TUTELA DEI DIRITTI FONDAMENTALI E PROMOZIONE DELL'INNOVAZIONE NEL PASSAGGIO DALLA STAGIONE ALL'AUTOMAZIONE A QUELLA DELL'AUTONOMIA

ORESTE POLLICINO*

1. Il consolidamento della società algoritmica e gli effetti sulle politiche di regolazione (giurisprudenziale e normativa). – 2. La reazione giurisdizionale al consolidamento dei poteri privati digitali e all'ascesa del fattore algoritmico: applicazione orizzontale dei diritti fondamentali in una prospettiva comparata e giurisprudenza creativa (e sue controindicazioni) della Corte di giustizia. – 3. Il legislatore europeo si riappropria del suo ruolo di *law maker*: la nuova stagione del costituzionalismo digitale in Europa. Un nuovo equilibrio tra regolazione ed innovazione tecnologica? – 4. Protezione dati e regolamentazione dell'algoritmo. – 5. Il passaggio da una dimensione (esclusivamente) assiologico-sostanziale ad una (anche) di matrice procedurale: coordinate teoriche e applicative. – 6. Libertà di espressione online, moderazione dei contenuti e algoritmo. – 6.1 Le coordinate costituzionali. – 7. Dalla Direttiva *e-Commerce* alla nuova stagione regolativa (DSA) della moderazione dei contenuti in rete. – 7.1. *Segue*. L'algoritmo nel DSA. – 8. Il nuovo Regolamento europeo sull'intelligenza artificiale: gli elementi portanti del nuovo sistema di regolazione. – 8.1. L'esplosione dell'intelligenza generativa ed i nuovi rischi per stato di diritto e democrazia: alcune definizioni di base. – 8.2. L'AI Act allo specchio: supera il test del costituzionalismo europeo? – 9. Riflessioni conclusive: quale futuro per il modello di regolazione del digitale in Europa?

1. *Il consolidamento della società algoritmica e gli effetti sulle politiche di regolazione (giurisprudenziale e normativa)*

La conformazione del cyberspazio e la fisionomia delle questioni problematiche che sono state tratteggiate nei paragrafi che precedono costituiscono il risultato di una serie di opzioni normative che i legislatori soprattutto di Stati Uniti e Unione europea hanno abbracciato tra il finire degli anni '90 e l'inizio del nuovo millennio.

Durata ben poco l'illusione di un web "libero" da possibili costrinimenti statali, si è posta un'esigenza di regolazione coerente con le

* Ordinario di Diritto costituzionale, Università Bocconi. Rappresentante italiano presso il Board della Agenzia europea per la protezione dei diritti fondamentali, Vienna.

peculiarità dell'ecosistema digitale, soddisfatta tanto in Europa quanto negli Stati Uniti secondo un'impostazione che riflette un approccio minimalista volto a favorire una circolazione ampia di contenuti.

L'approccio liberale seguito dall'Unione nel corso dei primi anni del ventunesimo secolo appare essere coerente alla luce delle coordinate storiche in cui i citati provvedimenti legislativi venivano adottati e, in particolare, alla luce dello stato dell'avanzamento tecnologico nei primi anni 2000. Gli anni successivi, peraltro, si sono caratterizzati per un vertiginoso evolversi di quelle stesse tecnologie digitali (ed, in particolare, l'ascesa del fattore algoritmico) le quali, a loro volta, hanno condotto a un progressivo e inarrestabile mutamento dello stesso paradigma sociale.

Ricorrendo alle parole di Jack Balkin¹, l'attuale contesto storico è dominato dall'avvenuta affermazione di una «società algoritmica», caratterizzata segnatamente da due fattori. Da un lato, quest'ultima si fonda, per l'appunto, sull'accresciuto rilievo dello strumento dell'algoritmo, anche grazie allo straordinario patrimonio di dati ormai a disposizione di attori pubblici e, soprattutto, privati. Dall'altro lato, si tratta di una società che si caratterizza anche per l'emersione di nuovi rilevanti attori, per l'appunto, privati nello scenario globale. Le cosiddette *big tech*, o le «compagnie del digitale», come osservato da Luciano Violante, riadattando al nuovo contesto globale il potere di fatto detenuto dalle «Compagnie delle Indie», ovvero le grandi società commerciali transnazionali dedite alla provvisione di servizi digitali, hanno assunto un ruolo di primaria importanza nella vita quotidiana di ognuno di noi, in particolare, e, più in generale, nella vita della società nel suo insieme².

Ciò è particolarmente evidente, per esempio, nel modo in cui le piattaforme in rete organizzano e gestiscono quelle nuove *agorà* digitali rappresentate dai *social network*: come si avrà modo di discutere

¹ J.M. BALKIN, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in *U.C.D. Law Review*, fasc. 51, 2018 1149.

² L. VIOLANTE, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *Rivista di BioDiritto*, fasc. 1, 2022 145-153, 148: «Le 'compagnie del digitale', potremmo definirle così, hanno un potere politico di fatto che nessuno ha mai avuto: creano opinioni, hanno una funzione regolatrice della vita dei privati e degli Stati, rendono servizi indispensabili e per questo condizionano la qualità dell'attività privata e pubblica».

più avanti, le modalità di gestione dell'informazione in internet sono al giorno d'oggi strettamente dipendenti dalle modalità in cui tali attori privati scelgono di amministrare i contenuti, generalmente attraverso l'utilizzo di sistemi automatizzati fondati sulla raccolta di dati concernenti gli utenti. Gli effetti della società algoritmica, d'altro canto, sono percepibili anche in contesti diversi da quella dell'informazione in senso stretto, alla luce, in particolare, della generale diffusione di sistemi decisionali automatizzati in una pluralità di contesti diversi: dalla sanità al lavoro, dalla giustizia³ alla pubblica sicurezza. Anche in questi settori si intravede, infatti, sia il sempre più frequente ricorso all'algoritmo, sia una crescente commistione tra pubblico e privato. Se ne parlerà in conclusione, quando si accennerà al modello di co-regolazione.

2. *La reazione giurisdizionale al consolidamento dei poteri privati digitali e all'ascesa del fattore algoritmico: applicazione orizzontale dei diritti fondamentali in una prospettiva comparata e giurisprudenza creativa (e sue controindicazioni) della Corte di giustizia*

Di fronte ai cambiamenti del panorama digitale, l'Unione Europea ha progressivamente ridefinito il proprio approccio regolatorio. Il primo vero motore di questa trasformazione è stata la Corte di Giustizia dell'UE, che dagli anni 2010 ha sviluppato una giurisprudenza volta a colmare l'inerzia legislativa e a rafforzare la protezione dei dati personali, spesso senza garantire adeguati meccanismi di enforcement e cooperazione internazionale.

Un aspetto cruciale di questa evoluzione è l'uso dell'applicazione orizzontale dei diritti fondamentali, che distingue il costituzionalismo europeo da quello statunitense. In risposta alla trasformazione degli attori digitali in *poteri privati* e all'ascesa dell'*automazione basata sui dati*, la Corte ha reinterpretato in modo audace le disposizioni dei trattati, rendendole strumenti direttamente azionabili dai singoli cittadini.

Da questo punto di vista, pare essere eccessivamente pessimista Tim Wu, in genere uno dei più attenti studiosi dei temi oggetto di indagine,

³ Per una lucida analisi, LONGO, *Giustizia digitale e Costituzione: Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, cit.

secondo il quale «colpisce il fatto che documenti come la Magna Carta, la Costituzione degli Stati Uniti, il Trattato di Lisbona e lo Statuto delle Nazioni Unite siano stati scritti per contenere l'esercizio di un potere pubblico privo di contrappesi, mentre non abbiano niente che faccia effettivamente la stessa cosa contro il potere privato incontrollato»⁴. Al contrario, invece, la giurisprudenza europea dimostra il contrario: attraverso un'interpretazione creativa, la Corte ha trasformato norme pensate per vincolare gli Stati in strumenti di tutela individuale, ampliando l'effetto diretto orizzontale in modi non previsti al momento della loro adozione.

Così come è eccessivamente ottimista quanto sostiene a questo riguardo Robert Alexy⁵, ovvero che la questione relativa agli effetti orizzontali dei diritti fondamentali previsti dalle Carte costituzionali o dai *Bills of rights* non possa essere concettualmente scissa dal problema più generale del riconoscimento di un effetto diretto agli stessi diritti. In altre parole, se è riconosciuto a un diritto fondamentale effetto diretto, tale riconoscimento dovrebbe essere caratterizzato da una doppia dimensione: quella verticale (autorità vs. libertà) e quella orizzontale (nei rapporti tra privati).

Tuttavia, l'idea di attribuire un'efficacia orizzontale ai diritti fondamentali, per quanto teoricamente solida, non trova un'applicazione uniforme a livello comparato, dipendendo dal paradigma costituzionale di riferimento. In Europa, questa possibilità si fonda sulla *Drittwirkung* di matrice tedesca, che ha consentito alle nostre Carte dei diritti di vincolare anche soggetti privati.⁶

Dal canto suo, la Corte di Giustizia dell'UE ha seguito un percorso simile, conferendo efficacia diretta orizzontale a disposizioni originariamente rivolte solo agli Stati membri. Un caso emblematico è *Defrenne II*⁷, dove l'art. 119 TCE (oggi art. 157 TFUE) sulla parità retributiva è

⁴ T. WU, *La maledizione dei giganti: un manifesto per la concorrenza e la democrazia*, Bologna, 2021 10.

