ISSN 1826-3534

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

INFORMATION DISORDER E SISTEMA DEMOCRATICO
30 MAGGIO 2025

La strategia normativa dell'Unione europea per un nuovo ordine digitale

di Licia Califano
Professoressa ordinaria di Diritto costituzionale
Università degli Studi di Urbino Carlo Bo

DAFNE

Questo Fascicolo speciale rappresenta il primo risultato di ricerca del Progetto PRIN 2022 *DAFNE* (*Democratic governance of Automated system for Fake News*), è finanziato dall'Unione europea - Next Generation EU, Missione 4 Componente 1, CUP H53D23010930001, Codice MUR P2022R7RS9 e raccoglie alcune delle relazioni e degli interventi presentati al Convegno "*Information disorder* e sistema democratico. Principi, regole e tecniche contro la disinformazione", Sapienza Università di Roma, 9 dicembre 2024.

La strategia normativa dell'Unione europea per un nuovo ordine digitale*

di Licia Califano
Professoressa ordinaria di Diritto costituzionale
Università degli Studi di Urbino Carlo Bo

Abstract [It]: Il saggio intende analizzare l'evoluzione della strategia normativa dell'Unione Europea nel contesto della trasformazione digitale, ponendo in luce il passaggio da un approccio autoregolativo a uno basato sulla centralità dell'*accountability* e della valutazione preventiva del rischio. Partendo dal *GDPR* quale pietra miliare di tale modello regolatorio, verrà esaminato l'impatto innovativo del *Digital Services Act* e dell'*Artificial Intelligence Act*, mettendo in luce come l'UE aspiri a creare un articolato sistema garantistico proiettato verso la centralità della tutela dei diritti fondamentali in un ecosistema dominato dalle *Big Tech*. La riflessione si concentra, infine, sull'urgenza di ripensare le categorie del costituzionalismo tradizionale alla luce delle nuove e pervasive forme di potere digitale, tra automazione, profilazione e disinformazione.

Title: The EU's normative strategy for shaping a new digital order
Abstract [En]: The paper aims at exploring the European Union's regulatory strategy in the digital age, highlighting the shift from self-regulation to procedural accountability and risk-based governance. Starting with the GDPR as a cornerstone of data protection, it will be examined the implications of the Digital Services Act and the Artificial Intelligence Act, focusing on the EU's effort to safeguard fundamental rights and democratic values in a scenario characterized by the dominance of Big Tech Companies. The study emphasizes the need to revisit traditional constitutional principles in response to emerging digital powers such as automation, profiling, and online disinformation.

Parole chiave: Innovazione tecnologica, GDPR, responsabilità dei fornitori, Digital Service Act, Artificial Intelligence Act
Keywords: Digital transformation, GDPR, accountability, Digital Service Act, Artificial Intelligence Act

1. Osservazioni introduttive al tema della ricerca: innovazione tecnologica e processi democratici

Di fronte al processo in atto di trasformazione tecnologica, così rapido e al contempo capace di incidere così profondamente sul tessuto sociale e sul conseguente cambiamento delle esigenze dell'uomo, il giurista non può esimersi dal comprenderne la portata e i possibili effetti sui sistemi democratici. Oggi la produzione, la memorizzazione e l'utilizzo dei dati, che noi stessi generiamo nel vissuto di una tecnologia digitale che sempre più ci accompagna nelle azioni quotidiane, avviene attraverso sistemi automatici a (apparente) costo zero che rendono disponibili le informazioni personali di una moltitudine di individui; informazioni che si prestano ad una infinità di utilizzi – aziendale, economico, sociale e, non certo ultimo,

* Articolo sottoposto a referaggio.

politico – e in molti settori che dal commercio via via si estendono al turismo, ai trasporti, trovando progressivamente spazio nel mondo della sicurezza e della sanità.

L'effetto della diffusione di *IoT*, delle tecnologie di *machine learning* e di intelligenza artificiale (AI) è la produzione di una enorme quantità di informazioni e dati, personali e non, mai visti prima nella storia dell'uomo. Si tratta di un fenomeno che oggi chiamiamo *big data*: banche dati di grandi dimensioni in cui le informazioni contenute vengono continuamente interconnesse e automaticamente rielaborate sulla base di complessi algoritmi, per dare vita a informazioni di secondo grado (*data mining*), riutilizzabili per altri fini.

Se anche volessimo ipotizzare che tali informazioni non consentono la re-identificazione degli interessati che avevano inizialmente ed inconsapevolmente fornito i dati grezzi, nondimeno questo perfetto automatismo, basandosi su leggi probabilistiche, potrebbe condurre a categorizzazioni e classificazioni della società che, oltre ad essere discutibili sul piano dell'esattezza e della correttezza, portano con sé il rischio di generare pregiudizi e discriminazioni.[1]

In un paradigma digitale fatto di *big data*, di Internet delle cose, di AI, di automazione di tutti i processi produttivi e comunicativi, l'incidenza sulla sfera individuale, sulla dignità e libertà dell'uomo da parte di chi detiene le conoscenze tecnologiche può manifestarsi in molti modi: dai sistemi che generano un controllo a distanza dell'individuo lavoratore all'informazione connessa al corredo genetico di ciascuno di noi, dalla profilazione piegata alle finalità elettorali e politiche alla massiva raccolta dei dati sanitari connessi a dispositivi medici che diventano un patrimonio economico inestimabile per le aziende farmaceutiche e le compagnie assicurative. E che dire, lungo questa strada, dell'intelligenza artificiale applicata al settore militare e della sicurezza che può sostituire l'essere umano con un robot o, ancora, l'uso di algoritmi in grado di sostituire il giudice, ad esempio, nella scelta di una famiglia cui affidare un

[1] È osservazione condivisa in dottrina che la classificazione fra dati personali e non, sulla carta semplice e netta, diviene poi in concreto evanescente, per almeno due ordini di motivi: se per un verso numerosi studi hanno dimostrato come le attuali tecniche di analisi dei dati aumentano le possibilità di re-identificazione di persone fisiche partendo da dati apparentemente anonimi, in quanto consentono di ricollegare i dati non identificati (compresi quelli anonimizzati o pseudonimizzati) ai soggetti interessati a cui tali dati fanno riferimento (in altri termini è sempre tecnicamente possibile fare il percorso inverso), per l'altro la filiera dei big data è gestita da algoritmi di AI la cui specificità è la non prevedibilità a priori della tipologia di connessioni che la macchina sarà in grado di individuare. Ciò comporta che una re-identificazione del soggetto potrebbe prodursi anche involontariamente. Così, ad esempio, quando nel 2006 la piattaforma di contenuti *on-demand* Netflix ha reso pubblici una serie di dati anonimizzati contenenti le valutazioni di film rese da 500.000 utenti abbonati, uno studio ha dimostrato che un utente del servizio poteva essere facilmente identificato. Per ottenere questo risultato, lo studio aveva confrontato e collegato le valutazioni dei film degli utenti di Netflix anonimizzati con le recensioni disponibili pubblicamente sul sito di informazioni cinematografiche *Internet Movie Database* (IMDb), dove gli utenti spesso usano i loro veri nomi. Lo studio ha dimostrato che in media sono necessarie da due a otto recensioni su IMDb per identificare gli utenti nel dataset anonimizzato di Netflix.

bambino o, ancora, nel valutare gli estremi e le ragioni che giustificano la carcerazione preventiva in relazione al rischio di fuga o reiterazione del reato.

