematica dei diversi *corpora* normativi in materia, delle differenze fondamentali intercorrenti tra modello giuridico cui risponde la tutela della *privacy* e dell'autodeterminazione informativa nel contesto ordinamentale statunitense e in quello europeo. Condurremo tale analisi necessariamente *per distinzione*, avendo già approfonditamente delineato nel capitolo precedente (cui si rinvia) i caratteri che contraddistinguono l'ordinamento europeo, i quali qui ci limiteremo a riepilogare. Allo stesso tempo, stante il suo inevitabile carattere classificatorio, e dunque il punto di vista *statico* di cui risente, condurremo tale analisi riconoscendone l'insufficienza epistemologica: con ciò ribadendone la strumentalità al solo scopo di dotarci di alcune coordinate essenziali per orientarsi nel successivo livello “specialistico”⁹⁴¹.

⁹³⁹ Cfr. già sul punto M. LETA JONES, «The right to a human in the loop: Political constructions of computer automation and personhood», 47, *Social Studies of Science*, 2, 2017, sul quale torneremo *infra*.

⁹⁴⁰ Per i temi in questione, e per le problematiche che circondano la sottodisciplina stessa della “sistemologia”, cfr. V. VARANO, V. BARSOTTI, *La tradizione giuridica occidentale. Testo e materiali per un confronto tra civil law e common law*, cit., I, in part. p. 41 ss.

⁹⁴¹ Sul carattere intrinsecamente relativo, e potenzialmente etnocentrico, di ogni classificazione, cfr. A. SOMMA, Introduzione al diritto comparato, cit., passim. Per una puntuale analisi dell'evoluzione del rapporto tra la disciplina statunitense ed europa della *privacy* e della

Innanzitutto, possiamo concordare con quelle proposte ricostruttive, confortate dalle considerazioni svolte nel capitolo precedente, che, accanto al suo carattere evidentemente *generale*, sottolineano come il modello di tutela della vita privata e dell'autodeterminazione informativa vigente in conteso eurounitario si configuri come *prevalentemente legislativo e tecnologicamente neutrale* (“*technology-independent*”)⁹⁴².

Al contrario, come noi stessi abbiamo ampiamente evidenziato nel corso del primo capitolo, l’approccio statunitense alla disciplina della *privacy property* (inizialmente) e della *privacy dignity* (successivamente al graduale processo di “trasformazione assiologica” seguito dall’organico della Corte Suprema), e dagli anni 70 in poi dell’*information privacy*, risulta tradizionalmente giurisprudenziale e casistico, e solo di riflesso legislativo o *statutario*. Ciò ha prodotto, come conseguenza, non solo la proliferazione di una moltitudine di fonti sul piano tanto federale quanto statale, di *statute law* come di *common law*, unificate solo dal quadro dei principi delineati dalla giurisprudenza costituzionale per lo più a partire dal fondamentale caso *Katz v. United States*⁹⁴³; ma anche il connotato

data protection, cfr. P.M. SCHWARTZ, «The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures», *Harv. L. Rev.*, 126, 2013, 1966ss.

⁹⁴² Cfr. in part. D. KLITOU, *Privacy-Invasive Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014, 40 ss, richiamato da C. TABARRINI, *La trasparenza algoritmica*, cit., p. 162.. È indispensabile ricordare, a tal proposito, il fondamentale incipit del considerando 15 del Regolamento UE 2016/679, che così recita: «Al fine di evitare l’insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere *neutrale sotto il profilo tecnologico* e non dovrebbe dipendere dalle tecniche impiegate». Sui vantaggi di un approccio tecnologicamente neutrale alla disciplina tanto dei prodotti della tecnica quanto degli interessi economici o piuttosto inerenti alla persona che con essi si confrontano, in quanto fondato sulla definizione di «principi generali che possono rimanere invariati per un certo periodo di tempo, senza essere vincolati al mutamento delle tecnologie», cfr. G. FINOCCHIARO, «Intelligenza Artificiale e protezione dei dati personali», cit., p. 1670 ss.; e più approfonditamente ID., «Riflessioni su diritto e tecnica», in *Dir. Inf.*, IV-V/2012, p. 831 ss.

⁹⁴³ Cfr. ancora una volta *Charles Katz v. United States*, 389 U.S. 347 (1967), laddove si afferma principio secondo cui «la tutela del diritto generale alla privacy spettante all’individuo dipende in gran parte dalla legge dei singoli Stati [federati]», che sono dunque liberi, dove lo

marcatamente “*technology-dependent*” della disciplina che ne è scaturita, dal momento che essa (come dimostra la storia della pluralità di *statutes* adottati dal Congresso a partire dal *U.S. Privacy Act* per rispondere alle sempre maggiori innovazioni tecnologiche, dai semplici *electronic records* fino al più recente *cloud computing storage*⁹⁴⁴) reagisce *caso per caso* ai nuovi prodotti del progresso tecnologico, mancando di disegnare un *legal framework* generale che prescindendo dalle singole declinazioni della tecnologia in costante divenire⁹⁴⁵.

Altra fondamentale differenza tra i due sistemi pare potersi identificare nella visione principalmente personalistica, o *human rights-oriented* che, come già ampiamente sottolineato, in conseguenza del generale percorso di costituzionalizzazione del diritto privato europeo su impulso fondamentale della Corte di Giustizia, caratterizza l’attuale disciplina della *data protection* vigente in Europa, principalmente per effetto del Regolamento UE 2016/679 (GDPR): visione dalla quale, come sappiamo, discende poi una generale diffidenza rispetto alla qualificazione del dato personale in termini di bene giuridico - anche - patrimoniale, stante il dogma dell’incommerciabilità degli attributi della personalità⁹⁴⁶. Al contrario, nel contesto ordinamentale statunitense persiste una cultura mercantilista che accoglie con favore il fenomeno dello sfruttamento commerciale dei dati personali e risulta propensa a considerare la potenziale

ritengano opportuno, nell’esercizio della propria discrezionalità normativa, di estendere la sfera di tutela della *privacy* rispetto al *minimo* costituzionalmente previsto.

⁹⁴⁴ Per una generale panoramica di tipo diacronico sui principali atti normativi intervenuti a livello federale, v. cap. 1, par. 2.

⁹⁴⁵ D. KLITOU, *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, cit.; S. H. BOYNE, «Data Protection in the United States», in *The American Journal of Comparative Law*, cit., U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa* cit.. In senso propriamente critico, F. BIGNAMI, «European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining», in *Boston College Law Review* 48(609), 2007; C. J. BENNETT, «In defense of privacy: the concept and the regime», in *Surveillance & Society*, 8 (4), 2011, pp. 485-496.

⁹⁴⁶ V. *retro*, cap. 3 par. 1 ss., e cfr. per una sintesi in punto di resistenza alla “commodification” dei dati personali V. ZENO- ZENCOVICH, «Do “Data Markets” Exist?», in *MediaLaws*, I, 2019, p. 22 ss.

implementazione di un sistema di garanzie rafforzate degli attributi della personalità, compresi dunque i primi, un *unfair burden for business*⁹⁴⁷; inoltre, per ragioni storiche, in punto specifico di tutela della *privacy* l'attenzione tanto del legislatore quanto della giurisprudenza (soprattutto, è evidente, della *Supreme Court*) è stata molto più orientata al rapporto tra privati e pubblici poteri, e dunque al fenomeno delle interferenze governative nella sfera privata, con la conseguente moltitudine di decisioni relative all'interpretazione del Quarto Emendamento come fondamento privilegiato del *constitutional right to privacy* nei rapporti verticali⁹⁴⁸.

I suddetti caratteri del sistema in esame, a dispetto dell'importante ruolo di garanzia svolto dalla dottrina e dalla giurisprudenza nell'enucleare un *right to privacy* - ed oggi *to data privacy* - davvero informato a principi liberal-umanitari, e dunque nel promuovere una concezione *costituzionale* di privacy come nucleo essenziale o “clausola implicita” di qualsiasi libertà fondamentale⁹⁴⁹, hanno condotto e tutt'ora conducono larga parte della dottrina, non solo europea, a rivolgere aspre critiche al modello di tutela della *privacy* che appare vigere nell'ordinamento statunitense. La ragione principale, tuttavia, sembra potersi identificare nella riscontrata assenza di una legislazione federale onnicomprensiva in materia di *privacy* e di *data protection*, a fronte di un'eterogeneità di *statutes* federali di natura settoriale cui solo di recente stanno reagendo i legislatori statali con l'implementazione di normative onnicomprensive - e di nuova generazione -

⁹⁴⁷ Cfr. S. COBB, «U.S. Data Privacy Legislation», cit., p. 3; P.M. REGAN, «Personal information policies in the United States and Britain: The dilemma of implementation considerations», in *Journal of Public Policy*, 4(01), 1984, pp. 19-38

⁹⁴⁸ V. *retro*, cap. 1, par. 1.3. Cfr. ancora S.M. BOYNE, *Data Protection in the United States*, cit.; G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. Inf. e inform.*, 2015, 697ss.; ed anche, in una prospettiva storica, A. Baldassarre, *Privacy e Costituzione*, cit., p. 159.

⁹⁴⁹ Cfr. ancora le brillanti riflessioni di W. O. DOUGLAS, «Dissenting Opinion», in *Public Utilities v. Pollak*, 343, U. S. 467, riprese nella sua magistrale *chief opinion* nel caso *Griswold v. Connecticut* di cui ci siamo ampiamente occupati.

in materia (sebbene ciò non faccia che accrescere la frammentazione normativa in seno all'ordinamento in esame)⁹⁵⁰. Altrettanto insufficienti parrebbero le forme di autoregolamentazione, o “*codes of conduct*”, approntate dai “corpi intermedi” di categoria, rinforzate dalla vigilanza della *Federal Trade Commission*⁹⁵¹.

In tale contesto, le critiche principali si appuntano sulle lacune esistenti, anche a livello positivo, proprio in relazione alla *data protection* nei rapporti tra privati, specialmente di carattere commerciale, dove il *data subject* (ovvero l'interessato) parrebbe sempre e solo degradato al livello di consumatore⁹⁵². Di conseguenza, esse si estendono alla sostanziale carenza di previsioni *general*i che garantiscano i diritti di accesso o di cancellazione dei dati, e i corrispondenti doveri informativi (ad esempio di predisposizione di dettagliata informativa e di *data breach*), e che prima ancora individuino le *tassative* basi giuridiche per il trattamento, in primis elevando il consenso informato degli interessati a cardine della disciplina medesima, e dunque a fondamento *generale* di liceità: tale scenario, si sottolinea, pare rendere infatti le *corporates*, e più nello specifico le società di *Data Analytics*, libere di operare in un contesto sostanzialmente privo

⁹⁵⁰ V. puntualmente i riferimenti a nota 933, a cui possiamo aggiungere I. BERLE, *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal*, in *Law, Governance and Technology Series*, Springer, Cham, 2020, 93ss.

⁹⁵¹ Sui *codes of conduct* la cui implementazione viene promossa dalla stessa FTC, sui poteri regolatori della quale ci sofferemmo un poco meglio *infra*, cfr. C. J. BENNET, D. MULLIGAN, «The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy», 2012, disponibile su dx.doi.org/10.2139/ssrn.2230369; D. SOLOVE, P.M. SCHAWRTZ, *Information Privacy Law*, cit., pp. 36-39.

⁹⁵² Cfr. ancora P.M. REGAN, «*Personal information policies in the United States and Britain: The dilemma of implementation considerations*», cit., laddove, con riflessioni sempre attuali, sottolinea che storicamente le lobbies rappresentative di interessi commerciali, oggi identificabili negli OTT, «*argued that including private sector data controllers in a comprehensive regime of data privacy protection stifles trade and unfairly burdens businesses*».

di restrizioni in funzione di garanzia degli attributi fondamentali dei *data subjects*
953.

Ebbene, in tali critiche non può non scorgersi una preferenza marcata per il modello implementato dal legislatore eurounitario: nel riceverle, e in buona parte condividerle, noi non dobbiamo tuttavia commettere, in questa sede, l'errore di giudicare con le lenti del *civil law* continentale, e più in generale del nostro sostrato culturale di estrazione, un'esperienza che da quella in cui è immerso il giurista europeo si distingue pressoché sotto ogni profilo.

Restando dunque aderenti al nostro proposito di descrivere, prima di giudicare, la realtà ordinamentale con cui ci confrontiamo, occorre qui riportare parimenti alcune delle voci che, piuttosto, hanno difeso il modello in commento, se non stimato quest'ultimo più garantista rispetto a quelli esistenti in altri ordinamenti nazionali o piuttosto sovranazionali. Tra quelle più temperate, vi sono le tesi di chi, pur condividendo le critiche su esposte, avverte di non sottovalutare molti dei profili virtuosi espressi dalla «*US privacy protection*»: ovvero, nello specifico, la crescente sensibilità dei legislatori di tutti e 50 gli Stati Federati, la maggior parte dei quali vanno dotandosi di normative idonee a garantire quanto meno un bilanciamento tra diritti fondamentali degli interessati e contrapposti interessi (per lo più) economici dei *data controllers*; il ruolo svolto dall'«*America's privacy watchdog*», ovvero la FTC; e la stessa vivacità della *case law*, e segnatamente del *common law* dei singoli Stati, intervenuto in materia di privacy sul piano dei rapporti tra privati, dove al contrario la pur considerevole

⁹⁵³ Cfr. ex multis J.N. SLOANE, «Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation», in *J. Marshall L.J.*, 12, 2019, pp. 23-29; A.C. RAUL, C.C. FRONZONE E S.S. TAPIA, «United States», in A.C. Raul (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019, 400 ss.

giurisprudenza della Corte Suprema ha sempre avuto riguardo essenzialmente alla *privacy* nei rapporti tra *individual* e *gouvernement*⁹⁵⁴.

Accanto a tale lettura temperata, bisogna anche riportare le voci di coloro che, come accennato, considerano più garantista l'ordinamento statunitense, perlomeno laddove *privacy* e *data protection* si legano alla materia dei *search and seizures* ed ai connessi profili delle intercettazioni e dell'accesso alle comunicazioni elettroniche, nonché dell'utilizzo nell'ambito del procedimento penale di prove illegalmente ottenute, stante la rigogliosa giurisprudenza della *Supreme Court* in relazione al Quarto Emendamento e alla *Due Process Clause* e agli atti normativi (anche in risposta agli interventi della Corte Suprema) implementati in materia⁹⁵⁵.

Tuttavia, è proprio sotto quest'ultimo profilo che appare più evidente il contrasto tra la predetta lettura e la "realtà dei fatti": nonostante l'innegabile attenzione riservata dalle Corti statunitensi ed anche dal legislatore federale, a partire dallo stesso *U.S. Privacy Act* del 1974, in punto di ingerenze pubbliche nella sfera privata del cittadino, questa - come puntualmente riscontrato nella ricognizione storica condotta nei primi due capitoli - non ha impedito

⁹⁵⁴ Cfr. in particolare S. COBB, «Data privacy and data protection», cit., p. 6. Per una prima analisi circa le basi giuridiche e il contenuto dell'attività svolta dalla *law enforcement Authority* in questione, v. *retro*, cap. 1, par. 1.2.

⁹⁵⁵ Cfr. in particolare P. SWIRE, D. KENNEDY-MAYO, «How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information», in L. J. EMORY., 55, 2017, pp. 617-642, che come sottolinea S.H. BOYNE, «Data Protection in the United States», cit., sarebbe tale, secondo gli autori, per otto ragioni, così sintetizzate: « (1) *oversight of searches by independent judicial officers*; (2) *probable cause of a crime as a relatively strict requirement for both physical and digital searches*; (3) *even stricter requirements for government use of telephone wiretaps and other real-time interception*; (4) *the exclusionary rule, preventing prosecutors' use of evidence that was illegally obtained, is supplemented by civil suits*; (5) *other legal standards that are relatively strict for government access in many non-search situations, such as the judge-supervised "reasonable and articulable suspicion" standard under the Electronic Communications Privacy Act of 1986 (ECPA)*; (6) *transparency requirements, such as notice to the service provider of the legal basis for a request*; (7) *lack of data retention requirements for Internet communications*; and (8) *lack of limits on use of strong encryption*.»

l'implementazione ,soprattutto in territorio statunitense, di programmi di sorveglianza di massa. In proposito, sembra opportuno ricordare anche in questa sede che il più recente di tali programmi, in seguito alle rivelazioni dell'ex dipendente dell'NSA Edward Snowden, ha costituito oggetto dello scandalo c.d. *Datagate*, che ha dato origine, in prima battuta, alla sentenza *Schrems I* con cui la Corte di Giustizia ha sancito l'invalidità della decisione di adeguatezza della Commissione Europea in relazione al *Safe Harbor Agreement* sulla cui base l'Unione europea e gli Stati Uniti sin dall'inizio del nuovo millennio avevano fondato il trasferimento transfrontaliero di dati personali⁹⁵⁶. In seconda battuta, lo scandalo ha dato origine alla stessa sentenza *Schrems II* con cui la Corte nel 2020, salvando la decisione 2010/87 sull'adeguatezza dei trasferimenti basati sulle c.d. Clausole Contrattuali Standard e sulle c.d. Norme Vincolanti d'Impresa (seppur a fronte della predisposizione di garanzie supplementari da parte dei titolari del trattamento), ha a sua volta invalidato la decisione con cui la Commissione Europea aveva riconosciuto l'adeguatezza del *Privacy Shield*, adottato nel 2016 per ri-autorizzare il medesimo trasferimento transcontinentale, carente di adeguata base giuridica dopo il primo caducatorio intervento della Corte⁹⁵⁷.

Senza ripetere rilievi già svolti in precedenza, ciò che qui appare importante sottolineare è come in entrambi i casi la motivazione precipua si fondi sulla riscontrata carenza di uno *standard di tutela dei diritti fondamentali sostanzialmente equivalente* a quello oggi garantito dal GDPR, letto alla luce della Carta dei diritti fondamentali dell'Unione europea⁹⁵⁸. Carenza che può imputarsi

⁹⁵⁶ V. ampiamente *retro*, cap. 2 par. 2.2.4. V. ancora una volta C. Giust. UE, C-362/14, *Maximilian Schrems/Data Protection Commissioner*, 6 ottobre 2015.

⁹⁵⁷ V. ampiamente *retro*, cap. 2 par. 2.2.4. V. ancora C. Giust. UE, C-311/18, *Data Protection Commissioner v. Maximilian Schrems e Facebook Ireland*, 16 luglio 2020. Cfr. anche in materia Cfr. E. TEROLLI, «Privacy e protezione dei dati personali IE vs USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza “Schrems II”», in *Diritto dell'informazione e dell'informatica*, 1, 2021, 49 ss.

⁹⁵⁸ Può essere qui utile sottolineare quali siano i principi in cui, secondo l'allora Gruppo di Lavoro Articolo 29, dovrebbe articolarsi lo standard di equivalenza che rappresenta il criterio

per molti aspetti alla forte propensione dell'ordinamento statunitense ad implementare pervasivi sistemi di garanzie per la sicurezza nazionale, anche attraverso disposizioni potenzialmente restrittive della *privacy* individuale, promuovendo lo sviluppo di tecnologie che sono state definite, con fortunata formula da noi già ricordata, tecnologie «pubblico protettive»⁹⁵⁹. Tale propensione peraltro può facilmente riscontrarsi nella successiva vicenda che ha

cui la Commissione Europea sarebbe tenuta a conformarsi nel giudicare circa l'adeguatezza del sistema di protezione dei dati oggetto di trasferimento transfrontaliero a norma della dir. 95/46/CE e del Reg. UE 2016/679: secondo il Gruppo, fondamentale rilievo dovrebbe essere assegnato all'esistenza nell'ordinamento del Paese terzo di: (i) una serie di concetti e nozioni base quali quelle di "dati personali", "trattamento", "titolare del trattamento", etc.; (ii) una chiara indicazione delle basi giuridiche idonee a rendere i trattamenti leciti; (iii) limiti alle finalità del trattamento; (iv) principi volti a garantire il rispetto di canoni di correttezza, aggiornamento e necessità dei dati trattati; (v) principi volti a garantire il rispetto di un canone di minimizzazione dei dati; (vi) regole di condotta deputate ad assicurare la sicurezza dei dati e prevenire accessi non autorizzati agli stessi; (vii) diritti informativi idonei ad assicurare un certo grado di trasparenza del trattamento; (viii) diritti di accesso, rettifica, opposizione e cancellazione dei dati; (ix) limitazioni al trasferimento dei dati verso soggetti terzi; (x) specifiche salvaguardie a tutela di particolari categorie di dati (come quelli sensibili); (xi) diritti di opposizione a trattamenti finalizzati a marketing personalizzato; (xii) condizioni di liceità di processi decisionali unicamente automatizzati e relativi diritti di conoscenza della logica seguita, di rettifica di eventuali erroneità nei dati utilizzati e di contestare decisioni assunte sulla base di presupposti fattuali scorretti. Dal punto di vista procedurale, invece, nel definire le caratteristiche minime di effettività dell'infrastruttura di *enforcement*, il Gruppo di Lavoro ha ribadito la necessità di rinvenire nell'ordinamento del paese terzo: (i) una autorità indipendente e imparziale competente a monitorare e far rispettare la normativa in materia di protezione dei dati; (ii) adeguati strumenti di *compliance* e sensibilizzazione degli operatori del settore quali ispezioni e misure sanzionatorie; (iii) misure di responsabilizzazione degli operatori volte ad imporgli la conduzione di valutazioni d'impatto o altre procedure intere idonee a consentirgli l'assolvimento dell'onere probatorio a loro carico in punto di compliance; (iv) rimedi effettivi volti a sanzionare violazioni accertate e riconoscere agli interessati risarcimenti per i danni eventualmente subiti. GRUPPO DI LAVORO ARTICOLO 29, *Adequacy Referential*, adottato il 29 novembre 2017, aggiornato al 6 febbraio 2018, (WP 254 rev.01), 3-9 adottato in revisione del WP12, *Working Document: Transfers of personal data to third countries. Applying Articles 25 and 26 of the EU data protection directive*, adottato il 24 luglio 1998; linee guida richiamate dalle stesse sentenze *Schrems I* e *Schrems II*.

⁹⁵⁹ Cfr. ancora una volta A. ETZIONI, *How Patriotic is the Patriot Act? Freedom versus Security in the Age of Terrorism*, Routledge, New York-London 2004. Per una riflessione sulle difficoltà che ha incontrato e tutt'ora incontra il sistema di check and balances statunitense nel settore della sicurezza nazionale, specialmente in relazione all'ascesa dei BigTechs, cfr. M.C. MENEGHETTI, «Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali», in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 423 ss

condotto all’invalidazione dell’*U.S. E.U. Privacy Shield*, se si considera che, contestualmente alla predisposizione del nuovo quadro per il trasferimento transfrontaliero dei dati personali tra Stati Uniti e UE, gli USA predisponavano unilateralmente l’assai criticato *Clarifying Lawful Overseas Use of Data Act* (meglio noto come *CLOUD Act*), diretto a disciplinare l’accesso transfrontaliero a materiale probatorio elettronico nel contesto di indagini in sostituzione del *Mutual Legal Assistance Treaty* (MLAT), e che dunque assicurava alle Corti statunitensi il potere di “autorizzare” *Internet Service Providers* a fornire accesso a informazioni da essi digitalmente archiviate, seppure in *servers* collocati al di fuori del territorio degli Stati Uniti⁹⁶⁰.

Il riferimento alle interferenze governative nella *privacy* individuale e agli scandali sulla sorveglianza di massa che, da *M.A.T.R.I.X.* a *Datagate*, hanno avuto ampia risonanza globale, ci introduce al secondo profilo che caratterizza il contesto della disciplina statunitense della *data privacy*, in senso altrettanto *evolutivo*. Ci riferiamo proprio al tema del flusso transnazionale, e nella specie transcontinentale, di dati personali, e a come questo rappresenti, in estrema sintesi, per gli Stati Uniti una risorsa strategica irrinunciabile, stante la concentrazione sul territorio statunitense dei principali attori della quarta rivoluzione industriale, e quindi del panorama ICTs: dalle aziende specializzate nella progettazione e nella produzione di microprocessori ai principali produttori di componentistica e di

⁹⁶⁰ A svolgere rilievi critici in relazione all’atto normativo in questione, che sembrava neutralizzare in partenza l’impegno assunto con il *Privacy Shield* dagli Stati Uniti nell’implementare un sistema di garanzie (in relazione al trattamento di dati personali “provenienti” dall’Europa) per soddisfare gli standard di tutela previsti dal diritto europeo, è stato sin da subito lo stesso EUROPEAN DATA PROTECTION BOARD, *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence*, Bruxelles, 10 luglio 2019. Sul punto cfr. C. TABARRINI, *La trasparenza algoritmica*, cit., p. 165 e in part. nota 536; J. DASKAL, «Microsoft Ireland, the Cloud Act, and International Lawmaking» 2.0, 71, *Stan. L. Rev. Online*, 9, 10ss.

digitized devices, dai motori di ricerca come Google e Yahoo ad altri OTT del calibro di Meta. Ebbene, vicende come *Datagate* hanno inevitabilmente condotto (e continuano a condurre) le istituzioni tanto federali quanto statali statunitensi ad aprire un dialogo sulla predisposizione di un modello legislativo in definitiva *generale* di tutela della *privacy*, sulla cui base poter soddisfare, nel quadro di un omogeneo regime internazionale di protezione dei dati personali, le pretese (principalmente) del partner europeo circa la protezione dei diritti fondamentali degli individui stabiliti “al di qua” dell’oceano, come condizione per il libero dispiegarsi di quel flusso - altrimenti interrotto dalla Corte di Giustizia dell’UE, in quanto guardiano dei diritti medesimi - che quasi unilateralmente corre dall’Europa verso gli Stati Uniti⁹⁶¹.

A tale processo sembrerebbero riconducibili alcuni dei più recenti interventi normativi tanto, sul piano interno quanto sul piano internazionale, implementati dalle istituzioni statunitensi. A tal scopo, si può guardare innanzitutto al nuovo accordo, da noi già citato, negoziato in materia di *transborder flows* di dati personali con gli USA, denominato «quadro UE-USA per la protezione dei dati personali» (c.d. *E.U.-U.S. Data Privacy Framework*)⁹⁶². Quest’ultimo, infatti, recependo le preoccupazioni espresse dalla Corte di Giustizia nelle sentenze *Schrems*, implementa ulteriori garanzie a favore dei *data subjects*: tra le molteplici, si riscontrano l’esplicita sanzione del principio di «*accountabilty for onward transfer*» e l’individuazione nello specifico del *right to access* degli interessati qualificato come «*fundamental to privacy protection*»,

⁹⁶¹ Sul ruolo di “traino” svolto dalla stessa Unione Europa rispetto al dibattito istituzionale in corso negli Stati Uniti in punto di modernizzazione in senso *fundamental rights-oriented* della disciplina nel proprio contesto ordinamentale vigente, cfr. R. PETRUCCO, «The Right to privacy and new technologies: between evolution and decay», cit., p. 20 ss.; S. CALZOLAIO, «Privacy by design», cit., p.6 ss.

⁹⁶² COMMISSIONE EUROPEA, *Commision implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final; al primo Annesso si trova il vero e proprio testo dell’accordo negoziato con gli USA.

dal momento che «*it allows individuals to verify the accuracy of information held about them*»⁹⁶³; la limitazione dell'accesso ai dati trasferiti dal territorio dell'Unione da parte dei servizi di intelligence statunitensi a quanto necessario e proporzionato⁹⁶⁴; e l'istituzione di un tribunale del riesame in materia di protezione dei dati (*Data Protection Review Court*, DPRC), accessibile ai cittadini dell'UE⁹⁶⁵. Ai nostri fini, come a breve vedremo, risulta importante un insieme di *considerando* dedicati al fenomeno degli *automated decision making* e all'effettiva sussistenza nell'ordinamento statunitense di un sistema di garanzie adeguate ai fini della tutela dei diritti degli interessati che sia sostanzialmente equivalente a quello incardinato nel diritto europeo, con particolare riguardo ai *completely automated systems*⁹⁶⁶.

Allo stesso processo può ricondursi anche quel complessivo movimento che sta attraversando gli Stati della Federazione, e che come accennato si identifica nella predisposizione di normative in punto di *data privacy and protection* debitorie al modello *generale* di tutela vigente nell'ordinamento europeo: se già la dottrina riscontrava quasi un decennio fa come «*many of America's 50 states have passed legislation mandating stronger protection of personal information than the federal government requires*» e che «*each state in the union has its own constitution and 10 of these include an explicit right of privacy*»⁹⁶⁷, negli ultimi anni sono entrate in vigore in diversi Stati normative di c.d. nuova generazione, ossia ancora più garantistiche per l'*information privacy* dei *data subjects* (ad esempio fondante sul principio dell'*opt in*, e dunque della centralità del consenso *attivo* informato quale base giuridica del trattamento), che

⁹⁶³ Ivi, cons. 20 ss.; *Annex I, EU-U.S. Data Privacy Framework Principles Issued by the U.S. Department of Commerce*, cap. II, par. 3 e par. 6, nonché cap. III, par. 8.

⁹⁶⁴ Ivi, cons. 171;

⁹⁶⁵ Ivi, cons. 185 ss.

⁹⁶⁶ Ivi, cons. 33-36, su cui v. *infra*.

⁹⁶⁷ Cfr. S. COBB, «Data Privacy and Data Protection», cit. p. 6.

della circolazione del modello giuridico rappresentato dall'archetipico *California Consumer privacy Act* (CCPA) hanno fortemente risentito⁹⁶⁸.

Infine, non può non ascriversi al medesimo processo anche la proposta presentata al Congresso il 21 giugno 2022 di un atto normativo *federale*, preordinato a dettare una regolamentazione *generale* in materia di *data privacy* sul piano dei rapporti interprivati, e segnatamente dunque dei trattamenti svolti da professionisti e *corporates* in relazione ai *consumer personal data*: ci riferiamo al *draft* del c.d. *American Data Privacy and Protection Act*⁹⁶⁹. Il progetto è stato definito come «*the first proposed federal online privacy bill*», incardinato attorno ai principi *data minimization* e *individual ownership*⁹⁷⁰; tuttavia, lo stesso ha incontrato le resistenze, tra l'altro, del *chair* of the *Senate Commerce Committee* Maria Cantwell e dei rappresentanti della categoria delle *BigTech Companies*, e il suo percorso di approvazione non è stato compiuto prima dell'aggiornamento del 117° Congresso, il 3 gennaio 2023⁹⁷¹. Pertanto, la proposta, finché non

⁹⁶⁸ V. subito *California Consumer Privacy Act* of 2018 (CCPA), in CAL. CIV. CODE §§ 1798.100–.192 (West 2018), *as amended by California Privacy Rights Act* of 2020 (CPRA), entrato in vigore nella sua versione emendata il 1 gennaio 2023, su cui ci soffermeremo alla fine del capitolo; le altre normative di nuova generazione attualmente in vigore sono *Nevada Privacy Law*, SB 220, *which amends Chapter 603 A (Security and Privacy of Personal Information) of Nevada Revised Statutes* (NRS); *Virginia Consumer Data Protection Act* (VCDPA) (*Effective January 1, 2023*), in Code of Virginia. Chapter 53 § 59.1-575 – 585; *Colorado Privacy Act* (CPA), SB 21-190, July 7, 2021 (*Effective July 1, 2023*); *An Act Concerning Personal Data Privacy and Online Monitoring (The Connecticut Data Privacy Act or “CTDPA”)*, SB 6, May 10, 2022 (*Effective July 1, 2023*).

⁹⁶⁹ V. H.R.8152 - *American Data Privacy and Protection Act*. Sul sito del Congresso, all'apposita sezione, sono consultabili tutte le *actions* intraprese sul punto alla Camera e al Senato: <https://www.congress.gov/bill/117th-congress/house-bill/8152/text>.

⁹⁷⁰ Cfr. ex multi M. DUMIAK, «Federal Privacy Bill: Breaking Down the ADPPA», in *JD Supra*, 24 giugno 2022, <https://web.archive.org/web/20220625161839/https://www.jdsupra.com/legalnews/federal-privacy-bill-breaking-down-the-9181745/>; Castro, Daniel (June 13, 2022). "A Review: The American Data Privacy and Protection Act". GovTech, <https://web.archive.org/web/20220717141916/https://www.govtech.com/policy/a-review-the-american-data-privacy-and-protection-act>.

⁹⁷¹ Cfr. MCGILL, MARGARET HARDING, «Online privacy bill faces daunting roadblocks», 4 agosto 2022 Axios, <https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress>.

ripresentata da un membro del Congresso, non potrà costituire oggetto di discussione: in ogni caso, stante l'importanza dei principi stabiliti nel suo quadro, essa costituirà oggetto di rapido commento a conclusione del presente capitolo.

4.1.1. *Automated decision making systems*: sulle tracce di una disciplina frammentaria. I rilievi della Commissione Europea nelle decisioni di adeguatezza del *Privacy Shield* e del *Data Privacy Framework*

Completato il quadro di riferimento, possiamo metterci sulle tracce della specifica disciplina statunitense degli ADP e degli ADM, principiando dal *legal framework* che connota l'ordinamento federale; ma ciò non prima di esserci nuovamente introdotti nel folto dei principi dettati dalla giurisprudenza della *Supreme Court* in punto di *constitutional privacy*, per interrogarci sulla loro applicabilità al contesto digitale.

È necessario svolgere ancora una premessa di ordine metodologico. Come già abbiamo sottolineato nella parte dedicate alle definizioni generali risultanti dall'impianto del GDPR, alla luce dell'esegesi condotta dalle Linee Guida del Gruppo di Lavoro Articolo 29 ampiamente commentate, nel contesto della *personal data protection* trattamento dei dati personali e processo decisionale rappresentano fenomeni, concetti o domini distinti, sebbene il secondo "racchiuda" il primo: con il primo termine infatti, nell'ordinamento angloamericano tradotto con l'espressione *data processing*, come sappiamo si fa riferimento a qualsiasi operazione compiuta in relazione ad una o più informazioni riguardante una persona fisica; il secondo concetto, nell'ordinamento in esame chiamato *decision-making*, individua piuttosto la complessiva sequenza di atti e

fatti che conduce ad adottare una decisione relativa ad una persona fisica, di cui l'elaborazione dei dati rappresenta *solo* la prima fase, prodromica alla produzione dell'output decisionale⁹⁷².

Ebbene, come sappiamo altrettanto bene, il trattamento stesso può essere (ed anzi oggi viene necessariamente) svolto attraverso l'impiego dell'automazione, e segnatamente della tecnologia algoritmica: a seconda del maggiore o minore coinvolgimento umano, saremo in presenza di un *solely* (o *completely*, o *fully*: tutti sinonimi in letteratura) o di un *semi- automated data processing*. Laddove il trattamento si iscriva nel quadro di un processo decisionale, saremo allora in presenza di una fattispecie di *automated decision making*, a sua volta parzialmente o interamente tale (*solely* o *semi*) a seconda di quanto significativo sia il contributo, in termini di esercizio della propria razionalità, offerto dall'essere umano "revisore" alla determinazione del contenuto della decisione.

Abbiamo premesso tale sintetica e chiaramente approssimativa ricognizione concettuale - a costo di essere ridondanti - al fine di circoscrivere esattamente l'oggetto della nostra indagine nel presente capitolo. È lapalissiano come oggi, stante l'ubiquità della tecnologia computazionale, informatica ed algoritmica, il trattamento anche solo parzialmente *automatizzato* dei dati (qui, da intendersi, personali), specialmente nel settore dei rapporti commerciali e consumeristici e nell'ambito dell'attività della pubblica amministrazione, rappresenti la regola, e quello manuale l'eccezione⁹⁷³. La stessa disciplina settoriale statunitense, per quanto non brilli in termini di teoria generale, raramente ricollegando ad un sistema di categorie generali (come quella di *data*

⁹⁷² V. cap. 3, par. 2.2.

⁹⁷³ V. cap. 2, par. 3, e cfr. ancora una volta *ex multis* G. BUTTARELLI, *Banche dati e tutela della riservatezza*, cit., passim, e in tempi non sospetti S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit.

processing) gli elementi delle fattispecie regolate, proprio in virtù della sua anima *technology dependent* sembra chiaramente individuare quale proprio referente oggettivo soprattutto (verrebbe da dire) gli «*automated personal data systems*»: sebbene le disposizioni considerino soltanto quelle *species* di operazioni rilevanti (e inevitabilmente coinvolgenti dati personali) nel settore di cui si occupano, queste ultime devono ritenersi concepite e regolamentate dalle prime specialmente nella loro declinazione “elettronica” o automatizzata⁹⁷⁴. A tal proposito, è infatti sufficiente ricordare come le disposizioni cui ci riferiamo nascano proprio *in conseguenza* dell’avvento dell’elaborazione elettronica dei dati, con l’obiettivo stesso di governare lo sviluppo tecnologico⁹⁷⁵.

La conseguenza naturale di tale premessa sarebbe quella di dire indagare, come abbiamo fatto nell’approcciarci al GDPR, in primo luogo sulle disposizioni dei molteplici *statutes* federali in materia di *privacy* (passati in rassegna, lo si ricorderà, alla fine del primo capitolo) che risultino applicabili anche -o, nella *società degli algoritmi*, soprattutto- alle ipotesi di *automated processing of personal data*. Senonché l’opera in questione, stante il denunciato carattere settoriale del modello di *data privacy* statunitense e le profonde differenze in termini di scopi e di strutture intercorrenti tra i corrispondenti sub-sistemi

⁹⁷⁴ V. *retro*, cap. 1, par. 2. In punto di definizioni, ricordiamo che lo stesso report dell’HEW raccomandava l’implementazione di un codice applicabile ad «*all automated personal data systems*»: cfr. ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens*; V. poi *U.S. Privacy Act*, che individua una fattispecie particolare di data processing, rilevante ai fini della disciplina che codifica, affermando che «*the term “matching program”—(A) means any computerized comparison of— (i) two or more automated systems of records (...)*»; l’FCRA, poi, come vedremo più nel dettaglio, nell’individuare come *species* di *data processing* il «*consumer reporting*», nell’ambito del c.d. *credit scoring* (che ne rappresenta una sottocategoria) si occupa anche dell’ipotesi di «*automated underwriting systems*».

⁹⁷⁵ V. ancora *retro*, cap. 2 par. 3.

normativi, si risolverebbe in un'analisi inevitabilmente approssimativa dei diversi prodotti della legislazione federale della *data protection*⁹⁷⁶.

Più utile appare allora assumere come punto di riferimento della nostra indagine proprio il fenomeno che, come abbiamo ampiamente sottolineato nel corso della trattazione, più di tutti sembra sfidare nella contemporaneità le capacità del diritto di rispondere alle istanze individuali e collettive di protezione della sfera privata: alludiamo, ovviamente, ai sistemi decisionali algoritmici, e dunque alle fattispecie di processo decisionale automatizzato, o *automated decision making*, che una qualsiasi forma di trattamento automatizzato inevitabilmente assumono come premessa. Tale focus specifico risulta, in definitiva, maggiormente coerente con l'intenzione di indagare l'attuale declinazione del rapporto tra tecnologia, intimità e diritto nel contesto ordinamentale statunitense, così come abbiamo fatto per l'ordinamento europeo.

Assumendo la predetta prospettiva, possiamo indirizzare la nostra ricerca verso gli atti normativi federali da cui siano desumibili, in base alla loro lettera, o alla luce di determinati indirizzi interpretativi promossi dalla dottrina e/o accolti dalla giurisprudenza, principi e regole di dettaglio applicabili ai processi decisionali automatizzati; una volta individuati, potremo allora “stringere l'obiettivo” su questi ultimi e prima ancora sulla loro struttura generale; e, infine, potremo interrogarci sulla loro idoneità a predisporre garanzie simili a quelle enunciate dall'art. 22 del GDPR. Così, pur dovendoci arrendere all'insussistenza di disciplina federale unitaria, potremo esprimere un giudizio più consapevole circa l'idoneità o meno della disciplina vigente in ciascun settore considerato (*rectius*: nei settori in cui sia vigente) a proteggere effettivamente l'“illesa intimità” dell'individuo. E, al contempo, potremo guardare agli sviluppi che

⁹⁷⁶ Per una sintetica ricostruzione del composito quadro della disciplina settoriale di livello federale della *data privacy and protection* statunitense, cfr. ancora S. H BOYNE, «Data Protection in the United States», cit.

all'orizzonte si profilano, e consentono di identificare il sistema di garanzie apprestato in favore dell'individuo in ordine ai sistemi di *automated decision making*, nel quadro della regolamentazione dei *data processing* (oggi, altrettanto *automated*), come una *disciplina (per lo più) in costruzione*.

Soffermandoci sull'individuazione degli atti normativi federali in cui rintracciare la disciplina in parola, risulta opportuno ascoltare, e qui riportare, le voci di quegli autori che hanno evidenziato come, se da una parte il legislatore europeo sembri tradizionalmente muovere dall'esigenza di proteggere gli interessati dai rischi configurati dall'utilizzo dell'automazione a fini decisionali, il legislatore statunitense muova dall'*opposto assunto* per cui il carattere automatizzato delle decisioni è garanzia di maggior «*accuracy, efficiency, and computational neutrality*»⁹⁷⁷.

Per tale ragione, la stessa Commissione europea, nel quadro della decisione di adeguatezza del *U.S. E.U. Privacy Shield*, al *considerando 25*, partendo dal riconoscimento del sempre più frequente ricorso, nell'ambito dell'economia digitale, a un «trattamento automatizzato (profilazione compresa) come base per l'adozione di decisioni che si ripercuotono sulle persone», affermava come

⁹⁷⁷ Si veda M. LETA JONES, «The right to a human in the loop: Political constructions of computer automation and personhood», 47, in *Social Studies of Science*, 2, 2017, pp. 216-239, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2758160 ; l'autrice, in un rilevante passaggio, afferma come «*[w]hile the person and people of Europe may be legally constituted as entities protected from automated decision-making and deserving of a human in the loop, those in the U.S. are protected from the flaws of humanity through the computational neutrality of information systems*». Il diametralmente opposto approccio delle istituzioni europee traspare, come è noto, da pressoché tutte le linee guida e dai disparati atti di soft law del Gruppo di Lavoro e dell'attualmente operante European Data Protection Board, della Commissione Europa, del Garante europeo e dei Garanti nazionali che abbiamo avuto modo di citare e, in alcuni casi, di commentare nel secondo e nel terzo capitolo, cui si fa integralmente rinvio. Per le sue ragioni storiche, cfr. anche ABRAHAM NEWMAN, «Protectors of Privacy: Regulating Personal Data in the Global Economy», 74-75 (2008), che afferma: «*[T]he EU data privacy directive can be traced to its roots in the historical sequencing of national data privacy regulation and the role that the resulting independent regulatory authorities played in regional politics.*».

l'*automated decision making* rappresentasse «un settore su cui esercitare un monitoraggio attento», per agevolare il quale si era convenuto con le autorità statunitensi «di comprendere nel primo riesame annuale e, secondo il caso, in quelli successivi un dialogo sul processo decisionale automatizzato, confrontandosi tra l'altro sulle analogie e sulle differenze d'impostazione tra l'UE e gli USA»⁹⁷⁸.

Occorre rilevare che allo stesso *considerando* la Commissione giustificasse la scelta di *non* riprodurre (o l'impossibilità di farlo) nel quadro del *Privacy Shield* la garantistica disposizione di cui all'art. 22 del GDPR, come già tra l'altro avvenuto all'art. 15 della previgente Direttiva Madre nel contesto del *Safe Harbor Agreement*, sulla base del rilievo (o pregiudizio?) secondo cui nei settori in cui più fosse «diffuso *tra le imprese* il ricorso al trattamento automatizzato dei dati personali per l'adozione di decisioni che si ripercuotono sulla persona (erogazione di credito, offerta di prestiti ipotecati, lavoro ecc.)» la legge statunitense offrisse «tutele specifiche contro le decisioni sfavorevoli»: il riferimento correva, in nota, a titolo di esempio all'*Equal Credit Opportunity Act*, al *Fair Credit Reporting Act* e al *Fair Housing Act*, e veniva sottolineato come le disposizioni degli atti in parola contemplassero diritti sostanzialmente analoghi alle «misure aeguate di tutela» imposte dal par. 3 dell'art. 22, nonché ai diritti di cui dagli art. 13 par. 2 lett g ss.⁹⁷⁹.

⁹⁷⁸ Cfr. Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (GU 2016, L 207, pag. 1), cons. 25.

⁹⁷⁹ *Ibidem*, nota 23, che si riporta testualmente: «Cfr., ad esempio, la legge sulle pari opportunità nel credito (ECOA — Codice degli Stati Uniti d'America, titolo 15, articolo 1691 e ss.), legge sull'informativa corretta nel credito (FRCA — Codice degli Stati Uniti d'America, titolo 15, articolo 1681 e ss.) o legge sulle pari opportunità negli alloggi (FHA, Codice degli Stati Uniti d'America, titolo 42, articolo 3601 e ss.).»

Tuttavia, tanto il primo report annuale della Commissione al Parlamento europeo⁹⁸⁰, quanto il report del Gruppo di Lavoro al primo *Joint Review* evidenziavano come i rilievi di cui al *considerando 25* necessitassero di un riscontro fattuale, non essendo noto se e in che misura i dati personali trasferiti dall'Europa ai titolari stabiliti negli USA costituissero oggetto di *automated decision making systems*⁹⁸¹.

Su tale base, e pertanto allo scopo precipuo di misurare «*the relevance of automated decision-making for transfers carried out on the basis of the Privacy Shield*»⁹⁸², la Commissione europea commissionava uno studio deputato a curare una ricognizione empirica e giuridica della disciplina sui processi decisionali automatizzati vigente negli Stati Uniti, le cui risultanze apparivano, e appaiono tutt'ora (a fronte del pressoché identico quadro normativo) ai nostri fini molto importanti⁹⁸³. In tale Studio, oltre a riscontrare la pressoché evidente realtà secondo cui «*automated processing—as distinct from decisions based solely on that processing—is taking place in many U.S. sectors, some of which are covered by specific laws*», in primo luogo si affermava chiaramente come, diversamente da quanto previsto dall'articolo 22 del GDPR, negli USA *non* sussistesse alcun

⁹⁸⁰ Cfr. COMMISSIONE EUROPEA, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield* (Bruxelles, 18 ottobre 2017) (COM (2017) 611 fin.).

⁹⁸¹ GRUPPO DI LAVORO ARTICOLO 29 SULLA PORTEZIONE DEI DATI PERSONALI, *EU – U.S. Privacy Shield – First annual Joint Review*, Bruxelles, 27 novembre 2017, https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782, in particolare laddove si sottolinea l'opportunità di indagare «*the extent of the practical relevance of automated decision making processes by Privacy Shield certified companies*» e, se necessario, «*the possibility to provide for specific rules concerning automated decision making to provide sufficient safeguards including the right to know the logic involved and to request reconsideration on a non-automated basis*».

⁹⁸² COMMISSIONE EUROPEA, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, cit.

⁹⁸³ G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (Commissione Europea, 2018), 8.

divieto generale relativo a «*decisions based solely on automated processing, including profiling, which produce legal or similarly significant effects*»⁹⁸⁴. In secondo luogo, gli autori dello Studio, prefiggendosi l'obiettivo di individuare, in relazione ai settori in cui l'impegno di *automated decision making systems* apparisse più frequente, le normative di riferimento e di esaminare l'effettiva adeguatezza delle garanzie predisposte dalle medesime (*rectius*: la loro equivalenza rispetto al sistema predisposto dall'UE), individuavano i predetti settori, tra gli altri, nei campi del trattamento di dati sanitari a fini assicurativi, ovvero del trattamento di altri dati sensibili in modo potenzialmente discriminatorio, nonché in quello dell'utilizzo di informazioni finanziarie a fini di valutazione del merito creditizio della clientela⁹⁸⁵. Orbene, coincidendo i settori elencati con quelli in cui la Commissione europea, nel *considerando* 25 della predetta decisione di adeguatezza, ritiene (ed anzi, *presuppone*) esistenti precipue garanzie (*sostanzialmente equivalenti* a quelle vigenti nell' UE) per l'interessato a fronte dell'impiego di processi decisionali automatizzati «*affecting the individual*», appare chiaro che lo scopo ultimo dello Studio sia quello di vagliare la validità della premessa “giuridica” sulla cui base l'UE ha giudicato adeguato il sistema di tutele offerto dal complessivo sistema normativo statunitense in punto di decisioni basate *unicamente* su trattamenti automatizzati dei dati personali.

Nel prosieguo della trattazione, anche sulla scorta dei fondamentali riscontri offerti dallo Studio appena richiamato, si analizzerà pertanto la disciplina federale (di natura, lo ricordiamo, settoriale) del fenomeno degli *automated decision making* nei settori menzionati (e scandagliati) dallo Studio medesimo:

⁹⁸⁴ *Ibidem*, p. 33, dove per esteso si afferma: «*in contrast to Article 22 of the GDPR, there is no general prohibition in the U.S. on decisions based solely on automated processing, including profiling, which produce legal or similarly significant effects*».

⁹⁸⁵ *Ibidem*, pp. 8 e 50 ss.

poiché è proprio lì dove la prassi tecnologicamente più evoluta appare maggiormente diffusa che risulta maggiormente necessario interrogarsi sulla qualità della risposta offerta dal diritto in funzione della protezione degli attributi fondamentali della persona umana.

Prima, tuttavia, stante il carattere gerarchico del sistema normativo statunitense, sarà opportuno tornare sul piano dei principi costituzionali, puntualmente enucleati dalla costante attività ermeneutica della *Supreme Court*, perché inevitabilmente incidenti sull'interpretazione della disciplina in esame. Ci interrogheremo, in special modo, sull'applicabilità delle *rationes decidendi* di alcuni precedenti al mutato e sempre più avanzato contesto tecnologico, e in particolare alla sua dimensione digitale: su tutte, dedicheremo particolare attenzione alla *rule of law* della *reasonable expectation of privacy* enunciata in *Katz v. United States*, in confronto con i limiti al principio medesimo emersi in seno alla successiva giurisprudenza⁹⁸⁶.

A conclusione di questo nostro discorso introduttivo, può essere significativo anche rilevare come l'art. 22 *non sia stato riprodotto nemmeno* nel testo del poc'anzi citato *Data Privacy Framework*, per motivi analoghi a quelli esplicitati nel suddetto cons. 25 della decisione 2016/1250, quest'ultima volta tuttavia articolati dalla Commissione in modo più puntuale ai *considerando* 33-36 della decisione di adeguatezza⁹⁸⁷. La Commissione, in primo luogo, sottolinea come lo Studio promosso dalla Commissione europea, di cui ci stiamo occupando, abbia confermato che, in relazione ai dati personali "raccolti" sul territorio

⁹⁸⁶ V. da subito *Charles Katz v. United States*, 389 U. S., 347 (1967); sulla dottrina in parola, e sui limiti della *voluntary exposure* nella sua declinazione in termini di third party doctrines, ci siamo già soffermati, come si ricorderà, nel cap. 1, par. 1.3., cui si fa rinvio.

⁹⁸⁷ Cfr. ancora COMMISSIONE EUROPEA, *Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final

dell'Unione, qualsiasi decisione pur basata su un trattamento automatizzato venga *principalmente* assunta dal *data controller* che operi in conteso europeo, e dunque in diretta relazione con il *data subject*, e pertanto risulta soggetto all'applicazione del regime di cui al GDPR⁹⁸⁸. In secondo luogo, e questa è l'affermazione per noi più rilevante, essa continua a sostenere che, nei settori (già richiamati) in cui maggiore risulta (anche alla luce dello Studio) l'implementazione di processi decisionali automatizzati incidenti («*affecting*») sulla persona fisica comunque «*U.S. law offers specific protections against adverse decisions*»: esplicitamente affermando, a tal proposito, e in relazione a una platea di atti normativi leggermente ampliata rispetto a quella cui faceva riferimento l'adequacy decision del Privacy Shield, che «*these acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress*»⁹⁸⁹.

La visione che permea il discorso della Commissione (lo dimostra il *considerando* 36) è, ancora una volta, quella della *sostanziale equivalenza*, rispetto all'omologo europeo, del sistema di tutele previsto dalla legislazione federale in punto di (secondo la Commissione, infrequenti) decisioni basate su trattamenti automatizzati (nel suo discorso, rilevanti allorché coinvolgano anche

⁹⁸⁸ Ivi, cons. 33-34; la Commissione ritiene che lo studio del 2018 abbia espressamente evidenziato come «*at the time, there was no evidence suggesting that automated decision-making was normally being carried out by Privacy Shield organisations on the basis of personal data transferred under the Privacy Shield*».

⁹⁸⁹ Ivi, cons. 35. Gli atti normativi richiamati sono ancora una volta, come si evince anche dalla nota 53, l' *Equal Credit Opportunity Act* (15 U.S.C. 1691 et seq.), il *Fair Credit Reporting Act* (15 USC § 1681 et seq.) e il *Fair Housing Act* (42 U.S.C. 3601 et seq.); a questi, la Commissione aggiunge il *Title VII of the Civil Rights Act* e *Health Insurance Portability and Accountability Act* (HIPAA) *Privacy Rule*, e valorizza inoltre la sottoscrizione degli «*Organisation for Economic Cooperation and Development Artificial Intelligence Principles, which inter alia include principles on transparency, explain ability, security and accountability*».

dati personali di interessati situati in territorio europeo) nei settori in cui più frequente risulta il loro impiego sul territorio statunitense⁹⁹⁰.

Precisando ancor più l'oggetto e la metodologia dell'indagine che ci proponiamo di svolgere, nel prosieguo allora, astraendo dal contesto del trasferimento internazionale dei dati personali e dell'incidenza dei predetti sistemi sul persone fisiche situate in Europa, analizzeremo la disciplina dei processi decisionali automatizzati - nel quadro dei principi applicabili alle fattispecie di *automated data processing* – nei settori e nei relativi atti regolatori considerati tanto dalla Commissione quanto dallo Studio menzionato, allo scopo precipuo di vagliare la validità giuridica della predetta premessa. Ci interrogheremo, essenzialmente, sull'esistenza di garanzie simili a quelle previste non solo dall'art. 22 GDPR in relazione alle assai rischiose decisioni basate unicamente su trattamenti automatizzati; ma anche a quelle previste semplicemente dalle disposizioni generali del GDPR (così come interpretate alla luce delle Linee Guida sul processo decisionale automatizzato del Gruppo di Lavoro Articolo 29) in relazione a *qualsiasi* tipo di trattamento, e conseguentemente a quei processi decisionali che contemplino un *effettivo* coinvolgimento umano.

Tutto ciò, sia consentito specificarlo, senza pretese di esaustività, bensì nei soli, consaputi limiti delle nostre capacità di indagare “dall'esterno” il panorama normativo dell'ordinamento statunitense rispetto ad un ancora così “opaco” fenomeno (in tutti i sensi), e di coglierne la declinazione nella concreta dinamica dei rapporti sociali.

In apertura della nostra indagine, è d'obbligo, come detto, volgere lo sguardo ancora una volta al panorama costituzionale: ciò risulta indispensabile a

⁹⁹⁰ Cfr. cons. 36, in cui la Commissione senza utilizzare “mezzi termini” conclude nel seguente modo: «*these rules offer protections similar to those provided under Union data protection law in the unlikely situation in which automated decisions would be taken by the EU-U.S. DPF organisation itself*».

maggior ragione in un ordinamento federale caratterizzato da un *legal dual system*, in cui è la stessa legge fondamentale a ripartire, su base gerarchica e materiale, le funzioni legislative, esecutive e giudiziarie tra livello federale e singoli Stati federati. Ricordiamo allora, per risalire in cima alla piramide normativa, come il Decimo Emendamento a chiare lettere sancisca: «*The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people*»; e che, pur tenendo a mente il principio enunciato nel caso Katz, la legislazione federale rappresenta «*the supreme law of the land*» e in caso di conflitto prevale, in linea generale, sulla difforme disciplina statale, se come afferma l'Art. VI della Costituzione Federale «*This Constitution, and the laws of the United States which shall be made in pursuance thereof (...) shall be the supreme law of the land; and the judges in every state shall be bound thereby, anything in the Constitution or laws of any State to the contrary notwithstanding*»⁹⁹¹.

4.2. *Automated data processing* nei rapporti tra *Gouvernement* e *Citizen*: la giurisprudenza della *Supreme Court* sul Quarto Emendamento nella società degli algoritmi. “*Is there any reasonable expectation of privacy in there*”?

Se la nostra attenzione, nell'analizzare a breve la disciplina federale di settore degli *automated decision making systems* si focalizzerà soprattutto sui rapporti tra privati, bisogna ricordare come la giurisprudenza costituzionale, nel confrontarsi essenzialmente con il perimetro applicativo del Quarto Emendamento e della sua idoneità, a rappresentare il fondamento costituzionale

⁹⁹¹ Per tutti i rilievi in parola, può essere utile il riferimento al tradizionale volume di L. MAYERS, *The American Legal System*, Harper & Row, 1964.

di un *right to privacy* (-*dignity*) nei rapporti tra individuo e Stato, si sia essenzialmente occupata di edificare il sistema di protezione della sfera privata della persona umana in relazione alle interferenze dei pubblici poteri⁹⁹². È stato tuttavia notato come risulti evidente che l'impostazione socioculturale sottesa alle giurisprudenza sviluppatasi in materia di *search and seizures* - stante la costruzione concettuale di ordine personalistico che, lo si evince, tende inevitabilmente a valicare i confini del rapporto pubblico-privato - non possa che riflettersi anche sui rapporti tra privati⁹⁹³.

Per questo motivo, indispensabile risulta interrogarsi su quegli orientamenti vincolanti espressi dalla Suprema Corte proprio in risposta allo sviluppo tecnologico che, al tempo della loro elaborazione, andava potenziando l'attitudine *privacy-invading* delle tecniche di "perlustrazione" nella sfera privata dell'individuo - sotto forma di perquisizioni e di sequestri - a disposizione della pubblica autorità. Orientamenti, lo ricordiamo, che hanno ad oggetto i limiti in cui le operazioni riguardanti informazioni di qualsiasi specie (soprattutto laddove immateriali, come quelle "contenute" nelle conversazioni telefoniche intercettate) relative ad una persona fisica ricadano o meno nel perimetro di tali nozioni, richiedendo un *judicial legal warrant* basato su una *probable cause* ai fini della loro legittimità. Ci riferiamo al principio della *reasonable expection of privacy* enunciato nel celebre caso *Katz v. United States*, che ha costituito oggetto di più analitico esame nel corso del primo capitolo; così come dei limiti alla dottrina in parola enucleati dalla successiva giurisprudenza, che si identificano essenzialmente nella già analizzata *third party doctrine* puntualmente costruita

⁹⁹² Ci siamo occupati approfonditamente della materia nel cap. 1, par. 1.3. Per un riscontro *ex multis*, cfr. ancora una volta U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit.

⁹⁹³ Cfr. sul punto M. ALLEN, A. ORHEIM, «Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them», 8, *Wash. J. L. Tech. & Arts*, 2, 2012, 137 ss..

nel caso *United States v. Miller* (e ulteriormente articolata nel caso *Smith v. Maryland*) e nella *plain-sight doctrine*, che più risalenti radici trova (seppur in maniera non evidente) nella *rule of trespass* di common law⁹⁹⁴.

Ebbene, se tanto il principio cardine quanto le eccezioni relative ambiscono ad estendere o piuttosto ad escludere, a fronte dei nuovi mezzi offerti dalla tecnologia, la protezione offerta dal Quarto Emendamento alle informazioni riguardanti un individuo nell'ambito delle perquisizioni e dei sequestri governativi, è opportuno esaminarne la validità nel contesto della società digitale, da qualcuno brillantemente definita “*naked society*”⁹⁹⁵: in tale mutato contesto, a fronte di sistemi di monitoraggio sempre più pervasivi basati sulla tecnologia algoritmica, si riscontra infatti l'inarrestabile fenomeno, sconosciuto tanto al giudice Brandeis in *Olmstead* quanto alla successiva stagione del *Chief Warrant*, per cui «*many of those previously private thoughts are displayed on social media for the world to see*»⁹⁹⁶.

Si impone, dunque, la necessità di esaminare l'attualità dei presupposti, articolati in senso tecnico dal giudice Harlan nella sua *concurring opinion* nel caso *Katz*, a fondamento dell'aspettativa ragionevole di *privacy* dell'individuo nel nuovo contesto *tecnosociale*, e principalmente nel contesto della rete. Al contempo, è opportuno interrogarsi sul rischio che le eccezioni a tale principio, se non rimodulate alla luce dei progressi della tecnologia, determinino una sconsiderata amplificazione delle già rilevanti tecniche e capacità di sorveglianza, individuale o piuttosto massiva, nella disponibilità dei pubblici poteri. Come è

⁹⁹⁴ V. più ampiamente *retro* e integralmente i fondamentali casi *Charles Katz v. United States*, 389 U. S., 347 (1967); *United States v. Miller*, 425 U.S. 435 (1976) e *Smith v. Maryland*, 442 U.S. 735 (1979).

⁹⁹⁵ V. Packard, *The Naked Society*, Brooklyn, Ig Publishing, 1964, 10, richiamato da C. TABARRINI, *La trasparenza algoritmica*, cit., p. 191 ss.

⁹⁹⁶ PRUNTY, A. SWARTZENDRUBER, «Social Media and the Fourth Amendment Privacy Protections», in N.S. LIND, E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 400.

stato opportunamente sottolineato, la contrazione (fino alla potenziale scomparsa) di uno spazio anche solo *intellettivo* immune da ingerenze esterne, e dunque *imperscrutabile*, non può (*rectius*, non dovrà mai) tradursi in una contestuale contrazione dei diritti degli interessati, e segnatamente dei loro diritti fondamentali⁹⁹⁷.

Alla base di tutto il discorso si colloca il problematico rapporto che, a maggior ragione a fronte dello sviluppo della tecnologia capace di introdursi nella sfera privata dell'individuo anche rispetto alle *espressioni immateriali* della sua personalità (prima attraverso *bugs* e *wiretaps*, oggi attraverso i *trojan*), intercorre tra interesse individuale alla riservatezza (ed al controllo sulle informazioni che la propria persona riguardino) e interesse alla sicurezza nazionale perseguito dalla pubblica autorità, animato da una tensione insanabile tra le due opposte prospettive della (ragionevole) aspettativa di privacy e quella della esposizione volontaria, o comunque “flagrante”, delle informazioni medesime⁹⁹⁸.

Rinviando al primo capitolo per più puntuali nozioni, è qui sufficiente ricordare che per *reasonable expectation of privacy* si intende la *rule of law* enunciata dalla Corte Suprema nel caso Katz, ove essa dichiara con forza come le garanzie costituzionali accordate alla *privacy* in nome del Quarto Emendamento

⁹⁹⁷ Cfr. K. LEIGH, «Developments on the Fourth Amendment and Privacy to the 21st Century» in N.S. LIND, E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 2. In particolare, meritevole di menzione risulta il passaggio in cui l'autore afferma brillantemente ed in modo parimenti preoccupante che «[i]t is possible that the only truly private communications we have are the thoughts in our heads». Per la disamina che seguirà, in generale, fondamentali risultano i contributi compresi nell'appena citato volume N.S. LIND, E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 413, cui si fa già da ora, al fine di approfondire i diversi punti che toccheremo, calorosamente rinvio.

