INTELLIGENZA ARTIFICIALE E DIRITTO: UNA RIVOLUZIONE?

A CURA DI
ALESSANDRO PAJNO, FILIPPO DONATI E ANTONIO PERRUCCI

VOLUME I
DIRITTI FONDAMENTALI, DATI PERSONALI E REGOLAZIONE

SOCIETÀ EDITRICE IL MULINO

Alla pubblicazione di questa ricerca ha contribuito il Gruppo AlmavivA, che Astrid vivamente ringrazia

ISBN 978-88-15-29967-3

Redazione e produzione: Edimill srl - www.edimill.it

CAPITOLO NONO

LA RILEVANZA DELLE BASI GIURIDICHE PER IL TRATTAMENTO DI DATI PERSONALI MEDIANTE SISTEMI DI INTELLIGENZA ARTIFICIALE

1. *Premessa*

L'apporto di macchine dotate di sistemi di intelligenza artificiale, o comunque capaci di svolgere azioni o di anticipare o influenzare processi decisionali senza il diretto intervento dell'uomo, è stato oggetto di riflessioni e speculazioni teoriche sin dai primi studi sull'impatto della cibernetica e dell'informatica nella società[1]. Oggi, diversamente dal passato, tali entità non operano soltanto seguendo programmi rigorosamente predeterminati (come lo stesso etimo della parola *programma* indica) ed attingendo esclusivamente alla propria *esperienza*, ma sono chiamati a sfruttare ed implementare il bacino indefinito di informazioni che fluisce nella rete, apparendo così capaci di potenziare in maniera indefinita le proprie capacità di base senza necessariamente dover emulare o sviluppare

Questo capitolo è di Giovanni Maria Riccio e Giorgio Giannone Codiglione. Lo scritto, pur se unitariamente concepito, deve essere nelle sue parti così attribuito: a G.M. Riccio, il paragrafo 2, a G. Giannone Codiglione i rimanenti paragrafi.

[1] Senza pretesa di esaustività si rimanda alle pionieristiche riflessioni di V. Frosini, *Cibernetica diritto e società*, Milano, 1968, in part. pp. 111 ss., il quale si interrogava sull'opportunità di considerare un robot dotato di intelligenza artificiale come un soggetto morale, in un conflitto tra coscienza interna (propria dell'uomo come essere che nasce da ζωή) e coscienza esterna (potenziamento della prima, frutto della tecnica); M.C. Ciampi (a cura di), *Artificial Intelligence and Legal Information Systems*, Amsterdam-Tokyo, 1982; G. Sartor, *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Milano, 1990; Id., *Gli agenti software: nuovi soggetti del cyberdiritto?*, in «Contratto e impresa», 2002, pp. 465 ss.

forme intuitive (cioè basate su meccanismi cognitivi causali induttivo-deduttivi) di coscienza[2].

Dall'approccio eziologico, che studia un determinato evento per ricollegarlo in maniera univoca ad un altro, si staglia nella sua elementare immediatezza un diverso schema operazionale che fa capo al concetto di correlazione, inteso come il risultato ottenuto dall'analisi e dalla sovrapposizione di un indefinito numero di informazioni, dal contenuto variabile e non necessariamente organizzato secondo criteri e standard prestabiliti, che disveli l'esistenza di rapporti biunivoci tra uno o più elementi (o valori) tali da potere constatare, sulla base di criteri statistico/percentuali, un certo grado di influenza reciproca[3]. In altre parole, l'approccio

[2] M.G. Losano, *Informatica per le scienze sociali*, Torino, 1985, pp. 38 ss.; B. Latour, *Politics of Nature: How to Bring the Sciences into Democracy*, Boston, 2004; E. Mazzarella, *L'androide Philip Dick. Identità umana e artificio. Idee per una libertà sostenibile*, in P. Barcellona, F. Ciaramelli e R. Fai (a cura di), *Apocalisse e postumano. Il crepuscolo della modernità*, Bari, 2007, pp. 415 ss.

[3] Secondo il pluricitato volume di V. Mayer-Schönberger e K. Cukier, *Big Data*, Milano, 2013, p. 76, la correlazione rappresenta una «relazione statistica tra i valori di due dati». La nozione di correlazione in generale si sviluppa sia nelle scienze sociali (come quelle economico/statistiche, la sociologia o, ancora, la linguistica) che nelle scienze di base o naturali (ad es. la fisica). In entrambi i campi si tratta di ricercare un rapporto di interdipendenza tra due elementi, caratteristiche o valori, per cui uno può variare in un certo modo in funzione dell'altro. In argomento cfr. anche R. Kitchin, *Big Data, New Epistemologies and Paradigm Shifts*, in «Big Data and Society», 2014, pp. 1-12; M.L. Ambrose, *Lessons from the Avalanche of Numbers: Big Data in Historical Perspective*, in «I/S: A Journal of Law and Policy for the Information Society», 201, 2015; V. Zeno-Zencovich e G. Giannone Codiglione, *Ten Legal Perspectives on the «Big Data Revolution»*, in «Concorrenza e mercato», 2016, n. 23, pp. 29-57; V. Zeno-Zencovich, *Legal Epistemology in the Times of Big Data*, in S. Faro e G. Peruginelli (a cura di), *Knowledge of the Law in the Big Data Age*, Amsterdam, 2019, pp. 3-9; J.-S. Bergé, S. Grumbach e V. Zeno-Zencovich, *The «Datasphere», Data Flows Beyond Control, and the Challenges for Law and Governance*, in «European Journal of Comparative Law & Government», 5, 2018, n. 2, pp. 144-178; T.E. Frosini, O. Pollicino, E. Apa e M. Bassini (a cura di), *Diritti e libertà in Internet*, Firenze, 2017, pp. 23 ss. Sui concetti di «causalità» e «correlazione» nella letteratura scientifica cfr. ad es. G.U. Yule, *On The Methods Of Measuring Association Between Two Attributes*, in «Journal of the

correlativo mira a fornire indicazioni *nuove* agli umani (o ancora ad entità non umane programmate per attuare ordini o elaborare schemi d'azione), formulate sulla base di un certo grado di parentela e coerenza tra determinate informazioni, che risultino *utili* nel senso di suggerire o confermare un risultato o un postulato, predire un determinato fenomeno o produrre inferenze orientando le attitudini e le capacità di scelta e comportamento nello spazio e nel tempo[4].

Il funzionamento efficiente dei sistemi di IA presuppone pertanto il costante afflusso di informazioni digitali, siano esse *nuove* – nel senso di essere state raccolte e immesse nel sistema per la prima volta (si pensi ai dati relativi a un fenomeno meteorologico accaduto qualche ora prima) – o ancora frutto di una precedente raccolta, archiviazione, rielaborazione ed aggiornamento[5].

Royal Statistical Society», 75, 1912, n. 6, p. 579; K. Pearson, *Notes on the History of Correlation*, in «Biometrika», 1920, pp. 1 ss.; M.C. Galavotti, *Causalità, leggi, spiegazione*, in «Quaderni di storia dell'economia politica», 1987/1988, n. 5/6, pp. 121-133; A. Marradi, *Linee guida per l'analisi bivariata dei dati nelle scienze sociali*, Milano, 1997, *passim*.

[4] L'approccio computazionale, imperniato sull'avvento dei *big data* viene considerato un modello di ricerca interdisciplinare tra scienze sociali, scienze informatiche e scienze complesse passibile di poter incidere in maniera netta sul generale metodo di studio della biologia e della fisica. In tale contesto sono state intraprese diverse esperienze empiriche o di ricerca basate su metodi computazionali e funzioni precipuamente predittive: grazie alla lettura incrociata di enormi dataset, frutto dell'afflusso di molteplici punti di raccolta, è possibile ad esempio ricostruire le interazioni che avvengono in un dato luogo geografico con una precisione pari quasi ad una scala di 1 a 1, raggiungendo una definizione elevata non solo con riguardo alla mera rappresentazione grafica. In questo modo, appare più agevole comprendere quale percorso stradale possa risultare maggiormente scorrevole al fine di raggiungere una determinata meta, quale elemento ambientale o comportamentale spinga uno o più soggetti ad agire per il perseguimento di un determinato scopo di consumo, o, ancora è possibile favorire l'elaborazione automatica di ordini e schemi comportamentali di un robot o di una protesi bionica innestata nel corpo umano, raggiungendo gradi di precisione tali da proclamarne l'autonomia o, comunque, favorendo la perfetta integrazione di una «cosa» nella sfera biologica della persona che ha subito l'impianto.