Un contesto nel quale l'affermazione della centralità della persona umana e delle garanzie individuali ha assunto un peso determinante, in ragione della consapevolezza che i sistemi di AI sono in grado di esercitare un impatto significativo sui diritti, le libertà e sui principi fondanti e irrinunciabili del costituzionalismo democratico.

Ma la riflessione ci porterebbe anche più lontano: così, se pensiamo ai social network dobbiamo chiederci se siamo in presenza di una piazza virtuale, un luogo neutro dove si formano e agiscono liberamente quelle formazioni sociali dove si svolge la personalità individuale, in conformità ai principi costituzionali, o abbiamo di fronte un orizzonte più complesso: dalla osservazione che siamo di fronte ad una grande agenzia pubblicitaria, che vende spazi pubblicitari e li mostra costantemente ai propri iscritti, possiamo giungere a chiederci quanto l'uso della rete per le interazioni sia funzionale a creare dialogo, tolleranza e attenzione per le ragioni degli altri o invece, all'opposto, quanto sia reale il rischio di irrigidire contrapposizioni e ostilità. A ben guardare buona parte dell'attuale ecosistema informativo digitale tende a sottrarre il cittadino alla regola base degli ordinamenti democratici, costruita sul confronto e la scelta fra opinioni diverse. Un mondo che, al contrario, tende alla creazione di enclavi che si chiudono, ciascuna in sé stessa, in una dinamica mirata a far arrivare a ciascuno opinioni confermative di ciò che si presume rappresenti già una posizione, comunque un orientamento già assunto da ciascuno sulla base di un giudizio o di un pregiudizio poco importa. Se davvero quelle che tendono a crearsi oggi in rete sono le formazioni sociali dei tempi nuovi, la funzione cui assolvono è esattamente opposta a quella educazione agli affari collettivi per cui le aveva valorizzate il costituente.

Ora, condiviso che la disciplina costituzionale della sfera dell'inviolabilità dei diritti e delle libertà da sempre si configura quale fattore determinante nella costruzione dei rapporti fra società civile e Stato, così come, al tempo stesso, le trasformazioni delle concezioni dello Stato si legano intimamente alla definizione stessa dell'ambito di applicazione delle categorie costituzionalmente sancite, non sfugge la centralità di scelte di regolazione del fenomeno capaci di coniugare la coerenza fra innovazione tecnologica, trasformazione della società e conseguente definizione dell'ambito oggettivo e soggettivo del contenuto delle garanzie costituzionali.

In altri termini, non sono in discussione i nuovi orizzonti di sviluppo che sistemi tecnologici capaci di interagire con l'uomo, fino alla produzione di linguaggi naturali e alla organizzazione dei pensieri, aprono al genere umano; sono piuttosto da considerare attentamente i profili di regolazione delle tecnologie digitali, per i loro inevitabili riflessi sull'idea stessa di democrazia.

Nella prospettiva della ricerca che caratterizzerà i contributi di questo Fascicolo speciale l'analisi è in particolare orientata al tema della disinformazione online, prodotta dalla crescente diffusione tramite i social network di contenuti definibili "falsi" in grado di orientare e condizionare l'opinione pubblica e di incidere sul corretto funzionamento del circuito democratico - rappresentativo.

Una nozione di disinformazione che non è circoscrivibile alle sole condotte che l'ordinamento espressamente riconosce come illecite, ma a tutti quei contenuti falsi, fuorvianti, artificiosamente creati, la cui produzione e diffusione configura un potenziale danno ai principi e valori democratici; in questo senso il profilo regolatorio non potrà prescindere dalla definizione di un punto di equilibrio possibile fra interessi pubblici al corretto funzionamento dello Stato democratico e libertà individuale dei consociati a porre in essere condotte (di per sé lecite) che non possono subire uno sproporzionato nocumento. [2]

Come si governa la tecnologia digitale diviene così il primo interrogativo: la ricerca di spazi di regolazione giuridica delle piattaforme digitali e la conseguente elaborazione di nuove forme e strumenti di tutela idonei a fissare la misura del potere ed a proteggere le libertà fondamentali è il compito del diritto.

Chiediamoci allora, anzitutto, se sia possibile regolare l'eco-sistema digitale: un mondo privo di confini e, dunque, caratterizzato dalla de-territorializzazione dei rapporti giuridici.[3] E, a fronte di una risposta che afferma la necessità di un intervento pubblico per continuare a garantire effettività alla tutela dei diritti, chiediamoci a quale livello di governo tale regolazione deve essere affidata e se rimane ancora uno spazio per il legislatore nazionale.[4]

Affermazione, questa, non così ovvia e scontata di fronte ad un modello di regolamentazione del digitale in cui ha prevalso la concentrazione del potere in capo ad un oligopolio di soggetti privati in grado di controllare sia i dati e le informazioni che gli utenti condividono in rete, sia le modalità della loro condivisione. Le Big Tech nel mondo occidentale sono soggetti privati in vantaggio competitivo sul mercato, rappresentano un nuovo potere privato capace di rapportarsi alla pari con gli Stati,[5]

[2] Così in particolare cfr.: O. POLLICINO, P. DUNN, *Disinformazione e intelligenza artificiale nell'anno delle global elections: rischi (ed opportunità)* in *Federalismi.it*, n.12/2024. Si consentito rinviare anche a L. CALIFANO, *La libertà di manifestazione del pensiero ... in rete; nuove frontiere di esercizio di un diritto antico. Fake news, hate speech e profili di responsabilità dei social network,* in *federalismi.it,* n. 26, 2021.

[3] K. KLONICK, *The new governors: the people, rules, and processes governing online speech*, in *Harvard Law Review*, vol. 131, n.6, 2018, p. 1662 ss; V. M. BASSINI, *Fundamental rights and private enforcement in the digital age*, in *European Law Journal*, vol. 25, Issue n. 2, 2019, p. 187.

[4] M. MOORE- D. TAMBINI, (a cura di), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, Oxford, Oxford University Press, 2018.