⁹⁹⁸ Per alcune importanti riflessioni sui temi di cui andiamo discorrendo, cfr. M.E. LEONARD, «The Changing Expectations of Privacy in the Digital Age», in N.S. Lind e E. Rankin (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 312.

valgano *indipendentemente* dalla natura pubblica o privata dei luoghi, dal momento che l'oggetto della tutela offerta è rappresentato dall'interesse del singolo alla tutela del nucleo essenziale della propria personalità, e configura un “*legal test*” ritenuto decisivo ai fini del giudizio di bilanciamento tra interesse in parola e concorrente interesse pubblico (in particolare, alla sicurezza nazionale e alla repressione dei reati): test fondato su un «duplice requisito, il primo dei quali è stabilire se la persona abbia mostrato *un'effettiva (e soggettiva) aspettativa di privacy*; il secondo dei quali consiste nella circostanza che quell'*aspettativa sia riconosciuta dalla società come ragionevole*»⁹⁹⁹. Parallelamente, ricordiamo qui sinteticamente il primo dei due indirizzi restrittivi enucleati in seno alla Corte negli anni a venire. Ci riferiamo anzitutto alla c.d. *Third Party Doctrine*, incardinata attorno al concetto di *voluntary exposure*, costruita dalla *Supreme Court* nel caso *United States v. Miller* del 1976, in cui la Corte, in un caso riguardante l'utilizzabilità come prova in giudizio della documentazione bancaria dell'imputato, afferma che la persona che *volontariamente* condivide informazioni con una “terza parte” non gode in ordine a tali informazioni di quella legittima *expectation of privacy* garantita dal Quarto Emendamento ai sensi del precedente *Katz*, di modo che l'attività del governo intesa ad acquisire le medesime presso il terzo non sarebbe giuridicamente qualificabile come *search* e, di conseguenza, non necessiterebbe ai fini della sua legittimità (e dell'utilizzabilità degli elementi di prova così raccolti) di legale mandato di

⁹⁹⁹ V. *Charles Katz v. United States*, 389 U. S., 347 (1967), in part. pp. 351-352, dove il giudice Stewart, con argomento di tipo evolutivo e di impostazione liberal-umanitaria, come sappiamo afferma perentoriamente che ««al pari di un individuo nel proprio ufficio o (...) in un taxi, una persona che si trovi in una cabina telefonica può far affidamento sulla protezione del Quarto Emendamento. Colui che occupa la cabina (...) è sicuramente *autorizzato a credere che le parole dette durante la telefonata non saranno diffuse nel mondo*. Leggere in maniera più ristretta la Costituzione significa ignorare il ruolo vitale che il telefono pubblico ha finito per avere nelle comunicazioni private»; e, per la *concurring opinion* del giudice Harlan, che in senso tecnico articola il concetto di *reasonable expectation of privacy*, v. p. 361 ss.

perquisizione dell'autorità giudiziaria, fondato su una *probable cause*¹⁰⁰⁰. Il principio in questione, come sappiamo altrettanto bene, riceve ancora più puntuale articolazione (con la contestuale e ulteriore “contrazione” della ragionevole aspettativa di *privacy*) in *Smith v. Maryland*: in tale caso, la Corte afferma infatti che non ricadrebbero nel concetto di *search*, agli effetti del Quarto Emendamento, nemmeno l'installazione e l'utilizzo di un *pen register* da parte della polizia per ottenere informazioni sulle conversazioni telefoniche tenute da un sospettato, dal momento che quest'ultimo avrebbe perso la sua ragionevole aspettativa di *privacy* nel momento stesso in cui avesse composto i numeri, notoriamente registrati dal provider del servizio di telecomunicazione¹⁰⁰¹. Così arricchita, la *third party doctrine*, come a breve vedremo, ha subito un progressivo allargamento del proprio perimetro applicativo ad opera di una parte della giurisprudenza, scontrandosi tuttavia anche con degli importanti *statement* a garanzia degli attributi fondamentali della persona umana.

Prima di indagare il confronto (e la tenuta) dei suddetti conflittuali principi con l'evoluzione vertiginosa della tecnologia disponibile, e dunque con il contesto della quarta rivoluzione industriale, è necessario brevemente concentrarci sul terzo termine della dialettica, nella sua funzione - al pari della *third party doctrine* - conservatrice. Ci riferiamo alla poc'anzi menzionata *plain sight doctrine*, che si può sinteticamente definire come quell'eccezione alla *reasonable expectation of privacy* in forza della quale ove agenti di polizia, nel condurre le loro ordinarie attività di indagine e perquisizione, rinvenivano materiale probatorio relativo ad

¹⁰⁰⁰ *United States v. Miller*, 425 U.S. 435 (1976). Cfr. sul punto D. J. SOLOVE, *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, CT, 2013, pp. 102–110.

¹⁰⁰¹ *Smith v. Maryland*, 442 U.S. 735 (1979). L'argomentazione si basa sul presupposto che gli utenti di un servizio di telecomunicazione sono, o dovrebbero essere, generalmente consapevoli che i numeri composti verranno registrati dalla compagnia telefonica, tanto al fine di consentire l'effettuazione di chiamate, quanto per la necessità di assicurare un corretto addebito dei costi in capo alla clientela.

altri reati “in piena vista”, questi sarebbero autorizzati a *sequestrarlo anche in assenza di uno specifico e legale mandato*: appare chiara, allora, la funzionalizzazione dell’istituto in parola a prevenire la distruzione di materiale potenzialmente idoneo a provare la colpevolezza degli imputati ¹⁰⁰². A dimostrazione del legame latente di tale dottrina con la originaria concezione dominicale del *right to privacy*, possono citarsi le parole di Lord Candem nel lontano caso *Entick v. Carrington*, laddove esso afferma che «*the eye cannot by the laws of England be guilty of a trespass*»¹⁰⁰³.

In una prospettiva diacronica, una delle più emblematiche affermazioni dell’eccezione in esame si è avuta nel caso *Florida v. Riley*, con cui la Corte Suprema ha negato che in capo al sig. Riley - condannato per produzione di sostanze stupefacenti dopo che un’agente di polizia, sorvolando in elicottero il suo terreno, aveva notato l’esistenza di coltivazioni sospette, chiedendo e ottenendo un mandato - sussistesse una *reasonable expectation of privacy* garantita alla luce del Quarto Emendamento, non potendosi qualificare come «*search*» l’operazione svolta dall’agente *prima* di ottenere il mandato come, e dunque risultando le evidenze raccolte nel suo quadro (pur in assenza di legale mandato) comunque utilizzabili ai fini della condanna¹⁰⁰⁴.

A propria volta, tuttavia, stante la potenziale portata liberticida dell’eccezione, e stante la consapevolezza del rischio che essa finisse per

¹⁰⁰² Cfr. per più approfondite analisi sul tema D. SCHULTZ, J.R. VILE, *The Encyclopedia of Civil Liberties in America*, New York, Routledge, 2015, 709; M.E. LEONARD, «The Changing Expectations of Privacy in the Digital Age», cit., p. 314 ss.

¹⁰⁰³ *Entick v. Carrington*, 19 Howell’s State Trials 1029 (1765). Cfr. sul punto C. TABARRINI, *La trasparenza algoritmica*, p. 179 ss., che rinvia a T.N. Mcinnis, *The Evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 94.

¹⁰⁰⁴ Cfr. *Florida v. Riley* (488 U.S. 455, 1989). Il rilievo centrale su cui la Corte ha fondato la statuizione risulta incentrato, da una parte, sul fatto che chiunque avrebbe potuto sorvolare l’abitazione dell’imputato; e, dall’altro, sulla circostanza che (regredendosi così ad una concezione *property*-centrica di *privacy*) l’operazione siffatta non avesse interferito con il godimento della sua proprietà

legittimare le c.d. *exploratory searches* (e pertanto quelle operazioni interferenti con la vita privata dell'individuo in difetto di alcun *judicial warrant* basato su una *probable cause*), la giurisprudenza in una famosa vicenda giudiziaria di inizio anni Settanta ha coniato un triplice ordine di limitazioni cui la *plain sight doctrine* andrebbe soggetta¹⁰⁰⁵. In primo luogo, l'autorità di pubblica sicurezza non può invocare l'eccezione in parola al fine di intraprendere una perquisizione *ex novo*, ma deve disporre di un preciso e diverso motivo che abbia inizialmente determinato (e che renda a posteriori legittimi) il suo accesso allo spazio poi oggetto di legale perquisizione; in secondo luogo, la deroga opera solo rispetto alla scoperta di oggetti che, pur non rientrando nello scopo del mandato, siano stati rinvenuti *accidentalmente* nello svolgimento delle legittime operazioni di perquisizione; e infine, il carattere incriminante di tale materiale probatorio deve risultare evidente ad "un primo sguardo", senza che sia necessario alcun diretto contatto con lo stesso¹⁰⁰⁶.

All'esito di questo rapido riepilogo dei due articolati poli che scatenano la tensione tra esigenze securitarie e istanze liberal umanitarie, nel mezzo della quale si trova la dimensione dell'intimità personale e familiare dell'individuo, possiamo finalmente concentrarci sui modi in cui la suddetta dialettica si declina nel contesto digitale, e pertanto sullo *stato della protezione* offerta dal Quarto

¹⁰⁰⁵ Ci si riferisce nella serie di opinioni scritte dal giudice Stewart (lo stesso che aveva presieduto il collegio giudicante nel caso *Katz*, autore del celebre e già citato passo «*the Fourth Amendment protects people, not places*») in occasione del caso *Coolidge v. New Hampshire* (403 U.S. 443, 1971), che prendeva le mosse dalle indagini sull'omicidio della giovanissima Pamela Mason, e dalla questione riguardante la legittimità di un mandato per la *seizure* del veicolo dell'imputato. Quest'ultima venne poi dichiarata invalida, dando modo alla Corte Suprema di pronunciarsi sui limiti della *plain-sight doctrine*

¹⁰⁰⁶ Cfr. ancora una volta M.E. LEONARD, «The Changing Expectations of Privacy in the Digital Age», cit., pp. 404-405; ed anche T.N. MCINNIS, «The Evolution of the Fourth Amendment», pp. 95-96. Leonard nota come, sebbene il carattere accidentale della scoperta fosse stato progressivamente abbandonato dalla giurisprudenza, questo ha continuato ad essere opportunamente valorizzato dalla dottrina.

Emendamento al singolo di fronte all'invasività dei pubblici poteri (iper)tecnologizzati.

Conviene principiare proprio dalla appena esaminata *plain sight doctrine*, dal momento che, come alcune autorevoli voci hanno lucidamente sottolineato, la sua applicazione nel contemporaneo panorama tecnosociale solleva numerosi dubbi in relazione al rischio che l'eccezione in parola possa aggravare la *già marcata invasività* di indagini che si sostanzino nella ricerca a scopo probatorio di materiale digitale archiviato su *personal computers*¹⁰⁰⁷.

Le prime, rilevanti incertezze sorgono rispetto al criterio esegetico che risulti opportuno assumere per “adattare” l'istituto in parola, inizialmente concepito per limitare l'applicabilità del Quarto Emendamento in relazione ad operazioni poste in essere in uno *spazio fisico*, anche alle operazioni (investigative) parimenti svolte negli *spazi virtuali*¹⁰⁰⁸. Numerosi ed eterogenei sono gli approcci implementati, specialmente dalla fine del nuovo millennio, per realizzare tale opera di “naturalizzazione” dell'istituto. Pare opportuno citare qui a titolo di esempio il c.d. *inadvertent approach*, che impedirebbe l'utilizzabilità di materiale utile a provare un determinato reato rinvenuto nell'atto delle legittime ricerche (perquisizioni autorizzate, dunque) su *devices digitali* intraprese in relazione ad un *diverso reato*¹⁰⁰⁹; o il c.d. *prophylactic test*, che totalmente ne vieta l'applicazione al modo virtuale, e che poco più di un decennio fa è stato

¹⁰⁰⁷ Cfr. M.E. LEONARD, op. cit., p. 312.

¹⁰⁰⁸ Cfr. R. PRUNTY, A. SWARTZENDRUBER, «Social Media and the Fourth Amendment Privacy Protections» in N.S. Lind, E. Rankin (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, cit., p. 413. Cfr. la ricognizione sintetica operata da C. TABARRINI, *La trasparenza algoritmica*, cit., p. 181 ss.

¹⁰⁰⁹ L'approccio in questione è stato ad esempio adottato dalla Corte nel caso *United States v. Carey* (US Court of Appeal, 10th Cir, 1999) dove i giudici ritennero che le immagini pedopornografiche casualmente trovate sul computer dell'indagato, nel corso di ricerche sullo stesso autorizzate da mandato per il diverso reato di traffico di stupefacenti, fossero inutilizzabili nell'ambito del diverso procedimento avviato in relazione al reato di pedopornografia.

adottato dalla *Supreme Court* nel caso *United States v. Comprehensive Drug Testing, Inc.*, in cui la Corte ha sostanzialmente *imposto*, ai fini del compimento delle suddette ricerche nella memoria del *personal computer*, il coinvolgimento di tecnici specializzati (cc.dd. *filter teams*) i quali dovrebbero (e avrebbero dovuto, nel caso di specie) trasmettere al *prosecutor* e ai giudici i soli dati pertinenti al capo d'imputazione, stralciando e restituendo al proprietario ogni altro file¹⁰¹⁰. Ma il più recente e più noto indirizzo interpretativo certamente consiste nel c.d. *computer-as-container approach* in base al quale le perquisizioni aventi ad oggetto documenti digitali (anche dette *plain view seizures*) dovrebbero essere in tutto e per tutto equiparate a quelle riguardanti materiale analogico-cartaceo, dal momento che, secondo la dottrina maggioritaria, le tradizionali garanzie insite nel Quarto Emendamento sarebbero di per sé sufficienti a prevenire ricerche eccessivamente ampie, indipendentemente dalla tecnologia impiegata¹⁰¹¹. Risulta evidente l'ingenuità, o piuttosto l'attitudine in fondo illiberale, che anima l'impostazione in parola, laddove, come autorevole dottrina dissenziente ha rilevato, non può invece sfuggire che la quantità, la varietà e, in definitiva, la *pervasività*, delle informazioni potenzialmente archiviabili (e generalmente archiviate) in un computer rendono inadeguata la semplice estensione analogica delle teorizzazioni della *plain sight doctrine* relative al mondo fisico¹⁰¹².

¹⁰¹⁰ *United States v. Comprehensive Drug Testing, Inc.* (621 F. 3d 1162 9th Cir, 2010). Il caso muoveva da indagini avviate sul sospetto che gruppo di giocatori professionisti di baseball avesse fatto uso illegittimo (in guisa, dunque, di doping) di steroidi.

¹⁰¹¹ Cfr. ex multis R. PRUNTY, A. SWARTZENDRUBER, «Social Media and the Fourth Amendment Privacy Protections», cit., p. 414 ss.; C.J. MANTEI, «Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches», 53, *Ariz. L. Rev.*, 2011, 985 ss. Un caso in cui si è fatta applicazione di tale approccio è ad es. *United States v. Williams* (553 US 285, 2008).

¹⁰¹² Cfr. per tutti D.C. BEHAR, «An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context», 66, *U. Miami L. Rev.*, 2012, 471 ss. Con le parole cristalline dell'autore: «*Applying the traditional plain view doctrine to the computer realm is dangerous because computer usage is widespread and computers hold a vast*

I timori da ultimo espressi, in assenza di una pronuncia unificante della Corte Suprema o di un intervento del legislatore sul punto, hanno determinato la dottrina e la stessa giurisprudenza ad elaborare soluzioni più adeguate al (e consapevoli del) contesto della società algoritmica, preordinate a salvaguardare l'aspettativa di *privacy* dell'individuo sempre più *trasparente* nonostante la sempre maggiore *opacità* della macchina¹⁰¹³.

Un prima proposta è stata allora quella di assimilare l'accesso alle informazioni disseminate ed archiviate in formato digitale, quanto meno laddove raccolte in Cloud o hardware personali, al principio applicato in *Riley v. California*: nel piuttosto recente caso in parola, infatti, la Corte Suprema ha ritenuto che la perquisizione del telefono cellulare trovato indosso al soggetto arrestato, in assenza di mandato, costituisca una violazione del Quarto Emendamento, poiché non coperta dalla c.d. *SITA doctrine* (*search-incident-to-arrest*), nella misura in cui quest'ultima, enucleata per legittimare l'ispezione di qualsiasi oggetto potenzialmente utilizzabile come arma (e ciò può ben valere per il cellulare come apparecchio elettronico), non potrebbe mai (o comunque potrebbe assai difficilmente) estendersi legittimamente alle informazioni contenute nel cellulare medesimo¹⁰¹⁴.

amount of data (...) Most people use computers for all of their private matters whether paying bills, writing personal emails, or storing photos of loved ones. With the increase in computer usage, if the Court applies its relaxed Fourth Amendment requirements in this realm, the Court will be providing the government with a snap shot of the citizenry's private life».

¹⁰¹³ Cfr. ancora la ricostruzione di C. TABARRINI, *La trasparenza algoritmica*, cit., p. 182 ss. Per i concetti già introdotti di trasparenza, opacità e di società degli algoritmi v. *amplius retro*, cap. 2 e 3, ma si fa contestualmente rinvio, ancora una volta, a R. MESSINETTI, «La privacy e il controllo dell'identità digitale», cit.; E. PELLECCIA, «Decisioni automatizzate e profilazione nel contesto della Black-Box Society», cit.

¹⁰¹⁴ *Riley v. California*, 573 U.S., 373 (2014). Particolarmente rilevanti risultano le parole del giudice Roberts a p. 28, laddove osserva lucidamente come «[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life"». Per la proposta dottrinale menzionata, cfr. su tutti J.C. DOMINO, *Civil Rights and Liberties in the 21st Century*, IV ed., New York, Routledge, 2018, 213 ss.

La seconda opzione ermeneutica percorribile risulta piuttosto desumibile da un precedente, importante soprattutto per la particolarità del caso che gli ha dato origine, da noi già richiamato nel corso del primo capitolo, e sul quale ora ci intratterremo un poco più diffusamente: il caso *Kyllo v. United States*, risalente al 2001¹⁰¹⁵. La controversia giunta davanti alla Suprema Corte concerneva l'utilizzabilità delle prove raccolte dagli agenti di polizia nell'ambito di indagini svolte sulla base del *legitimate suspect* che il Sig. Kyllo stesse coltivando sostanze stupefacenti nella sua abitazione: la peculiarità del caso, da cui in definitiva dipendeva la stessa problematica qualificazioni in termini di legittimità o piuttosto di illegittimità del materiale in tal guisa raccolto, risiedeva nel fatto che, per assicurare al procedimento i relativi "mezzi di prova", gli agenti si fossero avvalsi di strumenti di rilevazione a distanza di fonti di calore idonei a rilevare la presenza dei particolari dispositivi di illuminazione necessari a sostenere una tale coltura in spazi chiusi. Ciò, in assenza di un *judicial legal warrant*, e pertanto giustificando l'operazione in termini di *plain view seizure*, essendosi il calore venuto a manifestare "in luogo pubblico". Ebbene la Corte, non accedendo alla lettura dell'accusa, riteneva piuttosto che l'impiego di tecnologie di accrescimento sensorio strumentali ad ottenere «informazion[i] riguardanti l'interno dell'abitazione che non possa[no] altrimenti essere ottenut[e] senza intrusione fisica in un'area costituzionalmente protetta (...) costituisce una *perquisizione* [necessitante allora di legale mandato ai fini della sua legittimità] – almeno quando (come nel presente caso) la tecnologia in questione *non sia* di uso pubblico generale», riconoscendo dunque l'aspettativa ragionevole di *privacy* dell'imputato.¹⁰¹⁶

¹⁰¹⁵ V. *Kyllo v. United States*, 533 U. S., 27 (2001)

¹⁰¹⁶ Ivi, p. 34. Per un'analisi nel merito, cfr. U. PAGALLO, *La tutela della privacy negli Stati Uniti e in Europa*, cit., p. 73 ss.; D. J. SOLOVE, M. ROTENBERG, P. SCHWARTS, *Privacy, Information, and Technology*, cit., p. 82 ss.

L'argomento più importante, tuttavia, come già pagine indietro evidenziato, risulta quello che mutua l'approccio genetico-evolutivo così caro all'intera giurisprudenza statunitense a favore della costruzione del moderno istituto della *privacy* (da *Boston, 1890* in poi), e che afferma come la protezione accordata dal Quarto Emendamento rispetto alle interferenze pubbliche nella sfera privata attraverso i più recenti «*subtle means*» debba essere sempre aggiornata poiché «sarebbe stupido asserire che il grado di *privacy* assicurato ai cittadini dal Quarto Emendamento sia rimasto del tutto immune dal progresso tecnologico»; aggiungendo poi che la questione al vaglio della Corte è precipuamente «quali siano i limiti relativi a questo [nuovo] potere della tecnologia che restringe l'ambito protetto della *privacy*»¹⁰¹⁷.

Su tale base, e pertanto sul rilievo che ogni tipo di ricerca digitale compiuta dai pubblici poteri, che invada la sfera dell'intimità (oggi, non solo domestica) dell'individuo, se non supportata dalle dovute autorizzazioni giudiziarie, sia *costituzionalmente illegittima*, potrebbe allora sostenersi che, *mutatis mutandis*, in difetto delle predette condizioni eccezionali (e quindi al ricorrere dei limiti alla *plain sight doctrine* appena analizzati), a risultare indebitamente lesive della *reasonable expectation of privacy* dell'individuo siano anche tutte le operazioni di *Big Data analytics*, o comunque di *data mining*, basate sull'algoritmica tecnologia della *Knowledge Discovery in Database* (allo scopo precipuo di estrarvi informazioni utilizzabili come prove in giudizio, o comunque idonee ad influire sul convincimento del giudice), e per definizione *automatizzate*, poste in essere dalla pubblica autorità *in assenza di legale mandato* fondato su di una *probable cause*.

Tuttavia, il possibile collegamento, sul piano dei rapporti cittadino-autorità, con il tema che qui ci occupa risulta smorzato dallo stesso inciso con cui la Corte,

¹⁰¹⁷ Ivi, p. 30.

nella pur pregevole sentenza in esame, sembri suggerire che l'«uso pubblico generale» della tecnologia impiegata di volta in volta dal governo ed utile a “svelare pubblicamente” le informazioni altrimenti personali (nel nostro caso, a estrarre le medesime per mezzo di sistemi automatizzati dal flusso immateriale di dati ospitati da *smart phones*, laptop, *Cloud* ecc.) del singolo, incida sulla stessa legittimità dell'operazione svolta, e dunque sulla sua stessa qualificazione in termini di *search and/or seizure* alla luce del Quarto Emendamento¹⁰¹⁸. Se, in poche parole, i mezzi per esplorare gli altrui *data set* fossero disponibili “a buon mercato”, l'impiego da parte della pubblica autorità potrebbe esulare dal perimetro della perquisizione, e dunque dai rispettivi requisiti di legittimità. E proprio questa, tuttavia, appare essere la realtà dei fatti per quanto attiene alle tecnologie di cui stiamo discutendo, dacché, come ampiamente rilevato nel corso della trattazione, sistemi naturalmente automatizzati di *data mining*, di profilazione, di *behavioral advertisement* (che sulle prime tecniche si basano) e più in generale di (*Big*) *Data analytics* sono oggi ampiamente diffuse nella società, a cominciare dallo stesso settore produttivo. L'opzione ermeneutica prospettata appare, allora, almeno per tale verso, difficile.

A questo punto, possiamo passare ad interrogarci piuttosto sulle contemporanee declinazioni dell'altro limite interpretativo al Quarto Emendamento e al corrispondente principio di *reasonable expectation of privacy*, che abbiamo punto identificato nella *third party doctrine*: premettendo che, se da una parte si riscontra in giurisprudenza un indirizzo particolarmente estensivo

¹⁰¹⁸ Sulle debolezze, ed anzi sulle vere e proprie criticità che dischiude per la tutela della privacy individuale tale “coda” dell'argomentazione articolata dalla Corte nella ratio della sentenza si sofferma il giudice Stevens nella sua *dissenting opinion*, laddove afferma che «l'inciso almeno quando (...) è in qualche modo perverso dato che sembra altamente probabile che il pericolo per la privacy aumenterà, piuttosto che diminuire, nella misura in cui l'uso di congegni intrusivi diventerà sempre più facilmente disponibile». Sul punto cfr. ancora SOLOVE, ROTENBERG, SCHWARTS, *Privacy, Information, and Technology*, cit.

rispetto al contesto tecnologico oggi esistente, dall'altra vi sono state delle importanti pronunce in cui la Corte, accogliendo un'impostazione marcatamente personalistica, ha riaffermato la centralità dell'individuo e della sua aspettativa ragionevole di privacy nel quadro delle garanzie costituzionali, e segnatamente del Quarto Emendamento, anche nell'attuale panorama tecnosociale¹⁰¹⁹.

Partendo dalle letture estensive, innanzitutto sul combinato disposto del precedente *United States v. Miller* e di *Smith v. Maryland* (che della *third party doctrine* già estendeva la portata al contesto delle telecomunicazioni), le Corti hanno fondato le limitazioni alla *reasonable expectation of privacy* nel contesto delle comunicazioni elettroniche e della fornitura di servizi e contenuti digitali, considerando inapplicabili le garanzie del Quarto Emendamento alle informazioni condivise dal singolo per il tramite di e-mail e di *Internet Service Providers* (ISP). Per fare un esempio, nel caso *United States v. Bynum* i giudici hanno escluso la configurabilità di una ragionevole aspettativa di *privacy* sulle informazioni che un utente aveva volontariamente fornito ad un *Internet Service Provider*, in questo caso Yahoo!, ai fini della registrazione, e che avevano costituito oggetto di richiesta da parte dell'FBI (in assenza di un legale mandato giudiziario) nell'ambito delle indagini per il reato di pedopornografia svolte nei confronti dell'imputato¹⁰²⁰. Ed anche in ambito lavorativo la Corte Suprema si è orientata in alcuni casi, come *Ontario v. Quon* (per quanto attiene al settore pubblico) e *TBG Insurance Services v. Superior Court*, nel senso che i dipendenti non possono vantare una ragionevole aspettativa di riservatezza sulle comunicazioni effettuate

¹⁰¹⁹ Critica, in generale, la tendenza "estensiva" della giurisprudenza di *common law* H. NISSENBAUM, «Protecting Privacy in an Information Age: The Problem of Privacy in Public», in *Law and Philosophy*, 17 (5), 1998, pp. 559–596. Per la ricostruzione che seguirà, cfr. anche C. TABARRINI, *La trasparenza algoritmica*, cit., p. 184 ss.

¹⁰²⁰ *United States v. Bynum*, 604 F.3d 161 (2010)

per mezzo dei dispositivi elettronici, *laddove questi ultimi siano stati messi a disposizione dal datore di lavoro*¹⁰²¹.

Tuttavia, il settore dell'attuale panorama digitale in cui più controversa è risultata l'applicazione giurisprudenziale della *third party doctrine* come costruita nella sua "interezza" in *Miller* e in *Smith*, è stato quello della geolocalizzazione a mezzo tracciamento delle celle telefoniche (riguardante le c.d. *cell site location information*)¹⁰²².

In senso estensivo, si riscontrano pronunce come *United States v. Graham*, in cui la Corte Distrettuale del Maryland stabiliva espressamente che i dati storici relativi alla localizzazione spaziale di un telefono cellulare non ricadrebbero nell'alveo del diritto alla *privacy* garantito, a fronte di perquisizioni e sequestri illegittimi, dal Quarto Emendamento¹⁰²³. Ancora più emblematico a tal proposito risulta poi il caso *United States v. Skinner*, in cui la Corte ha statuito che il Sig. Skinner non potesse vantare una (ragionevole) «*expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone*», dal momento che

¹⁰²¹ Cfr. *Ontario v. Quon*, 560 U.S. 746 (2010), in cui la Corte Suprema ha ritenuto, stante l'incertezza in punto di riservatezza generalmente associato a dispositivi elettronici aziendali, che fosse preferibile adottare un'interpretazione ristretta alle specifiche circostanze del caso, sancendo così la legittimità della perquisizione operata dal datore di lavoro (in tal caso, una pubblica amministrazione, perciò provvista *anche* di poteri autoritativi) sui messaggi scambiati dai dipendenti con pagers aziendali. E cfr. poi *TBG Insurance Services v. Superior Court*, 96 C.A.4th 443 (2002), in cui a fronte del ricorso di un dipendente, licenziato per aver fatto indebito uso di due computer messi a disposizione dal proprio datore di lavoro privato, la Corte ha ritenuto che, proprio in virtù del consenso prestato, il dipendente non poteva vantare alcuna ragionevole aspettativa di *privacy* sulle informazioni contenute nei computer aziendali.

¹⁰²² Sul tema, e più in generale su quello della dialettica tra *reasonable expectation of privacy* e *voluntary exposure* nell'ambito dell'utilizzo degli smart devices, e dunque nel contesto digitale, cfr. ex multis H. PLOURDE-COULE, «Back to Katz: Reasonable Expectation of Privacy in the Facebook Age», 38, *Fordham Urb. L.J.*, 2, 2010, 571 ss; R. PRUNTY, A. SWARTZENDRUBER, «Social Media and the Fourth Amendment Privacy Protections», cit., p. 414 ss.; G. MANNING, «Alexa: Can You Keep a Secret? The Third-Party Doctrine in the Age of the Smart Home», in *American Criminal Law Review*, 56, 2019; ADRIENNE N. KITCHEN, «Smart Devices and Criminal Investigations: Protecting Suspects' Privacy and Fourth Amendment Rights», 54 NO. 3 *CRIM. LAW BULLETIN ART 1*, 2018.

¹⁰²³ *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012)

lo sfruttamento delle capacità di geolocalizzazione caratterizzanti i telefoni di nuova generazione non può essere precluso alle forze di polizia, a pena altrimenti del configurarsi di un ingiustificato vantaggio per i criminali¹⁰²⁴.

E tuttavia, di fronte alle posizioni eccessivamente securitarie espresse dalle Corti statali, ed anche dalla *Supreme Court* di Washington, nelle pronunce citate, l'ulteriore evoluzione del contesto tecnologico ha chiaramente imposto dei *revirements*, in funzione della tutela della sfera privata dell'individuo, che spunti importanti offrono per avvicinarci all'esame della eterogenea disciplina statunitense dei sistemi decisionali automatizzati (nel settore privato, ma anche, come vedremo a breve, nel rapporto tra individuo e autorità).

Il primo può già rintracciarsi nella famosa sentenza *U. S. v. Jones* del 2012, in cui la Corte è venuta ad occuparsi del limitrofo tema dell'utilizzazione di dispositivi GPS (la cui attività per definizione risulta qualificabile in termini di *automated data processing*) ai fini del tracciamento degli spostamenti di indagati: materia in relazione alla quale già sussisteva un precedente orientamento della Corte, che in ossequio ai limiti posti dalla *third party doctrine* alla *rule of law* del caso *Katz* sanciva l'insussistenza di alcuna aspettativa ragionevole di *privacy* in ordine agli spostamenti di un veicolo coinvolto, appunto, nel contesto di indagini di polizia¹⁰²⁵. Ebbene, nel caso *Jones* la Corte, adita dall'imputato avverso la sentenza di condanna fondata anche sugli elementi di prova ricavati da operazioni di tracciamento tramite GPS svolte dalla polizia oltre i limiti temporali stabiliti nel mandato giudiziario, ha ritenuto integrati gli estremi della violazione della *privacy*, in virtù dell'elevato grado di invasività del tracciamento¹⁰²⁶.

¹⁰²⁴ *United States v. Skinner*, 690 F.3d 772 6th Cir. (2012).

¹⁰²⁵ Cfr. *United States v. Knotts* (460 U. S. 276, 281, 1983) per cui "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."

¹⁰²⁶ Cfr. *U.S. v. Jones*, 565 U.S. 400 (2012).

Ai nostri fini, e quindi a suffragio della lettura che valorizza i rischi configurati dalle *privacy-invading technologies* nel contesto della società datificata, della sorveglianza o degli algoritmi (e, dunque, *naked*) che dir si voglia, si possono qui riportare alcune delle riflessioni cristallizzate in talune delle *opinions* del caso in parola. In particolare, è rilevante sottolineare quel passaggio dell'*opinion of the Court* in cui l'autore – il giudice Scalia – lucidamente sottolinea come «*before computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. (...) Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap*»¹⁰²⁷. E ancora più significative sono le parole del giudice Sonia Sotomayor, che nella sua *concurring opinion* si concentra su molte delle questioni che abbiamo ripetutamente affrontato, a cominciare dalle capacità insite nei sistemi algoritmici di tracciamento (o di monitoraggio, o di localizzazione che sia), e quindi in definitiva di “ubiquitario” trattamento dei dati personali, nel ricostruire spostamenti, comportamenti abituali, preferenze e i più disparati aspetti della vita di un numero sempre crescente di persone. Ivi, il giudice evidenzia, in modo particolarmente efficace, la necessità di riconsiderare il limite alla *reasonable expectation of privacy* rappresentato dalla *voluntary disclosure* delle proprie informazioni a terze parti, sul presupposto che «*this approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks*»¹⁰²⁸.

¹⁰²⁷ Ivi, par. 5.

¹⁰²⁸ Cfr. S. SOTOMAYOR, «Concurring Opinion», in *U.S. v. Jones*, 565 U.S. 400 (2012). Per approfondite considerazioni sul tema, si rinvia ancora una volta a D.J. SOLOVE, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, 2011, 102ss.

L'altro, fondamentale *restatement* promosso dalla Corte Suprema, questa volta più strettamente relativo alla materia della (automatizzata) geolocalizzazione a mezzo tracciamento delle celle telefoniche, è da rintracciarsi nella altrettanto famosa e più recente sentenza *Carpenter v. United States*¹⁰²⁹. Il caso risulta di nostro interesse perché si collega all'applicazione delle disposizioni dell'*Electronic Communication Privacy Act*. Di tale normativa infatti ci occuperemo a breve, in quanto (unica) legislazione oggi vigente negli U.S.A. preordinata a tutelare e a stabilire i limiti dell'*information privacy* nell'ambito delle comunicazioni elettroniche *anche* rispetto all'esercizio di poteri autoritativi da parte dei soggetti pubblico, e dalla quale, secondo determinate proposte dottrinali, sarebbe consentito desumere una specifica disciplina applicabile (anche) ai processi decisionali - o quanto meno ai trattamenti - automatizzati svolti in tale contesto (l'esempio paradigmatico è quello, appunto, del monitoraggio del traffico informatico)¹⁰³⁰.

Il caso *Carpenter* prendeva le mosse da un'indagine avviata su una rapina nel corso della quale uno degli arrestati, dopo aver confessato, aveva consegnato il suo telefono all'FBI, la quale aveva conseguentemente ottenuto l'autorizzazione per l'accesso ai dati della geolocalizzazione del dispositivo, ma ai soli sensi dello *Stored Communications*, la quale si limita a richiedere «*reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal*

¹⁰²⁹ V. *Carpenter v. United States* (No. 16- 402, 585 U.S. 2018). La sentenza ha costituito oggetto di una moltitudine di contributi; cfr. ex multis Cfr. S. KEFFER, «Too Big to Surveil: The Fourth Amendment Illuminated By 'Modern Lights' and Shadowed By Obsta Principiis in a Post-Carpenter World Concerned With Privacy», 2, *Information & Communications Technology Law*, 28, 2019, 161 ss.

¹⁰³⁰ V. par. 4.2.1., e cfr. subito S. FREIWALD, «First Principles of Communications Privacy», 3, *Stan. Tech. L. Rev.*, 2007, 1ss; C.R. GELLIS, «CopySense and Sensibility. How the Wiretap Act Forbids Universities from Using P2P Monitoring Tools», 12, *B.U. J. Sci. & Tech. L.*, 2006, 340.

investigation»¹⁰³¹. Tale autorizzazione, lo si sottolinea, si sostanzia in semplici “*court orders*”, giuridicamente distinti e lontani dal mandato giudiziario fondato sul ben più stringente presupposto essenziale rappresentato dalla *probable cause* richiesto per le attività d’indagine ricadenti nel perimetro applicativo del Quarto Emendamento¹⁰³².

Ottenuto in tal modo l’accesso allo storico della geolocalizzazione del dispositivo senza dover soddisfare il più stringere presupposto probatorio della *probable cause* di cui al Quarto Emendamento, l’autorità di polizia aveva potuto riscontrare come il Sig. Carpenter si trovasse nei pressi dei luoghi colpiti al momento delle rapine, producendo il relativo materiale in giudizio e sancendo la condanna in primo grado dell’imputato. La sentenza veniva poi confermata in appello, ma impugnata da Carpenter davanti alla Suprema Corte. Ebbene, quest’ultima nella sentenza in parola riafferma una rigorosa interpretazione delle garanzie offerte dal Quarto Emendamento e sintetizzate nel principio del *reasonable expectation of privacy*, ritenendo la *third party doctrine* inapplicabile al caso di specie: secondo la Corte, ai fini della legittimità delle operazioni in questione non sarebbe sufficiente la sussistenza di un *court order* basato sui semplici *reasonable grounds* ai sensi delle pertinenti norme dello *Stored Communication Act* (ritenuti «*a gigantic departure from the probable cause*»)¹⁰³³,

¹⁰³¹ *Stored Communication Act*, 18 U.S.C.§Sec.2703(d). Ricordiamo che, se i cell-site data possono comprendere indirizzi e-mail, indirizzi IP, numeri di telefono ecc., nel loro ambito le cell-site information data individuano quelle informazioni generate dai cellular phone provider che indicano quale cell tower un particolare telefono abbia “agganciato” quando viene instaurata una comunicazione. Cfr. M. RIEBER, «Fourth Amendment Applies to Cell Site Location Information», in *National Legal Research*, 26 novembre 2018, <https://www.nlrg.com/criminal-law-legal-research/fourth-amendment-applies-to-cell-site-location-information>.

¹⁰³² V. sempre *Stored Communication Act*, 18 U.S.C.§Sec.2703(d).

¹⁰³³ *Carpenter v. United States* (No. 16-402, 585 U.S. 2018) § B, IV. La Corte si esprime nei suddetti decisi termini: «*The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show “reasonable grounds” for believing that the records were “relevant and material to an ongoing*

dal momento che le *cell-site location information* rappresentano «*exhaustive chronicle of location information casually collected by wireless carriers today*»¹⁰³⁴.

Per i Giudici, quindi, il caso presentava affinità maggiori con la pervasività tecnologica già ravvisata in *U.S. v. Jones* del 2012 rispetto al più arretrato contesto tecnologico che faceva da sfondo a *Smith v. Maryland* del 1979. Di conseguenza in *Carpenter*, alla luce di tutte le considerazioni su esposte, la Suprema Corte ha ritenuto che le operazioni di monitoraggio e in ogni caso di trattamento ad opera della pubblica autorità delle informazioni in questione risulti qualificabile in termini di *search*, così da necessitare ai fini della loro legittimità (e dell'utilizzabilità degli elementi assicurati al procedimento penale per mezzo delle medesime) *legale mandato giudiziario* ai sensi del Quarto Emendamento, rigorosamente basato su una *probable cause*, e non già un semplice *court order* basato su *reasonable grounds* di cui allo *Stored Communication Act*¹⁰³⁵. Con le parole della Corte, insomma, «*an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant*»¹⁰³⁶.

investigation [v.infatti ancora una volta 18 U. S. C. §2703(d)] (...) *that showing falls well short of the probable cause required for a warrant* (...)»

¹⁰³⁴ *Carpenter v. United States* (No. 16-402, 585 U.S. 2018) § B. Ivi la Corte rileva lucidamente tra l'altro come «*seismic shifts in digital technology [...] made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years.*», derivandone subito come conseguenza che «*there is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today*».

¹⁰³⁵ Ivi, § III. Il giudice Roberts, a tal proposito, si esprime nei suddetti cristallini termini «*[t]he question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in Jones. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled*».

¹⁰³⁶ Ivi, § IV.

La ricognizione dei precedenti giurisprudenziali fin qui compiuta in punto di applicabilità al nuovo contesto digitale ed algoritmico della garanzia della *reasonable expectation of privacy*, e dei suoi spesso asfittici temperamenti, di fronte alle interferenze perpetrate dal governo per mezzo di sempre più sofisticate *privacy-invading technologies* ha evidenziato come oggi, nel fitto della *naked society*, tanto la prima teorizzazione quanto la dottrina della *volontaria o evidente esposizione* risultino potenzialmente insufficienti a garantire il bilanciamento tra interesse individuale alla protezione della propria sfera privata e interesse pubblico a reprimere le condotte penalmente riprovate¹⁰³⁷. Di fronte alla crescente assuefazione degli stessi individui rispetto ai rischi configurati dalla condivisione costante e spesso acritica delle informazioni che le riguardano, parte della dottrina ritiene preferibile abbandonare, ai fini del vaglio della legittimità di operazioni dei pubblici poteri in assenza di mandato giudiziario, il test della *reasonable expectation of privacy*, adottando una concezione che, al posto di concentrarsi sul regime di diffusione o di condivisione delle informazioni, fenomeno che oggi può definirsi inarrestabile (ed anche, in molti casi, auspicabile), si focalizzi maggiormente sulla ragionevolezza, o piuttosto sulla *prevedibilità*, delle *finalità di utilizzo dei dati*: approccio che, peraltro, risulterebbe più confacente alle concrete modalità di circolazione delle informazioni in rete, che eccedono pressoché interamente la capacità dell'individuo di governare il flusso informativo che lo riguarda¹⁰³⁸.

¹⁰³⁷ Ulteriormente sintomatico di tale critica declinazione contemporanea di tali concetti, in primis

¹⁰³⁸ Cfr. ancora il contributo di M.E. LEONARD, «The Changing Expectations of Privacy in the Digital Age», cit., p. 324 ss.; B.T. CROWTHER, «(Un)Reasonable Expectation of Digital Privacy», *Brigham Young University Law Review*, 1, 2012, 343 ss., che ascrive tale fenomeno alle soluzioni contrattuali generalmente predisposte dagli ISP.

E tuttavia, nonostante gli apprezzabili sforzi della dottrina e i suddetti *restatements* promossi dalla Corte Suprema, l'eccessiva dialettica esistente in punto di interpretazione delle garanzie e dei limiti disegnati dal Quarto Emendamento alla protezione della sfera privata di fronte ai pubblici poteri, per quanto attiene al conteso tecnologico contemporaneo e specialmente ai nuovi, difficilmente governabili (oltre che comprensibili) prodotti dell'automazione (dal monitoraggio GPS al *cell-site location information tracking*, passando per tutti gli strumenti di *Knowledge Based Discovery*), rende evidente che solo un intervento del legislatore federale sarebbe capace di ricondurre ad una sostanziale unità la materia: con le parole del giudice Scalia nella già citata *Opinion of the Court* nel caso *U.S. v. Jones*, «[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way»¹⁰³⁹

Ecco, allora, che proprio a tale urgenza risponde, almeno in parte, l'*Electronic Communication Privacy Act* (ECPA) come più volte novellato nel corso dei suoi cinquant'anni di vita, deputato a predisporre, in prima approssimazione, la disciplina di qualsiasi specie di intercettazione («electronic eavesdropping»), tanto laddove l'attività così qualificabile sia posta in essere dai pubblici poteri quanto laddove quest'ultima sia implementata dai privati, nell'esercizio o meno della loro iniziativa economica¹⁰⁴⁰. L'atto normativo in

¹⁰³⁹ V. ancora una volta *U.S. v. Jones*, 565 U.S. 400 (2012), § V.

¹⁰⁴⁰ Per un generale approfondimento sulla ratio, sulla struttura e sui nodi interpretativi che circondano l'ECPA, cfr. *ex multis* D.K. MULLIGAN, «Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act», 72, *Geo. Wash. L. Rev.*, 2004, 1557, 1558, S.L. SPLICHAL, «The evolution of computer/privacy concerns: Access to government information held in the balance», 1 *Communication Law and Policy*, 2, 1996, 203ss.

parola rileva soprattutto, ai nostri fini, nella misura in cui, come abbiamo accennato, parte (invero non maggioritaria) della dottrina statunitense ha ritenuto alcune delle sue disposizioni potenzialmente idonee a configurare una specifica disciplina del fenomeno dei processi decisionali automatizzati, e a monte degli stessi *automated data processing*, nella materia in questione. Rappresentando allora la normativa in questione un “ponte” tra la disciplina giuridica degli ADM nel quadro dei *rapporti Stato-cittadino* e quella piuttosto predisposta dagli atti normativi disciplinanti i settori in cui gli stessi appaiono più diffusi nei *rapporti (economici) tra privati*, almeno secondo lo Studio della Commissione europea già citato, tratteremo in un prossimo, conclusivo sotto-paragrafo la normativa medesima, con uno specifico riguardo a tali proposte esegetiche dottrinali.

4.2.1. *Electronic Communication Privacy Act*: le proposte della dottrina circa un divieto di monitoraggio automatizzato delle comunicazioni elettroniche

Sulla struttura generale dell’ECPA ci siamo già soffermati nel corso del primo capitolo¹⁰⁴¹. Qui, occorre riprendere ed ampliare alcune considerazioni ivi svolte, per meglio definire il contesto in cui si collocano le originali letture “estensive”, o piuttosto evolutive, della dottrina.

Introdotta, come sappiamo, nel 1986 in risposta alle pronunce della Corte Suprema successive al caso Katz, al fine di integrare il *Federal Wiretap Act* del 1968 (oggi Titolo I dell’ECPA), che nel disciplinare l’intercettazione delle conversazioni a mezzo telefono fisso lasciava scoperta l’emergente e sempre più diffusa fattispecie delle comunicazioni elettroniche senza filo¹⁰⁴², esso fa seguito

¹⁰⁴¹ V. cap. 1, par. 1.7.

¹⁰⁴² Cfr. per una ricognizione storica Cfr. D. J. SOLOVE, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, 2011, 73 ss.; D.K.

al Report con cui l'*Office of Technology Assessment* (OTA) denunciava i vuoti di tutela in questione, determinata dall'innovazione tecnologica e dalla diffusione dei computers¹⁰⁴³: il legislatore, per colmarli, decide di fissare una serie di presupposti e di garanzie procedurali ai fini dell'accesso al contenuto delle comunicazioni elettroniche tanto dai *terminali* del mittente e del destinatario, quanto dai *server di terzi providers* (seppur, in quest'ultimo caso, a fronte di presupposti meno stringenti)¹⁰⁴⁴. Il legislatore allora, oltre alla novella suddetta, tenta di regolare le sopravvenute trasformazioni del contesto tecnologico introducendo norme disciplinanti l'accesso al contenuto delle conversazioni svolte mediante mezzi elettronici archiviate e stabilendo condizioni e limiti al monitoraggio delle telecomunicazioni, cosicché oggi l'atto consiste di tre parti, o Titoli: in ordine, il *Wiretap Act*¹⁰⁴⁵; il *Pen Register Act*¹⁰⁴⁶; e lo *Stored Communication Act*¹⁰⁴⁷. Seconda la lettera delle relative disposizioni (secondo parte della dottrina tuttavia, come vedremo, suscettibili di interpretazione evolutiva), nel loro ambito applicativo ricadono pertanto le attività di "accesso" alle comunicazioni via cavo, alle conversazioni orali ed alle comunicazioni elettroniche; i primi due titoli disciplinando la c.d. *prospective surveillance*, ovvero il monitoraggio delle conversazioni in corso; e lo SCA detta la disciplina

MULLIGAN, «Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act», 72, *Geo. Wash. L. Rev.*, 2004, 1557, 1558.

¹⁰⁴³ Cfr. OFFICE OF TECH ASSESSMENT, *Electronic Surveillance and Civil Liberties* (Congresso degli Stati Uniti, 1985).

¹⁰⁴⁴ Cfr. ancora D.K. MULLIGAN, «Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act», cit., 1557, 1564-1565; M.L. RICH, «Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment», 164, *U. Pa. L. Rev.*, 2016, 871ss.

¹⁰⁴⁵ 18 U.S.C. §§2511-2522.

¹⁰⁴⁶ 18 U.S.C. §§ 3121-3127

¹⁰⁴⁷ 18 U.S.C. §§ 2701-2711

della c.d. *retrospective surveillance*, ovvero il regime di accesso alle conversazioni archiviate¹⁰⁴⁸.

Scendendo un poco più nel cuore della disciplina dettata da ciascuno dei tre Titoli, è necessario ricordare come, in primo luogo, il *Wiretap Act* (Titolo I dell'ECPA) oggi proceduralizza il regime di accesso, o piuttosto di intercettazione, rispetto alle comunicazioni intraprese oralmente o meno con qualsiasi mezzo, meccanico od elettronico, stabilendo che laddove l'attore lamenti un'illecita acquisizione del contenuto di una comunicazione della suddetta specie, il convenuto possa eccepire l'esistenza di una delle basi giuridiche contemplate dal Titolo, tra le quali in particolare figurano il consenso dell'interessato o la rilevante clausola imperniata sull'accidentalità dell'accesso nel corso dello svolgimento dell'attività imprenditoriale, la c.d. "*business extension defense*"¹⁰⁴⁹.

Lo *Stored Communication Act* (SCA) (Titolo II dell'ECPA) è dedicato alla disciplina dell'accesso al contenuto delle *stored electronic communications*, in linea generale vietato a meno che le stesse non siano già pubbliche ovvero non siano state divulgate da un utente che vi abbia avuto legittimo accesso¹⁰⁵⁰. Tale titolo, in particolare: (i) vieta l'accesso non autorizzato alle comunicazioni al fine di ottenere, alterare o distruggere conversazioni; (ii) vieta, salvo alcune eccezioni, la divulgazione di tali conversazioni; (iii) fissa garanzie procedurali per la richiesta governativa di accesso alle comunicazioni elettroniche per il tramite di ISP¹⁰⁵¹.

¹⁰⁴⁸ Cfr. D.K. MULLIGAN, «Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act», cit., 1557, 1566.

¹⁰⁴⁹ *Ibidem*. V. in part. 18 U.S.C. §§2515-2517.

¹⁰⁵⁰ Per una panoramica generale, cfr. S.M. BOYNE, «Data Protection in the United States», cit., pp. 299-317; D.J. Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security*, cit., 157ss; D.K. MULLIGAN, «Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act», cit., pp. 1557-1568.

¹⁰⁵¹ V. in part. 18 U.S.C. §2701-2702.

Il *Pen Register Act* (Titolo III dell'ECPA), invece, assumendo quale oggetto principalmente le c.d. *noncontent information* (come appunto i numeri di telefono digitati, balzati all'attenzione del legislatore successivamente all'importante, esaminato caso *Smith v. Maryland*) disciplina l'utilizzo di *pen registers*, ossia dispositivi di registrazione di numeri digitati, o di *trap and trace devices* in relazione a qualsiasi aspetto di una *wire or electronic communication*, vietandolo in assenza di un apposito *court order* (basato, lo si ricorda, su *reasonable grounds*, requisito meno stringente rispetto alla *probable cause* legittimante il *legal warrant* ai sensi del Quarto Emendamento), salve le eccezioni previste nelle disposizioni medesime¹⁰⁵².

Concentriamoci ora sui tentativi operati dalla dottrina per adattare alcune delle disposizioni della normativa in parola alla fattispecie dell'*automated data processing* (ed eventualmente all'utilizzo stesso di sistemi decisionali automatizzati) nel campo delle intercettazioni delle comunicazioni elettroniche, che tale legislazione si prefigge di regolamentare.

I tentativi che esamineremo si sono concentrati essenzialmente sulle disposizioni del primo Titolo, ovvero del *Wiretap Act*: una parte della dottrina, invero non maggioritaria (come abbiamo già anticipato), si è interrogata sulla potenziale estensione del perimetro applicativo del divieto configurato dal § 2511, e dai paragrafi seguenti specificato, di «*interception and disclosure of wire, oral, or electronic communications*» allo svolgimento delle operazioni in parola (e, soprattutto, del loro svolgimento sistematico, in guisa pertanto di monitoraggio) in modo *automatizzato*. Tale lettura scaturisce da un'impostazione esegetica di tipo teleologico e, ancora una volta, *evolutivo*, facente leva sulla funzione

¹⁰⁵² 18 U.S.C. § 3121-3127. Per una panoramica generale, cfr. J.N. SLOANE, «Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation», 12, J. Marshall L.J., 23, 2019, pp.23-38.

perseguita a suo tempo dall'introduzione della normativa in esame: quella di cristallizzare (inizialmente) un divieto - e successivamente di estenderlo - in relazione a tutte quelle attività risultanti in un'indebita ingerenza, indifferentemente perpetrata da un soggetto pubblico o da un soggetto privato, nel contenuto *immateriale* e tuttavia *personale* delle comunicazioni intraprese attraverso qualsiasi mezzo da un individuo, poiché espressione della “*privatezza*” del singolo (pur sempre, lo si ricorda, in un ottica di bilanciamento con i concorrenti interesse pubblici perseguiti dallo Stato)¹⁰⁵³.

Se si è ben inteso il “cuore” delle suddette proposte, si sta semplicemente affermando che tale indebita ingerenza si realizza soprattutto per mezzo dell'automazione, e quindi oggi della tecnologia algoritmica e di IA: valorizzandosi, tra le righe, il nesso fondamentale che intercorre tra tecnica, *privacy* e diritto, e l'attitudine di quest'ultimo ad adattarsi, in funzione della tutela della seconda, ai più attesi o in attesi sviluppi della prima. Ancora una volta,

¹⁰⁵³ In letteratura, le proposte di cui svolgeremo una sintetica analisi si ritrovano in contributi della più diversa -e, spesso, settoriale- specie; qui, si richiamano, anche alla luce della ricognizione compiuta da C. TABARRINI, *La trasparenza algoritmica*, cit., p. 194 ss., i lavori di S. CHOPRA, L.F. WHITE, *A Legal Theory for Autonomous Artificial Agents*, University of Michigan Press, Ann Arbor, 2011, 108 ss.; D.J. SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, New York University Press, New York, 2004; S. FREIWALD, «First Principles of Communications Privacy», 3, *Stan. Tech. L. Rev.*, 2007, 1ss; C.R. GELLIS, «CopySense and Sensibility. How the Wiretap Act Forbids Universities from Using P2P Monitoring Tools», 12, *B.U. J. Sci. & Tech. L.*, 2006, 340. Gli autori in questione, ciascuno secondo i propositi della propria ricerca, giustificano l'opportunità della proposta ricostruttiva in esame in ragione del sempre più diffuso utilizzo di strumenti di *automated data analytics* in ordine al contenuto delle comunicazioni elettroniche (categoria eterogena, come sappiamo, in cui attualmente ricadono tanto l'*aural transfer* compiuto con un mezzo meccanico quale il telefono fisso quanto l'e-mail o, per portare recenti esempi, il messaggio su Whatsapp o nella sezione Direct Message di Instagram) nei diversi settori della vita associata, dalla tutela della proprietà intellettuale alla lotta al terrorismo, sino alla tutela della salute pubblica, come dimostra lo stesso monitoraggio dei fenomeni epidemici su cui lo stesso Garante italiano, come si ricorderà, ha espresso preoccupazione nel Prov. n. 43 del 5 marzo 2020, [doc. web n. 9304455]. Su tale ultimo punto cfr. anche i risultati del recente studio condotto da TEODORO ALAMO DANIEL G. REINA, PABLO MILLÁN GATA, VICTOR M. PRECIADO, GIULIA GIORDANO, «Data-driven methods for present and future pandemics: Monitoring, modelling and managing», in *Elsevier*, 29 giugno 2021, articolo pubblicato online e disponibile al sito: <https://www.sciencedirect.com/science/article/pii/S1367578821000419?via%3Dihub>

insomma, ricorre quell'approccio genetico-evolutivo che domina l'intero discorso statunitense sulla *privacy*, e che ci riporta al lume acceso dal giudice Brandeis sui «*subtle and far reaching means of invading privacy*», nonché sui rilievi da ultimo svolti dalla Suprema Corte in *Kyllo*, dove l'adeguamento del diritto - anche solo nella dimensione *esegetica* - al costante divenire della tecnologia rappresenta l'unico mezzo per garantire continuità alla tutela del *foro intimo* del singolo, indispensabile ai fini della libera costruzione del proprio sé e della sua proiezione esterna¹⁰⁵⁴.

Venendo un poco più nello specifico al versante tecnico di tali proposte, un primo tentativo di adattare la disciplina dell'ECPA al contesto della società digitale ed *algorithmic driven*, sebbene in relazione al più ampio fenomeno dei sistemi di trattamento continuativo di dati personali degli utenti, è stato infruttuosamente esperito nel caso *DoubleClick Inc.*¹⁰⁵⁵. La vicenda, invero ormai datata, scaturisce dal ricorso giurisdizionale proposto da un gruppo di utenti che lamentavano di essere stati soggetti ad operazioni di profilazione da parte della società di marketing personalizzato *DoubleClick*, sostenendo che l'applicazione dei ben noti *cookies* nei loro *hard drives*, e il successivo accesso ai medesimi, evidentemente compiuto in modo automatizzato, costituisse un *unauthorized access* in spregio del divieto di intercettazioni non autorizzate prescritto dal Titolo I dell'ECPA, e quindi dal *Wiretap Act*. La Corte, nella sua decisione, ha tuttavia accolto il diverso orientamento secondo cui l'installazione dei *cookies* di

¹⁰⁵⁴ In proposito, come sappiamo, i riferimenti bibliografici sono molteplici, per cui si rinvia ai capitoli precedenti, dove questi sono stati puntualmente presi in esame; qui, tuttavia, è indispensabile nuovamente il richiamo a L. BRANDEIS, «Dissenting Opinion, in *Olmstead v. United States*», 277, U. S., p. 473; e *Kyllo v. United States*, 533 U. S., 27 (2001), p. 30 ss.

¹⁰⁵⁵ V. *In Re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); lo riporta C. TABARRINI, *La trasparenza algoritmica*, cit., p. 197 ss., che rinvia a D.J. SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, cit., p. 68 ss. che sottolinea come la vicenda sia evidente indice delle «difficulties of the ECPA in responding to the challenges of computer databases».

profilazione medesimi *non integri* gli estremi di una illegittima intercettazione online, nella misura in cui gli utenti dei siti web interessati dal trattamento in parola, nel momento stesso in cui accettano la *privacy policy* di questi ultimi - la quale (come nel caso di specie) consenta a terze parti di installare sui dispositivi degli utenti e successivamente di “recuperare” i *cookies* medesimi -, acconsentirebbero anche alle attività di profilazione di titolari del trattamento (dunque) “secondari”¹⁰⁵⁶. È evidente la distanza rispetto all’impostazione *risk based* e valorizzante l’*accountability* del titolare accolta dal GDPR, laddove - solo per fare un esempio - nel sancire espressamente il principio di specificità del consenso, il Regolamento subordina la sua validità alla puntuale descrizione nell’informativa della natura, degli effetti e delle finalità di ciascun trattamento, subordinando poi la stessa liceità dei trattamenti secondari alla compatibilità con le finalità esplicitate in relazione al trattamento primario¹⁰⁵⁷.

Tale vicenda offre un’idea della difficoltà che proposte evolutive di tal segno incontrano nel penetrare nella sensibilità della stessa giurisprudenza, anche in virtù di quella tradizionale fiducia riposta dal settore produttivo statunitense nell’ «*efficiency*» di un generale *computer-based approach*¹⁰⁵⁸. Ora però occorre restringere il campo e soffermarci più nello specifico sulle proposte dottrinali relative all’estensione della disciplina del *Wiretap Act* ad ipotesi in cui l’intercettazione o *eavesdropping* - oggi piuttosto qualificabile in termini di tracciamento - del contenuto di comunicazioni elettroniche personali sia

¹⁰⁵⁶ *Ibidem*.

¹⁰⁵⁷ V. ampiamente *retro*, cap. 3, par. 1.2. V. di nuovo, tra gli altri, art. 5 par. 1 lett. a), b) e c); art. 4, par. 1, n. 11); art. 6, par. 3, del Regolamento UE 2016/679 (General Data Protection Regulation).

¹⁰⁵⁸ Cfr. ancora M. LETA JONES, «The right to a human in the loop: Political constructions of computer automation and personhood», cit.

effettuato in modo *interamente* automatizzato, integrando pertanto una fattispecie di *automated data processsing*¹⁰⁵⁹.

Va premesso che tali proposte si scontrano con un diametralmente opposto orientamento dottrinale, che la riconducibilità delle operazioni di “accesso” e di elaborazione ai più disparati fini del contenuto di comunicazioni elettroniche in modo esclusivamente algoritmico al divieto di cui al Titolo I dell’ECPA tende ad escludere. Tale orientamento riposa sulla convinzione che sia impossibile qualificare in termini di intercettazione i sistemi di “monitoraggio” automatizzato, privi di alcun coinvolgimento umano attuale o potenzialmente successivo, sul presupposto che *«a computer is, at most, a tool that enables humans to spy on other humans; it cannot itself spy on people»*; il che conduce alla logica conclusione secondo cui *«automated processing that is not contemporaneously reviewable by humans, and does not produce a record for later human review, is not an interception and should not be defined as one in future revisions of the Wiretap Act»*.¹⁰⁶⁰ Tale impostazione, come è evidente, è anche diametralmente opposta a quella fatta propria dal legislatore europeo nella costruzione dell’art. 22 del GDPR e dalla maggior parte dei suoi commentatori, che della decisione basata

¹⁰⁵⁹ Cfr. nello specific S. FREIWALD, «First Principles of Communications Privacy», 3, *Stan. Tech. L. Rev.*, 2007, 1ss; C.R. Gellis, «CopySense and Sensibility. How the Wiretap Act Forbids Universities from Using P2P Monitoring Tools», 12, *B.U. J. Sci. & Tech. L.*, 2006, 340.

¹⁰⁶⁰ Le parole sono di B.E. BOYDEN, «Can a Computer Intercept your email?», 34, *Cardozo L. Rev.*, 2012, p.673. lo stesso autore, nel medesimo testo, si esprime nei seguenti termini: *«[s]uch automated processing does not by itself pose any threat to privacy. Although there is a tendency to anthropomorphize computers, just like we anthropomorphize cars and toasters, a computer scanning an email is the functional equivalent of a thermostat turning on the heat (...) it mechanically triggers a switch according to its programming. Automated processing of communications is similar. There is therefore no need to erect a legal barrier to such processing to protect privacy, and the current Wiretap Act does not impose one»*, e continua *«The Act has always required at least the prospect of human review because, as the drafters of the ECPA in 1986 understood, computer monitoring is qualitatively different from human monitoring. It is the threat of human use of personal information that reduces privacy, and not simply that one’s information may be used in some way»*, p. 716. Rilievi simili si riscontrano anche in R.A. POSNER, «Privacy, Surveillance, and Law», 75 *U. Chi. L. Rev.*, 2008, 245, 249; M. TOKSON, «Automation and the Fourth Amendment», 96, *Iowa L. Rev.*, 2011, 581

esclusivamente sul trattamento automatizzato sottolinea proprio l'idoneità a configurare pericoli per l'integrità degli attributi fondamentali della persona umana, in primis quello di discriminazione, prescrivendo tra le indefettibili garanzie da cui ulteriormente dipende la loro eccezionale liceità *proprio e come minimo* il diritto dell'interessato di ottenere l'intervento umano¹⁰⁶¹.

