Intelligenza Artificiale, data protection e responsabilità*

di Oreste Pollicino e Giovanni De Gregorio

Indice: 1. Tutela dei dati personali tra responsabilità e rischi. – 2. Intelligenza artificiale, dati personali e accountability. – 3. Il rapporto tra GDPR e Artificial Intelligence Act. – 4. L'approccio al rischio e i valori europei.

1. *Tutela dei dati personali tra responsabilità e rischi*

Lo sviluppo delle tecnologie digitali nel corso degli ultimi vent'anni ha sollevato domande e interrogativi in merito ai meccanismi di responsabilità che possano riflettere un corretto bilanciamento dei diritti in un nuovo paradigma tecnologico e sociale. La stagione della pandemia ha messo in luce il ruolo cruciale delle tecnologie digitali nella società dell'informazione[1]. Piattaforme pubbliche e private hanno contribuito a garantire la continuità delle attività quotidiane quali lo studio, il lavoro nonché le relazioni sociali. Non è un caso che la rilevanza di tali tecnologie per la gestione dell'emergenza abbia posto nuovamente al centro non solo il tema dei diritti in ambito digitale, ma anche il tema della responsabilità di soggetti pubblici e privati nell'utilizzo di tecnologie digitali che permettano il trattamento di grandi quantità di informazioni che includono dati personali.

L'analisi di dati attraverso l'implementazione di tecnologie algoritmiche permette di ottenere informazioni che possono essere utili a individuare nuovi modelli predittivi e spiegare fenomeni complessi. Tuttavia, l'utilità di tali tecnologie tende a scontrarsi con le numerose tensioni tra nuove tecnologie, privacy e tutela dei dati personali[2]. Quantomeno in astratto, la raccolta "silenziosa" di dati attraverso IoT, la modalità di trattamento automatizzata di grandi quantità di dati attraverso tecniche di *Big Data*

---

* Il presente scritto è stato elaborato nel contesto di una ricerca Astrid su Intelligenza artificiale e diritto, ed è stato pubblicato in ASTRID, "Intelligenza artificiale e diritto: una rivoluzione? Amministrazione, responsabilità, giurisdizione", a cura di Filippo Donati, Alessandro Pajno, Antonio Perrucci, vol. II, Ed. il Mulino, Bologna, 2022

[1] A. Pajno e L. Violante (a cura di), *Biopolitica, pandemia e democrazia. Rule of law nella società digitale*, Il Mulino, 2021.

[2] G. De Gregorio, R. Torino, *Big Data, privacy e tutela dei dati personali*, in Emilio Tosi (a cura di), *Privacy Digitale*, Giuffrè, 2020, pp. 447-484.

analytics e la conservazione ubiquitaria su *cloud* costituiscono soltanto alcune delle caratteristiche da tenere in considerazione al fine di comprendere "il ciclo dei dati", nonché l'impatto di tali sistemi sulla privacy e sulla tutela dei dati personali.

Non è un caso che il legame tra dati e tecnologie di intelligenza artificiale sembri essere uno dei punti centrali del futuro tecnologico dell'Europa[3]. Sin dalla sua elezione, difatti, la Presidente della Commissione Europea, Ursula von der Leyen, ha sostenuto la necessità di stabilire il percorso per sviluppare un'intelligenza artificiale che possa essere all'avanguardia e affidabile[4], come sottolineato dal *White Paper on AI*[5]. Da un punto di vista della connessione con la privacy, l'intelligenza artificiale per sua natura raccoglie una vasta quantità di dati, anche non personali, abbracciando così varie discipline giuridiche: dalla riservatezza alla protezione del consumatore. Questo accavallamento di differenti materie con differenti oggetti e scopi produce una certa confusione sul sistema di *compliance* e *accountability* di cui viene imposto il rispetto da parte degli operatori del mercato.

Vista la connessione tra dati e tecnologie algoritmiche, il legame tra la proposta di Regolamento europeo sull'intelligenza artificiale (*Artificial Intelligence Act*)[6] e il Regolamento generale sulla Protezione dei dati Personali (GDPR)[7] risulta di particolare importanza in materia di responsabilità per il trattamento dei dati personali anche attraverso tecnologie algoritmiche. Entrambe le misure adottano un approccio orientato al rischio spostando il concetto di responsabilità verso un modello che non è soltanto basato sull'osservanza di precise disposizioni che riconoscono diritti e doveri (*rights-based*) ma su un paradigma più elastico basato sulla responsabilizzazione dei soggetti coinvolti (*risk-based*)[8].