[5] Sul tema, in una sconfinata letteratura cfr. le riflessioni svolte secondo diversi angoli prospettici da J. Kaplan, *Intelligenza artificiale. Guida al prossimo futuro*, Roma, 2017; K. Crawford, *Atlas of AI*, New

Tale fondamento tecnico dei sistemi di IA (come della maggior parte delle attività economiche e sociali collegate alle tecniche di estrazione ed elaborazione di dati su larga scala) conduce a un'apparente crisi della regola giuridica, soprattutto ove si ponga mente all'impossibilità di individuare in maniera univoca lo statuto giuridico dell'informazione digitale[6].

Declinata tale questione in una prospettiva di tutela della persona umana, è giocoforza rilevare come tutte le tipologie di informazioni assorbite dai sistemi di IA risultino in astratto riconducibili entro la nozione di dato personale dettata dal legislatore europeo[7], da cui il connesso, centrale,

Haven-London, 2021, p. 57; L. Malvaldi e D. Leporini, *Capra e calcoli. L'eterna lotta tra gli algoritmi e il caos*, Roma-Bari, 2014; D. Cardon, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Milano, 2017; G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in «Politica del diritto», 2019, n. 2, pp. 199-236, ma sia consentito rimandare anche a G. Giannone Codiglione, *Metodo scientifico e funzioni del diritto nella società attuale: dalla causalità alla correlazione?*, in *Studi in onore di Pasquale Stanzione*, I, Napoli, 2019, pp. 137 ss.

[6] E. Resta, *Il tempo e lo spazio del giurista*, in G. Comandè e G. Ponzanelli, *Scienza e diritto nel prisma del diritto comparato*, Torino, 2003, pp. 253 ss., in part. 255 s., si interroga con profondità e chiarezza sul problema dell'afasia immanente alla ricerca di una dommatica del bene giuridico «informazione»; cfr. anche S. Rodotà, *Vivere la democrazia*, Bari-Roma, 2018, p. 17 e sia altresì consentito rimandare alla riflessione svolta in G. Giannone Codiglione, *Internet e tutele di diritto civile*, Torino, 2020, *passim*.

[7] Sulla portata dell'art. 4, n. 1, del GDPR, il quale estende la nozione di dato personale non solo a «qualsiasi informazione concernente una persona fisica identificata o identificabile» (art. 2, lett. *a*, dir. 95/46), ma all'insieme delle informazioni relative ad una persona fisica, anche nelle ipotesi di un trattamento multiplo, avendo riguardo per gli identificativi prodotti da dispositivi online (Indirizzo IP, cookies, ecc.) o di quei dati che, nonostante la pseudonimizzazione, possano essere oggetto di combinazione con ulteriori informazioni in modo da rendere possibile, direttamente o indirettamente, l'identificazione dell'interessato, sia consentito rinviare a G. Giannone Codiglione, *«Risk-based approach» e trattamento dei dati personali*, in S. Sica, V. D'Antonio e G.M. Riccio, *La nuova disciplina europea della privacy*, Padova, 2016, pp. 55 ss.; ma cfr. anche F. Pizzetti, *La protezione dei dati personali e le sfide dell'Intelligenza Artificiale*, in AA.VV., *Intelligenza artificiale, protezione dati*

problema della corretta individuazione della base giuridica del trattamento e, ancora, della rilevanza che tale operazione ricopre nell'ambito della liceità delle finalità perseguite dai sistemi di IA (e quindi del loro complessivo funzionamento).

2. *I limiti della base giuridica del consenso nel trattamento multiplo di dati da parte dei sistemi di IA*

Il GDPR rinnova il quadro delle regole generali in tema di liceità del trattamento dei dati personali, accostando alla regola di validità del consenso prestato dall'interessato (a1) ulteriori basi giuridiche, quali: a2) il collegamento tra attività di sfruttamento ed esecuzione di un contratto in cui una delle parti coincide con l'interessato; a3) l'adempimento di un obbligo legale da parte del titolare; a4) il perseguimento di un legittimo interesse del titolare o di un terzo, a patto che esso non prevalga sulle prerogative dell'interessato; a5) l'esecuzione di un compito di interesse pubblico o, ancora, a6) la salvaguardia degli interessi vitali dell'interessato o dei consociati (art. 6 del GDPR).

Focalizzando l'attenzione in via preliminare sulla regola del consenso[8], meglio esplicata nel successivo art. 7 e al-

personali e regolazione, Torino, 2018, pp. 5 ss., in part. p. 40; G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati*, in «Giurisprudenza italiana», 2019, n. 7, pp. 1657 ss., la quale rileva che «muovendo dalla definizione di dato personale, si può constatare che la maggior parte delle informazioni è costituita da dati personali»; S. Calzolaio, voce *Protezione dei dati personali (dir. pubbl.)*, in *Digesto discipline pubblicistiche*, Agg., Torino, 2017, pp. 594 ss.; G. Mobilio, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in «Federalismi.it», 2020, n. 16, pp. 266 ss., in part. p. 277.

[8] In argomento cfr. D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, in «Giurisprudenza italiana», 2019, n. 12, pp. 2783 ss.; Ead., *Art. 6. Liceità del trattamento*, in R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta, *Codice della privacy e data protection*, Milano, 2021, pp. 192 ss.; M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, pp. 179 ss., pp. 219 ss.; F. Resta, *Sub art. 6, reg. UE n. 679/2016*, in G.M. Riccio, G. Scorza e E. Belisario, *GDPR e Normativa Privacy. Commentario*,

tresì richiamata dall'art. 9, par. 2, del GDPR in materia di protezione di particolari categorie di dati personali, spicca un'aperta contraddizione tra effettività della norma e prassi operazionale. Se, infatti, il sistema di intelligenza artificiale opera in primo luogo in un'ottica di elaborazione quantitativa e multifunzionale dei dati raccolti, la prestazione del consenso dell'interessato, connessa in primo luogo all'adempimento dei doveri di informazione e trasparenza, è vincolata in termini di efficacia *pro futuro* dal principio di limitazione delle finalità, secondo cui il titolare deve raccogliere i dati per finalità preventivamente determinate, esplicite e legittime e, successivamente, deve trattare gli stessi in modo che tali attività non risulti incompatibile con tali finalità (art. 5, par. 1, lett. *b* del GDPR)[9].

Il gestore del sistema di IA – in questa sede inteso come il soggetto cui può essere ricondotta la nozione di titolare del trattamento – incontrerebbe pertanto non pochi problemi nel rinvenire una copertura completa in termini di liceità del trattamento nel caso di indicazione del consenso

Milano, 2018, pp. 63 ss.; F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, pp. 103 ss.; E. Pelino, *I diritti dell'interessato*, in L. Bolognini, E. Pelino e C. Bistolfi (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, pp. 171 ss.

[9] N. Forgó, S. Hänold e B. Schütze, *The Principle of Purpose Limitation and Big Data*, in M. Corrales, M. Fenwick e N. Forgó (a cura di), *New Technology, Big Data and the Law*, Singapore, 2017, pp. 20 ss.; Gruppo di lavoro *ex* art. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 6/2/2018, p. 12: «La compatibilità di tale ulteriore trattamento con le finalità originarie per le quali i dati sono stati raccolti dipenderà da una serie di fattori, tra gli altri, le informazioni che il titolare del trattamento ha inizialmente fornito all'interessato. Tali fattori si riflettono nel regolamento e sono così riassunti: – il rapporto tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento; – il contesto in cui i dati personali sono stati raccolti e le ragionevoli aspettative dell'interessato in merito al loro uso futuro; – la natura dei dati; – l'impatto dell'ulteriore trattamento sull'interessato; – le garanzie applicate dal titolare del trattamento per assicurare un trattamento corretto e prevenire qualsiasi impatto indebito sull'interessato».

dell'interessato quale base giuridica, atteso che il consenso è limitato sia in senso qualitativo (ovvero in relazione alla tipologia di finalità perseguita), sia in senso quantitativo, nel senso che si assesta perlopiù ad un primo stadio delle operazioni di trattamento, non contemplando ad esempio l'eventuale, successivo, trasferimento dei dati da un titolare all'altro o la loro condivisione[10].

Sul punto, la Suprema Corte ha sottolineato come il consenso al trattamento dei dati personali non possa essere equiparato al consenso in generale richiesto a fini negoziali[11]. Le norme europee in materia di validità della manifesta-

[10] Sulla nozione di consenso nell'ambito della liceità del trattamento dei dati personali cfr. S. Sica, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in «Rivista di diritto civile», 2001, pp. 621 ss.; F. Caggia, *Libertà ed espressione del consenso*, in Cuffaro, D'Orazio e Ricciuto, *I dati personali nel diritto europeo*, cit., pp. 253 ss.; S.F. Giovannangeli, *L'informativa agli interessati e il consenso al trattamento*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, pp. 99 ss.; L. Montuori e M. Siano, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. Busia, L. Liguori e O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Roma, 2016, pp. 101 ss.