L'orientamento dottrinale restrittivo, del resto, si fonda su quella stessa giurisprudenza che, pur a fronte dell'estensione dell'ambito di applicazione del divieto configurato dall'ECPA (sia in termini di *prospective* che di *retrospective surveillance*) in relazione a qualsiasi forma di «*electronic eavesdropping*», ha continuato ad escludere l'applicabilità delle disposizioni del *Wiretap Act* a fronte di operazioni di non autorizzato “monitoraggio” del contenuto di comunicazioni elettroniche che non contemplassero alcun coinvolgimento umano né in fase di *captazione*, né in fase di successiva *trascrizione*. Tale principio viene stabilito in termini di *binding precedent* dalla Suprema Corte già nel noto caso *United States v. Turk* del 1976 (e quindi in realtà prima dell'adozione dell'ECPA nella sua attuale configurazione), in cui la Corte esclude che una comunicazione elettronica possa definirsi «*aural acquired*» ogniquale volta sia riprodotta una registrazione, in ipotesi identificabile come *lawfully acquired communication* (ossia “appresa” al ricorrere di una opportuna base giuridica): e ciò poiché altrimenti qualsiasi successivo “replay” della medesima integrerebbe una nuova violazione del divieto. Piuttosto, la Corte ritiene integrata la definizione *solo* qualora l'utilizzo del dispositivo tecnico, o anche interamente automatizzato, di registrazione *si sostituisca* al soggetto privo di legale base giuridica, assurgendo (qui la formula famosa coniata dalla sentenza) ad «*agent of the ear*», e dunque a *substitute* del primo ascolto da parte del soggetto medesimo¹⁰⁶².

¹⁰⁶¹ V. ampiamente *retro*, cap. 3, par. 2 ss.

¹⁰⁶² *United States v. Turk* 526 F.2d 654 (5th Cir. 1976), in part. 657-658, puntualmente riportata da E. BOYDEN, «Can a Computer Intercept your email?», cit., p. 690 ss., che nei termini

Il precedente in parola è stato seguito dalla più gran parte delle Corti e ribadito dalla stessa Corte Suprema anche successivamente alle già esaminate novelle culminate con l'adozione dell'attualmente vigente ECPA, a dimostrazione della propensione del panorama giuridico – e più in generale culturale - americano a individuare nell'elettronica e nelle tecnologie computazionali uno strumento *servente* gli interessi dell'uomo, minimizzando i profili della qualità dei dati e dell'opacità che sempre più caratterizzano il fenomeno dei trattamenti automatizzati dei dati e di cui il tracciamento algoritmico sempre più si connota: già in *United States v. Rodriguez* ad esempio, i giudici hanno ribadito come la nozione di «*acquisition*» fosse rimasta immutata pur a seguito delle modifiche apportate con l'adozione dell'ECPA, continuando a richiedersi, in relazione alle registrazioni elettroniche e più in generale alle operazioni di “accesso” automatizzato ai contenuti delle comunicazioni medesimi, la strumentalità alla successiva ricezione da parte di un agente umano o comunque l'archiviazione a fini di successivo accesso da parte del medesimo¹⁰⁶³.

suddetti ricostruisce la vicenda da cui la pronuncia scaturisce: «*the defendant, Frederick Turk, had discussed a narcotics transaction over the phone with a fellow trafficker, Charles Kabbaby.92 Unfortunately for Turk, Kabbaby recorded the call, and Kabbaby had the tape in his car when he was arrested. The police listened to the tape, and Turk was convicted of perjury for having earlier lied to a grand jury. The issue before the Fifth Circuit was whether, in listening to Kabbaby's recording, the police “intercepted” the telephone call between Turk and Kabbaby.93 This required identifying the precise act that intercepted their conversation.94 If it was Kabbaby's act of recording, then the tape was covered by the consent exception, and listening to the tape was not a violation.95 But if it was the police's act of listening, then they did so without the consent of either party, and a court order was required*». Una domanda possiamo porci in relazione alle *conclusions* cui perviene la Corte: sono queste conclusioni ancora attuali, quando la tecnologia consente, ad esempio attraverso i sistemi di IA generativa, di manipolare il contenuto di qualsiasi specie di *eavesdropping*, anche audiovisiva, compromettendo le capacità dell'agente umano che successivamente le riproduca di vagliarne, senza l'impiego di strumenti a volte anche sofisticati di *fact-checking*, l'attendibilità?

¹⁰⁶³ V. *United States v. Rodriguez* 968 F.2d 130, 135-36 (2d Cir. 1992), riportato da E. BOYDEN, «Can a Computer Intercept your email?», cit., 689. Dello stesso segno, e più di recente, v. *ex multis United States v. Lewis*, 406 F.3d 11, 18 n.5 (1st Cir. 2005).

Bisogna, in ogni caso, citare almeno un caso in cui una Corte di ultima istanza statale, nella fattispecie la *New York Court of Appeals* paia aver accolto, seppur implicitamente, una lettura (peraltro basata su alcuni passaggi dell'argomentazione svolta dalla Corte Suprema in *Smith v. Maryland*) che estenda la nozione di *electronic eavesdropping* ai sensi del *Wiretap Act*, e dunque l'applicabilità del divieto, anche a quelle forme di *automated processing* non autorizzato delle informazioni che sostanziano il contenuto di comunicazioni elettroniche, assimilando dunque tali operazioni a «*human acquisition*». Ci riferiamo al caso *People v. Bialstock*, in cui la suddetta Corte ha ritenuto come l'installazione e l'utilizzo di un dispositivo di registrazione, anche laddove fosse semplicemente un *pen register*, esigesse un mandato giudiziario ai sensi della normativa dello stato di New York sulle intercettazioni e, in definitiva, dello stesso *Wiretap Act*, laddove il *device* stesso, come nel caso di specie, «*had the capability to redirect the signal from a telephone call meant that the device "acquired the 'contents of communications' from the moment it was installed"*»¹⁰⁶⁴.

La questione è evidentemente complessa, perché sarebbe del tutto controproducente rifiutarsi di riconoscere la realtà secondo cui, oggi, gli ISP, e più in generale gli operatori della società delle ICTs, hanno implementato infrastrutture tecnologiche potenzialmente idonee ad effettuare trattamenti ben più ampi di quelli comunicati agli utenti, e spesso necessari allo svolgimento delle

¹⁰⁶⁴ V. 610 N.E.2d 374 (N.Y. 1993), in part. 376 ss., sempre riportata da BOYDEN, op.cit., p. 693 ss., seppur per criticare la *ratio* svolta nella sua *opinion* dalla *New York Court of Appeals*. La normativa dello Stato di New York cui la Corte fa riferimento è N.Y. CRIM. PROC. LAW § 705.10. Su una simile lunghezza d'onda anche la pronuncia della *Supreme Court* *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994), in cui, con le parole di C. TABARRINI, *La trasparenza algoritmica*, cit., p.198, nota 665, «la Corte ritenne che le mere registrazioni fossero venute ad avere rilevanza ai sensi del *Wiretap Act* solo a seguito delle modifiche apportate con l'ECPA, per effetto del quale la disciplina è stata estesa alle "altre forme di acquisizione" e non solo a quelle operate per via dell'ascolto»

ordinarie attività del titolare (anche solo ai fini del miglioramento del servizio)¹⁰⁶⁵. E tuttavia, tale consapevolezza non dovrebbe tradursi in una sostanziale indifferenza rispetto ai rischi che tali stessi sistemi, laddove utilizzati (soprattutto) per condurre pratiche di *data mining* e conseguente *analytics*, fino ad adottare decisioni *solely based* sui loro risultati, configurano, in quanto fortemente idonei a condizionare indebitamente il comportamento degli interessati¹⁰⁶⁶. Come vedremo, il rilievo (e la preoccupazione) in parola costituisce la base delle riflessioni attualmente in corso nei più livelli in cui si articola il *legal system* statunitense in punto di *data privacy* sul tema del *behavioral advertising* e sulla sua identificabilità *non solo* in termini di *automated data processing*, pressoché scontata, *ma anche* in termini *automated decision making system*, così da ipotizzarsi l'applicabilità di alcune delle disposizioni settoriali dalla legislazione federale dedicate ai soli ADP *anche* al fenomeno degli ADM. È in tale contesto che si inscrivono le riflessioni sull'idoneità o meno della disciplina del *Wiretap Act* a confrontarsi con quest'ultimo fenomeno, e a garantire in modo opportuno il bilanciamento tra gli interessi all'autodeterminazione informativa del *data subject* e quelli piuttosto economici dei *data controllers* privati o di pubblico rilievo dell'autorità statale¹⁰⁶⁷.

¹⁰⁶⁵ Lo rileva D.J. SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, cit., p. 204 ss. Cfr. le considerazioni puntuali di C. TABARRINI, *La trasparenza algoritmica*, cit., p. 196 ss.

¹⁰⁶⁶ M.R. CALO, «The Boundaries of Privacy Harm», 86 Ind. L.J., 2011, 1131, 1146-52; S. Chopra, L.F. WHITE, *A Legal Theory for Autonomous Artificial Agents*, University of Michigan Press, Ann Arbor, 2011, 108 ss.

¹⁰⁶⁷ V. *infra*, par. 3 ss. Qui risulta pertinente menzionare la vicenda dell'accordo transattivo raggiunto da Google nel 2017 nell'ambito della *class action* cui aveva aderito un largo numero di utenti del servizio Gmail a fronte delle denunciate pratiche invasive di *behavioral advertising* svolte dalla società medesima: accordo con cui il motore di ricerca si è impegnato a interrompere (per un periodo di tre anni) qualsivoglia scansione automatizzata a fini pubblicitari della posta elettronica inviata a indirizzi Gmail. V. l'importante caso *Matera v. Google Inc.*, 5:15-cv-04062 LHK, in cui il punto centrale della controversia consisteva nel fatto che «according to the Gmail plaintiffs, Google's interception, scanning, and analyzing of email was done without the knowledge or consent of the plaintiffs» (p. 2). Occorre sottolineare come nel caso in esame non si sia raggiunta una pronuncia di merito; ciononostante, ivi, alla

Esaurita questa sintetica e tuttavia articolata ricostruzione, possiamo ora rivolgere lo sguardo alle normative che, come anticipato, disciplinano la *data privacy* nei rapporti tra privati in quegli specifici settori in cui più diffusa appare l'implementazione di *automated decision making systems* (ADM systems), e nel quadro delle quali possono allora rintracciarsi disposizioni dedicate a quest'ultimo fenomeno (o espressamente; o all'esito di letture esegetiche che possono tuttavia valersi di un dato letterale maggiormente "*suitable*" rispetto a tali operazioni ermeneutiche).

4.3. La disciplina federale degli *automated decision making systems* nei rapporti tra privati: *sector specific statutes* e *consumer protection*

Nell'approcciarci alla disciplina degli ADM (nel quadro, naturalmente, dei principi più generali dettati dalle normative che si affronteranno in materia di ADP) dobbiamo nuovamente, seppur in modo sintetico, richiamare due delle caratteristiche essenziali del *legal framework* statunitense in materia¹⁰⁶⁸.

luce delle prospettazioni dell'attore, si è discusso intorno all'applicabilità a tali pratiche, in conformità con le proposte dottrinali estensive che abbiamo qui ripercorso, delle normative statali e federali sul *wiretapping*, e conseguentemente del divieto di *electronic eavesdropping* di cui al Wiretap Act. Cfr. sul punto C. BOWMAN, J. GRANT, A Marketplace for Privacy: Incentives for Privacy Engineering and Innovation, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018, 451ss.

¹⁰⁶⁸ Si sottolinea, ancora una volta, come uno dei più importanti riferimenti ai fini della ricognizione che qui si opererà sia rappresentato dallo studio, da noi già parzialmente commentato, promosso dalla Commissione Europea nel 2018 in seguito al primo Joint Review dell'ormai invalidato E.U.-U.S. Privacy Shield, G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018).

Da una parte, bisogna infatti condividere le riflessioni di quanti hanno lucidamente rilevato come, a differenza del contesto culturale, prima ancora che ordinamentale, europeo, in quello statunitense «*[p]ostwar American technology policy was defined by the idea of technological development as national progress and national survival*», e che dunque, nonostante i pur apprezzabili sforzi di *policy makers* quali l'*Advisory Committee on Automated Personal Data Systems* - che nel 1973 implementò il famoso report in cui anticipava molti dei timori che ben avrebbero dovuto circondare l'impiego della tecnologia computazionale e dell'automazione¹⁰⁶⁹ -, «*the misuse of administrative and statistical data was at that time less of a concern in the U.S. than it was in Europe, where data protection laws reflect lessons learned during the Nazi and Gestapo regimes*»¹⁰⁷⁰. Stante, allora, il già richiamato focus sui benefici dell'«*accuracy, efficiency, and computational neutrality*» garantita dai sistemi di *automated processing*, gli *statutes* predisposti a livello federale dagli anni Settanta in poi hanno mostrato una certa ritrosia nel proibire, o comunque nel limitare, l'uso della tecnologia nel trattamento dei dati personali, ed anche nell'adozione di decisioni basate (unicamente o parzialmente) sul trattamento automatizzato degli stessi¹⁰⁷¹.

¹⁰⁶⁹ Cfr. ancora una volta il fondamentale *Records, Computers and the Rights of Citizens*, Report del *Secretary's Advisory Committee on Automated Personal Data Systems*, primo documento a proporre l'implementazione di un codice delle FIPs.

¹⁰⁷⁰ Per le citazioni, cfr. ancora una volta MEG LETA JONES, «The right to a human in the loop: Political constructions of computer automation and personhood», in *Social Studies of Science* Vol. 47(2) (2017), p. 225; per l'enfasi posta sull'esperienza totalitaria quale una delle principali ragioni della già riscontrate differenze nel sistema di tutela della *data privacy* in Europa e negli Stati Uniti, cfr. DAVID H. FLAHERTY, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, 1989, pp. 373-744.

¹⁰⁷¹ Cfr. sempre MET LEGA JONES, *op. cit.*. Cfr. anche, G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 42 ss., laddove si afferma che :« *Concerns with the biases embedded in the data are raised,79 but—at least historically—did not alter the generally optimistic perspective on the technologies' potential to constrain the explicit and implicit biases of human decision makers*». Altri importanti contributi

Ciononostante, anche nell'ordinamento statunitense la crescente sensibilità dell'opinione pubblica e della cultura giuridica sul punto ha condotto alla predisposizione di alcuni settoriali *sub-sistemi di garanzie* in punto, segnatamente, di processi decisionali automatizzati, e proprio di questi ora ci occuperemo. Inoltre, il recente accresciuto interesse per la dimensione dei *Big Data analytics*, del trattamento algoritmico e dei rischi da questi strumenti inevitabilmente configurati in relazione alle libertà fondamentali degli individui ha, come meglio vedremo nel prosieguo, promosso l'attività dei *policy makers* tanto federali¹⁰⁷² quanto statali (in quest'ultimo caso conducendo anche alla predisposizione di veri e propri progetti di legge dedicati *esclusivamente* a tale fenomeno)¹⁰⁷³.

Dall'altra parte, bisogna di nuovo evidenziare, a titolo introduttivo, come a livello federale l'*information privacy*, nell'ambito dei rapporti economici tra privati (e, specialmente, commerciali, ossia in sostanza professionista-consumatore), sia disciplinata per mezzo di *sector-specific statutes* ed attraverso

citati in quest'ultimo documento sono Josh Lauer, «Creditworthy: A History of Consumer Surveillance and Financial Identity in America», (2017), in cui si sottolinea come la percezione del carattere neutrale della tecnologia derivi anche come reazione alla discriminazione razziale radicata nella storia americana: «*As a technological fix for the problem of discrimination, scoring systems seemed idea*»; sulla convinzione circa la capacità della tecnologia di ovviare ai *bias* cognitivi dell'essere umano, altrettanto radicata (pare) nella cultura statunitense, viene richiamato RACHLINSKI, JEFFREY J., SHERI LYNN JOHNSON, ANDREW J. WISTRICH, CHRIS GUTHRIE. «Does unconscious racial bias affect trial judges?» in *Notre Dame L. Rev.* 84 (2008): 1195.

¹⁰⁷² Cfr. ad es. gli importanti report recentemente dedicati ai fenomeni in parola: FEDERAL TRADE COMMISSION, *Big Data: A Tool for Inclusion or Exclusion?* (January 2016); EXECUTIVE OFFICE OF THE PRESIDENT, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (May 2016);

¹⁰⁷³ Ci si riferisce essenzialmente al *Draft for Automated Decisionmaking Technology Regulations predisposto dal California Privacy Protection Agency (CPPA)* e pubblicato il 27 novembre 2023, che avrà l'obiettivo di integrare a livello secondario e nel dettaglio il *California Consumer Privacy Act (as emended by the California Privacy Rights Act)*, in punto di disciplina degli *ADM systems*, il quale già rappresenta oggi il modello più avanzato di *data privacy and protection law* esistente (e circolato) a livello statale negli U.S.A. Su quest'ultimo ci soffermerà nel prossimo e conclusivo paragrafo, dedicato appunto ad indagare il modello giuridico di riferimento predetto e gli orizzonti in punto di *ADM regulation* dischiusi dal *draft* in questione.

l'attività di *law enforcement* di *generic consumer protection laws* svolta dall'Agenzia Governativa maggiormente investita dei poteri in materia, ossia la *Federal Trade Commission*¹⁰⁷⁴. Aggiungiamo ora che a completare il quadro, accanto ai gerarchicamente sovraordinati principi costituzionali di cui ci siamo già occupati, intervengono le disposizioni delle Costituzioni statali, le singole legislazioni statali e i *binding precedents* di common (e, al suo interno di *tort*) *law* statale; nonché i c.d. *self-regulatory acts*, quali i c.d. *codes of conduct*, la cui adozione è stata continuamente promossa dal governo federale¹⁰⁷⁵, resi ulteriormente effettivi dai poteri di *enforcement* di cui la FTC gode rispetto alle imprese che, aderendovi, assumano l'impegno giuridicamente vincolante di adeguarsi ai *self-regulatory principles* medesimi¹⁰⁷⁶.

Fatte queste doverose premesse, nel paragrafo in esame ci si soffermerà principalmente sul piano dei *sector specific statutes*, in particolare di quelli che regolamentano i settori in cui, come abbiamo detto, gli *ADM systems* paiono più diffusi (e i rischi per l'*information privacy* più elevati), interrogandoci sull'esistenza nel loro contesto di disposizioni specifiche dedicate al fenomeno in questione, e in particolar modo di garanzie simili a quelle previste dall'art. 22 del GDPR. Occorre comunque evidenziare, a titolo introduttivo, che in qualsiasi caso nessuno degli atti normativi che andremo ad analizzare, pur confrontandosi con il

¹⁰⁷⁴ Sui punti in questione ci siamo già soffermati nel cap. 1, par. 2. Ricordiamo che i poteri della Federal Trade Commission in punto di *law enforcement* in materia derivano all'Agenzia medesima principalmente dal *Federal Trade Commission Act*. 15 U.S.C. § 41 ss..

¹⁰⁷⁵ Cfr. a titolo di ESEMPIO EXECUTIVE OFFICE OF THE PRESIDENT, *Consumer Data Privacy in a Networked World* (Washington DC, February 2012) (*promoting codes of conduct to implement the Administration's proposed Consumer Privacy Bill of Rights through voluntary private sector participation*). Sui *codes of conduct*, cfr. l'approfondita analisi di COLIN BENNETT, DEIRDRE MULLIGAN, *The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy* (2012). Disponibile SSRN: <https://ssrn.com/abstract=2230369> or <http://dx.doi.org/10.2139/ssrn.2230369>

¹⁰⁷⁶ Cfr. per una disamina anche SCHWARTZ, PAUL M, «The value of privacy federalism», in *Social dimensions of privacy: Interdisciplinary perspectives*, Roessler, Beate, and Dorota Mokrosinska, eds. Cambridge University Press, 2015.

fenomeno dei *fully ADM systems*, detti un esplicito divieto di decisioni basate unicamente su un trattamento automatizzato riguardante una persona fisica che produca effetti giuridici o incida in modo analogo significativamente su di essa (senza distinguere dunque, in linea di principio, i regimi giuridici previsti a fronte di un processo nel cui *loop* entri un essere umano, intervenendovi significativamente, da quelli in cui l'eventuale coinvolgimento sia solo "fittizio", e allora meccanico)¹⁰⁷⁷. Ciò non toglie che alcune garanzie, come anticipato, sussistano anche nel loro quadro.

Senza passare nuovamente in rassegna tutti i più importanti *sector-specific statutes* vigenti a livello federale in punto di *information privacy*¹⁰⁷⁸, ci limitiamo a dire che i settori nell'ambito dei quali la normativa sulla *data privacy*, agli scopi suddetti, sarà presa in esame sono essenzialmente e in prima battuta il *consumer credit system* e più in generale la *credit industry* (le normative di riferimento saranno l'FCRA e l'ECCA, *subpar.1*). In seconda battuta, ci si concentrerà sui settori in cui, a fronte dell'esponenziale diffusione della tecnologia algoritmica, maggiori appaiono i rischi configurati dalla sua attitudine potenzialmente discriminatoria: l'attenzione sarà rivolta in particolare al settore dei rapporti di lavoro e a quello del mercato residenziale, e ci interrogheremo sull'idoneità delle c.d. *equal protection laws* a governare i rischi in parola (le normative esaminate saranno allora, in particolare, il Title VII del CRA e l'FHA, *subpar.2*). Dedicheremo poi alcune brevi riflessioni alla normativa in materia di trattamento dei dati sanitari nel settore assicurativo (*subpar.3*). In conclusione, esamineremo

¹⁰⁷⁷ G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 40: «n the U.S. there is no parallel to the EU's "general prohibition" on decisions based solely on automated processing that produce legal or similarly significant effects».

¹⁰⁷⁸ Per tale panoramica, si rinvia integralmente al cap. 1, par. 1.2.

in breve il fondamentale ruolo svolto nell'implementazione della disciplina “concreta” della *data privacy* - e nel suo quadro anche dei fenomeni di ADM - dalla FTC: ruolo svolto non solo per mezzo dell'esercizio dei suoi poteri di *law enforcement* ai sensi della *Section 5* del *Federal Trade Commision Act*, ma anche mediante l'esercizio dei poteri di *non legislative guidance* (e di quelli, mai ancora esercitati, di legislative *rulemaking*) che gli derivano dalla *Section 18* del medesimo atto (sempre *subpar. 3*).

Procediamo nell'ordine appena delineato.

4.3.1. ADM e *consumer credit system*: i regimi di *consumer disclosure* e di *adverse action notice* nel *Fair Credit Reporting Act* e nell'*Equal Credit Opportunity Act*

Il settore che dagli anni Settanta ad oggi ha forse conosciuto più di tutti, in contesto statunitense, una graduale, costante proliferazione dell'*automated data processing*, e in particolare della declinazione di tale fenomeno nella specie della profilazione, è il sistema di *consumer credit*, che nel contesto in esame rappresenta l'anima della *credit industry*, regolamentata da una cospicua serie di *sector specific statues* federali¹⁰⁷⁹. Tale sistema risulta essenzialmente fondato, da una parte, sull'attività delle agenzie di *credit reporting* (*Credit Reporting*

¹⁰⁷⁹ Accanto al *Fair Credit Reporting Act* e all'*Equal Credit Opportunity Act*, dedicati al sistema del credito al consumo e dei quali ci occuperemo nel presente paragrafo, bisogna segnalare gli *statues* che regolano i *credit terms*, come il *Truth in Lending Act* che contiene il *Credit Card Act*, nonché le linee guida implementate dal governo federale in materia di *payday lending* implementato da parte delle banche, *OCC Advisory Letter* No. 2000-10 (Nov. 27, 2000). Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit. p. 50

Agencies, o CRAs), che sempre più si avvalgono, ai fini della predisposizione dei loro *credit files*, di sistemi algoritmici capaci di associare numeri di identificazione personale ai singoli consumatori e di collegarli poi, secondo le tecniche di *Knowledge Discovery in Database* che abbiamo già analizzato, alle informazioni in possesso dei *furnishers*. Dall'altra, esso appare basarsi sui sistemi di *credit scoring* predisposti dalle agenzie suddette (fenomeno al centro del *leading case* europeo SCHUFA da noi commentato), nell'ambito dei quali i *credit-risk models* strumentali a *prevedere* il comportamento -economico e non solo-, e più in generale l'attribuzione del punteggio relativo al merito creditizio fondato su preciso tasso di probabilità, come è stato notato, risultano «*calculated from an algorithm or mathematical model*»¹⁰⁸⁰.

L'importanza del fenomeno e del mercato in questione è testimoniata dal fatto che nella più gran parte dei settori merceologici, al fine di consentire l'accesso al credito da parte delle persone fisiche ("degradata" allo status di *consumatore*, in una prospettiva in stile *homo oeconomicus*), che si articola in una eterogenea platea di servizi (dalle carte di credito al noleggio auto, dai mutui di scopo o ipotecari al prestito erogato agli studenti), le *companies* e gli stessi istituti finanziari cui esse si rivolgono (generalmente identificati con il termine *lenders*) si avvalgono dei suddetti report o dello score calcolato dalle CRAs ai fini della valutazione sulla attuale e soprattutto futura solvibilità (e, più in generale, affidabilità) del potenziale cliente, e dunque per adottare una decisione sulla

¹⁰⁸⁰ *Ibidem*. Cfr. in particolare NATIONAL CONSUMER LAW CENTER, *Fair Credit Reporting* § 16.2.2.2 (9th ed. 2017); per una panoramica generale sul volume, sull'attività e sulla disciplina del Credit Reporting Industry nel contesto statunitense, cfr. CONSUMER FINANCIAL PROTECTION BUREAU, *Key Dimensions and Processes in the U.S. Credit Reporting System*, December 2012, at 22, che oltre a delineare alcune definizioni generali dei concetti introdotti (credit report, credit files e credit scoring), sui quali tuttavia ci soffermeremo nel contesto degli atti normativi che analizzeremo, rileva lucidamente come «*Credit reports play an increasingly important role in the lives of American consumers. Most decisions to grant credit – including mortgage loans, auto loans, credit cards, and private student loans – include information contained in credit reports as part of the lending decision*».

application medesima¹⁰⁸¹. E il ricorso ai complementari servizi di *credit reporting* e di *credit scoring* offerti dalle suddette Agenzie pare non limitarsi alla sfera del *decision-making* in punto di accesso al credito - o *credit eligibility* - in senso stretto, bensì estendersi, solo per fare alcuni esempi, alla valutazione del rischio in ambito assicurativo (è il fenomeno definito come *credit-based insurance scoring*)¹⁰⁸² o piuttosto in punto di *bank account application*, ossia di apertura di un conto corrente in un diverso istituto bancario ¹⁰⁸³, e addirittura all'apprezzamento dell'affidabilità di un potenziale locatario¹⁰⁸⁴. Ma l'idoneità delle pratiche in esame ad incidere negativamente sulle libertà fondamentali degli individui-consumatori, e pertanto la loro potenziale attitudine discriminatoria, risulta ancor più evidente laddove si consideri, come è stato sottolineato, che i report creditizi (sempre più, come vedremo subito, prodotti algoritmicamente) possono essere utilizzati - ed attualmente lo sono sempre più spesso - da professionisti e imprese per valutare il profilo di un candidato ad una posizione di lavoro aperta: un recente studio ha dimostrato come il 60% della larga platea di *employers* coinvolti nel sondaggio si fosse avvalsa dei suddetti *credit reports* per decidere sulle singole *applications*.¹⁰⁸⁵

¹⁰⁸¹ CONSUMER FINANCIAL PROTECTION BUREAU, *Key Dimensions and Processes in the U.S. Credit Reporting System*, cit., p. 5.

¹⁰⁸² È quanto emerge da un approfondito report della FTC, FEDERAL TRADE COMMISSION, *Credit-Based Insurance Scores: Impacts on Consumers of Automobile Insurance, A Report to Congress* (2007).

¹⁰⁸³ MARCIE GEFFNER, «Banking and your credit score», in *Bankrate.com* (Mar. 17, 2011), disponibile su: <http://www.bankrate.com/finance/savings/banks-checking-credit-scores-more-often-1.aspx>.

¹⁰⁸⁴ Altri esempi possono rintracciarsi IN EXPERIAN – OLIVER WYMAN, «Comprehensive Consumer Credit Review», *Experian-Oliver Wyman Market Intelligence Report*, at 7 (2011 Q4), che riscontra come «Of 113 million credit card and retail card accounts, auto loans, personal loans, mortgages, and home equity loans originated in the United States in 2011, the vast majority of approval decisions used information furnished by credit reporting agencies».

¹⁰⁸⁵ Cfr. CONSUMER FINANCIAL PROTECTION BUREAU, *Key Dimensions and Processes in the U.S. Credit Reporting System*, cit., laddove in part. alla nota 6 ricorda come «The FCRA allows for the sharing of credit reports for employment purposes. See 15 U.S.C. § 1681b(a)(3)(B)». Lo studio a cui si fa riferimento è invece quello indetto poco

Questo, il contesto tradizionalmente esistente. Ciò che rende tuttavia importante interrogarsi sulla disciplina della *data privacy*, e più nello specifico dei sistemi di trattamenti e di decisione automatizzati, nel settore in esame è l'accresciuta portata discriminatoria assunta nel contesto della *data driven economy* e della *algorithmic society* dalle attività in parola¹⁰⁸⁶. Difatti, parallelamente al fatto che il sistema di *consumer credit reporting*, e dunque quello del *credit scoring*, gestisce un flusso di dati di enormi dimensioni, che va ad alimentare l'input dei trattamenti suddetti, le CRAs hanno implementato un numero sempre maggiore di modelli algoritmici deputati ad automatizzare tanto i processi di «*quality control on incoming data*» quanto i «*matching process by which the NCRAs [ossia Nationwide Credit Reporting Agencies] assign incoming trade line data to consumer-specific credit files*».¹⁰⁸⁷ Con l'incremento senza precedenti dell'impiego della tecnologia algoritmica nella definizione dei profili sui quali si baseranno tutte le decisioni in punto di credito al consumo, aumenta pertanto l'importanza della qualità e dell' «*accuracy*» delle informazioni di partenza¹⁰⁸⁸: non è un caso che già nel 2007 la *Federal Reserve* sottolineasse

più di un decennio fa da THE SOCIETY FOR HUMAN RESOURCE MANAGEMENT, *SHRM Research Spotlight: Credit Background Checks*, Society Human Resource Management, 2010; lo studio ha coinvolto *small, medium and large employers*, ed ha ulteriormente riscontrato come ben il 47 % dei datori di lavoro avesse controllato il “profilo creditizio” di singoli candidati, e di come ben il 13% si fosse avvalso dei *consumer credit reports* per valutare il profilo di *tutti* i candidati.

¹⁰⁸⁶ E dunque del *reporting* e dello *scoring*, che accedendo alla lettura sancita dalla Corte di Giustizia nel cas *SCHUFA* in contesto europeo risultano già qualificabili, laddove non contemplino in alcuna delle loro fasi un coinvolgimento umano effettivo, come decisioni basate unicamente sul trattamento automatizzato e pertanto ricadenti nell'ambito applicativo del divieto di cui all'art. 22 del GDPR: v. ampiamente *retro*, cap. 2, par. 3.2.4.

¹⁰⁸⁷ Cfr. CONSUMER FINANCIAL PROTECTION BUREAU, «Key Dimensions and Processes in the U.S. Credit Reporting System», cit., p. 2 ss.

¹⁰⁸⁸ Nel rinviare alle considerazioni già svolte nei capitoli precedenti, rinviamo ancora una volta ad uno dei contributi che meglio affronta la questione sul piano generale, G. D'ACQUISTO, Qualità dei dati e intelligenza artificiale: intelligenza dai dati e intelligenza dei dati, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., 285. Cfr. di nuovo anche il fondamentale T. ZARSKY, «Understanding Discrimination in the Scored Society», in *Washington Law Review*, 2014, 89, 1375 ss.

l'importanza dell'accuratezza dei *credit reports*, affermando che «*for the full benefit of the credit-reporting system to be realized, credit records must be reasonable, complete and accurate*»¹⁰⁸⁹.

Il monito, oggi, suona ancora più importante in relazione al fenomeno dei *Big Data*, che ha notevolmente ampliato la pletora di informazioni di cui le CRAs dispongono per elaborare ed integrare -algoritmicamente- i propri report e per calcolare i *credit scores*: tali informazioni, infatti, eccedono i semplici dati di natura finanziaria (puntualità nei pagamenti, dilazioni richieste ecc.) e, come è stato puntualmente analizzato, sono acquistate dai *Data Broker* o attraverso le consuete tecniche di *Big Data analytics* a partire dagli stessi *user-generated contents*¹⁰⁹⁰. *Big Data* e tecnologia algoritmica, in particolare nella sua declinazione in termini di *Unsupervised ML* e ancor più di *DL*, rappresentano allora una “miscela esplosiva”. Da una parte, se i *Big Data* in ipotesi, accrecendo la base informativa di cui dispongono le Agenzie, possono implementare la precisione dell'output, sappiamo tuttavia che l'eccesso di informazioni circolanti e la potenziale inattendibilità della fonte rendono assai elevato il rischio di inserire nel processo *Bad Data*, e conseguentemente di perpetuare pregiudizi, *bias* e modelli discriminatori insiti nel contesto sociale di riferimento¹⁰⁹¹. Dall'altra, lo stesso impiego di sistemi di IA, e ancor più di *ML* e *DL*, stante la crescente

¹⁰⁸⁹ FEDERAL RESERVE BOARD, *Report to Congress on Credit Scoring and its Effects on the Availability and Affordability of Credit* (August 2007) (Board Credit Scoring Report), disponibile su <http://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf>.

¹⁰⁹⁰ Per un'analisi di sistema, cfr. V.A. HERTZA, «Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?», 93, N.Y.U. L. Rev., 2018, 1707, 1710; sul punto cfr. poi la ricognizione attenta di C. TABARRINI, *La trasparenza algoritmica*, cit., p. 200 ss.

¹⁰⁹¹ Oltre ai rilievi generali svolti da E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della black-box society», cit., cfr. per quanto attiene più nello specifico anche al contesto statunitense S. BAROCAS, A.D. SELBST, «Big Data's Disparate Impact», 104, Calif. L. Rev., 2016, 671, 678ss.

complessità tecnologica dei modelli alternativi di calcolo di punteggi di credito, non fa che aggravare la già denunciata opacità dei processi decisionali¹⁰⁹².

Ebbene, in tale contesto tecnologico e socioeconomico non possono che aumentare i rischi cui risulta esposto l'individuo in seno alla collettività di risultare vittima di processi per lo più automatizzati di valutazione del merito creditizio poco o per nulla affidabili, o di restare a priori escluso dal credito, anche a causa delle difficoltà in punto di intervento umano nella rettificazione ed integrazione dei dati di partenza¹⁰⁹³.

Nella materia che ci occupa, di cristallina importanza risultano i due atti normativi federali di natura settoriale di maggior rilievo, poiché dal sistema normativo che disegnano – secondo le voci che qui si è scelto di seguire – sembra possibile inferire un *corpus* di garanzie simili (o per lo meno assimilabili) a quelle predisposte dal GDPR (e pure dallo stesso art. 22) a fronte di processi decisionali automatizzati. Ci riferiamo al *Fair Credit Reporting Act* (FCRA)¹⁰⁹⁴, precipuamente dedicato ai doveri d'informazione delle CRAs nei confronti dei consumatori (e ai corrispondenti loro diritti) circa il fatto che le loro informazioni siano utilizzate ai fini di decisioni riguardanti l'accesso al credito, ai rapporti di lavoro o ad altri oggetti analoghi; e l'*Equal Credit Opportunity Act* (ECOA)¹⁰⁹⁵,

¹⁰⁹² Cfr. ancora una volta F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, cit., p. 25 ss.; sul punto specifico cfr. C. TABARRINI, La trasparenza algoritmica, cit., che con Barocas e Selbst (op. cit. nella nota precedente) introduce il fenomeno degli *altscores* o *e-scores*, rinviando anche, tra l'altro, a M. SEGAL, *What Is Alternative Finance?* (Office of Advocacy, U.S. Small Business Administration), 2016, sottolineando come le società che sviluppano *altscores* non identificandosi sempre, quanto al proprio oggetto sociale, come CRAs, esulino dall'ambito di applicazione dell'FCRA.

¹⁰⁹³ Cfr. V.A. HERTZA, «Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?», 93, *N.Y.U. L. Rev.*, 2018, 1707, 1713; CONSUMER FINANCIAL PROTECTION BUREAU, *Key Dimensions and Processes in the U.S. Credit Reporting System*, cit., p. 6 ss.

¹⁰⁹⁴ Public Law No. 91-508, tit. VI, 84 Stat. 1114 (1970); consolidato nello *United States Code*, al Titolo VI del *Consumer Credit Protection Act*: 15 U.S.C. § 1681 ss.

¹⁰⁹⁵ Pub. L. No. 94-239, 90 Stat. 251 (1976); consolidato anch'esso nello *United States Code*, 15 U.S.C. § 1691 ss.

ispirato dalla *ratio* di assicurare ai soggetti che si rivolgono al sistema di credito al consumo di non essere discriminati su alcune delle basi dallo stesso atto specificamente individuate, tra i quali l'etnia e il genere¹⁰⁹⁶.

Sebbene i due atti in parola, stante il loro specifico ambito di applicazione che di seguito si delineerà, si applichino (per esprimerci con le categorie a noi note in contesto europeo) *indipendentemente* dalla circostanza che il trattamento, e la decisione conseguentemente adottata sulla sua base, sia interamente o solo parzialmente automatizzata, occorre sottolineare che nel settore considerato è pressoché totale la prevalenza dell'*automated processing* e dell'*automated decision making*. Parallelamente, come detto, secondo parte della letteratura – cui aderiamo - tali atti recherebbero disposizioni che edificano un sistema di garanzie assimilabile (ma non sempre, lo si premette, equivalente) al sistema previsto dal GDPR (specialmente dove letto alla luce delle ampiamente esaminate Linee Guida del Gruppo di Lavoro Articolo 29) *anche* in punto di processi decisionali *interamente* automatizzati. Ciò risulta ancora più rilevante, ai nostri fini, se si considera che gli *statutes* in questione si applicano nei confronti di enti statunitensi, e in primis di *Credit Reporting Agencies*, che operano anche in relazione ai dati provenienti dall'Europa, qualora in precedenza avessero certificato la propria adesione al *Privacy Shield*; ed oggi, qualora operino sulla base di Clausole Contrattuali Standard o Norme Vincolanti d'Impresa alle condizioni stabilite dalla Corte di Giustizia dell'UE nella sentenza *Schrems II*, o

¹⁰⁹⁶ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 150 ss.; per alcune analitiche indicazioni sulla struttura, sulle definizioni e sulla disciplina dell'FCRA, cfr. *Fair Credit Reporting* (The consumer credit and sales legal practice series, NATIONAL CONSUMER LAW CENTER, IX ed.), 2017; sull'ECOA, cfr. 3 Cfr. J. H. MATHESON, «The Equal Credit Opportunity Act: A Functional Failure», 21, *Harv. J. On Legis.*, 1984, 371, 388; mentre, per una panoramica generale e sintetica, cfr. S. H. BOYNE, *Data Protection in the United States*, cit.,

laddove abbiano certificato la propria adesione al neo-nato *Data Privacy Framework*¹⁰⁹⁷.

Cominciamo, anche per ragioni cronologiche, dall'FCRA, rinviando al primo capitolo per quanto attiene alla sua genesi e all'iter di approvazione. In questa sede, sul punto, aggiungiamo solo che, come evidenziato dal Report del Congresso che ne ha accompagnato la predisposizione, l'intervento normativo in parola mirava ad implementare la precisione e la riservatezza delle informazioni raccolte dalle *credit bureaus* (qui da tradursi, se si vuole, avvalendosi del concetto italiano di "Centrale Rischi") nel contesto del fiorente fenomeno del *credit reporting* e del *credit scoring*, dal momento che tali enti troppo spesso fondavano i propri processi valutativi su dati erronei o incompleti¹⁰⁹⁸. I motivi suddetti conducono, come sappiamo all'adozione (nel 1970) di quella che è tradizionalmente considerata la prima normativa espressamente dedicata, secondo un approccio *sector-specific*, alla *data privacy* nei rapporti interprivati, anche a dimostrazione del peso precocemente assunto dalla circolazione delle informazioni e dalla loro elaborazione elettronica nel contesto della *credit reporting industry*¹⁰⁹⁹.

¹⁰⁹⁷ V. *retro*, cap. 2, par. 2.4., e cap. 4, par. 1.

¹⁰⁹⁸ Cfr. 115 Congressional Records 2410, 2411 (1969), che espressamente rileva come « [t]he banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system».

¹⁰⁹⁹ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 52 ss.; per una ricognizione del contesto tecnologico e giuridico in cui la normativa in questione fiorisce, cfr. ancora *Fair Credit Reporting (The consumer credit and sales legal practice series*, NATIONAL CONSUMER LAW CENTER, IX ed.), 2017, par. 1.4.

Passiamo ad analizzare la struttura normativa generale dello *statute*, seguendone anche diacronicamente le trasformazioni imputabili alle novelle succedutesi.

Circoscrivendo l'ambito di applicazione soggettiva dell'atto, dobbiamo in primo luogo rilevare come esso si applichi alle *Consumer Reporting Agencies* (CRAs), definite dal §1681a(f) come «*any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports*». La definizione, come sottolinea lo stesso Studio della Commissione europea ¹¹⁰⁰, appare sufficientemente ampia da ricomprendere, accanto alle CRAs tradizionali, definite anche *Nationwide* (da qui, NCRAs), come Equifax, TransUnion ed Experian, anche altre *credit bureaus*, spesso denominate «*special CRAs*», come «*tenant screening bureaus, check approval services, and employment screening agencies*»¹¹⁰¹. E può essere interessante rilevare come taluni autori notino che tale definizione, stante la sua ampia portata, consenta di ascrivervi anche i social network, come Facebook, qualora questi vendano informazioni a terze parti rispetto alle quali sussista una ragionevole aspettativa sociale circa il fatto che esse useranno tali informazioni per adottare «*credit decisions*»¹¹⁰².

¹¹⁰⁰ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 52

¹¹⁰¹ Cfr. sul punto NATIONAL CONSUMER LAW CENTER, *Fair Credit Reporting* § 1.2.1 (9th ed. 2017).

¹¹⁰² Cfr. ADAM LEVITIN, «Facebook: The New Credit Reporting Agency?», in *Credit slips* (August 21, 2018), disponibile su <http://www.creditslips.org/creditslips/2018/08/facebook-the-new-credit-reporting-agency.html>.

La disposizione in parola introduce il concetto di *consumer report*, che ai fini della normativa in questione, ai sensi del § 1681a (d)(1), indica «*any communication of any information by a consumer reporting agency bear[s] on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, and is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for one or more of several purposes specifically enumerated in the statute.*». Definizione complessa, quest'ultima, la quale tuttavia, come è stato notato, «*is a broad term that encompasses many different kinds of reports*», che in ogni caso implica quale autore del medesimo una CRAs, e si estende dalle comunicazioni incentrate sulle informazioni strettamente relative al *consumer credit* - e quindi a monte alla situazione finanziaria dell'individuo - fino a quelle che attengono alla sua situazione lavorativa, o piuttosto derivanti dai c.d. *user generated contents* (su tutti, ad esempio, dai social media)¹¹⁰³.

Per effetto della novella apportata dal *Consumer Credit Reporting Reform Act* del 1996, inoltre, l'ambito di applicazione soggettivo è stato esteso, da una parte, ai soggetti che utilizzano (e dunque che adottando decisioni basate sui) *consumer reports* emessi dalle CRAs, i c.d. *users*, quali banche ed istituti finanziari; e, dall'altra, ai soggetti che forniscano «*consumer-reporting information*», i c.d. *furnishers*, come le *credit card companies*¹¹⁰⁴.

¹¹⁰³ Cfr. sul punto G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 53 ss., che rinvia anche all'interessante articolo di CHARLES DUHIGG, «What Does Your Credit-Card Company Know About You?», in *New York Times*, May 12, 2009, available at <https://www.nytimes.com/2009/05/17/magazine/17credit-t.html>. Sulle definizioni in parola, cfr. ancora S.H. BOYNE, «Data Protection in the United States», cit., pp. 299-304

¹¹⁰⁴ 15 USCA § 1681a (r), (s) e (t).

Passando all'ambito di applicazione materiale della disciplina predisposta dall'atto, è importante evidenziare come, nonostante il necessariamente più ristretto perimetro rispetto al GDPR, l'FCRA nell'individuare le finalità legittimamente perseguibili attraverso le attività di *consumer reporting*, ossia la comunicazione delle informazioni suddette ai terzi individuati dall'atto (a cui è funzionalmente collegata la liceità delle decisioni e più in generale dei comportamenti adottati dai terzi sulla base delle informazioni medesime), faccia riferimento, accanto alla concessione di finanziamenti, ad un disparato novero di settori, quali ad esempio l'utilizzo «*for employment purpose*» o «*in connection with the underwriting of insurance involving the consumer*», o l'erogazione di servizi pubblici¹¹⁰⁵.

Può essere utile introdurre qui anche la definizione di *credit score* accolta dall'FCRA, che, così come interpretata dallo Studio della Commissione europea cui ci stiamo qui ripetutamente riferendo, consiste in «*a numerical value used to predict the likelihood that a consumer will engage in certain behavior, such as missing loan payments or entering into bankruptcy*»¹¹⁰⁶. Tradizionalmente, si distingue poi tra *credit risk score*, di natura “generica”, che è anche la declinazione più nota della categoria in questione, da intendersi come «*a number derived from information in a consumer's file at one of the nationwide CRAs*»; e «*“industry” scores*», definiti come quei punteggi utilizzati «*to predict payment behavior for a specific type of credit, such as automobile or student loans, and*

¹¹⁰⁵ V. infatti 15 USCA § 1681b., rubricato «*Permissible purposes of consumer reports*». Da notare come l'atto circoscriva esplicitamente la legittimità del consumer credit reporting in relazione ai servizi di marketing di prodotti finanziari, laddove al 1681s-3 afferma che il soggetto che il report riceve «*may not use the information to make a solicitation for marketing purposes to a consumer about its products or services*».

¹¹⁰⁶ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 59. La definizione dell'FCRA è collocata in 15 USC § 1681g(f)(2)(A)(i).

“custom” scores, which large lenders develop internally to predict their customers’ performance»¹¹⁰⁷. Assai importanti appaiono, in merito, alcune delle riflessioni articolate dal *National Consumer Law Center*, laddove l’istituto osserva quanto segue: «*The credit score may be the single most influential, critical piece of information associated with a consumer’s file at a CRA*» dal momento che esso può essere utilizzato per una molteplicità di scopi, tra cui, solo a titolo di esempio «*pre-screen and preselect consumers for direct marketing, to determine interest rates and credit limits, to collect on mortgage loans, and for sale of loans to Wall Street and secondary market purchasers*»¹¹⁰⁸.

Bisogna ricordare, incidentalmente, come il *Fair and Accurate Credit Transactions Act* del 2003 (FACTA) abbia a sua volta integrato la disciplina del FCRA con la predisposizione di misure finalizzate a contrastare frodi e furti d’identità nel contesto delle attività medesime e a ridurre i danni eventualmente subiti dai consumatori in conseguenza di tali illeciti¹¹⁰⁹.

Veniamo allora, finalmente, al piano dei diritti di informativa ed ai doveri di *notice* previsti dall’atto in parola, premettendo che faremo sul punto solo un riepilogo, concentrandoci poi su quelli più rilevanti ai nostri scopi (essenzialmente, lo si anticipa, il diritto e insieme il dovere di *consumer disclosure*)¹¹¹⁰. L’FCRA sembra articolare la propria disciplina su tre livelli, il

¹¹⁰⁷ *Ibidem*, ma cfr. per una più ricognizione più dettagliata CFPB, *The impact of differences between consumer- and creditor-purchased credit scores*, luglio 2011, disponibile al seguente link: https://s3.amazonaws.com/files.consumerfinance.gov/f/2011/07/Report_20110719_CreditScore_res.pdf.

¹¹⁰⁸ Cfr. NATIONAL CONSUMER LAW CENTER, *Fair Credit Reporting* § 16.3.2 (9th ed. 2017).

¹¹⁰⁹ FTC, *Forty Years of Experience With the Fair Credit Reporting Act* (July 2011), 2-3

¹¹¹⁰ Ai fini della ricognizione che di qui in avanti si compierà (anche in relazione alla *consumer disclosure*) i riferimenti principali saranno (in parte, lo si ripete), G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 58 ss.;

primo dei quali attiene essenzialmente ai doveri d’informativa attraverso notifica¹¹¹¹; il secondo alle procedure amministrative di risoluzione delle controversie, essenzialmente incardinate davanti alla FTC¹¹¹²; e il terzo al rafforzamento dello standard probatorio per l’accesso governativo a tali informazioni (c.d. *State Claims*)¹¹¹³.

Il livello che più ci interessa, e laddove è possibile rintracciare norme che predispongono un sistema di garanzie assimilabile, seppur entro determinati limiti, a quello previsto dal GDPR in punto di processi decisionali automatizzati, è certamente il primo, che tra i diversi diritti speculari alle disparate *notices* imposte tanto alle *nationwide* quanto alle *special* CRAs (con terminologia appropriata in contesto *data protection*, qualificabili come *data controllers*), prevede il diritto dell’interessato-consumatore ad essere preventivamente informato laddove una determinazione assunta nei suoi confronti si basi su un *credit report* di qualsiasi specie; un diritto di accesso al contenuto del report che si estende alla fonte e alla natura dei dati “in possesso” delle CRAs¹¹¹⁴ e a contestarne conseguentemente l’eventuale erroneità; ed anche il diritto di conoscere il *credit score* ad esso assegnato¹¹¹⁵.

NATIONAL CONSUMER LAW CENTER, *Fair Credit Reporting*, cit., cap. 2 ss.; C. TABARRINI, *La trasparenza algoritmica*, cit., p. 205 ss.; FTC, «Forty Years of Experience With the Fair Credit Reporting Act» (July 2011), cit, p. 3 ss.

¹¹¹¹ Lo stesso studio cui costante riferimento andiamo facendo di G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, op. cit., rileva come, accanto al dovere che costuirà oggetto di approfondita trattazione a breve (ossia quello di consumer disclosure), «*The FCRA also requires numerous notices that will not be discussed in detail in this report. These include negative information notices, notices related to disputes under the FCRA, notice when information may be shared by affiliates, notices required of government agencies, and notices related to the possible fraudulent use of credit.*»

¹¹¹² La disciplina delle funzioni di law enforcement in relazione al FCRA della FTC è contenuta nella Section 621, 15 USC 1681s.

¹¹¹³ Cfr. sul punto approfonditamente National Consumer Law Center, *Fair Credit Reporting*, cit., cap. 3 ss.

¹¹¹⁴ 15 USC 1681 (a)(4)

¹¹¹⁵ 15 USC A 1681g

Soprattutto, nel corpo del primo livello è possibile individuare un sub-sistema di diritti e di doveri rispettivamente dei consumers e delle CRAs, degli *users* e dei *furnishers* il quale risulta forse il più significativo ai fini dell'analisi che stiamo conducendo, e dunque ai fini dell'individuazione delle adeguate garanzie per l'interessato-consumatore in relazione alle ipotesi di *fully automated credit reporting* idonee ad incidere significativamente sulla sua persona: ci riferiamo al regime dei c.d. *discollosure requirements*, anche definito più semplicemente *consumer disclosure*, nel suo complesso configurato dalla sezione 1681g del Titolo XV dello *United States Codes* (rubricato, appunto, «*Discollosures to consumers*»), che lo stesso Studio della Commissione Europea alla cui struttura argomentativa spesso qui ci ricollegiamo definisce come «*a pillar of FCRA*»¹¹¹⁶. Senza qui soffermarci su ciascuno dei puntuali doveri di *notice* previsti dalle norme ivi raggruppate, procediamo a prendere in esame le previsioni, e le posizioni giuridiche soggettive che ne scaturiscono, utili ad un confronto con la disciplina garantistica dettata dal GDPR in materia di processi decisionali automatizzati (in particolare, lo si ripete, laddove *interamente* tali).

In primo luogo, ai sensi della lettera (a), ogni CRAs è tenuta a comunicare («*disclose*») all'interessato «*clearly and accurately*», laddove l'interessato-consumatore ne faccia richiesta, e salva una serie di eccezioni che non prenderemo analiticamente in esame: «(1) *All information in the consumer's file at the time of the request* [e dunque, a ottenere una *copia completa* del report] (...); (2) *The sources of the information* [e dunque le fonti, e laddove l'interessato agisca in giudizio anche quelle delle informazioni preparatorie di un *investigative consumer report*]; (3) *Identification of each person* [compresi gli *end-users* di cui

¹¹¹⁶ G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 60.

abbiamo già parlato] *that procured a consumer report* (a) *for employment purposes* [solo laddove fornite entro i due anni precedenti la richiesta] (b) *for any other purpose* [solo laddove fornite entro i 12 mesi precedenti la richiesta] (...)»¹¹¹⁷. Le previsioni in parola, nell'articolare il contenuto del diritto d'informativa degli interessati, laddove ricorra un'ipotesi di *consumer reporting* interamente automatizzato, appaiono già in parte consonanti con l'art. 15 par. 1 lett. h) del GDPR, come interpretato dal WP 29, poiché «*help data subjects gain some understanding of how the system works*»¹¹¹⁸. Ricordiamo poi, sempre sul piano generale, che il par. 1681h, alla lett. c), tra le forme e le modalità di *consumer disclosure* esplicitamente annovera l'educazione del personale, o meglio il fatto di dover disporre di «*trained personnel to explain to the consumer any information furnished*» ai sensi delle norme suddette e di quelle che analizzeremo a breve. Su tale aspetto si tornerà tra poco.

Affinché, tuttavia, l'interessato possa indirizzare la suddetta richiesta alla CRA, e dunque esercitare il proprio *right to disclosure*, indispensabile risulta il fatto che egli sia consapevole di esserne titolare. Pertanto, ai nostri fini, ancor più importante appare la complementare previsione espressa nella subito successiva lettera (c), rubricata «*Summary of Rights to Obtain and Dispute Information in Consumer Reports and to Obtain Credit Scores*», la quale, analogamente a quanto

¹¹¹⁷ V. 15 U.S.C. § 1681g, lett. (a), nn.(1)-(3)-rubricata «*Information on file; sources; report recipients*».

¹¹¹⁸ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 63, che richiamano peraltro GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 30, laddove nell'interpretare la disposizione in parola afferma che «*L'articolo 15, paragrafo 1, lettera h), afferma che il titolare del trattamento deve fornire all'interessato informazioni sulle conseguenze previste del trattamento (...) Il titolare del trattamento dovrebbe fornire all'interessato informazioni di carattere generale (in particolare, sui fattori presi in considerazione per il processo decisionale e sul rispettivo "peso" a livello aggregato) che sono utili all'interessato anche per contestare la decisione*».

sia possibile desumere dal combinato disposto tra gli art. 5, 6, 12, 13 e 14 del GDPR, seppur nello specifico settore considerato, configura in capo alle CRAs un vero e proprio dovere d'informativa dettagliata¹¹¹⁹. Nella materia che ci occupa, la sub-disposizione più rilevante è certamente quella articolata nelle lettere di cui al sottostante n. (1), rubricato « *Bureau Summary of Rights Required*», che in primo luogo prescrive all'Authority preposta al *rulemaking* di carattere secondario in relazione alla più gran parte delle disposizioni dell'FCRA, ossia il *Bureau of Consumer Financial Protection* (di seguito, solo *Bureau* o piuttosto CFPB), di predisporre un « *model summary* [potremmo tradurlo, letteralmente, come un “modello d'informativa”] *of the rights of consumers*» cui le singole Agenzie dovranno conformarsi nel redigere l'opportuna informativa¹¹²⁰. La fisionomia dei diritti in parola è declinata nella successiva lettera (B), che nell'individuare il contenuto del *summary* prescrive in sostanza che l'Agenzia/il titolare del trattamento comunichi puntualmente all'interessato, in primo luogo, l'esistenza del «*right of a consumer to obtain a copy of a consumer report*» di cui abbiamo appena parlato, e dunque definito dalla lettera (a); poi, l'altrettanto fondamentale diritto di contestare (*to dispute*) le informazioni nel report medesimo contenute; ed il diritto di ottenere dalla stessa CRA un *credit score*, oltre che una descrizione sulle modalità attraverso cui ottenerlo¹¹²¹.

Quest'ultimo rappresenta la posizione giuridica forse più importante nel discorso che stiamo svolgendo. Dobbiamo infatti tenere bene a mente il dibattito

¹¹¹⁹ V. 15 U.S.C. § 1681g, lett.(c).

¹¹²⁰ Ivi, (1). Cfr. lettera (w), che puntualmente precisa come ai fini dell'FCRA, «*Bureau means the Bureau of Consumer Financial Protection*». Ricordiamo infatti, sul punto, che nel 2010 *Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)* ha attribuito *rulemaking authority* in relazione all'FCRA (ad eccezione della sezione 615(e)) e alla sezione 628, al CFPB. Cfr. sul punto CFPB, «Fair Credit Reporting Act. Manual 2.0», in *CFPB Consumer Laws and Regulations*, ottobre 2014, p. 1 ss., https://files.consumerfinance.gov/f/documents/102012_cfpb_fair-credit-reporting-act-fcra_procedures.pdf

¹¹²¹ Ivi, (1), in part. (A) e (B), nn. (i), (iii) e (iv).

che in contesto eurounitario ha circondato la questione relativa alla *natura* del *credit score* automatizzato, e dunque circa la qualificazione dello stesso già di per sé in termini di decisione basata unicamente su un trattamento automatizzato ai sensi dell'art. 22 del GDPR, laddove la sua elaborazione non avesse coinvolto se non passivamente alcun “revisore” umano, *indipendentemente* dal successivo utilizzo ad opera di un terzo operatore economico. Tale questione, come sappiamo, è stata positivamente risolta dalla Corte di Giustizia nel recente *leading case* sui processi decisionali interamente automatizzati, c.d. *SCHUFA*¹¹²². In ogni caso, certamente automatizzata, se basata esclusivamente sul punteggio medesimo, nonché incidente significativamente sulla sfera giuridica o comunque sulla sfera d'interessi rilevanti della persona fisica, risulta la decisione adottata dall'*end-user* che accolga o piuttosto rifiuti la richiesta (della più disparata natura) di un *consumer*¹¹²³.

Stante, allora, la potenziale idoneità del *credit score* “algoritmico”, e quindi del calcolo esclusivamente automatizzato del punteggio di merito creditizio (o in ogni caso della decisione dal terzo *user* adottata sulla sua esclusiva base) a rappresentare un processo decisionale *interamente* automatizzato «*significantly affecting an individual*», e pienamente ricadente nell'ambito applicativo dell'FCRA, occorre interrogarsi sulle specifiche garanzie predisposte dall'FCRA sul punto: poiché è su tale piano che, data l'omogeneità delle fattispecie di

¹¹²² V. ampiamente *retro*, cap. 3., par. 2.4.; cfr., in ogni caso, di nuovo C. Giust. UE 7.12.2023, causa C-634/21, *OQ contro Land Hessen*, in part. par. 47 ss. Per alcuni riscontri sul punto già nel quadro delle riflessioni del WP 29, cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 23. Per una più approfondita analisi del funzionamento degli scoring mechanisms, in materia creditizia e non solo, cfr. ancora una volta BRENDA REDDIX-SMALLS, «Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market», (2011); T. ZARSKY, «Understanding Discrimination in the Scored Society», in *Washington Law Review*, 2014, 89, 1375 ss.

¹¹²³ V. la sentenza e le linee guida citate nella nota precedente, pressoché negli stessi punti ivi indicati.

riferimento, può svolgersi una puntuale comparazione con il sub-sistema predisposto dall'art. 22, e quindi con quelle misure adeguate di tutela imposte dall'art. 22 par. 3 e rafforzate dagli artt. 13-15.

Sul tema, pertinenti risultano molte delle norme incardinate nella lett. (f) del medesimo paragrafo, rubricato proprio «*Disclosure of Credit Scores*»¹¹²⁴. Il sub-sistema settoriale che ne deriva, ai sensi del n. (1) ss., impone all'Agenzia, laddove l'interessato eserciti il suddetto *right to obtain a credit score*, di fornire determinate informazioni sul punto analiticamente articolate: tuttavia, bisogna sottolineare come la previsione di cui al n. (8) autorizzi la CRA destinataria della richiesta a subordinare l'accesso richiesto dall'interessato al proprio credit score al pagamento di una *fair and reasonable fee* stabilita nel suo ammontare dalla stessa CFPB¹¹²⁵. Il che pare già rappresentare una prima sostanziale differenza con i diritti d'informativa saniti dal GDPR, tanto con quelli di ordine generale quanto con quello previsto dall'art. 15 par. 1 lett (h) a conoscere l'esistenza di un processo decisionale di cui all'art. 22: la *fee* in questione, in sostanza, appare come un *nudge* disincentivante il singolo all'esercizio dei propri diritti di *consumer disclosure* sul punto, e perciò rischia di affievolire l'effettività del diritto d'informazione medesimo.

Ai sensi delle lettere (A) e ss., i diritti di *consumer disclosure* rispetto al *credit score* (anche interamente automatizzato), contemplano, preliminarmente, un'informazione circa la circostanza che il *credit scoring model* utilizzato potrebbe differire dal punteggio effettivamente calcolato e successivamente utilizzato da uno *user*, per adottare una decisione nei confronti dell'interessato. Ciò premesso, l'interessato ha allora il diritto di ottenere le seguenti informazioni (in senso proprio, la *disclosure*): il *credit score* attualmente assegnato al richiedente nonché il più recente tra quelli precedentemente calcolati dall'agenzia

¹¹²⁴ 15 U.S.C. § 1681g, lett. (f).

¹¹²⁵ Ivi, n. (8).

per scopi collegati alla concessione di un prestito o di un finanziamento; l'intervallo dei valori minimi e massimi in cui oscilla il modello di *credit scoring*; i fattori principali («*key factors*»¹¹²⁶) che hanno inciso negativamente sul proprio punteggio, puntualizzandosi che «*the total number of which shall not exceed 4*»; la data in cui il *credit score* medesimo sia stato elaborato; e, “*last but not least*”, l'identità del soggetto che abbia fornito il *credit score* o il *credit file* sul quale poi la CRA abbia basato l'elaborazione del *credit score* in questione¹¹²⁷.