⁵ R. ALEXY, *Teoria dei diritti fondamentali*, Bologna, 2012 570-571.

⁶ BVerfGE, 7, 198, 15 gennaio 1958.

⁷ C. giust. CE 8 aprile 1976, *Gabrielle Defrenne c. Société anonyme belge de navigation aérienne Sabena*, causa 43/75. La sentenza è stata ampiamente discussa in dottrina. Tra i primi commenti, O. STOCKER, *Le second arrêt Defrenne. L'égalité de rétribution des travailleurs masculins e des travailleurs féminin*, in *Cahiers droit européen*, 1977 180 ss.;

stato reinterpretato per essere immediatamente applicabile nei rapporti tra privati. Questa sentenza ha avuto un impatto paragonabile a *Costa c. Enel*⁸ per la supremazia del diritto UE e *Simmenthal*⁹ per l'effetto utile.

Tale approccio si è esteso al digitale, dove la Corte ha reagito alla crescita del *potere algoritmico* in assenza di un intervento legislativo tempestivo. Tra il 2014 e il 2015, ha di fatto applicato in modo surrettizio gli artt. 7 e 8 della Carta dei diritti fondamentali,¹⁰ rafforzando la tutela della privacy e della protezione dei dati nei confronti delle grandi piattaforme, anticipando la regolazione poi formalizzata con il GDPR¹¹.

Un esempio lampante di quanto si diceva si ha in *Google Spain*, sentenza che si è avuto già modo di richiamare per la sua rilevanza a proposito della dimensione “spaziale”, la Corte estende anche ai motori di ricerca, attraverso un'applicazione orizzontale surrettizia della Carta, le tutele previste dagli artt. 7 e 8 della Carta di Nizza. Più precisamente, l'Autorità garante spagnola per la protezione dei dati aveva richiesto a Google di rimuovere alcuni link che comparivano nel momento in cui il nome del ricorrente fosse stato utilizzato come parola-chiave di ricerca. Google aveva rifiutato di adempiere alla richiesta, sostenendo di non essere soggetta al diritto dell'UE, in quanto avente sede negli Stati Uniti. Secondo Google, un'obbligazione in tal senso avrebbe, per di più, comportato una restrizione alla libertà di espressione degli utenti.

W. VAN GERVEN, *Contribution dell'arret defrenne au development du droit comunitarie*, in *Cabiers droit européen*, 1977 131 ss.; G. CATALANO SGROSSO, *Il principio della parità di trattamento tra lavoratori e lavoratrici nel diritto comunitario*, in *Rivista di diritto europeo*, 1979 245 ss.

⁸ C. giust. CE 15 luglio 1964, *Flaminio Costa c. ENEL*, causa 6/64.

⁹ C. giust. CE 9 marzo 1978, *Amministrazione delle Finanze dello Stato c. Simmenthal SpA*, causa 106/77.

¹⁰ O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *La Carta dei Diritti Fondamentali dell'Unione Europea. Efficacia ed effettività*, a cura di V. Piccone, O. Pollicino, Napoli, 2018, 264 ss.

¹¹ O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *La Carta dei Diritti Fondamentali dell'Unione Europea. Efficacia ed effettività*, a cura di V. Piccone, O. Pollicino, Napoli, 2018, 264 ss.

Ancora, in *Schrems I* si è di fronte a un'interpretazione – *melius* manipolazione – della Direttiva 95/46 “illuminata” dagli artt. 7 e 8 della Carta di Nizza. In questa decisione, il nodo cruciale è se i regolatori nazionali abbiano un qualche margine di manovra per opporsi a una decisione della Commissione europea che valutasse l'adeguatezza del livello di protezione assicurato dai sistemi giuridici di Paesi terzi. Nel caso di specie, il riferimento è alla Decisione 2000/520 (*Safe Harbour Decision*), relativa al trasferimento di dati personali dall'UE agli Stati Uniti. La risposta della Corte è positiva e comporta l'invalidazione della Decisione 2000/520.

Più precisamente, la Corte si è trovata a valutare se la decisione citata rispettasse le condizioni fissate dall'art. 25 della Direttiva 95/46, che richiedeva un adeguato livello di protezione per i dati personali trasferiti in Paesi terzi. Sulla base di tale norma, la CGUE riteneva opportuno andare a valutare se il sistema giuridico statunitense fosse o meno in grado di fornire un livello di protezione adeguato ai dati personali dei cittadini dell'Unione.

La Corte, dunque, ha reinterpretato il concetto di “livello di protezione adeguato” dell'art. 25 della Direttiva 95/46/CE, legandolo agli artt. 7 e 8 della Carta di Nizza. Questo ha portato a una trasformazione dello standard di adeguatezza, che la Corte ha ridefinito in termini di “equivalenza sostanziale” tra i sistemi di tutela europei e quelli dei Paesi terzi¹².

Un aspetto distintivo della decisione è che, a differenza di *Digital Rights Ireland*, qui il giudizio di conformità riguarda il sistema statunitense, influenzato dallo scandalo NSA. L'impatto è stato transatlantico: la decisione ha trovato eco nella sentenza *ACLU v. Clapper*¹³, che

¹² Si vedano in tal senso anche le Conclusioni dell'Avvocato Generale 23 settembre 2015, *Maximillian Schrems c. Data Protection Commissioner* (Schrems I), causa C-362/14. In particolare, il paragrafo 141 argomenta: «È per questo motivo che ritengo che la Commissione possa constatare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che un paese terzo assicura un livello di protezione adeguato solo qualora, al termine di una valutazione di insieme del diritto e della prassi nel paese terzo in questione, essa sia in grado di dimostrare che tale paese offre un livello di protezione sostanzialmente equivalente a quello offerto da tale direttiva, anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione».

¹³ Corte d'appello federale degli Stati Uniti d'America per il Secondo Circuito 7 maggio 2015, *ACLU v. Clapper*, in 785 F3d 787 (2d Cir 2015).

ha limitato la sorveglianza di massa negli Stati Uniti. Questo dimostra come le idee costituzionali nel digitale possano migrare in entrambe le direzioni.

Più in generale, la Corte ha operato una “manipolazione interpretativa”, sostituendo il concetto di adeguatezza con quello di equivalenza, rafforzando così la sovranità europea sulla privacy digitale come risposta alla crescente influenza degli attori privati e all'ascesa del *fattore algoritmico*.

Questa tendenza riflette una caratteristica peculiare del costituzionalismo europeo: l'applicazione orizzontale dei diritti fondamentali, assente invece nel modello statunitense. In altre parole, come ha osservato Mark Tushnet, «*the judicialisation of relations between private persons [is] as an intolerable intrusion of the state into the sphere of private autonomy*»¹⁴. Negli USA, infatti, la *state action doctrine* limita l'efficacia dei diritti costituzionali ai soli rapporti tra individui e Stato, escludendo i rapporti tra privati. Questa resistenza deriva da un humus culturale che pone al centro *liberty* e *individual freedom*, principi fondanti dell'autonomia privata.

Non solo, ma come è stato giustamente notato «nell'interpretazione della Corte d'Appello, mancano totalmente possibili punti di contatto tra un prestatore di servizi, come Youtube, e ciò che nel diritto costituzionale statunitense rappresenta uno *state actor*: non vi sarebbe alcuna partecipazione a quel novero limitato di funzioni che sono tradizionalmente riservate in via esclusiva allo Stato»¹⁵; al contrario, questi non sarebbero altro che soggetti privati che adottano decisioni relative alla *governance* del proprio spazio¹⁶.

La metafora dei social network come nuova piazza pubblica è spesso evocata, ma assume un significato ben diverso quando implica con-

¹⁴ S. GARDBAUM, *The «Horizontal Effect» of Constitutional Rights*, in *Michigan Law Review*, fasc. 102, 2003 388 ss.; M. TUSHNET, *The Issue of State Action/Horizontal Effect in Comparative Constitutional Law*, in *International Journal of Constitutional Law*, fasc. 1, 2003 79 ss.; W.R. HUHNS, *The State Action Doctrine and The Principle of Democratic Choice*, in *Hofstra Law Review*, fasc. 84, 2006 1380 ss.

¹⁵ BASSINI, *Libertà di espressione e social network, tra nuovi «spazi pubblici» e «poteri privati»*. *Spunti di comparazione*, cit. 22.

¹⁶ Ivi, 68.

seguenze normative¹⁷. La giurisprudenza statunitense ha riconosciuto questa dimensione solo per gli *state officials*, considerando il blocco di utenti come una potenziale violazione del Primo Emendamento¹⁸. Inoltre, ha chiarito che spazi privati possono acquisire una natura pubblica come *designated public forums*, trasformandosi in luoghi di espressione soggetti a vincoli costituzionali¹⁹.