[5] Sul punto cfr. T. GILLESPIE, *Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media*, New Haven-London, Yale University Press, 2018, p. 5; O. POLLICINO, *Potere digitale (voce)*, in *Enc. Dir., I Tematici*, *Vol. V, Potere e Costituzione*, presentazione, Giuffrè Francis Lefebvre, Milano, 2023, pp. 410-448; G. DE GREGORIO – O. POLLICINO - P. DUNN, *Digitisation and the central role of intermediaries in a post-pandemic world*, in *Medialaws.eu*, 2021.

riproponendo il tema del limite al potere quale essenza del costituzionalismo e fine ultimo dello Stato di diritto.[6]

Solo di recente, abbandonata l'illusione che il controllo dei dati ed il conseguente fenomeno della disinformazione online possa trovare una risposta nelle capacità autocorrettive del mercato delle idee, il legislatore europeo ha adottato un corpus normativo orientato verso una governance europea, con l'obiettivo di stabilire adeguate protezioni all'esercizio dei diritti individuali e collettivi nello spazio digitale. Una risposta normativa che vede l'Europa attore principale di una sfida che non può che essere affrontata nel più vasto ambito territoriale possibile[7] e che se per un verso conduce la riflessione sulla tipologia dello strumento prescelto, per l'altro ripropone all'attenzione il tema dell'attualità delle categorie tradizionali del costituzionalismo liberal-democratico trasferite nella dimensione virtuale caratterizzata da un diversificato, o forse più correttamente, capovolto rapporto fra soggetto pubblico e privato. Un quadro d'insieme cui occorre aggiungere la dimensione, che potremmo definire esplosiva, dell'interazione fra disinformazione e applicazione dell'AI alle forme di comunicazione politica.

2. Governo dei dati e tutela dei diritti: il GDPR e la regolazione del rischio quale scelta anticipatoria degli interventi normativi successivi

L'applicazione di nuove modalità di calcolo e di analisi, le sempre maggiori capacità sia di raccolta che di conservazione e analisi di dati personali hanno completamente modificato il concetto stesso di tutela della privacy, rendendo di fatto obsolete, o comunque non più efficienti, le norme che fino a qualche anno fa tutelavano la riservatezza degli individui intesa semplicemente come diritto ad essere lasciati soli. Nel mondo digitale "essere lasciati soli" non basta, dal momento che è l'individuo stesso che, più o meno consapevolmente, produce contenuti e con essi genera dati personali che viaggiano liberamente in rete. Il paradigma è cambiato completamente perché appare mutato il concetto stesso di "solitudine" e, dunque, di riservatezza nell'epoca digitale. Se nel passato l'individuo voleva e poteva "semplicemente" evitare che ingerenze esterne entrassero nella sfera della propria riservatezza ed intimità (una logica, dunque, protettiva), nell'attuale realtà digitale l'individuo deve prima di tutto poter decidere di sottrarre i propri dati personali a quei processi di raccolta, aggregazione e riutilizzo che caratterizzano i *big data* e che sono alla base anche dei sistemi di AI.

[6] Per un più ampio approfondimento cfr. G. DI GREGORIO, *Digital Constitutionalism in Europe*, Cambridge University Press, Cambridge, 2022 e G. RESTA, *Diritti fondamentali e diritto privato nel contesto digitale*, in G. RESTA-F. CAGGIA (a cura di), *I diritti fondamentali in Europa e il diritto privato*, Roma, Roma Tre Press, 2019, p. 117 ss.; M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista "Gruppo di Pisa",* fasc. n.2, 2021, pp.180-181.

[7] G. PALOMBELLA, *È possibile una legalità globale*? Bologna, Il Mulino, 2012, p. 161. Sul concetto di "aterritorialità" si veda L. FLORIDI, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach, in Philosophy & Technology,* 34, June 2021, p. 220.

La logica, dunque, è prima di tutto *ablativa* nel senso che non è tanto il mondo ad essere tenuto fuori (privacy *protettiva*), quanto piuttosto l'individuo a sottrarsi al mondo (privacy *ablativa*).

Una prima prospettiva di analisi, questa, che intende mettere al centro gli utenti dei sevizi digitali in qualità di persone, di esseri umani titolari di diritti e non di consumatori, cercando un punto di equilibrio possibile tra cultura costituzionale del principio personalista e logica degli algoritmi.

Riflessione che conduce a domandarci in che misura la Costituzione repubblicana, interpretata usando la lente dell'innovazione tecnologica, conservi intatta la sua capacità di garantire effettività alla tutela dei diritti. In secondo luogo occorre guardare l'eco-sistema digitale dalla prospettiva dei proprietari degli algoritmi, monopolizzato dai privati. Chi ha la capacità di implementare e sviluppare gli algoritmi sono pochi oligopoli, colossi che si contendono il dominio digitale del pianeta (le cd Smart Tech, o Big Tech, o OTT). E' proprio qui che il costituzionalismo, nato e costruito come limite al potere dello Stato, fatica a trovare risposte, a fronte di un legislatore che troppo a lungo ha cercato di inseguire le ricadute problematiche (spesso ormai oltre la soglia di regolamentazione) senza svolgere la funzione di direzione dell'innovazione e, con essa, il corretto sviluppo della società ad esso costituzionalmente affidato.

Un primo passo verso il cambiamento è rappresentato dal Regolamento Generale sulla Protezione dei Dati,[8] quale strumento innovativo e ancora idoneo a fornire almeno qualche soluzione ai tanti interrogativi che ci stiamo ponendo. Vediamo in che termini.

Certamente la normativa in materia di protezione dati rappresenta un primo fondamentale presidio di garanzia, tanto in termini di diritti esercitabili dall'utente, quanto nella direzione di stimolo verso una logica di responsabilizzazione dei titolari coinvolti a vario titolo nella sempre più articolata filiera in cui si svolgono i trattamenti. Una direzione, questa, che considera prioritaria la necessità di escludere, o quantomeno minimizzare, il rischio di intendere la cessione dei propri dati quale tributo necessario alla fruizione dei vantaggi offerti dalla rete: una prospettiva preoccupante e inaccettabile sul piano culturale, prima ancora che giuridico.

[8] 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 personali).
Il riconoscimento del valore costituzionale del diritto alla privacy quale espressione della universale dignità dell'uomo, ha vissuto un percorso di progressiva positivizzazione (caratterizzato dall'intrecciarsi della elaborazione giurisprudenziale agli interventi del legislatore a livello tanto europeo quanto nazionale) che ha trovato una compiuta definizione nella Carta dei diritti fondamentali dell'UE del 2000 la quale, oltre a confermare all'art. 7 il tradizionale diritto alla riservatezza (mutuato dall'art. 8 della CEDU), all'art. 8 stabilisce il fondamento costituzionale del diritto alla protezione dei dati personali. Su questa cornice si è poi inserito saldamente l'art. 16 del Trattato sul funzionamento dell'UE, come riscritto dai Trattati di Lisbona del 2007, che ha affidato al legislatore europeo il compito di fissare il nuovo quadro normativo comune all'intera Unione, riconoscendo il ruolo di controllo delle competenti Autorità indipendenti (uniche Autorità espressamente citate nei Trattati europei): all'interno di questa costruzione giuridica si trova oggi il Regolamento (UE) 2016/679.

Una disciplina nata in funzione della necessità di una migliore tutela della dignità della persona in una società in cui sempre di più le relazioni personali, così come quelle economiche, politiche e sociali, risultano caratterizzate dallo scambio di dati che, usati anche per profilare l'interlocutore, devono rispondere a parametri di esattezza e affidabilità e consentire agli interessati trasparenza sul loro utilizzo e possibilità di esercizio dei diritti.