Occorre dedicare alcuni cenni più specifici alle disposizioni da ultimo esaminate, in quanto, come detto, centrali nella comparazione dell'adeguatezza del sistema di garanzie di cui all'FCRA applicabile *anche* al *credit scoring*, rispetto a quello edificato dal GDPR. E a tal riguardo, in primo luogo, è necessario notare come, in forza del n. (7) del paragrafo in esame, nell'uniformarsi ai doveri di informativa suddetti, l'obbligo di *consumer disclosure* risulti in realtà essenzialmente circoscritto al primo tipo sopra richiamato di *credit scores*, ossia i *credit-risk scores*, e in particolare a quelli impiegati per compiere previsioni sull'attuale o potenzialmente futuro *credit behavior* dei clienti degli *end-users* del “punteggio” medesimo e dagli stessi per erogare prestiti¹¹²⁸. Ebbene, ciò in primo luogo implica, *a contrario*, che le CRAs dispongano di un margine assolutamente ampio di libertà nello svolgere attività di *credit scoring*, potendo i modelli predittivi da questi elaborati consistere in “*educational scores*”, che come è stato notato sono ormai impiegati anche per scopi diversi dalla concessione di prestiti

¹¹²⁶ Ai sensi del § 1681g (f)(2)(B), per *key factors* si intendono «*all relevant elements or reasons adversely affecting the credit score for the particular individual, listed in the order of their importance based on their effect on the credit score*».

¹¹²⁷ 15 U.S.C. § 1681g, lett. (f), n. (1), lett. (A)-(E).

¹¹²⁸ Ivi., n. 7, lett. (a), che nel richiedere la compliance alle norme suddette delle CRAs dispone che esse «*shall supply the consumer with a credit score that is derived from a credit scoring model that is widely distributed to users by that consumer reporting agency in connection with residential real property loans or with a credit score that assists the consumer in understanding the credit scoring assessment of the credit behavior of the consumer and predictions about the future credit behavior of the consumer*».

e di finanziamenti, o piuttosto del c.d. “*VantageScore*”, sviluppato dalla joint venture delle note CRAs Equifax, Experian e TransUnion per competere con i modelli di *scoring* più diffusi, elaborati dalla FICO, azienda leader nel settore¹¹²⁹. In secondo luogo, e ciò è ancora più rilevante ai nostri fini, la norma suddetta limita considerevolmente il diritto di *disclosure* dell’interessato, non avendo al contrario le CRAs l’obbligo di informare il consumer circa l’elaborazione e quindi l’esistenza di altri tipi di *credit scores*, come gli *speciality* sopra richiamati e largamente impiegati nei più disparati ambiti, tra i quali quello assicurativo e lavorativo¹¹³⁰. La limitazione è ulteriormente aggravata dall’esplicita esclusione dal diritto in parola dei c.d. *mortgage scores*, ai sensi del n. (2) della lett. (f) del par. in esame: tale formula indica quei punteggi di merito elaborati nell’ambito di sistemi automatizzati di sottoscrizione di mutui ipotecari (c.d. *underwriting systems*) che ai fini della definizione del profilo, e conseguentemente del calcolo dello *score* su cui si baserà la decisione finale in punto di erogazione del mutuo, prendono in considerazione fattori ulteriori, per molti versi più “sensibili”, rispetto alle informazioni creditizie¹¹³¹.

¹¹²⁹ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit, p. 65, che ai fini di una più precipua analisi tra i modelli di credit score implementabili rinvia a CFBP, *Analysis of Differences between Consumer- and Creditor-Purchased Credit Scores*, September 2012, disponibile su https://files.consumerfinance.gov/f/201209_Analysis_Differences_Consumer_Credit.pdf. Sul modello brevettato dalla suddetta joint venture, VantageScore, cfr. invece CFPB, *The impact of differences between consumer- and creditor-purchased credit scores*, July 2011, p. 7. Experian, sul proprio sito ufficiale, lo definisce come «the most consistent, predictive and accurate measure of consumer creditworthiness in the market and utilizes an easy to understand grading scale that takes the mystery out of credit scores for consumers»: v. <https://www.experian.com/consumer-products/vantage-score.html>.

¹¹³⁰ *Ibidem*. Sul punto cfr. poi analiticamente NATIONAL CONSUMER LAW CENTER, *Fair Credit Reporting* § 16.4.1.4 (9th ed. 2017)

¹¹³¹ 15 U.S.C.A. § 1681g (f) (2) (A), che al n.(ii) afferma come nella definizione di credit score rilevante ai fini del sub-sistema normativo in questione non ricada «*any mortgage score or rating of an automated underwriting system that considers one or more factors in addition to credit information, including the loan to value ratio, the amount of down payment, or the*

Ebbene, come rileva lo stesso Studio promosso dalla Commissione Europea, le difficoltà che risultano dal tale articolato sistema, e che rendono le garanzie predisposte a favore dell'interessato invero non sovrapponibili, almeno in relazione al *credit scoring*, a quelle che sia possibile ricostruire alla luce del GDPR, risiedono nel fatto che, sebbene l'interessato possa alla luce delle informazioni «*disclosed*» a suo favore acquisire una «*more detailed yet general*» conoscenza del modo in cui un determinato modello di *scoring* (purché riconducibile alle specie suddette) inquadri *prognosticamente* le sue attitudini e i suoi potenziali comportamenti, e del contesto (*report, origin, recipient*) in cui sia venuto ad essere, l'interessato non può sapere se esso rappresenti in definitiva l'*unico* modello, o comunque un modello *simile*, a quello dall'*end-user* utilizzato per adottare una decisione incidente sulla sua sfera giuridica (dalla concessione di un prestito all'accoglimento della sua *job application*)¹¹³². E la situazione non cambia nemmeno valorizzando i doveri educativi rispetto al personale in capo alle CRAs esplicitamente sanciti dall'FCRA, che abbiamo brevemente esaminato sopra, strumentali a consentire al *trained personal* di spiegare le informazioni cui gli interessati hanno diritto di accedere. La limitata possibilità di *disclosure*

financial assets of a consumer», così come «*any other elements of the underwriting process or underwriting decision*». Appare importante sottolineare come, secondo lo Studio della Commissione cui facciamo frequente rinvio, «*Automated underwriting is a blanket term that generally applies to the process of creating a mortgage rating and issuing an approval or denial decision for a borrower based on her credit score (traditionally the FICO score) as well as her ability to carry debt and a collateral assessment using a statistical appraisal of property*». Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 68, che per una più approfondita analisi rinviano a WAYNE PASSMORE AND ROGER SPARKS, *The Effect of Automated Underwriting on the Profitability of Mortgage Securitization* (Draft, April 8, 1997), at 4, available at SSRN: <https://ssrn.com/abstract=36643> or <http://dx.doi.org/10.2139/ssrn.36643>.

¹¹³² G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 65.

appena rilevata determina infatti che tali spiegazioni siano al più utili al consumatore per determinare la propria *futura condotta*, al fine di ottenere un miglior punteggio, e non già per “reagire” consapevolmente al precedente calcolo automatizzato del suo *credit score* e alla decisione adottata dall’*end-user* sulla sua base¹¹³³.

Il panorama normativo delineato, quanto meno in relazione alla assai rilevante fattispecie del *credit scoring*, rende ardua una valutazione positiva circa l’esatta corrispondenza del regime di garanzie, in punto di *explanation* o comunque *explanability*, predisposto dall’FCRA in materia rispetto a quello delineato dal subsistema normativo di cui agli art. 22 e 13-15 del GDPR¹¹³⁴. A ciò concorre certamente la mancata differenziazione della disciplina a seconda della natura interamente automatizzata o meno del processo che coinvolge il *credit*

¹¹³³ *Ibidem*. Il diritto di *disclosure* che pare scaturire dal sistema così ricostruito sembra presentare delle analogie con l’interpretazione del disposto degli artt. 13-15 in punto di processi decisionali interamente automatizzati prospettata da quella parte della dottrina che ritiene desumibile dal GDPR un c.d. *right to counterfactual explanation*, di cui ci siamo brevemente occupati nel cap. 3, par. 2.3.: cfr. SANDRA WACHTER, BRENT MITTELSTADT, CHRIS RUSSELL, «Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR», in *Harvard Journal of Law & Technology*, 31 (2), 2018. Disponibile su SSRN: <https://ssrn.com/abstract=3063289> or <http://dx.doi.org/10.2139/ssrn.3063289>, 4. Cfr. anche sul punto le interessanti considerazioni di C. TABARRINI, *La trasparenza algoritmica*, cit., p. 207 ss.

¹¹³⁴ Lo stesso deve in sostanza affermarsi anche per quella subspecie di *credit scoring* relativa a *certain mortgage lenders*, e dunque ai fini della valutazione di richieste di mutui o aperture di linee di credito garantite da ipoteche sugli immobili (c.d. *home loans*), anche attraverso gli automatizzati underwriting systems già incontrati. Rispetto alla fattispecie in parola, infatti, nello specifico l’FCRA al § 1681g (g) predispone un autonomo sub-regime di consumer disclosure: tuttavia, sebbene il n. (1) configuri un dovere di comunicare (oltre alle informazioni già analizzate, di cui alla lettera f)) lo *specifico credit scoring* utilizzato, dall’altra la distanza del regime di cui al GDPR è ribadita dai numeri successivi, che limitano le informazioni sul punto ai *key factors* che abbiano influenzato l’elaborazione dello score, e non impongono uno specifico dovere di spiegazione di tali informazioni, autorizzando la CRA (n. (1), lett. (C)) ad emettere esclusivamente un educational score, idoneo ad orientare, come detto, il consumatore nei suoi futuri comportamenti al fine di ottenere un punteggio migliore. Per un approfondimento, cfr. ancora G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 68 ss.

scoring ed (eventualmente) la decisione dell'*end-user*. In ogni caso, per quanto comunque idonei ad offrire una certa protezione all'interesse all'autodeterminazione informativa dell'interessato, gli aspetti in cui si articola il *right to consumer disclosure* di quest'ultimo non può ritenersi sovrapponibile al diritto a ricevere informazioni significative (sull'esistenza del processo, sulla logica utilizzata, sulle conseguenze attese e sull'importanza della decisione medesima) derivante dall'art. 15, par. 1, lett. h) del GDPR; e stesso discorso vale per il corrispondente dovere del titolare del trattamento. Ciò appare ancora più evidente se, accedendo alla lettura promossa dalla CGUE nella sentenza *SCHUFA*, si identifica già lo stesso calcolo del punteggio di merito creditizio, e dunque dello *score*, dove risultante da un processo privo di coinvolgimento umano effettivo, *di per sé* una decisione basata interamente su un trattamento automatizzato incidente in modo significativo sulla sfera giuridica dell'interessato.

Possiamo solo notare, sul punto, che a livello ulteriormente settoriale un effettivo dovere, e corrispondente diritto, alla spiegazione della decisione (*eventualmente* basata su un *credit score* automatizzato) di erogare o meno un prestito, e dunque quanto meno a fornire informazioni realmente significative sull'intero *background* da cui la medesima origine, risulta attribuito all'interessato sotto l'egida dell'*Equal Credit Opportunity Act*, sul quale ci soffermeremo a breve.

Ad ogni modo, è possibile desumere dallo stesso FCRA diritti, o comunque garanzie, più simili a quelle previste dal GDPR in relazione alla fattispecie delle c.d. *adverse actions*: fattispecie la disciplina della quale attiene principalmente alla seconda categoria di soggetti ricadenti nell'ambito di applicazione *ratione personae* della normativa, ossia quella dei c.d. *users*. Veniamo ad indagare

brevemente tale profilo (sub-regime normativo, intrecciato com'è naturale a quello previsto in materia di *credit scoring*).

L'FCRA, innanzitutto, al par.1681a, lett. (k), non delinea una definizione generale e onnicomprensiva di *adverse action*, bensì assume un approccio anche in questo caso *sector specific*, pertanto individuando un certo ventaglio di situazioni tipo a seconda del settore materiale considerato: a titolo di esempio, per *adverse action*, con riferimento al settore assicurativo, s'intende «*a denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance*»; mentre in ambito lavorativo un'*adverse action* si riscontra in «*a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee*»¹¹³⁵. La disposizione prevede, in ogni caso, al n. (iv), (II), una clausola generale che estende la definizione in parola a qualsiasi «*action taken or determination*» che sia «*adverse to the interests of the consumer*»¹¹³⁶.

Ebbene, una disciplina puntuale pare dettata dall'FCRA in relazione alle c.d. *adverse action notices* che per l'appunto si indirizzano, piuttosto che alle CRA, agli end-users degli scores dai primi predisposti: a predisporla è il § 1681m, rubricato «*Requirements on users of consumer reports*», che alla lett. (a) stabilisce

¹¹³⁵ V. 15 U.S.C.. § 1681a, lett. (k), n. (1).

¹¹³⁶ Lo Studio della Commissione Europea cui andiamo riferendoci porta degli esempi maggiormente concreti di cosa voglia dire, nei diversi settori produttivi che risultano interessati dalle norme dell'FCRA, un *adverse action*: oltre a quanto puntualmente recitato dalle norme citate, ad esempio nel settore creditizio si avrebbe *adverse action* sarebbe «*a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested*»; mentre in punto di *business transactions* si identifica in «*an action taken or determination that is made in connection with an application that was made by, or a transaction that was initiated by, any consumer*». Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit. p. 70.

(citiamo la rubrica) i «*Duties of users taking adverse actions on the basis of information contained in consumer reports*». Il contenuto dei doveri ivi articolati a carico dei soggetti in questione, e quindi quello dei corrispondenti diritti in capo ai *consumers*, appare già a prima vista più nutrito di quello che sostanzia i diritti e i doveri generici di cui alla lett. f), nonché di quelli specificamente previsti in materia di *credit scoring*. Se gli *users* adottano *decisioni sfavorevoli* alle condizioni suddette (ossia esclusivamente o anche parzialmente sulla base delle informazioni contenute in un *consumer report*), questi hanno il *dovere* di inviare (e gli interessati dunque il diritto di ricevere) una notifica orale, scritta o elettronica non solo circa *l'adverse action* intrapresa, bensì anche e soprattutto riguardante lo *specifico credit score* sul quale la decisione si sia in tutto o in parte fondata; parallelamente, sono tenuti a notificare il nominativo della CRA che abbia fornito il *credit report* o il menzionato *score*¹¹³⁷.

Sembrerebbe insomma configurarsi un diritto più vicino a quello che nel contesto del GDPR garantisce la pretesa ad ottenere informazioni significative sui diversi aspetti del processo che ha condotto alla decisione, e in particolare sulla logica utilizzata: inciso che, come sappiamo, anche laddove non sia da interpretarsi come base di un più ampio e garantistico e tuttavia assai controverso *right of explanation ex post* della decisione, nondimeno accedendo alla lettura del WP 29 dovrebbe garantire l'accesso a informazioni «sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione»¹¹³⁸. Cosa che, invero, la conoscenza del *credit score* specifico e attualmente seguito, nonché i fattori alla base del calcolo, consente almeno in parte¹¹³⁹.

¹¹³⁷ 15 U.S.C. § 1681m, lett. (a).

¹¹³⁸ Cfr. ancora una volta GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., p. 28 ss. V. *amplius retro*, cap. 3, par. 2.3.

¹¹³⁹ Lo sottolineano anche G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and*

E tuttavia, a limitare anche questa volta la portata dei doveri di *notice* e del diritto corrispondente (d'informazione, piuttosto che di spiegazione), è la lettera (B) del n. (3) del par. in esame, laddove questa espressamente impone allo *user taking adverse action* di inviare, parimenti alle altre notifiche, «*a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken*». Ciò vuol dire che, ancora una volta, la CRA (che la dichiarazione, in sostanza, solleva da ogni diretto coinvolgimento, e dunque responsabilità, in relazione alla decisione adottata dall'*end-user* pur sulla base dello *score* da questa predisposto) viene *esclusa dai doveri informativi di dettaglio* previsti dall'FCRA, a ciò conseguendo che essa, nei confronti dell'interessato, non sarà tenuta né ad illustrare, pur sinteticamente, il procedimento inferenziale concretamente seguito dal sistema (essenzialmente) algoritmico nell'elaborazione del profilo, né ad esplicitare il conseguente calcolo del punteggio "di merito"¹¹⁴⁰. Inoltre, come è stato notato, non sussiste nemmeno alcun esplicito «*requirement*» circa il fatto che il decisore sveli le ragioni dell'*adverse action* in sé e per sé: regime che, invece, sussiste nel quadro dei doveri di *adverse action notice* ai sensi dell'ECOA, su cui ci soffermeremo tra poco¹¹⁴¹.

Al contrario, nutriti e sufficientemente garantistici appaiono i diritti previsti dal n. (4) della lett. (a) del medesimo paragrafo in punto di *disclosure* (generale) e di *disputing* del *consumer report*: tra i doveri di notifica in capo al titolare del trattamento, infatti, le norme ivi collocate ascrivono anche quello di informare (con una *notice* orale scritta o elettronica) l'interessato che *entro 60 giorni* dalla

assessment of safeguards provided by U.S. law, cit., a p.71 «What is noteworthy about these requirements is that the consumer will receive the actual credit score used and the statutorily required factors for how the credit score was calculated».

¹¹⁴⁰ V. 15 U.S.C. § 1681m(a), n. (3), lett. (B).

¹¹⁴¹ G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, op. cit., p. 71. Vedi subito *infra*.

notifica esso possa richiedere ed ottenere una copia *gratuita* del *consumer report*, in suo possesso, che lo riguardi; e, contestualmente, di informarlo dell'esistenza del diritto di contestare (in inglese, precisamente, *to dispute*) nei confronti della CRA stessa che il report abbia emesso e fornito all'*end-user* l'accuratezza e la completezza del report (precisamente, «*of any information in a consumer report furnished by the agency*») ¹¹⁴². La posizione giuridica così delineata risulta ampiamente risonante rispetto tanto al diritto di accesso (non solo alle informazioni sul trattamento, quanto piuttosto agli input utilizzati per creare il profilo) quanto al conseguente diritto di rettifica previsti, rispettivamente, dagli art. 15 e 16 del GDPR.

Possiamo ricordare che parimenti più garantistico in termini di “*notice*” appare il regime previsto dall'FCRA in caso di *adverse actions* adottate nel contesto dei rapporti di lavoro - una definizione delle quali abbiamo già dato poc'anzi ai sensi del par. 1681a(k): in tal caso infatti, secondo una dominante interpretazione, per poter basare le proprie decisioni riguardanti il lavoratore su un *consumer report*, e pertanto richiedere ad una CRA la sua elaborazione e l'accesso al medesimo, l'*employee* è innanzitutto tenuto ad ottenere il consenso del primo; in secondo luogo, esso sarebbe soggetto a determinati doveri di *disclosure antecedenti* rispetto all'adozione della decisione medesima, tra i quali ricadrebbero quelli ad una breve descrizione della natura del *consumer report* e la richiesta scritta dell'autorizzazione stessa del lavoratore, parallelamente, dunque, all'avviso circa l'intenzione di adottare l'*adverse action* medesima ¹¹⁴³. A questi seguono, ovviamente, i doveri di *adverse action notification ex post* già esaminati.

¹¹⁴² V. 15 U.S.C. § 1681m(a), n. (4).

¹¹⁴³ V. 15 USC § 1681b(b)(3). Cfr. sul punto FTC, *Forty Years of Experience With the Fair Credit Reporting Act* (July 2011), p. 50; . BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., a p.73.

Le disposizioni configurerebbero dunque un regime di *disclosure* obbligatorio *ex ante* rispetto alla particolare decisione sfavorevole.

Concludiamo l'analisi del regime (anzi, sarebbe meglio dire, della miriade di sub-regimi) di *consumer disclosure* configurato dall'FCRA riscontrando che, sempre in punto di doveri di *adverse action notices*, ma soprattutto di corrispondenti diritti ad un'informazione completa e *significativa*, un parzialmente diverso regime è previsto laddove l'*adverse action* che abbia coinvolto il consumatore si sia basata su informazione ottenute da «*Third Parties Other than Consumer Credit Reporting Agencies*»: ipotesi contemplata dalla lett. (b) del paragrafo in esame, che riguarda ancor più nello specifico il caso in cui l'*adverse action* basata su tali informazioni consista nel rifiuto o nell'aumento dei “pesi” previsti per la concessione di un credito «*for personal, family or household purposes*»¹¹⁴⁴. Ebbene, in tal caso l'FCRA prevede che il “decisore” (*the user of such information*) debba informare il consumatore che quest'ultimo dispone del diritto di ottenere, dietro richiesta scritta che non pervenga oltre il termine di 60 giorni dalla conoscenza dell'*adverse action*, la “spiegazione” «*[of] the nature of the information upon which the action is based*», entro il termine di 30 giorni dalla ricezione della richiesta¹¹⁴⁵.

Per quanto opportuna, e sebbene la vaghezza concettuale del termine “natura” potrebbe consentire di ricomprendere nel suo alveo le ragioni della specifica decisione, recentemente l'FTC, in un suo recente *White Paper* sul generale funzionamento dell'FCRA nei suoi quarant'anni di vita, pare aver promosso un'interpretazione restrittiva, affermando che «*the creditor need to disclose only the nature of the information that led to the adverse action (e.g.,*

¹¹⁴⁴ Ivi, (b), n. (1).

¹¹⁴⁵ Ivi, (b), n. (2), in part. lett.(A)

history of late rent payments or bad checks) (...)»¹¹⁴⁶. Allo stesso tempo, non sussiste alcuna espressa disposizione che imponga al potenziale creditore di identificare specificamente (al pari di quanto previsto laddove l'informazione provenga dalle CRAs) i soggetti dai quali provengano le informazioni suddette, né tantomeno i criteri che abbiano condotto all'*adverse action* medesima¹¹⁴⁷.

Per questo motivo, la previsione in questione finisce per sovrapporsi a quella, come vedremo più garantistica, che più puntualmente definisce il dovere di *adverse action notice* in capo al creditore prevista dall'ECOA. E proprio di quest'ultimo atto passiamo, di seguito, ad occuparci.

Abbiamo già anticipato che per alcuni aspetti l'*Equal Credit Opportunity Act* (ECOA) configura nella materia specifica che esso disciplina un regime di garanzie, in termini di doveri di "informazione significativa" e, come vedremo, di intervento umano a fronte di processi decisionali automatizzati, relativamente più approfondito rispetto all'FCRA.

Adottato nel 1974 al fine di rimuovere gli ostacoli emersi nella concessione di finanziamenti a clienti di sesso femminile, la riforma del 1976 ne ha ampliato la portata antidiscriminatoria, sempre in materia di credito: l'attuale § 1691 (a) del Titolo XV del Codice degli Stati Uniti dispone infatti che «*it shall be unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction (1) on the basis of race, color, religion, national origin, sex or marital status, or age (provided the applicant has the capacity to contract); (2) because all or part of the applicant's income derives from any public assistance*

¹¹⁴⁶ Cfr. FTC, *Forty Years of Experience With the Fair Credit Reporting Act* (July 2011), at 86.

¹¹⁴⁷ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit. p. 71.

*program; or (3) because the applicant has in good faith exercised any right under this chapter»*¹¹⁴⁸.

Bisogna subito specificare che l'ECOA è considerato un'*equal protection law*, ovverosia un'espressione di quella serie di atti normativi che, seppur *sector-specific*, perseguono una comune finalità antidiscriminatoria¹¹⁴⁹. Esso, proprio per tale portata generale, costituisce uno *statute* relativamente breve, se comparato all'FCRA. Tuttavia, le disposizioni di principio ivi previste sono state specificate ed integrate a livello di dettaglio dalle normative secondarie, e quindi dalle *regulations*, adottate dalle Agenzie preposte all'implementazione dell'impianto normativo definito dall'atto: queste sono oggi raggruppate nella c.d. *Regulation B*, alla predisposizione, all'aggiornamento e all'interpretazione della quale è oggi preposto il *Consumer Financial Protection Bureau* (CFPB)¹¹⁵⁰.

La prima differenza di ordine tecnico con l'FCRA attiene al suo ambito di applicazione soggettivo: a differenza di questo, che individua come categorie di soggetti destinatarie della disciplina, oltre alle CRAs, i *consumers*, gli *users* e i *furnishers*, l'ECOA più semplicemente disciplina le *credit transactions* tra *applicants* (ovvero «*any person who applies to a creditor directly for an extension, renewal, or continuation of credit, or applies to a creditor indirectly by use of an existing credit plan for an amount exceeding a previously established credit limit*») e *creditors* (ovvero «*any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal,*

¹¹⁴⁸ V. 15 U. S. C., § 1691 (a).

¹¹⁴⁹ Sul punto cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law, cit.*, p. 86. Le altre *equal protection laws* nei settori in cui si ritiene maggiormente diffuso l'impiego di *ADM systems*, e la relativa disciplina di tale fenomeno nel loro contesto, costituirà oggetto del successivo sottoparagrafo.

¹¹⁵⁰ V. 12 C.F.R. part 1002.

or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit»)¹¹⁵¹.

Venendo sinteticamente al contenuto della disciplina generale prevista dallo *statute*, secondo parte della dottrina, valorizzando anche il disposto della lett. b) ss. del par. 1691, da cui traspare la *ratio* dello *statute*, al fine di provare l'attitudine discriminatoria della condotta come circoscritta dalle norme in parola, l'*applicant* dovrebbe dimostrare, alternativamente: di aver subito un trattamento diverso a fronte di una "situazione analoga", rispetto ad un *tertium comparationis*, in virtù di quegli aspetti della propria persona ricostruiti dalla normativa medesima (c.d. *disparate treatment*); ovvero di essere stato sottoposto a «pratiche commerciali apparentemente neutrali» ma che producono un «*disproportionate adverse effect*» (è il caso del c.d. *disparate impact*). Tale seconda, più coraggiosa ricostruzione ermeneutica beneficia in realtà di un orientamento già espresso dalla *Supreme Court* prima dell'entrata in vigore dell'ECOA, nel caso *Griggs v. Duke Power*, e, contemplando essenzialmente l'ipotesi di *discriminazione indiretta*, consente di estendere considerevolmente la portata applicativa dell'ECOA¹¹⁵².

Arrivati a questo punto della trattazione, risulterà tuttavia ormai chiaro come la questione della portata discriminatoria delle operazioni svolte a partire dalle informazioni riguardanti una persona (*provided* o anche solo *inferred*) si sia oggi oltremodo complicata, a fronte degli ormai noti fenomeni dei *Big Data* e

¹¹⁵¹ V. 15 U.S.C. § 1691a(b) ed (e)

¹¹⁵² Cfr. sul punto la sintetica ma efficace ricognizione storica di C. TABARRINI, *La trasparenza algoritmica*, cit., p. 210 ss., che in relazione alla dottrina del *disparate impact* richiama V.A. HERTZA, «Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?», 93, *N.Y.U. L. Rev.*, 2018, 1707, 1724; O.C.A. JOHNSON, «The Agency Roots of Disparate Impact», 49, *Harvard Civil Rights-Civil Liberties Law Review*, 2014, 125, 140. Il precedente citato è *Griggs v. Duke Power Co.* 401 U.S. 424 (1971), la cui *ratio decidendi* è stata poco dopo ribadita da *McDonnell Douglas Corp. v. Green* 411 U.S. 792 (1973); seguito da numerose pronunce successive, quest'ultimo ha trovato recente conferma in *Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Cmty. Project, Inc.*, 135 S. Ct. 2507, 2518 (2015), riportato da A.D. SELBST, S. BAROCAS, «The Intuitive Appeal of Explainable Machines», in *Fordham Law Review*, 87, 2018, p. 1105.

della proliferazione di tecniche di *analytics* fondate su sistemi algoritmici che seguono percorsi inferenziali tanto più opachi quanto più diventano “efficienti”. Attitudine discriminatoria che, se non sulla sfera giuridica, certamente incide sulla dimensione relazionale dell’individuo, quando il fenomeno della *black-box* interessi la valutazione automatizzata del merito creditizio¹¹⁵³.

Occorre interrogarsi allora sulla capacità dell’ECOA, anche alla luce dell’estensiva interpretazione seguita dalle Corti sulla scorta del citato precedente, di governare il fenomeno in esame; e, anche in tal caso, sul livello di omogeneità della disciplina da questo dettata rispetto a quella del GDPR in punto di processi decisionali automatizzati.

Cominciamo subito col dire che, al pari dell’FCRA, l’ECOA prevede e articola specifici doveri informativi, e quindi di *disclosure*, in capo ai *creditors* a fronte di *adverse actions* da questi intraprese a scapito degli *applicants*. Tuttavia, il suo ambito di applicazione risulta più limitato rispetto all’FCRA, risultando coincidente con le sole decisioni sfavorevoli in punto di concessione di finanziamenti (e restandovi pertanto esclusi i dinieghi e le modifiche restrittive in ambito lavorativo, assicurativo o piuttosto di licenze governative, che ricadono così sotto l’ombrello del solo FCRA). Difatti, l’ECOA definisce *adverse action* «*a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested*» mentre non include «*a refusal to extend*

¹¹⁵³ V. ancora una volta *retro*, cap. 2, par. 3, e su tutti i fondamentali contributi di F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Shape Our Minds*, Harvard University Press, 2005; D.K. CITRON, F. PASQUALE, «The Scored Society: Due Process for Automated Predictions», in *Washington Law Review*, 2014, 89, 1 ss.; T. ZARSKY, «Understanding Discrimination in the Scored Society», in *Washington Law Review*, 2014, 89, 1375 ss.; e, sebbene già più volte citato nel presente paragrafo, V.A. HERTZA, «Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?», cit.

additional credit under an existing credit arrangement where the applicant is delinquent or otherwise in default, or where such additional credit would exceed a previously established credit limit»¹¹⁵⁴.

Nonostante tale più ristretto ambito di applicazione, sembrerebbe al contrario che l'ECOA preveda un regime di *discolosure requirements* più garantista rispetto a quello enucleato dall'FCRA, e pertanto più vicino a quello configurato dal GDPR, specialmente in punto di «*meaningful* [non solo *information*, bensì] *explanations*»¹¹⁵⁵. Difatti, laddove, come abbiamo visto, ai sensi dell'FCRA, e più nello specifico delle disposizioni sub par. 1681 lett. m), a fronte di un'*adverse action* gli *end-users* soggiacciono in sintesi al dovere di notificare i c.d. *key factors* che abbiano concorso all'elaborazione del *credit score*, laddove anche su di esso si sia basata la decisione, il regime previsto dall'ECOA prevedrebbe in capo al *creditor* anche (e qui risiede la differenza principale) il dovere di fornire (o illustrare) all'interessato *le specifiche ragioni alla base della singola decisione sfavorevole* adottata nei suoi confronti, in sé e per sé considerata¹¹⁵⁶.

¹¹⁵⁴ V. 15 USC § 1691(d)(6). La conclusione in parola si evince dallo stesso precedente *Treadway v. Gateway Chevrolet Oldsmobile Inc.*, 362 F.3d 971, 982 (7th Cir. 2004), laddove la Corte afferma che «*The FCRA defines adverse action' more broadly than does the ECOA*», rinviando a propria volta al precedente *Cannon v. Metro Ford*, 242 F.Supp.2d 1322, 1331-1332 (S.D. Fla.2002).

¹¹⁵⁵ È questa la tesi in definitiva accolta da G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 79 ss., che andiamo di seguito a ricostruire; una ricostruzione invero più problematica, in prospettiva di più ampio respiro, che intende piuttosto sottolineare la centralità, accanto alla prospettiva della *inscrutability* su cui le normative esistenti (FCRA, ECOA e GDPR comprese) parrebbero pressoché esclusivamente concentrarsi, della *nonintuitiveness* ai fini dell'effettiva idoneità della disciplina dell'*algorithmic decision making* a garantire la libertà di autodeterminazione informativa dell'individuo, offrono invece A.D. SELBST, S. BAROCAS, *The Intuitive Appeal of Explainable Machines*, in *Fordham Law Review*, cit., p. 1100 ss.

¹¹⁵⁶ *Ibidem*.

Il regime in parola risulta delineato dalla *Regulation B* della CFPB, poc'anzi citata, che specifica il contenuto delle *general provisions* dell'ECOA¹¹⁵⁷. Se da una parte, allora, non è previsto dallo *statute*, così come integrato a livello regolamentare, un diritto alla *disclosure* della logica generale del sistema (e dunque ad esempio, in un'ottica di comparazione con l'FCRA, del *credit report* a disposizione dell'*end-user*), dall'altra il sistema suddetto configura una serie di *notice requirements* in capo al *creditor* successivamente all'adozione della specifica decisione sfavorevole per l'*applicant*, l'atto apparendo dunque, come a breve sottolineeremo, permeato dall'intenzione di assicurare che «*when creditors make decisions they do not discriminate against applicants and they provide applicants with reasons for the actions they take*»¹¹⁵⁸.

Ai sensi del § 1002.9, lett. (a), n. (2) del Titolo 12 del *Code of Federal Regulations*, infatti, laddove un *creditor* (secondo la definizione puntualmente adottata dall'ECOA e già qui riportata) intraprenda un'*adverse action* nei confronti di un *applicant*, il primo soggiace al dovere di notificare, innanzitutto uno «*statement of the action taken*», nonché il proprio nome e il proprio indirizzo; poi, una dichiarazione che informi l'*applicant* circa le previsioni della Section 701(a) dell'ECOA¹¹⁵⁹; il nome dell'Agenzia Federale che garantisce la *compliance* dei creditori alle norme dell'ECOA; e, disposizione che qui rileva più di tutte, «*a statement of the specific reasons for the action taken*», o in alternativa la *disclosure* del diritto dell'*applicant* di ottenere la dichiarazione medesima entro

¹¹⁵⁷ V. da subito 12 C.F.R. § 1002.9(a)(2)

¹¹⁵⁸ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 81, che a tal proposito citano anche il Record del Congresso sulla legislazione che nel 1976 ha emendato l'ECOA, e sul quale a breve spenderemo qualche parola: S. Rep. No. 94-589 (1976),

¹¹⁵⁹ Si tratta della disposizione di apertura dell'ECOA, già citata, che prescrive il divieto di adottare condotte discriminatorie sulla base delle situazioni tipo ivi indicate.

30 giorni dalla sua richiesta, purché inviata al creditore entro 60 giorni dalla notifica¹¹⁶⁰.

Ebbene, il contenuto di quest'ultimo dovere, e del corrispondente diritto, parrebbe davvero avvicinarsi a quel controverso *right to explanation* della singola, decisione basta unicamente sul trattamento algoritmico di cui all'art. 22 par. 1 la cui configurabilità nel contesto del GDPR divide la dottrina, seppur ovviamente nel caso che ci occupa declinato in un ben più specifico settore materiale; o, quanto meno, a quel diritto ad informazioni significative che risulta dagli artt. 13-15 del GDPR. Bisogna aggiungere, tra l'altro, che sempre la *Regulation B* prescrive che lo *statement* in parola sia «*specific and indicate the principal reason(s) for the adverse action*», precisando poi che «*statements that the adverse action was based on the creditor's internal standards or policies or that the applicant (...) failed to achieve a qualifying score on the creditor's credit scoring system are insufficient*»¹¹⁶¹.

A rafforzare le garanzie in questione, e la lettura delle medesime in termini di diritto “alla spiegazione”, si aggiunge certamente il complesso articolato di *model forms* predisposti dall'Autorità preposte al *rulemaking* e al *law enforcement* in relazione all'ECOA, ossia, come già anticipato, il CFPB, di cui sono tenuti ad avvalersi i *creditors* al fine di adempiere puntualmente al proprio dovere di *disclosure* delle specifiche ragioni della loro *adverse action*: ai nostri fini, certamente i più importanti risultano i Form C-1, C-2 e C-3¹¹⁶². E se il C-1

¹¹⁶⁰ 12 C.F.R. § 1002.9(a)(2). Aggiunge, rispetto alla disclosure del diritto allo statement of specific reasons, il n. (ii) che «*The disclosure shall include the name, address, and telephone number of the person or office from which the statement of reasons can be obtained. If the creditor chooses to provide the reasons orally, the creditor shall also disclose the applicant's right to have them confirmed in writing within 30 days of receiving the applicant's written request for confirmation*».

¹¹⁶¹ 12 C.F.R. § 1002.9(b)(2).

¹¹⁶² V. nello specifico 12 CFR § 1002.9 Appendix C. Ricostruiscono l'articolazione dei formati standard di c.d. adverse notification, la loro ratio e la loro funzione anche A.D. SELBST, S. BAROCAS, «The Intuitive Appeal of Explainable Machines», cit., 1101.

presenta una lista di venti ragioni che il titolare del trattamento può contrassegnare (solo per fare alcuni esempi, «*Credit application incomplete*»; «*Insufficient number of credit references provided*»; «*Unacceptable type of credit references provided*»), il C-2 al contrario individua 4 macrocategorie («*income, employment, credit history, and application*») sotto alle quali sono articolate una serie di ragioni che il *creditor* può a sua volta “spuntare”¹¹⁶³. Ma il modello che qui certamente risulta più interessante fare riferimento è il Form C-3, che il *creditor* è tenuto ad usare quando la sua *adverse action* si basi *esclusivamente* su di un *credit score*. L’aver destinato uno specifico e separato Form a tale ipotesi sottolinea ancora una volta la consapevolezza (già allora) diffusa a livello istituzionale circa le forti potenzialità discriminatorie che le attività, ed oggi ancora più i sistemi automatizzati, di *credit scoring* sono idonei ad esprimere. Tanto che sul modo in cui i doveri di *disclosure* di cui al § 1002.9(a)(2) si declinano laddove sia per l’appunto impiegato un sistema di *credit scoring* nel quadro processo decisionale che abbia condotto all’*adverse action* dedica alcune pagine importanti nell’ambito della sua “interpretazione ufficiale” della *Regulation B* lo stesso CFPB, che prescrive come *tutte* le “*principal reasons*” della decisione sfavorevole debbano costituire oggetto di *disclosure*. Con le parole del Bureau, «*if a creditor bases the denial or other adverse action on a credit scoring system, the reasons disclosed must relate only to those factors actually scored in the system*», cosicché il creditore è tenuto a fornire «*the actual reasons for denial (for example, “age of automobile”) even if the relationship of that factor to predicting creditworthiness may not be clear to the applicant*»¹¹⁶⁴. Un inciso, quest’ultimo, che rileva proprio

¹¹⁶³ Entrambi tali modelli consentono poi di indicare se la decisione si sia basata anche su un *credit score* ottenuto da una CRA. Cfr. sul punto G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 82.

¹¹⁶⁴ Cfr. approfonditamente *Official Interpretations of Reg. B*, 12 CFR. pt. 1002, supp. I, § 1002.9(b)(2) paras. 4-5.

perché interpreta come connaturato al dovere di *disclosure* quello di esplicitare al destinatario i «*major factors that influenced the scores*»: le corrispondenze con il concetto di informazioni significative fatto proprio dal GDPR, come interpretato dal WP 29, non sono poche¹¹⁶⁵. Inoltre, sotto il profilo delle modalità attraverso cui adempiere al dovere in questione, il CFPB afferma che «*various methods will meet the requirements of the regulation*», individuando essenzialmente un metodo di tipo “selettivo” «*[which] focuses on the most salient information*», ed uno insieme «*selective and contrastive*» che aggiunge ulteriori informazioni «*allowing an applicant to understand their position among other candidates*»; per poi concludere che «*any other method that produces results substantially similar to either of these methods is also acceptable under the regulation*»¹¹⁶⁶.

L’ECOA sembrerebbe, insomma, configurare un diritto ad “ottenere una spiegazione” (o, comunque, quelle informazioni significative di cui discorre il GDPR), ed *ex post*, che, seppure limitatamente alle sole decisioni sfavorevoli assunte in ambito creditizio, parrebbe in linea generale con il sistema di garanzie previsto dal GDPR.

Sul punto, in qualsiasi caso, non può qui tacersi una maggior predisposizione dell’ECOA in sé e della sua normativa secondaria di attuazione a

¹¹⁶⁵ Di tale avviso sembrano, sostanzialmente, anche alla luce delle “Conclusioni” in punto di ECOA da cui la citazione è attinta, G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, op.cit., p. 84-85.

¹¹⁶⁶ *Official Interpretations of Reg. B*, 12 C.F.R.CFR. pt. 1002, supp. I, § 1002.9(b)(2) paras. 4-5. I principi in parola paiono almeno relativamente incorporati nel Form C-3, la cui prima sezione si esprime in tal modo, adottando un linguaggio semplice e chiaro (quasi coerentemente con le raccomandazioni che, in contesto europeo, rivolge ai Titolari del trattamento in punto di doveri di fornire informazioni significative il Gruppo di Lavoro Articolo 29 nelle Linee Guida esaminate): «*The information you provided in your application did not score a sufficient number of points for approval of the application. The reasons you did not score well compared with other applicants were: (1) insufficient bank references; (2) Type of occupation; (3) Insufficient credit experience; (4) Number of recent inquiries on credit bureau report*». V. 12 CFR § 1002.9 Appendix C.

presidiare l'interesse della persona fisica (sebbene concepita solo nella veste di soggetto di rapporti economici) ad autodeterminarsi nella gestione del proprio patrimonio informativo, attraverso la prescrizione di un dovere di trasparenza più significativo in relazione alla specifica, concreta determinazione del creditore, coerentemente con la natura antidiscriminatoria dell'atto. Tale soglia ulteriore di trasparenza può risultare molto utile proprio in relazione ai processi decisionali interamente algoritmici, assai diffusi nella *credit industry*, che più di tutti – strutturalmente - ne difettano, pur incidendo profondamente sugli interessi fondamentali del *data subject*. Il regime in parola garantisce al singolo di potersi meglio determinare anche in relazione ai rimedi, giudiziali o stragiudiziali, da attivare: nonostante la loro omogeneità rispetto a quelli dell'FCRA¹¹⁶⁷, in tale contesto, stante la minor asimmetria informativa, l'*applicant* sarà potenzialmente più consapevole dei presupposti della decisione da censurare al fine di ottenere una pronuncia favorevole, la maggior informazione riverberandosi positivamente sullo (e dunque rafforzando le garanzie dello) stesso *right to contest*¹¹⁶⁸.

Avviandoci alle conclusioni, bisogna rilevare tuttavia come la ricostruzione del regime di *adverse action disclosure* configurato dall'ECOA e dalla *Regulation B* in termini di analogia, seppur *sector specific*, con la disciplina di cui la subsistema normativo edificato dal GDPR in punto di processi decisionali

¹¹⁶⁷ Propone tale lettura NATIONAL CONSUMER LAW CENTER, *Credit Discrimination* § 11.8.1 (7th ed. 2018).

¹¹⁶⁸ Per quanto attiene al regime di responsabilità scaturente dalla violazione dei *disclosure requirements* in parola, v. 15 U.S.C. § 1691e(a) «[a]ny creditor who fails to comply with any requirement imposed [by the statute] shall be liable to the aggrieved applicant for any actual damages sustained by such applicant acting either in an individual capacity or as a member of a class.». Sul *right to contest*, cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 85, che riassume «Finally, the ECOA provides a right to contest by providing access to judicial procedures when the requirements of the statute have been violated».

interamente automatizzati (ed in particolare la corrispondenza tra «*statement of specific reasons*» e «informazioni significative») non sia inattaccabile.

In primo luogo, la ragione che storicamente informa la disciplina in questione, e dunque il dovere in capo ai *creditors* di comunicare le ragioni specifiche delle loro singole *adverse action*, parrebbe risiedere in una finalità educativa, di matrice quasi paternalistica. Come si evince infatti dal Record del Congresso che accompagna la normativa di emendamento dell'ECOA del 1976, a muovere il legislatore non sarebbe stata solo l'esigenza di introdurre un grado di trasparenza dei processi decisionali sufficiente a disincentivare condotte discriminatorie dei finanziatori; ma anche, ed anzi soprattutto, con le parole del Congresso, l'opinione che l'introduzione dei doveri di *disclosure* in questione avrebbero fatto sì che «*rejected credit applicants [would have] now be[en] able to learn where and how their credit status is deficient and this information should have [had] a pervasive and valuable educational benefit*»; in definitiva, «*the statement of reasons gives the applicant a chance to rectify the mistake*»¹¹⁶⁹. Tale primo rilievo risulta comunque superabile: la diversa e spesso anacronistica volontà storica sottesa ad un prodotto normativo non toglie che, alla luce di un'interpretazione evolutiva la quale (ancora una volta) valorizzi quella tendenza fondamentale che muove il diritto, tanto positivo quanto *vivente*, a reagire all'evoluzione incessante della tecnica, lo stesso dato letterale possa (ed anzi debba) essere interpretato in modo da costruire un sistema – anche settoriale - di garanzie che più efficacemente tuteli la libertà del singolo di autodeterminarsi nelle scelte significative relative alla propria esistenza.

Il secondo rilievo appare più difficile da superare. Accanto alle letture fiduciose che abbiamo richiamato, infatti, bisogna tuttavia riportare le voci che

¹¹⁶⁹ Cfr. S. Rep. No. 94-589 (1976), in part. punto 4.

rilevano, altrettanto lucidamente e in senso critico, come gli obblighi di *disclosure* inerenti ai motivi specifici dell'*adverse action* (in ipotesi, completamente automatizzata) in ambito finanziario previsti dall'ECOA, seppur analiticamente delineati, contemplino quale oggetto principale se non esclusivo *i soli fattori della decisione*, invero potenzialmente fungibili, e non piuttosto la descrizione del *rapporto eziologico* intercorrente tra gli stessi e la decisione, e dunque in senso proprio della *logica* del processo. Gli stessi modelli esplicativi attraverso i quali l'adempimento degli obblighi in parola dovrebbe realizzarsi si concentrano essenzialmente sulle *variabili*, ed è lo stesso CFPB che nell'interpretazione ufficiale sopra già citata sottolinea con fermezza come le *specific reasons* comunicate debbano comprendere tutti i c.d. *major keys* della decisione sfavorevole, anche laddove le relazioni logico-inferenziali tra premesse e conclusioni non siano chiare all'*applicant* che ne risulta il destinatario (problema che, come ormai sappiamo bene, connota strutturalmente i sistemi algoritmici e di IA, e dunque la “logica” che al loro funzionamento dovrebbe presiedere)¹¹⁷⁰. Allo stesso tempo, il fatto che il Form C-2 preveda solo quattro fattori suscettibili di contrassegno, se

¹¹⁷⁰ L'opinione è lucidamente espressa da C. TABARRINI, *La trasparenza algoritmica*, cit., p. 214 ss., che a suffragio delle cautele da essa avanzate nel riconoscere al regime di *adverse action disclosure* dell'ECOA uno standard di tutela pari a quello del GDPR, rinvia alla già citata ricostruzione di A.D. SELBST, S. BAROCAS, «The Intuitive Appeal of Explainable Machines», cit., 1096; e nell'evidenziare come il principale limite (sul quale tante volte ci siamo già soffermati), autenticamente lesivo della libertà di autodeterminazione informativa degli interessati, riguardante i processi decisionali automatizzati sia quello dell'opacità che circonda la “logica algoritmica”, e dunque i rapporti di causa effetto tra input di cui il sistema algoritmico dispone e decisioni prodotte, rinvia a Y. BATHAEE, «The Artificial Intelligence Black Box and the Failure of Intent and Causation», 31, *Harv. J.L. & Tech.*, 2018, 889ss. Noi, sul punto, rinviando ancora a E. PELLECCIA, «Profilazione e decisioni automatizzate al tempo della Black Box society», cit.; R. MESSINETTI, «Privacy e controllo dell'identità algoritmica», cit.; J. BURRELL, «How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms», in *Big Data & Soc'y*, Jan.–June 2016, 1ss; J. A. KROLL, J. HUEY, S. BAROCAS, E. W. FELTEN, J. R. REIDENBERG, D. G. ROBINSON & H. YU, «Accountable Algorithms», 165 *Un. Pennsylvania L. R.*, 633ss. (2017). Per un ritratto più approfondito del fenomeno della *black-box* e delle sue ripercussioni sulle libertà fondamentali dei *data subject*, v. di nuovo *amplius* la panoramica sul contesto “tecnosociale” svolta nel cap. 2, par. 3.

da una parte ha alla base l'intenzione virtuosa di contenere l'altrettanto diffuso problema dell'*overinformation*, dall'altra, come è stato notato, non garantirebbe affatto la maggior intellegibilità del processo e della decisione che ne scaturisce ogni qualvolta questo risulti complesso, stante il carattere semplificato della descrizione "vincolata" dal form¹¹⁷¹.

E allora, secondo la ricostruzione che andiamo illustrando, quando a fronte di processi interamente automatizzati la "spiegazione" delle *specific reasons* dell'*adverse action* consista in una semplice descrizione dei soli fattori che si sono rivelati rilevanti ai fini della decisione (c.d. *outcome-based explanation*), e non anche del peso relativo da ciascuno di essi esercitato sulla stessa (c.d. *logic-based explanation*), il regime disegnato parrebbe *non* rispecchiare i diritti di cui agli art. 13-15 e 22 del GDPR, non integrando in primis il requisito della "significatività" dell'informazione¹¹⁷².

La prospettiva appena richiamata ci ricorda come il problema dell'intellegibilità del processo decisionale, alle radici viziata nel contesto di sistemi algoritmici, e ancor più di ML e di DL che apprendono dall'esterno ed elaborano la regola di giudizio senza pattern predefiniti, non sia risolto dalla mera informazione sulla relazione statistica tra input e output. L'unica *disclosure* potenzialmente risolutiva sarebbe quella di esplicitare la relazione causale tra i due termini, e in questo senso i criteri che presiedono alle inferenze che dentro la "scatola [non più] nera" della macchina abbiano preso forma.

¹¹⁷¹ C. TABARRINI, *La trasparenza algoritmica*, cit., p. 214 ss.; A.D. SELBST, S. BAROCAS, «The Intuitive Appeal of Explainable Machines», cit., 1104 e 1115. Cfr. A. DATTA, S. SEN, Y. ZICK, «Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems», in *Proceedings of the 2016 IEEE Symposium on Security & Privacy*, p. 598 ss.;

¹¹⁷² A.D. SELBST, S. BAROCAS, «The Intuitive Appeal of Explainable Machines», cit., 1099-1100.

Venendo ad un bilancio generale dei due *sector-specific statutes* in materia di *credit reporting system* e di discriminazione finanziaria analizzati nel presente paragrafo, entrambi, pur non distinguendo tra operazioni di *data processing* e di *decision making* che coinvolgano o piuttosto che escludano un essere umano dal *loop* algoritmico, presentano dei caratteri che riecheggiano alcune delle garanzie previste dal sub-sistema del GDPR dedicato agli ADM. Il maggior livello di specificità dei doveri di *disclosure post adverse action* enucleati dall'ECOA rispetto al sistema che risulta dall'FCRA (livello di specificità che a propria volta come abbiamo visto potenzia il *right to relevant information* e il *right to dispute*) va di certo valutato positivamente in quest'ottica. Tuttavia, si nota, la contenuta estensione dell'ambito di applicazione tanto soggettivo quanto oggettivo che caratterizza tanto l'FCRA quanto l'ECOA rende facilmente aggirabile la normativa, e dunque sviscerisce l'effettività del sistema di garanzie -anche laddove si ritenessero simili a quelle del GDPR- di cui possano avvalersi gli interessati a fronte dell'impiego di (*solely* o *human involved*) ADM systems nei settori considerati¹¹⁷³.

¹¹⁷³ Cfr. ancora V.A. HERTZA, «Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?», 93, *N.Y.U. L. Rev.*, 2018, 1707, 1729, che rileva come nel contesto *Big Data*, caratterizzato dall'atipicità e dalla varietà dei dati, nonché dei modelli di *business emergent*, ad aggirare il sistema predisposto da tali *statutes* ed esulare dal loro perimetro applicativo sarebbe sufficiente che il finanziatore concentri su di sé tanto il ruolo di *credit reporter* e di *credit scorer* quanto quello di *end-user*, raccogliendo e trattando i dati a scopo operativo in autonomia. Incidentalmente, si può richiamare anche il rilievo svolto da C. TABARRINI, *La trasparenza algoritmica*, cit. p. 214 ss. secondo cui a privare di effettività il sistema di garanzie in questione o comunque a renderlo non assimilabile a quello del GDPR sarebbe anche una ragione di ordine strutturale, ovvero il fatto che parte della dottrina statunitense escluderebbe dalla nozione di dato personale (e dunque, nei casi in commento, delle informazioni relative al *consumer* e all'*applicant*) proprio i dati che in contesto *Big Data* risultano più idonei a fornire, attraverso il *data mining*, informazioni sul singolo, ossia le informazioni che rendano solo indirettamente identificabile l'interessato, come l'indirizzo IP: la dottrina statunitense sarebbe incline, infatti, a qualificarli come *Non Personally Identifiable Information*. Cfr. per un riscontro J. BARRETT GLASGOW, «Data Brokers: Should They Be Reviled or Revered?», in E. Selinger, J. Polonetsky, O. Tene (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018, 26.

La questione resta, pertanto, controversa.

4.3.2. Discriminazione algoritmica ed *Equal Protection Laws*: in particolare, il Titolo VII del *Civil Rights Act* e il *Fair Housing Act*

Lasciamoci alle spalle il settore della *credit industry*, in senso lato, per indagare l'esistenza di regimi analoghi a quello edificato dal GDPR in materia di processi decisionali automatizzati nel quadro di altri settori essenziali della vita di relazione - in cui come anticipato - maggiore appaia la diffusione, o comunque la portata "*decettiva*", dei primi.

Ad orientarci nella ricerca dei settori, e conseguentemente delle normative, di cui sopra, è ancora una volta la consapevolezza dell'attitudine discriminatoria insita nella sostanziale imperscrutabilità del processo algoritmico. In proposito, non ci sorprenderà che anche in contesto statunitense ci si sia attentamente interrogati sulla ormai nota idoneità degli algoritmi e delle tecnologie ricadenti nella generale categoria dei *Big Data analytics* di far sì che i processi medesimi «*reproduce existing patterns of discrimination, inherit the prejudice of prior decision makers, or simply reflect the widespread biases that persist in society*»¹¹⁷⁴. Si è, tra l'altro, affermato che «*because human beings program predictive algorithms, their biases and values are embedded into the software's instructions*»¹¹⁷⁵. Ancora più emblematica in questo senso appare la recente attenzione, già denunciata, che ha coinvolto le stesse istituzioni federali, e che ha condotto al recente *White Paper* della Casa Bianca (simile al Libro Bianco, già

¹¹⁷⁴ Cfr. S. BAROCAS, A. SELBST, «Big Data's Disparate Impact», 104 *California Law Review* 671, 673 (2016). V. *retro* per una più approfondita disamina, cap. 2, par. 3 e cap. 3, par. 2 ss.

¹¹⁷⁵ Cfr. DANIELLE KEATS CITRON, FRANK PASQUALE, «The Scored Society: Due Process for Automated Predictions», 89 *Wash. L. Rev.* 1, 4 (2014)

menzionato, emerso in contesto europeo) in cui la proposta di una dichiarazione, quanto meno politica, sui principi fondamentali che informino i sistemi di Intelligenza Artificiale affinché questi lavorino «*for the people*» viene introdotta, tra l'altro, dalla considerazione che «*in America and around the world, systems supposed to help with patient care have proven unsafe, ineffective, or biased. Algorithms used in hiring and credit decisions have been found to reflect and reproduce existing unwanted inequities or embed new harmful bias and discrimination. Unchecked social media data collection has been used to threaten people's opportunities, undermine their privacy, or pervasively track their activity—often without their knowledge or consent*»¹¹⁷⁶.

Di fronte a questo scenario, che ormai ci è ben noto, in contesto statunitense è parallelamente cresciuto l'interesse per quelle normative che abbiamo definito ricadenti nella composita categoria delle *equal protection laws*, unificate dalla comune finalità di vietare qualsiasi tipo di discriminazione sulla base di determinate caratteristiche (*features*) legalmente protette, quali l'etnia, il genere, l'orientamento sessuale e l'età¹¹⁷⁷. Abbiamo già rilevato poc'anzi, introducendo l'ECOA (generalmente ricompreso nella categoria in esame), come tali normative siano per la maggior parte settoriali; dobbiamo qui aggiungere che, stante il loro

¹¹⁷⁶ V. WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY, *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the People*, ottobre 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>

¹¹⁷⁷ Lo rileva lo stesso G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 86. Operando qui una sintetica ricognizione delle normative in questione, le più importanti, divise per settore, sono le seguenti: in ambito lavorativo, il Titolo VII del *Civil Rights Act* e l'*Age Discrimination in Employment Act*, cui si aggiunge il *The Genetic Information Nondiscrimination Act*; nel settore del mercato degli "alloggi", il *Fair Housing Act*; in ambito sanitario, ma con più limitato riferimento al trattamento dei dati sanitari per scopi assicurativi, *Health Insurance Portability and Accountability Act* (HIPAA); in punto di contrasto alle fattispecie di discriminazione (settorialmente, invero, trasversale, per motivi di disabilità, l'*Americans with Disabilities Act* (ADA).

carattere generale, esse non contengono alcuna disposizione esplicitamente dedicata alla dimensione dell'automazione, men che meno (risalendo la più gran parte di queste alla seconda metà del secolo scorso) ai sistemi algoritmici. E tuttavia, considerata la profonda incidenza che la diffusione dell'automazione nei settori da queste coperte produce sulle libertà fondamentali dei singoli, e valorizzandosi ancora una volta l'attitudine evolutiva dell'esperienza giuridica statunitense¹¹⁷⁸, proprio il carattere generale delle loro disposizioni parrebbe consentirgli di rispondere, attraverso l'inesausta attività di mediazione tra principi generali e cangiante realtà storica compiuta dal formante dottrinale e giurisprudenziale, alle nuove fattispecie discriminatorie emergenti nella società degli algoritmi. Ed è infatti proprio con l'estensione della copertura offerta dalle disposizioni che andremo ad esaminare ai pregiudizi cagionati da tali fattispecie che la dottrina e la giurisprudenza si sono sempre più confrontate, anche attraverso l'elaborazione di originali proposte interpretative¹¹⁷⁹. Nel loro quadro, ugualmente a quanto accaduto con l'FCRA e l'ECOA, la nostra attenzione non potrà che focalizzarsi sulla possibilità di desumerne un regime normativo simile a quello disegnato dal GDPR.

Stante il carattere *sector-specific* delle *equal protection laws*, per individuare quelle da sottoporre alla nostra analisi è prima necessario individuare i settori ai quali circoscrivere la nostra attenzione. I criteri da noi seguiti sono essenzialmente due, già accennati, e tra loro cumulati: ovvero, insieme, la crescente automatizzazione delle pratiche, dei processi decisionali e in definitiva degli stessi rapporti in cui si articolano i settori medesimi; e il *sensitive impact* (il

¹¹⁷⁸ V. *retro*, cap. 1, par. 1.3.

¹¹⁷⁹ Cfr. soprattutto, e.g., S. BAROCAS, A. SELBST, «Big Data's Disparate Impact», 104 *California Law Review* 671, 673 (2016); PAULINE KIM, «Data-Driven Discrimination at Work», 58 *Wm. & Mary L. Rev.* 857, 861-62 (2017).

carattere particolarmente pregiudizievole) delle discriminazioni originate dal trattamento e ancor più dal processo decisionale algoritmico sugli individui, stante il rilievo anche costituzionale degli interessi coinvolti.

Il primo tra i settori che meritano attenzione è sicuramente quello dei rapporti di lavoro, in cui pressoché pacifica, oltre che ampiamente documentata, risulta la crescente automazione dei trattamenti e delle stesse decisioni su questi fondate. Si rileva infatti come ormai la tecnologia algoritmica sia impiegata in molteplici vesti, dalla valutazione dei candidati alla videosorveglianza dei posti di lavoro, fino ad estendersi al monitoraggio dei comportamenti dei dipendenti fuori dall'orario di lavoro¹¹⁸⁰. Con evidenti, inevitabili rischi di sorveglianza continuativa e, pertanto, di discriminazioni sulla base di dati sensibili. Nell'ambito in questione, al precipuo scopo di fronteggiare la discriminazione algoritmica (attraverso, lo ripetiamo, un'interpretazione essenzialmente evolutiva delle relative disposizioni), rilevante, seppur non pacificamente, è apparso soprattutto il *Title VII del Civil Rights Act*¹¹⁸¹.

Il secondo settore sul quale è opportuno soffermarsi è quello del mercato immobiliare: sebbene nel suo contesto, com'è stato rilevato, il fenomeno delle

¹¹⁸⁰ Cfr. ex multis PAULINE KIM, «Data-Driven Discrimination at Work», 58 *Wm. & Mary L. Rev.* 857, 861-62 (2017), in cui l'autrice rileva (p. 860) tra l'altro che « *Using highly granular data about workers' behavior both on and off the job, entrepreneurs are building models that they claim can predict future job performance*». Ben si ricorderà anche l'esempio portato dal Gruppo di Lavoro nelle linee guida esaminate, a dimostrazione della centralità del fenomeno dell'automazione in materia di *employment*: «In ragione del volume eccezionalmente elevato di candidature l'azienda potrebbe ritenere che non è possibile individuare i candidati idonei senza prima utilizzare mezzi unicamente automatizzati per scartare le candidature non pertinenti». V. ancora una volta GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., p. 26.

¹¹⁸¹ V. da subito 42 USC § 2000 ss. Non altrettanto interesse è stato indirizzato all'Age Discrimination in Employment Act, (ADEA), 29 U.S.C. § 621 ss: cfr. sul punto G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., pp. 93-94.

decisioni unicamente basate su trattamenti automatizzati e la questione della loro attitudine discriminatoria non abbiano ancora ricevuto la stessa attenzione dedicata da dottrina e giurisprudenza al settore dell'*employment*, anche ivi si registrano alcune prassi che sollevano le problematiche di cui ci stiamo occupando: ci riferiamo, in particolare, alla traslazione nel contesto online del c.d. *housing steering*, anche su basi diverse rispetto a quella tradizionalmente rappresentate dal pregiudizio razziale, e quello dell'*housing advertisement*, sempre più demandato, al pari di qualsiasi altra specie di *targeting advertisement*, a sistemi algoritmici¹¹⁸². In tale contesto, a rilevare è certamente il *Fair Housing Act*, che offre un sistema di garanzie ai soggetti che siano stati discriminati sulle basi dall'atto indicate nel contesto delle c.d. *residential dwellings*¹¹⁸³.