In tale quadro, come si avrà modo di descrivere, il soggetto responsabile, in particolare il titolare del trattamento, riveste un ruolo che non è soltanto di formale

---

[3] Commissione Europea, *Plasmare il futuro digitale dell'Europa*, Bruxelles, 2020, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0067>.

[4] Commissione Europea, *A Union that strives for more: the first 100 days*, comunicato stampa, 6 marzo 2020, <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_403>.

[5] Commissione Europea, *White Paper on Artificial Intelligence - A European approach to excellence and trust*, Bruxelles, 2020, <https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>.

[6] *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.

[7] *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)*.

[8] R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford, Oxford University Press, 2020, p. 2.

adeguamento al quadro normativo, ma anche di valutazione contestuale dei diritti degli interessati che costituiscono la guida dell'approccio di responsabilizzazione orientato al rischio. Tuttavia, quando il titolare del trattamento ricorre a tecnologie algoritmiche per raccogliere e analizzare informazioni e dati personali., l'intreccio tra i due regimi giuridici solleva questioni in materia di responsabilità per il trattamento di tali dati.

2. *Intelligenza artificiale, dati personali e* accountability

Il consolidamento delle tecnologie di intelligenza artificiale ha posto in discussione il paradigma di tutela dei dati personali che cerca di rendere trasparente il trattamento dei dati agli occhi dell'interessato. L'intelligenza artificiale sta infatti dimostrando il contrario, ossia un sistema decisionale opaco che limita la possibilità per i *data controller* di spiegare la logica del trattamento[9], in particolare come gli input costituiti da dati, anche di natura personale, portano a un determinato output.

Più in generale, è possibile notare come le tecnologie di intelligenza artificiale si scontrino con i principi generali del GDPR[10]. Il principio di trasparenza viene particolarmente posto in crisi a causa della protezione offerta dagli ordinamenti giuridici agli algoritmi, ad esempio attraverso la tutela giuridica garantita ai segreti commerciali, o più in generale alla proprietà intellettuale, e, come già sottolineato, alle complessità tecniche che caratterizzano tali tecnologie. Allo stesso modo, i principi di limitazione delle finalità e di minimizzazione si scontrano con il potenziale riutilizzo dei dati personali per scopi diversi da parte di sistemi automatizzati[11]. In particolare, il principio di minimizzazione dei dati è messo in discussione dalla necessità di alimentare alcune tecnologie di intelligenza artificiale con una grande quantità di dati per aumentare il grado di accuratezza e affidabilità del processo decisionale.

In un tale contesto, il principio di *accountability* introdotto dal GDPR svolge un ruolo centrale nel sistema di tutela dei dati personali, richiedendo al titolare del trattamento di dimostrare il rispetto dei suddetti principi generali[12]. In un tale contesto, il GDPR prevede, difatti, che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare,

[9] F. Pasquale, *The Black Box Society. The Secret Algorithms that Control Money and Information*, Cambridge: MA, Harvard University Press, 2015.
[10] T. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, in «Seton Hall Law Review», 47, 2017, pp. 995-1020.
[11] *Ibidem*, Art. 5(1)(b), 5(1)(c)
[12] *Ibidem*, Art. 5(2).

che il trattamento dei dati personali sia effettuato conformemente al GDPR[13]. Il GDPR richiede espressamente al titolare del trattamento di attuare misure tecniche e organizzative adeguate che siano progettate per attuare i principi di protezione dei dati in modo efficace e per integrare le garanzie necessarie nel trattamento (*privacy by design*). Inoltre, i titolari del trattamento sono anche obbligati ad attuare misure tecniche e organizzative adeguate a garantire che, per impostazione predefinita, vengano trattati solo i dati personali necessari per ciascuna specifica finalità (*privacy by default*)[14].

I principi della *privacy by design* e *privacy by default* costituiscono un chiaro esempio dei margini di discrezionalità che il titolare del trattamento può esercitare nella definizione delle misure che tutelino i diritti degli interessati. Anche guardando alla responsabilità del *data controller*, il GDPR sottolinea che l'attuazione di misure tecniche e organizzative in grado di dimostrare la conformità alle regole in materia di tutela dei dati personali dovrebbe comunque essere letta tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà della persona fisica[15].