Sul versante europeo, la Corte di Giustizia ha progressivamente ridefinito la responsabilità dei fornitori di servizi digitali. Se la Direttiva *e-Commerce* garantiva loro un'ampia esenzione, i giudici di Lussemburgo hanno ristretto questa protezione, escludendola per gli operatori che non si limitano a una funzione meramente "tecnica, automatica e passiva". L'obiettivo era adeguare una normativa ormai obsoleta rispetto all'ascesa di attori privati con un potere economico crescente²⁰.

Questo attivismo giurisprudenziale, pur comprensibile di fronte all'inerzia legislativa, ha però generato alcune criticità. La prima è uno squilibrio tra poteri: la *judicial globalization*²¹ ha amplificato il ruolo delle Corti rispetto a legislativo ed esecutivo, aggravato dall'accelera-

¹⁷ Corte Suprema federale degli Stati Uniti d'America 15 marzo 2024, *Lindke c. Freed LLC*, in 601 U.S. 187 (2024).

Corte Suprema federale degli Stati Uniti d'America 15 marzo 2024, *O'Connor-Ratliff c. Garnier*, in 601 U.S. 205 (2024).

¹⁸ Corte distrettuale degli Stati Uniti d'America per il distretto meridionale di New York 23 maggio 2018, *Knight First Amendment Inst. at Columbia Univ. c. Trump*, n. 1:17-cv-5205 (S.D.N.Y.); Corte d'appello federale degli Stati Uniti d'America per il Secondo Circuito 9 luglio 2019, *Knight First Amendment Inst. at Columbia Univ. c. Trump*, n. 18-1691 (2d Cir.); Corte Suprema federale degli Stati Uniti d'America 5 aprile 2021, *Joseph Biden Jr., President of the United States, et al., c. Knight First Amendment Inst. at Columbia Univ.*, in 593 U.S. (2021); Corte d'appello federale degli Stati Uniti d'America per il Quarto Circuito 7 gennaio 2019, *Davison c. Randall*, n. 17-2002 (4th Cir.).

¹⁹ Corte Suprema federale degli Stati Uniti d'America 15 marzo 2024, *Lindke c. Freed LLC*, in 601 U.S. 187 (2024).

Corte Suprema federale degli Stati Uniti d'America 15 marzo 2024, *O'Connor-Ratliff c. Garnier*, in 601 U.S. 205 (2024).

²⁰ CGUE, cause riunite C-236/08, *Google France SARL e Google Inc. c. Louis Vuitton Malletier SA*, C-237/08, *Google France SARL c. Viaticum SA e Luteciel SARL*, e C-238/08, *Google France SARL c. Centre national de recherche en relations humaines (CNRRH) SARL e altri*, sentenza del 23 marzo 2010; causa C-324/09, *L'Oréal SA e altri c. eBay International AG e altri*, sentenza del 12 luglio 2011.

²¹ A. SLAUGHTER, *Judicial Globalization*, in *Virginia Journal of International Law*, fasc. 40, 2000 1103 ss.

zione tecnologica che rende il legislatore riluttante a intervenire su un terreno in continua evoluzione. La seconda riguarda la frammentazione normativa: l'assenza di un intervento legislativo chiaro ha portato a una proliferazione di categorie giurisprudenziali per definire il ruolo degli *Internet service providers*, generando incertezza giuridica.²²

Infine, emerge un rischio insidioso: la delega, di fatto, a soggetti privati del bilanciamento tra diritti fondamentali. Il caso *Google Spain* è emblematico di questa dinamica, in cui la decisione su cosa rimuovere dal web è stata affidata direttamente a un operatore privato, senza adeguate garanzie procedurali. Questo spostamento di potere, benché nato dalla necessità di colmare un vuoto regolatorio, solleva interrogativi sulla trasparenza e la democraticità delle scelte che plasmano l'ecosistema digitale.

3. *Il legislatore europeo si riappropria del suo ruolo di law maker: la nuova stagione del costituzionalismo digitale in Europa. Un nuovo equilibrio tra regolazione ed innovazione tecnologica?*

Preso atto dell'improrogabilità di un intervento normativo per tutte le ragioni esposte nel paragrafo precedente, il legislatore dell'Unione ha deciso, a partire dalla metà degli anni 2010 e sempre più dagli inizi degli anni 2020, di riappropriarsi del ruolo di legislatore, temporaneamente assunto dalla Corte di giustizia, così avviando quello che è stata da più parti definita come la nuova stagione del "costituzionalismo digitale"²³ in Europa.

²² *ex multis*, C. gius. UE 23 marzo 2010, *Google France*, cause C-236/08, C-237/08 e C-238/08; C. gius. UE 12 luglio 2011, *L'Oréal e altri*, causa C-324/09; C. gius. UE 3 ottobre 2019, *Glawischnig-Piesczek*, causa C-18/18. Per quanto concerne la giurisprudenza italiana Cass. pen. 19 marzo 2019, n. 7708. Sul piano nazionale, cfr. Tribunale di Roma, sez. IX, 27 aprile 2016, n. 8437.

²³ G. DE GREGORIO, *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, Cambridge, 2022; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, cit. Invero, la nozione stessa di «costituzionalismo digitale» è ancora un concetto, per così dire, «in divenire»: si vedano in tal senso, tra gli altri, E. CELESTE, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Londra, 2022 77-87; A.J. GOLIA, *Critique of digital constitutionalism: Deconstruction and reconstruction from a societal perspective*, in *Global Constitutionalism*, 2023 1-31.

Con tale espressione si vuole, in particolare, esprimere il plesso di interventi legislativi dell'Unione volti direttamente a regolare il fenomeno tecnologico e digitale, nelle sue varie forme, al fine precipuo di salvaguardare e promuovere i valori propri del costituzionalismo europeo, a cominciare da quello della dignità.

In altre parole, si tratta di una nuova stagione quanto al rapporto tra regolazione e innovazione, in cui è stato il processo politico a riprendere in mano il pallino relativo alle modalità espressive della sovranità digitale di reazione al contenimento del nuovo potere privato da una parte, e all'ascesa del fattore algoritmico, dall'altra.

Una precisazione è d'obbligo prima di proseguire oltre.

Al di là delle etichette, e delle possibili confusioni concettuali che sono state attribuite, non sempre a ragione, con riferimento all'asserita assonanza, in realtà non fondata, tra le teorie del *global constitutionalism*²⁴ e le diverse elaborazioni del c.d. costituzionalismo digitale, una cosa è certa: il costituzionalismo digitale abbraccia un concetto più ampio che non è limitato all'ambito globale, ma che, al contrario, include anche le prospettive del costituzionalismo sociale e liberale²⁵.

Questa nuova fase europea segna un tentativo del legislatore di riappropriarsi del proprio ruolo di *law maker*, rimasto troppo a lungo nelle mani della Corte di Giustizia, soprattutto in ambito digitale. A differenza della stagione del *liberismo digitale* degli anni 2000, dominata dall'antitrust, il legislatore oggi riconosce la necessità di un approccio costituzionalmente orientato per contenere l'influenza dei *poteri privati* e prevenirne gli abusi.

I prossimi paragrafi analizzeranno le principali tappe di questa *nuova stagione costituzionale* dell'Unione, esaminando le strategie adottate per contrastare le esternalità negative dell'ascesa del *fattore algoritmico* (par. 6) e, successivamente, dell'intelligenza artificiale vera e propria (par. 7), che introduce elementi di autonomia, deduzione, predizione e adattabilità. L'obiettivo è garantire la tutela dei valori democratici e dello Stato di diritto in un ecosistema digitale sempre più complesso.

²⁴ M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, cit.

²⁵ F. de A. DUARTE *et al.*, *Perspectives on digital constitutionalism*, in B. BROZEK *et al.*, *Research Handbook on Law and Technology*, Northampton, 2023.

4. Protezione dati e regolamentazione dell'algoritmo

La nuova stagione della regolamentazione europea del digitale si è aperta con l'adozione, nel 2016, del Regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR)²⁶ il quale ha sostituito la summenzionata Direttiva 95/46/CE.

Ai nostri fini, in quanto emblematico del cambiamento di rotta che si è tratteggiato in precedenza, l'aspetto più rilevante della nuova (ai tempi) normativa europea sembra essere rappresentato da un significativo ripensamento, a livello assiologico-sostanziale, dello stesso metodo di regolazione dell'Unione in tema di tutela della privacy. La nuova disciplina, infatti, sebbene pur sempre volta a un temperamento tra gli interessi economici alla libera circolazione dei dati e la tutela dei valori democratici e costituzionali²⁷, si caratterizza, tuttavia, per una connotazione spiccatamente personalistica e un orientamento maggiormente attento alla stretta interrelazione tra diritto alla privacy e diritto alla protezione dei dati, da un lato, e tutela della dignità umana²⁸. Una tale dimensione "costituzionale" dei diritti alla privacy e alla protezione dei dati personali emerge, tra l'altro, dal considerando 4 del Regolamento:

«Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e

²⁶ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GU L.,119/2016.

²⁷ Invero, l'articolo 1 del GDPR, se specifica al paragrafo 2 che esso mira a proteggere «i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali», allo stesso tempo chiarisce anche al paragrafo 3 che «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

²⁸ Sul rapporto tra *privacy*, *data protection* e dignità sotto un profilo filosofico si veda, in particolare, L. FLORIDI, *On Human Dignity as a Foundation for the Right to Privacy*, in *Philosophy & Technology*, fasc. 29, 2016 307-312.

osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica»²⁹.