[11] Ossia quello «prestato da un soggetto capace di intendere e volere e non viziato da errore, violenza o dolo, ovvero, in determinati frangenti, da pericolo o da bisogno: consenso, quello così previsto, che pur sussiste quantunque perturbato, al di sotto di una determinata soglia, in ragione dei vizi indicati, secondo quanto risulta dagli articoli 1428, 1435 e 1439 c.c.». Nel caso di specie, attinente a un'ipotesi di consenso al trattamento dei dati personali per finalità di marketing, connessa all'offerta di un servizio di newsletter, la S.C. ha rilevato che «il consenso in discorso, alla luce del dato normativo, è tale da non ammettere compressioni di alcun genere e non sopporta di essere sia pure marginalmente perturbato non solo per effetto di errore, violenza o dolo, ma anche per effetto dell'intero ventaglio di possibili disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate dal titolare del trattamento». Così Cass., sez. I, 2/7/2018, n. 17278, *Garante protezione dati personali c. Soc. Ad spray*, in «Giurisprudenza italiana», 2019, p. 530, con nota di S. Thobani. Sui requisiti del consenso nella giurisprudenza eurounitaria cfr. CGUE, grande sez., 1/10/2019, causa C-673/17, *Planet49*, in «Raccolta digitale», 2019; CGUE, 11/11/2020, causa C-61/19, *Orange România c. ANSPDCP*, *ibidem*, 2020.

zione della volontà dell'interessato rispetto al trattamento effettuato dal titolare prescrivono infatti che il consenso debba essere: *a*) espresso e, dunque, dotato di una propria autonomia; *b*) libero, ossia pienamente consapevole e non già frutto di alcun condizionamento; *c*) specifico, ossia inequivocabilmente riferito a ciascun particolare effetto del trattamento; *d*) informato, ovvero condizionato alla circostanza che all'interessato siano state previamente offerte le informazioni.

Tale indirizzo interpretativo – che pone sul titolare un vincolo informativo-procedimentale fortemente limitativo della propria libertà di trasferire e conglomerare dati ai fini del loro utilizzo nell'ambito dei sistemi di IA – ha trovato ampia conferma nella prassi applicativa, come testimonia l'ampia casistica formatasi in materia di attività di telemarketing svolto con mezzi automatizzati.

In ambito municipale, il d.lgs. 196/2003 (cd. Codice privacy) così come modificato dal d.lgs. 101/2018 stabilisce infatti, all'art. 130, primo comma che

> l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso del contraente o utente,

per poi specificare al comma 3 che «ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 6 e 7 del Regolamento nonché ai sensi di quanto previsto dal comma 3-bis»[12].

[12] Il menzionato comma 3-bis dispone poi che, in deroga a quanto previsto dall'art. 129 del Codice, il trattamento dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico mediante l'impiego del telefono e della posta cartacea per le finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale «è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario e degli altri

Il codice individua in generale nel consenso la base giuridica del trattamento dei dati personali a fini di marketing, prevedendo tre distinte regole: *a*) nel caso di telemarketing attuato con funzioni automatizzate (e dunque senza l'intervento dell'operatore), il trattamento è lecito solo con il consenso dell'interessato; *b*) nel caso di telemarketing attuato con modalità diverse da quelle indicate alla precedente lett. *a*, il trattamento è consentito ai sensi degli articoli 6 e 7 del Regolamento, oppure, *c*) nel caso di trattamento dei dati presenti negli elenchi pubblici di cui all'art. 129, comma primo del codice, se l'interessato non ha espresso il diritto di opposizione (cd. *opt-out*).

Con particolare riferimento all'ipotesi di cui alla lett. *b*, il tenore della disposizione ripropone l'art. 130, comma 3, del codice previgente per cui «fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24», con l'unica differenza che gli artt. 23 e 24 del codice previgente disciplinavano il «Consenso» e i «Casi nei quali può essere effettuato il trattamento senza consenso» (nel senso che l'uno avrebbe pertanto escluso l'applicazione dell'altro), mentre gli artt. 6 e 7 del Regolamento rispettivamente enumerano le diverse basi giuridiche ai fini della declaratoria di liceità del trattamento sembra porre il consenso in una posizione di alternatività e di equiordinazione rispetto al legittimo interesse del titolare, disciplinando poi in una disposizione separata le condizioni per il consenso[13].

La copiosa casistica del Garante precedente all'entrata in vigore del GDPR ha poi circoscritto il regime di cd. *opt-out* (che consentiva di iniziare liberamente il trattamento, riconoscendo all'interessato il diritto di opporsi successivamente)

dati personali di cui all'articolo 129, comma 1, in un registro pubblico delle opposizioni».

[13] Per mera completezza, va osservato che l'art. 130, comma 3, fa salvo l'utilizzo di «mezzi diversi» da quelli indicati ai precedenti commi 1 e 2, quali, ad esempio, messaggi tipo *pop-up* nelle applicazioni per dispositivi mobili o nei siti internet.

alle sole comunicazioni commerciali mediante posta cartacea e alle chiamate con operatore (cd. marketing tradizionale), per il fatto che tali attività avrebbero una portata meno invasiva[14]. Al contrario, il preventivo consenso dell'interessato è risultato sempre necessario per l'invio di comunicazioni elettroniche promozionali con sistemi automatizzati[15]. In

[14] GPDP, provv. 15/5/2013, doc. web n. 2543820: «nella richiamata ottica di contemperamento degli interessi coinvolti e di valorizzazione del principio di semplificazione di cui al citato art. 2, comma 2, del Codice, l'interessato che esprime il proprio consenso, sulla base del menzionato art. 130, commi 1 e 2, del Codice, relativamente al trattamento svolto per le precipue finalità indicate dalla norma e con le specifiche modalità automatizzate ivi richiamate, acconsente anche alla ricezione di comunicazioni a carattere promozionale inviate attraverso modalità tradizionali di contatto meno invasive, come la posta cartacea e le chiamate telefoniche con operatore»; GPDP, provv. 19/1/2011, doc. web n. 1784528, oltreché ai casi di cd. soft-spam (Opinione WP29, 27/2/2004, n. 5, 9 ss).

[15] Cass., 24/6/2014, n. 14326; Trib. Padova, 4/4/2013; Cass., 4/2/2016, n. 2196, nonché linee guida GPDP, 4/7/2013, doc. web n. 2542348: «Ai trattamenti effettuati ai fini promozionali tramite strumenti automatizzati o a questi equiparati si applica l'art. 130, commi 1 e 2, del Codice, in base al quale l'utilizzo di tali strumenti per le finalità di marketing è consentito solo con il consenso preventivo del contraente o utente (cd. opt-in). Quindi, ai fini della legittimità della comunicazione promozionale effettuata, non è lecito, con la medesima, avvisare della possibilità di opporsi a ulteriori invii, né è lecito chiedere, con tale primo messaggio promozionale, il consenso al trattamento dati per finalità promozionali. Pertanto, senza il consenso preventivo – come costantemente ribadito dal Garante a partire dal provvedimento generale sullo *spamming* del 29/5/2003 (doc. web n. 29840) – non è possibile inviare comunicazioni promozionali con i predetti strumenti neanche nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti web, atti o documenti conosciuti o conoscibili da chiunque. Analogamente, senza il consenso preventivo degli interessati, non è lecito utilizzare per inviare e-mail promozionali gli indirizzi pec contenuti nell'"indice nazionale degli indirizzi pec delle imprese e dei professionisti" – di cui al d.l. 18/10/2012, n. 179, convertito con modificazioni dalla l. 17/12/2012, n. 221, che ha introdotto l'apposito art. 6-bis del d.lgs. 7/3/2005, n. 82 (Codice dell'amministrazione digitale) – istituito per favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica. È possibile, invece, contattare telefonicamente mediante operatore (per chiedere al contraente di esprimere un consenso a ricevere comunicazioni promozionali secondo le modalità di cui all'art. 130, commi 1 e 2) i numeri presenti in elenchi telefonici e non iscritti

particolare, le linee guida in materia di *spamming* emanate dal Garante nel 2013 hanno rilevato in via preliminare che «il titolare del trattamento deve acquisire un consenso specifico per ciascuna distinta finalità quali ad esempio: marketing, profilazione, comunicazione a terzi dei dati»[16]; tuttavia puntualizzando che «le suddette attività sono funzionali, nella maggior parte dei casi, a perseguire un'unica finalità (*lato sensu*) di marketing, con la conseguenza che il connesso trattamento appare giustificare – sempre di norma – l'acquisizione di un unico consenso»[17].