Prima di addentrarci nell'analisi delle normative su richiamate, è necessario fare una premessa di sistema: ricollegandoci alle considerazioni già svolte nell'analisi dell'ECOIA, anch'esso qualificato pacificamente come *equal protection laws*, dobbiamo nuovamente sottolineare come il principale strumento di protezione offerto dai soggetti che lamentino l'adozione ai loro danni di una condotta discriminatoria in violazione dell'*equal protection laws* sia quello di dimostrare di esser stato soggetto ad un *disparate treatment* o ad un *disparate impact*. Quest'ultima fattispecie è stata enucleata dalla giurisprudenza

¹¹⁸² Ivi, p. 92 ss. Sulla segregazione residenziale, intesa come occupazione (se non giuridicamente, socialmente imposta) da parte di gruppi sociali, caratterizzati da determinati e omogenei parametri distintivi e identitari, di un determinato contesto spaziale, cfr. in generale THOMAS C. SCHELLING, «Models of segregation», in *American Economic Review*, vol. 59, n. 2, 1969, pp. 488–493; sulla sua traslazione online, cfr. TEKE WIGGIN, «Steering 2.0? Data may undermine fair housing laws», in *Inman News* (April 2014), available at <https://www.inman.com/2014/04/29/steering-2-0-data-may-undermine-fair-housing-laws/>. Sul fenomeno dell' "*Housing Advertisement*", nella sua chiave essenzialmente discriminatoria, cfr. l'importante contributo di R. C. OLIVIERI, «Discriminatory Housing Advertisements Online: Lessons from Craigslist», in *Indiana Law Review*, 42, 2010, pp. 1125- 2010, <https://mckinneylaw.iu.edu/ilr/pdf/vol43p1125.pdf> ,

¹¹⁸³ V. 42 USC § 3601 ss.

statunitense nel già richiamato caso *Griggs v. Duke Power* e che ricorrerebbe laddove «*a company employs facially neutral policies or practices that have a disproportionate adverse effect or impact on a protected class, unless those practices or policies further a legitimate business need that cannot reasonably be achieved by means that have less disparate an impact*»¹¹⁸⁴. Il rilievo, come subito vedremo, è importante, perché parte della dottrina ha escluso l'idoneità delle ricostruzioni dottrinali in esame - filtro indispensabile alla giurisprudenziale declinazione nei diversi casi di specie delle "generiche" disposizioni previste dalle normative in commento - a governare il fenomeno delle discriminazioni algoritmiche, e dunque la loro idoneità a configurare sistemi di garanzie analoghi a quelli previsti dal GDPR; e perché, conseguentemente, ha spinto alcuni autori ad indirizzare l'attenzione a diversi istituti¹¹⁸⁵.

Occupiamoci, in primo luogo, delle discriminazioni algoritmiche nel settore dei rapporti di lavoro. Occorre sottolineare come il Titolo VII del *Civil Rights Act*, adottato nel 1964, sia stato storicamente enucleato al fine di proibire qualsiasi condotta discriminatoria sul posto di lavoro basata sulla razza, sul colore, sulla religione, sul sesso e sulla nazionalità del dipendente¹¹⁸⁶. L'atto differenzia leggermente la disciplina a seconda della categoria di soggetti con i quali si

¹¹⁸⁴ La citazione è tratta da FEDERAL TRADE COMMISSION, «Big Data: A Tool for Inclusion or Exclusion? (January 2016)», p. 19. Sull'argomento si rinvia subito a p. 430 ss. della presente trattazione, e in part. a nota 1137.

¹¹⁸⁵ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., pp. 86-87.

¹¹⁸⁶ V. 42 USC § 2000e ss. In part., la lett. (a) definisce "employer": «*a person engaged in an industry affecting commerce who has fifteen or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person (...)*», escludendo poi tutta una serie di ipotesi in cui a figurare come tale risulti una pubblica amministrazione statunitense; e "employee" «*an individual employed by an employer (...)*»

confronti l'*individual* o l'*employee*, (essenzialmente le categorie sono tre: *employer*, *employment agency* e *labor organization*); e in particolare, con riferimento alle condotte degli *employer*, identifica come condotte vietate; « (1) *to fail or refuse to hire or to discharge any individual, or otherwise to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin*; or (2) *to limit, segregate, or classify his employees or applicants for employment in any way which would deprive or tend to deprive any individual of employment opportunities or otherwise adversely affect his status as an employee, because of such individual's race, color, religion, sex, or national origin*»¹¹⁸⁷.

Prima di esaminare lo *statute* nel merito, occorre richiamare quell'indirizzo dottrinale cui abbiamo fatto poc'anzi riferimento, e che diversi fautori trova nel settore in esame: secondo alcune voci, infatti, né il regime del *disparate treatment* né tantomeno quello del *disparate impact* risulterebbero idonei a confrontarsi con le ipotesi di discriminazione nel contesto delle decisioni automatizzate¹¹⁸⁸. Il tema è complesso, ma in sintesi a sostegno delle predette tesi è stato addotto, in particolare, l'argomento secondo il quale le *Uniform Guidelines* dell'*Equal*

¹¹⁸⁷ V. 42 U.S. Code § 2000e-2 -, rubricato «Unlawful employment practices», e nel suo ambito al lett. (a). Evidenti appaiono le affinità di molte norme dello Statuto dei Lavoratori (l. 300/1970), sul quale ci siamo già soffermati nel secondo capitolo, con le previsioni dell'atto in esame; la corrispondenza risulta ancora più marcata confrontando la previsione di cui al n. (2) appena citata e l'art. 8 dello Statuto, che abbiamo indicato come la prima norma in contesto italiano a presidio della privacy, sebbene di ordine settoriale, laddove prevede (la si cita di nuovo) che «È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

¹¹⁸⁸ Per un'analisi molto dettagliata delle dottrine del *disparate treatment* e del *disparate impact* e della loro interazione con il Titolo VII del CRA, soprattutto con riguardo al fenomeno del c.d. *Data Mining Discrimination*, cfr. il lavoro, ricco tra l'altro di riferimenti bibliografici e giurisprudenziali, di S. BAROCAS, A. SELBST, «Big Data's Disparate Impact», 104 *California Law Review* 671, 701 (2016).

Employment Opportunity Commission, deputate a promuovere l'interpretazione "autentica" del Titolo VII del *Civil Rights Act*, al paragrafo 1607.3 individuano quale eccezione al divieto introdotto dalla normativa (e specificato dalla lett. A della stessa norma di esecuzione) i c.d. *business legitimate interests*. Tale eccezione, in sostanza, legittima tutte quelle pratiche commerciali (e dunque anche tutte quelle operazioni degli *employers*) che, in assenza di pratiche alternative idonee a perseguire i suddetti interessi in modo ugualmente efficace, soddisfino questi ultimi pur risolvendosi in una discriminazione *indiretta*¹¹⁸⁹. È stato allora sottolineato come la maggior parte delle decisioni dei datori di lavoro (naturalmente, *adverse actions*) che si servano di modelli di *data mining* o di altri sistemi automatizzati di profilazione - per esempio le assunzioni - valorizzerebbe a titolo di input anche delle informazioni sensibili, il cui utilizzo, pur risolvendosi in una discriminazione, risponderebbe a specifiche esigenze lavorative¹¹⁹⁰.

A tale dottrina si contrappongono invece le voci che, pur riconoscendo l'esistenza di taluni profili problematici nell'applicabilità del Titolo VII alle fattispecie di *employer's adverse actions* che si risolvano in una discriminazione algoritmica, e segnatamente in un'ipotesi di c.d. *Data mining discrimination*, ritengono che le stesse disposizioni siano idonee a proibire i c.d. «*classification bias*» e pertanto a disciplinare, in senso restrittivo, i fenomeni di *automated discrimination* in ambito lavorativo¹¹⁹¹.

¹¹⁸⁹ V. nello specifico 29 CFR § 1607.3.

¹¹⁹⁰ S. BAROCAS, A.SELBST, «Big Data's Disparate Impact», cit. p. 701 ss cfr. S. HOFFMAN, «Big Data and the Americans with Disabilities Act», 68 *Hastings L.J.* 777, 779 (2017); nonché C. TABARRINI, *La trasparenza algoritmica*, cit., che a tale tesi sembra aderire.

¹¹⁹¹ Cfr. PAULINE KIM, «Data-Driven Discrimination at Work», 58 *Wm. & Mary L. Rev.* 857, 861-62 (2017). Per una ricostruzione della dialettica in materia, cfr. 1137.

¹¹⁹¹ Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 86 ss.

Addentrandoci nell'analisi del Titolo VII, e collegandoci subito alla questione di nostro interesse, occorre sottolineare come tra le diverse declinazione delle potenziali *adverse action* discriminatorie compiute per mezzo dell'automazione particolare attenzione abbiano suscitato sin dalla fine degli anni Settanta le pratiche di *employee screening*¹¹⁹². Sono pratiche che ancor più vivo interesse suscitano oggi, dal momento che, come si è già più volte ricordato, le procedure di selezione del personale, così come di mansionamento e più in generale di esercizio dello *jus variandi* da parte del datore di lavoro, si avvalgono sempre più spesso di sistemi di profilazione e di *decision-making* algoritmici¹¹⁹³.

La stessa *Equal Employment Opportunity Commission* (EEOC), ovvero l'autorità deputata all'*enforcement* in relazione al Titolo VII del *Civil Rights Act*, già nel 1978 varò infatti le c.d. *Uniform Guidelines on Employee Selection Procedures* (*Uniform Guidelines*), già citate poc'anzi, specificando come nel quadro dello *statute* suddetto fosse vietata qualsiasi procedura selettiva relativa ad *employees* idonea a produrre un *adverse impact* nei confronti e insieme sulla base di quelle caratteristiche protette dalla normativa in parola, ossia essenzialmente «*on grounds of race, color, religion, sex, and national origin*»¹¹⁹⁴. Le parole delle *guidelines*, al riguardo, sono cristalline: «*The use of any selection procedure which has an adverse impact on the hiring, promotion, or other*

¹¹⁹² Ivi, p. 88.

¹¹⁹³ Per un'analisi, di tipo informatico e neuroscientifico ma con importanti riflessi sulla nostra materia, dei problemi e insieme dei (presunti) vantaggi configurati dalla recente introduzione di sistemi di AI abilitati al reclutamento lavorativo, cfr. l'interessante articolo di Z. CHEN, «Ethics and discrimination in artificial intelligence-enabled recruitment practices», in *Nature, Humanities and Social Sciences Communications*, 10, 2023, <https://www.nature.com/articles/s41599-023-02079-x>. Per un'analisi giuridica di respiro più generale, cfr. AISLINN KELLY-LYTH, «Algorithmic discrimination at work», in *ELLJ*, 14(2), 2023, pp. 152-171, <https://ora.ox.ac.uk/objects/uuid:1126de23-b973-4000-a510-4f23840be2c0/files/sr207tq95s>.

¹¹⁹⁴ V. 29 CFR Part 1607. Le guidelines in parola sono appunto deputate «to assist employers, labor organizations, employment agencies, and licensing and certification boards to comply with requirements of Federal law prohibiting employment practices which discriminate on grounds of race, color, religion, sex, and national origin».

*employment or membership opportunities of members of any race, sex, or ethnic group will be considered to be discriminatory and inconsistent with these guidelines, unless the procedure has been validated in accordance with these guidelines, or the provisions of section 6 below are satisfied*¹¹⁹⁵.

Ebbene, sebbene siano trascorsi trent'anni dall'entrata in vigore della *regulation* in questione, a rendere le *guidelines*, e di conseguenza il Title VII che si propongono di interpretare in funzione applicativa, tutt'ora attuali nel contesto dell'*algorithmic decision making* in ambito lavorativo è proprio l'attenzione che le prime riservano all'aspetto dell'*impact*, e quindi dell'effetto determinato dalla procedura sull'individuo. Ad esserne per prima consapevole è la stessa EEOC, che ha recentemente promosso attività dirette a sensibilizzare sui potenziali vantaggi e insieme sui potenziali rischi che i *Big Data* possono avere nell' "*employment context*"¹¹⁹⁶.

Sotto il profilo più strettamente giuridico, allora, stante il sempre più frequente ricorso, da parte di *employers*, *employment agencies* e *labor organizations*, ad *algorithmic actions* potenzialmente idonee a produrre, in una qualsiasi *employment selection procedure*, un *adverse impact*, dobbiamo tentare di rintracciare gli istituti che il divieto in parola rendano effettivo, munendo l'interessato degli strumenti di tutela opportuni. Tali istituti sembrano potersi identificare nell'apparato rimediale, invero complesso, predisposto dalle norme di cui al § 2000e-5, rubricato per l'appunto «*Enforcement provisions*», che essenzialmente si incardina sulla *civil action* prevista dalla lett. (f) del medesimo

¹¹⁹⁵ 29 CFR § 1607.3.

¹¹⁹⁶ Si veda ad esempio, tra le diverse iniziative, EEOC, Meeting of October 13, 2016 - *Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law*, disponibile su <https://www.eeoc.gov/eeoc/meetings/10-13-16/>. Nel suo ambito, sottolineando la costante dialettica cui abbiamo fatto riferimento, la Commissione si esprime tra l'altro nei seguenti termini: «As we consider how to best apply our anti-discrimination protections to this reality, we are mindful of the value in promoting innovation, while at the same time, recognizing that it is critical to ensure that reliance on these vast sources of data do not create new barriers to opportunity».

paragrafo; tale *action*, tuttavia, risulta subordinata ad almeno una condizione di procedibilità, di natura essenzialmente *amministrativa* (a dimostrazione della dimensione superindividuale dell'interesse protetto), rappresentata dal potere-dovere di ricorrere all'EEOC affinché la stessa incardini una complessa procedura che culmini in un'*investigation* e se del caso in un provvedimento sanzionatorio¹¹⁹⁷. Parallelamente, le lett. (c) ss. aggiungono, quale ulteriore ed in tal caso aprioristica condizioni di procedibilità ai fini dell' "accesso" ai rimedi di ordine federale, che laddove l'*adverse action* abbia luogo nel territorio di uno Stato che contempli «*a State or local law prohibiting the unlawful employment practice*», il singolo non potrà nemmeno promuovere la procedura davanti alla EEOC prima di aver esaurito i rimedi interni (di natura, anch'essi, essenzialmente amministrativa)¹¹⁹⁸.

Sul punto, ha avuto modo di pronunciarsi tra le altre la stessa *United States Court of Appeals for the Fourth Circuit* in un caso del 1995, in cui la Corte, con sintetico ma efficace ritratto, precisa la fisionomia del suddetto apparato rimediale: «*Title VII of the Civil Rights Act of 1964 creates a federal cause of action for employment discrimination. Before a federal court may assume jurisdiction over a claim under Title VII, however, a claimant must exhaust the administrative procedures enumerated in 42 U.S.C. Sec. 2000e-5(b), which include an investigation of the complaint and a determination by the EEOC as to whether "reasonable cause" exists to believe that the charge of discrimination is true*»; e ancora, con riferimento all'eventuale filtro statale: «*[W]here state law protects persons against the kind of discrimination alleged, "complainants are required to resort" to "state and local remedies" before they may proceed to the*

¹¹⁹⁷ V. 42 U.S. Code § 2000e-5 - Enforcement provisions, e in part. le citate lett. (b) e let. (f). In realtà, sebbene prevista quale condizione *necessaria* di procedibilità, l'istituto in questione appare prima di tutto uno mezzo di tutela preordinato ad instaurare un procedimento amministrativo di natura autoritativa e sanzionatoria.

¹¹⁹⁸ Ivi, in part. lett. (c) (d) (e) (e) .

EEOC, and then to federal court, on their claims of discrimination under federal law»¹¹⁹⁹.

Pertanto, sebbene in ipotesi il Titolo VII predisponga delle apprezzabili garanzie rispetto all'interesse dell'individuo-*employee* a non essere oggetto di *adverse action* parzialmente o interamente automatizzate che si risolvano in un *disparate treatment* (o in un *disparate impact*); e sebbene queste garanzie, seppur di natura eminentemente rimediale, “somigliano” (c'è da dirlo, lontanamente) al *right to contest* che sostanzia una delle misure minime di tutela imposte dall'art. 22 par. 3 del GDPR come ulteriori condizione di eccezionale liceità di un processo decisionale interamente automatizzato; tuttavia la complessità che circonda il sistema in esame, unita alla mancata riproduzione di istituti analoghi a quelli di *adverse action notice* o di (preventiva o successiva) *disclosure* previsti dall'FCRA e dall'EOA lo rende difficilmente qualificabile come idoneo a soddisfare uno standard di tutela equivalente a quello previsto dal GDPR.

Merita allora richiamare ed approfondire la principale soluzione elaborata dalla giurisprudenza, e sostenuta dalla dottrina (e dallo stesso Studio della Commissione europea rilevata nel contesto del precedente *Privacy Shield*), per far fronte alla carenza di effettività che parrebbe circondare il sistema di garanzie di cui al *Civil Rights Act*, appena descritto. Ci riferiamo all'applicazione nella materia in esame della c.d. *Due Process Clause*, di matrice costituzionale, quale strumento idoneo ad infondere maggior equità e trasparenza nei processi decisionali automatizzati, e in primis in quelli implementati in ambito lavorativo (e segnatamente di *employee procedure selection*)¹²⁰⁰.

¹¹⁹⁹ Cfr. *Davis v. N. Carolina Dep't of Correction*, 48 F.3d 134, 136–37 (4th Cir. 1995), par. II, che rinvia ad una pluralità di precedenti, tra i quali *New York Gaslight Club, Inc. v. Carey*, 447 U.S. 54, 62, 100 S.Ct. 2024, 2030, 64 L.Ed.2d 723 (1980).

¹²⁰⁰ Per la ricognizione che seguirà, si veda sin da subito principalmente G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of*

Ci siamo già nel principio in esame nella nostra opera di ricognizione storica circa l'evoluzione della *privacy costituzionale*, cui facciamo pertanto integrale rinvio¹²⁰¹. In questa sede, ci limitiamo a ricordare come la “clausola” in parola, il cui significato solo parzialmente è espresso, nel nostro ordinamento e più in senso lato in quello europeo, dal concetto e dal contestuale principio del *giusto processo*, trova le proprie radici nel Quinto¹²⁰² e nel Quattordicesimo Emendamento¹²⁰³. In particolare, sulla base di quest'ultimo fondamento, laddove la disposizione statuisce che «*nor shall any State deprive any person of life, liberty, or property, without due process of law*», la giurisprudenza già prima dell'ampiamente esaminato caso *Griswold v. Connecticut* aveva interpretato la clausola in questione quale “valvola permanente d'ingresso” negli ordinamenti statali di pressoché tutti i diritti previsti dal *Bill of Rights*, nonché di quelli indirettamente garantiti dagli stessi¹²⁰⁴. Ecco, allora, che nel suddetto *leadign case* *Griswold* la *Supreme Court* non fa che rafforzare l'accezione sostanziale del

personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law (Commissione Europea, 2018), 90, i quali constatano che «In addition to Title VII protection, the U.S. Constitution can also provide more general protections that are relevant in the context of automated decisions and employment.»; D. KEATS CITROW, «Technological Due Process», 85, *Wash UL Rev*, 2008, 1249ss.; C. TABARRINI, *La trasparenza algoritmica*, cit.

¹²⁰¹ V. *retro*, cap. 1, par. 1.3.

¹²⁰² Il testo integrale dell'Emendamento in parola così recita: «*No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.*»

¹²⁰³ La Section 1 recita: «All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws».

¹²⁰⁴ Cfr. P. G. KAUPER, «Penumbras Peripheries, Emanations, Things fundamental and Things forgotten: the *Griswold* Case», in *Michigan Law Review*, 1965, vo. 64, p. 235 ss.

principio in esame, rendendolo strumentale ad assicurare che nessun procedimento, per quanto insindacabile dal punto di vista formale, possa incidere, dal punto di vista sostanziale, sul nocciolo duro e intangibile delle libertà individuali¹²⁰⁵.

Per quanto concerne le ragioni a sostegno dell'applicazione del principio in parola al contesto delle decisioni automatizzati (in qualsiasi ambito e specialmente) in ambito lavorativo, giurisprudenza e dottrina sembrano anzitutto valorizzarne proprio la funzione sostanziale: tale principio nasce e si afferma come garanzia di trasparenza (*fairness*) nel dialogo, ed anzi nella dialettica, tra individuo ed autorità pubblica, in tutte e tre le dimensioni in cui si articola la funzione generale di governo (legislativa, amministrativa e giurisdizionale), specialmente laddove siano coinvolti interessi fondamentali della persona umana, così tutelata rispetto all'ineliminabile possibilità (prima, tutta umana, oggi soprattutto algoritmica) di errore, e di conseguente *unfair or mistaken deprivation*¹²⁰⁶. La *Due Process Clause* trova allora declinazione di dettaglio in una platea di importanti principi sanciti in una pluralità di atti di *administrative law*: *transparency*, *expertise*, *rationality*, *public participation*, e *accountability* sono solo alcuni di quelli che il diritto statunitense codifica al fine di assicurare la *conoscibilità* del procedimento con cui le autorità di governo adottano le proprie

¹²⁰⁵ Ivi, p. 467 ss. Cfr. A. Baldassarre, *Privacy e Costituzione*, cit.; ed anche M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 27.

¹²⁰⁶ È questa una declinazione essenziale del principio in parola, che trova esplicitazione in numerosi precedenti, tra i quali si annovera *Fuentes v. Shevin*, 407 U.S. 67, 80–81 (1972), in cui la Corte Suprema, nelle sue motivazioni, si esprime cristallinamente nel seguente modo: «*The constitutional right to be heard is a basic aspect of the duty of government to follow a fair process of decision-making when it acts to deprive a person of his possessions. The purpose of this requirement is not only to ensure abstract fair play to the individual. Its purpose, more particularly, is to protect his use and possession of property from arbitrary encroachment—to minimize substantively unfair or mistaken deprivations of property*»..

decisioni relative all'implementazione delle *regulation* e delle politiche pubbliche, e i singoli organi dello Stato esercitano le proprie funzioni nei casi concreti¹²⁰⁷.

Il limite che certamente incontra la ricostruzione in parola è che, pur volendo applicare la *Due Process Clause* e i principi in cui si articola nel dettaglio ad una pluralità di contesti in cui i procedimenti decisionali escludano del tutto o parzialmente l'intervento umano (e per quanto qui ci riguarda, in particolare, nell'ambito delle *employment decision*), tale *Clause*, stante non solo la sua natura costituzionale, bensì anche la precisa delimitazione positiva del suo ambito di applicazione, disciplina *esclusivamente* il rapporto tra cittadino e autorità costituita, e dunque pone limiti esclusivamente alle *government authorities* (e, più in generale, agli organi dello Stato Federale e degli Stati Federati)¹²⁰⁸. Ciononostante, quanto meno nella dimensione pubblica e quindi nei rapporti orizzontali, il principio in esame pare ampiamente in grado di rispecchiare quelle (minime) garanzie adeguate di tutela che il GDPR prescrive all'art. 22 par. 3 in ordine a processi decisionali automatizzati eccezionalmente consentiti ai sensi del

¹²⁰⁷ V. solo a titolo di esempio, tra gli atti che già abbiamo incontrato, il *Freedom of Information Act* 5 U.S.C. § 552 (2012) e il *Privacy Act*, 5 USC § 552a; a cui possiamo aggiungere il *Administrative Procedure Act* 5 USC §§ 552-3 (2012); e il *The Government in the Sunshine Act*, 5 USC § 552b. Gli stessi G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., a p. 90, affermano che «*Due process precedent as well as, administrative law, and regulatory and administrative rules affirm the importance U.S. law places on transparency and rationality in both the development of rules and their application to specific individuals in specific cases*».

¹²⁰⁸ È importante qui richiamare l'altro fondamentale precedente con cui la Corte ha stabilito un *three factor test* per vagliare il soddisfacimento da parte delle Autorità Governative nell'esercizio delle proprie funzioni, in particolari amministrative, della *Due Process Clause*: *Mathews v. Eldridge* 424 U.S. 319 (1976), in cui la *Supreme Court* così si esprime: «*(...) a three factor test for considering whether due process is provided: (1) the private interest that will be affected by the official action; (2) the risk of an erroneous deprivation of such interest through the procedures used, and probable value, if any, of additional procedural safeguards; and (3) the Government's interest, including the fiscal and administrative burdens that the additional or substitute procedures would entail.*».

par. 2: e pertanto come minimo «il diritto ad ottenere l'intervento umano, ad esprimere la propria opinione e a contestare la decisione», in quanto puntualmente ricadenti nel concetto di *Due Process*. Tale principio costituzionale, dunque, appare in grado di tutelare l'individuo rispetto a decisioni algoritmiche adottate nelle più diverse declinazioni materiali del rapporto tra individuo ed Autorità, e non da ultimo dunque nei rapporti di lavoro alle dipendenze della Pubblica Amministrazione¹²⁰⁹. Questa sembra se non altro la posizione di larga parte della giurisprudenza, che, come vedremo subito, la clausola del Quattordicesimo Emendamento ha applicato in numerosi casi in cui le *adverse action* denunciate fossero dipese dall'impiego anche solo parziale di sistemi algoritmici¹²¹⁰. Parte della dottrina, poi, articolando riflessioni in punto di *tort law*, depone a favore della soluzione in questione in base alla tesi secondo cui l'impossibilità di conoscere il percorso logico seguito dalla macchina per addivenire ad una decisione poi rivelatasi dannosa (ad esempio perché erronea o discriminatoria) non integrerebbe gli estremi di un danno alla *privacy*, bensì di un pregiudizio al *due process*¹²¹¹.

Prima di affrontare un recente, emblematico caso che afferisce alla materia dei rapporti di lavoro nell'ambito della pubblica amministrazione, può essere utile ripercorrere alcuni recenti casi, pur riguardanti ambiti diversi rispetto a quello lavorativo, in cui la *Due Process Clause* si è trovata ad interagire con processi decisionali interamente automatizzati intervenuti nei rapporti tra individuo ed

¹²⁰⁹ Per alcune riflessioni più approfondite sull'applicazione della Due Process Clause nel contesto Big Data, cfr. CRAWFORD, KATE, AND JASON SCHULTZ, «Big data and due process: Toward a framework to redress predictive privacy harms», in *BCL Rev.* 55 (2014): 93.

¹²¹⁰ Il tema non può che riportarci alle essenziali pronunce sulla trasparenza algoritmica che hanno contrassegnato la giurisprudenza amministrativa italiana negli ultimi anni, e sulle quali ci siamo puntualmente soffermati nel cap. 3, par. 3, cui si fa rinvio per un confronto relativo al tenore delle decisioni.

¹²¹¹ Cfr. sul punto C. TABARRINI, *La trasparenza algoritmica*, che richiama D. KEATS CITROW, «Technological Due Process», 85, *Wash UL Rev.* 2008, 1249ss.e M.R. CALO, «The Boundaries of Privacy Harm», 86, *Ind. L.J.*, 2011, 1131, 1146-52.

Autorità Pubblica (segnatamente, in tutte le specie esaminate, Autorità Giudiziaria). Si tratta di casi in cui, invero, la tecnologia algoritmica veniva impiegata piuttosto come supporto; e in cui le Corti evitano largamente di sciogliere la questione relativa al riconoscimento in capo all'interessato (in tal caso, imputato) di un diritto ad ottenere informazioni sulla logica del sistema algoritmico.

Merita in proposito sottolineare che le pronunce che qui riporteremo, com'è stato notato, sono espressioni di una tendenza che sta lentamente affermandosi: pertanto, le contraddizioni che le animano sono certamente imputabili allo stato ancora embrionale del processo di adattamento all'universo dei sistemi decisionali automatizzati, e segnatamente algoritmici, dei principi cui si è fatto riferimento, sintetizzati nella clausola del *Due Process*¹²¹².

Si può fare riferimento innanzitutto al caso *Malenchik v. State of Indiana*, in cui la Corte Suprema dell'Indiana ha giudicato legittimo l'utilizzo di un *algorithmic assesment risck score* da parte di un Tribunale, acconsentendo a che venisse considerato « *as a supplemental source of information to assist a trial court in formulating the manner a sentence is to be served* », purché tuttavia questo non si sostituisca alle determinazioni stesse della Corte, valorizzando a tal proposito « *the accused's due process rights not to be sentenced on the basis of unreliable information* »¹²¹³.

Sempre nel senso di un'apertura relativa all'impiego dei sistemi algoritmici di cui andiamo discorrendo, deve citarsi il ben più noto caso *State of Wisconsin v.*

¹²¹² G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 90, dove gli autori affermano: « *Constitutional due process protections will limit and shape the use of automated decision-making systems. It will take time for the courts to sort out how due process principles apply to automated decision-making systems (...) While applying these [principles] to various automated processing and decision-making systems will take time these bedrock principles will channel and determine their use* ».

¹²¹³ *Malenchik v. State*, 928 N.E.2d 564, 575 (Ind. 2010), in part. par. 574 ss.

Loomis, di cui ripercorreremo brevemente la vicenda, stante l'eco che essa, prima ancora che la decisione, ha avuto nell'opinione pubblica e prima ancora nel mondo del diritto¹²¹⁴. La controversia aveva sullo sfondo l'elaborazione e il dibattito circa l'impiego nel circuito giudiziario e di polizia del programma *COMPAS* (acronimo di *Correctional offender management profiling for alternative sanctions*), concepito per prevedere il rischio di recidiva: esso, sulla base di un test strutturato in 137 domande sottoposto all'indagato o, successivamente, all'imputato e del fascicolo delle indagini o del processo, assegnava un punteggio su una scala da 1 a 10 circa la probabilità di commissione di nuovi reati¹²¹⁵. Ciò premesso, il caso concreto poi giunto davanti alla Corte Suprema del Wisconsin riguardava Eric Loomis, il quale, mentre guidava un'automobile usata durante una sparatoria, veniva arrestato con l'accusa di non essersi fermato al controllo della polizia. Rinvitato a giudizio, in primo grado il giudice decideva anche sulla base del punteggio attribuito da *COMPAS* all'imputato, che lo individuava come un soggetto ad alto rischio di recidiva¹²¹⁶. Impugnata la sentenza, la Corte di ultima istanza statale si ritrovava anche essa a riconoscere la legittimità del sistema *COMPAS*, e in particolare sul rilievo che l'algoritmo (il *risk assesment tool*) fungesse da mero strumento nelle mani del giudice, peraltro servendosi di *available data* o comunque forniti dall'interessato: essa concludeva infatti che «*if used properly, observing the limitations and*

¹²¹⁴ Cfr. da subito *State v. Loomis*, 881 N.W.2d 749, 753 & n.10 (Wis. 2016). Sulla sentenza è fiorita un'eterogenea pluralità di commenti, tanto di segno positivo quanto di tenore più critico: cfr. ex multis S. CARRER, «Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin», in *Giurisprudenza Penale Web*, 2019, 4; K. FREEMAN, «Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in *State v. Loomis*», in *North Carolina Journal of Law & Technology*, Vol. 18, 2016, <https://scholarship.law.unc.edu/ncjolt/vol18/iss5/3/>.

¹²¹⁵ Per più puntuali informazioni sul funzionamento del programma Compas, cfr. ex multis J. DRESSEL, H. FARID, «The accuracy, fairness, and limits of predicting recidivism», in *Sci Adv.*, 4(1), 4 gennaio 2018, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5777393>.

¹²¹⁶ Per la ricostruzione del caso, vedi anche il ritenuto in fatto della sentenza: *State v. Loomis*, 881 N.W.2d 749, 753 & n.10, par. 1 ss.

*cautions set forth herein, a circuit court's consideration of a COMPAS risk assessment at sentencing does not violate a defendant's right to due process»; e tuttavia, tra le cautions in questione, la principale viene riscontrata nel fatto che i «risk scores may not be considered as the determinative factor in deciding whether the offender can be supervised safely and effectively in the community»¹²¹⁷. Nonostante le evidenti aperture all'impiego della tecnologia in parola mostrate dalla sentenza, e l'eccessiva fiducia riposta nell'“indipendenza” anche cognitiva del giudice persona fisica, la Corte sembra qui ribadire il principio del *necessario*, ed anzi in tal caso prevalente, intervento umano, affinché il procedimento risulti sempre ricondotto ad un principio di razionalità. E tuttavia, i limiti della motivazione (rispetto ai pregi) paiono amplificati dal fatto che, come è stato riscontrato, la clausola del *due process* viene ritenuta rispettata «*even though the methodology used to produce the assessment was disclosed neither to the court nor to the defendant*»¹²¹⁸. Evidentemente, tale circostanza contraddice in principio l'esigenza di trasparenza dell'intero procedimento, a cominciare dalla logica che *ex ante* lo informa¹²¹⁹.*

¹²¹⁷ Ivi, par. 137 ss. Cfr. anche sul punto G. PESCE, «Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale», cit.,

¹²¹⁸ Cfr. in particolare Criminal Law — Sentencing Guidelines — Wisconsin Supreme Court Requires Warning Before Use Of Algorithmic Risk Assessments In Sentencing — *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016)., laddove si legge «*hile the Loomis court provided a procedural safeguard to alert judges to the dangers of these assessments — a “written advisement” to accompany PSIs — this prescription is an ineffective means of altering judges' evaluations of risk assessments. The court's “advisement” is unlikely to create meaningful judicial skepticism because it is silent on the strength of the criticisms of these assessments, it ignores judges' inability to evaluate risk assessment tools, and it fails to consider the internal and external pressures on judges to use such assessments.*».

¹²¹⁹ In tal senso, essa appare del tutto dissonante con una delle sentenze che nell'ordinamento italiano vanno concorrendo a sancire il principio di “trasparenza algoritmica” nei procedimenti amministrativi, ossia Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881, laddove questa ai fini del ricorso ad algoritmi ai fini dell'elaborazione della decisione amministrativa impone, innanzitutto «la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati».

A fronte di tali pronunce, invero non ancora cristalline nel trarre dalla pur ferma affermazione del principio del *Due Process* le dovute conseguenze in termini di tutela dell'individuo di fronte alla discriminatoria opacità dell'algoritmo, è possibile invece rintracciare proprio in materia di *employment* nel settore pubblico una sentenza che offre un positivo esempio di come la *Due Process Clause* possa concorrere a contrastare l'attitudine discriminatoria insita nei processi (non solo parzialmente bensì *interamente*) algoritmici, e gli effetti pregiudizievoli che ne derivino a carico degli interessati. Ci riferiamo al caso *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist.*, che prende le mosse dall'impugnazione promossa un gruppo di insegnanti precedentemente alle dipendenze di una scuola pubblica di Houston, in Texas, avverso il provvedimento di licenziamento, che lamentavano essere basato sull'utilizzo di un sistema algoritmico introdotto nel 2012 ai fini di valutazione della performance degli insegnanti medesimi ¹²²⁰. Il software in esame, prodotto da un'azienda privata e denominato *Educational Value-Added Assessment*, aveva infatti assegnato ai dipendenti in questione un basso punteggio, su cui la scuola si era basata per interrompere il rapporto di lavoro. Stante, come rilevato dal *background* ritratto dalla sentenza della Corte distrettuale del Texas, *Houston Division*, la vigenza nello Stato del Texas di normative che la legittimità del licenziamento subordinano al previo esperimento di determinati mezzi di conservazione del rapporto contrattuale, in particolare attribuendo al lavoratore il diritto di accedere alle evidenze su cui si basa la "proposta" di provvedimento terminativo, e di presentare essi stessi evidenze e memorie orali prima che questo diventi effettivo; il principale motivo di ricorso articolato dagli attori consisteva proprio nella violazione dei diritti in parola, nella specie determinata dal rifiuto della loro richiesta di accedere al sistema algoritmico medesimo ed ai dati su cui gli *scores*

¹²²⁰ *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist.*, 251 F. Supp. 3d 1168, punto 1171 (S.D. Tex. 2017).

da questo prodotti si sarebbero basati, allo scopo di accertarne l'accuratezza¹²²¹. Nelle deduzioni degli insegnanti, si legge infatti che la *Due Process Clause* richiederebbe « *an opportunity by teachers to test on their own behalf the accuracy of their HISD-sponsored value-added scores*»¹²²².

Ebbene, la Corte ha aderito sostanzialmente alla lettura prospettata dagli attori, accogliendone le doglianze, affermando come l'utilizzo da parte di un ente pubblico di un algoritmo *inaccessibile*, poiché coperto da diritti di proprietà intellettuale, peraltro strumentale a prendere *high stakes employment decisions* (ed anzi, guardando alla vicenda, *adverse actions* basate esclusivamente sullo *score* algoritmico, verrebbe da dire) violerebbe i principi in cui si articola la *Due Process Clause*: l'impossibilità di accedere alla formula-tecnico matematica cui risulti improntato il funzionamento dell'algoritmo e, insieme, ai suoi input (i dati degli interessati), dimidiava inevitabilmente il diritto al contraddittorio (e a monte la capacità di contestare nelle opportune sedi la decisione), corollario indefettibile del principio del giusto processo; e quindi in definitiva -leggendo tra le righe- la trasparenza dell'intera procedura, sostanzialmente automatizzata, di licenziamento¹²²³.

La pronuncia in questione pare collocarsi sulla stessa scia di quelle che la nostra giurisprudenza amministrativa ha dedicato al tema della trasparenza algoritmica, fissando quel "decalogo" di principi di cui abbiamo approfonditamente parlato nel capitolo precedente, da cui strettamente dipende la

¹²²¹ Ivi, punto 1176.

¹²²² Ivi, punto 1178.

¹²²³ *Ibidem*. Da notare come la Corte, al punto successivo, si determini l'opportunità di un bilanciamento tra il principio del contraddittorio – e dunque, tradotto nel conteso della *data protection*, del diritto ad ottenere le informazioni significative indispensabile per contestare la decisione interamente automatizzata, e i diritti di brevetto, o comunque di proprietà industriale, insistenti sulla formula algoritmica, così affermando: « *[w]hen a public agency adopts a policy of making high stakes employment decisions based on secret algorithms incompatible with minimum due process, the proper remedy is to overturn the policy, while leaving the trade secrets intact.*»

legittimità del procedimento amministrativo interamente algoritmico, ed individuati essenzialmente nel *principio di conoscibilità dell'algoritmo*, in quello di *non esclusività della decisione algoritmica* e in quello di *non discriminazione algoritmica*: principi che bene sembrano rispecchiare l'essenza della *Due Process Clause*, che quando si confronti con i processi decisionali interamente automatizzati, come il caso appena esaminato dimostra, pare offrire agli interessati importanti garanzie, idonee a temperarne l'effetto discriminatorio e, in definitiva, a presidiarne la libertà di autodeterminarsi consapevolmente¹²²⁴.

A questo punto, possiamo introdurci nel secondo settore in cui abbiamo riscontrato una crescente rilevanza degli *ADM systems*; la loro potenziale idoneità a incidere gravemente sui diritti fondamentali degli interessati; nonché l'esistenza di una *equal protection law* che, esplicitamente, sembra offrire alcune garanzie suscettibili di applicazioni anche al fenomeno in esame: il mercato immobiliare residenziale.

Il *Fair Housing Act* parrebbe, infatti, predisporre alcuni strumenti di tutela esperibili (anche) a fronte di decisioni automatizzate nel contesto delle *residential dwellings*, rispetto alle quali, lo ricordiamo, lo *statute* in parola proibisce qualsiasi discriminazione sulla base dell'etnia, del sesso o di altre caratteristiche protette¹²²⁵. Il § 3602(b) dà infatti una definizione ampia di «*dwelling*», ricomprendendovi «*any building, structure, or portion thereof which is occupied as, or designed or intended for occupancy as, a residence by one or more families, and any vacant land which is offered for sale or lease for the construction or location thereon of any such building, structure, or portion thereof*».

¹²²⁴ Cfr. ancora una volta Cons. Stato Sez. VI, Sent., 13-12-2019, n. 8472 in www.giustizia-amministrativa.it; v. ampiamente *retro*, cap. 3, par. 2.4.

¹²²⁵ V. 42 USC § 3601 ss.

L'atto prescrive come sia «*unlawful to refuse to sell, rent, or otherwise make unavailable a dwelling on the basis of race, color, religion, sex, familial status, national origin, or handicap*», parimenti statuendo l'illegalità di qualsiasi discriminazione in termini di prezzo o di canoni d'affitto, così come l'*advertising* di residenze secondo modalità discriminatorie e la "falsa rappresentazione" della disponibilità di una residenza¹²²⁶.

Ora, come abbiamo già anticipato, sebbene minor oggetto di attenzione da parte dei giuristi, fenomeni di ADP e soprattutto di ADM cominciano a trovare ampia diffusione anche nel settore in esame, specialmente a fronte della proliferazione di *online marketplaces* in grado di svolgere la ricerca di alloggi abitativi e di negoziarne la compravendita o piuttosto l'affitto a breve, medio o lungo termine. In tale quadro poi, specialmente nel contesto del *rental housing*, sempre maggiore appare il ricorso a società di (*Big*) *data brokerage* e soprattutto *analytics* per determinarsi nelle trattative con i potenziali clienti, con il rischio che gli algoritmi impiegati, replicando i *pattern* esistenti nel contesto sociale di riferimento, promuovano dinamiche di segregazione (anche) online¹²²⁷.

¹²²⁶ 42 USC § 3604, rubricato «*Discrimination in the sale or rental of housing and other prohibited practices*»

¹²²⁷ Oltre ai contributi citati *retro*, nota 1151, cfr. l'interessante articolo, ricco di riferimenti giurisprudenziali e di spunti bibliografici, di V. SCHNEIDER, «Locked Out By Big Data: How Big Data Algorithms and Machine Learning May Undermine Housing Justice», in *Columbia Human Rights Law Review*, p. 268, che riscontra come le società di Big Data specificamente deputate ad assistere individui ed imprese nel *decision making*, e dunque anche owners e landlords in relazione a tenants application (come Core Logic e General Information), «pulls data from its "proprietary records" including an applicant's "eviction records, address history, criminal records, identity fraud and credit data», richiamandosi a tal proposito il caso *Conn. Fair Hous. Ctr. v. Corelogic Rental Prop. Sols., LLC*, 369 F. Supp. 3d 362, 369 (D. Conn. 2019). Opportunamente l'autrice fa rinvio anche alle già scandagliate considerazioni di BAROCAS, SELBST, «Big Data disparate impact», cit. dove notano come l'utilizzo di algoritmi, Big Data e Machine Learning «*form of statistical (and therefore seemingly rational) discrimination*», a cui l'autrice (p. 258) aggiunge che «*The problem with big data, however, is that it must use existing data, which often reflects existing patterns of discrimination and this can perpetuate the unequal status quo*».

Ora, di fronte all'implementazione di *algorithmic decision making* nel settore in esame, attivabili risultano gli strumenti che il *Fair Housing Act* offre a fronte di *adverse action* che producano effetti pregiudizievoli di natura discriminatoria sui potenziali *tenants*. Nello specifico, l'impianto normativo, al pari di tutte le *equal protection laws*, pare fondarsi sulla dicotomia (esegetica) tra *disparate treatment* e *disparate impact*, garantendo tutela in relazione a entrambe le fattispecie; e, soprattutto, questo appare predisporre, sul piano rimediale, una serie di istituti analoghi a quelli previsti, nel rispettivo settore, dal Title VII del *Civil Rights Act*, eliminando tuttavia (opportunamente) i vincoli di condizionalità esistenti tra rimedi amministrativi e rimedi civilistici. Nel disciplinare infatti gli istituti di «*Administrative enforcement*», i §§3610 ss. non individuano condizioni di procedibilità della specie di *civil action* prevista e disciplinata dal §3613, peraltro indifferentemente esperibile davanti ad una *federal* o piuttosto *state district court* (sebbene entro il termini di 2 anni dall'inizio o piuttosto, se continuativa, dalla fine di una «*discriminatory housing practice*») ¹²²⁸.

Bisogna allora concordare con il *Fair Housing Legal Support Center and Clinic* laddove ha avuto modo di dire che: «*Perhaps no area of the law accords a complainant a greater choice of procedures to remedy discrimination than fair housing law. Many states and local governments provide remedies. Federal remedies range from HUD conciliation efforts to federal court litigation*» ¹²²⁹. E,

¹²²⁸ V. in part. 42 U.S. Code § 3613 - Enforcement by private persons, lett. (a), rubricata «*Civil action*», che al n. (2) espressamente stabilisce l'indipendenza tra i rimedi in parola: «*An aggrieved person may commence a civil action under this subsection whether or not a complaint has been filed under section 3610(a) of this title and without regard to the status of any such complaint*», aggiungendo poi tuttavia, in una prospettiva di promozione dei mezzi di deflazione del contenzioso giudiziario, che «*if the Secretary or a State or local agency has obtained a conciliation agreement with the consent of an aggrieved person, no action may be filed under this subsection by such aggrieved person with respect to the alleged discriminatory housing practice which forms the basis for such complaint except for the purpose of enforcing the terms of such an agreement*».

¹²²⁹ FAIR HOUSING LEGAL SUPPORT CENTER AND CLINIC, «A Primer on Fair Housing Law», in *The John Marshall Law School*, 2014, p. 16 ss..

insieme, constatare che tale apparato rimediale rappresenta anche più di quello delineato dal *Title VII Civil Rights Act* un sistema idoneo a riprodurre, a fronte di processi decisionali interamente automatizzati, talune delle garanzie previste (*rectius* imposte) dal par. 3 dell'art. 22 del GDPR, e in particolar modo del diritto di contestare la decisione, sebbene in sede amministrativa e/o giurisdizionale. Tuttavia, va certamente evidenziato come nemmeno l'atto in parola preveda istituti affini a quelli del dovere di *information disclosure* e di *adverse action notice* previsti nell'ambito dell'FCRA e del ECOA (a propria volta, come abbiamo visto, vicini ma non speculari ai doveri d'informativa e ai diritti di accesso rafforzati in ordine ai processi di ADM di cui all'art. 22 del GDPR)¹²³⁰.

Prima di concludere, un accenno va fatto alle altre *equal protection laws* vigenti nel panorama statunitense, e ai motivi per cui, pur riguardando settori che coinvolgono importanti attributi fondamentali dell'individuo e in cui sempre maggiore appare l'impiego della tecnologia algoritmica, si è deciso di non affrontarle nel merito.

La FTC, in uno dei suoi già menzionati report, ha infatti segnalato come altrettanto rilevanti in contesto *Big Data* potrebbero essere, al fine di contrastare i potenziali effetti discriminatori derivanti dal data processing e dal *decision making algoritmico*, altre *equal protection laws*, come i già citati *Americans with Disabilities Act* (ADA), *the Age Discrimination in Employment Act*, (ADEA), and *the Genetic Information Nondiscrimination Act* (GINA). Al pari del Title VII del Civil Rights Act e dell'FHA, questi *statutes* infatti proibiscono (dirette e indirette) discriminazione sulla base, rispettivamente, della disabilità, dell'età e

¹²³⁰ Cfr. anche G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 93

dell'informazione genetica, e predispongono anch'essi un apparato rimediale che, pur differenziandosi nelle particolarità, nei suoi caratteri generali rassomiglia a quello edificato dai due atti normativi appena esaminati¹²³¹.

E tuttavia, gli *statutes* in questione, nonostante le rilevanti prescrizioni antidiscriminatorie, conoscerebbero una limitazione che quasi ne neutralizza l'efficacia protettiva in materia di (*adverse*) *automated decision*: le loro norme parrebbero inidonee ad offrire tutela rispetto a quelle condotte che si traducano in pur altamente probabili *discriminazioni future*. Esemplificando, per quanto riguarda il GINA, come è stato lucidamente notato lo *statute* in questione, pur vietando le discriminazioni sulla base dei dati genetici (che, come sappiamo, in contesto europeo rappresentano una categoria particolare di dati – o dati sensibili - ex art. 9 GDPR, che ne assoggetta il trattamento ad un regime particolarmente gravoso), « *does not limit the use of information about such a disposition—even if it is grounded in genetics—inferred through machine learning techniques that mine other sorts of data. In other words, machine learning that predicts future health status from nongenetic information—including health status changes due to genetic predisposition—would circumvent existing legal protections* »¹²³².

E allo stesso modo, in contesto lavorativo, l'ADA « *protects only individuals who are currently disabled, have records of past disabilities, or are regarded as having existing impairments. As such, it (...) does not stretch to cover individuals who are perfectly healthy at present but whom an employer suspects of being at risk of serious ailments later in life based on big data analysis* »¹²³³.

¹²³¹ FEDERAL TRADE COMMISSION, *Big Data: A Tool for Inclusion or Exclusion?* (January 2016); EXECUTIVE OFFICE OF THE PRESIDENT, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (May 2016).

¹²³² Cfr. sul punto l'importante contributo di ERIC HORVITZ, DEIRDRE MULLIGAN, «Data, Privacy, and the Greater Good», 349 *Science* 6245, 253-54 (2015); MARK ROTHSTEIN, «Is GINA Worth the Wait?», 36 *J. Law, Medicine & Ethics* 174, 177 (2008).

¹²³³ SHARONA HOFFMAN, «Big Data and the Americans with Disabilities Act», 68 *Hastings L.J.* 777, 779 (2017).

Questo “stato dell’arte”, di fronte alle crescenti potenzialità predittive (e, quindi, alla crescente capacità di discriminare *pro futuro*) dei sistemi algoritmici di trattamento e di *decision making*, insieme a tutta la loro denunciata capacità di inferire dati sensibili da dati anche a-personali¹²³⁴, rende le normative in questione, di fatto, inefficaci in funzione dell’obiettivo di massimizzare la tutela dei *fundamental rights* della persona.

Alla luce di tutti i rilievi svolti, possiamo concludere che, almeno nei settori coperti dal *Title VII* del *Civil Rights Acts* e dall’FHA, il diritto statunitense, pur non delineando una invero opportuna architettura di posizioni giuridiche soggettive attive e passive che offrano una protezione rafforzata agli *individuals* a fronte - almeno- di *fully automated decision making*, offre strumenti di tutela duttili, capaci di adattarsi anche a tale più evoluto contesto di tecniche e, conseguentemente, di pericoli di discriminazione cui la persona risulta esposta nella società degli algoritmi. Ciò, lo ripetiamo, appare espressione di quell’approccio evolutivo che la giurisprudenza americana - tanto costituzionale quanto di *common law* - sembra incline a seguire (sebbene non sempre, come abbiamo constatato ad esempio nel caso Loomis), necessariamente in senso “*privacy oriented*”.

E tuttavia, pur intendendosi rifuggire da una prospettiva, come abbiamo detto, “eurocentrica”, non si può non constatare come tali strumenti riflettano solo in minima parte - lo si ripete - il sistema di garanzie predisposto dal GDPR: nelle normative in questione, per tutte le ragioni ampiamente esposte nelle pagine che

¹²³⁴ Cfr. ancora una volta, ex multis, BAROCAS, SELBST, «Big-data’s Disparate Impact», in *California Law Review*, 2016, p. 671 ss.; e si rinvia ancora una volta all’opportuna classificazione fatta propria da ABRAMS, «Origins of Personal Data and its Implications for Governance», in *The Information Accountability Foundation*, marzo 2014, in <http://informationaccountability.org/wp-content/uploads/Data-Origins- Abrams.pdf>

precedono, e complice certamente la loro estraneità ad una concezione di *data privacy* come *materia specifica* (pur trasversale), non solo non si rinviene un nucleo di diritti e di doveri “informativi” rafforzati in punto di ADM; ma nemmeno, in partenza, è dato ravvisare un panorama normativo generale che l'*accountability* del titolare valorizzi e l'autodeterminazione informativa dell'interessato garantisca, al pari di quanto i doveri di cui agli art. 12-14 e i diritti di cui agli art. 15-22 consentono nel GDPR. Com'è d'altronde naturale, visto che le normative in questione risalgono, rispettivamente, al 1964 e al 1978.

La giurisprudenza, conformemente al ruolo creativo che svolge nell'ordinamento statunitense, potrebbe certamente inferire tale sistema dall'articolato degli *statutes*, come dimostra la recente estensione della portata applicativa della *Due Proces Clause*: il dato letterale, come abbiamo visto, vi si presta.

Ma anche prescindendo dal contesto delle *equal protection laws* (il discorso, come abbiamo visto, ben vale anche per l'FCRA e l'ECOA), l'approccio *sector specific*, e quindi l'assenza di una normativa generale che di *data privacy and protection* si occupi già a livello federale, sembra fino ad ora indebolire l'efficacia delle soluzioni elaborate dalla dottrina e dalla giurisprudenza per ovviare all'approccio *technology dependent* storicamente assunto dal legislatore. E ciò vale a maggior ragione se si considera che le *altre equal protection laws*, altrettanto settoriali, sembrerebbero *unfittable* ad una esegesi che dall'articolato inferisca un sistema di garanzie relativo al fenomeno dei trattamenti e dei processi decisionali demandati agli algoritmi, dove (come è quasi sempre) di segno predittivo.

4.3.3. La Sezione 5 del *Federal Trade Commission Act*: *unfairness, deception* e processi decisionali automatizzati

A fronte dello scenario delineato nei precedenti paragrafi, nel chiudere la nostra panoramica sul diritto federale statunitense applicabile agli *automated data processing and decision making systems*, occorre soffermarsi sull'importanza del ruolo che la *Federal Trade Commission* ha svolto e continua a svolgere in punto di *enforcement* delle disposizioni di diritto positivo in materia di protezione dei consumatori le quali, seppur *sector specific*, abbiano ricadute (come tutte le normative fin qui analizzate) nella dimensione della *data privacy*: ruolo di assoluto rilievo nel contesto del diritto privato statunitense, caratterizzato, come abbiamo visto, da una forte *deregulation* ¹²³⁵. Senza pretendere di ripercorrere qui l'intera evoluzione dei poteri di *enforcement* e di *rulemaking* attribuiti originariamente - e progressivamente estesi - alla FTC, qui si intende, dopo alcune considerazioni di sistema, analizzare il positivo impatto che l'attività di tale Agenzia è in grado di svolgere in punto di tutela dell'individuo-consumatore di fronte al fenomeno che ci occupa.

Come già abbiamo accennato nel primo capitolo, la *Section 5* del *Federal Trade Commission Act* attribuisce sostanzialmente alla FTC il potere di *enforcement* rispetto ad un vasto numero di *generic consumer protection laws*: se la lett (a) del par. 45 del Titolo XV dell'*U.S.C. Code* prevede infatti generalmente come *unlawful* tanto qualsiasi « *unfair methods of competition in or affecting commerce*» quanto qualsiasi «*unfair or deceptive acts or practices in or affecting commerce*», al n. (2) la disposizione medesima delinea in modo assai ampio la sfera dei poteri formalmente attribuiti alla FTC, stabilendo, consequenzialmente

¹²³⁵ Sulla storia, sul ruolo e sulle competenze della FTC la letteratura è, naturalmente, vasta: qui si adottano come principali riferimenti S.M. BOYNE, «Data Protection in the United States», cit. 299, 301; SOLOVE, DANIEL J., KENNETH BAMBERGER, WOODROW HARTZOG, «The FTC and the new common law of privacy», in *Colum. L. Rev.* 114 (2014): 583; CHRIS HOOFNAGLE, «Federal Trade Commission: Privacy Law and Policy» (2016), 132; FEDERAL TRADE COMMISSION, *Big Data: A Tool for Inclusion or Exclusion?* (January 2016), at 21.

che: «*The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations (...) from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce*»¹²³⁶.

Va in ogni caso preliminarmente notato che, conformemente alle eccezioni invero rilevanti delineate dallo stesso paragrafo, dalla sfera di competenza dell'FTC esulano in linea di principio le condotte, della predetta specie, di gran parte delle agenzie federali e statali, delle organizzazioni non governative e degli enti commerciali operanti nei settori di trasporto, assicurativo, bancario e delle telecomunicazioni.

In questo senso, proprio perché la competenza della FTC può, in senso proprio, dirsi limitata alla “protezione del consumatore”, possiamo in prima battuta affermare che essa svolge un ruolo di *enforcement* in punto di *data privacy* nella misura in cui la legislazione che, settorialmente, prevede norme a riguardo attenga alla *consumer protection*¹²³⁷. Tuttavia, proprio a dimostrazione della funzione di “garante” avverso le violazioni delle *privacy policies* da parte delle

¹²³⁶ V. 15 U.S. Code § 45, rubricato «*Unfair methods of competition unlawful; prevention by Commission*». In conseguenza dell'ampio margine applicativo delle disposizioni in esame, ed anche in conseguenza degli interventi federali che ne hanno progressivamente esteso la sfera di competenza, possono in prima battuta ritenersi ricadenti nella *jurisdiction* della Commissione le seguenti normative: *Right to Financial Privacy Act* (RFPA) of 1978, 12 U.S.C. §§ 3401-3422 (2006); *Electronic Communications Privacy Act* (ECPA) of 1986, 18 U.S.C. §§ 2510-2522; *Video Privacy Protection Act* (VPPA) of 1988, 18 U.S.C. §§ 2710-2712; Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), 15 U.S.C. §§ 6801-6809, 6821-6827 *Health Insurance Portability and Accountability Act* (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) e 45 CFR parti 160 and 164.

¹²³⁷ S.M. BOYNE, «Data Protection in the United States», cit., 299, 301. Si può anche dire, piuttosto, che essa intanto persegua la violazione delle *privacy policies* perpetrata da *individual* e soprattutto *businesses* in quanto integri una pratica commerciale ingannevole o scorretta ai sensi del par. 45, lett. (a) in esame, lesiva degli interessi dei consumatori, alla luce quindi di una delle normative che, settorialmente, della *consumer protection* si occupi: cfr. anche D.J. SOLOVE, W. HARTZOG, «The FTC and the New Common Law of Privacy», cit., 583, 603; D. KLITOU, *Privacy-Invasive Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014, 40

companies già di fatto svolta a partire dagli anni Novanta, il Congresso ha progressivamente esteso, con interventi normativi specifici, il potere di vigilanza e di “repressione” della FTC anche in relazione ad una serie di atti normativi non puntualmente inerenti alla protezione del consumatore, e tuttavia rilevanti in materia di *data privacy*: tali sono, in particolare, il *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN- SPAM) Act*, il *Children’s Online Privacy Protection Act (COPPA)*, nonché, come ormai sappiamo, l’EOA e il FCRA¹²³⁸. E bisogna anche aggiungere come la sua *jurisdiction* fosse, nella vigenza del *Safe Harbor* e del *Privacy Shield*, ulteriormente estesa, stante l’attribuzione in via pressoché esclusiva a quest’ultima della competenza a vigilare sulla *compliance* delle *harborities*, e delle società comunque iscritte alla lista del secondo sistema, ai principi degli accordi in parola. In tal modo, l’FTC assumeva una generale funzione di monitoraggio sul regime normativo del trasferimento transfrontaliero di dati personali; tale competenza, in realtà, sembra esser stata confermata, ad un primo sguardo, anche dal *Data Privacy Framework*¹²³⁹.

¹²³⁸ *Ibidem*; emblematico è il fatto che dal 2006 sia operativa la *Division of Privacy and Identity Protection* competente in materia di *privacy* attraverso attività di *enforcement* e *policy-making*. Cfr. sul punto anche C. TABARRINI, «La trasparenza algoritmica», cit., che richiama S. HETCHER, «The De Facto Federal Privacy Commission», in *J. Marshall J. Computer & Info. L.*, 2000, 19, pp. 109-131.

¹²³⁹ Anzi, in contesto DPF affinché una *organisation* possa ottenere la certificazione (che la liceità del trattamento dei dati personali trasferiti dal territorio dell’UE condiziona) ai sensi dell’EU-US DPF è necessario che la stessa ricada già sotto la *jurisdiction* della FTC: v. Commissione Europea, *Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final, in part. cons. 9, in cui si legge: «*The EU-U.S. DPF is based on a system of certification by which U.S. organisations commit to a set of privacy principles - the ‘EU-U.S. Data Privacy Framework Principles’, including the Supplemental Principles (together: the Principles) - issued by the U.S. Department of Commerce (DoC) and contained in Annex I to this Decision 16. To be eligible for certification under the EU-U.S. DPF, an organisation must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the U.S. Department of Transportation (DoT)*». E poi, previsione ancor più rilevante, v. Annex I, punto 2, dove recita «*An organization’s failure to comply is enforceable by the FTC under Section 5*

Possiamo venire, a questo punto, ai motivi per cui la *Section 5* stessa dell'FTC *Act*, e i poteri di cui la Commissione dispone ai sensi del medesimo, siano ritenuti un importante strumento di tutela per gli individui (seppur tutelati, lo si ripete, in quanto consumatori) anche a fronte di trattamenti automatizzati e, soprattutto, di *automated decision making systems*¹²⁴⁰. Ebbene, ciò dipende essenzialmente dalla natura sempre più “normativa” assunta dalle azioni adottate dall'FTC nell'esercizio dei propri poteri di *enforcement* in virtù della *Section 5*¹²⁴¹. A tale scopo, i provvedimenti più rilevanti sono certamente i c.d. *consent orders*: si tratta di *settlement agreements* “negoziati” con la FTC ad opera della parte destinataria di un *complaint* (non impugnato) emesso all'esito di una delle procedure amministrative che la Commissione, storicamente, intraprende per perseguire le violazioni più macroscopiche delle normative a protezione dei consumatori, perpetrate da imprese di grandi dimensioni. In questo modo, consequenzialmente, gli “accordi” in parola, formalmente vincolanti per la singola impresa, acquistano di fatto una funzione interpretativa privilegiata e soprattutto di *indirizzo generale*, svolgendo una considerevole efficacia deterrente ed educativa rispetto alle condotte delle altre *organisations*¹²⁴².

of the Federal Trade Commission (FTC) Act prohibiting unfair or deceptive acts in or affecting commerce (15 U.S.C. § 45)», sebbene questa volta alla competenza della Commissione si aggiunga quella, come già *retro* accennato, del DOT. V. *retro*, cap. 4 par. 1

¹²⁴⁰ Per una generale ricostruzione, cfr. anche G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law*, cit., p. 95 ss., Studio che concorre ad “orientare” la nostra ricerca.

¹²⁴¹ Tanto che alcuni autori nel qualificare i provvedimenti adottati dalla FTC in tale quadro e nell'analizzarne gli effetti discorrono di “*new common law of privacy*”: cfr. D.J. SOLOVE, W. HARTZOG, «The FTC and the New Common Law of Privacy», cit., 583

¹²⁴² Ivi, p. 611. V. in part. 15 U.S. Code § 45, lett. (b) rubricato «*Proceedings by Commission; Modifying and Setting Aside Orders*». Occorre sinteticamente descrivere il modo in cui la procedura per addivenire ad un *consent order* si articola. Essa principia con un'*investigation*, svolta dalla FTC a fronte di una presunta violazione delle normative presidiate, che si conclude, in caso di positivo accertamento, con un *complaint* recante

Spostandoci sul versante sostanziale, nel contesto di tale procedura (ma non solo di questa) le due macrocategorie di condotte perseguite siccome *unlawful*, come abbiamo accennato, sono essenzialmente due: gli *unfair act or practices*, che identificherebbero tutte quelle condotte idonee a determinare una «*substantial injury*», purché tale che essa «*could non have been reasonably avoided*» e che non sia controbilanciata da «*countervailing benefits*»¹²⁴³; e i *deceptive acts or practices*, che si riscontrerebbe, secondo la stessa FTC «*if it involves a material statement or omission that is likely to mislead a consumer acting reasonably under the circumstances*», e dunque alla quale sono riconducibili tutte le false rappresentazioni, le omissioni o qualsiasi altra pratica ingannevole che induca il consumatore ad agire in modo a sé stesso pregiudizievole¹²⁴⁴.