Seppur il sistema introdotto dal GDPR cerchi di rendere la tutela dei dati personali maggiormente ancorata al contesto di riferimento, tale quadro giuridico lascia ai titolari del trattamento un margine di discrezionalità nel decidere come implementare le garanzie di protezione dei dati, anche nel caso di un conflitto strutturale come quello delle tecnologie algoritmiche. Il risultato di un tale approccio risulta di particolare rilevanza non solo per i diritti degli interessati ma anche per il principio di *rule of law*, lasciando alla determinazione del titolare del trattamento la definizione dello standard di protezione dei dati personali basato su una valutazione del rischio interna. Pertanto, il principio di responsabilizzazione, o *accountability*, del titolare del trattamento solleva questioni che non sono solo legate alla certezza del diritto, ma anche alla flessibilità riconosciuta ai *data controller* pubblici e privati che tendono a determinare lo standard di protezione dei diritti degli interessati in base a una logica orientata al rischio.

Una tale logica risulta particolarmente rilevante quando si guarda alla distinzione tra attori pubblici e privati. Mentre il margine di discrezionalità dei primi è comunque soggetto al controllo della conformità del trattamento dei dati personali non solo al GDPR ma anche al rispetto del principio di *rule of law*, la situazione è diversa quando ci si concentra su attori privati che non sono vincolati dalle garanzie costituzionali. In questo contesto, seppur il GDPR svolga un ruolo centrale traslando valori e principi

[13] *Ibidem*, Art. 24.
[14] *Ibidem*, Art. 25(1).
[15] *Ibidem*, Art. 24.

costituzionali nei rapporti tra privati, non si possono trascurare i margini di discrezionalità del titolare del trattamento che derivano dal principio di *accountability*.

Nel caso di trattamento di dati personali attraverso sistemi di decisione automatizzata, risulta opportuno esaminare il diritto degli interessati a non essere soggetti a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardano o li influenzi in modo significativo[16]. Il dibattito internazionale sul punto si è concentrato in larga parte sul diritto alla spiegazione ossia su come il titolare del trattamento debba fornire informazioni significative sulla logica nonché sull'importanza e sulle conseguenze previste del trattamento[17]. In particolare, il GDPR sembra fornire un criterio interpretativo secondo cui, al fine di assicurare un trattamento equo e trasparente nei confronti dell'interessato, tenuto conto delle circostanze e del contesto specifici in cui i dati personali sono trattati, il titolare del trattamento dovrebbe utilizzare procedure matematiche o statistiche appropriate per la profilazione, attuare misure tecniche e organizzative adeguate per garantire, in particolare, che i fattori che determinano inesattezze nei dati personali siano corretti e il rischio di errori sia ridotto al minimo, nonché proteggere i dati personali in modo da tener conto dei potenziali rischi per i diritti dell'interessato e prevenire, tra l'altro, effetti discriminatori sulle persone fisiche o che il trattamento si traduca in misure aventi tale effetto[18].

Tuttavia, i margini di discrezionalità in questo ambito sono piuttosto ampi per il titolare del trattamento considerando che non vi è una definizione dell'espressione «decisione basata unicamente sul trattamento automatizzato» o «[decisione] che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona»[19]. La mancanza di definizioni costituisce una chiara sfida per il principio di *rule of law* considerando l'ampia implementazione delle tecnologie di intelligenza artificiale e la molteplicità di situazioni in cui questi sistemi possono produrre effetti sugli individui. Inoltre, il GDPR ha definito alcuni limiti all'applicazione di tale diritto dell'interessato, permettendo, quindi, ai titolari del trattamento di avvalersi di diverse eccezioni quando, in particolare, la decisione sia

[16] *Ibidem*, Art. 22.
[17] *Ibidem*, Artt. 13-15. M. Kaminski, *The Right to Explanation, Explained*, in «Berkeley Technology Law Journal», 2019, 34(1), pp. 189- Berkeley Technology Law Journal 189-218; S. Wachter, B. Mittelstadt e 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», 7, 2017, pp. 76-99; G. Malgieri e G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in «International Data Privacy Law», 7, 2017, pp. 243-265; B. Goodman e S. Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, in «AI Magazine», 38(3), 2017, pp. 50-57.
[18] GDPR, cit., Considerando 71.
[19] *Ibidem*.

necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; quando il trattamento sia autorizzato dal diritto dell'Unione o dello Stato membro cui è soggetto il *data controller* e che prevede altresì misure idonee a tutelare i diritti, le libertà e i legittimi interessi; o si basi sul consenso esplicito dell'interessato[20]. Inoltre, il GDPR lascia ampi margini di discrezionalità a livello nazionale consentendo anche agli Stati membri di limitare l'applicazione di questo diritto degli interessati[21].