Quanto alla peculiare ipotesi di comunicazione a terzi dei dati personali raccolti dal titolare per finalità di marketing – caso che ben si potrebbe adattare alle attività svolte in seno ai sistemi di IA, basate sovente sulla condivisione, cessione o comunicazione di basi di dati – il Garante ha chiarito che la comunicazione o cessione a terzi di dati personali per finalità di marketing non può fondarsi sull'acquisizione di un unico e generico consenso da parte degli interessati per siffatta finalità, per cui

chi, quale titolare del trattamento, intenda raccogliere i dati personali degli interessati anche per comunicarli (o cederli) a terzi per le loro finalità promozionali deve previamente rilasciare ai medesimi un'idonea informativa, ai sensi dell'art. 13, comma 1, del Codice, che individui, oltre agli altri elementi indicati nella norma, anche ciascuno dei terzi o, in alternativa, indichi le categorie (economiche o merceologiche) di appartenenza degli stessi

nel Registro pubblico delle opposizioni (istituito con il d.l. 25/9/2009, n. 135, convertito, con modificazioni, dalla l. 20/11/2009, n. 166), nonché quelli presenti in elenchi pubblici "con i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati", fra i quali "vi è il vincolo di finalità in base al quale i dati sono raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altri trattamenti in termini compatibili con tali scopi (art. 11, comma 1, lett. *b* del Codice)": cfr. provvedimento 19/1/2011 (doc. web n. 1784528)».

[16] Cfr. GPDP, provv. 24/2/2005, punto 7, doc. web n. 1103045.

[17] Cfr., fra gli altri, anche GPDP, provv. 9/3/2006, doc. web n. 1252220; provv. 24/5/2006, doc. web n. 1298784; provv. 15/11/2007, doc. web n. 1466985.

(ad esempio: «finanza», editoria», «abbigliamento»: cfr. lettera *d* della detta norma)[18].

A conferma di tale assunto, le citate linee guida prescrivevano che

occorre che il titolare acquisisca un consenso specifico per la comunicazione (e/o cessione) a terzi dei dati personali per fini promozionali, nonché distinto da quello richiesto dal medesimo titolare per svolgere esso stesso attività promozionale. Qualora l'interessato rilasci il suddetto consenso per la comunicazione a soggetti terzi, questi potranno effettuare nei suoi confronti attività promozionale con le modalità automatizzate di cui all'art. 130, comma 1 e 2, senza dover acquisire un nuovo consenso per la finalità promozionale. Si chiarisce che, ai fini del Codice, il terzo o i terzi in questione possono appartenere a categorie economiche o merceologiche anche diverse da quella del titolare del trattamento che provvede alla raccolta dei dati dell'interessato[19].

[18] Cfr., *ex multis*, GPDP, provv. 11/10/2012, doc. web n. 2089777; provv. 19/5/2011, doc. web n. 1823148; provv. 12/5/2011, doc. web n. 1813953; provv. 7/10/2010, doc. web n. 1763037; provv. 15/7/2010, doc. web n. 1741998; cfr. anche Trib. Roma 5/10/2011 n. 19281, ma cfr. anche il vademecum *Marketing e privacy* pubblicato dal GPDP nel 2015, per cui «se si è chiesto a una persona il consenso per il trattamento dei suoi dati per attività di marketing, non si può far finta che questo consenso valga anche per scopi differenti come la profilazione o la comunicazione dei dati a terzi. È quindi necessario acquisire un autonomo consenso per ogni finalità, prevedendo apposite caselle nel modulo eventualmente predisposto a tale scopo».

[19] Sul punto, il GPDP ha aggiunto che «nel caso in cui i terzi siano stati individuati singolarmente e siano stati forniti all'interessato anche gli altri elementi previsti all'art. 13 del Codice relativi al trattamento che verrà da questi svolto, non sarà necessario che i predetti soggetti rilascino agli interessati un'ulteriore informativa in quanto, come specificato all'art. 13, comma 2 del Codice, l'informativa "può non comprendere gli elementi già noti alla persona che fornisce i dati". Laddove invece la richiesta di consenso non sia accompagnata da un'informativa con tali requisiti, i terzi – ai sensi dell'art. 13, comma 4, del Codice – potranno inviare ai medesimi interessati le comunicazioni promozionali in questione solo dopo il rilascio di una propria informativa, che contenga, oltre agli elementi previsti dall'art. 13, comma 1, anche l'origine dei dati personali a loro comunicati, in modo tale che ciascun interessato possa rivolgersi anche al soggetto che li ha raccolti e comunicati per opporsi al trattamento ai sensi dell'art. 7, comma 4, lett. *b* del Codice.

Sempre in tema di attività di marketing diretto svolto attraverso l'invio di messaggi di posta elettronica, la Suprema Corte ha ribadito che l'interessato deve essere con certezza posto in condizione di raffigurarsi, in maniera inequivocabile, gli effetti del consenso prestato al trattamento dei propri dati, da cui la conseguenza che

se detto consenso comporta una pluralità di effetti – come nel caso di specie, in cui esso si estende alla ricezione di messaggi promozionali anche da parte di terzi –, lo stesso va singolarmente prestato in riferimento a ciascuno di essi, di modo che, con totale trasparenza, risulti palese che proprio ciascuno di tali effetti egli ha voluto. È dunque senz'altro da escludere che il consenso possa dirsi specificamente, e dunque anche liberamente, prestato in un'ipotesi in cui, ove gli effetti del consenso non siano indicati con completezza accanto ad una specifica «spunta» apposta sulla relativa casella di una pagina Web, ma siano invece descritti in altra pagina Web linkata alla prima, non vi sia contezza che l'interessato abbia consultato detta altra pagina, apponendo nuovamente una diversa «spunta» finalizzata a manifestare il suo consenso[20].

In entrambi i casi, inoltre, i terzi dovranno fornire all'interessato un idoneo recapito – di cui all'art. 130, comma 5 – presso il quale poter esercitare utilmente i diritti di cui all'art. 7 (cfr. provvedimento 7/4/2011, doc. web n. 1810207), ed essere assicurata al medesimo la possibilità di avvalersi, a tal fine, dello stesso canale comunicativo utilizzato per l'invio delle comunicazioni promozionali e comunque di uno strumento quanto più possibile agevole, rapido, economico ed efficace (cfr. al riguardo parere n. 5/2004 del Gruppo art. 29). Ad esempio, se i terzi intendono inviare e-mail pubblicitarie, devono consentire agli interessati di potersi opporre al trattamento inviando una e-mail a un indirizzo di posta indicato nell'informativa resa ed eventualmente riservato alla gestione delle problematiche sul trattamento dati sottoposte loro da utenti e clienti».

[20] Cass., 2/7/2018, n. 17278, cit.: «Perché il consenso possa essere detto specifico, che esso, per la contraddizione che non lo consente, non possa essere genericamente riferito a non meglio identificati messaggi pubblicitari, sicché colui il quale abbia chiesto di fruire di un servizio di informazioni giuridico-fiscali, si debba vedere poi raggiunto da pubblicità di servizi o prodotti non attinenti alle ricerche effettuate. È allora specifico, per questo aspetto, il consenso se riferito "ad un trattamento chiaramente individuato", il che comporta la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti».

Ancora più di recente, con provvedimento dell'11/12/2019 (cd. provvedimento EGL), il Garante ha fissato il principio per cui le considerazioni espresse con riferimento alla specificità del consenso dell'interessato, in particolare sotto il profilo della individuazione del titolare e delle finalità del trattamento cui sono destinati i dati personali,

permettono di affermare la illiceità delle cessioni di dati personali effettuate da titolari del trattamento che non abbiano acquisito direttamente dagli interessati uno specifico consenso al riguardo. Il complesso delle disposizioni contenute negli articoli 6 e 7 del Regolamento e dei correlati Considerando (nn. 42 e 43) mirano a conferire all'interessato il pieno controllo dei trattamenti di dati personali per i quali egli stesso ha prestato il consenso. Tale controllo sarebbe del tutto irrealizzabile se le comunicazioni di dati personali potessero avvenire in assenza di un consenso direttamente riconducibile ad ogni soggetto cedente e fossero solamente ancorate ad una iniziale manifestazione di volontà capace di dispiegare effetti a catena del tutto imprevedibili per l'interessato[21].