Ebbene, è proprio con riferimento a quest'ultima categoria che le teorizzazioni e l'attività della FTC hanno offerto, e possono offrire sempre più, quel presidio per l'*information privacy* dei consumatori-*data subjects* nel contesto dei processi decisionali automatizzati¹²⁴⁵. In particolare, a tale scopo il ruolo più importante apparirebbe fino ad ora essere stato svolto dalla fattispecie di c.d. «*broken promise of privacy*», che, approssimando, ricorrerebbe laddove il trattamento dei dati del *data subject* sia posto in essere in violazione della *privacy*

indicazioni circa gli illeciti commessi. A questo punto, il destinatario può impugnare il *complaint* davanti ad una Corte distrettuale o amministrativa, o piuttosto avviare un negoziato con la FTC che si conclude, appunto, con l'*agreement* in parola, in cui il soggetto s'impegna ad adottare le condotte ivi indicate per ripristinare l'osservanza della normativa *senza ammettere alcuna responsabilità*. Deda importanti riflessioni all'influenza esercitata sull'interpretazione giurisprudenziale da parte dei provvedimenti della FTC, e segnatamente dei *consent orders*, J. BRAUCHER, «Deception, Economic Loss and Mass-Market Customers: Consumer Protection Statutes as Persuasive, Authority in the Common Law of Fraud», 48, *Ariz. L. Rev.*, 2006, 829, 85. Cfr. anche la ricostruzione effettuata da C. TABARRINI, *La trasparenza algoritmica*, cit., p. 223 ss.

¹²⁴³ V. 5 U.S.C. § 45(n); e cfr. CHRIS HOOFNAGLE, *Federal Trade Commission: Privacy Law and Policy*, 2016, 132.

¹²⁴⁴ FEDERAL TRADE COMMISSION, *Big Data: A Tool for Inclusion or Exclusion?* (January 2016), p. 21.

¹²⁴⁵ Ivi, p. 22.

policy (e quindi, come sappiamo, l'informativa -dettagliata e "olistica" - sul trattamento) predisposta dall'*organisation* e accettata prima della fruizione del servizio¹²⁴⁶. Per citare solo un esempio, paradigmatico, di tale importanza, facciamo qui riferimento al caso *CompuCredit*, scaturito nel 2008 quando la FTC ha deciso di perseguire, con la procedura di cui alla lett. (b) del par. 45 prima brevemente descritta, una società di marketing nell'ambito delle carte di credito (la "CompuCredit Corporation") che, ad opinione della Commissione, avrebbe adottato pratiche "deceptive" nei confronti dei consumatori attraverso l'impiego di un sistema (chiaramente, algoritmico) di *behavioral scoring*¹²⁴⁷. La vicenda, a fronte dell'opposizione della società stessa al *complaint* della Commissione, approdava davanti alla *Court for the Northern District of Georgia (Atlanta Division)*, e si concludeva con un «*Order for Permanent injunction and other equitable relief*» che le censure articolate dalla FTC, e le corrispondenti misure correttive già indicate da questa come opportune nel provvedimento impugnato, sostanzialmente riproduceva. In sostanza, la FTC ha qualificato come *deceptive practice*, e segnatamente come ipotesi di *broken promise of privacy*, la condotta della società che, nel pubblicizzare la possibilità dei clienti di estendere - apparentemente senza controprestazioni- l'importo limite della propria carta, aveva omesso di informarli che, in conseguenza dell'utilizzo di un modello di *behavioral scoring*, la linea di credito sarebbe stata al contempo contratta in relazione ad un'eterogena categoria di spese (quali, ad esempio, quelle effettuate

¹²⁴⁶ Cfr. in particolare D.J. SOLOVE, W. HARTZOG, «The FTC and the New Common Law of Privacy», cit., 628 ss., che propongono tra l'altro la seguente classificazione: «*The types of broken promises cases include: promises to maintain confidentiality or to refrain from disclosing information to third parties; promises to only collect data consistent with the company's privacy policy; promises to provide adequate security for personal data; promises to maintain anonymity; and promises not to disclose personal data to third parties by selling in bankruptcy proceedings*».

¹²⁴⁷ *FTC v. CompuCredit Corporation e Jefferson Capital Systems, LLC*. Civil No. 1:08-CV-1976- BBM-RGV 2008, riportato in FEDERAL TRADE COMMISSION, *Big Data: A Tool for Inclusion or Exclusion?*, Gennaio 2016, p. 22.

per consulenti personali e matrimoniali e per saloni di bellezza)¹²⁴⁸. Il caso, insomma, evidenzia come la fattispecie in questione abbia consentito e possa consentire alla FTC di scongiurare l'attitudine potenzialmente lesiva dei sistemi decisionali algoritmici sulla libertà di autodeterminazione degli individui, pur considerati alla sola stregua di consumatori, in special modo rafforzando (o meglio, garantendo rigorosamente l'osservanza) dei doveri di trasparenza insistenti in capo alle *companies-data controllers*.

All'esito del sintetico quadro qui tracciato, si può allora affermare come, pur in assenza di qualsiasi specifico riferimento al fenomeno dei processi decisionali interamente automatizzati, la *Section 5* del FTC offra in realtà naturale protezione anche a fronte di tale fattispecie, tutte le volte che queste ricadano nelle due larghe categorie - suscettibili di duttili ed evolutivamente orientate interpretazioni - di *unfair and/or deceptive acts (or practices)*, dacché condotte di tal sorta ben possono essere poste in essere (e, nel nostro tempo, sempre più lo sono e lo saranno) per mezzo di - o piuttosto *da* - sistemi algoritmici.

Se la dottrina, come abbiamo visto, ha già sottolineato l'idoneità dell'interpretazione seguita dalla FTC nello svolgimento del proprio ruolo di *enforcement* dei *consumer protection statues* in punto di *privacy* a configurare un

¹²⁴⁸ Si veda più nello specifico il *Complaint for Permanent Injunction* emesso dalla *Federal Trade Commission* all'esito della procedura di cui alla lett. (b) del par. 45 in esame, che a p. 34 recita: «*CompuCredit has based these credit line reductions on an undisclosed "behavioral" scoring model that penalized consumers for using their cards for certain types of transactions, including transactions touted in their solicitation materials such as cash advances and transactions with the following types of merchants Direct marketing merchants, Marriage counselors, Personal counselors, Automobile tire retreading and repair shops, Bars and night clubs, Pool and billiard establishments, Pawnshops, Massage parlors*». V. *Federal Trade Commission v. CompuCredit Corporation e Jefferson Capital Systems, LLC*. Civil No. 1:08-CV-1976- BBM-RGV, 10 giugno 2008, reperibile qui: <https://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditchmptsignd.pdf>

vero e proprio “*new common law of privacy*”¹²⁴⁹, a reale conclusione del paragrafo non si può non fare un breve riferimento a quelle proposte dottrinali che, guardando al futuro, valorizzano le previsioni della *Section 18* dell’FTC. Quest’ultima, infatti, attribuisce alla FTC sia una potestà normativa “non legislativa”, consistente nel potere di adottare «*interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices*» (c.d. *non-legislative guidance*), sia una potestà normativa di segno legislativo, o piuttosto di adottare norme giuridiche vincolanti nei settori di sua competenza, ossia «*rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce*», definita anche potestà di *Magnuson-Moss rulemaking*¹²⁵⁰.

Ebbene, se la FTC ha fino ad ora prediletto lo strumento della *non legislative guidance*, sia attraverso i *consent orders* sia attraverso l’adozione di vere e proprie linee guida, recente dottrina, anche alla luce di alcuni casi emblematici, ha sottolineato come nonostante l’estrema “volubilità” della *data driven society*, che porterebbe a prediligere un approccio flessibile e di natura casistica, seppur inferendone principi che hanno la tendenza a diffondersi nella prassi alla luce dell’autorevolezza della fonte (essenzialmente, sono quelli sanciti nei *consent order agreements* dalla la FTC nei casi “macroscopici” suddetti), dall’altra l’esercizio della potestà di c.d. *Magnuson-Moss RuleMaking* rappresenterebbe un buon compromesso, in quanto meno complessa e di portata più generale rispetto alle procedure amministrative esperibili dietro *notice*, ma

¹²⁴⁹ Cfr. ancora D.J. SOLOVE, W. HARTZOG, «The FTC and the New Common Law of Privacy», cit., 628 ss

¹²⁵⁰ V. 15 USCA § 57a (a)(1)(A) e (B). Per la ricostruzione delle proposte *de iure condendo*, il debito principale è con C. TABARRINI, *La trasparenza algoritmica*, cit., p. 228 ss.; cfr. anche FEDERAL TRADE COMMISSION, *Privacy & Data Security Update: An Overview Of The Commission’s Enforcement, Policy Initiatives, And Consumer Outreach And Business Guidance In The Areas Of Privacy And Data Security*, 2017;

allo stesso tempo più flessibile e più al riparo dal pericolo di “obsloescenza normativa” degli interventi ad opera del legislatore¹²⁵¹.

Insomma, per tali proposte, il futuro della *data privacy* giacerebbe in una strategia di «*hybrid rulemaking*»¹²⁵², che ovvi all’assenza di un quadro normativo federale unitario senza “sclerotizzare” l’incessante divenire della tecnologia, e conseguentemente delle risposte alle istanze mutevoli di protezione che percorrono il corpo sociale, in una trama di categorie tendenti all’obsolescenza.

Per vedere se un approccio simile possa soddisfare quelle aspettative sempre maggiori di integrità della sfera privata, direttamente proporzionali alla sempre maggior contrazione di uno spazio di imperscrutabilità del pensiero, scaturenti dall’ubiquità della tecnologia, non resta che attendere l’eventuale implementazione in concreto di tale “forma” di *rulemaking*.

¹²⁵¹ Le proposte in parola possono rintracciarsi in Cfr. G.M. STEGMAIER, W. BARTNICK, P«sychics, Russian Roulette, and Data Security: The FTC’s Hidden Data Security Requirements», 20 *Geo. Mason L. Rev.*, 2013, 673, 713; P. STRAUSS, T. RAKOFF, C. FARINA, G. METZGER, *Gellhorn and Byse's Administrative Law: Cases and Comments*, XI ed., Foundation Press, 2011, 129. Cfr. T. GARVEY, *A Brief Overview of Rulemaking and Judicial Review*, Congressional Research Service, 2017, p. 4 ss.. Uno dei casi emblematici cui si fa riferimento è *LabMD, Inc.*, FTC File No. 102-3099, No. C-9357, 9 (F.T.C. July 29, 2016). Cfr. J. KOSSEFF, *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020, 10ss. Ivi, un laboratorio analisi privato era stato accusato di aver posto in essere “*unfair data security practices*” sfociate poi in un massiccio accesso non autorizzato a dati sanitari particolarmente sensibili della propria clientela, resi pubblicamente accessibili online: ebbene, non solo il laboratorio rifiutò l’accordo transattivo proposto dalla Commissione, ma la Corte davanti al quale fu impugnato il *complaint* diede ragione alla società, ritenendo necessaria la prova della probabilità del verificarsi dell’evento dannoso. Il caso in questione testimonia della non costante efficacia del sistema di vigilanza basato su *consent orders* implementato tradizionalmente dalla FTC, e dunque nella fiducia da questa riposta nella spontanea recezione nella prassi dei rapporti tra business e consumatori delle *case rules* (per i *defendants* vincolanti, per i terzi soft) esplicitate negli agreements raggiunti. Del caso parla C. Tabarrini, La trasparenza algoritmica, cit., p. 230 ss. Cfr. per un commento del caso J. KOSSEFF, *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020, 10ss.

¹²⁵² Cfr. ancora *A Brief Overview of Rulemaking and Judicial Review*, Congressional Research Service, 2017.

4.4. *California Consumer Privacy Act*: il modello giuridico di riferimento della legislazione statale in materia di *data privacy*. Un passo avanti: il recente *Draft for Automated Decisionmaking Technology Regulations*

L'obiettivo che ci siamo dati nei paragrafi precedenti era quello di esplorare, in un'ottica di comparazione con il modello europeo, la frammentaria disciplina (positiva e giurisprudenziale) statunitense della *data privacy*: per ricostruire, dove esistenti, quei sub-sistemi normativi che, per quanto settoriali, offrissero una regolamentazione dello specifico fenomeno dei trattamenti automatizzati, e più nello specifico del *decision making* algoritmico. Pertanto, coltivando l'intenzione - in conformità di quella *tendenza fondamentale* che costituisce l'oggetto ultimo della nostra complessiva indagine - di sondare l'idoneità degli strumenti in questione a rispondere alle nuove istanze di protezione della sfera privata scaturite nel corpo sociale dagli sviluppi trans-settoriali della tecnologia, in un contesto interazionale che trascende sempre più i confini materiali e dunque anche nazionali, la nostra prospettiva privilegiata non poteva che essere quella del diritto federale.

Studiare lo stato della disciplina della *data privacy*, e, nel suo ambito, di quella dei sistemi di ADM (laddove esistente), in ciascuno dei singoli ordinamenti dei (ricordiamo, 50) Stati federati sarebbe, ovviamente, esercizio che trascende le facoltà di chi scrive, e potrebbe al più costituire oggetto di autonoma trattazione. Approssimando, vorrebbe dire prendere in considerazione e valorizzare innanzitutto le differenze tra i rispettivi contesti culturali e tra i rispettivi sistemi giuridici, nel cui orizzonte vanno necessariamente inquadrare le rispettive normative (anche qui, dove esistenti); ma soprattutto, vorrebbe dire focalizzarsi sull'intrico di precedenti che caratterizza il *common law* di ciascuno di essi, spesso, pur in relazione ad una stessa "classe di fattispecie", profondamente

distinto da Stato a Stato, dove non campeggi una uniforme e pervasiva disciplina federale.

Tuttavia, dal momento che il nostro scopo resta quello di individuare quelle manifestazioni dell'esperienza giuridica statunitense che testimonino la sensibilità delle istituzioni e degli operatori del diritto rispetto alla necessità che l'ordinamento evolva per rispondere a tutte le trasformazioni del panorama tecnosociale globale, prima di avviarci alle conclusioni possiamo spostare, pur sinteticamente, il nostro sguardo sul piano statale. E qui, ai nostri fini, appare assai utile prendere in considerazione quello che nell'intero panorama statunitense ha storicamente rappresentato il primo tentativo (seppur a livello statale) di introduzione di una disciplina generale, unitaria e sistematica in materia di *data privacy*. Ci riferiamo al *California Consumer Privacy Act* (CCPA), entrato inizialmente in vigore il primo gennaio del 2020, e successivamente modificato per effetto dell'approvazione del c.d. *California Privacy Rights Act* del 2020, di modo che la sua versione emendata e attualmente vigente risulta entrata in vigore il primo gennaio del 2023¹²⁵³. Stante la recente introduzione della normativa, ci si limiterà ad abbozzare l'architettura normativa edificata dall'atto in parola, individuando le definizioni, i principi e gli istituti che cruciali appaiono ai fini di

¹²⁵³ CAL. CIV. CODE §§ 1798.100-.192 (West 2018), *as amended by California Privacy Rights Act of 2020* (CPRA). Sul punto, i contributi della dottrina, stante la recente introduzione della normativa, vanno infittendosi con il tempo, e vedono contrapporsi voci più entusiaste a letture più critiche dell'architettura delineata, anche in relazione al sistema costituzionale californiano: per alcuni riscontri, di tenore eterogeneo, cui si deve per la maggior parte la sintetica ricostruzione della disciplina che qui seguirà, cfr. A.C. RAUL, C.C. FRONZONE, S.S. TAPIA, «United States», in A.C. Raul (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Ltd, Londra, 2019, 416ss.; N.F. III PALMIERI, «Data Protection in an Increasingly Globalized World», 94, *Ind. L.J.*, 2019, 297, 298-306; W.C. FREEMAN, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, Congressional Research Service, novembre 2018; W. HARTZOG, N. RICHARDS, «Privacy's Constitutional Moment and the Limits of Data Protection», 61, *Boston College Law Review*, 2020, 1687ss.

una valutazione della sua idoneità a garantire il bilanciamento tra interessi dei *data subjects*, pur sempre concepiti alla sola stregua di *consumers*, e contrapposti interessi economici dei *data controllers*, interrogandoci sulle analogie e le differenze che corrono, ancora una volta, rispetto al modello rappresentato dal GDPR. In ultima battuta dedicheremo alcune riflessioni al recentissimo progetto, presentato dalla *California Privacy Protection Agency* (CPPA) al relativo *board meeting* dell'8 dicembre 2023, diretto ad integrare - o meglio, declinare - nel dettaglio, a livello secondario, la disciplina prevista dal CCPA in materia di *ADM systems* (non dedicando la normativa primaria alla fattispecie, lo si anticipa, alcuna disposizione specifica), rafforzando opportunamente i diritti dei *data subjects*¹²⁵⁴.

Possiamo introdurci all'analisi svolgendo una breve ricostruzione del panorama normativo statale negli anni in cui il CCPA è stato adottato. Già nel 2015, infatti, si notava come nella maggior parte dei 50 Stati della Federazione si riscontrassero proposte di legge preordinate a rafforzare i *requirements* imposti ai *businesses* in relazione alla raccolta e al trattamento di informazioni relative ai consumatori, in particolar modo rispetto al livello federale; e come almeno dieci Stati (tra questi, la California, la South Carolina, la Florida e l'Illinois) contemplassero ciascuno nelle proprie Costituzioni una previsione a tutela del *right to (data) privacy*¹²⁵⁵. Altrettanto elevato (pari a 47) era il numero degli Stati dotato di c.d. *security breach notification laws*, deputate a conferire agli interessati il diritto di ottenere una *notice* circa l'eventuale compromissione della

¹²⁵⁴ Cfr. già da ora CALIFORNIA PRIVACY PROTECTION AGENCY, *Draft for Automated Decisionmaking Technology Regulations*, December 2023, https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf

¹²⁵⁵ Cfr. S. COBB, «U.S. Data Privacy Legislation», cit., p. 6; per un riscontro cfr. NATIONAL CONFERENCE OF STATE LEGISLATURES (2015a) *Privacy Protections in State Constitutions*, <http://www.ncsl.org/research/telecommunication-s-and-information-technology/privacy-protections-in-state-constitutions.aspx>

sicurezza dei propri dati¹²⁵⁶. Tuttavia, almeno fino all'adozione del CCPA, non era dato riscontrare nei singoli Stati alcuna normativa “onnicomprensiva” in materia di *data privacy and protection*, pur inerente al solo settore dei rapporti privati di natura commerciale, e dunque intercorrente tra *businesses* ed individui concepiti come *consumers*, e pertanto “*across all industry sectors*” e relativa a qualsiasi tipologia di dato¹²⁵⁷. La predisposizione, l'adozione e la successiva entrata in vigore dell'atto che ci accingiamo ad analizzare ha rivoluzionato il quadro, promuovendo nei singoli Stati il dibattito circa l'opportunità di introdurre un *legal framework* unitario in materia per far fronte ai pericoli esistenti nel contesto della *data driven-society*¹²⁵⁸.

Guardando, infatti, al panorama attualmente vigente, non si può ignorare come l'introduzione della normativa di cui ora ci occuperemo abbia innescato una virtuosa spirale, aprendo la strada non solo ad un'ulteriore proliferazione della normativa settoriale (come quella in materia di *data brokerage* o di *children's*

¹²⁵⁶ *Ibidem*. Cfr. per un riscontro NATIONAL CONFERENCE OF STATE LEGISLATURES (2015b) *Security Breach Notification Laws*, <http://www.ncsl.org/research/telecommunication-s-and-information-technology/security-breach-notification-laws.aspx>

¹²⁵⁷ Cfr. W.C. FREEMAN, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, Congressional Research Service, novembre 2018, p. 1

¹²⁵⁸ Cfr. infatti il panorama della legislazione statale, in vigore così come in fieri, che emerge da NATIONAL CONFERENCE OF STATE LEGISLATURES, *2019 Consumer Data Privacy Legislation* disponibile all'indirizzo www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx. Ne risulta che nel 2018 stesso, anno in cui il CCPA è stato adottato, lo Stato del Vermont ha infatti adottato una disciplina relativa ad un determinato profilo della *data privacy*, e in particolare configurante in capo ai data broker doveri più dettagliati di *disclosure* ai *data subjects* delle loro informazioni oggetto di trattamento, e attribuendo ai secondo un vero e proprio diritto di opt out rispetto alla “data collection”. Lo stesso report annuale rileva come «*The year 2019 began with a significant increase in bill introductions addressing various aspects of data privacy, compared to previous years*»: a prescindere dall'analitica ricognizione di tutte le normative, pur sempre *sector-specific* e non dunque generali come il CCPA, adottate nei singoli Stati nell'anno di cui si parla, ciò che merita sottolineare è come in almeno 25 Stati fossero in discussione proposte legislative in materia di *data privacy*, alcune anche onnicomprensive (parallelamente a quelle già nell'anno medesimo fallite, come la proposta del *Mississippi Consumer Privacy Act*), come quella proposta nello Stato di New York «*It's Your Data Act*» volta a dettare un generale regime di tutela in materia di protezione dei dati personali.

online privacy), ma soprattutto all'introduzione in alcuni degli Stati Federati di regimi normativi generali in punto di *data privacy*, seppur limitati al settore dei rapporti commerciali. Infatti già prima del 2023, accanto alla California, anche Colorado¹²⁵⁹, Connecticut¹²⁶⁰, Utah¹²⁶¹ e Virginia¹²⁶² si sono dotate di «*comprehensive consumer data privacy laws*», tutte attualmente entrate in vigore, nelle quali, nonostante alcune indiscutibili differenze - anche importanti - a livello di singoli istituti (su tutti, la scelta del principio di *opt-in* o piuttosto di *opt-out* come pilastro della disciplina dei fondamenti di liceità del trattamento), non può non riscontrarsi, a cominciare dalla struttura e dalle finalità, un debito con il modello giuridico rappresentato dal CCPA. In questo senso, e in prima approssimazione, può ben parlarsi nella specie di un fenomeno di circolazione di un modello giuridico¹²⁶³.

Passiamo, allora, ad esaminare la struttura generale e i profili essenziali della disciplina dettata dalla prima *comprehensive consumer data privacy law* che gli Stati Uniti abbiano conosciuto, compresi i suoi principali limiti; interrogandoci, poi, sulla possibilità di desumerne un regime rafforzato applicabile alla materia dei processi decisionali interamente automatizzati.

¹²⁵⁹ *Colorado Privacy Act*, 2021 SB 190 (Colo. Rev. Stat. §6-1-1301 et seq.)

¹²⁶⁰ *Connecticut Personal Data Privacy and Online Monitoring* (2022 SB 6)

¹²⁶¹ *Utah Consumer Privacy Act*, 2022 SB 227 (Utah Code Ann. §13-61-101 et seq. – Effective Dec. 31, 2023.)

¹²⁶² *Virginia Consumer Data Protection Act* (Va. Code §59.1-575 et seq.)

¹²⁶³ Cfr. ancora una volta la ricognizione operata nel più recente NATIONAL CONFERENCE OF STATE LEGISLATURES, *2023 Consumer Data Privacy Legislation*, disponibile all'indirizzo <https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation#:~:text=Relates%20to%20personal%20data%20privacy,to%20reveal%20a%20trade%20secret>. L'ente riscontra come « *consumer privacy issues have grown in importance in state legislatures recently, including in 2023*»; e, soprattutto, come accanto al solito *enacting*

di normative sector specific in ambito *data privacy* (parrebbero essere stati introdotti o discussi in 40 Stati, nel loro complesso, ben 350 *privacy bills*!), altri 8 Stati abbiano adottato una normativa onnicomprensiva in materia di *consumer (data) privacy*, destinate ad entrare in vigore nei prossimi anni: questi sono Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee e Texas.

Innanzitutto, bisogna individuare lo specifico ambito di applicazione della normativa, collocata nel Codice Civile della California. Il CCPA, come emerge già dal par. 1798.100, rubricato «*General Duties of Businesses that Collect Personal Information*», risulta invero dettare una disciplina confinata alla specifica dimensione dei rapporti commerciali, laddove per la maggior parte risulta applicabile a qualsiasi «*business*» che tratti (o meglio, «*collects*») le «*personal information*» di un «*consumers*», essenzialmente per finalità “commerciali” («*business purposes*»)¹²⁶⁴. Nella definizione che abbiamo adottato per circoscrivere il perimetro applicativo della normativa, già si rinvencono tutti i concetti la cui definizione risulta essenziale per delimitare, oggettivamente così come soggettivamente, tale perimetro. Tuttavia, è prima necessario rilevare come l’atto sia ancora figlio di quell’approccio, tipico del contesto ordinamentale che abbiamo studiato e descritto nel nostro lavoro, che concepisce la *data privacy (and protection)* come un *aspetto* della più generale *consumer protection*: così, nella configurazione dei diritti dell’interessato, rischiando (si vedrà in che termini) di svilirne la strumentalità a presidiare alcuni attributi fondamentali della persona, piuttosto che il solo interesse economico alla gestione del dato quale bene giuridico patrimoniale¹²⁶⁵.

Il CCPA delinea in modo preciso la definizione di ciascuna delle suddette categorie, articolandole tutte nel nutrito par. 1798.40. La più semplice è senza dubbio quella di «*consumer*» (concetto che in contesto euronunitario, traslato nello specifico ambito della *data privacy*, equivale alla nozione di «interessato»), che,

¹²⁶⁴ Cfr. W.C. FREEMAN, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, cit., p. 2 ss.

¹²⁶⁵ Più in generale, sulle problematiche di un approccio esclusivamente “consumeristico”, nonché “mercataista”, alla dimensione della protezione dei dati personali, cfr. ex multis G. ALPA, «La proprietà dei dati personali», in *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 30.

in sostanza, identifica qualsiasi persona fisica residente nello Stato della California¹²⁶⁶. Più complessa appare, invece, la definizione di «*business*» (che in contesto eurounitario, nel senso sopra specificato, equivale alla nozione di «titolare del trattamento») appare più complessa: sostanzialmente, prescindendosi dalle modalità di trattamento dei dati e dallo specifico settore commerciale in cui operi, ricade nella categoria qualsiasi «*company*» che raccolga le «*personal information*» (la cui controversa definizione affronteremo a breve) di un *consumer* come sopra definito, e lo faccia «*for profit*» (dunque per scopo di lucro), svolgendo la propria attività economica (anche) sul territorio della California; a ciò la previsione aggiunge la necessità di soddisfare alternativamente la condizione per cui la *company* guadagni più di 25 milioni in «*annual gross revenues*», o piuttosto che intraprenda la compravendita di più di 50.000 informazioni relative ai *Californian resident*, o ancora che il 50% dei propri annuali ricavi derivi sostanzialmente dalla compravendita dei dati suddetti¹²⁶⁷. In dottrina è stata prontamente sottolineata l'idoneità della definizione in parola a ricomprendere nella categoria medesima una composita ed invero vasta platea di

¹²⁶⁶ V. CAL. CIV. CODE §§ 1798.140 (i).

¹²⁶⁷ Ivi, lett. (d). Le condizioni, in particolare sono così definite nel testo: «(A) *As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185; (B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households; (C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information*». La necessità che, in qualsiasi caso, il *business* svolga almeno parzialmente la propria attività nel territorio della California, pur rappresentando un presupposto facilmente integrabile, si spiega anche con l'impossibilità di introdurre clausole di "estensione" dell'efficacia territoriale della disciplina come quelle previste dal GDPR (art. 3), in quanto capaci di produrre costituzionalmente illegittime interferenze nella libertà di commercio garantita agli attori economici in ogni Stato. Per una panoramica su tale problematica, e sulla stessa c.d. *Dormant Commerce Clause* (dottrina di matrice giurisprudenziale applicata per invalidare le disposizioni statali aventi effetti discriminatori verso attori che operano al di fuori del singolo Stato interessato), cfr. N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», 11, *Hastings Sci. & Tech. L.J.*, 2020, 37, 48.

operatori economici, risultando sufficiente a titolo esemplificativo la semplice apertura di un sito web accessibile anche in California affinché un relativamente “*small business*” possa soddisfare, quanto meno, la seconda delle condizioni suddette¹²⁶⁸.

Altra definizione fondamentale è quella, naturalmente, di «*personal information*», che il legislatore californiano, alla lett. (v) n. 1, identifica in qualsiasi «*information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*»¹²⁶⁹: le lettere in cui a sua volta si articola il n.1 individuano una serie nutrita di informazioni, molte delle quali ricalcano le definizioni adottate nel GDPR, a dimostrazione del debito che il CCPA riconosce nei confronti dell'avanzata normativa generale vigente in contesto eurounitario¹²⁷⁰. Tra queste, tuttavia, originali e meritevoli di menzione, stante lo scopo del nostro lavoro, sono certamente le *informazioni inferite* di cui alla lett. (K), la cui definizione è strettamente aderente a quella che già la dottrina - più volte richiamata - ha messo in luce, essenzialmente identificandosi nelle *informazioni derivate da preesistenti informazioni* allo scopo di classificare l'individuo sulla base di determinati aspetti della sua personalità¹²⁷¹. Tale nozione,

¹²⁶⁸ Cfr. W.C. FREEMAN, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, cit., p. 2 ss.

¹²⁶⁹ CAL. CIV. CODE §1798.140 (v)(1).

¹²⁷⁰ Ivi, (v) 1; v. la subspecie degli *identifiers* alla lett. A), che esplicitamente vi ricomprende gli Indirizzi IP, nella lettera del GDPR assente ma, come sappiamo, pacificamente ascrivibile al perimetro dell'art. 4 par. 1 anche alla luce della sentenza *Breyer*. E v. anche quella di *biometric information* di cui alla lett. E; e di *sensitive personal information* di cui alla lett. L. Ricordiamo poi che dalla categoria esulano le c.d. *de-identified information*, ex lett. (h), e le *aggregated information* ex lett. (a), n. 5.

¹²⁷¹ Ivi, (v), (1), lett. (K), che appunto nella categoria in parola ascrive «*Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.*» Altra subspecie che appare indice di una consapevolezza dell'attuale panorama tecnosociale risulta quella di cui alla lett. (F), che identifica un'informazione personale anche in «*internet or other electronic network activity information, including, but not limited to, browsing history, search history,*

esplicitando un profilo assente nella stessa lettera dell'art. 4 del GDPR, pare riflettere una concezione estremamente contemporanea di dato personale, che riconosce l'attitudine delle macchine a creare nuove informazioni, attraverso l'applicazione e, nei sistemi più avanzati, la stessa creazione e trasformazione della formula logico-matematica applicata all'elaborazione dell'input. Ci sia consentito notare che una definizione simile, dove mutuata a livello federale, concorrerebbe a garantire in capo agli individui un effettivo diritto alla c.d. *disclosure*, e quindi di accesso, ai dati che - per restare nel quadro della *credit industry* - l'algoritmo di *credit scoring* abbia complessivamente "impiegato" per elaborare l'output; e, al contempo, dove declinato anche in contesto europeo, amplificherebbe l'effettività dello stesso diritto ad ottenere informazioni significative (che, in tal modo, agli stessi *inferred data* allargherebbe per definizione il proprio perimetro) a fronte di processi decisionali interamente automatizzati sancito dal subsistema edificato dall'art. 22 e dagli art. 13-15 del GDPR¹²⁷².

Spostandoci sul versante della disciplina sostanziale, occorre passare brevemente in rassegna l'insieme dei principi che individuano i presupposti di liceità della raccolta delle *personal information*, esplorando il panorama di

and information regarding a consumer's interaction with an internet website application, or advertisement»; invero, quest'ultima appare in una certa misura *technology dependent*, ma è pur vero che il Web (almeno 2.0) va ormai considerato, da qui al futuro, attributo indefettibile dello statuto di qualsiasi società tecnologicamente organizzata.

¹²⁷² Affiora prepotentemente qui la nozione di matrice dottrinale, già spesso introdotta e commentata, di *algo-created data*, di cui discorre anche R. MESSINETTI, «Privacy e identità digitale», cit.; e la classificazione su cui già più volte siamo tornati secondo l'origine del dato proposta da ABRAMS, «Origins of Personal Data and its Implications for Governance», in *The Information Accountability Foundation*, marzo 2014, in <http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf>, che individua le quattro categorie dei *provided, observed, derived and inferred data*, constatando come le ultime tre comportino un basso livello di consapevolezza per l'interessato.

posizioni giuridiche definite dalla normativa in capo ai *businesses* ed ai *consumers* (principi dalla dottrina sintetizzati nella formula «*stewartship*»)¹²⁷³.

Ebbene, la principale differenza tra il modello giuridico, pur “onnicomprensivo”, implementato dal legislatore californiano, e quello che caratterizza il contesto eurounitario sussiste proprio in punto di individuazione, e conseguentemente di disciplina, delle basi giuridiche del trattamento (*rectius*, della «*collection*»). Infatti, almeno in relazione ai trattamenti primari, il primo parrebbe rappresentare un *consent-based model*, ma nel solo senso di ritenere genericamente lecito il trattamento dei dati raccolti presso l’interessato quando questi abbia accettato le *privacy policies* che all’atto della raccolta i *businesses* abbiano somministrato al *consumer*, disinteressandosi di prescrivere quei requisiti specifici di validità cui larga attenzione dedica il legislatore europeo all’art. 4 par. 1 n. 11 del GDPR¹²⁷⁴. Per il resto, il CCPA non individua un sistema tassativo di basi giuridiche che, al pari delle fattispecie individuate dall’art. 6 del GDPR, condizioni a priori la liceità del trattamento: e ciò viene da alcuni commentatori imputato alla difficoltà di articolare un sistema di limiti al trattamento dei dati personali in quanto concepita dalla giurisprudenza costituzionale (anch’essa)

¹²⁷³ Sul punto, cfr. la suddivisione seguita da Così N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», cit., che oltre a questa dimensione distingue il profilo del “*balance of harms*” (valutazione costi-benefici per la definizione dei mezzi e delle finalità del trattamento) e “*redressability*” (rimedi a disposizione degli interessati danneggiati da violazioni commesse dal titolare del trattamento)

¹²⁷⁴ Cfr. in particolare JAMES P. NEHF, «Incomparability and the Passive Virtues of Ad Hoc Privacy Policy», 76 *U. Colo. L. Rev.* 1, 4–18 (2005); ma soprattutto N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», cit. p 41 ss, che pone in luce i profili su cui già ci siamo ampiamente soffermati in sede di commento del GDPR e del fondamento di liceità generale rappresentato dal consenso qualificato, ossia quello del take-it-or-leave-it, affermando che nelle *privacy policies* predisposte dai business «*consent is rarely actually “informed”*».

come *libertà fondamentale*, ricondotta alla più generale libertà di manifestazione del pensiero tutelata dal Primo Emendamento¹²⁷⁵.

A fronte dell'assenza di tale sistema fondamentale di basi giuridiche, la disciplina del trattamento, secondo un modello in realtà tipico delle varie esperienze normative statali così come federali in punto di (*sector specific*) *data privacy*, e conseguentemente il bilanciamento tra interessi dei *businesses* e quelli dei *consumers*, si articola nella definizione puntuale dei doveri di informazione del *business*, cui corrispondono determinati diritti dei *consumers*¹²⁷⁶. A dimostrazione della centralità di tale *corpus* normativo, il CCPA si apre con il sistema di doveri in parola, articolati dalle diverse lettere in cui è suddiviso il par. 1798.100: il modello adottato è, segnatamente, quello di c.d. *notice-and-consent*, nella misura in cui si fonda su obblighi di notifica *ex ante* imposti ai *businesses*, indipendentemente dalla fonte del dato, preordinati a far conoscere agli interessati quali siano le informazioni (già) raccolte (ed eventualmente la loro natura “*sensitive*”), le finalità di utilizzo delle medesime, la durata della loro conservazione ed eventuali modifiche del trattamento rispetto ad una precedente notifica¹²⁷⁷.

¹²⁷⁵ Il discorso è complesso, ma cfr. i due importanti contributi di P.M. SCHWARTZ, K.N. PEIFER, «Transatlantic Data Privacy Law», 106, *Geo. L.J.*, 2017, 115, 134ss; C.J. COLE, N. COULSON, *California V. GDPR: Compare and Contrast*, Wolters Kluwer Legal Insights, 20 settembre 2018. Per una ricognizione in punto di trattamento dei dati personali come oggetto di un autonomo diritto, espressione non solo del diritto d'iniziativa economica privatata e in ogni caso costituzionalmente tutelato, cfr. C. TABARRINI, *La trasparenza algoritmica*, cit.

¹²⁷⁶ Cfr. ancora la ricognizione operata da N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», cit., p. 48 ss.; e da W.C. FREEMAN, «California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress», cit.

¹²⁷⁷ I doveri in parola sono puntualmente articolati in CAL. CIV. CODE §§ 1798.100, la cui lettera (a), prescrive «*A business that controls the collection of a consumer's personal information shall, at or before the point of collection, inform consumers of the following: (1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed*

Alla specifica trama di doveri configurati in capo ai titolari del trattamento, corrisponde un sistema puntuale di diritti, enucleati dal par. 1798.105 e ss., che rappresentano le effettive garanzie previste dal CCPA a favore dei *consumers*: questi, procedendo ad una rapida carrellata e seguendo l'ordine in cui li articola la normativa, in seguito alla novella del 2020 - e dunque nella versione della legge attualmente vigente -, sono il «*right to delete personal information*» (1798.105); il «*right to correct inaccurate personal information*» (1798.106); il «*right to know what personal information is being collected*», completato dal «*right to access*» (1798.110); il «*right to opt out*» che consegue al diritto di conoscere «*what personal information are sold and to whom*» (1798.115-120), nonché il *right to not discrimination* (riconducibile al dettato del par. 1798.125.) e il *right to limite use and disclosure of sensitive information* (1798.121)¹²⁷⁸.

Svolgendo una succinta analisi di taluni delle posizioni giuridiche elencate, sicuramente, accanto al *right to know* che rappresenta la speculare declinazione in chiave attiva del dovere di *notice* gravante sul *business*, e al *right to delete*, grande centralità assume il *right to opt out*, che fondamentalmente si identifica in un *diritto di opposizione alla vendita dei propri dati personali*, introdotto dal legislatore californiano - secondo alcune voci - per reagire al sistema di *take it or leave it* e alla sostanziale inconsapevolezza degli interessati in punto di utilizzo dei propri dati¹²⁷⁹. Per rafforzare tale diritto e agevolarne l'esercizio, accanto allo

purpose for which the personal information was collected without providing the consumer with notice consistent with this section». Cfr. Anche P.M. SCHWARTZ, «The EU-US Privacy Collision», 126, *Harv. L. Rev.*, 2013, 1966, 1976, che pone in luce il «*fundamental dilemma of notice*», individuando le criticità del modello del notice-and consent nella difficoltà di contemperamento tra le istanze di comprensibilità degli interessati e quelle di esaustivo tecnicismo delle Autorità di vigilanza.

¹²⁷⁸ Cfr. per una ricognizione generale W.C. FREEMAN, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress*, cit. p. 3 ss.

¹²⁷⁹ V. CAL. CIV. CODE §1798.120. (a) che recita «*A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer's personal information. This right may be referred to as the right to opt-out of sale or sharing*». Sulla lettura proposta, cfr. Cfr. N.

strutturale dovere di *notice*, ribadito dalla lett. b, il CCPA a livello di dettaglio dispone l'inclusione di un «*clear and conspicuous link*» nella pagina iniziale del sito web di ogni business recante la dicitura «*Do Not Sell My Personal Information*» e vieta contestualmente agli imprenditori, laddove il *consumer* abbia esercitato il diritto in parola, di sottoporli nuove richieste di consenso alla vendita dei suoi dati personali per i dodici mesi successivi¹²⁸⁰. Il risvolto negativo del diritto in questione consiste nel fatto che la sua previsione necessariamente dimidia l'effettività dell'approccio *consent-based* (rispetto a quello del consenso informato di matrice eurounitaria), dal momento che il *business* risulta ammesso a desumere il consenso al trattamento da parte del *consumer* dal suo semplice rifiuto di esercitare il *right to opt out* opportunamente segnalato. Pur presidiato dallo strumentale *right to not discrimination*, ossia a che «*a business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title*», tale regime appare difficilmente capace di contrastare il fenomeno dell'«accettazione per stanchezza» (*consent fatigue*) che caratterizza il contesto della attuale società digitale, rispetto piuttosto ad un modello basato sul principio del consenso preventivo e qualificato quale fondamento generale di liceità del trattamento, come è appunto quello risultante dal GDPR¹²⁸¹.

Spostandoci ora sul piano del *balance of harm*, possiamo affermare come il CCPA, a differenza del GDPR incentrato sui principi di *privacy by design* e *by*

RICHARDS, W. HARTZOG, «The Pathologies of Digital Consent», 96 Wash. U. L. Rev., 2019, 1461. e ancora N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», cit..

¹²⁸⁰ V. CAL. CIV. CODE §§ 1798.135 (a), rispettivamente (1) e (5).

¹²⁸¹ Per una posizione critica sul modello di *opting-out*, cfr. R.C. WILLIAMS, «Due Process, Class Action Opt Outs, and the Right Not to Sue», 115, Colum. L. Rev., 2015, 599, 615; cfr. anche N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», cit., p. 41 ss.

default in cui si articola il principio di *accountability*, non ha prescritto obblighi puntuali in capo ai *businesses* in punto di gestione e di bilanciamento dei rischi derivanti dalle prassi aziendali nel trattamento (*collecting, use, selling*), dei dati dei *consumers*. In letteratura, tale scelta è stata ricondotta alla criticata tendenza dell'ordinamento statunitense a non dotarsi di regole che dettino standard di sicurezza comuni in materia di *data privacy*, e dunque che promuovano un approccio *risk based* (simile, in sostanza, a quello accolto dal GDPR), basato sulla prevenzione (ipoteticamente, sin dalla progettazione del trattamento) dei rischi di lesione dell'*information privacy*, e degli altri interessi tutelati in capo ai *consumers*, scaturenti dal trattamento¹²⁸².

Tale lacuna appare ancora più grave nella misura in cui, come si può constatare dal dato letterale, seppur sia ormai pacificamente riconosciuto il carattere algoritmico dei trattamenti di dati nel contesto della società datificata, nessuna norma del CCPA risulti specificamente dedicata (segnatamente allo scopo di costruire un sistema di garanzie rafforzato per gli interessi fondamentali - prima ancora che economici - degli individui-*consumers*) al fenomeno dei processi decisionali interamente automatizzati.

Tuttavia, bisogna subito aggiungere che, in realtà, il legislatore californiano pare avveduto dei rischi che la nuova dimensione tecnologica possa configurare a carico della «*consumer's privacy or security*». Ciò si evince dal fatto che al par. 1798.185., nel definire e circoscrivere l'oggetto e l'estensione della *rulemaking authority* imputata, a decorrere dal 1° luglio 2021, all'Agenzia appositamente istituita per vigilare sull'applicazione e sulla implementazione a livello di

¹²⁸² Cfr. S.J. HYMAN G.R. WALSER-JOLLY, E. FARREL, «What Is a “Reasonable Security Procedure And Practice” Under the California Consumer Privacy Act's Safe Harbor?», 73 *Consumer Fin. L.Q. Rep.*, 173, 181ss.; cfr. Poi ancora anche N.F. III PALMIERI, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», cit., p. 37, che sottolinea appunto l'importanza di un approccio fondato sulla prevenzione.

dettaglio del CCPA, ossia la *California Privacy Protection Agency*, alcune delle norme preposte ad assegnare i suddetti compiti di *rulemaking* secondario si occupano proprio del tema, in senso lato, della *cybersecurity*¹²⁸³. Su tutte, a spiccare ai nostri fini è proprio la previsione che, a dimostrazione ulteriore del debito che il legislatore californiano pare aver contratto con la riflessione europea *anche* in punto di tecnologie *privacy invading* e di corrispondenti presidi giuridici *privacy oriented*, ricomprende tra le funzioni in parola quelle di adottare «*regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling*». Soprattutto, però, a rilevare è l'inciso per cui tali disposizioni debbano rafforzare gli obblighi dei *businesses* di soddisfare le richieste di accesso dei *consumers* tali da includere «*meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer*»¹²⁸⁴. Non può non risuonare, nelle suddette parole, un'analogia profonda con quel sistema di diritti ad un'informazione significativa sulla logica, sulle conseguenze e sull'importanza per l'interessato del processo decisionale interamente automatizzato che lo riguarda edificato dal GDPR.

Alla luce dei precedenti rilievi, allora, va salutato con favore l'intervento, cui abbiamo accennato in apertura del paragrafo, con cui la *California Privacy*

¹²⁸³ V. CAL. CIV. CODE §1798.185. Un esempio, oltre a quello che più ci interessa di cui parleremo *infra*, è il n (15), let. (B), che recita «*Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (...) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information*» concludendosi poi, in un'ottica di bilanciamento tra *information privacy* e diritti di *privative* che «*Nothing in this section shall require a business to divulge trade secrets*».

¹²⁸⁴ Ivi, n. (16), che precipuamente recita: «*Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer*».

Protection Agency (CPPA), esercitando la competenza normativa ad essa attribuita ai sensi della disposizione appena richiamata, ha predisposto un progetto di *regulation* diretto a declinare nel dettaglio la disciplina del CCPA proprio in materia di *automated decision making technologies* (e, conseguentemente, *systems*) predisponendo un sistema che implementi tanto i doveri di *notice* quanto il diritto di *opt-out* e di *information access* dell'interessato a fronte di imprese-*businesses*-titolari che impieghino le tecnologie in parola per trattare i dati, e conseguentemente adottare decisioni, «*affecting individuals*». Come si legge nel comunicato stampa contestuale alla sua pubblicazione, attraverso il progetto di regolamento, o comunque di *regulations* da adottare sulla sua base, la CPPA persegue l'obiettivo «*[to] support the responsible use of automated decisionmaking while providing appropriate guardrails with respect to privacy, including employees' and children's privacy*»¹²⁸⁵. L'intento istituzionale è, allora, quello di promuovere il dibattito pubblico sull'opportunità di introdurre tale disciplina di dettaglio e potenzialmente di avviare e di concludere il *rulemaking process* in materia nel corso dello stesso 2024. Stante il considerevole rilievo che, alla luce dell'intero quadro delineato nel presente capitolo, potrebbe assumere una regolamentazione di questo tipo, pur di carattere subprimario e insieme statale, nel contesto del diritto statunitense, fungendo da leva del dibattito in tema di ADM e di opportunità di una disciplina specifica sul punto anche negli altri Stati federati se non proprio a livello federale (potendo poi assurgere a modello giuridico dei rispettivi interventi normativi, come è stato per il primario CCPA),

¹²⁸⁵ V. CALIFORNIA PRIVACY PROTECTION AGENCY, *Draft for Automated Decisionmaking Technology Regulations*, December 2023, https://cppa.ca.gov/meetings/materials/20231208_item2_draft.pdf. Per una prima, embrionale e tuttavia efficace analisi, cfr. da subito D. L. RICE, K.C. HALM, K. K. TROWELL, A. SISTO, «Automated Decisionmaking Technology in California: New Rules Would Impose Transparency, Notice, and Consumer Opt-Out Obligations on Businesses», in *Davis Wright Tremain LLP*, <https://www.dwt.com/blogs/privacy--security-law-blog/2023/12/california-drafts-automated-decisionmaking-ai-rule>.

pare opportuno dedicarsi in conclusione del presente capitolo ad una succinta analisi delle *draft rules* enucleate nella proposta normativa in parola.

Occorre, innanzitutto, soffermarci sulla definizione di «*automated decision making technology*», che opportunamente ci sembra abbastanza ampia e dunque informata a quell'approccio tecnologicamente neutrale che abbiamo ritenuto il più idoneo ad evitare l'obsolescenza (altrimenti, implicitamente, programmata) della norma positiva: la *draft rule* elaborata dall'Agenzia identifica come tale «*any system, software, or process — including one derived from machine-learning, statistics, or other data-processing or artificial intelligence — that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking (...)*», in ciò quasi interamente rispecchiando l'approccio anche terminologico seguito dal legislatore europeo nel dettare una definizione di IA nella proposta di Regolamento sull'Intelligenza Artificiale attualmente in discussione¹²⁸⁶. La definizione in questione, tra l'altro, specificamente include, accanto all'impiego esclusivo della tecnologia algoritmica nell'elaborazione dei dati e nella conseguente adozione delle decisioni incidenti sull'interessato, anche il *semplice contributo* da questa prestato; e quindi accoglie nel suo alveo *qualsiasi tipo di sistema decisionale automatizzato*, tanto parzialmente quanto interamente tale, senza distinguere (in ciò la differenza, di matrice anche più garantistica, rispetto al GDPR) tra le due

¹²⁸⁶ Ricordiamo infatti che nell' Art. 3, Par. 1, n. 1), della *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*, OM(2021) 206 final, 21.4.2021, un «sistema di Intelligenza Artificiale» è definito come «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I [es. *Machine Learning, Deep Learning*, approcci basati su logica e conoscenza, approcci statistici], che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

specie ai fini dell'applicabilità del sistema rafforzato di garanzie che il progetto è deputato delineare.

Le altre definizioni contenute nella disposizione paiono ulteriormente rilevanti, poiché sembrano testimoniare ancor più come il quadro normativo eurounitario, e segnatamente il GDPR, appaia il modello giuridico cui la CPPA guarda (e verso il quale intende far orientare lo sguardo del pubblico) nella sue proposte di *Regulation*: troviamo ivi, infatti, una definizione di profilazione (premesso opportunamente che «*Automated decisionmaking technologies include profiling*») pressoché identica rispetto a quella delineata dall'art. 4 n. 4 del GDPR¹²⁸⁷. E inoltre, nel trasporre (anche qui) il concetto normativo che forte risuona nel par. 1 del art. 22 del GDPR, senza tuttavia ivi trovare una definizione, ossia quello di «*Decision that produces legal or similarly significant effects concerning a consumer*», la CPPA si spinge fino ad esplicitarne il contenuto semantico: forse, in tal caso, pur tentandosi di ovviare ai rischi di indeterminatezza configurati dalla clausola generale di cui al GDPR, rischiando tuttavia al contrario di circoscrivere troppo le potenzialità applicative della nozione, laddove l'elenco delle specie di decisione indicate dalla previsione fosse da ritenersi tassativo; ma, allo stesso tempo, non potendo non avvertirsi in tale catalogo alcuni degli esempi già portati dal *considerando* 71 ed ulteriormente articolati dal Gruppo di Lavoro Articolo 29 nelle Linee Guida da noi esaminate¹²⁸⁸.

¹²⁸⁷ CALIFORNIA PRIVACY PROTECTION AGENCY, *Draft for Automated Decisionmaking Technology Regulations*, December 2023, [ADDITIONS TO] § 7001. *Definitions*, dove per «*profiling*» si intende «*any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements*».

¹²⁸⁸ Ivi, «*Decision that produces legal or similarly significant effects concerning a consumer*» means a decision that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice,

Passando allora, brevemente e in conclusione, al piano del sistema rafforzato di *requirements* e di *rights* previsto dalle *draft rules* a fronte delle fattispecie così ricostruite, esso innanzitutto propone di implementare il regime di *notice* cui è soggetto il *business*, prevedendo come quest'ultimo «*shall provide consumers with the Notice of Rights to Opt-Out of, and Access Information About, the Business's Use of Automated Decisionmaking Technology* ("Pre-use Notice")»¹²⁸⁹. Il modello di *Pre-use notice* ha lo scopo di implementare un'informativa che massimizzi la trasparenza in relazione a processi altamente rischiosi per la *data privacy and security* dell'interessato, come ormai sappiamo bene: questa deve avere precipuamente ad oggetto «*the business's use of automated decisionmaking technology and consumers' rights to opt-out of, and to access information about, the business's use of automated decisionmaking technology*». L'articolazione specifica dell'oggetto riecheggia, poi, i doveri di informativa dettagliata delineati dall'art. 12 del GDPR ed ulteriormente estesi in relazione alle fattispecie dell'art. 22, con particolare riguardo alle informazioni significative di cui agli art. 13 par. 2 lett. g e 14 par. 2 lett. f, come peraltro interpretati dal WP 29 (questo sembra il punto più rilevante). La *pre-use notice*, ai fini del rafforzamento degli stessi doveri di trasparenza insisti nel modello di *notice-and consent* accolto dal CPPA, deve infatti necessariamente contenere anche «*a simple and easy-to-use method (e.g., a layered notice or hyperlink) by which the consumer can obtain additional information about the business's use of the automated decisionmaking technology*»; e tra queste informazioni aggiuntive, redatte peraltro in un «*plain language*» sono esplicitamente contemplate, in particolare, «*the logic used in the automated decisionmaking*

employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services».

¹²⁸⁹ V. [ADDITION] § 7017. «*Notice of Rights to Opt-Out of, and Access Information About, the Business's Use of Automated Decisionmaking Technology*».

technology, including the key parameters that affect the output of the automated decisionmaking technology», con la centrale precisazione secondo cui «*the business shall explain why these parameters are key*»; «*the intended output of the automated decisionmaking technology (e.g., a numerical score of compatibility)*»; e, non ultima per importanza, «*how the business plans to use the output to make a decision, including the role of any human involvement*», cui si aggiunge la necessaria spiegazione dei motivi per cui il *business* abbia ritenuto l'impiego della tecnologia capace di garantire «*validity, reliability, and fairness*»¹²⁹⁰.

Passando invece al contenuto dei diritti della cui esistenza il *business* deve dettagliatamente e con linguaggio semplice informare il *consumer*, accanto al già sottolineato (sul piano dei doveri, ma ciò vale specularmente sul piano del corrispondente diritto) l'allargamento delle informazioni “significative” che andrebbero a sostanziare il *right to access* nella fattispecie, spiccano certamente le garanzie rafforzate che la *regulation* si propone di introdurre in punto di *right to opt out*, laddove, nell'esplicitarsi che «*consumers have a right to opt-out of businesses' use of automated decisionmaking technology as set forth in this section*»¹²⁹¹, si estende l'oggetto di quest'ultimo a qualsiasi «*decision that produces legal or similarly significant effects concerning a consumer*», così come in relazione alla descritta fattispecie di «*profiling a consumer who is acting in their capacity as an employee, independent contractor, job applicant, or student*»,

¹²⁹⁰ Ivi, n. (4), in part. lett. (D). Appare scontato ma necessario sottolineare come nel dovere di *pre-use notice* ricada anche l'informazione circa l'esistenza e la latitudine del *right to access* di cui dispone il singolo, opportunamente rafforzato in quanto tale da ricomprendere tutte le informazioni appena richiamate: in particolare, il par. [ADDITION] § 7031. *Requests to Access Information About the Business's Use of Automated Decisionmaking Technology* propone che la lett. a) stabilisca chiaramente «*Consumers have a right to access information about the business's use of automated decisionmaking technology as set forth in this section*».

¹²⁹¹ V. V. [ADDITION] § 7030. *Requests to Opt-Out of the Business's Use of Automated Decisionmaking Technology*, in part. (a)

di cui successivamente la CPPA riporta una serie di lucidi esempi¹²⁹²; ed anche rispetto alle operazioni di profilazioni del consumatore «*while they are in a publicly accessible place*»¹²⁹³. Importante risulta notare come la CPPA proponga al *Board* di estendere il diritto di opporsi anche alle operazioni di «*profiling consumers for behavioral advertising*» quando l'interessato abbia meno di 16 anni e il *business* ne sia consapevole, o alle ipotesi in cui le informazioni del *consumer* siano utilizzate «*to train automated decisionmaking technology*».¹²⁹⁴

La proposta di disposizione, invero, conosce una serie nutrita di eccezioni: in particolare, il *right to opt out* sarebbe escluso laddove la tecnologia di ADM fosse necessaria (e usata esclusivamente) «*to provide the good or perform the service specifically requested by the consumer*», che per molti aspetti richiama l'eccezione al divieto generale di processi decisionali interamente automatizzati prevista dal par. 2 dell'art. 22 del GDPR, e consistente nella necessità del processo medesimo ai fini dell'esecuzione del rapporto configurato da un contratto con l'interessato¹²⁹⁵. Tuttavia, il loro non indifferente numero, unito al fatto che la

¹²⁹² V. n. (2), «(...) *For example, this includes profiling an employee using keystroke loggers, productivity or attention monitors, video or audio recording or live-streaming, facial- or speech- recognition or -detection, automated emotion assessment, location trackers, speed trackers, and web-browsing, mobile-application, or social-media monitoring tools*».

¹²⁹³ Il par. 7001 afferma: «*“Publicly accessible place” means a place that is open to or serves the public. Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, transit, streets, or parks.*». Ai fini del *right to opt out*, gli esempi riportati dal par. 7030 lett a n. (3) sono «*For example, this includes profiling a consumer while they are in a publicly accessible place using wi-fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, facial- or speech- recognition or -detection, automated emotion assessment, geofencing, location trackers, or license-plate recognition*».

¹²⁹⁴ V. in part. lett. a), n. 4) *SUBCOMMITTEE OPTION FOR BOARD DISCUSSION: Profiling a consumer for behavioral advertising*; e i successivi «(5) *Profiling a consumer that the business has actual knowledge is under the age of 16*; or (6) *Processing the personal information of consumers to train automated decisionmaking technology*».

¹²⁹⁵ V. in part. lett. (m), che tra i *purposes legittimi* del *business* individua, oltre al predetto, «(1) *To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information*; (2) *To resist malicious, deceptive, fraudulent, or illegal actions directed at the*

tutela dell'interessato è ivi declinata in termini di “diritto di opporsi”, seppur *ex ante*, piuttosto che di “divieto generale”, potrebbe vanificare buona parte dell'attitudine garantistica propria della disciplina prevista in relazione al principale strumento di cui l'individuo, nel sistema in esame, disporrebbe per governare l'impatto della tecnologia computazionale sulla propria persona¹²⁹⁶. Quale sarà la prospettiva “vincente”, se quella personalistica o quella, ancora una volta, “mercatista”, sarà solo l'iter di (eventuale) approvazione a rivelarlo.

Sebbene l'analisi qui condotta sconti necessariamente la novità della proposta in esame, e non abbia potuto che articolarsi in pochi e sommari rilievi, in prima approssimazione il quadro che traspare dal *regulation draft* in parola, anche alla luce delle intenzioni che lo animano, e che necessariamente ne guidano l'interpretazione, appare positivo. Certo, il regime di cui si propone l'introduzione non contempla quello che il Gruppo di Lavoro Articolo 29, in ciò ormai supportato dalla stessa CGUE, ha interpretato come un *divieto generale ex ante* di processi decisionali *interamente* automatizzati (pur avvicinandovisi, attraverso il menzionato sistema di *pre-use notice*); ma, in ogni caso, rappresenta un primo passo verso la definizione di una disciplina *specificamente* dedicata al fenomeno, e in funzione di garanzia degli interessi dell'individuo (sebbene ancora, lo si

business and to prosecute those responsible for those actions; (3) To protect the life and physical safety of consumers»

¹²⁹⁶ Per il rilievo posto dallo stesso Gruppo di Lavoro sulla maggior capacità di un'interpretazione dell'art. 22 par. 1 del GDPR, in termini di divieto generale di massimizzare la tutela della persona a fronte di decisioni interamente algoritmiche significativamente incidenti sulla sua persona, e, in tal contesto, di illuminare la *ratio* del regime di eccezioni previsto dal par. 2 e delle *suitable measures* imposte dal par. 3, v. cap. 3, par. 2. 3, e cfr. ancora GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/67*, cit., p. 21, e per un commento Mendoza-Bygrave, «The right not to be subjected», cit.

ripete, concepito essenzialmente quale *consumer*, e dunque quale operatore economico).

A prescindere da qualsiasi giudizio tecnico, che data la novità della proposta non può che essere embrionale, l'importanza di tali previsioni (*de iure condendo*) è evidente, alla luce del discorso che abbiamo condotto circa la centralità della trasparenza e della conoscibilità delle inferenze - o comunque della *leggibilità* - del processo da cui scaturisce la decisione incidente sull'individuo ai fini dell'effettiva tutela del diritto alla libera costruzione della propria personalità, per mezzo della salvaguardia della sua autodeterminazione informativa, di fronte alla *black-box* dell'IA.

È altrettanto vero che tali disposizioni andrebbero comunque ad iscriversi in un'architettura normativa che, per quanto apprezzabile nell'intenzione di predisporre un *comprehensive legal framework* in materia di *data privacy* nei rapporti tra privati, non appare immune da critiche: un'architettura che, ad un primo confronto con il modello giuridico europeo, dove volessimo instaurarlo assumendo come criterio di giudizio l'idoneità a tutelare gli interessi fondamentali della persona umana (prospettiva, come sappiamo, tradizionalmente non prioritaria - o comunque non esclusiva - per i legislatori statunitensi), appare lontana da garantire uno standard di protezione corrispondente o comunque analogo. L'adozione stessa del modello di *notice-and-consent*, non integrato da un approccio *risk-based* e quindi immune ai principi di protezione dei dati sin dalla progettazione (almeno) del trattamento e per impostazione predefinita, sembra deporre a sostegno di questa lettura¹²⁹⁷.

¹²⁹⁷ Per una puntuale analisi del modello giuridico edificato dal GDPR, v. ampiamente *retro*, cap. 3, par. 1.

Ciononostante, l'auspicio (accompagnato da una certa consapevolezza) è quello che tale iniziativa, non isolata invero nel panorama degli Stati federati¹²⁹⁸, possa stimolare, come già detto, la stessa riflessione e lo stesso pubblico dibattito sulla necessità di far fronte, in modo razionale ma non di meno tempestivo, alla proliferazione di una tecnologia che, da prezioso supporto per l'essere umano, può trasformarsi in terribile tiranno della sua sfera giuridica e, a monte, esistenziale, privandolo, prima ancora che della capacità di determinarsi in autonomia, di quella preliminare e indispensabile facoltà di comprendere i motivi delle decisioni che lo escludono, o piuttosto lo includono, nella società digitale, globalizzata e nuda del nostro tempo. Tale impulso potrebbe essere recepito non solo a livello dei singoli Stati, bensì anche sul piano federale, in seno al Congresso, concorrendo a promuovere un processo di unificazione - "nel rispetto delle differenze" - della disciplina dell'integrità della sfera privata e delle informazioni in cui si frantuma; e nel suo ambito, soprattutto, dell'utilizzo della tecnologia nell'elaborazione di decisioni provenienti da quel *loop* che, se un essere umano *non coinvolge*, comunque un altro essere umano *può travolgere*. Per una tecnologia che lavori per - o comunque in sinergia con - l'uomo. Non contro l'uomo¹²⁹⁹.

¹²⁹⁸ V. infatti, ad esempio, le *Proposed Colorado Privacy Act (CPA) Rules* adottate dall'*Attorney General* del Colorado il 10 ottobre 2022, e dunque ben prima che la CPPA implementasse il *draft* in analisi; *proposed rules* nell'ambito delle quali si articola un sistema di obblighi rafforzati in punto di utilizzo di sistemi e tecnologie di ADM, differenziandosi pertanto questi ultimi a seconda che la tecnologia si basi su « *Solely Automated Processing*», oppure «*Human Reviewed Automated Processing*», o altrimenti «*Human Involved Automated Processing*».

¹²⁹⁹ Sono le parole che, come sappiamo, campeggiano nel titolo e si ritrovano nel corpo della già menzionata, apprezzabile iniziativa del *White Paper* adottato da WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY, *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the People*, ottobre 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>, preordinato a stabilire i principi fondamentali che guidano un auspicato *rulemaking* istituzionale in punto di Intelligenza Artificiale.