Dunque, il quadro giuridico di responsabilità risulta non soltanto frammentato in termini dei diversi gradi di *accountability* dei titolari del trattamento ma anche in base alla possibilità che gli Stati membri possano introdurre deroghe a livello nazionale in merito alle regole sull'utilizzo di decisioni automatizzate da parte dei titolari del trattamento. Il contesto di responsabilità diventa ancora più complesso considerando l'*Artificial Intelligence Act* che introduce un approccio orientato al rischio che non sembra lasciare ampi margini di discrezionalità ai *provider*.

3. *Il rapporto tra GDPR e Artificial Intelligence Act*

L'introduzione dell'*Artificial Intelligence Act* costituisce un ulteriore passo verso l'approccio *risk-based* con il quale l'Unione si sta approcciando alla società algoritmica. In un'ottica più cauta guidata in particolare dai valori europei e dalla tutela dei diritti fondamentali, l'*Artificial Intellignce Act* identifica diversi livelli di rischio nell'utilizzo di tali tecnologie, prevedendo limiti all'implementazione di tecnologie algoritmiche nel settore pubblico e privato.

La Commissione considera un «rischio inaccettabile» e, pertanto, vietato quello legato a sistemi di intelligenza artificiale che costituiscano, ad esempio, una minaccia alla tutela dei diritti fondamentali. Si annoverano in questa categoria le applicazioni che manipolano il comportamento umano per eludere il libero arbitrio degli utenti (ad esempio, giocattoli con assistenza vocale che incoraggiano i minori a comportamenti pericolosi) o che impostano la creazione di un sistema di valutazione personale sulla base del cd. social credit system.

La Commissione inserisce, invece, in soglie di "rischio elevato" quei sistemi e tecnologie di intelligenza artificiale utilizzati nel campo di strutture statali o para-statali

[20] *Ibidem*, Art. 22(2).
[21] *Ibidem*, Art. 23.

incaricate dall'ordinamento di preservare o attuare determinati diritti fondamentali, come nel caso delle *critical infrastructure*, o della formazione scolastica o professionale, ove tali sistemi possono essere impiegati per valutare il merito di un candidato di accedere a una borsa di studio, oppure, nell'ambito dell'occupazione e selezione dei lavoratori, ove gli uffici di risorse umane utilizzino sistemi di intelligenza artificiale per automatizzare le procedure di assunzione; nella gestione di servizi di credito privati e pubblici e per l'opportunità di accedere ad un prestito; nell'assicurare la pubblica sicurezza, ambito in cui le forze dell'ordine interagiscono con algoritmi che, spesso, esacerbano situazioni in cui l'ordinamento già di per sé invoca una particolare attenzione al potenziale *vulnus* ai diritti fondamentali, come nei casi di valutazione delle prove in un procedimento penale o del controllo degli ingressi migratori nel territorio statale.

In terzo luogo, un "rischio di tipo limitato" viene assegnato a quei sistemi di intelligenza artificiale per i quali vengono previsti obblighi di trasparenza specifici come, ad esempio, le *chatbot*. L'apprezzamento della pericolosità di un tale strumento è da ricondursi al fatto che la *chatbot* ingenera nell'individuo una consapevolezza errata, ovverosia la non chiarezza sull'interazione con una macchina, anziché con una persona fisica. La conseguenza di questo meccanismo è da rinvenirsi nella potenziale pericolosità di manipolazione dell'utente con conseguente detrimento all'autonomia decisionale.

Un "rischio minimo" è associato ad applicazioni dell'intelligenza artificiale che non hanno la stessa invasività delle altre descritte precedentemente. Ad esempio, vengono inseriti in questa categoria i videogiochi o i filtri antispam applicati ai servizi di e-mail. Da questa ricognizione, si comprende bene che l'ampio spettro che abbraccia l'insieme dei sistemi di intelligenza artificiale a rischio minimo è molto ampio e fornisca un opaco, sebbene vasto, ventaglio di possibilità applicative.