Oltre ad avere sostanzialmente codificati gran parte degli orientamenti giurisprudenziali espressi negli anni precedenti dalla Corte di Lussemburgo, ivi inclusa l'introduzione di una specifica norma dedicata alla previsione di un "diritto all'oblio"³⁰, il GDPR, si è osservato, configura un approccio legislativo peculiare che, focalizzandosi sul principio di "responsabilizzazione" (*accountability*) del titolare del trattamento, richiede a quest'ultimo di attivarsi per la protezione dei diritti fondamentali dell'interessato. Infatti, la disciplina rilevante non si focalizza tanto sulla previsione di una serie di prescrizioni e obblighi, il rispetto dei quali consentirebbe al titolare del trattamento di proteggersi dall'inflizione di sanzioni legislative, piuttosto il GDPR prevede che siano gli stessi titolari a valutare l'entità dei rischi – in termini, ovviamente, di tutela della *privacy* e di protezione dei dati – che derivino dalle loro attività e, conseguentemente, ad adottare i necessari correttivi per mitigare tali rischi³¹. Il Regolamento in questione ha, così, segnato un'evoluzione strutturale nell'approccio euro-unitario alla tutela dei

²⁹ GDPR, considerando 4.

³⁰ GDPR, art. 17.

³¹ G. DE GREGORIO, *The rise of digital constitutionalism in the European Union*, cit., spec. p. 64. Sulla connessione tra principio di *accountability* e concetto di «rischio», alla luce del cosiddetto «*risk-based approach*» caratterizzante il GDPR, vedi inoltre G. DE GREGORIO, P. DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, in *Common Market Law Review*, fasc. 59, 2, 2022 473-500, spec. 478-483. Il concetto e le finalità del principio di *accountability* sono state in tal senso ben sintetizzate da Giusella Finocchiaro:

«Le norme del GDPR sull'*accountability* hanno lo scopo di promuovere l'adozione di misure concrete e pratiche, trasformando i principi generali della protezione dei dati in politiche e procedure concrete, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento deve anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. Quindi, responsabilità e prova delle misure adottate per far fronte alla responsabilità» G. FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, Bologna 2024, spec. 85.

diritti considerati, mirando in particolare alla costituzione (e, per così dire, alla costituzionalizzazione) di una vocazione assiologico-sostanziale della normativa in materia di privacy e data protection in Europa. Una vocazione, del resto, così pregnante da aver condotto alcuni commentatori a definire, come si è anticipato in precedenza, il diritto alla privacy come il «Primo emendamento» dell'Unione³².

La disciplina introdotta dal GDPR, peraltro, ha riflessi significativi nel contesto della regolamentazione dell'algoritmo e dei processi decisionali automatizzati sotto diversi profili.

Proprio con riguardo all'ascesa del fattore algoritmico e conseguente reazione in termini di cambio di passo della regolamentazione a livello europeo, di particolare pregnanza è una specifica norma contenuta nel GDPR. L'articolo 22, rubricato come "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione", prevede che, fatta eccezione per determinati casi eccezionali³³, all'interessato spetti «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». L'articolo 22 ha, comprensibilmente, suscitato il vivo interesse della dottrina, determinata a comprenderne le effettive implicazioni, la portata e le finalità. Peraltro, come si è brillantemente osservato, tale previsione rappresenta forse una delle massime espressioni di quell'approccio alla tutela di privacy e data protection fondato sulla promozione dei valori democratici e costituzionali intimamente connessi alla dignità umana³⁴.

Infatti, se il ricorso all'algoritmo e alla decisione automatizzata rappresenta in ultima analisi uno strumento particolarmente appetibile

³² B. PETKOVA, *Privacy as Europe's first amendment*, in *European Law Journal*, fasc. 25, 2019, 140-154.

³³ In particolare, ai sensi dell'art. 22(2), «nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato».

³⁴ E. CELESTE, G. DE GREGORIO, *Digital Humanism: The Constitutional Message of the GDPR*, in *Global Privacy Law Review*, fasc. 3, 1, 2022 4-18.

sotto il profilo economico e di mercato – alla luce della rapidità ed efficienza con cui tali sistemi possono produrre *output* a fronte delle ben più limitate capacità computazionali umane – l’articolo 22 sembra porre un freno a un tale utilizzo, laddove esso possa implicare conseguenze sul piano giuridico di significativa importanza. In tali contesti, il GDPR richiede che, a fronte della potenziale efficienza delle tecnologie in esame, prevalgano altri valori connessi alla necessità di un intervento umano. Invero, non sarebbe plausibile affermare che l’intervento umano rappresenti sempre una garanzia per il corretto funzionamento di processi decisionali concernenti la persona interessata: gli stessi esseri umani sono, infatti, fallibili. Purtuttavia, l’intelligenza umana si differenzia dall’algoritmo e dall’intelligenza artificiale, perché non si fonda su meri procedimenti logico-formali o su (pur complessi) calcoli statistici, ma è sovente in grado di interpretare e dare rilievo a importanti circostanze di fatto attinenti al singolo caso concreto e la singola persona umana. Detto in altri termini, l’intelligenza umana non corre quel rischio (o, *rectius*, lo corre in misura minore) di ridurre la persona a una semplice serie di dati, disumanizzandola e potenzialmente conducendo a risultati e conseguenze non rispettose della sua individualità e dignità³⁵.

Inoltre, l’uso di sistemi automatizzati, e in particolare di sistemi di profilazione, comporta concreti rischi di discriminazione e *bias* algoritmici, in aperto contrasto con le più basilari condizioni di esercizio della dignità umana. Questi rischi, sebbene in molti casi non molto diversi dalla capacità umana di discriminare nel mondo analogico, richiedono che il legislatore adegui gli strumenti offerti dal diritto, in generale, e dal diritto costituzionale, in particolare.

D’altra parte, occorre sottolineare come l’articolo 22 non abbia solo una valenza significativa sotto il piano sostanziale e, per così dire, ide-

³⁵ *Ibidem*. 13: «Article 22(1), therefore, implicitly provides that, when a decision affects important aspects of human life, machines, alone, do not suffice, and human intervention is needed. In other words, this norm establishes that human life is more important than economic efficiency. Human life requires an anti-economic effort to safeguard its unicity and unrepeatability ... Attempting to reduce [human life] to a series of machine-readable data would be impossible. It would imply an objectification, a radical de-humanization of the individual».

ologico, ma anche sotto il profilo pratico-procedurale. In particolare, si è da più parti sottolineato come la norma intenda promuovere una maggiore trasparenza dei processi decisionali concernenti la persona umana: il ricorso ad algoritmi e sistemi di IA, infatti, è soggetto al noto problema della cosiddetta “scatola nera” (*black box*)³⁶, ovvero alla inerente difficoltà nel comprendere le ragioni sottese a una decisione automatizzata – difficoltà che generalmente si acuisce tanto più quanto più il sistema stesso sia sofisticato. Alla luce di ciò, è stata particolarmente rilevante l'interpretazione della regola introdotta dall'articolo 22(3). Questa disposizione stabilisce che, anche quando il processo decisionale automatizzato o la profilazione sono legittimi, ad esempio in caso di consenso dell'interessato, quest'ultimo ha sempre «il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione».

La portata e rilevanza di tale paragrafo sono state oggetto di un importante dibattito dottrinale, soprattutto negli anni immediatamente successivi all'adozione del GDPR³⁷. In ogni caso, l'opinione ormai prevalente è quella che riconosce nell'articolo 22 quanto meno *in nuce*³⁸, un diritto dell'interessato alla “spiegazione” sottesa alla decisione presa³⁹. Una tale direzione è stata recentemente ribadita dalla CGUE che, interpretando l'Art. 22 GDPR, ha stabilito per gli interessati il diritto a ricevere “informazioni significative sulla logica utilizzata” dal processo decisionale automatizzato impiegato eventualmente dal titolare del trattamento per effettuare, ad esempio, una valutazione sulla solvibilità del credito di un richiedente. Ebbene, in questo caso, la Corte ha ribadito che per informazioni significative si intende «informazioni pertinenti e in forma concisa, trasparente, comprensibile e facilmente accessibile, la procedura e i principi concretamente applicati per utilizzare, con mezzi automatizzati, i dati personali relativi a

³⁶ F. PASQUALE, *The black box society: the secret algorithms that control money and information*, Cambridge, Mass.-London, 2015.

³⁷ G. MALGIERI, *Automated decision-making in the EU Member States: The right to explanation and other «suitable safeguards» in the national legislations*, in *Computer Law & Security Review*, fasc. 35, 5, 2019, spec. 3-4.

³⁸ G. FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit., spec. 83.

³⁹ Cfr. Cons. 71, GDPR.

tale interessato al fine di ottenerne un risultato determinato, come un profilo di solvibilità».⁴⁰

È chiaro, dunque, come la disciplina del trattamento dei dati contenuta nel GDPR e, in particolare, il descritto articolo 22 rappresentino un primo e assai significativo passo in avanti nel contesto della regolamentazione dell'algoritmo⁴¹ e, in particolare, nel contesto di quel summenzionato processo di iniezione, da parte dell'Unione, di valori democratico-costituzionali all'interno del mercato digitale. D'altra parte, come si vedrà di seguito, tale processo è andato ulteriormente evolvendosi negli anni successivi all'entrata in vigore del Regolamento in questione, modificando anche le sue coordinate di sviluppo: non soltanto di ordine assiologico-sostanziale, ma anche tecnico-procedurale.