Fondamentale, in primo luogo, l'impiego di una fonte normativa sovranazionale, capace tanto di uniformare, quanto di lasciare margini all'implementazione in ambito statuale. Così come fondamentale, in secondo luogo, la positivizzazione e la conseguente giustiziabilità del principio di responsabilizzazione e della valutazione di impatto preliminare (nel senso della loro invocabilità come parametri normativi nelle controversie e come parametri di accertamento da parte delle Autorità di controllo); regole, queste, già testate in altri settori e che, chiamando in causa i soggetti privati, tenuti a definire e giustificare i limiti della propria azione, hanno dato buona prova di sé. In terzo luogo, se per far fronte alle sfide che l'era digitale comporta, le Autorità pubbliche necessitano di nuovi strumenti normativi, in grado di superare i confini territoriali dei singoli Paesi e persino dei continenti (si pensi al principio del c.d. *targeting*[9]), il GDPR si configura quale strumento in grado di essere applicato in maniera omogena in tutta Europa, conciliando la massima circolazione delle informazioni con la massima tutela per gli individui.[10]

In particolare, da questo punto di vista, due sono i punti di forza del GPDR che vanno sottolineati e che lo rendono strumento particolarmente duttile e, dunque, utile, per "governare" molti aspetti della sfida digitale;[11] anzitutto il linguaggio parlato fondamentalmente basato su "clausole a fattispecie aperta" quali in particolare il principio di correttezza, liceità e trasparenza (art. 5.1.a.), il principio di limitazione della finalità (art. 5.1.b) e quello di minimizzazione che sottende il giudizio di proporzionalità (art. 5.1.c); la flessibilità che tali formulazioni recano è patrimonio prezioso per l'interprete a fronte della complessità della società digitale.

Vi è poi da considerare il tentativo di fornire una risposta al tema del superamento dei confini territoriali da parte della società digitale sia attraverso una coraggiosa interpretazione (basata anche su precedenti giurisprudenziali e sulla Direttiva 95/46/CE) dell'applicazione territoriale (art.3), sia con la costruzione

[9] Con questa espressione ci si riferisce al criterio del c.d. indirizzamento (*targeting*) del trattamento (art. 3, par. 2 GDPR), uno dei due criteri relativi all'ambito di applicazione del GDPR (il primo è il c.d. stabilimento, art. 3, par. 1). Cfr.: *Linee-guida 3 del 2018 sull'ambito di applicazione territoriale del GDPR (articolo 3)*, Versione 2.1, adottate dall'EDPB il 12 novembre 2019, dove si chiarisce che «l'applicazione del "criterio dell'indirizzamento (*targeting*) del trattamento" nei confronti di interessati che si trovano nell'Unione, come disposto nell'art. 3, par. 2, può configurarsi in rapporto ad attività di trattamento svolte da un titolare o da un responsabile.

[10] Sul punto sia consentito un rinvio a L. CALIFANO, *Il regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO-C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona, il diritto alla protezione dei dati personali nel regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017, p. 11.

[11] F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè Francis Lefebvre, Milano, 2019.

di un procedimento che è, al contempo, un controllo congiunto e un vero e proprio procedimento codecisionale, unico nel panorama comparato, quale il meccanismo di cooperazione e coerenza disegnato dal Capo VII.

Peraltro, se il processo codecisionale europeo rappresenta a tutti gli effetti l'unica strada perseguibile perché efficace, oltre che un passo importante nel processo di integrazione perseguibile, è altrettanto ovvio che alcune correzioni dovranno essere introdotte al fine di migliorare, probabilmente nei tempi e nei modi, l'intero procedimento, in modo da renderlo pienamente compatibile, anche in concreto, con l'estrema velocità che caratterizza lo sviluppo digitale e la diffusione dei rischi ad essa connessi in materia di protezione dei dati. A maggior ragione in una Europa che, come osserveremo a breve, si sta muovendo, unica al mondo da questo punto di vista, nella direzione di una cornice normativa mirata a stabilire obblighi e responsabilità in capo alle piattaforme digitali e che ha portato all'approvazione del Digital Markets Act (DMA) e del Digital Services Act (DSA) nonché, al primo tentativo regolatorio dell'IA.[12]

Ad un approccio iniziale, che ha mostrato tutti i suoi limiti, improntato prevalentemente alla logica dell'auto-regolazione e del liberismo "digitale"[13] basato sull'idea di una "rete libera" sia con riguardo ai profili economicistici sia in relazione ai contenuti, anche sul modello statunitense, l'Europa ha progressivamente sostituito una strategia maggiormente interventista, costruendo le basi di un sistema regolatorio ben preciso e ponendo a sua tutela un meccanismo di *law enforcement* di carattere nuovamente pubblicistico e, in qualche caso[14], anche fortemente accentrato.

Le nuove iniziative legislative europee sui mercati digitali, tra cui particolare rilievo assumono la Legge sui servizi digitali (il c.d. Digital Services Act), e sull'intelligenza artificiale,[15] delineano, infatti, un quadro normativo a tutto tondo (dati, contenuti, software) della responsabilità degli attori delle digitali, aprendo orizzonti ad una declinazione del costituzionalismo capace di governare l'innovazione digitale all'interno della tenuta delle categorie giuridiche tradizionali, rivisitate e rivitalizzate, quale strumento di democrazia.

---

[12] Sugli approcci regolatori in questo settore si veda il recente scritto di A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, in *Rivista Trimestrale di Diritto Pubblico*, 4/2022, pp. 1031-1050.

[13] Le manifestazioni più note, almeno in ambito UE, possiamo individuarle nei codici di condotta, nelle linee guida, nelle buone pratiche, nei cd *standards* quali misure che, se riconducibili alla categoria degli atti di *soft-law*, perché formalmente non vincolanti, ciò nondimeno sono in grado di indirizzare la condotta di amministrazioni, imprese e dei cittadini stessi.

[14] Il riferimento è al *Digital Market Act*, Regolamento UE/2022/1925, il quale ha previsto un modello di *law enforcement* fortemente accentrato sulla Commissione UE, a differenza dei precedenti interventi in materia di normativa anti-trust che coinvolgevano molto le Autorità competenti degli Stati membri. Si veda in generale sul tema del DMA e il rapporto con le leggi antitrust A. LALLI, *Il Digital Market Act: quale concorrenza e quale regolazione*, in A. LALLI (a cura di), *L'amministrazione pubblica nell'era digitale*, Giappichelli, Torino, 2022.

[15] Si fa riferimento al Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) e al Regolamento che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, v. Regolamento sull'intelligenza artificiale (COM(2021)0206 - c9-0146/2021 - 2021/0106(COD)), 6 marzo 2024.

In questo, forse, il Regolamento generale sulla protezione dei dati ha rappresentato una sorta di antesignano, dal momento che ha coniugato la responsabilizzazione dei soggetti privati con un sistema di vigilanza e controllo di carattere pubblico ben definito, strutturato e coordinato.