Alla luce degli indirizzi interpretativi sin qui sintetizzati[22], la base giuridica del consenso preventivo e informato, ove

[21] Nel medesimo provvedimento, il Garante conclude affermando che «le cessioni, da C4b s.r.l. a EGL, nonché i correlati successivi trattamenti da parte di quest'ultima, di liste di contattabilità provenienti da Facile.it S.p.A., le quali non sono sorrette da alcun consenso rilasciato dagli interessati a C4b s.r.l., così come tutte le altre cessioni e i correlati trattamenti di liste provenienti da editori, acquisite da *list provider* e cedute a EGL senza che i *list provider* si siano dotati di un consenso specifico alla comunicazione dei dati, sono illeciti e ne deve essere disposto il divieto. Le condotte poste in essere dalla società configurano la violazione delle disposizioni di cui all'art. 5, par. 1, lett. *a*, all'art. 5, par. 2, all'art. 6, par. 1, lett. *a*, all'art. 7, par. 1, del Regolamento».

[22] Per un'interpretazione difforme cfr. ad es. Trib. Cagliari, sez. I, sent., 18/5/2017, in «Dejure», in materia di cessione di dati genetici, per cui «occorre partire dalla premessa per cui non è dato di rinvenire nell'ordinamento giuridico alcuna disposizione di legge, o comunque contenuta in atti a contenuto normativo, che disciplina specificamente l'ipotesi in cui all'originario titolare del trattamento dei dati personali succeda un altro titolare. È quanto avvenuto nel caso di specie, dato che a S.D. s.r.l., dichiarata fallita, è succeduta l'odierna ricorrente, acquirente dell'azienda. Non risulta neppure che la questione sia stata mai affrontata dalla giurisprudenza italiana, tanto di legittimità quanto di merito. (…) Pur

declinata nella prospettiva di trattamento multiplo attuato da un sistema di IA, da un lato appare in contrasto con la garanzia effettiva del *pieno controllo* dei dati da parte dell'interessato. Dall'altro lato, guardando al bilanciamento degli interessi del titolare, la configurazione di un obbligo indiscriminato di raccolta di una nuova manifestazione di volontà qualora il trattamento si discosti in maniera oggettiva (ad es. sotto il profilo delle modalità, finalità o del tempo del trattamento) o soggettiva (qualora per esempio trovi modifica la figura del titolare) si pone in conflitto con il limite normativo dell'impossibilità o della sproporzione dell'intervento o delle misure adottate. Tale limite, menzionato dal legislatore europeo in relazione all'esecuzione degli obblighi di notifica di cui all'art. 19 del GDPR[23], è stato applicato in altri ambiti dalla Corte di giustizia, tenendo in debita considerazione la necessità di garantire un equo bilanciamento tra gli obiettivi normativi perseguiti e la sostenibilità economica da parte del soggetto che si deve far carico dell'attuazione della misura, ad esempio nel senso di eccessiva onerosità[24].

con le indubbie difficoltà del caso, ritiene questo giudice che la soluzione adottata dal Garante non sia corretta, non condividendosi la premessa di fondo, ovverosia che in caso di mutamento del titolare del trattamento, e perciò soltanto, sia sempre e comunque necessaria l'acquisizione di una nuova manifestazione del consenso da parte degli interessati».

[23] R. Torino, *Sub art. 19, Reg. UE n. 679/2016*, in Riccio, Scorza e Belisario, *GDPR e Normativa Privacy. Commentario*, cit., pp. 199-201; M. Renna, *Sub art. 19, reg. 2016/679/UE*, in E. Gabrielli (dir.), *Commentario del codice civile*, A. Barba e S. Pagliantini (a cura di), *Delle persone. Leggi collegate*, vol. II, Torino, 2019, pp. 355-378, in part. 369 ss.; G. Giannone Codiglione, *Art. 19. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento*, in D'Orazio, Finocchiaro, Pollicino e Resta, *Codice della privacy e data protection*, cit., pp. 342 ss.

[24] Cfr. ad es. CGUE, 12/7/2011, C-324/09, *L'Oréal c. eBay e al.*, in «Raccolta», 2011, p. I-06011; CGUE, 4/11/2011, C-70/10, *Scarlet c. SABAM*, ivi, 2011, p. I-11959, par. 48: «Un'ingiunzione di questo genere causerebbe una grave violazione della libertà di impresa del FAI in questione, poiché l'obbligherebbe a predisporre un sistema informatico complesso, costoso, permanente e unicamente a suo carico, il che risulterebbe peraltro contrario alle condizioni stabilite dall'art. 3, n. 1, della Direttiva 2004/48, il quale richiede che le misure adottate

Nel rapporto tra norme comunitarie e norme nazionali, emergono tuttavia dei toni di grigio, nel senso che, in talune fattispecie, il consenso non appare l'unica base giuridica potenzialmente utilizzabile dal titolare del trattamento. Si allude, in particolare, alle ipotesi dei soggetti già clienti del titolare del trattamento o dei clienti cosiddetti *prospect* ossia di quei soggetti che, pur non avendo concluso un contratto, hanno richiesto informazioni sui prodotti o sui servizi del titolare.

In merito a tali ultimi soggetti, occorre innanzitutto osservare che, con riferimento all'attività di marketing, l'art. 130, comma 4 del Codice privacy declina il meccanismo del consenso «nel contesto della vendita di un prodotto o di un servizio». Stando a un'interpretazione letterale della norma, parrebbe, pertanto, che per poter utilizzare una base giuridica diversa dal consenso (compreso il legittimo interesse), è necessario che tra il titolare e l'interessato sussista una relazione contrattuale (legata, appunto, a una vendita); circostanza che, com'è evidente, non sussiste con riferimento al cliente cd. *prospect*. Un caso diverso, a parere di chi scrive, è però quello del soggetto che faccia richiesta di un preventivo, atteso che, in tale fattispecie, si realizza un rapporto di natura contrattuale, seppur atipica, che potrebbe legittimare, adottando un'interpretazione più ampia dell'art. 6, par. 1, lett. *f* del GDPR, l'invio di ulteriori informazioni sino a quando sopraggiunga l'eventuale opposizione da parte del soggetto interessato.

3. *Basi giuridiche diverse dal consenso dell'interessato e trattamento di dati nei sistemi di IA, tra flessibilità applicativa e «accountability»*

Al di là della complessa adattabilità della base giuridica del consenso ai trattamenti svolti attraverso sistemi di IA, l'art. 6 del GDPR si contraddistingue per una spiccata aper-

per assicurare il rispetto dei diritti di proprietà intellettuale non siano inutilmente complesse o costose».

tura verso l'evoluzione dei servizi offerti nell'ambito del cd. web 2.0, nonché di tutti i sistemi connessi all'elaborazione massificata di dati, prendendo in considerazione il problema del trattamento svolto per finalità diverse da quelle per cui i dati sono stati raccolti (cd. trattamento secondario).

La base giuridica del trattamento di dati personali effettuato da sistemi di IA può infatti essere individuata nella necessità di dare esecuzione di un contratto tra titolare o interessato (o ancora nell'esistenza stessa di un rapporto di natura negoziale), nel perseguimento di obiettivi *lato sensu* pubblicisti o nell'adempimento di un obbligo legale, la tutela di un interesse vitale dell'interessato e il perseguimento di un legittimo interesse del titolare o di un terzo.

Se nell'ipotesi di sistemi di IA gestiti ed implementati da soggetti pubblici o per il perseguimento di obiettivi di pubblico interesse, il GDPR indica necessariamente nella disciplina di dettaglio delegata al legislatore il presupposto di liceità del trattamento, nelle altre ipotesi il titolare è tenuto comunque ad effettuare un'attività di valutazione della conformità del trattamento ai principi di necessità e proporzionalità, con particolare riguardo agli scopi perseguiti dal trattamento principale. Come specificato dall'art. 6, par. 4 del GDPR, tale vaglio preventivo di compatibilità dovrebbe tenere in considerazione ogni possibile nesso sussistente tra le diverse finalità, il contesto in cui i dati personali sono stati raccolti, la loro natura, le possibili conseguenze dell'ulteriore trattamento e l'esistenza di garanzie adeguate volte a minimizzare i rischi ad esso sottesi, quali la cifratura o la pseudonimizzazione. Soltanto qualora il trattamento ulteriore risultasse compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti, non sarebbe richiesta alcuna base giuridica separata[25].

Una peculiare ipotesi di base giuridica introdotta dal GDPR e in astratto affine all'implementazione dei sistemi di IA è poi rappresentata dal perseguimento di un interesse legittimo da parte del titolare o di un terzo: secondo il Regolamento,

[25] Considerando n. 50 del GDPR.

i legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi, possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento[26].