5. *Il passaggio da una dimensione (esclusivamente) assiologico-sostanziale ad una (anche) di matrice procedurale: coordinate teoriche e applicative*

Nel paragrafo precedente si è evidenziato come il GDPR abbia trasformato il diritto alla protezione dei dati personali da una prospettiva economicamente orientata (come nella Direttiva 95/46/CE) a una dimensione costituzionale. Questa evoluzione è stata possibile grazie alla codificazione nella Carta dei diritti fondamentali del diritto alla privacy, sia nella sua connotazione statica (art. 7) che dinamica (art. 8)⁴².

Oltre alla sua proiezione globale attraverso il *Brussels effect*, il GDPR ha rafforzato la *fortezza normativa europea*, proteggendo il paradigma valoriale dell'Unione dall'espansione incontrollata del po-

⁴⁰ C. giust. UE 27 febbraio 2025, *CK contro Magistrat der Stadt Wien, con l'intervento di Dun & Bradstreet Austria GmbH*, causa C-203/22.

⁴¹ Sul punto si pensi alla importante pronuncia C. giust. UE 7 dicembre 2023, *OQ c. Land Hessen con l'intervento di Schufa Holding AG*, causa C-634/21, dove si è affermato che il *credit scoring* (ossia la probabilità relativa alla capacità di onorare impegni di pagamento calcolata in maniera automatica) costituisce un processo decisionale automatizzato relativo alle persone fisiche, allorché venga sfruttato in maniera decisiva da un terzo per assumere determinazioni circa la stipula, l'esecuzione o la cessazione di un rapporto contrattuale. Pertanto, deve trovare applicazione la tutela apprestata dall'art. 22 GDPR.

⁴² O. POLLICINO, M. BASSINI, *Il diritto all'oblio*, in T.E. FROSINI *et al.*, *Internet: libertà e diritti*, Firenze, 2017, 125-140.

tere digitale privato. Questo approccio di “fortificazione” si è esteso a diverse normative settoriali recenti, dalla riforma del copyright alla regolazione dei servizi media audiovisivi e alla legislazione sulla prevenzione del terrorismo.

Questa fase iniziale del *costituzionalismo digitale* ha rappresentato una reazione del legislatore europeo allo “strapotere giurisdizionale” della stagione precedente, ma porta con sé due criticità. La prima è il rischio di frammentazione interna: le molteplici discipline settoriali e le numerose “clausole aperte” nei regolamenti, come nel GDPR e nell’AI Act, concedono agli Stati membri un ampio margine di manovra, trasformando spesso i regolamenti in *direttive mascherate* e impedendo una vera uniformità normativa.

Il secondo rischio è l’isolamento normativo dell’Europa. L’adozione di un quadro regolatorio rigidamente ancorato ai valori europei potrebbe risultare inefficace nel disciplinare un ecosistema digitale per sua natura transnazionale. L’assenza di un *ponte normativo* con altre aree, in particolare con gli Stati Uniti, comprometterebbe l’enforcement delle regole europee e accentuerebbe il divario con l’altra sponda dell’Atlantico.⁴³

Per rispondere a queste sfide, la fase attuale del costituzionalismo digitale europeo sta evolvendo verso un approccio meno assiologico e più procedurale, adottando strumenti normativi trasversali piuttosto che settoriali, con l’obiettivo di ridurre frammentazione e asimmetrie nell’applicazione delle regole. Non si può ignorare che qualsiasi tentativo di proceduralizzazione disconnesso da una base valoriale di riferimento sia destinato a diventare un esercizio sterile di «feticismo procedurale»⁴⁴.

Un esempio può, forse, aiutare a fare emergere il valore aggiunto, almeno potenziale, che i meccanismi di garanzia procedimentale pos-

⁴³ Il quale, talvolta, appare fondarsi anche su equilibri «precari» legati alle diverse interpretazioni sulla portata dei diritti fondamentali online, che permettono la coesistenza di approcci regolatori all’apparenza inconciliabili: M. MONTI, *The Unity of Opposites in the Regulation of Social Media Platforms: Content Moderation Between the EU Digital Services Act and the US First Amendment Theories*, in *EUI LAW Working Paper*, 7, 2024.

⁴⁴ M. ZALNIERUTE, *Technology and the Courts: Artificial Intelligence and Judicial Impartiality*, Rochester, NY, 2021.

sono attribuire al livello di protezione dei diritti fondamentali in gioco. Si pensi al diritto all'oblio, nuovo diritto, o meglio riedizione digitale di un diritto sempre esistito, di creazione giurisprudenziale. La sua elaborazione da parte della Corte di Giustizia, nella sentenza *Google Spain*, già richiamata, ha sicuramente aggiunto un nuovo tassello alla costellazione dei diritti di cui può usufruire l'utente nei confronti delle grandi piattaforme.

Il che, però, non è detto che effettivamente innalzi il livello di protezione dei diritti in gioco, e non solo perché l'inflazione di diritti sostanziali, ormai fin troppo alla moda, guardando al numero delle dichiarazioni dei diritti su Internet⁴⁵, rischia di amplificare la possibilità di collisioni costituzionali e, quindi, di conflitti.

Ma anche perché – ed è questo il punto più rilevante in questa sede – la Corte di Giustizia affida, come già anticipato, a un operatore privato – un motore di ricerca – il compito di operare il bilanciamento tra diritto ad essere dimenticati da una parte e diritto ad essere informati dall'altro, senza adottare alcuna linea guida di carattere procedurale per strutturare il rapporto tra motore di ricerca e utente nelle modalità concrete di esercizio di tale diritto. Senza salvaguardie di carattere procedurale di nessun tipo, è stato lo stesso soggetto privato a decidere quali dovessero essere tali modalità, ovviamente indebolendo, in questo modo, anche sostanzialmente la posizione del singolo. Così come le obbligazioni di carattere procedimentale che non abbiano un *humus* valoriale alle spalle si tramutano in un vuoto esercizio di nomenclatura, anche la previsione di nuovi diritti sostanziali senza le opportune salvaguardie procedimentali rischia di produrre diritti che esistono solo sulla carta.

Nell'ambito della ricerca sui big data e sulle violazioni della privacy (comprese quelle causate dall'uso di algoritmi predittivi), Crawford e Schultz⁴⁶ hanno sottolineato la necessità di inquadrare una forma di «*procedural data due process*». L'applicazione di una tale forma di

⁴⁵ D. REDEKER *et al.*, *Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights*, in *The International Communication Gazette*, fasc. 80, 4, 2018 302–319.

⁴⁶ K. CRAWFORD- J. SCHULTZ, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, in *Boston College Law Review*, fasc. 55, 1, 2014 93.

procedura tecnologica avrebbe anche un impatto sui diritti di natura sostanziale, poiché essa dovrebbe preservare, in conformità con il modello di Redish e Marshal⁴⁷ di giusto processo, valori come l'accuratezza, l'equità, l'uguaglianza di *input*, la prevedibilità, la trasparenza, la razionalità e la partecipazione.

Citron⁴⁸ ha indicato alcuni dei requisiti che i sistemi automatizzati dovrebbero soddisfare per rispettare i requisiti del *due data process*, inclusi, *inter alia*, un adeguato sistema di notifica agli individui interessati delle decisioni assunte e la possibilità per gli individui di essere ascoltati prima che tali decisioni vengano adottate. Secondo Crawford e Schultz⁴⁹, il requisito della notifica, in particolare, può essere soddisfatto fornendo agli individui «un'opportunità di intervenire nel processo predittivo» e di conoscere (cioè di ottenere una spiegazione riguardo) il tipo di previsioni e le fonti dei dati. D'altro canto, il diritto di essere ascoltati è visto come uno strumento per garantire che, una volta divulgati i dati, gli individui abbiano la possibilità di contestare l'equità del meccanismo automatizzato di natura predittiva. Il diritto di essere ascoltati implica, quindi, l'accesso al codice sorgente di un programma per computer o alla logica su cui si basa la decisione di un programma per computer. Infine, questo modello richiede garanzie sull'imparzialità del "giudicante", inclusa la possibilità di impugnare i provvedimenti di quest'ultimo. Come vedremo, il tema dei rimedi effettivi contro una decisione automatizzata e, in generale, quello dell'accesso alla giustizia è uno dei potenziali talloni d'Achille, in una prospettiva costituzionalistica, del più volte citato AI Act, recentemente adottato dall'Unione.

In sintesi, l'enfasi sulla dimensione procedurale, definibile come un'applicazione europea a geometria orizzontale (tra privati) del *due process*, ha il grande vantaggio di poter consolidare un ponte transatlantico nel contesto algoritmico. Questo renderebbe la forza europea meno isolata e più dialogante, evitando l'imperialismo digitale del

⁴⁷ M. H. REDISH- L. C. MARSHALL, *Adjudicatory Independence and the Values of Procedural Due Process*, in *The Yale Law Journal*, fasc. 95, 3, 1986, 455-505.