C'è, infatti, una linea che può dirsi comune e che tiene insieme atti normativi tra loro anche sensibilmente diversi come il GDPR, il DSA, il DMA - e da ultimo l'AI Act - l'idea di fondo per cui attraverso il concetto di "rischio", si mira a realizzare un bilanciamento tra gli interessi in gioco, interessi che si concretizzano, da una lato, nella spinta, anche di matrice economica, all'innovazione e allo sviluppo di un mercato unico digitale competitivo sul piano internazionale e, dall'altro lato, nella perdurante attenzione alla tutela dei valori democratici e dei diritti e delle libertà fondamentali degli individui.[16]

Un profilo di avanguardia nella disciplina del GDPR, che precorre i tempi anticipando le principali evoluzioni tecnologiche e digitali, là dove si orienta nella previsione di regole applicabili alla procedimentalizzazione algoritmica quasi dieci anni prima della approvazione del AI Act: conoscibilità, non esclusività e non discriminazione.[17]

In tale direzione l'articolo 22 del G.D.P.R. dispone che "l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Inoltre, gli articoli 13 par 2 lett. *f* e 14 par 2 lett. *g* impongono di notificare i dati che sono oggetto di un trattamento automatizzato e le informazioni importanti relative alla logica seguita, così come le conseguenze che ne derivano (richiamando così l'art. 22). Analogamente, l'art. 15 stabilisce il diritto di accesso ai dati e alle informazioni qualora vi sia «l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato» (par. 1 lett. *h*).[18]

Di fronte al dominio incontrollabile dell'automatizzazione si comincia a parlare di una "riserva di umanità" proprio a partire da tale atto normativo. Certo, si tratta di un diritto la cui configurazione è

---

[16] Sul punto cfr. G. DI GREGORIO, P. DUNN, O. POLLICINO, *Approccio basato sul rischio: come è applicato nelle normative UE sul digitale*, in *Agenda Digitale*,15 settembre 2022; M. GRAZIADEI, *La regolazione del rischio e il principio di precauzione: Stati Uniti e Europa a confronto*, in *Sistemi Intelligenti*, 2/2017, p. 499; A. ODDENINO, *Intelligenza artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente proposta di regolamento della IA con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?,* vol. I, Il Mulino, Bologna, 2022, p. 196; J. CHAMBERLAIN, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in *European Journal of Risk Regulation*, 14, p. 1 ss.

[17] Si veda anche G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati*, in *Giurisprudenza italiana*, 7/2019, p. 1657 ss. e M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI Lezioni di Diritto dell'Intelligenza artificiale*, Giappichelli, Torino, 2020, p. 66.

[18] S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law*, 2017, 7(2), p. 76-99.

ancora incerta e che può essere soggetto a varie accezioni e gradi di vincolatività; si potrebbe anzi osservare che l'assenza di una definizione in positivo che delinei i connotati fondamentali di questo diritto e l'ampio catalogo di eccezioni ivi previste rendono l'affermazione del primo paragrafo più un'enunciazione di principio, più formale che sostanziale.[19]

Tuttavia, essa ha esercitato una evidente funzione ispiratrice nei confronti delle fonti successive, divenendo - se non un diritto - un istituto garantistico di riferimento ogni qual volta l'individuo si interfacci con un sistema automatizzato: una forma di tutela che utilizza il paradigma tradizionale della "riserva", baluardo classico di tutela dei diritti fondamentali e lo plasma sulla contemporaneità, caratterizzata dal dominio dell'automatizzazione.[20]

3. Il nuovo regime "a responsabilità condizionata" delle grandi piattaforme digitali: il primo passo dell'Europa nella direzione degli oneri procedurali

Cercare un percorso, per quanto difficile, di regolazione pubblica omogenea nell'ambito territoriale degli Stati membri che possa offrire maggiore garanzia ai diritti della persona-utente è, dunque, la strada che ha scelto l'Unione europea.[21]

Il *Digital Service Act* (DSA), ha raccolto l'eredità garantistica del GDPR, divenendo uno dei principali strumenti operativi per affermare la strada della "sovranità digitale o tecnologica dell'Unione". Con quest'ultima espressione si identifica l'aspirazione all'edificazione di un'azione strategica autonoma attraverso la creazione di meccanismi difensivi e offensivi in un settore in cui l'influenza economica e sociale delle *Big Tech* ha acquisito risvolti preoccupanti.[22] L'Unione si è dunque orientata a ridisegnare la cornice normativa, con specifico riguardo agli obblighi e alle responsabilità in capo alle piattaforme digitali, introducendo misure orizzontali per tutte le categorie di contenuti, prodotti e attività sui servizi di intermediazione.

Un insieme di misure che se per un verso si innestano nel quadro normativo preesistente (Direttiva 2000/31 CE sul commercio elettronico) relative alla responsabilità dei prestatori di servizi intermediari, così come interpretate dalla Corte di giustizia, per l'altro innovano là dove impongono, soprattutto alle

[19] Per un approfondimento cfr. G. GALLONE, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, CEDAM, Padova, 2023.

[20] D.U. GALETTA, *Human stupidity in the loop? Riflessioni (di un giurista) sule potenzialità e i rischi dell'Intelligenza Artificiale,* in *federalismi. it*, fasc. n. 5, 2023, iv ss.

[21] L. FLORIDI, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philosophy and Technology*, 2020. Sulle ambiguità connesse all'idea di "sovranità digitale" cfr. V. BERTOLA, *La sovranità digitale e il futuro di Internet*, in *Rivista italiana di informatica e diritto*, fasc. 1/2022, p. 39 ss.

[22] Per una lettura onnicomprensiva del provvedimento e delle diverse fasi di elaborazione cfr. S.F. SCHWEMER, *Digital Services Act: A Reform of the e-Commerce Directive and Much More*, prepared for A Savin, Research Handbook on EU Internet Law, October 2022, p. 1 ss.

piattaforme di grandi dimensioni, vincoli procedurali legati agli obblighi di trasparenza e all'*accountability*. La regolamentazione dell'offerta dei servizi digitali si focalizza, in questa prospettiva, su tre presupposti cardine: trasparenza, responsabilità e garanzia nei confronti dell'utente.[23]

In realtà, il dichiarato obiettivo perseguito dalla riforma è più complesso ed ambizioso, in quanto il legislatore europeo aspira a tradurre in via normativa l'acquisita consapevolezza che il mutamento radicale della configurazione dei provider, rappresentando un fattore di rischio per i diritti dei cittadini, richieda un intervento che apporti una correzione del mercato unico dei servizi di intermediazione al fine di favorire la creazione di un «*safe, predictable and trusted online environment*». Un sistema normativo non armonizzato, aggravato dall'assenza di un adeguato servizio di vigilanza e coordinamento di tipo amministrativo, rendeva quanto mai necessaria la modifica della disciplina previgente, in materia di responsabilità dei provider, posta dall'ormai obsoleta direttiva 2000/31/CE100.

Di qui l'introduzione di un regime a responsabilità diversificato, una serie di obblighi e doveri di vigilanza per i diversi fornitori, modulata sulla base della tipologia del servizio di intermediazione offerto e della dimensione del soggetto operante.[24] In forza di tali previsioni i destinatari delle prescrizioni devono assicurare di aver posto in essere i rigidi adempimenti individuati dall'atto normativo affinché possano essere considerati esenti da responsabilità per i contenuti illegali che si trovino involontariamente ad ospitare. In particolare, quelle che l'atto identifica come "*very large online platforms*" (VLP) diventano destinatarie di specifici adempimenti.[25]

Si può osservare che, in linea di principio, la regola chiave rimane ancora quella di una generale irresponsabilità del fornitore, ma fino al momento di venuta a conoscenza del contenuto illegale[26]; quest'ultimo fungerebbe da *dies a quo* dal quale emergerebbe un dovere di rapida attivazione per individuare la fonte, bloccare la disseminazione del contenuto, nonché impedirne l'accessibilità.