Nonostante la connessione tra intelligenza artificiale e dati personali, l'approccio *risk-based* adottato dall'*Artificial Intelligence Act*, seppur orientato alla tutela dei valori europei, non sembra aderire allo stesso approccio del GDPR. La proposta, infatti, non riproduce lo stesso meccanismo che rende un soggetto responsabile al fine di tutelare i diritti degli interessati. Il focus sull'individuo che è al centro dell'intera disciplina della protezione dei dati personali in Europa è assente nella proposta europea di regolamentazione dell'intelligenza artificiale. Il grande pregio del GDPR è da rintracciarsi nella estrema versatilità che deriva dal principio di *accountability* che permette di adattare il sistema di tutela ai cambiamenti sociali e tecnologici mantenendo al centro la tutela dei diritti dell'interessato. Mentre il GDPR responsabilizza il titolare del trattamento ponendo al centro gli interessati, l'*Artificial Intelligence Act* introduce un approccio al rischio definito dall'alto dalla Commissione.

Seppur si possa comprendere la *ratio* di una tale scelta, il rischio è che l'approccio adottato dalla Commissione porti a una frammentazione del regime di responsabilità. In altre parole, lo scopo di definire regole generali che non riconoscano ampi spazi di discrezionalità può condurre a una nuova proliferazione di linee-guida che cerchino di definire i limiti applicativi nell'implementazione delle tecnologie di intelligenza artificiale. Di conseguenza, se da un lato il GDPR sembra riconoscere ampi margini di manovra al titolare del trattamento, dall'altro la regolazione *ex ante* richiesta al *provider* dall'*Artificial Intelligence Act* rischia di imbrigliare il mercato in rigidi meccanismi di *compliance.*

Un meccanismo che cerca di ovviare più ampiamente al problema è costituito dall'introduzione delle c.d. *regulatory sandboxes,* che prevedono l'adozione di meccanismi regolatori che vedono la collaborazione di differenti *stakeholders* nella definizione delle regole, favorendo così il rispetto delle salvaguardie normative e la diffusione di nuove idee innovative.

Seppur l'*Artificial Intelligence Act* miri a ridurre i rischi legati all'intelligenza artificiale, tuttavia, la scelta dell'approccio *top-down* rischia di elevare le soglie di rischio e che queste si traducano in una rigidità che non lasci margini di valutazione al *provider* su come adoperarsi nella pratica. Ciò che (almeno per ora) manca nell'*Artificial Intelligence Act* è la capacità del GDPR di tenere in considerazione il contesto di riferimento.

Una tale mancanza di comunicazione tra i due regimi risulta evidente quando, ad esempio, si guardi all'obbligo dei *provider* di svolgere un c.d. *conformity assessment*, ovvero di mettere in atto un processo, prima che il prodotto sia commercializzato, che possa dimostrare se i requisiti previsti dall'*Artificial Intelligence Act* siano stati rispettati. I nuovi obblighi di conformità introdotti dalla proposta sembrano non tenere in considerazione il quadro giuridico che tutela i dati personali in Europa. Non risulta infatti chiaro se il *conformity assessment* includa anche gli obblighi di *compliance* finora previsti solo per i dati personali, come il *Data Protection Impact Assessment*, o se si tratti di analisi separate, costituendo quindi un ulteriore obbligo in capo al *provider*.

Le differenze diventano ancora più marcate quando si osserva che l'*Artificial Intelligence Act* non prevede meccanismi di rimedio per gli individui. Seppur la proposta si proponga di avere un approccio «umano-centrico» e di plasmare IA che siano *trustworthy* e sicure per gli individui, l'attuazione in concreto di queste dichiarazioni programmatiche è stata ben diversa. Al contrario, il GDPR prevede meccanismi di *redress* come proprio nel caso delle decisioni automatizzate. Manca, dunque, un riferimento centrale alla possibilità per gli individui di intervenire che, invece, era il cuore della disciplina dell'art. 22 del GDPR.

Ciò nonostante, occorre osservare che, similmente al GDPR, il mancato rispetto delle regole previste dall'*Artificial Intelligence Act* comporta l'applicazione di sanzioni amministrative pecuniarie a scaglione da parte dell'autorità competente fino a 30 milioni di euro o, se l'autore del reato è una società, fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente[22].