⁴⁸ D. K. CITRON, *Technological due process*, in *Washington University Law Review*, fasc. 85, 6, 2008 1249.

⁴⁹ CRAWFORD- SCHULTZ, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, cit.

“*Bruxelles effect*”. Tale dimensione, e il principio del *due process* applicato alla sfera digitale, non sono affatto estranei al costituzionalismo statunitense.

6. *Libertà di espressione online, moderazione dei contenuti e algoritmo*

6.1. *Le coordinate costituzionali*

L'evoluzione della moderazione dei contenuti online in Europa richiede un'analisi delle coordinate costituzionali che influenzano la tutela della libertà di espressione, in un confronto inevitabile con il modello statunitense. Le diverse scelte di politica del diritto riflettono approcci valoriali distinti: mentre negli Stati Uniti il Primo Emendamento garantisce alla libertà di espressione una posizione quasi assoluta, in Europa essa è bilanciata con altri diritti fondamentali, come la dignità e la protezione dei dati personali.

La Corte Suprema statunitense, in *Reno v. ACLU*⁵⁰, nella celebre *dissenting opinion* di Justice Holmes in *Abrams*⁵¹, ha fatto utilizzo della metafora del *free marketplace of ideas*, la cui importazione nell'ordinamento europeo è stata la causa principale delle questioni costituzionali sollevate dal consolidamento di nuovi attori privati. Difatti, in Europa, invece, la libertà di espressione non gode di una prevalenza assiologica e si colloca in un equilibrio dinamico con altri diritti, come confermato dall'articolo 10 CEDU, che prevede esplicitamente limitazioni e restrizioni fondate sul principio di responsabilità.

Un altro elemento distintivo del modello europeo è il concetto di abuso del diritto, assente nel diritto costituzionale statunitense, ma previsto sia dalla CEDU che dalla Carta dei diritti fondamentali dell'Unione.⁵² Questo principio rafforza un approccio regolativo che privilegia il bilanciamento tra diritti, favorendo la costruzione di un quadro normativo più articolato.

⁵⁰ *Reno c. Aclu* 521 U.S. 844 (1997), cit.

⁵¹ *Abrams c. United States* 250 U.S. 616 (1919), cit. Si veda, nello specifico, la *dissenting opinion* di Holmes, 624 ss.

⁵² Art. 17 CEDU e art. 54 Carta dei diritti fondamentali dell'Unione europea.

Questa impostazione ha reso possibile l'adozione di interventi legislativi come il GDPR⁵³, la direttiva *Copyright*⁵⁴, e la revisione della Direttiva in tema di servizi media audiovisivi⁵⁵, e, in particolare, il DSA e l'AI Act, su cui sarà rivolta l'attenzione nei prossimi paragrafi, perché costituiscono il regime privilegiato in termini di moderazione dei contenuti.

7. *Dalla Direttiva e-Commerce alla nuova stagione regolativa (DSA) della moderazione dei contenuti in rete*

Nel contesto europeo, alcune delle garanzie procedurali prima evocate sotto il profilo teorico, sono state "codificate" con l'adozione del Digital Services Act (DSA).

Bisogna, però, fare un passo indietro per tentare di fare emergere una cornice unitaria del percorso evolutivo (o involutivo) oggetto di indagine.

La Direttiva *e-Commerce* del 2000⁵⁶ ha introdotto un regime favorevole agli intermediari digitali, esentandoli dalla responsabilità per contenuti illeciti caricati dagli utenti e vietando l'imposizione di obblighi generali di sorveglianza. Questa scelta rispondeva all'esigenza di proteggere sia la libertà d'impresa dei provider (art. 16 CDFUE) sia i diritti fondamentali degli utenti, come privacy e libertà di espressione.

Tuttavia, con il crescente potere degli intermediari e l'ascesa del *fattore algoritmico*, la giurisprudenza e il legislatore europeo hanno progressivamente rivisto questo quadro⁵⁷. Così, con la Direttiva (UE)

⁵³ GDPR, cit.

⁵⁴ Direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale, cit.

⁵⁵ Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato, GU L. 303/2018.

⁵⁶ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico, E-Commerce Directive), GU L. 178/2000.

⁵⁷ E-Commerce Directive, considerando 42.

2018/1808⁵⁸, il legislatore ha modificato la disciplina del mercato audiovisivo, introducendo una serie di obblighi in capo ai fornitori di piattaforme per la condivisione di video. Inoltre, la Direttiva (UE) 2019/790⁵⁹ ha innovato la materia del diritto d'autore per adeguare la normativa di settore alle nuove sfide di internet; mentre, il Regolamento (UE) 2021/784⁶⁰ ha introdotto una specifica disciplina volta al contrasto dei contenuti terroristici online.

Parallelamente, gli algoritmi sono diventati protagonisti della moderazione dei contenuti, sollevando criticità per lo Stato di diritto. La delega all'intelligenza artificiale nel definire i limiti della libertà di espressione crea uno *standard privato di tutela*, riduce la certezza giuridica e rende opachi i confini tra regole pubbliche e private.⁶¹ Questa mancanza di trasparenza e accountability solleva interrogativi sulla legittimità delle restrizioni imposte online, incidendo sull'equilibrio tra innovazione, diritti fondamentali e governance digitale.

Proprio alla luce di tali nuove insidie, nel 2022, con l'approvazione del già menzionato *Digital Services Act*⁶², si è infine provveduto a una riforma generale e, per così dire, "orizzontale" del quadro normativo europeo in materia di moderazione dei contenuti in rete

Tale regolamento è stato proposto e approvato come parte di un "pacchetto" di due atti legislativi dell'Unione europea, comprendente anche il Regolamento sui mercati digitali (*Digital Markets Act*, DMA)⁶³. Obiettivo del pacchetto era quello di riformare nel suo complesso il mercato digitale, combinando insieme, da un lato, novità concernenti gli obblighi dei *provider* alla tutela di un ambiente digitale trasparente e sicuro e, dall'altro lato, nuove regole relative alla promozione della con-

⁵⁸ Direttiva sui servizi di media audiovisivi, cit.

⁵⁹ Direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale, cit.

⁶⁰ Regolamento relativo al contrasto della diffusione di contenuti terroristici online, cit.

⁶¹ O. POLLICINO- G. DE GREGORIO, *Constitutional Law in the Algorithmic Society*, in H.-W. MICKLITZ *et al.*, *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

⁶² 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, DSA), GU L 277/2022.

⁶³ Regolamento sui mercati digitali, cit.

correnza. Come è stato sottolineato fin dagli inizi, scopo ultimo era (ed è) quello di «addomesticare» i giganti del mercato digitale⁶⁴ e, quindi, andare direttamente a intervenire su uno degli aspetti caratterizzanti la società algoritmica.

Il pacchetto DSA/DMA si caratterizza peraltro, come anticipato, per una trazione non (soltanto) assiologico-sostanziale, ma anche per una dimensione intrinsecamente procedurale o procedimentale ed un campo di applicazione “orizzontale”. Si è già anticipato che, in tal senso, il pacchetto costituisce una nuova declinazione del costituzionalismo digitale, una nuova stagione rispetto al paradigma del GDPR, che tenta di risolvere le problematiche in termini di opacità che emergono frequentemente nei meccanismi algoritmici propri dei nuovi poteri, attraverso la predisposizione soprattutto di garanzie procedurali⁶⁵.

Infatti, una delle più grandi novità del DSA è quello di avere introdotto, a fianco del pregresso regime di responsabilità degli intermediari digitali, tutta una serie di nuovi «obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro»⁶⁶.

Il *Digital Services Act* (DSA) introduce un sistema di obblighi *asimmetrico*, differenziando le responsabilità degli intermediari digitali in quattro livelli: obblighi *universali* per tutti i provider, *base* per gli hosting provider, *avanzati* per le piattaforme online e *speciali* per le piattaforme e i motori di ricerca molto grandi (VLOP e VLOSE).

La normativa si sviluppa lungo tre direttrici principali. In primo luogo, rafforza la *trasparenza*, imponendo la pubblicazione di relazioni sulle pratiche di moderazione e obbligando gli hosting provider a motivare le rimozioni di contenuti (artt. 14 e 17).⁶⁷ In secondo luogo, introduce garanzie *procedurali* per gli utenti, tra cui sistemi di gestione dei reclami per le decisioni delle piattaforme. Infine, il DSA incrementa la *responsabilità* degli intermediari, mantenendo il regime di esenzione

⁶⁴ G. WAGNER *et al.*, *Taming the giants: The DMA/DSA package*, in *Common Market Law Review*, fasc. 58, 4, 2021, 987-1028.

⁶⁵ Volendo, ora, O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, 569-594.

⁶⁶ DSA, Capo III.

⁶⁷ DSA, artt. 15, 24, 39.

della Direttiva *e-Commerce*, ma prevedendo sanzioni amministrative per la mancata osservanza delle nuove regole di diligenza⁶⁸.

Un punto chiave riguarda i VLOP e VLOSE, tenuti a identificare e mitigare *rischi sistemici* legati alla diffusione di contenuti illegali, alla tutela dei diritti fondamentali e all'integrità del dibattito democratico (artt. 34-35).⁶⁹ Questa disposizione è centrale nel processo di *costituzionalizzazione* del potere esercitato dai giganti digitali, adeguando il loro impatto alla tutela dei valori democratici e dello Stato di diritto nell'ecosistema algoritmico.