Un nuovo regime "a responsabilità condizionata" che viene poi implementato mediante l'adozione di differenti misure caratterizzate da procedure più celeri ed articolate sia per l'eliminazione di elementi o prodotti illegali, sia per la presentazione di reclami e segnalazioni da parte degli utenti.

---

[23] R. BUCCA-M. SABATINI, *Digital Services Act, la Ue a una svolta: cosa cambia per utenti, aziende e big tech*, in *Agenda Digitale*, 19 maggio 2022.

[24] V. G. DE GREGORIO, *L'alba di nuove responsabilità sulle piattaforme digitali: il Digital Services Act*, in *Agenda Digitale*, 15 dicembre 2020; V. G. BAZZONI, *L'evoluzione normativa dell'intermediazione digitale: nuovi profili di responsabilizzazione*, in *Rivista italiana di informatica e diritto*, 1/2022, p. 201 ss.

[25] G. RUOTOLO, *Le proposte europee di riforma della responsabilità dei fornitori di servizi su Internet*, in *Rivista italiana di informatica e diritto*, fasc. 1/2022, p. 19.

[26] La cui definizione è affidata all'art. 3 lett. *h* dell'atto normativo, il quale lo definisce come «qualsiasi informazione che, di per sé o in relazione a un' attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto».

Un panorama di obblighi e di misure puntuali in particolare finalizzato, come già osservato, all'introduzione di limitazioni ulteriori a carico delle piattaforme di notevoli dimensioni.[27] Si prevede, ad esempio, che le VLPs – identificate sulla base di un criterio quantitativo – effettuino periodicamente una valutazione dei rischi sistemici connessi all'erogazione dei loro servizi, utilizzando come criterio la gravità e probabilità dell'evento. Inoltre è significativo segnalare come, in caso di inadempienza, gli Stati membri possano erogare delle sanzioni pecuniarie a carico delle grandi piattaforme che possono raggiungere anche il 6% del fatturato annuo.[28]

L'effettività di un controllo pubblico sull'operato degli intermediari appare poi rafforzata dalle numerose prescrizioni concernenti gli obblighi di trasparenza fra cui, di particolare interesse, la richiesta di pubblicazione di una dettagliata relazione annuale nella quale ogni provider dovrebbe rendere note tutte le informazioni concernenti l'attività di moderazione effettuata; una vera e propria rendicontazione da cui la Commissione può individuare una formula standard in via esecutiva.[29]

In aggiunta a tali adempimenti richiesti dall'articolo 15, l'articolo 24 esige poi che le piattaforme comunichino le segnalazioni pervenute aventi ad oggetto la presenza di contenuti illegali, specificando altresì l'avvenuto accertamento di notifiche manifestamente infondate, nonché le eventuali controversie sottoposte a meccanismi di risoluzione extragiudiziale.[30]

Per altro verso, va segnalata la centralità che il criterio della trasparenza assume all'interno del provvedimento, una pervasività tale da esercitare una diretta ricaduta sulle posizioni soggettive dei destinatari. In primo luogo l'obbligo gravante su ogni categoria di prestatori di rendere chiare, inserendole all'interno delle proprie condizioni generali, «le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana, nonché le regole procedurali del loro sistema interno di gestione dei reclami». L'obiettivo di fissare, in merito all'attività di moderazione dei contenuti illegali, regole intellegibili e solidamente ancorate al rispetto del principio di legalità, sembra inoltre essere assolto dalla "proceduralizzazione" e articolazione puntuale dei meccanismi di segnalazione e reclamo posti dall'articolo 16, nonché dalle garanzie che lo accompagnano.

---

[27] S. RUDOHRADSKÁ - D. TRESCÁKOVÁ, *Proposals for the digital markets act and digital services act: broader considerations in context ofonline platforms*, in *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 5/2021, p. 495 ss.

[28] Sul punto cfr. M.R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Rivista italiana di informatica e diritto*, 2/2021, p. 14 ss.

[29] A. NICITA, *Le piattaforme online tra moderazione e autoregolazione: verso il Digital Services Act*, in *Medialaws.eu*, 25 novembre 2020.

[30] M. HUSOVEC- I. ROCHE LAGUNA, *Digital Services Act: A Short Primer*, in M. HUSOVEC- I. ROCHE LAGUNA (eds.), *Principles of the Digital Services Act*, Oxford University Press, 2023, disponibile a https://ssrn.com/abstract=4153796 or http://dx.doi.org/10.2139/ssrn.4153796.

Nella prospettiva di promuovere un'attenuazione della discrezionalità dei fornitori in favore dei diritti dell'utente, appaiono poi di assoluto rilievo le garanzie poste dagli articoli 20, 21 e 23 del regolamento. L'articolo 20, infatti, introduce l'obbligo, per le piattaforme online, di procedere all'istituzione di un sistema interno di gestione dei reclami presentati dai destinatari del servizio in merito a segnalazioni precedenti, o contro le decisioni della piattaforma di sospensione, disabilitazione o definitiva cessazione dell'account per un periodo di almeno sei mesi. Inoltre, l'eventuale sospensione del servizio in presenza di abusi (art.23) richiede comunque una valutazione caso per caso che vada a contemplare anche la sistematicità e reiterazione della violazione: entrerebbero in gioco, dunque, i già evocati parametri di obiettività, tempestività, diligenza e proporzionalità, uniti a un giudizio fondato su un criterio numerico e sulla gravità del contenuto prodotto. Nella medesima logica appare egualmente essenziale, infine, la norma che introduce un diritto di accesso a meccanismi di risoluzione extragiudiziale delle controversie di fronte ad organismi la cui idoneità è accertata dal coordinatore dei servizi digitali in cui è stabilito l'organo giudicante.

L'azione dei colossi digitali appare così riorganizzata all'interno di un nuovo e composito regime normativo che assoggetta l'azione dei prestatori ad un solido controllo del soggetto pubblico e all'esigenza, dotata del medesimo peso assiologico in un sistema che aspira comunque a conformarsi sulle basi fondanti della *rule of law*, che tale opera di innalzamento delle garanzie non si traduca in un vulnus collaterale a danno dei diritti fondamentali dell'utente.[31]

Tale aspirazione non si coglie soltanto dai ricorrenti ed espliciti riferimenti a valori nodali, dal principio della certezza del diritto a quello di eguaglianza, ma si deduce implicitamente dalle dettagliate garanzie procedurali, disseminate nell'atto, che ricalcano da vicino i fondamenti tipici dello Stato di diritto costituzionale: dall'obbligo di motivazione della decisione al diritto di appello di fronte ad un soggetto indipendente e imparziale.