CONCLUSIONI

Aprire la scatola nera: una “prospettiva fondamentale” per una società della dignità

Siamo giunti alla fine di questo lungo percorso teorico, in cui, partendo da un saggio di poco più di trenta pagine, pur figlio di una lunga elaborazione filosofica, che prendeva spunto dai potenzialmente distorti utilizzi dell'allora inedito strumento dell'istantanea fotografica per evidenziare la necessità di predisporre un *presidio giuridico* all'integrità della vita privata, si è giunti al nostro *datificato* panorama tecnosociale, in cui proliferano sistemi computazionali capaci non solo di coadiuvare l'uomo nello svolgimento delle proprie operazioni intellettive, bensì di sostituirlo interamente nel loro svolgimento, e di tradurle in azioni capaci di incidere sensibilmente sulla vita degli esseri umani, sulla base di pattern *autonomamente* costruiti, e tuttavia sempre meno perscrutabili ¹³⁰⁰. Nel fitto di tale secolare processo di trasformazione della fisionomia delle nostre società e dello stesso ecosistema in cui si inscrivono, e dunque della *mutazione antropologica* che l'essere umano, anche in conseguenza del suo rapportarsi con le macchine sempre più intelligenti, ha sempre più interessato, giacciono (esprimendoci con quelle formule non sempre fungibili, e tuttavia almeno complementari, che l'elaborazione teorica sul punto hanno scandito) la vita privata, il domicilio ideale, l'illesa intimità, la riservatezza, l'autodeterminazione informativa. Ci troviamo, insomma, nel

¹³⁰⁰ Sull'attuale panorama tecnologico e sui suoi riflessi sociali (in particolare sui tre livelli della c.d. società datificata), compreso un ritratto sintetico e tuttavia necessario di impronta scientifica in relazione ai concetti di Intelligenza Artificiale, di *Machine Learning* e di *Deep Learning*, v. retro cap. 2, par. 3. Sulla categoria, cui facciamo implicito riferimento, della c.d. strong AI, come insieme di tecnologie che si propongono come autonomo sistema razionale, dotato di un proprio status cognitivo, v. ancora il fondamentale contributo “iniziale” di J.R. SEARLE, *Minds, «Brains and Science»*, in *Behavioral and Brain Sciences*, 1980, 3, 417 ss.

composito dominio della *privacy*, stretto tra esigenze di liberalizzazione delle informazioni in cui si frantuma il sé individuale allo scopo di massimizzare benefici derivanti da una tecnologia che *migliora se stessa* attraverso i dati e l'opposta istanza di salvaguardarsi, in quanto principio che a tutte le altre libertà fondamentali conferisce «vita e sostanza»¹³⁰¹.

Arrivati a questo punto, è ormai noto come lo scopo dell'indagine che abbiamo condotto fosse quello di illuminare il nesso profondo che intercorre tra sviluppo tecnologico, nucleo più intimo della personalità umana e divenire del diritto, quest'ultimo reagendo in senso *evolutivo* al primo in funzione della tutela dell'integrità del secondo; e di come questo rapporto sia venuto a manifestarsi nell'esperienza giuridica statunitense e in quella europea. Nel farlo, si è dimostrato (si ritiene), preliminarmente e in una prospettiva diacronica, come esso informi tutto il multidisciplinare discorso che ha condotto alla nascita dell'istituto giuridico della *privacy*, rappresentando il motore delle sue successive declinazioni. Dipanandosi dal “bostoniano” *right to privacy* (e dal relativo, autonomo *tort*) di ispirazione milliana ma ancora radicato nella struttura del tradizionale *right to property*, passando per il fondamentale riconoscimento della «*privacy as an aspect of human dignity*», approdando poi all'*information privacy* e all'autodeterminazione informativa che sostanzia l'autonomo diritto fondamentale alla protezione dei dati personali a chiare lettere sancito nella Carta dei diritti fondamentali dell'Unione Europea, l'istituto appare chiaramente arricchirsi e trasformarsi per accogliere in sé le sempre nuove dimensioni (su tutte, quella *informativa*) del *prisma* della persona umana esposte all'intelligenza, e, insieme, agli utilizzi distorti (in primo luogo “dossieristici” e sorvegliativi) della tecnica.

¹³⁰¹ Le parole, lo si ricorderà, sono del giudice W.O. Douglas, autore dell'*opinion of the Court* nel celebre caso *Griswold v. Connecticut*, 381 U. S., p. 483 ss.

Arrivando ai giorni nostri, del nesso in parola si è colta l'epifania nella disciplina di quella frontiera della tecnologia che più sfida la capacità dell'uomo di coltivare una sfera di "imperscrutabilità" cognitiva, sentimentale, familiare, ovvero l'impiego delle macchine, e quindi dei sistemi algoritmici, nel trattamento delle informazioni in cui si frantuma la sua attuale identità de-materiale, proteiforme, virtuale, e nelle stesse decisioni che sui risultati di tale elaborazione si basano, svolgendo una dettagliata analisi comparatistica della sua differente declinazione nel quadro dei due sistemi in esame. Tale indagine è stata supportata dall'opinione che interrogarsi sullo *stato del diritto* in materia significasse interrogarsi sullo *stato dei diritti fondamentali*, tanto nel rapporto con la Pubblica Autorità quanto nel rapporto con gli interpreti dell'iniziativa economica, laddove dal controllo delle informazioni riguardanti la propria persona dipende la costruzione del proprio «corpo [sempre più] elettronico», e dunque, oggi, della propria personalità. D'altronde, solo per citare uno tra i molteplici esempi presi in esame, «i profili [si intende, qui, *algo-created*] determinano (...) effetti di selezione delle persone, con conseguente possibilità di stigmatizzazione e di esclusione sociale»¹³⁰².

Non è poi un mistero (e lo si già esplicitato all'inizio) il fatto che nello svolgere l'indagine in parola si sia scelto di adottare una *prospettiva personalistica o antropocentrica*, che specialmente nell'ambito della comparazione svolta (nel terzo e nel quarto capitolo) tra i regimi in materia di trattamenti automatizzati vigenti in Europa e negli Stati Uniti ci ha consentito di assumere come criterio privilegiato a tal scopo l'idoneità della disciplina stessa a massimizzare la tutela della sfera privata, come presupposto della libertà di consapevole e *non-interamente-condizionata* autodeterminazione individuale, sempre più fragile di fronte alle ormai note *privacy-invading technologies*, o, per

¹³⁰² Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 328.

esprimersi con una lungimirante, celebre e ormai nota espressione, ai sempre maggiori «*subtler and more far reaching means of invading privacy*»¹³⁰³.

Dell'indagine di ordine più squisitamente tecnico condotta nella seconda parte del lavoro, indissolubilmente legata alla ricognizione storica operata nella prima, passiamo allora qui ad illustrare, sinteticamente, i risultati più importanti.

Seguendo la prospettiva appena menzionata, l'analisi comparatistica ci ha condotto a riscontrare l'esistenza, in Europa, nel quadro di un modello generale e uniforme di matrice sovranazionale della disciplina della *data protection*, tendenzialmente neutrale dal punto di vista tecnologico, di un sistema articolato di disposizioni generali disciplinanti *anche* la fattispecie dei trattamenti automatizzati dei dati personali¹³⁰⁴; e parallelamente, di un subsistema normativo incentrato su un divieto generale di processi decisionali interamente algoritmici (art. 22 par. 1), temperato da un elenco tassativo di eccezioni, e articolato in un quadro di posizioni giuridiche (art. 13-15 e 22, par. 3) che, seppur oggetto di contrasti interpretativi e in parte espressione della tradizionale anima mercantilista dell'Unione, sembra idoneo a garantire un primo, fondamentale presidio alla capacità del soggetto di "aprire" la scatola nera dei procedimenti inferenziali che ne manipolano l'identità informativa, opponendovi quella richiesta di trasparenza necessaria ad autodeterminarsi, anche in ordine alla scelta circa il coinvolgimento o meno del revisore umano nel *loop* algoritmico¹³⁰⁵.

Certo, il disposto degli articoli che configurano il diritto ad un'informazione significativa, vero discrimine dell'effettività della relativa protezione, nonostante l'indirizzo ermeneutico fornito dal *considerando* 71, stante la loro

¹³⁰³ La citazione è ancora una volta, è di L. BRANDEIS, «Dissenting Opinion», in *Olmstead v. United States*, 277, U. S, p. 473

¹³⁰⁴ Ce ne siamo occupati nel cap. 3, al par. 1 e ai parr. 2-2.2.

¹³⁰⁵ V. di seguito i par. 2.3 e 2.4 del cap. 3.

indeterminatezza si prestano ad interpretazioni che gli interessi al segreto industriale e alla proprietà intellettuale antepongano a quello dell'interessato a conoscere il funzionamento dell'algoritmo nel caso concreto: e, dunque, in sostanza, ad apprendere le inferenze (gli *inferred data*) sui quali la decisione che su di lui pesantemente incide si fonda¹³⁰⁶. Tuttavia l'inesausto dibattito dottrinale; l'unificatrice e luminosa operazione esegetica svolta dal Gruppo di Lavoro Articolo 29; il recente monumentale intervento della CGUE (nel *leading case SCHUFA*) che alla fattispecie di processo decisionale interamente automatizzato ha ricondotto già il calcolo algoritmico dello *score* creditizio in sé e per sé; l'attenta vigilanza dei Garanti che i dati personali considerano «oggetto di un diritto fondamentale prima che merce»; nonché una crescente sensibilità della giurisprudenza nazionale sul tema della trasparenza algoritmica (come dimostrano i casi *Mevaluate* e la sentenza decalogo del Consiglio di Stato), sembrano spie della volontà di vivificare il dato positivo in senso personalista, massimizzando, appunto, la garanzia dell'intimo nucleo della persona umana¹³⁰⁷.

A fronte di tale scenario, il contesto americano risulta più frastagliato. Pur assumendo una doverosa prospettiva di *law in the making*, che tenga conto della centralità della giurisprudenza nordamericana di qualsiasi ordine nella costruzione del diritto, attraverso il costante adeguamento della tradizione (a livello esegetico o, *in extremis*, per mezzo dell'*overruling*) all'innovazione tecnologica, l'indagine ci ha mostrato un quadro dominato, anzitutto, da una prospettiva *technology dependent*, in cui la profonda corrente liberl-umanitaria che trova la propria origine nel contributo di Warren e Brandeis e la sua consacrazione nell'attività del *Chief Warrant* si confronta storicamente con una

¹³⁰⁶ La questione in parola occupa una parte considerevole del par. 2.4. suddetto.

¹³⁰⁷ V. ancora par. 2.4. e i restanti parr. del cap. 3.

fiducia tutta “positivistica” nell’efficienza e nella strutturale neutralità della tecnica¹³⁰⁸.

In materia di *information privacy*, l’ordinamento statunitense risulta caratterizzato anzitutto da un forte *corpus* di principi trasparenti dalla giurisprudenza della *Supreme Court* sul Quarto Emendamento a garanzia della *privacy-dignity*, e tuttavia essenzialmente limitati ai rapporti tra privato e Pubblica Autorità nel contesto delle *searches* e *and seizures* disciplinate dal Quarto Emendamento¹³⁰⁹; da una serie di *sector-specific statutes*, che la *data privacy* nei rapporti tra privati considerano essenzialmente come profilo della materia dei rapporti tra *business* e *consumer* (e dunque la *data protection* considerano come emanazione della *consumer protection*) e che una certa unità trovano nelle soluzioni enucleate nei *consent order agreements* e nelle proprie linee guida dalla FTC nell’esercizio delle competenze di cui alla *Section 5* dell’*FTC Act*¹³¹⁰; e poi dal variegato panorama del *common law* e della legislazione dei singoli Stati, in cui si riscontrano le prime tendenze a un approccio incentrato sull’adozione di *comprehensive consumer data privacy laws* (è l’esempio paradigmatico del CCPA, già seguito da Colorado, Utah, Virginia e Nevada)¹³¹¹. In tale contesto, la disciplina federale dell’*automated data processing*, e ancor più nello specifico degli *automated decision making systems*, appare, oltre che embrionale, lacunosa sotto il profilo positivo, e rispetto ad essa solo in parte ha funzionato la supplenza normativa della giurisprudenza, guidata dal vivace dibattito dottrinale. In proposito, accanto alla sensibilità di quel fronte della *Supreme Court* che ha tentato di ripristinare la garanzia di una *reasonable expectation of privacy* nel contesto digitale nei casi *Jones* e *Carpenter*, sul piano dei rapporti tra privati,

¹³⁰⁸ V. cap. 4, par. 1 e 1.1.

¹³⁰⁹ V. *retro*, cap. 4, par. 2 ss.

¹³¹⁰ Ivi, par. 3 ss.

¹³¹¹ Ivi, par. 4 ss.

guardando ai settori in cui più diffuso e insieme più rischioso appare l'utilizzo della tecnologia in parola, la protezione pare essere offerta da un sistema di doveri e di corrispondenti diritti di *consumer disclosure* e di *adverse action notification* (nel quadro della *credit industry*) o piuttosto dagli istituti del *disparate treatment* e del *disparate impact* e del conseguente *right to contest* (in sede amministrativa e giurisdizionale, e dunque piuttosto concepibile come strumento di *redress*) su cui si fondano le c.d. *equal protection laws* (essenzialmente, nel settore dei rapporti di lavoro e dell'*housing*): doveri, diritti e istituti che, da soli, non sempre appaiono idonei a soddisfare quel livello di "informazione significativa" necessario a garantire all'individuo la capacità di non subire passivamente, bensì di comprendere e di contestare le decisioni che lo riguardano, a partire dal controllo sui dati (oggi, anche *inferred*)¹³¹².

Un fondamentale contributo nella costruzione di una disciplina più garantista per l'individuo *anche* in relazione al fenomeno emergente dell'ADM, cui nessuna disposizione positiva dedica una specifica attenzione, sta certamente arrivando dal fronte della dottrina e della giurisprudenza, il cui comune denominatore si identifica in quella tendenza evolutiva che abbiamo riconosciuto come uno degli elementi strutturali dell'ordinamento statunitense. A campeggiare sono, ad esempio, le proposte di una parte della dottrina di applicare, attraverso una loro interpretazione appunto evolutiva, le disposizioni del *Wiretap Act* anche a quelle attività che si sostanzino in un monitoraggio automatizzato del contenuto delle comunicazioni elettroniche¹³¹³; la giurisprudenza che, supportata dalla dottrina, nei rapporti tra privati e pubblica amministrazione valorizza la *Due Process Clause* come ineludibile garanzia di *transparency* e di *fairness* nei procedimenti amministrativi "governati" dall'algoritmo¹³¹⁴; l'estensione, da parte

¹³¹² Ivi, in ordine dal par. 2 ss.

¹³¹³ V. *retro* cap. 4, par. 2.1.

¹³¹⁴ Ivi, par. 3.2.

della FTC, nell'esercizio dei propri poteri di *enforcement*, della *deceptivness* ai processi decisionali automatizzati come quelli di *behavioral scoring*¹³¹⁵. Allo stesso tempo, nel quadro della tendenza degli Stati federati ad adottare legislazioni onnicomprensive in materia di *consumer data privacy*, assai meritevole di attenzione risulta l'implementazione da parte di alcuni di questi, come il Colorado e soprattutto la California (sul cui *Draft for Automated Decisionmaking Technology Regulations* ci si è soffermati) di *regulations* che articolino una disciplina di dettaglio in materia di *Solely e/o Human Involved automated decision making systems*¹³¹⁶. Ma resta un monito, scolpito nelle parole del giudice Scalia nella sentenza *U.S. v. Jones*, che qui ci sentiamo di condividere: «[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way»¹³¹⁷.

Prima di volgere uno breve, ma significativo sguardo al futuro, si vogliono dedicare alcune riflessioni di chiusura ai risultati di questa ricognizione, condotta alla luce di un punto di vista che abbiamo definito personalistico, o antropocentrico, o *fundamental rights-oriented*¹³¹⁸.

¹³¹⁵ Ivi, par. 3.3.

¹³¹⁶ Ivi, par. 4.1.

¹³¹⁷ *U.S. v. Jones*, 565 U.S. 400 (2012).

¹³¹⁸ Per alcune considerazioni sulla prospettiva in questione, come implementata (opportunamente), secondo tali autori, dalla Corte di Giustizia e dal legislatore europeo nella predisposizione del GDPR, cfr. ancora una volta O. POLLICINO, «Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale», in *Federalismi.it*, in Comunicazione, media e nuove tecnologie, n. 3/2014; e soprattutto M. BASSINI, «La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali», in *Quad. cost.*, 2016, 588; F. BRAVO (a cura di), *Dati Personali. Protezione, libera circolazione e governance. Vol. 1: i principi*, Pacini Giuridica, p. 23 ss. Per alcune riflessioni di tenore più generale in relazione al contesto digitale, cfr. anche G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, Giappichelli, Torino 2022.

Nello svolgere l'indagine di cui abbiamo esposto i risultati, l'obiettivo non è stato e continua a non essere quello di esprimere un giudizio *assoluto* di merito o piuttosto di demerito in relazione all'approccio coltivato rispettivamente dal legislatore europeo (e dal circuito ermeneutico che con i suoi prodotti si confronta), e dai diversi formanti che in contesto americano si relazionano con la protezione giuridica della vita privata, oggi soprattutto a fronte dell'invadente fenomeno dell'automazione dei *data processing and decision making systems*, Sarebbe, questa, una soluzione facile e tuttavia deficitaria della sensibilità che il giuscomparatista deve sempre mostrare per le differenze specifiche intercorrenti tra i contesti culturali e le tradizioni giuridiche di riferimento.

Tuttavia, nell'interrogarci sull'idoneità degli strumenti implementati nei rispettivi ordinamenti, ciascuno in relazione al proprio contesto sociogiuridico di riferimento, non possiamo non considerare il carattere ormai prevalentemente transfrontaliero del trattamento dei dati personali, che l'attuale potenza computazionale dei *digital devices* amplifica senza precedenti: tendenza che rende evidente la necessità di implementare, sempre più, un regime normativo, se non unitario, comunque tendente all'*uniformità*, ravvicinando i rispettivi modelli giuridici.

Combinando questo rilievo con quella visione che ci conduce ad individuare nella tutela della persona umana, pur nel necessario bilanciamento con gli altri interessi pubblici così come economici in gioco, il *fine ultimo* del discorso giuridico, alla luce dell'analisi svolta ci sembra possibile individuare almeno alcuni principi capaci di plasmare una modello di riferimento veramente *antropocentrico*, che indipendentemente dalle specificità dei singoli ordinamenti garantisca l'autodeterminazione informativa dei singoli, e in una doverosa prospettiva comunitaria quella delle formazioni sociali in cui la loro personalità si svolge, governando i rischi che i *Big Data* e l'impiego della tecnologia algoritmica a scopo, essenzialmente, di profilazione e di sorveglianza configurano

per l'individuo: salvaguardandone, pertanto, quell'indisponibile nucleo di intimità di fronte all'«*insatiable appetite of information*»¹³¹⁹ delle macchine contemporanee. Ci sembra, essenzialmente, che tali principi possano identificarsi in un *principio di uniformità* della disciplina vigente, che tanto ai fenomeni di autoregolamentazione del settore privato quanto all'introduzione di esasperate discipline (e relative tecnologie) «pubblico-protettive» ponga un argine¹³²⁰; in un *approccio tecnologicamente neutrale*, ossia orientato alla definizione di «principi generali che possono rimanere invariati per un certo periodo di tempo, senza essere vincolati al mutamento [aggiungiamo, esponenzialmente sempre più rapido] delle tecnologie», così impedendo tutt'altro che infrequenti ipotesi di “obsolescenza normativa”¹³²¹; in quel principio “olistico”, portatore di una più ampia prospettiva *risk-based* e di *accountabilty* dei titolari del trattamento, che è la *privacy by design*, espresso nelle sue massime potenzialità applicative e quindi in termini di incorporazione di tecnologie *privacy-oriented*, o comunque di misure a garanzia della protezione dei dati personali, sin dalla progettazione (non solo del trattamento, ma) dell'architettura ICTs, e quindi degli hardware e dei software che ospiteranno il trattamento algoritmico, e spesso ne “agiranno” il prodotto decisionale¹³²²; e, non da ultimo, in un *approccio evolutivo*, quest'ultimo indirizzato soprattutto agli interpreti, nella prospettiva in esame tuttavia

¹³¹⁹ A. R. MILLER, *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Cambridge, 1971, p. 3.

¹³²⁰ Sul tema, ex multis, si rinvia a A. ETZIONI, *How Patriotic is the Patriot Act? Freedom versus Security in the Age of Terrorism*, Routledge, New York-London 2004; U. Pagallo, La tutela della privacy in Europa e negli Stati Uniti, cit.

¹³²¹ Cfr. ancora una volta sul punto G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, cit., p. 1670 ss.; e più approfonditamente Id., *Riflessioni su diritto e tecnica*, in *Dir. Inf.*, IV-V/2012, p. 831 ss.

¹³²² Sul principio di *privacy by design*, oltre alla disamina svolta nel cap. 3, par. 1.3., cfr. nello specifico A. CAVOUKIAN, «7 foundational principles of privacy by design», in *Office of the Information & Privacy Commissioner of Ontario*, 2010; U. PAGALLO, «Privacy e design», in *ID*, n. 1/2009; per la declinazione di tale principio nello specifico contesto del GDPR, cfr. ancora S. CALZOLAIO, «Privacy by design. Principi, dinamiche, ambizioni del nuovo Re. Ue. 2016/679», in *federalismi.it*, n. 24/2017, 20 dicembre 2017.

(declinabile anche in contesti di *common law*) considerati indefettibili mediatori tra i principi consacrati nel tessuto normativo positivo e la varietà dell'esperienza concreta, nel suo perpetuo divenire tecnosociale.

Appare chiaro che a tale modello risulta attualmente più “vicino” il sistema disegnato dal testo del GDPR e dalla costante esegesi *personalistica* promossa dalla Corte di Giustizia dell'UE e dai principali attori istituzionali eurounitari e nazionali. Non a caso, lo si è già detto, è stata sottolineata in letteratura la fondamentale vocazione del GDPR a rappresentare uno «standard globale»¹³²³ di tutela della *privacy* e dell'autodeterminazione informativa, «diffondendosi viralmente grazie alla ragionevolezza e all'utilità dell'approccio in esso contenuto»¹³²⁴. Tuttavia, la tendenza sempre maggiore dei legislatori statali, in area statunitense, a guardare la *data privacy* in senso onnicomprensivo, così come la proposta discussa al Congresso, per ora (ma solo per ora) naufragata, dell'*American Data Privacy and Protection Act*, unita alle proposte di esercizio da parte della FTC della potestà di c.d. *Magnuson-Moss Rulemaking*, sembrano indice di una lenta penetrazione (anche eterodeterminata, sembrando questa in larga parte conseguire alla reazione del partner europeo al *Datagate*), anche in tale contesto, di una spinta verso l'uniformazione in materia di *data privacy*.

Aggiungiamo, peraltro, il rilievo per cui al giurista continentale spesso difetta quella *elasticità interpretativa* che gli consenta di trascendere la razionale geometria delle definizioni positive, per quanto “generalì”, propria invece di chi, come il *common lawyer* americano, è abituato ad inferire modelli di condotta prescrittivi dal magma dell'esperienza concreta e dalle tendenze sociali che la percorrono, raccordandoli ad un panorama di principi generali che riflettano,

¹³²³ L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, Editoriale scientifica, 2016, 70.

¹³²⁴ G. BUTTARELLI, «The EU GDPR as a clarion call for a new global digital gold standard», in *International Data Privacy Law*, 2/2016, 77-78.

anche qui evolutivamente, i valori emergenti dalla dialettica sociale nel periodo storico in cui si trovi ad operare. Tale attitudine appare davvero indispensabile, anche in una prospettiva di dettaglio, di fronte a sistemi algoritmici che, come nel caso dell'*Unsupervised Machine Learning* e ancor più del *Deep Learning*, “apprendono” dal contesto e accrescono in autonomia le proprie capacità logico-inferenziali, e quindi predittive, sfuggendo alle categorie epistemologiche fino a quel momento esistenti¹³²⁵.

Possiamo allora concludere la nostra trattazione rivolgendo uno sguardo al futuro, e considerando perciò brevemente quelle dimensioni, cui già più volte abbiamo fatto riferimento nel corso del lavoro, in cui più evidentemente appaia oggi svolgersi la dialettica tra tecnologia, *privacy* e diritto; dimensioni nelle quali si sta intervenendo a livello (non solo) normativo - o comunque nelle quali appare opportuno intervenire - per governare i rischi che lo sviluppo insieme felice e problematico della tecnologia (dell'informazione e della comunicazione, ma non solo) configura per la vita privata.

Sulla prima, in realtà, ci siamo già soffermati poc'anzi: ci riferiamo alla dimensione transfrontaliera del trattamento, e a monte del trasferimento incessante di dati al di là di qualsiasi frontiera fisica o virtuale, da una parte all'altra del globo. Circoscrivendo l'attenzione al rapporto tra le due esperienze giuridiche di cui abbiamo sondato i sistemi normativi di *data privacy and protection*, possiamo recuperare le considerazioni che abbiamo svolto a suo tempo. Se negli invalidati *Safe Harbour* e *Privacy Shield* mancavano disposizioni che introducessero uno specifico regime di garanzie applicabile dai *businesses*

¹³²⁵ V. cap. 2, par. 3. Per una panoramica su tali temi, ex multis si rinvia a R. ANGELINI, «Intelligenza Artificiale e governance. Alcune riflessioni di sistema», in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 295 ss.

operanti negli Stati Uniti e aderenti al rispettivo quadro di principi alle decisioni *solely based* sui trattamenti algoritmici aventi ad oggetto i dati provenienti dal contesto europeo, lo stesso può purtroppo dirsi per l'attualmente vigente *Data Privacy Framework*. Quest'ultimo, infatti, in un *considerando* essenziale ai nostri fini, nei settori che si ritengono investiti in modo cruciale – e potenzialmente più pregiudizievole per i diritti fondamentali dell'individuo – dal fenomeno dell'automazione, ha ritenuto che in punto di processi decisionali automatizzati «*U.S. law offers specific protections against adverse decisions*»: esplicitamente affermando, a tal proposito, e in relazione a una platea di atti normativi leggermente ampliata rispetto a quella cui faceva riferimento l'*adequacy decision* del *Privacy Shield*, che «*these acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress*»¹³²⁶. Ebbene, all'esito della nostra analisi risulterà chiaro come questa affermazione, se non infondata, risulti comunque sovrastimare le capacità del diritto positivo vigente (quanto meno a livello federale) di tutelare adeguatamente l'autodeterminazione informativa dell'individuo, anche dove concepito e trattato nella sola veste di consumatore¹³²⁷.

¹³²⁶ COMMISSIONE EUROPEA, *Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final. Cfr. Cons. 35. Gli atti normativi richiamati sono ancora una volta, come si evince anche dalla nota 53, l'*Equal Credit Opportunity Act* (15 U.S.C. 1691 et seq.), il *Fair Credit Reporting Act* (15 USC § 1681 et seq.) e il *Fair Housing Act* (42 U.S.C. 3601 et seq.); a questi, la Commissione aggiunge il *Title VII of the Civil Rights Act* e l'*Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, e valorizza inoltre la sottoscrizione dei c.d. «*Organisation for Economic Cooperation and Development Artificial Intelligence Principles, which inter alia include principles on transparency, explain ability, security and accountability*». Sul punto per un'analisi più approfondita v. *retro* cap 4 par. 1 ss.

¹³²⁷ Aggiungiamo qui incidentalmente che di certo un ruolo fondamentale nell'implementazione di un regime che garanzie adeguate predisponga in relazione ai processi medesimi *anche* laddove riguardanti dati trasferiti a *businesses* statunitensi dal continente europeo potrebbe essere svolto dalla FTC, investita assieme al DOP, come sappiamo, di compiti di *enforcement* rispetto all'accordo DPF: e ciò tenendo conto della tendenza dominante in seno

Sembrerebbe, insomma, opportuno che le parti coltivassero un approccio di più ampio respiro, pur non essendo escluso che, nel frattempo, il panorama normativo statunitense si modifichi, implementando a livello settoriale (o, chissà, generale) le garanzie in questione.

La seconda dimensione, invece, attiene nello specifico a quel fenomeno e insieme a quella disciplina di cui, come sappiamo, il panorama dell'automazione, ed oggi della tecnologia algoritmica, rappresenta il presupposto e insieme lo sfondo. Ci riferiamo all'Intelligenza Artificiale, come oggetto precipuo di indagine, e quindi come tecnologia oggetto di specifica disciplina, in cui tutte le riflessioni che abbiamo svolto in materia di trattamenti algoritmici e di sistemi decisionali automatizzati confluiscono. In questa sede non si intende riproporre analisi, anche tecniche, già svolte nel corso della trattazione (v. cap. 2 par. 3). Si intende solo sottolineare che la protezione della persona umana, nel suo nucleo indisponibile di libertà personale, e dunque di pensare, di sentire, di interagire con lo spazio che la circonda, passa attraverso una opportuna regolamentazione di tutti quei sistemi che ridisegnano il panorama delle città e più in generale delle *civiltà* in cui viviamo, trasformandola in *infosfera*: dagli *smart objects* ai sistemi di riconoscimento vocale capaci di raccogliere e finanche di inferire quantità senza precedenti di informazioni dal comportamento dell'essere umano, e a reagire pressoché immediatamente agli stimoli con decisioni, della più diversa latitudine

alla Commissione, poc'anzi richiamata, ad interpretare le funzioni di cui alla Sezione 5 dell'*FTC Act*, ed anche di *non-legislative guidance* ai sensi della Sezione 18, nel senso della promozione di soluzioni esegetiche unificanti e, per quanto attiene alla materia che qui ci occupa, evolutive. E tuttavia, abbiamo già evidenziato anche i limiti che incontra nella prassi il recepimento generale dei principi (solo per le parti vincolanti) enunciati nei *consent order agreements*, e la ritrosia all'esercizio dei poteri di "*legislative*" *rulemaking*: limiti che qui sembrano ulteriormente valere e dimidiare la capacità della FTC di edificare un sistema coerente di soluzioni esegetiche evolutive rispetto al dato positivo applicabili all'impiego degli *ADM systems* nel trattamento dei dati "europei". Per un'analisi di maggior dettaglio rinviamo alle riflessioni svolte *retro*, cap. 4, par. 3.3.

(dalla ricerca di un brano musicale fino al farmaco da assumere in caso di malessere stagionale), capaci di incidere in modo significativo sulla stessa *autonomia di giudizio* del primo¹³²⁸.

Molteplici sono le raccomandazioni, le comunicazioni, i *white papers* e più in generale gli atti di *soft law*, a pressoché tutti i livelli normativi (nazionale, sovranazionale, internazionale), in materia di IA, animati dall'obiettivo di definire un quadro unitario di principi che orienti tanto i processi di *self-regulation* delle aziende di Hi-Tech, quanto, soprattutto, l'attività dei legislatori. Nel nostro lavoro abbiamo richiamato molti di tali interventi, ed abbiamo riportato alcune delle più felici definizioni in essi contenute, tra cui quella che, in contesto europeo, individua un sistema di Intelligenza Artificiale nei «sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato», seguita anche dalla Commissione nel quadro della proposta di Regolamento Europeo attualmente in discussione al Parlamento Europeo.¹³²⁹

¹³²⁸ Per le fondamentali riflessioni di sistema cui si è fatto più volte rinvio nella presente trattazione, cfr. ancora a L. FLORIDI, *The Fourth Revolution: How Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

¹³²⁹ Sono, infatti, le parole del Gruppo Indipendente di esperti ad alto livello sull'Intelligenza Artificiale, istituito dalla Commissione Europea nel giugno 2018, nei recenti *Orientamenti Etici per un'AI affidabile*, B-1049 Bruxelles, 4 aprile 2018, p. 45, che prosegue sottolineando come: «I sistemi di IA possono usare regole simboliche o apprendere un modello numerico, e possono anche adattare il loro comportamento analizzando gli effetti che le loro azioni precedenti hanno avuto sull'ambiente». È importante rilevare che la definizione in questione pare essere stata recepita anche dalla Commissione Europea nella predisposizione della proposta di Regolamento sull'Intelligenza Artificiale attualmente in discussione al Consiglio e al Parlamento Europeo. V. infatti. art. 3, par. 1, n. 1), *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*, OM(2021) 206 final, 21.4.2021, che definisce un «sistema di Intelligenza Artificiale» come «un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I [es.

Dello stesso tenore, sebbene più orientata al pratico, anche quella consacrata nella deliberazione dell'OCSE contenente i c.d. *AI Principles*, cui, gli stessi Stati Uniti hanno esplicitamente aderito: vi si legge come «*an AI system is a machine-based system that is capable of influencing the Environment by making recommendations, predictions or decisions for a given set of Objectives. It does so by utilising machine and/or human-based inputs/data to: i) perceive real and/or virtual environments; ii) abstract such perceptions into models manually or automatically; and iii) use Model Interpretations to formulate options for outcomes*»¹³³⁰.

Al di là delle definizioni di principio sappiamo già come già nell'aprile 2021 la Commissione abbia presentato la fondamentale, già citata proposta di Regolamento UE in materia di Intelligenza Artificiale, che per la prima volta sancisce nel diritto europeo una definizione di sistemi di IA neutra dal punto di vista tecnologico e predispone un corpus normativo fondato sul principio di precauzione (c.d. *risk-based approach*). Ed è del 9 novembre 2023 l'annuncio circa il raggiungimento da parte della presidenza del Consiglio e dei negoziatori del Parlamento europeo di un accordo provvisorio sulla proposta in questione, che conterrebbe alcune previsioni importanti in termini di implementazione dei doveri di trasparenza cui le aziende produttrici dovrebbero *sin dalla costruzione* informare i sistemi in parola, esigenza fondamentale ai fini della garanzia dei diritti fondamentali dell'individuo; e che, tra l'altro, vieterebbe radicalmente alcune tipologie di sistemi di IA ad alto rischio, quali, ad esempio, quelli

Machine Learning, Deep Learning, approcci basati su logica e conoscenza, approcci statistici], che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

¹³³⁰ Cfr. OECD, *Scoping the OECD AI Principles. Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)*, OECD Digital Economy Papers, No. 291, Novembre 2019. <https://www.oecd-ilibrary.org/docserver/d62f618a-en.pdf?expires=1709255583&id=id&accname=guest&checksum=BF50769FD2BC914823A0C66151EEF51B>

strumentali alla manipolazione comportamentale, all'assegnazione di un punteggio sociale (il caso emblematico che si intende evitare è quello del Sistema del Credito Sociale implementato in Cina¹³³¹), ed alla categorizzazione biometrica per dedurre dati sensibili¹³³².

Poco prima di tale passo avanti in contesto europeo, poi, il Governo statunitense, precisamente il 30 ottobre 2023, ha pubblicato un *Executive Order*, firmato dal Presidente degli Stati Uniti, intitolato « *Safe, secure and trustworthy*

¹³³¹ Ci riferiamo qui all'ormai noto, "sperimentale" Sistema del Credito Sociale avviato in alcune parti della Cina già nel 2014, e in sintesi basato su un complesso sistema di *data mining* effettuato su ampi set di *Big Data* provenienti da più di quaranta organismi al progetto partecipanti: a risultarne è un programma di "credito" (inteso nel più ampio senso di "affidabilità sociale") di massa, nell'ambito del quale le informazioni sono trattate al fine di attribuire a ciascun cittadino un "punteggio sociale" sul quale ampiamente si basano le decisioni in punto di erogazione al medesimo di determinati servizi, quali la possibilità di accedere al sistema finanziario, o anche pubblici e di natura *essenziale*, come la locazione a canone agevolato di alloggi popolari. Sul tema, *ex multis*, cfr. C. NGUYEN, «China might use data to create a score for each citizen based on how trustworthy they are», in *Business Insider*, 26 ottobre 2016; Y. CHEN, A. CHEUNG, «The Trasparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System», in *Journal of Comparative Law*, 2018, pp. 356-378; A. ALÙ, «Il Sistema Cinese di Credito Sociale: così si materializza la nuova era della sorveglianza», in *Agenda Digitale*, 19 gennaio 2023, disponibile qui: <https://www.agendadigitale.eu/cultura-digitale/sistema-cinese-credito-sociale-sorveglianza/>.

¹³³² V. il comunicato stampa ufficiale: CONSIGLIO EUROPEO, CONSIGLIO DELL'UNIONE EUROPEA, *Regolamento sull'intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole per l'IA al mondo*, 9 dicembre 2023, <https://www.consilium.europa.eu/it/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/>. Ivi si legge anche: «L'accordo di compromesso stabilisce un livello orizzontale di protezione, compresa una classificazione ad alto rischio, al fine di garantire che non siano inclusi i sistemi di IA che non presentano il rischio di causare gravi violazioni dei diritti fondamentali o altri rischi significativi. I sistemi di IA che presentano solo un rischio limitato sarebbero soggetti a obblighi di trasparenza molto leggeri, ad esempio rendere noto che il contenuto è stato generato dall'IA, affinché gli utenti possano prendere decisioni informate in merito all'ulteriore utilizzo»; passaggio importante è quello che si concentra sui modelli di base, ovvero « i grandi sistemi in grado di svolgere con competenza un'ampia gamma di compiti distintivi, quali la generazione di video, testi, immagini, la conversazione in linguaggio laterale, il calcolo di dati o la generazione di codici informatici. L'accordo provvisorio prevede che i modelli di base debbano rispettare specifici obblighi di trasparenza prima di essere immessi sul mercato. È stato introdotto un regime più rigoroso per i modelli di base "ad alto impatto". Si tratta di modelli di base addestrati con grandi quantità di dati e di complessità, capacità e prestazioni avanzate ben al di sopra della media, che possono diffondere i rischi sistemici lungo la catena del valore.».

Artificial Intelligence», che, a fronte della esponenziale accelerazione dell'IA Generativa, conferisce ampi mandati normativi e insieme esecutivi ai principali Dipartimenti competenti in materia, esigendo l'implementazione nell'arco di 12 mesi di *best practices*, standard e persino nuove *regulations* in punto di sviluppo e di utilizzo dell'IA in molteplici settori chiave nella vita di relazione, quali la finanza al dettaglio, il mercato del lavoro, l'istruzione e l'assistenza sanitaria incardinato attorno al principio di «*safe and trustworthy AI*»¹³³³.

Prescindendo da qualsiasi analisi nel dettaglio della (opportuna) disciplina in costruzione, appare evidente come solo un approccio olistico, garantito da norme che l'intero ciclo di vita dei sistemi decisionali automatizzati (si legga: di IA) considerino e regolamentino in tutti i suoi risvolti, garantisca, oggi, l'individuo rispetto ai rischi altrimenti ingovernabili di lesione dei suoi diritti fondamentali derivanti dall'interazione con i sistemi in questione: interazione spesso inconsapevole, o non meditata, ma inevitabile stante la pervasiva e incrementale diffusione di tali sistemi nei più disparati settori della vita di relazione; ed anzi, socialmente *pretesa*, a pena di esclusione dal consesso civile (è possibile, oggi, una vita senza *smartphones*?)¹³³⁴. E altrettanto evidente appare

¹³³³ Cfr. THE WHITE HOUSE, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 ottobre 2023, <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>. In apertura della sezione 1, si leggono tali emblematiche parole: «*Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society*».

¹³³⁴ Di più, c'è chi si chiede se, nella contemporanea società digitale, sussista o meno un diritto a «vivere sconnessi»: KARABOGA, MATZNER, OBERSTELLER, OCHS, «Is There a Right to Offline Alternatives in a Digital World?», in *Data Protection and Privacy: (In)visibilities and Infrastructures*, a cura di Leenes, van Brakel, Gutwirth, De Hert, Springer, 2017, 31 ss. (ma spec. 38-39).

il fatto che, ancora una volta, l'interesse alla protezione dell'autodeterminazione informativa assuma rilievo superindividuale, chiamando in causa la consolidata esperienza "nel digitale" delle Autorità Garanti (o, oltreoceano, delle *law enforcement Agencies*), illuminando la dimensione *sociale* della *privacy*: come è stato affermato in seno al Garante italiano, infatti, nel contesto di alcune riflessioni sulla *governance* del fenomeno, «quel che è certo è che non si potrà prescindere né dai principi del GDPR – considerato che la stessa Intelligenza Artificiale si nutre di dati e, in particolare, proprio di quelli di natura personale – né da un ruolo centrale delle Autorità garanti per la protezione dei dati a livello nazionale nelle decisioni strategiche complessive e nelle regolazioni settoriali»¹³³⁵.

Perché nessuna garanzia risulta effettiva se effettiva non è la vigilanza di chi, in *extrema ratio*, può aprire quella scatola nera, che dalle nostre molteplici maschere informazionali viene attraversata e nella quale le stesse subiscono potenziali e impreviste distorsioni.

Perché di fronte all'assegnazione automatizzata di identità che derivano dall'arbitraria manipolazione delle proprie informazioni personali, "offerte in dono" alla macchina; di fronte alla consequenziale segregazione in profili che sono «gabbie sociali»; di fronte a questa «riduttiva astrazione», che determina uno «svuotamento dell'umano», l'unica soluzione possibile risulta quella di «mantenere al centro della riflessione e della progettazione istituzionale i diritti fondamentali»¹³³⁶. Non già, si badi, per in alcun modo arrestare il rigoglioso (e, di fatto, inarrestabile) progresso tecnologico, che tanti benefici può apportare

¹³³⁵ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Intelligenza artificiale e ruolo della protezione dei dati personali. L'analisi di Ginevra Cerrina Feroni*, Intervento di Ginevra Cerrina Feroni, vice Presidente del Garante per la Protezione dei Dati Personali, 14 febbraio 2023.

¹³³⁶ Le espressioni tra virgolette caporali sono ancora una volta di S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 340.

all'umano: ma affinché l'umano continui ad esistere, per godere di tali stessi benefici.

Per conservare alle macchine lo statuto di strumento, o al più di ordine che conviva con l'umano; e all'uomo lo statuto di *fine* di quel progetto costituzionale che sta alla base di ogni società che intenda definirsi, autenticamente, democratica¹³³⁷. Nel contesto di una società in cui all'uomo sia garantita, ora e per sempre, la libertà di costruire in autonomia la propria personalità, che principia a sua volta dalla libertà di determinare cosa esibire, e cosa piuttosto custodire in sé e nella propria intimità, della propria intangibile *esperienza personale*, privata o familiare che sia. Una libertà che principia dalla *privacy*, come presupposto indefettibile della dignità umana.

¹³³⁷ Ancora una volta, il riferimento implicito è (anche) alle luminose parole dell'art. 2 della Costituzione italiana, che a chiusura del lavoro, nel loro ruolo di bussola e insieme di orizzonte vincolante per il potere costituito e inviolabile per il singolo, si ritiene doveroso riportare per intero: «La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale».

BIBLIOGRAFIA

DOTTRINA E SOFT LAW:

- ABERNATHY, CH. F. «Defing Privacy: The Power of culture in the Digital Age», in *Privacy digitale. Giuristi e informatici a confronto*, (a cura di) F. BERGADANO, A. MANTELERO, G. RUFFO, G. SARTOR, Giappichelli, 2006
- ABERNATHY CH. F., *Law in the United States*, Thomson/West, St. Paul, MN, 2006
- ABRAMS M., «Origins of Personal Data and its Implications for Governance», in *The Information Accountability Foundation*, 2014
- ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the Rights of Citizens*, Washington D.C., 1973
- AIELLO G. F., «La protezione dei dati personali dopo il Trattato di Lisbona», in *Oss. del dir. civ. e comm.*, n. 2/2015
- ALLEN M., ORHEIM A., «Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them», 8, in *Wash. J. L. Tech. & Arts*, 2, 2012
- ALPA G., BESSONE M. (a cura di), *Banche dati, telematica e diritti della persona*, Cedam, Padova 1984
- ALPA G., *La cultura delle regole. Storia del diritto civile italiano*, Laterza, Roma-Bari, 2009.
- ALPA G., RESTA G., *Le persone fisiche e i diritti della personalità*, in R. Sacco (diretto da), *Trattato di diritto civile*, Vol. I, II ed., Torino, Utet, 2019
- ALPAYDIN E., *Introduction to machine learning*. MIT press, 2014
- ALÙ A., «Il Sistema Cinese di Credito Sociale: così si materializza la nuova era della sorveglianza», in *Agenda Digitale*, 19 gennaio 2023.

- AMIGONI, SCHIAFFONATI V., SOMALVICO M., «Intelligenza artificiale (voce)», in *Treccani, Enciclopedia della Scienza e della Tecnica*, 2008
- ARISTOTELE, *Politica*, Laterza, Bari 2007
- AULETTA T. A., *Riservatezza e tutela della personalità*, Milano, 1978
- AUSIELLO G., BATINI C., FROSINI V., «Informatica», in *Enciclopedia Italiana - Appendice VI*, Roma, Istituto dell'Enciclopedia Italiana, 2000
- AUTOREIT PERSOONSgegevens, *Websites moeten toegankelijk blijven bij weigeren tracking cookies*, 7 marzo 2019
- BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni Editore, Roma 1974
- BARATTA R., *Complexity of EU Law in the Domestic Implementing Process*, 2 *The Theory and Practice of Legislation*, 293, 2014
- BARBERA A., «Art. 2», in *Commentario della Costituzione*, G. Branca (a cura di), Bologna 1975
- BAROCAS S., SELBST A. D., *Big Data's Disparate Impact*, in *California L.R.*, 104, 2016
- BARTOLE S., DE SENA P., ZAGREBELSKY G., *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, Art. 8
- BASSINI M., «La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali», in *Quad. cost.*, 2016
- BATHAEE Y., «The Artificial Intelligence Black Box and the Failure of Intent and Causation», in *Harv. J.L. & Tech.*, 31, 2018
- BAUMAN Z., *Modernità Liquida*, trad. it. di Sergio Minucci, Editori Laterza, Roma-Bari 2002
- BELLOCCI M., MAGNANESI S., PASSAGLIA P., RISPOLI E. (a cura di), *Tutela della vita privata e prospettive costituzionali*, 2006

- BENEDETTI D., «IA e (in)sicurezza informatica» in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018
- BENNET C. J., MULLIGAN D., *The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy*, 2012
- BENNETT C.J., *In defense of privacy: the concept and the regime*, *Surveillance & Society*, 8 (4), 2011
- BERLE I., *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal, Law, Governance and Technology Series*, Springer, Cham, 2020
- BERNERS-LEE T., *Weaving the Web. The original design and ultimate destiny of the World Wide Web by its inventor*, San Francisco, Harper, 1999
- BIFULCO R., «La sentenza Scherms e la costruzione del diritto europeo della privacy», in *Giurisprudenza costituzionale*, 1, 2016
- BIGNAMI F., «European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining» in *Boston College Law Review*, 48(609), 2007
- BIONDO C., «Secondary Sources: ALRs, Encyclopedias, Law Reviews, Restatements, & Treatises», in *Harvard Law School Library*, (a cura di) Deanna, 12/09/23
- BLACKSTONE W., *Commentaries on the laws of England*, 11 ed., Londra, I, 1791.
- BLOUSTEIN E. J., «Privacy as an aspect of Human Dignity: an answer to Dean Prosser», in *N.Y.U.L. Rev.*, 1964
- BO C., «La carente disciplina sull'uso degli algoritmi nella PA: come interviene il giudice amministrativo?» *In Media Laws*, 7 ottobre 2021

- BODEA G., KARANIKOLOVA, K., MULLIGAN D.K., MAKAGON J., *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (Commissione Europea 2018)
- BOISTEL A., *Cours de philosophie du droit*, Parigi, 1899
- BOLDRINI, *AI. Artificial Intelligence*, Milano Finanzia S.p.a., Milano, 2018
- BONINI M., «Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti “violabili” in nome della lotta al terrorismo e ad altri pericoli, nell’esperienza statunitense ed europea», *Rivista AIC*, n. 3/2016
- BOSCO, CREEMERS, FERRARIS, GUAGNIN, KOOPS, «Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities», in Gutwirth, Leenes, De Hert (edited by), *Reforming European Data Protection Law*, Springer, 2015
- BOYDEN B.E., «Can a Computer Intercept your email?» In *Cardozo L. Rev.*, 34, 2012
- BOYNE S. H., «Data Protection in the United States», in *The American Journal of Comparative Law*, vol. 66, 2018
- BRANDEIS L., «Dissenting Opinion», in *Olmstead v. United States*, 277, U. S.
- BRAUCHER J., «Deception, Economic Loss and Mass-Market Customers: Consumer Protection Statutes as Persuasive, Authority in the Common Law of Fraud», in *Ariz. L. Rev.*, 48, 2006, 829, 85
- BRAVO F. (a cura di), *Dati Personali. Protezione, libera circolazione e governance. Vol. 1: i principi*, Pacini Giuridica

- BRUGIOTTI E., «La privacy attraverso le “generazioni dei diritti”. Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico», in *dirittifondamentali.it*, 2/2013
- BURREL J., «How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms», in *Big Data & Soc’y*, 2016
- BUSIA A., «Riservatezza (diritto alla)», in *Dig. disc. pubbl.*, Torino, UTET, 2000
- BUTTARELLI G., *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit [Valutazione della necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali. Uno strumentario]*, Garante europeo della protezione dei dati (EDPS), 11 aprile 2017
- BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella Società dell’Informazione*, Milano, 1997
- BUTTARELLI G., «The EU GDPR as a clarion call for a new global digital gold standard», in *International Data Privacy Law*, 2/2016
- BYGRAVE L. A., «Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making», in K. Yeung, M. Lodge (a cura di), *Algorithmic Regulation*, Oxford University Press, 2019
- BYGRAVE L. A., «Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling», in *Computer Law & Security Review*, 19, 2001
- BYGRAVE L.A., *Data protection law: approaching its rationale, logic and limits*, Kluwer Law International, 2002
- BYGRAVE L.A., MENDOZA I., «The Right not to be Subject to Automated Decisions based on Profiling», in Tatiani Synodinou, Philippe Jougleux,

- Christiana Markou, Thalia Prastitou (eds.), *EU Internet Law: Regulation and Enforcement*, Springer, 2017
- C. K. ALLEN, *Law in the Making*, Clarendon Press, Oxford 1955
 - C. K. ALLEN, *Uneasy Access: Privacy for Women in a Free Society*, Rowman and Littlefield, Totowa, N.J., 1988
 - CALIFANO L., *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, Editoriale scientifica, Napoli 2017
 - CALIFANO L., *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli 2016
 - CALIFORNIA PRIVACY PROTECTION AGENCY, *Draft for Automated Decisionmaking Technology Regulations*, December 2023
 - CALO M.R., «The Boundaries of Privacy Harm», in *Ind. L.J.*, 86, 2011
 - CALO R., Artificial Intelligence Policy: a Primer and Roadmap, in 51 Univ. California *D. L. Rev.*, 421 (2017)
 - CALZOLAIO S., «Introduzione. *Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati», in *RIID*, 1, 2021
 - CALZOLAIO S., «Protezione dati personali», in *Dig. disc. pubbl., Agg.*, (a cura di) R. Sacco, Milano, 2017
 - CALZOLAIO S., «Privacy by design. Principi, dinamiche, ambizioni del nuovo Re. Ue. 2016/679», in *federalismi.it*, n. 24/2017, 20 dicembre 2017
 - CALZOLAIO, PAGNANELLI, «From data protection to privacy by research. Food for thoughts in the light of the new General data Protection Regulation», in *Law and Administration XXI Century*, n. 4(41)/2016
 - CAMERA DEI DEPUTATI (a cura di), *Banche dati e tutela della persona*, Roma, 1983

- CAMPOGRANDE G., «I diritti sulla propria persona», in *Antologia Giuridica*, 1896, 65 ss. (del fascicolo 2) e 155 ss. (del fascicolo 3)
- CANNIZZARO E., *Il diritto dell'integrazione europea. L'ordinamento dell'Unione*, Giappichelli Editore, 2017
- CARNELUTTI F., «Diritto alla vita privata», in *Riv. Trim. Dir. Pubbl.*, Giuffrè editore, Milano, 1955
- CARRER S., «Se l'amicus curiae è un algoritmo: il chiacchierato caso Loomis alla Corte Suprema del Wisconsin», in *Giurisprudenza Penale Web*, 2019
- CARTABIA M., *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana, Relazione alla Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola*, Roma, 24-26 ottobre 2013
- CARTABIA M., «Le sentenze “gemelle”: diritti fondamentali, fonti, giudici», in *Giur.cost.*, 2007, 3565 ss.
- CARTABIA M., *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, Conferenza trilaterale delle Corti costituzionali italiana, portoghese e spagnola, Roma, Palazzo della Consulta 24-26 ottobre 2013,
- CASTELVECCHI D., *Can we open the black-box of AI?* Nature, 2016
- CASTRO DANIEL, *A Review: The American Data Privacy and Protection Act*, GovTech, June 13, 2022
- CAVOUKIAN A., «Patience, Persistence, and Faith: Evolving the Gold Standard in Privacy and Data Protection», in *Future Challenges in Security and Privacy for Academia and Industry*, a cura di Camenisch, Fischer Hubner, Murayama, Portmann, Rieder, Springer, 2011

- CAVOUKIAN A., *7 foundational principles of privacy by design*, Office of the Information & Privacy Commissioner of Ontario, 2010
- CAVOUKIAN A., *Privacy by Design: Leadership, Methods, and Results*, in *European Data Protection: Coming of Age*, a cura di Gutwirth-Leenes-de Hert-Poullet, Springer, 2013
- CERQUITELLI T., QUERCIA D., Pasquale F., *Transparent Data Mining for Big and Small Data*, Springer International, New York, 2017
- CERRINA FERONI G., «Intelligenza artificiale e ruolo della protezione dei dati personali», intervento del 14 febbraio 2023
- CERULLI G., *Fundamentals of Supervised Machine Learning*, SpringerLink, 2023
- CFPB, *Analysis of Differences between Consumer- and Creditor-Purchased Credit Scores*, September 2012
- CFPB, *Fair Credit Reporting Act. Manual 2.0*, CFPB Consumer Laws and Regulations, ottobre 2014
- CHEN Y., CHEUNG A., «The Trasparent Self Under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System», in *Journal of Comparative Law*, 2018
- CHEN Z., «Ethics and discrimination in artificial intelligence-enabled recruitment practices», in *Nature, Humanities and Social Sciences Communications*, 10, 2023
- CHOPRA S., L.F. WHITE L.F., *A Legal Theory for Autonomous Artificial Agents*, University of Michigan Press, Ann Arbor, 2011
- CIANCIMINO M., *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*, Edizioni Scientifiche Italiane, Napoli, 2020

- CITRON D. K., PASQUALE F., «The Scored Society: Due Process for Automated Predictions» in *Washington Law Review*, 2014
- CIVITARESE MATTEUCCI S., «Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità», in *Dir. pubbl.* 1/2019
- COBB S., «Data Privacy and Data Protection: U.S. Law and Legislation», in *WeLiveSecurity*, 2016
- COBB S., «Data Privacy and Data Protection: U.S. Law and Legislation», in *WeLiveSecurity*, 2016
- COHEN JULIE E., *Configuring The Networked Self: Law, Code, And The Play Of Everyday Practice*, Yale University Press, 2012
- COLAPIETRO C., «I principi ispiratori del Regolamento UE 2016/679 e la loro incidenza sul contesto normativo nazionale», in *federalismi.it*, n. 22/2018, 21 novembre 2018
- COLAPIETRO C., IANNUZZI A., «I principi generali del trattamento dei dati personali e i diritti dell'interessato», in AA. VV., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, a cura di L. Califano e C. Colapietro, Milano, ES, 2017
- COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema di fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla privacy*, Editoriale Scientifica, Napoli, 2018
- COMMISSIONE EUROPEA, *Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, (COM (92) 422 final – SYN 287).
- COMITATO CONSULTIVO DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A

CARATTERE PERSONALE (Convenzione 108), *Guidelines on Artificial Intelligence and Data Protection*, Strasburgo, 25 gennaio 2019

- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, 13 febbraio 2019
- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, 2018
- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – Explanatory Report*, 17-18 maggio 2018
- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, CM/Rec (2010)13, 23 novembre 2010
- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Raccomandazione sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione*, CM/Rec(2010)13, 23 novembre 2010
- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, CM/Rec (2020)
- COMITATO DEI MINISTRI DEL CONSIGLIO D'EUROPA, *Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector*, 1973

- COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 14 maggio 2020
- COMITATO EUROPEO PER LA PROTEZIONE DEI DATI, *Linee guida 8/2020 sul targeting degli utenti dei social media*, 13 aprile 2021
- COMMISSIONE EUROPEA, *Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023) 4745 final
- COMMISSIONE EUROPEA, *Communication: Shaping Europe's digital future*, Febbraio 2020
- COMMISSIONE EUROPEA, *Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, L'intelligenza artificiale per l'Europa*, COM (2018) 237, 25 aprile 2018
- COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo, al Consiglio delle Regioni. Un'agenda digitale europea*, COM (2010)245 definitivo, Bruxelles 19 maggio 2010
- COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Una strategia europea per i dati*, COM (2020) 66 final, 19 febbraio 2020
- COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, relativa alla definizione di una*

dichiarazione europea sui diritti e i principi digitali, COM (2022) 27 final, 26 gennaio 2022

- COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime “Approdo sicuro” dal punto di vista dei cittadini dell’UE e delle società ivi stabilite*, COM(2013) 847 final, 27 novembre 2013
- COMMISSIONE EUROPEA, *Comunicazione della Commissione delle Comunità europee al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, Un’iniziativa europea in materia di commercio elettronico*, COM (97) 157, 15 aprile 1997
- COMMISSIONE EUROPEA, *Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Strategia per il mercato unico digitale in Europa*, COM (2015) 192 final, 6 maggio 2015
- COMMISSIONE EUROPEA, *Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni. Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM/2021/118 final, 9 marzo 2021
- COMMISSIONE EUROPEA, *Decennio digitale europeo: obiettivi digitali per il 2030*
- COMMISSIONE EUROPEA, *Digital Economy and Society Index (DESI)*, 2022
- COMMISSIONE EUROPEA, *Europa 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM (2010) 2020, marzo 2010
- COMMISSIONE EUROPEA, *Explanatory text for Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data*, COM (90) 314 final – SYN 287

- COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, COM (2020) 65 final, 19 febbraio 2020
- COMMISSIONE EUROPEA, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, Bruxelles, 2012
- COMMISSIONE EUROPEA, *Proposta di Direttiva del Parlamento Europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi*, COM/2022/495 final, 2022
- COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione*, COM/2021/206 final, 21 aprile 2021
- COMMISSIONE EUROPEA, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield*, Bruxelles, 18 ottobre 2017, (COM (2017) 611 fin.), 2017
-
- CONFESSORE N., «*Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*», in *The New York Times*, 4 aprile 2018
- CONFORTI B., *Diritto Internazionale*, (a cura di) Massimo Iovine, Editoriale Scientifica, Napoli 2018, XI Edizione
- CONGRESSIONAL RESEARCH SERVICE LIBRARY OF CONGRESS, *The Constitution of the United States of America: Analysis and Interpretation, Centennial Edition, Interim Edition: Analysis of Cases Decided by the*

Supreme Court of the United States to June 26, 2013, U.S. Government Printing Office, Washington D.C., 2013

- CONSIGLIO D'EUROPA, *Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data - Explanatory Report*, ETS No. 108, 1981
- CONSIGLIO EUROPEO, CONSIGLIO DELL'UNIONE EUROPEA, *Regolamento sull'intelligenza artificiale: il Consiglio e il Parlamento raggiungono un accordo sulle prime regole per l'IA al mondo*, 9 dicembre 2023
- CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, 23 gennaio 2017
- CONSUMER FINANCIAL PROTECTION BUREAU, *Key Dimensions and Processes in the U.S. Credit Reporting System*, December 2012
- CORDESCHI, L'intelligenza artificiale, in: Geymonat, Ludovico, *Storia del pensiero filosofico e scientifico. Il Novecento* a cura di Enrico Bellone, Corrado Mangione, Milano, Garzanti, 1996
- CORMEN, LEISERSON, RIEVEST, STEIN, *Introduction to Algorithms*, The MIT Press, 2022
- CORRADINO M., *Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future*, 10 settembre 2021
- CRAWFORD K., JASON SCHULTZ J., «Big data and due process: Toward a framework to redress predictive privacy harms», in *BCL Rev.*, 55, 2014
- CROWNIN E. , *La Costituzione degli Stati Uniti nella realtà odierna*, tr. It. di Oriani, Pisa, 1958

- CROWTHER B. T., «(Un)Reasonable Expectation of Digital Privacy», in *Brigham Young University Law Review*, 1, 2012
- CUBEDDU M.G., «Commento art. 13», in C.M.Bianca, F.D. Busnelli (a cura di), *La protezione dei dati personali*, in Le Nuove Leggi civ. comm., 2007
- CUCCURU P., «Blockchain ed automazione contrattuale. Riflessioni sugli smart contract», in *NGCC*, 2017
- CUFFARO, D’ORAZIO, RICCIUTO, *Il codice del trattamento dei dati personali*, Torino, 2007
- D.C. BEHAR, «An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context», in *U. Miami L. Rev.*, 66, 2012
- D’ACQUISTO G., DOMINGO-FERRER J., KIKIRAS P., TORRA V., DE MONTJOYE Y.A., BOURKA A., *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, European Union Agency for Network and Information Security, dicembre 2015
- D’ACQUISTO G., NALDI M., *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2017
- D’ACQUISTO G., NALDI, *Big data e privacy by design*, Torino, 2017
- D’ORAZIO R., «Protezione dei dati by default e by design», in S. Sica, V. D’Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Cedam-Wolters Kluwer, 2016
- DAHRENDORF R., *Classi e conflitto di classe nella società industriale*, Laterza, Bari 1977
- DANIELLE KEATS CITRON, AND FRANK A. PASQUALE, «The Scored Society: Due Process for Automated Predictions», in *Washington Law Review*, Vol. 89, 2014

- DASKAL J., «Microsoft Ireland, the Cloud Act, and International Lawmaking 2.0» in *Stan. L. Rev. Online*, 71, 9, 10ss.
- DATTA A., SEN S., ZICK Y., *Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems*, IEEE Symposium on Security and Privacy, 2016
- DE CUPIS A., *I diritti della personalità*, Milano, 1959
- DE GREGORIO G., TORINO R., Privacy, Tutela dei dati personali e Big Data, in E. Tosi (a cura di), *Privacy digitale*, Giuffrè Francis Lefebvre, 2019
- DE MAURO A., GRECO M., GRIMALDI M., «A Formal Definition of Big Data Based on its Essential Features», in *Library Review*, 2016
- DE SIERVO U., «La privacy», in *I diritti fondamentali e le Corti in Europa*, (a cura di) Panunzio, Napoli, 2005
- DEL NINNO, «Il caso Promusicae-Telefonica: la Corte di Giustizia UE si pronuncia sul rapporto tra tutela della privacy e protezione del copyright nell'ordinamento comunitario», in *Diritto e Giustizia*, 2012
- DI MAJO A., *La tutela civile dei diritti*, IV ed., Milano, 2003
- DI MARTINO A., *Profili Costituzionali della Privacy in Europa e negli Stati Uniti*, Jovene Editore, Napoli 2017
- DI NICOLA, ESPA, BRESSAN, DICKSON, NICOLAMARINO, *Metodi statistici per la predizione della criminalità. Rassegna della letteratura su predictive policing e moduli di data mining*, e-Crime Working papers, n. 2/2014
- DI PORTO F. (a cura di), «Big Data e Concorrenza», in *Concorrenza e Mercato*, Giuffrè Editore, n. speciale 23/2016
- DOMINIO J.C., *Civil Rights and Liberties in the 21st Century*, IV ed., New York, Routledge, 2018
- DONATI F., «Art. 8. Protezione dei dati di carattere personale», in R. Bifulco, M. Cartabia, A. Celotto (a cura di), *L'Europa dei diritti*.