7.1. Segue. L'algoritmo nel DSA

Un aspetto particolarmente significativo del DSA è, peraltro, la rilevanza che esso riconosce al tema dell'algoritmo, dei processi decisionali automatizzati e dell'intelligenza artificiale, nella consapevolezza dell'ormai centrale ruolo ricoperto da tali tecnologie nel contesto della *governance* dei contenuti in rete. Mentre il *GDPR* tutela la dignità dell'individuo nei processi decisionali automatizzati, il DSA si propone di *incanalare* il potere computazionale delle piattaforme digitali, bilanciando l'uso degli algoritmi con i valori democratici dell'Unione.

Un aspetto chiave è il meccanismo di *valutazione e attenuazione dei rischi sistemici* (art. 35), che impone ai provider di adattare i loro sistemi algoritmici per limitare la diffusione di contenuti illeciti senza compromettere i diritti fondamentali. In parallelo, il regolamento introduce *garanzie procedurali*: gli utenti devono essere informati sulle decisioni automatizzate (art. 14), sui tassi di errore degli strumenti di moderazione (art. 15) e devono poter contestare le decisioni con un controllo umano (art. 42)⁷⁰.

Questa regolazione non solo estende al digitale i principi del costituzionalismo europeo, ma struttura una semi-costituzione per la moderazione dei contenuti online, introducendo obblighi di trasparenza, sistemi di reclamo e meccanismi di risoluzione delle controversie extra-giudiziali. Inoltre, il DSA preserva un principio personalistico, richie-

⁶⁸ Ivi, art. 23(1).

⁶⁹ DSA, artt. 15, 24, 39.

⁷⁰ *Ibidem*, art. 17(3)(c).

dedo alle piattaforme di garantire un'interazione umana nei processi decisionali e nei canali di comunicazione con gli utenti.⁷¹

Infine, l'art. 42 impone alle *Very Large Platforms* di dichiarare le risorse umane dedicate alla moderazione, sottolineando una differenza fondamentale tra l'automazione algoritmica e l'autonomia dell'intelligenza artificiale generativa: un tale obbligo non avrebbe senso con riferimento ai servizi offerti dai detti modelli. Qui risiede, difatti, una delle differenze sostanziali tra automazione, che caratterizza la stagione della combinazione tra algoritmo e dati, e autonomia, elemento distintivo di quell'ecosistema digitale – non di una semplice tecnologia, lo si ribadisce – costituito dall'intelligenza artificiale, alla cui analisi saranno dedicati i prossimi paragrafi.

8. *Dall'algoritmo all'intelligenza artificiale: il magistero dell'Artificial Intelligence Act*

Come si è mostrato nelle pagine precedenti, il tema della regolamentazione del ricorso a sistemi decisionali automatizzati e all'algoritmo ha assunto un ruolo progressivamente centrale nel contesto delle politiche dell'Unione europea sin dalla metà degli anni 2010. In tal senso, il GDPR rappresenta il capostipite illustre della strategia euro-unitaria di *governance* di tali sistemi. D'altro canto, gli interventi legislativi posti in essere dall'Unione successivamente denotano una progressiva presa di consapevolezza della vertiginosa crescita e della pervasività della stessa automazione, la quale richiede, in ultima analisi, un ulteriore ripensamento delle strategie legislative.

In effetti, se, come si è detto, il GDPR ha introdotto per primo una fondamentale previsione in tema di soggezione a decisioni prese secondo modalità automatizzate, lo stesso sembra, peraltro, trattare tale fattispecie come un'ipotesi, per così dire, "residuale", a fronte del tradizionale trattamento umano dei dati. Inoltre, come è stato osservato da Giusella Finocchiaro, il GDPR manca di tener conto delle applica-

⁷¹ Si coglie proprio in questo senso la declinazione del *risk-based approach* nel DSA, fondato, come si è detto, su un approccio asimmetrico agli obblighi di diligenza cui i *provider* sono soggetti. V. DE GREGORIO, DUNN, *The European risk-based approach: Connecting constitutional dots in the digital age*, cit.

zioni di intelligenza artificiale fondate sui *big data* e, dunque, manca di considerare il sempre più rilevante fenomeno dei trattamenti di dati di massa⁷².

Del resto, sebbene detto regolamento sia stato approvato nel 2016 e, quindi, in anni relativamente recenti, il panorama si è andato evolvendo in modo significativo. Sotto il profilo dello sviluppo della IA, si potrebbe dire che la società sta andando incontro a un vero e proprio cambiamento di paradigma tecnologico⁷³. In tal senso, Luciano Violante ha osservato come nel mondo contemporaneo convivano tre diversi tipi di società: la società analogica, fondata sul principio di rappresentanza; la società digitale, caratterizzata dalla disintermediazione; infine, la *cybersociety*, che è «frutto della modernizzazione della società digitale, per effetto delle molteplici, interconnesse e alluvionali applicazioni del digitale»⁷⁴.

Le trasformazioni normative più recenti dell'Unione riflettono il passaggio da un approccio incentrato sull'*algoritmo* a una prospettiva sempre più orientata all'intelligenza artificiale. Come si è visto, il *Digital Services Act* (DSA) è un esempio emblematico di questa transizione: riconosce l'inevitabilità dell'automazione nella moderazione dei contenuti e nel trattamento massivo di dati, ma cerca al contempo di incanalare queste tecnologie verso la tutela dei valori costituzionali e democratici dell'Unione.

La distinzione tra automazione algoritmica e intelligenza artificiale

⁷² La logica del GDPR è sempre basata sul dato personale, rispetto al trattamento del quale il singolo individuo esprime una determinazione: l'interessato controlla e, in taluni casi, gestisce il suo dato, seguendone la circolazione. Altre basi giuridiche concorrono a legittimare il trattamento dei dati personali, ma il modello culturale, prima ancora che giuridico, sul quale si basa il Regolamento è quello dell'autodeterminazione. Tale logica, benché mitigata dall'*accountability*, non può essere applicata ai *big data*. Non è possibile pensare a una gestione di tipo individuale dei dati, tanto meno se basata sul consenso. Sembra quasi che si tenti di governare le onde del mare «goccia a goccia», individualmente considerando la goccia. Appare, dunque, necessario ripensare il modello culturale di riferimento. V. G. FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit., 86-87.

⁷³ A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, fasc. 1, 2019, 87-106.

⁷⁴ VIOLANTE, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, cit.

è cruciale per comprendere l'evoluzione normativa. Mentre l'algoritmo esegue istruzioni predefinite in modo meccanico, l'IA, basata su *machine learning* e *deep learning*, elabora autonomamente regole di inferenza, adattandosi ai dati di allenamento.

Occorre, peraltro, chiarire cosa si intende dire attraverso la distinzione tra i due concetti, atteso che la nozione "ampia" di intelligenza artificiale ricomprende certamente la stessa nozione di algoritmo. In questo contesto, il riferimento è a quella distinzione – richiamata anche dal Consiglio di Stato⁷⁵ –, secondo la quale, mentre l'algoritmo si sostanzia in una sequenza di istruzioni ben definite, non ambigue e, dunque, applicate in modo meccanico dalla macchina, l'intelligenza artificiale, fondandosi per lo più su sistemi di *machine learning*, si caratterizza per il fatto di essere in grado di elaborare autonomamente regole di inferenza a partire dai dati usati per l'allenamento⁷⁶. In altre parole, come intuito da Andrea Simoncini, mentre l'automazione algoritmica è utilissima ad accelerare il processo di esecuzione delle decisioni, l'intelligenza artificiale è in grado, grazie alla sua autonomia, di prendere delle decisioni⁷⁷. La definizione che l'AI Act dà di intelligenza artificiale, che sarà esaminata nel paragrafo successivo, sembra confermare le caratteristiche appena evidenziate in quanto si fonda, alla luce del meccanismo di apprendimento automatico, sui concetti di autonomia, adattabilità e capacità di deduzione e predizione.

⁷⁵ Cons. Stato, Sez. III, sentenza del 25 novembre 2020, n. 7891, paragrafo 9.1 in diritto.

⁷⁶ Andrea Simoncini ha fatto emergere chiaramente le caratteristiche peculiari di questo nuovo ecosistema digitale, facendo presente come «*in primis*, i sistemi tecnologici qualificati come 'IA' sono utilizzati per svolgere attività particolari quali: prendere decisioni, realizzare previsioni o raccomandazioni, intraprendere azioni autonomamente, esprimere giudizi o valutazioni. La particolarità sta nel fatto che queste attività sinora erano ritenute facoltà esclusive degli esseri umani (o quantomeno degli esseri viventi). In secondo luogo, questi sistemi di IA 'interagiscono biunivocamente' con l'ambiente sociale in cui sono inseriti, nel duplice senso che, da un lato, le elaborazioni effettuate sono fondate su dati provenienti (anche) dall'ambiente in cui sono inserite; ma, dall'altro, tali sistemi contribuiscono a modificare lo stesso ambiente in cui si trovano e, così, generano nuovi dati da esaminare. L'IA applicata a macchine 'sociali' riceve segnali dall'ambiente ed al tempo stesso invia segnali all'ambiente, modificandolo». Si veda A. SIMONCINI, *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, fasc. 2, 2023, 1–39.