Tuttavia, nonostante tali elementi positivi, permangono diffuse criticità che ridimensionano in radice gli intenti garantistici dell'atto e le sue potenzialità di salvaguardia nei confronti dei diritti della persona-utente. Il regolamento si distingue per essere una normativa ispirata alla volontà di inquadrare l'azione degli intermediari all'insegna dei principi fondanti del diritto europeo e della Carta di Nizza e, quindi, ad un agire «diligente, obiettivo, non discriminatorio e proporzionato, tenendo debitamente conto dei diritti e degli interessi legittimi di tutte le parti coinvolte e fornendo le necessarie garanzie contro la rimozione ingiustificata di contenuti legali»; la lotta ai contenuti illeciti sembra dunque rimanere il principale obiettivo posto a fondamento dall'intervento e la primigenia vocazione dell'atto. Proprio intorno ad essa

[31] G. DE GREGORIO, *The Digital Services Act: A Paradigmatic Example of European Digital Constitutionalism*, in *Diritti Comparati*, 17 maggio 2021.

e alla effettiva concretizzazione della tutela delle posizioni soggettive coinvolte nello spazio digitale, tenderebbe a modellarsi il complesso regime di responsabilità che, come più volte sottolineato, diventa particolarmente stringente per le *very large platforms*.[32]

Il complesso di vincoli procedurali che condizionano l'operato degli intermediari, dagli obblighi di trasparenza alle periodiche valutazioni dei rischi sistemici, appare comunque funzionale al raggiungimento del primario scopo dell'intervento, quello di rafforzare il contrasto all'illecito.[33] Analogamente, le garanzie procedurali istituite a tutela dell'utente risultano logicamente secondarie rispetto allo scopo primario che muove il legislatore europeo. Per tali ragioni, una conseguenza non voluta - ma probabile - che potrebbe verificarsi è che il rigido sistema di obblighi stringenti introdotto dal regolamento possa in realtà incentivare una politica volta all'eliminazione indiscriminata di elementi qualificabili come "illegali". Più nel dettaglio, anche all'interno del nuovo quadro regolatorio andrebbero a riproporsi le criticità sollevate in merito al funzionamento del meccanismo del *notice and takedown*: in presenza di doveri e sanzioni, lo sforzo di svolgere un'attività di moderazione scevra da errori di valutazione viene sovrastato dall'esigenza di porre in essere un blocco sistematico dei contenuti sospetti. In conclusione, ciò che affiora sembra confermare il fatto che l'intervento perseguito dal legislatore continentale di "porre le briglie" al dilagante potere delle piattaforme, mediante un'onnicomprensiva articolazione delle garanzie, rimanga esso stesso imbrigliato in una logica di espansione delle tutele di natura meramente procedurale. In un contesto globale in cui il costituzionalismo digitale *in fieri* si confronta ancora con divergenze sensibili intorno ai principi fondanti, tale approccio rappresenta certamente la via più percorribile per costruire un soddisfacente sistema di salvaguardia dei diritti fondamentali nel cyberspazio. Tale compromesso, tuttavia, se non accompagnato da una robusta azione sul fronte sostanziale, rischia di creare dei presidi garantistici formalmente imponenti, ma vuoti sul piano sostanziale, perché ancora esposti alla discrezionalità interpretativa e applicativa delle piattaforme libere, ancora una volta, di plasmarne il significato.

4. Il nuovo AI Act alla prova dell'effettività della tutela

Simili perplessità possono applicarsi, d'altra parte, alla vocazione garantistica sottesa al nuovo atto normativo europeo, il recentissimo Regolamento sull'intelligenza artificiale.[34]

[32] Cfr.: G. FROSIO, *Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering*, in A. SAVIN- J. TRZASKOWSKI (a cura di), *Research Handbook on EU Internet Law*, Edward Elgar, 2023.
[33] V. C. CAUFFMAN-C. GOANTA, *A New Order: The Digital Services Act and Consumer Protection*, in *European Journal of Risk Regulation*, vol. 12, issue 4, 2021, p. 758 ss.
[34] Si veda S. PAJNO-M. BASSINI-G. DE GREGORIO-M. MACCHIA-F.P. PATTI-O. POLLICINO-S. QUATTROCOLO-D. SIMEOLI-P. SIRENA, *Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *Bio Law Journal*, fasc. n. 3, 2019, p. 205 ss.

Nel Regolamento in materia di intelligenza artificiale (*Artificial Intelligence Act*) si riprende un approccio normativo basato sulla valutazione del rischio (*risk based approach*) e sulla graduazione delle responsabilità dei fornitori di sistemi di AI: l'obbligo di provvedere a una valutazione di conformità *ex ante* grava sul fornitore stesso e l'intensità della procedura auto-valutativa è direttamente proporzionale ai rischi potenziali che l'impiego del sistema automatizzato potrebbe comportare.[35]

In questo senso, anche il quadro regolatorio introdotto dall'IA, dopo un primo sforzo volto a definire il concetto di sistema automatizzato, classifica i sistemi di AI sulla base del livello di rischio che pongono per l'individuo e i suoi diritti fondamentali.

Premessa l'identificazione di una categoria di sistemi automatizzati il cui utilizzo è proibito a causa dell'elevato livello di rischio che essi pongono per la sicurezza, la salute e, più in generale, i principi dello Stato di diritto - una categoria di tecnologie "a rischio inaccettabile" in ragione di sistemi il cui utilizzo comporta potenziali gravi effetti discriminatori (quali, ad esempio, i sistemi di classificazione biometrica fondati su dati sensibili quali etnia, sesso, orientamento religioso e politico) - la classificazione procede con una distinzione fra sistemi ad alto rischio e sistemi a rischio basso o minimo, cui corrisponde proporzionalmente un sistema di oneri gravanti principalmente a carico del fornitore e finalizzati a disporre una adeguata tutela nei confronti degli utenti. In merito ai primi il regolamento prevede l'assolvimento di adempimenti di controllo preventivo a carico del fornitore nonché il rispetto di alcuni requisiti, fra i quali ritornano quelli concernenti la sicurezza, la *governance* dei dati e la trasparenza.

Una disciplina in cui però, in particolare, i pilastri rappresentati dal principio di trasparenza e di *accountability* si fondono con il principio cardine del controllo umano.

Un intervento regolatorio ispirato alla volontà di garantire un utilizzo dell'intelligenza artificiale "*human centered*", in cui l'impiego di strumenti automatizzati si coniughi con un elevato grado di tutela dei diritti fondamentali e il principio della *rule of law*.[36]

Il modello di responsabilità si sostanzia, nel concreto, ancora una volta sulla logica della valutazione preventiva del rischio.[37] Modello cui, d'altronde, non si ispira soltanto l'architettura garantistica dello strumento ma anche la stessa categorizzazione delle diverse forme di intelligenza artificiale adoperate,

[35] A. AMIDEI, *La governance dell'Intelligenza Artificiale: profili e prospettive di diritto dell'Unione Europea*, in U. RUFFOLO (a cura di), *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Milano, Giuffrè, 2020, p. 571 ss.