Commento alla Carta dei diritti fondamentali dell'Unione europea,
Bologna, 2001

- DONATI F., «La CEDU nel sistema italiano delle fonti del diritto alla luce delle sentenze della Corte costituzionale del 24 ottobre 2007», in *www.osservatoriosullefonti.it*, n. 1/2008
- DONATI F., sub art. 8. Protezione dei dati di carattere personale, in Bifulco-Cartabia-Celotto, *L'Europa dei diritti*, Bologna, 2001
- DOUGLAS W.O., «Dissenting Opinion», in *Public Utilities v. Pollak*, 343, U. S. 467
- DRESSEL J., FARID H., «The accuracy, fairness, and limits of predicting recidivism», in *Sci Adv.*, 4(1), 4 gennaio 2018
- DUCATO R., «La crisi della definizione di dato personale nell'era web 3.0», in F. Cortese -M. Tomasi (a cura di), *Il diritto e le definizioni*, Editoriale Scientifica Italiana, Napoli 2016
- DUHIGG CHARLES, *What Does Your Credit-Card Company Know About You?* New York Times, May 12, 2009
- DUMIAK M., *Federal Privacy Bill: Breaking Down the ADPPA*, JD Supra, 24 giugno 2022
- EDWARDS L., VEALE M., «Slave to the Algorithm: Why a “Right to an Explanation” is Probably not the Remedy You are Looking for», in *Duke Law & Technology Review*, 16 (1), 2017
- EDWARDS L., VEALE M., «Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For», in *Duke Law & Technology Review*, 2017
- EEOC, *Big Data in the Workplace: Examining Implications for Equal Employment Opportunity Law*, Meeting of October 13, 2016

- ELLISS-BROOKES L., *Big data in action: the story behind Routes to Diagnosis*, Public health matters blog, 2015
- ETZIONI A., *How Patriotic is the Patriot Act? Freedom versus Security in the Age of Terrorism*, Routledge, New York-London 2004
- EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 7/2015, Meeting the challenges of Big Data*, novembre 2015
- EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *Opinion in the review of the ePrivacy Directive (2002/58/CE)*, 22 luglio 2016
- EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7-3-2012
- EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion in the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, n. 4/2017
- EUROPEAN PARLIAMENT COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, A7–0402/2013
- EXECUTIVE OFFICE OF THE PRESIDENT, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016
- EXECUTIVE OFFICE OF THE PRESIDENT, *Consumer Data Privacy in a Networked World*, Washington DC, February 2012
- EXPERIAN – OLIVER WYMAN, *Comprehensive Consumer Credit Review*, Experian-Oliver Wyman Market Intelligence Report, at 7 (2011 Q4)
- FADDA C., BENSA, *Note al Libro Secondo*, in Windscheid, *Diritto delle Pandette*, a cura di Fadda e Bensa, Vol. 1, I, Torino 1902

- FAINI F., «Dati, algoritmi e Regolamento europeo 2016/679», in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, A. Mantelero, D. Poletti (a cura di), Pisa Univeristy Press, 2018
- FAIR HOUSING LEGAL SUPPORT CENTER AND CLINIC, *A Primer on Fair Housing Law*, The John Marshall Law School, 2014
- FAMIGLIETTI G., «Il diritto alla riservatezza o la riservatezza come diritto. Appunti in tema di riservatezza ed *intimidad* sulla scorta della giurisprudenza della Corte costituzionale e del *Tribunal Constitucionale*», in *Biotechnologie e valori costituzionali. Il contributo della giustizia costituzionale*, A D'Aloia (a cura di), Giappichelli Editore, Torino 2005
- FAVOREAU L., «Diritti dell'uomo», in *Enciclopedia Treccani*, Roma, 1998
- FAYYAD U., G. PIATETSKY-SHAPIO, P. SMYTH, From data mining to knowledge discovery: an overview, in U. Fayyad, (ed.) *Advances in Knowledge Discovery and DataMining*. AAAI Press, Menlo Park, CA (1996).
- FEDERAL RESERVE BOARD, *Report to Congress on Credit Scoring and its Effects on the Availability and Affordability of Credit*, 2007
- FEDERAL TRADE COMMISSION (FTC), *Credit-Based Insurance Scores: Impacts on Consumers of Automobile Insurance, A Report to Congress*, 2007
- FEDERAL TRADE COMMISSION, *Privacy & Data Security Update: An Overview Of The Commission's Enforcement, Policy Initiatives, And Consumer Outreach And Business Guidance In The Areas Of Privacy And Data Security*, 2017
- FEDERAL TRADE COMMISSION, *Big Data: A Tool for Inclusion or Exclusion?* January 2016

- FEDERAL TRADE COMMISSION, *Forty Years of Experience With the Fair Credit Reporting Act*, July 2011
- FERRARA, SANTAMARIA, «Il diritto alla illesa intimità privata», in *Riv. dir. privato*, 1937
- FICI A., PELLECCIA E., «Il consenso al trattamento», in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003
- FINOCCHIARO G. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017
- FINOCCHIARO G., «Identità personale (diritto alla)», in *Digesto/civ., Agg.*, Torino, 2010
- FINOCCHIARO G., «Intelligenza artificiale e protezione dati personali», in *Giur. It.*, 07/2019
- FINOCCHIARO G., «Introduzione al regolamento europeo sulla protezione dei dati», in *Nuove leggi civ.*
- FINOCCHIARO G., «La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Scherms», in G. Resta –V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai “Safe harbour principles” al “Privacy shield”*, Roma 2016
- FINOCCHIARO G., «Riflessioni su diritto e tecnica», in *Dir. Inf.*, IV-V/2012
- FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli Editore, 2012
- FINOCCHIARO G., «La memoria della rete e il diritto all’oblio» in *Dir. inf.*, 2010
- FIORILLO V., «Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizia», in *Federalismi.it*, n. 15/2017

- FLAHERTY DAVID H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, 1989
- FLORIDI L., «Four Challenges for a Theory of Informational Privacy», in *Ethics and Information Technology*, 2006, 8.3
- FLORIDI L., *The Fourth Revolution: How Infosphere Is Reshaping Human Reality*, Oxford University Press, 2014; anche nella sua trad. It. ID., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, 2017.
- FLORIDI L., *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer Link, 2015
- FLORIDI L., *The Philosophy of Information*. Oxford: Oxford University Press, 2011
- FOCARELLI C., *Privacy. Proteggere i dati personali oggi*, Bologna, 2015
- FRANCESCHELLI, *Il diritto alla riservatezza*, Napoli, 1960
- FRANCHI, *La protezione del nome commerciale, dell'insegna e del marchio nel diritto italiano*, Mantova, 1896
- FREEMAN K., «Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis», in *North Carolina Journal of Law & Technology*, Vol. 18, 2016
- FREEMAN W.C., «California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress», Congressional Research Service, 2018
- FREIWALD S., «First Principles of Communications Privacy», in *Stan. Tech. L. Rev.*, 3, 2007

- FRIED C., «Privacy: A Rational Context», in *Computers, Ethics and Society*, (a cura di) M.D. ERMANN, M.B.WILLIAMS, e C.GUTIERREZ, Oxford University Press, New York 1990
- G. ALPA, «La proprietà dei dati personali», in *Persona e mercato dei dati. Riflessioni sul GDPR*, Zorzi Galgano N. (a cura di), CEDAM, 2019
- GABBRIELLI M., RUFFO U., (a cura di), *Intelligenza Artificiale, dispositivi medici e diritto. Un dialogo fra saperi: giuristi, medici e informatici a confronto*, Giappichelli, Torino 2023
- GALETTA D. U., CORVOLAN J. C., «Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto», in *Federalismi.it*, 2019
- GAMBARO A., voce «Proprietà in diritto comparato», in *Digesto/civ.*, XV, Torino, 1997
- GAMBINO M., «La protezione “multilevel” dei diritti fondamentali (tra Costituzioni, trattati comunitari e giurisdizioni)», in *Scritti in onore di Michele Scudiero*, AA.VV., Napoli, 2007
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (GPDP), *Intelligenza artificiale e ruolo della protezione dei dati personali. L’analisi di Ginevra Cerrina Feroni*, Intervento di Ginevra Cerrina Feroni, vice Presidente del Garante per la protezione dei dati personali, 14 febbraio 2023
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Linee guida cookie e altri strumenti di tracciamento*, 10 giugno 2021
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Rider: Garante privacy, no a discriminazioni basate sugli algoritmi. Sanzione di 2,6 milioni di euro a una piattaforma del gruppo Glovo*, comunicato stampa, 5 luglio 2021

- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Privacy e intelligenza artificiale: vigilare sugli algoritmi. Il contributo del Garante italiano nel Comitato consultivo della Convenzione 108*, Notiziario n. 451 del 25 marzo 2019
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Tik Tok rinvia la pubblicità basata sul legittimo interesse. Per il Garante privacy “una decisione responsabile”*, comunicato stampa del 12 luglio 2022
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Tik Tok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network*, 22 dicembre 2020
- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Tik Tok: Altolà del Garante Privacy alla pubblicità “personalizzata” basata sul legittimo interesse. Base giuridica inadeguata e rischi che la pubblicità arrivi anche ai minori*, comunicato stampa del 11 luglio 2022
- GARDINI G., *Le regole dell’informazione*, Milano, 2009
- GAREIS K., «Die privatrechtssphären in modernen Kulturstaate insbesondere in Deutschen Reiche», in *Zeitschrift für Gesetzgebung und Praxis auf dem Gebiete des Deutschen öffentlichen Rechtes*, 1877
- GARVEY T., *A Brief Overview of Rulemaking and Judicial Review*, Congressional research service, 2017
- GARZONIO «Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social», in *Media Laws*, 2019
- GAVISON, «Privacy and the Limits of the Law», in *Yale Law Journal*, 89, 1980

- GELLIS C.R., «CopySense and Sensibility. How the Wiretap Act Forbids Universities from Using P2P Monitoring Tools», in *B.U. J. Sci. & Tech. L.*, 12, 2006
- GELLMAN, «Edward Snowden, after months of NSA revelations, says his mission's accomplished», in *The Washington Post*, 24 dicembre 2013
- GELLMAN, SOLTANI, B. A., «NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say», in *The Washington Post*, 2013
- GIACOBBE, «Riservatezza (diritto alla)», in *Enc. dir.*, vol. XL, Milano, Giuffrè, 1989
- GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing, 2014
- GOODMAN B., FLAXMAN S., «European Union Regulations on Algorithmic Decision Making and a “Right to Explanation” », in *AI Magazine*, 2017
- GOODMAN B., FLAXMAN S., EU regulations on algorithmic decision-making and a "right to explanation", in *AI magazine*, 83, 2017
- GREENWALD G., «NSA collecting phone records of millions of Verizon customers daily», in *The Guardian*, 6 giugno 2013
- GREENWALD G., *No place to hide. Edward Snowden e la sorveglianza di massa*, Rizzoli, Milano, 2014
- GROPPI, sub art. 7. Rispetto della vita privata e della vita familiare in Bifulco-Cartabia-Celotto, *L'Europa dei diritti*, Bologna, 2001
- GROSSI P., «Inviolabilità dei diritti», in *Enc. Dir.*, XXII, Milano, 1972
- GROSSI P., *Scienza giuridica italiana. Un profilo storico*, Milano 2002
- GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla*

profilazione ai fini del regolamento 2016/679, WP 251 rev.01, adottate il 3 ottobre 2017 (versione emendata e adottata in data 6 febbraio 2018)

- GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Working Document providing guidance on obtaining consent for cookies*, Document n. 2/2013, 2° October 2013 (WP n. 208)
- GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 4/2007 sul concetto di dati personali*, 01248/07/IT, WP 136, 20 giugno 2007
- GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Opinion 03/2013 on purpose limitation*, 00569/13/EN, (WP 2032), aprile 2013
- GUASTALLA E., «Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori», in *Contr. e Impr.*, 1/2018
- H. PLOURDE-COLE H., *Back to Katz: Reasonable Expectation of Privacy in the Facebook Age*, 38, *Fordham Urb. L.J.*, 2, 2010
- HARTZOG W., RICHARDS N., «Privacy's Constitutional Moment and the Limits of Data Protection», in *Boston College Law Review*, 61, 2020
- HEIDEGGER M., *Saggi e discorsi*, Milano 1991
- HELMONS S. M., «La quatrième génération des droits de l'homme», in *Les droits de l'homme au seuil du troisième millénaire*, Bruxelles, Bruylant, 2000
- HERTZA V.A., «Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit? », in *N.Y.U. L. Rev.*, 93, 2018
- HETCHER S., «The De Facto Federal Privacy Commission», in *J. Marshall J. Computer & Info. L.*, 19, 2000

- HILDEBRANDT M., «The Dawn of a Critical Transparency Right for the Profiling Era», in *Digital Enlightenment Yearbook 2012*, (a cura di) HILDEBRANDT ET AL., Amsterdam 2012
- HILDEBRANDT M., *Smart Technologies and the End(s) of Law Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Northampton,
- HILDEBRANDT MIREILLE, «The Dawn of a Critical Transparency Right for the Profiling Era», in *Digital Enlightenment Yearbook*, (IOS Press 2012)
- HODNETT E J.F. WILEY, *Deep Learning Essentials*, Packt Publishing, Birmingham, 2018
- HOOFNAGLE C., *Federal Trade Commission: Privacy Law and Policy*, 132, 2016
- HORVITZ ERIC AND MULLIGAN DEIRDRE, «Data, Privacy, and the Greater Good», in *Science* 6245, 349, 2015
- HYMAN S.J., WALSER-JOLLY G.R., FARRELL E., «What Is a “Reasonable Security Procedure and Practice” Under the California Consumer Privacy Act's Safe Harbor?» in *Consumer Fin. L.Q. Rep.*, 73
- IASELLI, Intelligenza artificiale e robotica, in G. Cassano, V. Colarocco, G. Battista Gallus, F.P. Micozzi (a cura di), *Il processo di adeguamento al GDPR*. Aggiornato al D. lgs. 10 agosto 2018
- IGUAL, SEGUÌ, *Introduction to data science*, Springer, 2017
- INFORMATICS EUROPE & EUACM, *When Computers Decide: European Recommendations on Machine-Learned Automated Decision Making*, 2018
- INFORMATION COMMISSIONER’S OFFICE (ICO), *Big data, artificial intelligence, machine learning and data protection*, versione 2.0, 3/2017
- INFORMATION COMMISSIONER’S OFFICE (ICO), *Big data, artificial intelligence, machine learning and data protection*, versione 2.0, 3/2017

- INFORMATION COMMISSIONER’S OFFICE (ICO), *Feedback request- profiling and automated decision- making*, 2017
- INGRAO, Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act, in Riv. It. Dir. Lav., 2017
- INTERNET SOCIETY, *The Internet of Things: An Overview*, October 2015
- J. H. MOOR, «Towards a Theory of Privacy in the Information Age», in *Computers and Society*, 27, 3, 1997
- JAIN, M. GYANCHANDANI, N. KHARE, «Big Data privacy: a Technological Perspective and Review», in *Journal of Big Data*, 2016
- JOHNSON O.C.A., «The Agency Roots of Disparate Impact», in *Harvard Civil Rights-Civil Liberties Law Review*, 49, 2014
- JOHNSON, H. NISSENABUM, *Computers, Ethics and Social Values*, Prentice Hall, Englewood Cliffs, 1995
- KALTHEUNER F., BIETTI E., «Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR», in *Journal of Information Rights Policy and Practice*, 2018
- KARABOGA, MATZNER, OBERSTELLER, OCHS, «Is There a Right to Offline Alternatives in a Digital World?», in *Data Protection and Privacy: (In)visibilities and Infrastructures*, a cura di Leenes, van Brakel, Gutwirth, De Hert, Springer, 2017
- KAUPER P.G., «Penumbra Peripheries, Emanations, Things fundamental and Things forgotten: the Griswold Case», in *Michigan Law Review*, 1965, vo. 64
- KAUPER, «Penumbra Peripheries, Emanations, Things fundamental and Things forgotten: the Griswold Case», in *Michigan Law Review*, 1965, vo. 64
- Keats Citrow D., «Technological Due Process», in *Wash UL Rev*, 85, 2008

- KELLY-LYTH AISLINN, «Algorithmic discrimination at work», in *ELLJ*, 14(2), 2023
- KIM PAULINE, «Data-Driven Discrimination at Work», in *Wm. & Mary L. Rev.*, 58, 2017
- KITCHEN N. ADRIENNE, «Smart Devices and Criminal Investigations: Protecting Suspects' Privacy and Fourth Amendment Rights», in *crim. Law bulletin* art. 1, 54 NO. 3, 2018
- KLIMAS, VAICIUKAITE J., «The Law of Recitals in European Community Legislation», in *15 Journal of International & Comparative Law* 32, 2008
- KLITOU D., *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014
- KOHLER J., «Das Autorrecht», in *Iherings Jahrbucher*, XVIII, nuova serie VI, stampata a parte nel 1880
- KORFF, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments* (European Commission Directorate-General Justice, Freedom and Security, Working Paper n.2/2010)
- KOSINSKI M., STILWELL D. E GRAEPEL T., *Private traits and attributes are predictable from digital records of human behaviour* [Tratti e attributi privati sono prevedibili dalle registrazioni digitali del comportamento umano], University of California, Berkeley, 2013
- KOSSEFF J., *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020
- KROLL J.A., J. HUEY, BAROCAS S., FELTEN E.W., REIDENBERG J.R., ROBINSON D.G. YU H., *Accountable Algorithms*, 165 Un. Pennsylvania L. R., 633ss. (2017)

- KUNER , D. J. B. SVANTESSON , F.H. CATE , O. LYNSKEY, C. MILLARD, «Machine learning with personal data: is data protection law smart enough to meet the challenge» In *7 International Data Privacy Law*, (2017)
- LA GIOIA F., SARTOR G. «Profilazione e decisione algoritmica: dal mercato alla sfera pubblica» in *federalismi.it*, n. 11/2020
- LANEY, *3D Data Management: Controlling Data Volume, Velocity and Variety*, META Group, 2001
- LAREN, *Allgemeiner Teil des Bürgerlichen Rechts*, C. H. Beck, 8° edizione
- LAUER J., *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*, Columbia University Press, 2017
- LENCA M., ADORNO R., «Towards new human rights in the age of neuroscience and neurotechnology», in *Life Sciences, Society and Policy*, 2017
- LEONARD M.E., «The Changing Expectations of Privacy in the Digital Age» in Lind N.S e Rankin E. (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015
- LESSIG L., *Code 2.0*, Basic Books, 2006
- LETA JONES M., «The right to a human in the loop: Political constructions of computer automation and personhood», in 47, *Social Studies of Science*, 2, 2017
- LEVITIN ADAM, *Facebook: The New Credit Reporting Agency?* Credit slips, 2018
- LIND N.S E RANKIN E. (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015

- LINDON, *La création prétorienne en matière de droits de la personnalité et son incidence sur la notion de famille*, Parigi, 1974,
- LIPPERT, RASMUSSEN, «We Are All Different: Statistical Discrimination and the Right to Be Treated as an Individual», in 15 *J. Ethics*, 54, 2011
- LOSANO M. G., «La legislazione tedesca sulla protezione dei dati», in Camera dei deputati (a cura di), *Banche dati e tutela della persona* Roma, 1983
- LUCCHINI GUASTALLA E., «Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori», in *Contr. e impr.*, n. 1/2018
- LUCIANI M., «Nuovi diritti fondamentali e nuovi rapporti fra cittadino e pubblica amministrazione», in *Riv. crit. dir. priv.*, 1985
- LUCIANI M., *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, studio commissionato dal Servizio Ricerca del Parlamento Europeo (EDPRS), 10/2018
- LYON D., «The Snowden Stakes: Challenges for Understanding Surveillance Today», in *Surveillance and Society*, 13, 2015
- LYON D., *Surveillance After Snowden*, Polity, 2015
- LYON D., Z. BAUMANN, *Liquid surveillance*, Polity Press, 2013
- MACARIO, La protezione dei dati personali nel diritto privato europeo, in Cuffaro e Ricciuto (a cura di), *La disciplina del trattamento di dati personali*, Torino, 1997
- MALGIERI G., «Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' for Algorithmic Decisions in the EU National Legislations», in *Computer Law & Security Review*, 2019

- MALGIERI G., COMANDÈ G., «Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation», in *International Data Privacy Law*, 2017
- MANCINI (a cura di), *L'età di Roosevelt*, Bologna 1962
- MANNING G., «Alexa: can you keep a secret? The third-party doctrine in the age of the smart home», in *American Criminal Law Review*, 56, 2019
- MANTELERO A., «Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo», in *Dir. Inform.* XXVII, I, 2012
- MANTELERO A., «I Big Data nel quadro della disciplina europea della tutela dei dati personali», in *Il Corriere giuridico, ed. speciale*, 2018
- MANTELERO A., «Responsabilità e rischio nel Reg. UE 2016/679», in *NLCC*, 1/2017
- MANTELERO A., *La privacy all'epoca dei Big Data*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino 2019
- MANTELERO A., VACIAGO, *Internet of Things (IoT)*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016*
- MANTELERO, «Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of Data Protection», in *Computer Law & Security Review*, 32, 238, 2016
- MANTEI C.J., «Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches», 53, in *Ariz. L. Rev.*, 2011
- MANYKA ET AL., *Big data: The next frontier for innovation, competition, and productivity*, McKinsey Global Institute, 2011

- MARINELLI, Internet e Web, *Enciclopedia della Scienza e della Tecnica*, Treccani, 2008
- MARINI, «Diritto alla privacy», in *Commentario del Codice Civile*, (diretto da) E. GABRIELLI, UTET, Milano, 2013
- MARR, *What Is The Difference Between Deep Learning, Machine Learning and AI?* Forbes, 2016
- MARTINOTTI M., «La difesa della privacy», in *Pol. dir.*, 1971, p. 771 ss.
- MATHESON J. H., *The Equal Credit Opportunity Act: A Functional Failure*, 21, Harv. J. On Legis., 1984
- MATTEI U., *Common Law. Il diritto anglo-americano*, in *Trattato di diritto comparato*, (diretto da) R. SACCO, Utet, Torino 1992
- MAYER SCHONBERG K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad.it., Garzanti, Milano, 2013
- MAYERS L., *The American Legal System*, Harper & Row, 1964
- MCAFEE, BRYNJOLFSSON, «Big data: the management revolution», in *Harv. Bus. Rev.*, n. 10/2012
- MCCARTHY, MINSKY, ROCHESTER, SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, <https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802>.
- MCINNIS T.N., *The Evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010
- McThomas M., *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013
- MELE, SPADA M., Internet, in *Enciclopedia Italiana – IX Appendice*, Treccani, 2015

- MELUCCI M., *Information Retrieval. Metodi e modelli per i motori di ricerca*, Franco Angeli, 2013
- MENDOZA A., BYGRAVE L.A., The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. Synodinou, P. Jougoux, C. Markou, E T. Prastitou (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017
- MESSINA, «Le prospettive del diritto all’oblio nella società dell’informazione e della comunicazione», in *Inform. dir.*, 2009
- MESSINETTI R., La privacy e il controllo dell’identità algoritmica, in *Contr. impr./Eur.*, 1/2021
- METZGER, «Data as Counter-Performance: What Rights and Duties do Parties Have?» In *Journal of Intellectual Property*, 2017
- MILL J.S., *La libertà* (1859), a cura di L. Einaudi, Torino 1925
- MILL J.S., *Principi di economia politica*, tr. it. di Campolongo, Torino 1953
- MILL J.S.; su tutte: *Sulla “Democrazia in America” di Tocqueville*, tr.it di Valsi, Napoli 1971
- MILLER A., *The Assault on Privacy: Computers, Data Banks and Dossiers*, University of Michigan Press, Cambridge, 1971
- MILLS C.W., «Società di massa e istruzione liberale», in ID., *Sociologia e Conoscenza*, tr. It. Barghini, Milano 1971
- MITTELSTADT B., «From Individual to Group Privacy in Big Data Analytics» in *Philosophy & Technology*, 2017
- MODUGNO F., *I “nuovi diritti” nella giurisprudenza costituzionale*, Giappichelli, Torino 1995
- MORTIER R., HADDADI H., HENDERSON T., MCAULEY D., CROWCROFT J., «Human Data Interaction: The Human Face of the Data-Driven Societ’», in *MIT Technology Review*, 2014

- MULLIGAN D.K., «Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act», in *Geo. Wash. L. Rev.*, 72, 2004
- MUMFORD L., *La cultura delle città*, Edizioni di Comunità, Milano 1954
- MURPHY, «The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment and Statutory Law Enforcement Exceptions», in *Michigan Law Review*, 111, 2013 and 20 USC, 1232g (2012)
- N. RICHARDS N., HARTZOG W., «The Pathologies of Digital Consent», in *Wash. U. L. Rev.*, 96, 2019
- NATIONAL CONFERENCE OF STATE LEGISLATURES (2015a) *Privacy Protections in State Constitutions*, 2015
- NATIONAL CONFERENCE OF STATE LEGISLATURES (2015b) *Security Breach Notification Laws*, 2015
- NATIONAL CONFERENCE OF STATE LEGISLATURES, *Consumer Data Privacy Legislation*, 2019
- NATIONAL CONFERENCE OF STATE LEGISLATURES, *Consumer Data Privacy Legislation*, 2023
- NATIONAL CONSUMER LAW CENTER, *Credit Discrimination § 1.8.1* (7th ed. 2018)
- NATIONAL CONSUMER LAW CENTER, *Fair Credit Reporting, the consumer credit and sales legal practice series*, IX ed., 2017
- NEHF J.P., «Incomparability and the Passive Virtues of Ad Hoc Privacy Policy», in *U. Colo. L. Rev.*, 76, 2005
- NEWELL-MARABELLI, «Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal

effects of “datification”», in *Journal of Strategic Information Systems*, 24/2015

- NEWMAN L. ABRAHAM, *Protectors of Privacy: Regulating Personal Data in the Global Economy*, 2008
- NGUYEN C., «China might use data to create a score for each citizen based on how trustworthy they are», in *Business Insider*, 26 ottobre 2016
- NISSENBAUM H., «Protecting Privacy in an Information Age: The Problem of Privacy in Public», in *Law and Philosophy*, 17 (5), 1998
- NISSENBAUM H., «Protecting Privacy in an Information Age: The Problem of Privacy in Public», in *Law and Philosophy*, 17 (5), 1998
- NOCI, *Biomarketing*, Milano, 2018
- OCSE, *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data*, 1980
- OCSE, *Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data - Explanatory Memorandum*, 1980
- OCSE, *Scoping the OECD AI Principles. Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)*, OECD Digital Economy Papers, No. 291, Novembre 2019
- OFFICE OF TECH. ASSESSMENT, *Electronic Surveillance and Civil Liberties* (Congresso degli Stati Uniti 1985)
- OLIVIERI R.C., «Discriminatory Housing Advertisements Online: Lessons from Craigslist», in *Indiana Law Review*, 42, 2010
- ONDEI E., «Esiste un diritto alla riservatezza», in *Riv. dir. civ.*, 1955
- OPPO G., «Sul consenso dell’interessato», in V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998

- OREFICE M., *I big data e gli effetti su privacy, trasparenza e iniziativa economica*, Roma, 2018
- ORESTANO R., *La riservatezza ancora una volta in Cassazione: fondamento, contenuto e limiti all'indomani dell'entrata in vigore della legge 675/96*
- PACE A., MANETTI M., sub «art. 21. La libertà di manifestazione del proprio pensiero», in *Comm. della Cost.*, (a cura di) Branca, Bologna- Roma, 2006
- PACE G. L., «The Origins of Mass Media in the United States», in A. WELLS; E. A. HAKENEN (a cura di.), *Mass media & society*, Greenwood Publishing Group, 1997
- PAGALLO U., «Three Lessons Learned for Intelligent Transport Systems That Abide by the Law», in *Jusletter IT RZ* 13, 2016
- PAGALLO U., *La tutela della privacy negli Stati Uniti e in Europa. Modelli giuridici a confronto*, Giuffrè, Milano 2008
- PAGALLO U., «Privacy e design», in *Informatica e Diritto*, n. 1/2009
- PALMIERI N.F. III, «Data Protection in an Increasingly Globalized World», in *Ind. L.J.*, 94, 2019
- PALMIERI N.F. III, «Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws», in *Hastings Sci. & Tech. L.J.*, 11, 2020
- PANCONESI, «Programmazione (algoritmi di)», in *Treccani, Enciclopedia della scienza e della tecnica*, 2008
- PAOLUCCI F., «Consenso, intelligenza artificiale e privacy. Commento a: Corte di Cassazione, sez. I Civ. – 25/05/2021, n. 14381», in *Media Laws*, 16 giugno 2021
- PARISER E., *The Filter Bubble: What The Internet Is Hiding From You*, Paperback, 2012

- PARISI A. G., *Privacy e mercato*, Pacini giuridica, Pisa 2020
- PARISI A. G., «Dati, proliferazione e social network: l'emersione di un nuovo modello giuseconomico», in *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, (a cura di) P. STANZIONE, Giappichelli, Torino 2022
- PARKINSON, «Click and Elect: How Fake News Helped Donald Trump Win a Real Election», in *The Guardian*, 14 novembre 2016
- PARLAMENTO EUROPEO, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))(A7- 0402/2013; PE501.927v05-00), 2013
- PARLAMENTO EUROPEO, Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate, Bruxelles, 20 ottobre 2020
- PARLAMENTO EUROPEO, *Risoluzione del Parlamento europeo sull'utilizzo dei dati degli utenti Facebook da parte di Cambridge Analytica e l'impatto sulla protezione dei dati*, 2018/285, 28 ottobre 2018
- PARLAMENTO EUROPEO, *Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD))

- PARRINGTON, *Storia della cultura americana*, tr. it. di Rossi Landi, Torino 1969, III
- PASQUALE F., «Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries», in 104 *Nw. U. L. Rev.*, 2010
- PASQUALE F., *The Black Box Society: The Secret Algorithms that Control Money and Shape Our Minds*, Harvard University Press, 2005
- PASSAGLIA P., «Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità», in *Consulta online, Fascicolo 3*, 2016
- PELINO E., «IA, storica sentenza UE su mutui: nuovi obblighi per le aziende», in *Network Digital 360*
- PELLAEON LIN, «TikTok vs Douyin. A Security and Privacy Analysis», in *The Citizen Lab*, 22 Marzo 2021
- PELLECCIA E., «Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation», in *Nuove leggi civ.*, 2018
- PERLINGIERI C., «Data as the Object of a Contract and Contract Epistemology», in *The Italian Law Journal*, 2019
- PERLINGIERI, «L'informazione come bene giuridico», in *Rass. Dir. Civ.*, 1990
- PERREAU J. A., «Les droits de la personnalité», in *Rev. Trim. dr. Civ.*, Parigi, 1909
- PESCE G., «Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale», in *Giustizia-amministrativa.it*, 2020

- PETRUCCO R., «The Right to privacy and new technologies: between evolution and decay», in *Rivista di diritto dei media*, 1/2019
- PIRAINO F., «Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato», in *Nuove Leggi civ. comm.*, II, 2017
- PITRUZZELLA, «L'Europa del mercato e l'Europa dei diritti», in *federalismi.it*, n.6/2019
- PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, I (Dalla dir. 95/46 al nuovo regolamento europeo) e II (Il regolamento europeo 2016/679), Torino, 2016
- PIZZETTI F., *La Privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, Giuffrè, Milano, 2017
- PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento Europeo*, Torino 2016
- POLANYI K., *La grande trasformazione. Le origini economiche e politiche della nostra epoca*, Torino 1974
- POLLICINO O., M. BASSINI, «La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo», in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, Roma, 2016
- POLLICINO O., M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e di ordine pubblico*, in *Dir. Pen. Cont.*, 2017
- POLLICINO O., «Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale», in *Federalismi.it*, n. 3/2014
- POLLICINO O., «Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli art. 7 e 8 della Carta di Nizza nel

- reasoning di Google Spain», in *Dir. dell'Informazione e dell'Informatica*, 2014
- POLLICINO O., BASSINI M., sub «art. 8», in *Carta dei diritti fondamentali dell'Unione europea*, a cura di Mastroianni, Pollicino, Allegrezza, Pappalardo, Razzolini, Milano, 2017
 - POSNER R.A., «Privacy, Surveillance, and Law», in *U. Chi. L. Rev.*, 75, 2008
 - POUSSON PETIT, «Le personne humaine sur la scène d'un théâtre d'ombres», in *Liber Amicourm Marie-Theres Meulders-Klein*, Bruxelles, 1998
 - PROSSE W. R., «Privacy, a legal analysis», in *California Law Review*, n. 48, 196
 - PUGLIESE G., «Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche», in *Foro it.*, 1954.
 - R. PRUNTY R., SWARTZENDRUBER A., «Social Media and the Fouth Amendment Privacy Protections» in Lind N.S e Rankin E. (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015.
 - RACHLINSKI, JEFFREY J., SHERI LYNN JOHNSON, WISTRICH ANDREW J., AND GUTHRIE C., «Does unconscious racial bias affect trial judges?», in *Notre Dame L. Rev.*, 84, 2008.
 - RATCLIFF, M. WOSKYA, B. MARTINELLO, D. FRANCO, «L'Agenda Digitale Europea», in *Note Tematiche sull'Unione Europea*, 2023
 - RATCLIFF, WOSYKA, MARTINELLO, FRANCO, «L'Agenda Digitale Europea», in *Note Tematiche sull'Unione Europea*, 2023
 - RAUL A. C., FRONZONE C.C E TAPIA S.S., «United States», in Raul A.C. (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019

- RAUL A.C., FRONZONE C.C. E TAPIA S.S., «United States», in Raul A.C (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019
- RAVÀ, *I diritti sulla propria persona nella scienza e nella filosofia del diritto*, RISG, 1901, vol. XXXI, pp. 289-378, vol. XXXII, pp. 1-27
- RAVÀ, *Istituzioni di diritto privato*, Cedam, Padova, 1938
- RAVÀ, *Istituzioni di diritto privato*, Cedam, Padova, 1938
- REDDIX SMALLS B., «Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market», in *12 U.C. Davis Bus. L.J.* 87, 2011
- REDDIX-SMALLS B., «Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market» in *12 U.C. Davis Bus. L.J.* 87, 2011
- REGAN, «Personal information policies in the United States and Britain: The dilemma of implementation considerations», in *Journal of Public Policy*, 4(01), 1984,
- RESTA F., «Art. 7 Condizioni per il consenso», in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Ipsoa, 2018
- RESTA G., «La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE», in *Dir. Inf. e inform.*, 2015
- RESTA G., ZENCOVICH V., «Volontà e consenso nella fruizione dei servizi in rete», in *Rivista trimestrale di diritto e procedura civile*, 2018
- RESTA G., «I diritti della personalità», in G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, in UTET Giuridica, Torino, 2006
- RESTA G., «Identità personale e identità digitale», in *Dir. Inform.*, 2007, III

- RESTA G., «Il diritto alla protezione dei dati personali», in F. Cardarelli, S. Sica, V. Zeno-Zencovich, *Il codice dei dati personali. Temi e problemi*, Milano, 2004
- RESTA G., *Autonomia privata e diritti della personalità*, Napoli, 2005
- RESTA G., V. ZENO-ZENCOVICH, «Volontà e consenso nella fruizione dei servizi in rete», in *Riv. trim. dir. proc. civ.*, 2018
- RICCIO G. M., «Commento artt. 23-27», in S. Sica e P. Stanzione (a cura di), *La nuova disciplina della privacy*, Bologna, 2003
- RICCIUTO V., «Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali», in *Riv. dir. civ.*, 2020
- RICCIUTO V., «Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali», in *Riv. dir. civ.*, 2020
- RICCÒ, «Legge di Moore», in *Treccani, Enciclopedia della Scienza e della Tecnica*, 2008
- RICE D.L., HALM K.C., TROWELL K.K., SISTO A., «Automated Decisionmaking Technology in California: New Rules Would Impose Transparency, Notice, and Consumer Opt-Out Obligations on Businesses», in *Davis Wright Tremain LLP*
- RICH M.L., «Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment», in *U. Pa. L. Rev.*, 164, 2016
- RICHARDS N.M., KING J.H., «Three Paradoxes of Big Data», in *Stanford Law Review Online*, 2013
- RIEBER M., «Fourth Amendment Applies to Cell Site Location Information, in *National Legal Research*», 26 novembre 2018
- RODOTÀ S., «Introduzione», in D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano 2003
- RODOTÀ S., «La “privacy” tra individuo e collettività», *Pol. dir.*, 1974

- RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Jovene Editore, Bologna 1973; ma oggi rist. anast., Jovene Editore, Napoli 2018
- RODOTÀ S., *Il diritto di avere diritti*, Editori Laterza, Roma-Bari 2015
- RODOTÀ S., *Il mondo nella rete. Quali diritti, quali vincoli*, Editori Laterza, Roma Bari, 2014
- RODOTÀ S., *Intervista su privacy e libertà*, a cura di P. Conti, Editori Laterza, 2005
- RODOTÀ S., *Privacy, libertà, dignità*, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati del 16 settembre 2004, Wroclaw, Polonia
- RODOTÀ S., *Riservatezza*, Treccani, Roma 2021
- RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Editori Laterza, Roma Bari 2004
- RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, Eur. Dir. priv., 2004
- ROTHSTEIN MARK, «Is GINA Worth the Wait?», in *J. Law, Medicine & Ethics*, 36, 2008
- RUBECHI, «Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)» in *federalismi.it*, 23/2016
- R. SACCO, *Introduzione al diritto comparato*, UTET, 1992
- SARTOR G., Tutela della personalità e normativa per la protezione dei dati. La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici della «Datenschutz», in *Informatica e diritto*, XII Annata, Vol. XII, 1986
- SARZANA F., «La Corte di Giustizia UE tra GDPR e Artificial Intelligence Act», in *Il Sole 24 Ore*, 8 dicembre 2023

- SAVATIER G., «La promotion juridique contemporaine de la personne, in Id., Les métamorphoses économiques et sociales du droit privé d'aujourd'hui», in *Revue Internationale de Droit Comparé*, III, 1959
- SCARCHILLO G., «Dal Safe Harbor al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems», in *Diritto del Commercio Internazionale*, Anno XXX, Fasc. 4, 2016, p. 901 ss.
- SCHARTUM D. W., «Personvernforordningen og helt automatiserte avgjørelser innen forvaltningsretten », in *Lov&Data*, 2018
- SCHELLING THOMAS C., «Models of segregation (PDF)», in *American Economic Review*, vol. 59, n. 2, 1969
- SCHERMER, *The limits of privacy in automated profiling and data mining*, 27 *Computer law & security review*, (2011)
- SCHNEIDER V., «Locked Out By Big Data: How Big Data Algorithms and Machine Learning May Undermine Housing Justice», in *Columbia Human Rights Law Review*
- SCHONBERG, CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2018
- SCHULTZ D. E J.R. VILE J.R., *The Encyclopedia of Civil Liberties in America*, New York, Routledge, 2015
- SCHWARTZ P.M., «The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures», in 126, *Harv. L. Rev.*, 2013
- SCHWARTZ P.M., PEIFER K.N., «Transatlantic Data Privacy Law», in *Geo. L.J.*, 106, 2017
- SCHWARTZ, PAUL M. «"The value of privacy federalism" in Social dimensions of privacy: Interdisciplinary perspectives», Roessler, Beate, and Dorota Mokrosinska, eds., Cambridge University Press, 2015

- SCORZA G., «L'algoritmo deve essere trasparente, la Cassazione rilancia il GDPR», in *Agenda Digitale*, 26 maggio 2021
- SCORZA GUIDO, «Un hackathon per rendere le privacy policy qualcosa che tutti possano leggere (e capire)», intervento su *Wired*, 2 dicembre 2020
- SCOTT M.D., *Scott on Multimedia Law*, IV ed., Wolters Kluwer, New York, 2019
- SEARLE, *Minds, Brains and Science*, 3, Behavioral and Brain Sciences, 1980
- SEGAL M., *What Is Alternative Finance?* Office of Advocacy, U.S. Small Business, 2016
- SELBST A.D. AND POWLES J., «Meaningful information and the right to explanation», in *7 International Data Privacy Law*, 233, 2017
- SELBST. A.D., BAROCAS S., «The Intuitive Appeal of Explainable Machines», in *Fordham Law Review*, 87, 2018
- Selinger E., Polonetsky J., Tene O. (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018
- SENATO DEGLI STATI UNITI, COMITATO PER IL COMMERCIO, LA SCIENZA E I TRASPORTI, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* [Rassegna del settore degli intermediari: raccolta, utilizzo e vendita di dati sui consumatori per finalità di marketing], rapporto informativo per il presidente Rockefeller, 18 dicembre 2013
- SEVERINO, *La tendenza fondamentale del nostro tempo*, Adelphi, Milano 1988
- SHARONA HOFFMAN, «Big Data and the Americans with Disabilities Act», in *68 Hastings L.J.*, 2017

- SICA S., D'ANTONIO V., «Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles», in V. Zeno Zencovich e G. Resta (a cura di), *La protezione transnazionale dei dati personali: dai Safe Harbour Principles al "Privacy Shield"*, Roma Tre E-Press, Roma, 2016
- SICA S., D'ANTONIO V., RICCIO G.M. (a cura di), *La nuova disciplina europea della privacy*, CEDAM, 2016
- SIMONCINI A., ADINOLFI A. (a cura di), *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, ESI, 2022
- SIMONCINI, Sovranità e potere nell'era digitale, in Frosini-Pollicino-Apa-Bassini, *Diritti e libertà in internet*, Milano, 2017
- SLOANE J.N., «Raising Data Privacy Standards: The United States Need for a Uniform Data Protection Regulation», in 12, *J. Marshall L.J.*, 23, 2019
- SLOUGH, *Privacy, Freedom and Responsibility*, Thomas, 1969
- SOLOVE D., *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, CT, 2013
- SOLOVE D., P.M. SCHWARTZ, *Information Privacy Law*, New York, 2011
- SOLOVE D.J., ROTENBERG M., SCHWARZ P.M., *Privacy, Information and Technology*, Aspen Law & Business, 2006
- SOLOVE D.J., *The Digital Person: Technology and Privacy in the Information Age*, George Washington University of Law School, 2004
- SOLOVE, DANIEL J., BAMBERGER K. AND HARTZOG W., «The FTC and the new common law of privacy», in *Colum. L. Rev.* 114 (2014): 583
- SOLOVE, M. ROTENBERG, P.M. SCHWARZ, *Privacy, Information and Technology*, Aspen Law & Business, 2006,
- SOMMA A., *Introduzione al diritto comparato*, Giappichelli, 2019

- SOMMA A., «I diritti della personalità e il diritto generale della personalità nell'ordinamento della Repubblica Federale Tedesca», in *Riv. Trim. Dir. Proc. Civ.*, Anno L, Fasc. 3, 1996
- SOTOMAYOR S., «Concurring Opinion», in *U.S. v. Jones*, 565 U.S. 400, 2012
- SPLICHAL S.L., «The evolution of computer/privacy concerns: Access to government information held in the balance» in *I, Communication Law and Policy*, 2, 1996
- STANZIONE M.G., «Il Regolamento europeo sulla privacy: origini e ambito di applicazione», in *Europa e Dir. Priv.*, IV/2016
- STANZIONE P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino, 2022
- STANZIONE P. (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino 2022
- STANZIONE P., «Il regolamento europeo sulla privacy: origini e ambito di applicazione», in *Eur. dir. priv.*, 2016
- STANZIONE P., «Introduzione», in *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino 2022
- STEFANINI, *Dati genetici e diritti fondamentali. Profili di diritto comparato ed europeo*, Roma, 2008
- STEGMAIER G.M, W. BARTNICK W., «Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements», in *Geo. Mason L. Rev.*, 20, 2013
- STEINMÜLLER, «Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung», in *NJW*, 1984
- STRAUSS P., RAKOFF T., FARINA C. E METZGER G., *Gellhorn and Byse's Administrative Law: Cases and Comments*, XI ed., Foundation Press, 2011

- SURACE M., *Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di Internet*
- SWIRE P., KENNEDY-MAYO D., *How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information*, 55, EMORY L.J., 2017
- SWIRE P., AHMAD K., *Foundations of Information Privacy And Data Protection*, International Association of Privacy Professionals, Portsmouth, 2012
- TABARRINI C., *La trasparenza algoritmica nel trattamento dei dati personali. Prospettive eurounitarie e statunitensi*, Università Ca' Foscari, Venezia, 2022
- TADDEO, FLORIDI, «New civic responsibilities for online service providers», in *The Responsibilities of Online Service Providers*, (a cura di) TADDEO-FLORIDI, Springer, 2017
- TAVANI H. T., «Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy», in *Metaphilosophy*, 2007
- TEODORO ALAMO T., REINA D.G., GATA P.M., PRECIADO V.M., GIORDANO G., *Data-driven methods for present and future pandemics: Monitoring, modelling and managing*, in Elsevier, 29 giugno 2021
- TEROLLI E., *Privacy e protezione dei dati personali IE vs USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, Diritto dell'informazione e dell'informatica, 1, 2021
- THE SOCIETY FOR HUMAN RESOURCE MANAGEMENT (SHRM), *Research Spotlight: Credit Background Checks*, Society Human Resource Management, 2010
- THE WHITE HOUSE, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 ottobre 2023

- THOBANI S., «Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente», in *Media Laws*, 2018
- THOBANI S., «La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità», in *Europa e Diritto Privato*, 2016
- TIMIANI M., «Un contributo allo studio sul diritto alla riservatezza», in *SPPC*, 2/2012
- TOKSON M., «Automation and the Fourth Amendment», in *Iowa L. Rev.*, 96, 2011
- TOSI E. (a cura di), *Privacy digitale*, Giuffrè Francis Lefebvre, 2019
- TRUCCO L., *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione europea*, Torino, 2013
- TRUCCO L., «Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali», in *Giur. it.*, 2014,
- TSAI, LAI C., CHAO H., VASILAKOS A. V., «Big Data analytics: a survey», in *Journal of Big Data*, 2015
- TURILLI M., FLORIDI L., «The ethics of information transparency», in *Ethics and Information Technology*, 2009, 11, 2, 105
- TURING A., *Computing Machinery and Intelligence*, Mind, 1950
- U.S. DEPARTMENT OF HOMELAND SECURITY, *Report to the Public on the Transportation Security Agency's Security Flight Program and Privacy Recommendations*, Washington D.C., Dicembre 2006
- UFFICIO DEL COMMISSARIO AUSTRALIANO PER L'INFORMAZIONE, *Bozza di consultazione: Guide to big data and the Australian Privacy Principles* [Guida ai megadati e ai principi australiani in materia di tutela della vita privata], 05/2016

- UMBERTAZZI T. M., *Diritto alla privacy, natura e funzioni giuridiche*, CEDAM, Pavia 2005
- VALSECCHI A., «Algoritmo, discrezionalità amministrativa e discrezionalità del giudice (nota a Cons. Stato, sez. VI, sent. del 4 febbraio 2020, n. 881)», in *Ius in itinere*, 14 settembre 2020
- VANNUCCHI G., «Internet e le dinamiche dei ruoli degli OTT (Over The Top) e Telco nel panorama ICT», in *Mondi digitale*, n. 5/ 2015
- VARANO V., BARSOTTI V., *La tradizione giuridica occidentale. Testo e materiali per un confronto tra civil law e common law*, G. Giappichelli Editore, Torino 2021, 3, sez. I e III
- VEALE E EDWARDS, «Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling», in *Computer Law & Security Review*, 2018
- VIGLIANISI FERRARO A., «La sentenza Google Spain ed il diritto all’oblio nello spazio giuridico europeo», in *Contr. impr./Eur.*, 2015
- VILLANI, *Dalla Dichiarazione universale alla Convenzione europea dei diritti dell’uomo*, Bari, 2015
- VIVANTE, *Trattato di diritto commerciale*, vol I, Le persone, 2^a edizione, Torino 1902
- WACHTER S., MITTELSTADT B., RUSSELL C., «Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR», in *Harvard Journal of Law & Technology*, 31 (2), 2018
- WACHTER S., MITTLESTADT B., «A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI» in *Colum. Bus. L. Rev.*, 2019

- WACHTER S., «Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR», in *Computer L. & Security Rev.*, 2018
- WACHTER S., MITTELSTADT B., FLORIDI L., «Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», in *International Data Privacy Law*, 2017
- WACHTER S., MITTELSTADT B., RUSSEL C., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 2017
- WARREN S., BRANDEIS L., «The Right to Privacy», in *Harvard Law Review*, 1890, vol. V, n. 5, pp. 193-220
- WATCHER S., MITTELSTADT B., RUSSEL C., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 2017
- WEISS R. M., MEHROTRA A. K., Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce, in 6 *Va. J.L. & Tech.*, 11 (2011)
- WESTIN A.F., in M. Greenberger (a cura di), *Computers, Communications, and the Public Interest* (Baltimore, Md.: The Johns Hopkins Pr.ss), 1971
- WESTIN A. F., *Privacy and Freedom*, Atheneum Press, New York 1967
- WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY, *Blueprint for an AI Bill of Rights. Making Automated Systems Work for the People*, ottobre 2022
- WHITMAN, «The Two Western Culture of Privacy: Dignity Versus Liberty», in *The Yale Law Journal*, Vol. 113, No. 6, 2004
- WIGGIN TEKE, «Steering 2.0? Data may undermine fair housing laws», in *Inman News*, April 2014
- WILLIAMS R.C., «Due Process, Class Action Opt Outs, and the Right Not to Sue», in 115 *COLUM. L. Rev.*, 2015

- WINKLER M.M., MOSCA J., «Cloud computing e protezione dei dati personali», in M. Fumagalli Meraviglia (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?* Napoli, Editoriale Scientifica, 2015
- WITTEN, FRANK, HALL, PAL, *Data Mining. Practical Machine Learning Tools and Techniques*, Morgan Kaufmann-Elsevier, 2017
- WOLF R. P., MARCUSE H., MOORE B. JR., *Critica della tolleranza*, Einaudi, 1970
- YEUNG, «Towards an understanding of regulation by design», in *Regulating technologies. Legal futures, regulatory frames and technological fixes*, a cura di Brownsword-Yeung, London, Hart publishing, 2008
- ZARSKY T. «Understanding Discrimination in the Scored Society» in *Washington Law Review*, 2014
- ZARSKY T., «Transparent predictions», in 4 *University of Illinois Law Review*, 2013
- ZENO-ZENCOVICH V., Informazione (profili civilistici), in *Dig. disc. Priv.*, sez. civ., IX, Torino, 1993
- ZENO-ZENCOVICH V. (a cura di), *Le banche dati in Italia*, Napoli, 1985
- ZENO-ZENCOVICH V., «Do “Data Markets” Exist?», in *MediaLaws*, I, 2019
- ZORLONI L., «Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto», in *Wired*, 23 marzo 2021
- ZUBOFF S., *Il Capitalismo della Sorveglianza. Il Futuro dell’Umanità nell’Era dei Nuovi Poteri*, Luiss University Press, 2019
- ZUIDERVEEN BORGESIUUS F., «Online Price Discrimination and Data Protection Law», in *Amsterdam Law School Research Paper*, 2015

- ZWEIGERT K., KOTZ H., *Introduzione al diritto comparato. Vol. I: principi fondamentali*, Giuffrè, Milano 1998

GIURISPRUDENZA E PROVVEDIMENTI ESSENZIALI

- App. Milano, 26.8.1960, in *Foro it.*, 1961, I, 43
- App. Roma, 17.5.1955, in *Foro it.*, 1956, I, 793.
- BGH, 26.11.1954, in *BGHZ*, vol. 13 (1954), p. 34 ss.
- BGH, 28.1.2014, in *VI ZR*, 156/13
- BVerfG, 14 gennaio 1973, in *BVerfGE*, vol. 34, 1973, p. 269 ss
- BVerfG, 15.12.1983, in *BVerfGE*, 1984, 65, pp. 1-71
- C. Cost, 139/1990, in *Foro it.*, 1990, I, p.2410
- C. Cost, 7.08.05, n. 271, in *Foro it.*, 2006, 129, X, p. 2661 ss.
- C. Cost., 12.4.1973, n. 38, in *Foro it.*, 1973, I, 170.
- C. Cost., 26 Giugno 1969, n. 104, in *Foro It.*, vol. 92, no. 9, 1969,
- C. Cost., sentt. nn. 348 e 349 del 2007.
- C. Giust. UE 19 ottobre 2016, C-582/2014, *P. Breyer c. Bundesrepublik Deutschland*
- C. Giust. UE 7.12.2023, causa C-634/21, *OQ c. Land Hessen*, c.d. *SCHUFA*
- C. Giust. UE, 13-5-2014, causa C-131/12, *Google Spain SL*.
- C. Giust. UE, 16-07-2020, C-311/18, *Data Protection Commissioner/Maximilian Schrems e Facebook Ireland*, c.d. *Schrems II*
- C. Giust. UE, 21-12-2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*
- C. Giust. UE, 29-1-2008, C-275/06, *Promusicae*

- C. Giust. UE, 4 maggio 2017, C-13/16, *Rīgas satiksme*
- C. Giust. UE, 6-10-2015, C-362/14, *Schrems*, c.d. *Schrems I*
- C. Giust. UE, 8-4-2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*
- C. Giust. UE, 9-11-2010, C-92/09 e C-93/09, *Volker und Markus Schecke GbR*
- C. Giust. UE, procedimenti riuniti C-509/09 (*eDate Advertising GmbH c. X*)
- C.Giust.UE, 1-10-2019, C-673/17, *Planet 49*
- *Carpenter v. United States* (No. 16-402, 585 U.S. 2018)
- Cass. civ., Sez. I, 2 luglio 2018, n. 17278, in *Giur. It.*, 2019, 3
- Cass. Civ., sez. I, ordinanza n. 14381/21, depositata il 25 maggio 2021.
- Cass. n. 17278-18, Cass. n. 16358-18.
- Cass., 20.4.1963, n. 990, in *Foro it.*, 1963, I, 877,
- Cass., 20.4.1963, n. 990, in *Giur. it.*, 1963, I, 1, 961
- Cass., 22.6.1985, n. 3769, in *Nuova giur. comm.*, 1985, 647
- Cass., 9.6.1998, n. 5658, in *Foro it.*, 1998, I, 2387
- Cass., sez. I, 22.12.1956, n. 4487, in *Foro it.*, 1957, I, 4.
- Cass., sez. I, 27.5.1975, n. 2129, in *Foro It.*, 1976, I
- *Charles Katz v. United States*, 389 U. S., 347 (1967)
- Cons. Stato Sez. VI, Sent., 13-12-2019, n. 8472
- Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881
- Cons. Stato, Sez. VI., 8 aprile 2019, n. 2270
- Corte EDU (Grande Camera), nn. 12738/10, *Jeunesse c. Olanda*, 3 ottobre 2014;
- Corte EDU *Godelli c. Italia*, 2 sez., 25 settembre 2012.
- Corte EDU, *Henry Kismoun c. Francia*, V sez., 5 dicembre 2013.

- Corte EDU, *I c. Finlandia*, n. 20511/03, 17 luglio 2008.
Corte EDU, *Leander c. Svezia*, 26 marzo 1987.
- Corte EDU, *Malone c. Regno Unito*, 2 agosto 1984
- Corte EDU, *Mennesson c. Francia*, Grande Camera, 26 giugno 2014;
- Corte EDU, *S. e Marper c. Regno Unito*, 4 dicembre 2008
- Corte EDU, *Von Hannover c. Germania*, V. sez., 19 settembre 2013.
- *Florida v. Riley* (488 U.S. 455, 1989).
- *FTC v. CompuCredit Corporation e Jefferson Capital Systems, LLC*. Civil No. 1:08-CV-1976- BBM-RGV 2008
- GPDP, Provv. Doc. web. N. 7496252 del 21 dicembre 2017
- GPDP, Provv. 14 luglio 2013, n. 330, doc. web n. 2542348.
- GPDP, Provv. 28 maggio 1997, doc. web. 40425
- GPDP, Provv. n. 134 del 14 giugno 2019, [doc. web n. 9121486]
- GPDP, Provv. N. 234 del 10 giugno 2021, [doc. web n. 9675440]
- GPDP, Provv. N. 234 del 10 giugno 2021, [doc. web n. 9675440]
- GPDP, Provv. N. 285 del 22 luglio 2021, [doc. web n. 9685994]
- GPDP, Provv. n. 321 del 20 luglio 2017, [doc. web n. 6843736],
- GPDP, Provv. n. 488 del 24 novembre 2016, doc. web n. 5796783
- GPDP, Provv. N. 5 del 10 gennaio 2019, [doc. web n. 9080914]
- GPDP, Provv. N. 50 del 10 febbraio 2022, [doc. web n. 9751362]
- GPDP, Provv. N. 50 del 10 febbraio 2022, [doc. web n. 9751362]
- GPDP, Provv. n. 515 del 21 novembre 2013, [doc. web n. 2765110]
- GPDP, Provv. n. 861 del 15 novembre 2012, [doc. web n. 2099774],
- GPDP, Provv. n. 248 del 7 luglio 2022, [doc. web n. 9788429]
- GPDP, Provv. n. 43 del 5 marzo 2020, [doc. web n. 9304455],
- *Griswold v. Connecticut*, 381, U. S. 479 (1965).

- *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist.*, 251 F. Supp. 3d 1168, punto 1171 (S.D. Tex. 2017).
- *In Re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001)
- *Kyllo v. United States* 533 U.S. 27 (2001),
- *Lawrence v. Texas*, 539 U.S. 558 (2003)
- *Olmstead v. United States*, 277, U.S. (1928)
- *Public Utilities v. Pollak*, 343, U. S. 467
- *Riley v. California*, 573 U.S., 373 (2014)
- *Roe v. Wade*, 410 U.S., 113 (1973)
- *Smith v. Maryland*, 442 U.S. 735 (1979)
- T. Roma, 14.9.1953, in *Foro it.*, 1954, I, 115
- T. Roma, 14.9.1953, in *Foro it.*, 1954, I, 115
- T.A.R. Lazio-Roma, Sez. III bis, sentenza n. 3742/2017.
- T.A.R. Lazio-Roma, sez. III, sentenza n. 4409 del 15 aprile 2021.
- T.A.R. Lazio, Roma, Sez. III-bis, 22 marzo 2017, n. 3769.
- T.A.R. Lazio, Roma, Sez.III-bis, 10-13 settembre 2019, n. 10964.
- *U.S. v. Jones*, 565 U.S. 400 (2012).
- *United States v. Bynum* ,604 F.3d 161 (2010)
- *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012)
- *United States v. Miller*, 425 U.S. 435 (1976)
- *United States v. Skinner*, 690 F.3d 772 6th Cir. (2012)

NORMATIVA ESSENZIALE

- Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 10 des Gesetzes vom 22. Dezember 2023 (BGBl. 2023 I Nr. 414) geändert worden ist (Normativa Federale sulla Protezione dei Dati)
- Carta dei diritti fondamentali dell'Unione Europea, (2000/C 364/01)
- Children's Online Privacy Protection Act (COPPA), 1998 (15 U.S.C. § 6501-06)
- Civil Rights Act, Title VII, 1964 (42 USC § 2000e ss.)
- Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act), 2003 (15 U.S.C. §§ 7701–7713 and 18 U.S.C. § 1037)
- Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, n. 108 del 1981
- D.lgs. 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR (GU Serie Generale n.205 del 04-09-2018)
- D.lgs. 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali», (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174)
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

- Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali
- Direttiva 2002/58/CE del Parlamento e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; c.d. Direttiva E-Privacy
- Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori
- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- Electronic Communications Privacy Act (ECPA), 1986 (18 U.S.C. § 2510 ss.)
- Equal Credit Opportunity Act (ECOA), 1976, (15 U.S.C. § 1691 ss.)
- Fair Credit Reporting Act (FCRA), 1970 (15 USC § 1681 ss.)
- Fair Housing Act (FHA), (42 U.S.C. § 3601ss.)
- Federal Trade Commission Act, 1914 (15 U.S.C. §§ 41–58)
- Financial Services Modernization Act (Gramm–Leach–Bliley (GLB) Act), 1999 (15 U.S.C. §§ 6801–6827).
- Health Insurance Portability and Accountability Act (HIPAA), 1996 (42 U.S.C. §§ 1301ff.)

- Loi no. 78-17 du 6. janvier 1978 relative à l’informatique, aux fichiers et aux liberté
- Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), 2017/0003 (COD)
- Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)
- R. d., 16 marzo 1942, n. 262, Approvazione del testo del Codice civile, (GU Serie Generale n.79 del 04-04-1942)
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- Trattato sul funzionamento dell’Unione Europea (TFUE)
- Trattato sull’Unione Europea (TUE)
- U. S. Patriot Act, 2001, (H.R. 3162)
- U.S. Privacy Act, 1974 (5 U.S.C. § 552 ss.)

SITOGRAFIA ESSENZIALE

- Academia.edu: <https://www.academia.edu>
- Altalex: <https://www.altalex.com>
- California Law Review: <https://www.californialawreview.org>

- Commissione Europea: https://commission.europa.eu/index_it
- Congressional Research Service: <https://crsreports.congress.gov>
- National Conference of State Legislatures: <https://www.ncsl.org>
- Consiglio d'Europa: <https://www.coe.int/it/web/portal>
- Cornell Law School - Legal Information Institute: <https://www.law.cornell.edu>
- Corte Costituzionale: <https://www.cortecostituzionale.it/default.do>
- Corte di Cassazione: <https://www.cortedicassazione.it>
- Corte di Giustizia: https://curia.europa.eu/jcms/jcms/j_6/it/
- Corte Europea dei Diritti dell'Uomo: <https://www.echr.coe.int>
- EDPB: https://edpb.europa.eu/edpb_en
- EDPS: <https://www.edps.europa.eu/en>
- Enciclopedia Treccani: <https://www.treccani.it/enciclopedia/>
- EUR-Lex: <https://eur-lex.europa.eu/homepage.html?locale=it>
- Federalismi.it: <https://www.federalismi.it>
- Federal Trade Commission: <https://www.ftc.gov/>
- Garante Privacy: <https://www.garanteprivacy.it>
- Gazzetta Ufficiale: <https://www.gazzettaufficiale.it>
- Giustizia Amministrativa: <https://www.giustizia-amministrativa.it>
- IBM: <https://www.ibm.com/it-it>
- JSTOR: <https://www.jstor.org>
- Library of Congress: <https://www.loc.gov>
- ResearchGate: <https://www.researchgate.net>
- SSRN: <https://www.ssrn.com/index.cfm/en/>