In via esemplificativa, il GDPR enumera alcune situazioni in cui potrebbero sussistere dei legittimi interessi: *a*) la sussistenza di 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; *b*) il trattamento di dati personali strettamente necessari a fini di prevenzione delle frodi; *c*) il trattamento di dati personali per finalità di marketing diretto; *d*) il trattamento svolto per finalità amministrative interne all'interno di un gruppo imprenditoriale o di enti collegati a un organismo centrale; *e*) il trattamento di dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione[27].

[26] Considerando n. 46 del GDPR.

[27] Secondo il parere del Gruppo di lavoro *ex* art. 29 n. 6/2014, *Sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9/4/2014, rimarcava come «il concetto di interesse legittimo potrebbe comprendere un'ampia serie di interessi, sia di scarso rilievo che decisamente preminenti, evidenti oppure più controversi. Sarà poi in una seconda fase, quando si tratterà di valutare questi interessi rispetto agli interessi e ai diritti fondamentali degli interessati, che occorrerà adottare un approccio più restrittivo ed effettuare un'analisi più sostanziale». L'elenco stilato dal Gruppo comprende: – esercizio del diritto alla libertà di espressione e d'informazione, anche nei mezzi di comunicazione e di espressione artistica; – commercializzazione diretta tradizionale e altre forme di commercializzazione o pubblicità; – messaggi indesiderati non commerciali, anche a fini di campagne politiche o di raccolta fondi per scopi benefici; – esercizio di un diritto in via giudiziale, compreso il recupero del credito tramite procedure extragiudiziali; – prevenzione di frodi, uso improprio dei servizi o riciclaggio di denaro; – controllo del personale a fini di sicurezza o gestione; – procedure per la denuncia delle irregolarità; – sicurezza fisica, sicurezza informatica e sicurezza

Resta escluso da tale ambito di applicazione il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei propri compiti, atteso che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali.

In ogni caso,

> 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. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali[28].

La prospettiva dell'individuazione del legittimo interesse quale base giuridica alternativa al consenso dell'interessato, o ancora sussidiaria e comunque equiordinata rispetto a quest'ultimo, obbliga pertanto il titolare a un attento vaglio preventivo dell'architettura del trattamento progettato in una prospettiva di ragionevole (e consapevole, poiché informata) aspettativa da parte dell'interessato che possa aver luogo un trattamento per finalità ulteriori[29].

Tale principio è stato di recente confermato dal Garante italiano, il quale sempre in materia di telemarketing ha sottolineato come il legittimo interesse del titolare del trattamento «deve essere accompagnato da un attento bilanciamento, peraltro adeguatamente documentato, tra i diritti degli interessati e le aspettative circa il trattamento

della rete; – trattamento di dati a scopi statistici o di ricerca storica o scientifica; – trattamento a scopi di ricerca (compresa la ricerca a fini commerciali)».

[28] Considerando n. 47 del GDPR.

[29] G. Finocchiaro, *Il principio di «accountability»*, in «Giurisprudenza italiana», 2019, p. 2781; C. D'Agata, *Il legittimo interesse del titolare o di un terzo nel quadro dei diversi presupposti di legittimità del trattamento*, in Panetta, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 81 ss.

dei relativi dati personali e l'interesse del titolare stesso»[30]. L'applicazione della base giuridica del legittimo interesse presuppone

la prevalenza in concreto (in base a un bilanciamento rimesso al titolare, ma sempre valutabile dall'Autorità di controllo) di quest'ultimo sui diritti, libertà e meri interessi degli interessati (nello specifico, i destinatari delle comunicazioni promozionali non assistite dal consenso). In tale confronto, è necessaria l'attenta ponderazione dell'impatto del trattamento, che si intende effettuare su tali diritti, libertà ed interessi (fra cui, nel caso del marketing, sono ravvisabili anzitutto il diritto alla protezione dei dati e il diritto alla tranquillità individuale dell'interessato)[31].

In materia giova ricordare come nel parere n. 6/2014 del Gruppo di lavoro *ex* art. 29 sia stato tracciato uno schema con alcuni fattori utili da considerare nell'esecuzione del test comparativo e tra di essi interconnessi, quali: *a*) la valutazione della natura e dell'origine dell'interesse legittimo del titolare del trattamento; *b*) l'impatto sugli interessati; *c*) il raggiungimento di un soddisfacente bilanciamento provvisorio con i diritti e le libertà dell'interessato e *d*) l'eventuale adozione di garanzie supplementari per evitare qualsiasi indebito impatto sugli interessati[32].

La disciplina del trattamento per finalità ulteriori di cui all'art. 6, par. 4 del GDPR e il cd. test di comparazione, previsto nel caso in cui il titolare individui la base giuridica del perseguimento del legittimo interesse quale presupposto di liceità del trattamento, rappresentano delle declinazioni del generale principio di trattamento dei dati personali in maniera non rischiosa[33], cui deve necessariamente accostarsi

[30] GPDP, provv. 25/3/2021, doc. web n. 9670025.

[31] GPDP, provv. 15/1/2020, doc. web n. 9256486.

[32] Gruppo di lavoro *ex* art. 29, *Sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, parere n. 6/2014, adottato il 9/4/2014.

[33] In generale sul tema della regolazione del rischio in relazione alla tutela dei dati personali si vedano i contributi di R. Gellert, *Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative*, in «International Data Privacy Law»,

l'innovativa disciplina in materia di valutazione dell'impatto e consultazione preventiva, che sostituisce l'obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali previsto dall'art. 18, dir. 95/46.

Com'è noto, il GDPR implementa un sistema di responsabilizzazione del titolare del trattamento che si sostanzia anche nel dovere di sottoporre a una valutazione d'impatto alcune particolari tipologie di trattamenti dei dati personali previamente indicati dall'Autorità di controllo e, in generale, che presentino «un rischio elevato per i diritti e le libertà delle persone fisiche» (art. 35)[34]. Una volta svolta la preventiva valutazione dei rischi sottesi a un determinato trattamento, il titolare prima di iniziare a svolgere quell'attività deve comunque consultare l'autorità di controllo qualora emerga che il trattamento presenti «un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio».

Ai sensi dell'art. 35, nel contesto di attività di sfruttamento che implicano l'uso di nuove tecnologie e che presentano rischi elevati per i diritti e le libertà delle persone fisiche, il titolare è tenuto ad effettuare una valutazione dell'impatto sortito da tali trattamenti sul generale assetto di protezione dei dati personali. La valutazione d'impatto rappresenta dunque una tappa obbligatoria per tutte quelle forme di trattamento molto rischiose: tra queste attività, l'art. 35, n. 3 individua in via esemplificativa la sorveglianza

2015, n. 5, pp. 3 ss.; D. Kloza, N. van Dijk e P. De Hert, *Assessing the European Approach to Privacy and Data Protection in Smart Grids. Lessons for Emerging Technologies*, in F. Skopik e P. Smith, *Smart Grid Security*, Amsterdam, 2015, pp. 37 ss.

[34] Sul punto cfr. R. Torino, *La valutazione d'impatto*, in Cuffaro, D'Orazio e Ricciuto, *I dati personali nel diritto europeo*, cit., pp. 855 ss.; Riccio, Scorza e Belisario, *GDPR e Normativa Privacy. Commentario*, cit., pp. 322 ss.; A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in «Computer Law & Security Review», 2018, n. 34, pp. 754-772; S. Vigliar, *Regole di responsabilità e «self-assessment»: analisi comparatistica del complesso equilibrio tra diritto e tecnica nei modelli di prevenzione del danno*, in «Cardozo Electronic Law Bullettin», 2018, e, volendo, Giannone Codiglione, *«Risk-based approach» e trattamento dei dati personali*, cit., pp. 55 ss.

su larga scala e, ancora, il trattamento globale, automatizzato e sistematico di informazioni riguardanti aspetti personali volto ad incidere sulla capacità decisionale di detti soggetti e che produca effetti significativi sul piano giuridico o personale.

È l'autorità di controllo a fornire periodicamente un elenco aggiornato delle tipologie di trattamento soggette al requisito della valutazione preventiva o, in via alternativa, a specificare quali siano le attività non sottoposte a tale obbligo: conformemente all'elenco pubblicato dal Garante in allegato al provvedimento n. 467/2018[35], le attività di trattamento svolte nell'ambito dell'esecuzione dei sistemi di IA rientrano in una molteplicità di tipologie di trattamento da sottoporre a valutazione d'impatto[36].

[35] GPDP, *Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto*, Allegato 1 al provvedimento n. 467 dell'11/10/2018, doc. web n. 9058979.