[36] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1/2019, pp. 63-89; A. D'ALOIA, *Ripensare il diritto al tempo dell'Intelligenza Artificiale*, in G. CERINA FERRONI-C. FONTANA-A. RAFFIOTTA (a cura di*), AI Anthology*, Il Mulino, Bologna, 2022, p. 120; D. MARTIRE, *Intelligenza artificiale e Stato costituzionale*, in *Diritto Pubblico*, fasc. n. 2, 2022, p. 397 ss.

[37] A. BARONE, *Amministrazione del rischio e intelligenza artificiale*, *in European Review of Digital Administration & Law*, 2020, 1, p. 66.

classificate, come già osservato, proprio sulla base del livello di danno potenziale che pongono per i diritti fondamentali del singolo.[38]

Sotto il profilo dell'effettività della tutela offerta, ma anche della continuità con le fonti preesistenti, (interamente proiettate, come già osservato, sul modello della valutazione del rischio preventivo) appaiono sicuramente di maggior rilievo le prescrizioni poste dal paragrafo 9 dell'articolo 26, il quale, richiamando l'art. 35 del GDPR, pone a carico dell'operatore lo svolgimento della valutazione di impatto sulla protezione dei dati. Questo necessario adempimento, unito agli obblighi di trasparenza posti dall'articolo 13 a carico del fornitore, realizza una sinergia garantistica che appare soddisfacente. Inoltre, qualora l'operatore rilevi che il sistema di AI possa ragionevolmente costituire una minaccia per i diritti umani, ha l'obbligo di avvisare immediatamente il fornitore del servizio (paragrafo 5).

Tuttavia, la previsione più significativa è quella posta dall'art. 27 che introduce l'obbligo per l'operatore di svolgere il cosiddetto FRIA (*Fundamental rights impact assessment*), ossia una valutazione preventiva sui rischi che il sistema potrebbe porre per i diritti fondamentali dell'utente, un *iter* i cui tratti salienti vengono enunciati pedissequamente, dalla dettagliata descrizione dei procedimenti a cui verrà applicata alla enucleazione dei rischi specifici che potrebbe implicare, dalla indicazione delle persone maggiormente interessate dall'uso del sistema ai possibili rimedi che passino, ovviamente, per il rafforzamento della supervisione umana. Tale requisito, pur modellato, a tutta evidenza, sull'art. 35 del GDPR, ha carattere autonomo e distinto, essendo una valutazione di impatto che concerne la tutela del destinatario del procedimento a tutto tondo, non riguardando soltanto la garanzia dei dati personali (che trova, appunto, un suo parallelo e specifico richiamo, come evidenziato).

Di fronte a questo quadro, è senza dubbio opportuno sottolineare la centralità dell'AI Act in presenza del sempre più frequente impiego di sistemi automatizzati. La centralità che assumono i diritti fondamentali della persona all'interno della versione definitiva del provvedimento costituisce senza dubbio il positivo risultato di quel percorso riformatore a cui è stato sottoposto l'atto. Quest'ultimo sviluppo ha contribuito a modificare l'ossatura del provvedimento in favore di un sistema molto più orientato a salvaguardare le posizioni soggettive e proiettato verso le garanzie individuali.[39] Questo approccio risultava piuttosto secondario nella prima bozza, come si evince dal fatto che l'intero impianto normativo trovava nell'articolo 114 TFUE la sua principale base giustificatoria. Attualmente, invece, il riferimento alla tutela dei diritti fondamentali pare assumere lo stesso peso dell'obiettivo di garantire un funzionamento efficiente del mercato unico, come si evince, in primis, dall'articolo 1 che fissa il fine di

[38] A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?* in *federalismi.it,* fasc. n. 25, 2023, spec. p. 140 ss.

[39] G. DE GREGORIO-F. PAOLUCCI-O. POLLICINO, *L'intelligenza artificiale made in Ue è davvero "umano-centrica"? I conflitti della proposta*, 22 luglio 2021.

fondare una "*human centric and trustworthy artificial intelligence*"; ma anche dagli obiettivi indicati al Considerando n. 1 e seguenti che richiamano la centralità della persona e della sua tutela, sottolineando l'importanza di un *framework* garantistico che si fondi sui valori fondanti dei Trattati, della Carta dei diritti fondamentali e dell'articolo 2 TUE.[40]

Nonostante ciò, le ambiziose aspirazioni sottese alla disciplina, tradotte nelle varie previsioni prese ad esame, appaiono solide da un punto di vista formale-procedimentale ma, ancora una volta, carenti sotto il profilo sostanziale, benché sia opportuno attendere la resa applicativa del provvedimento. Allo stato attuale permangono, infatti, alcuni aspetti di opacità che pregiudicano l'effettività delle garanzie poste dal nuovo atto normativo.

In primo luogo, infatti, se rileva sottolineare la puntuale articolazione del procedimento ex art. 27 per effettuare la valutazione d'impatto sui diritti fondamentali, a testimonianza dell'attenzione per la tutela della persona di fronte all'uso di sistemi automatizzati nei tanti settori in cui oggi è possibile, ciò nondimeno, rimane prevalente la centralità della dimensione procedurale delle garanzie, senza che la previsione attui alcuno sforzo nel fornire una specifica definizione di "rischio" o di "danno irreparabile" per i diritti fondamentali, né tantomeno si prefigga di definirne alcuni. Una scelta discutibile che, se per un verso è imputabile alle differenti sensibilità e culture giuridiche presenti all'interno del sistema giuridico eurounitario, ha come conseguenza che la concreta definizione della valutazione risulta nei fatti affidata ad un soggetto privato (duplice, per giunta, perché gravante sia sulla figura del fornitore che dell'operatore- *deployer*).

In secondo luogo, dall'atto emerge un sistema sanzionatorio severo, che contempla le eventuali violazioni delle previsioni poste dall'articolo 26; purtuttavia, le garanzie non sembrano presidiate da adeguati strumenti riparativi i quali paiono essere relegati, peraltro, ai casi di maggior gravità. Risulta, inoltre, non del tutto chiarito il profilo della responsabilità, non essendo intuibile, in caso di accertata discriminazione o violazione prodotta dall'uso di uno strumento algoritmico, l'identificazione del soggetto responsabile sotto il profilo risarcitorio. Proprio alla rilevanza di tali problematiche è da imputare la scelta parallela del legislatore europeo di agire in senso correttivo mediante l'aggiornamento della disciplina sulla responsabilità.

Inoltre a parte le potenzialità racchiuse nel *Fundamental Rights Impact Assessment* che dovranno ancora essere indagate e scoperte alla luce della dimensione applicativa e delle linee guida che verranno prodotte, le

[40] Cfr. A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europea tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini Giuridica, Pisa, 2020, p.13; M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, fasc. n. 1, 2022, pp. 47-48.

previsioni dell'AI Act di frequente pongono in essere un richiamo esplicito a strumenti normativi già consolidati, fra i quali in particolare proprio il GDPR: una preminenza del Regolamento per la protezione dei dati personali il quale sembrerebbe porsi, allo stato attuale, come la fonte più consolidata e robusta cornice di garanzia per i diritti fondamentali dell'individuo, supportata anche da una consolidata applicazione giurisprudenziale.