La relazione tra GDPR e *Artificial Intelligence Act* solleva quindi interrogativi riguardo al coordinamento tra il regime giuridico dei dati personali e dell'intelligenza artificiale, e, in particolare, riguardo al concetto di responsabilità, portando quindi verso un intreccio che potrebbe non solo rallentare l'innovazione nel mercato interno ma anche influenzare la tutela dei diritti fondamentali.

4. *L'approccio al rischio e i valori europei*

Il sistema di responsabilità in materia di dati personali in Europa sembra essere messo a dura prova dal consolidamento delle tecnologie di intelligenza artificiale. Più in particolare, il sistema di *accountability* previsto dal GDPR sembra non trovare spazio all'interno dell'*Artificial Intelligence Act* che invece adotta un approccio verticale al rischio.

Il GDPR sottolinea l'importanza dei diritti fondamentali diventando la guida per i *data controller* nella valutazione dei rischi per l'interessato nel trattamento dei dati personali. Anziché limitarsi a fornire una serie di diritti e obblighi basati sulla conformità a determinate regole giuridiche, il GDPR si concentra sulla responsabilizzazione e sui principi generali che possono essere considerati una traduzione orizzontale del diritto alla privacy e alla protezione dei dati. La designazione dei mezzi adottati per conformarsi ai principi generali è, tuttavia, un compito lasciato alla discrezionalità degli stessi titolari del trattamento. I diritti fondamentali diventano così un parametro che le organizzazioni devono considerare quando bilanciano i propri interessi.

L'*Artificial Intelligence Act* introduce una valutazione dei rischi operata direttamente dalla Commissione sulla base di quattro categorie di rischio e riduce i margini di discrezionalità per le misure da adottare per la mitigazione di tali rischi. In questo senso, a differenza del GDPR, un tale approccio sembra prendere una svolta pubblica verso un modello di *command and control*[23]. Inoltre, la proposta

[22] *Artificial Intelligence Act*, cit., Art. 71.
[23] B.M. Hutter, *Risk, Regulation, and Management*, in P. Taylor-Gooby e J. Zinn (a cura di), *Risk in Social Science*, Oxford, Oxford University Press, 2006, pp. 203-204.

probabilmente sacrifica in una certa misura il principio di *accountability*, lasciando la definizione delle scelte alla Commissione.

Tuttavia, pur differenziandosi nei mezzi impiegati, i due strumenti condividono un progetto e una direzione comuni, in quanto rappresentano un tassello della nuova fase del costituzionalismo digitale europeo caratterizzata dal consolidamento di un approccio costituzionale democratico per affrontare le sfide della società algoritmica[24], come in particolare, sottolineato dal ruolo delle corti in Europa.[25] La nozione di rischio nelle attuali politiche digitali dell'Unione viene in definitiva utilizzata come *proxy* per un'operazione di bilanciamento tra i diversi interessi in gioco: da un lato, la tutela dei diritti fondamentali e le sue numerose declinazioni; dall'altro, la ricerca di un mercato comunitario forte in cui l'iniziativa economica possa essere pienamente goduta. In questo senso, il GDPR e l'*Artificial Intelligence Act* sono espressione del Mercato Unico Digitale europeo che non si basa soltanto sulla corsa all'innovazione ma anche sulla tutela dei diritti e dei valori democratici.

La differenza nell'approccio orientato al rischio sembra trovare un punto di incontro nella tutela dei valori europei, tra cui in particolare la tutela dei diritti fondamentali. Sarebbe quindi questo un ponte che collegherebbe le due misure permettendo di interpretare l'approccio orientato al rischio come comunque orientato a un obbiettivo comune, ossia la tutela dei diritti e dei valori democratici. Un tale approccio può essere ricondotto alla questione principale ossia se e in che modo l'*Artificial Intelligence Act* si collochi in un percorso dell'Unione orientato all'umanesimo digitale nell'era del capitalismo digitale.

[24] G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in «International Journal of Constitutional Law», 19(1), 2021, pp. 41-270.
[25] O. Pollicino, *Judicial Protection of Fundamental Rights Online: A Road Towards Digital Constitutionalism?*, Oxford, Hart, 2021.