[36] Essa infatti concerne «trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche online o attraverso app, relativi ad "aspetti riguardanti 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"» (n. 1), sia «trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)» (n. 2), che «trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti)» (n. 4), di «trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)» (n. 7) e, infine, «trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di

A prescindere dalla tipologia di base giuridica individuata nell'ambito delle attività di trattamento, appare pertanto intuitivo rilevare come il gestore del sistema di IA, coadiuvato anche dal responsabile della protezione dei dati (cd. DPO), debba in ogni caso procedere all'analisi dei punti di criticità, redigendo un documento contenente la descrizione dei trattamenti e delle loro finalità rapportata ai principi di necessità e proporzionalità e ai rischi per i diritti e le libertà dell'interessato, nonché il dettaglio delle misure previste per contrastarne l'occorrenza sul piano della sicurezza, della protezione degli interessi dei soggetti coinvolti e della generale conformità alla disciplina vigente. Ove gli esiti della disamina conducano all'individuazione di un rischio elevato in assenza dell'adozione di misure idonee ad attenuarne gli effetti pregiudizievoli (art. 36, par. 1), i risultati della valutazione d'impatto sono posti al vaglio preventivo dell'autorità amministrativa di controllo. Quest'ultima, nel caso di trattamento illecito o non adeguatamente vagliato sul piano del rischio, ha l'onere di produrre entro otto settimane dalla ricezione della richiesta (prorogabile per altre sei previa informativa al titolare) un parere scritto, esercitando altresì i poteri investigativi, correttivi, autorizzativi e consultivi di cui all'art. 58.

La valutazione d'impatto, imposta in via preventiva attraverso una selezione delle tipologie di trattamento maggiormente rischiose, trova una deroga nelle ipotesi di trattamenti necessari ad adempiere un obbligo legale al quale è soggetto il titolare o per l'esecuzione di compiti di interesse pubblico. In tali casi, se il diritto dell'Unione o quello degli Stati membri abbia già dettato una disciplina specifica e sia già stata effettuata una valutazione d'impatto di carattere generale, salvo che gli Stati membri non ritengano comunque necessario effettuare tale valutazione prima di procedere al trattamento. Come già evidenziato, ai sensi dell'art. 6, par. 3 del GDPR, è infatti il legislatore europeo o quello dello Stato membro a dover indicare preventivamente

cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse» (n. 10).

la base su cui si fonda il trattamento svolto per adempiere a un obbligo legale o per perseguire un fine di pubblico interesse o connesso all'esercizio di pubblici. In tale ultima ipotesi, la disciplina potrebbe quindi contenere disposizioni di dettaglio, tra cui: le condizioni generali relative alla liceità del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto.

4. *Liceità del trattamento e classificazione dei livelli di rischio dei sistemi di IA, tra disciplina settoriale e coordinamento normativo*

Il principio di stretta necessità del trattamento rispetto agli scopi previamente dichiarati ed eventualmente oggetto di consenso da parte dell'interessato è pertanto integrato dalla previsione di limiti e obblighi in relazione ai trattamenti svolti per finalità diverse da quelle per cui sono stati raccolti. Come si è avuto modo di osservare, tali tipologie di trattamento sono oggetto di un obbligo di valutazione preventiva da parte del titolare, il quale dovrà vagliarne i rischi e le conseguenze in rapporto alle finalità del trattamento primario, al contesto in cui è avvenuta la raccolta, alla natura dei dati e all'esistenza di misure di temperamento quali la pseudonimizzazione o la cifratura.

L'informazione in astratto riferita o riferibile ad una determinata persona fisica è pertanto immessa in uno schema di elaborazione e condivisione progettato in modo tale da fornire all'interessato un controllo a distanza, nel senso di una costante informazione sui trattamenti effettuati e del libero esercizio dei diritti ad esso riconosciuti (accesso, revoca del consenso, opposizione, portabilità, rettifica, cancellazione, limitazione). L'agevole passaggio delle informazioni da un titolare all'altro e la ricorrenza di ulteriori attività di trattamento correlate alla prima, paiono

però limitare la portata di tale principio solo ad un primo stadio vitale dei dati raccolti.

La possibilità che il dato, a seguito della sua agglomerazione e rielaborazione, possa essere utilizzato ai fini predittivi e in generale per incidere sull'apparato decisionale della popolazione è difatti contemplata dal GDPR, seppur sottoposta ad un complesso procedimento di vaglio preliminare e costante monitoraggio da parte del prestatore e dell'autorità di controllo.

L'approccio *by design* e soprattutto gli obblighi di prevenzione del rischio indicano la chiara volontà legislativa di modellare le strategie imprenditoriali dei titolari verso il consolidamento di meccanismi di minimizzazione del trattamento, il filtraggio e la destrutturazione in forma anonima o pseudonima dei dati[37], favorendo così attività successive di compressione e stoccaggio che rimarrebbero in astratto estranee alla portata applicativa del GDPR, a meno che non sia possibile dimostrare che una loro combinazione possa condurre all'identificazione di una persona fisica[38].

Leggendo l'art. 4, n. 1 del GDPR si osserva infatti come la norma copra tutte le forme di trattamento multiplo di dati che conducono, anche astrattamente, all'identificazione di una persona fisica, con l'esclusione dei dati anonimi (ovvero le informazioni che non si riferiscono a una persona fisica identificata o identificabile) e dei dati personali trattati in maniera tale da impedire o da non consentire l'identificazione dell'interessato[39].

[37] Il Considerando n. 28 del GDPR, ad esempio, afferma che «l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati» puntualizzando poi come l'introduzione esplicita della «pseudonimizzazione» nel Regolamento non sia intesa a precludere altre misure di protezione dei dati.

[38] Cfr. l'art. 32 sulla sicurezza del trattamento e, ancora, l'art. 25 del GDPR.

[39] Si cfr. i Considerando nn. 26 e 30 del GDPR. Secondo il parere Gruppo *ex* art. 29, *Sulle tecniche di anonimizzazione*, WP216, adottato il 10/4/2014, p. 21, la pseudonimizzazione consiste nel sostituire un attributo (solitamente un attributo univoco) di un dato con un altro. L'art. 4, n. 5) del GDPR aggiunge come essa consista nel «trattamento

In questo quadro e, soprattutto, nella prospettiva condivisa di un approccio basato sul rischio si installano le disposizioni contenute nella Proposta di Regolamento UE sull'intelligenza artificiale[40], suggerendo una lettura coordinata e multilivello dei due (possibili) insiemi di norme uniformi.

Se, da una parte, il Regolamento sull'IA lascia impregiudicata l'effettività (e la preminenza gerarchica) delle norme in materia di protezione dei dati personali non introducendo nuove basi giuridiche per il trattamento[41], dall'altra esso si propone di introdurre importanti regole che si innestano necessariamente sulla disciplina di settore.

In primo luogo, la Proposta di Regolamento fissa i criteri-base al fine di individuare, in un'ottica preventiva e di adattamento all'evoluzione tecnologica, le applicazioni

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». Il Gruppo di lavoro in relazione alle procedure di anonimizzazione discerne tra randomizzazione e generalizzazione dei dati: nel primo caso si tratterebbe di tecniche che modificano la veridicità dei dati al fine di eliminare la forte correlazione che esiste tra i dati e la persona; la generalizzazione, invece diluisce gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza. In argomento si rimanda ancora a I. Walden, *Anonymising Personal Data*, in «International Journal of Law and Information Technology», 2002, n. 10, pp. 224 ss.; G. Finocchiaro, voce *Anonimato*, in *Digesto discipline privatistiche*, Agg. V, Torino, 2010, pp. 12 ss.

[40] *Proposta di Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21/4/2021, COM(2021) 206 final.

[41] Considerando n. 41 della proposta: «Il fatto che un sistema di IA sia classificato come ad alto rischio a norma del presente regolamento non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia necessariamente lecito a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, ad esempio in materia di protezione dei dati personali, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità ai requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale. Il presente regolamento non dovrebbe essere inteso».

di IA che dovrebbero essere considerate ad «alto rischio», ovvero quei sistemi che per la funzione svolta e per le finalità e modalità specifiche di utilizzo pongano rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone[42]. Per tali applicazioni di IA, il Regolamento fissa una serie di requisiti standard, tra cui l'obbligo di adottare un sistema di gestione dei rischi che segua l'intero ciclo di vita del sistema e individui le misure idonee per mitigarne o eliminarne gli effetti, *ex ante* (ad esempio nella fase di progettazione) o *ex post*, introducendo altresì procedure di test che permettano la valutazione della conformità prima dell'immissione in commercio (art. 9).

Di particolare rilevanza appaiono poi le misure relative alla cd. qualità dei dati: l'art. 10 della proposta individua, infatti, precisi criteri obbligatori di qualità per tutti i sistemi di IA ad alto rischio che utilizzino tecniche per l'addestramento di modelli basati sull'utilizzo di dati. In queste peculiari ipotesi, in cui l'operatività dell'algoritmo è modellata partendo da un dataset predefinito, l'obiettivo principale perseguito è quello di garantire la pertinenza, la completezza e la correttezza dei dati al fine di prevenire futuri effetti distorsivi in rapporto allo specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA è destinato a trovare applicazione. In tal senso, l'art. 9, par. 5 della Proposta di Regolamento autorizza i fornitori di tali sistemi ad utilizzare anche dati col

[42] Cfr. l'art. 6 della proposta, secondo cui: «A prescindere dal fatto che sia immesso sul mercato o messo in servizio in modo indipendente rispetto ai prodotti di cui alle lettere *a* e *b*, un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:

a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;

b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.

2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III».

precipuo scopo di garantire il monitoraggio, il rilevamento e la correzione di eventuali distorsioni, fatta salva l'applicazione di misure adeguate quali la pseudonimizzazione o la cifratura, «qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita»[43].

Sotto un diverso angolo visuale, emerge l'esigenza di apprestare meccanismi di controllo di ogni processo tecnico che sia basato sugli automatismi del calcolo computazionale e di garantire tutele effettive rispetto alle conseguenze negative potenzialmente connesse all'applicazione su larga scala dei sistemi di IA.

L'articolato complesso di misure offerto dal diritto europeo aumenta il proprio indice protettivo ponendosi anche in forma di *divieto*, ove a venire in rilievo siano tipologie di trattamento altamente rischiose per i diritti e le libertà fondamentali dell'interessato, quali le attività che presuppongono il trattamento automatizzato di dati al fine di ottenere risultati che in qualche modo possano influenzare le scelte e le decisioni dei consociati.

Nel quadro dell'inderogabilità del principio di dignità umana affermato dall'art. 41 Cost. e, ancora più incisivamente, posto al centro del sistema europeo dei diritti fondamentali dall'art. 1 della Carta di Nizza[44], spicca l'elenco

[43] Cfr. altresì il Considerando n. 40 della proposta, per cui «alcuni sistemi di IA destinati all'amministrazione della giustizia e ai processi democratici dovrebbero essere classificati come sistemi ad alto rischio, in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale. È in particolare opportuno, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, classificare come ad alto rischio i sistemi di IA destinati ad assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti. Non è tuttavia opportuno estendere tale classificazione ai sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi o l'assegnazione delle risorse».

[44] Cfr. G. Resta, *La disponibilità dei diritti fondamentali e il limite della dignità (Note a margine della Carta dei diritti)*, in «Rivista di diritto

di pratiche di IA vietate di cui all'art. 5 della Proposta di Regolamento, che previene l'implementazione di tecniche distorsive del comportamento umano, discriminatorie, pregiudizievoli o fortemente invasive[45].

In tale segmento di *policy* normativa si colloca altresì l'innovativa disposizione di cui all'art. 22 del GDPR, sul diritto dell'interessato «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». Il diritto/divieto di cui al primo paragrafo dell'art. 22 del GDPR, limitato in alcune specifiche ipotesi ove non ulteriormente disciplinato dal le-

civile», 2002, pp. 801-848, in part. 847, per cui «la progressiva e sempre più inarrestabile espansione dell'autonomia privata nella sfera della cd. personalità morale, se è un fenomeno evidente e molto diffuso, appare però bilanciata dall'emersione di un nuovo strumento di controllo della libertà contrattuale: il principio della dignità della persona»; più di recente con riferimento alla tutela del cd. corpo elettronico cfr. Rodotà, *Vivere la democrazia*, cit., in part. pp. 62 ss.: «previsto per il corpo fisico, tale principio può essere esteso al corpo elettronico, come già fanno alcune norme, come quelle che prevedono una autorizzazione pubblica per trattare i cosiddetti dati sensibili, che riguardano gli aspetti più intimi della vita o della collocazione sociale della persona. Qui il principio di dignità si congiunge con quello di eguaglianza, per evitare discriminazioni o stigmatizzazioni sociali».

[45] Cfr. ad es. il Considerando n. 17 della proposta: «I sistemi di IA che forniscono un punteggio sociale delle persone fisiche per finalità generali delle autorità pubbliche o di loro rappresentanti possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano l'affidabilità delle persone fisiche sulla base del loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note o previste. Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. È pertanto opportuno vietare tali sistemi di IA». In argomento cfr. anche F. Lagioia e G. Sartor, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in «Federalismi.it», 2020, n. 11, pp. 85 ss.

gislatore[46], impone comunque al titolare di garantire misure appropriate a tutela dell'interessato, quali l'informazione sull'architettura tecnica di tali processi decisionali e «almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[47].

Declinata in tale prospettiva, l'effettività del processo algoritmico di controllo dei dati (e il connesso assetto dell'adozione della corretta base giuridica da parte del ti-

[46] Ovvero nel caso in cui: *a*) la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, *b*) sia autorizzata e regolamentata nel dettaglio dal diritto dell'Unione o dello Stato membro oppure *c*) si basi sul consenso esplicito dell'interessato.

[47] Conformemente al quadro appena sintetizzato, le linee-guida in materia di intelligenza artificiale e protezione dei dati pubblicate dal Comitato consultivo della Convenzione n. 108 in seno al Consiglio d'Europa prescrivono a sviluppatori, produttori e fornitori di servizi di IA di «adottare forme di vigilanza sugli algoritmi che promuovano la responsabilizzazione di tutte le parti interessate durante l'intero ciclo di vita di tali applicazioni, al fine di garantire l'osservanza dei principi e delle norme in materia di protezione dei dati e diritti umani». Tali indicazioni ricalcano pilastri del GDPR, quali la valutazione sul rischio di impatti negativi e la garanzia dei diritti degli interessati a «essere informati se interagiscono con un'applicazione IA», di «ottenere informazioni sulla logica alla base dei trattamenti di dati che li coinvolgono», comprese le conseguenze derivanti dall'applicazione di tale logica e ancora di opporsi al «trattamento basato su tecnologie che influenzano le opinioni e lo sviluppo personale degli individui». Cfr. Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108), *Linee-guida in materia di intelligenza artificiale e protezione dei dati*, T-PD (2019) 01, 25/1/2019. In ogni caso, le decisioni algoritmiche non dovrebbero avere come oggetto dati sensibili, eccetto qualora l'interessato abbia prestato il proprio consenso o il trattamento sia necessario per motivi di interesse pubblico rilevante e siano in vigore misure di tutela adeguate. Cfr. il Considerando n. 71 del GDPR, nonché il combinato disposto tra l'art. 8 della *Dichiarazione dei diritti in Internet* approvata nel 2015 dalla Commissione dei diritti e dei doveri in internet istituita presso la Camera dei Deputati italiana e presieduta dal prof. Stefano Rodotà (in camera.it/leg17/1174), in tema di divieto di trattamenti automatizzati e l'art. 6, par. 1, ultimo inciso sull'autodeterminazione informativa, per cui «ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano».

tolare) deve necessariamente contemplare meccanismi che garantiscano la corretta instaurazione di un contraddittorio minimo ed informato tra persona umana e macchina, nel senso di diritto a conoscere (e comprendere) le regole matematiche e statistiche che sovrintendono il processo decisionale automatizzato ed eventualmente di incidere su di esso in termini di contestazione o correzione del suo funzionamento. Il rispetto del principio di trasparenza, inteso come informazione dinamica dell'interessato, accostato a una logica di protezione dei dati sin dalla progettazione dei sistemi di IA è stata di recente affermata dalla S.C., per cui non può affermarsi che:

> l'adesione a 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 resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati[48].

[48] Cass., sez. I, 25/3/2021, n. 14381, *inedita*. Il ricorso trae origine dalla parziale riforma della decisione del Garante italiano per la protezione dei dati personali, che aveva vietato lo svolgimento di attività di raccolta di informazioni liberamente accessibili al pubblico e la loro successiva elaborazione attraverso algoritmi ai fini dell'offerta di informazioni sulla reputazione commerciale di una persona fisica, poiché ritenute lesive della dignità degli interessati. GPDP, 24/11/2016, n. 488, *Piattaforma web per l'elaborazione di profili reputazionali*, in «Il diritto dell'informazione e dell'informatica», 2016, pp. 1022 ss.; Trib. Roma, 4/4/2018, *Mevaluate*, *ibidem*, 2019, pp. 514 ss., con nota di G. Giannone Codiglione.