⁷⁷ *Ibidem*.

Questa autonomia decisionale, come evidenziato dall'AI Act, introduce concetti chiave come adattabilità, deduzione e predizione, segnando un mutamento profondo nel modo in cui le macchine interagiscono con il diritto e la società. Se da un lato l'uso di *deep learning* e modelli generativi migliora l'efficienza e la capacità di analisi, dall'altro solleva interrogativi critici sullo *stato di diritto*: trasparenza decisionale, rischio di errore, discriminazione e fenomeni emergenti come i *deepfake*. Questo cambiamento radicale comporta una progressiva *emarginazione del fattore umano*, con implicazioni profonde per le democrazie costituzionali fondate sul *principio personalistico*.

Prima di esaminare il rapporto tra IA e disinformazione, sarà fondamentale analizzare come l'Unione Europea abbia regolato questo mutamento tecnologico, in particolare per quanto riguarda l'IA generativa, e quali strategie normative siano state adottate per preservare i diritti fondamentali in un contesto sempre più dominato dall'automazione.

8. *Il nuovo Regolamento europeo sull'intelligenza artificiale: gli elementi portanti del nuovo sistema di regolazione*

A livello europeo, la risposta a tali mutamenti socio-tecnologici si è avuta con l'adozione del Regolamento sull'intelligenza artificiale⁷⁸. Si tratta del primo caso di regolamentazione organica dell'intelligenza artificiale a livello internazionale e, come tale, ha coagulato intorno a sé un importante dibattito dottrinale, sociale e politico sin dalla presentazione della sua proposta da parte della Commissione⁷⁹.

Il nuovo Regolamento contiene al suo interno una definizione del concetto stesso di intelligenza artificiale, che, essendo stata elaborata

⁷⁸ Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale, cit. Per una disamina del Regolamento, si veda O. POLLICINO *et al.* (a cura di), *La disciplina dell'intelligenza artificiale*, Milano, 2025.

⁷⁹ A fine maggio 2024, peraltro, la Corte dei Conti europea ha rilasciato una relazione contenente un'analisi critica dell'approccio dell'Unione all'IA, sottolineando tra l'altro la necessità di finanziare e incentivare la ricerca in tale settore. V. Corte dei Conti europea, *Le ambizioni dell'UE in materia di intelligenza artificiale. Per il futuro, una governance più forte e investimenti più consistenti e mirati sono essenziali*, 29 maggio 2024, https://www.eca.europa.eu/ECAPublications/SR-2024-08/SR-2024-08_IT.pdf.

nel tentativo di renderla quanto più *future-proof* possibile, sembra tra l'altro riflettere una presa di consapevolezza del summenzionato passaggio dall'"algoritmo" all'"intelligenza artificiale", quale passaggio dall'*automazione* all'*autonomia* in quanto descrive la nozione di sistema di IA «come un sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduca dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»⁸⁰.

La definizione di IA contenuta nel Regolamento riprende quella già elaborata dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD)⁸¹. A differenza dall'approccio "controfattuale" proposto da Floridi,⁸² l'AI Act ne segue uno funzionale, vale a dire che un sistema è considerato IA se è in grado di "inferire" autonomamente – ossia capire – come generare *output* a partire dagli *input* ricevuti, con un certo grado di autonomia e, potenzialmente, di adattabilità.⁸³ Questo criterio consente di comprendere nella definizione un ampio spettro di tecnologie, incluse quelle emergenti, e di non limitare la regolamentazione a specifiche tecniche come il *machine learning* o i sistemi di IA generativa. Tuttavia, proprio questa scelta concettuale solleva alcune criticità interpretative, in particolare ri-

⁸⁰ AI Act, art. 3(1). Interessante notare che nella proposta normativa della Commissione europea, che precede il cataclisma prodotto dall'esplosione dell'AI di tipo generativo, la definizione di intelligenza artificiale faceva ancora riferimento ad una supervisione umana. Riferimento scomparso invece nella definizione presente nel testo finale che ha dovuto essere di fatto parzialmente riscritto, a cominciare dai profili definitori, proprio a causa del cataclisma prima evocato. Per un commento sulla definizione di IA e sulle premesse concettuali dell'AI Act, si veda M. BASSINI, *Oggetto, campo di applicazione e ambito territoriale*, in O. POLLICINO et al. (a cura di), *La disciplina dell'intelligenza artificiale*, cit.

⁸¹ Recentemente aggiornata in OECD, *Explanatory memorandum on the updated OECD definition of an AI system*, OECD Artificial Intelligence Papers, n. 8, OECD Publishing, Parigi, 2024, <https://doi.org/10.1787/623da898-en>, p.7.

⁸² L. FLORIDI, *Present: AI as a New Form of Agency, Not Intelligence*, in L. FLORIDI (a cura di), *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, 2023.

⁸³ *Inter alia*, sulla capacità di inferire, S. LEONELLI, *What distinguishes data from models?*, in *European Journal for Philosophy of Science*, fasc. 9, 2, 2019 22.

spetto alla distinzione tra sistemi di intelligenza artificiale e software tradizionali avanzati⁸⁴.

Come ha avuto modo di chiarare la Commissione Europea nelle Linee Guida che integrano la definizione contenuta nell'Art. 3 comma 1 del Regolamento, di recente pubblicazione,⁸⁵ il regolamento esclude esplicitamente dall'ambito di applicazione i sistemi basati esclusivamente su regole predefinite, ma la linea di demarcazione tra automazione complessa e intelligenza artificiale rimane incerta. Le *Linee Guida* della Commissione Europea chiariscono che i sistemi basati esclusivamente su regole predefinite sono esclusi dall'*AI Act*, ma la distinzione tra automazione complessa e intelligenza artificiale resta incerta. Alcuni strumenti di analisi predittiva avanzata non rientrano nella definizione di IA, mentre i modelli di *machine learning supervisionato* sono considerati regolabili. Questa ambiguità crea difficoltà sia per gli sviluppatori, che operano in un contesto normativo poco chiaro, sia per le autorità di vigilanza, costrette a valutazioni caso per caso.

Un'ulteriore incertezza riguarda la differenza tra *automazione* e *autonomia*: il regolamento enfatizza la capacità dell'IA di operare indipendentemente dall'intervento umano, ma nella pratica il confine non è netto. Alcuni sistemi automatizzati avanzati potrebbero essere regolati come IA, mentre strumenti con effettiva capacità di apprendimento potrebbero sfuggire alla disciplina.

Questa incertezza porta a due rischi opposti: da un lato, la *sovra-regolamentazione* potrebbe ostacolare l'innovazione; dall'altro, la *sotto-regolamentazione* potrebbe favorire strategie elusive, con aziende che classificano i propri prodotti come software tradizionali per evitare gli oneri normativi.

Come si è avuto modo di osservare altrove⁸⁶, l'*AI Act* si caratterizza per l'adozione di un approccio basato su un rischio radicalmente diver-

⁸⁴ S. WACHTER, *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, in *Yale Journal of Law and Technology*, fasc. 26, 3, 2024.

⁸⁵ Commissione Europea, *Approval of the content of the draft Communication from the Commission – Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, Brussels, 6 febbraio 2025.

⁸⁶ DE GREGORIO, DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, cit.

so da quello del GDPR: se quest'ultimo si fondava su una sostanziale delega al titolare del trattamento degli obblighi di valutazione dell'impatto del trattamento stesso sui diritti alla riservatezza e alla protezione dei dati dell'interessato e, di conseguenza, si caratterizzava per un approccio "bottom-up" della regolazione del rischio, il regolamento in questione segue, invece, una prospettiva "top-down", introducendo una categorizzazione dall'alto che rischia di non tenere sufficientemente conto delle dimensioni e delle capacità dei soggetti privati regolati⁸⁷.

L'ormai fin troppo conosciuta classificazione del rischio proposta nell'AI Act presenta una struttura divisa in tre categorie principali (*rectius*, tre più una), a seconda del livello di rischio che ciascuna presenta: 1) rischio inaccettabile; 2) alto rischio e 3) rischio limitato. A tali tre categorie se n'è aggiunta, in seguito alle modifiche introdotte a giugno 2023 dal Parlamento Europeo, nella proposta presentata dalla Commissione Europea, una quarta relativa ai sistemi di GenAI (ossia ai sistemi di intelligenza artificiale a uso generale) che presentino un rischio sistemico per l'Unione Europea, i produttori e distributori dei quali vengono assoggettati ad ulteriori obblighi rispetto a quelli previsti in generale per i sistemi di IA a rischio limitato.

Così, il primo livello è costituito da quei sistemi di IA considerati capaci di impattare così severamente sui diritti individuali da essere proibiti *tout-court*. Divieti che sono, peraltro, entrati in applicazione il 2 febbraio 2025, pur in assenza della nomina delle autorità nazionali che dovranno sorvegliare la corretta applicazione dei divieti previsti dall'Art. 5 del Regolamento⁸⁸. Le pratiche vietate includono, tra l'altro, l'immissione sul mercato o la messa in servizio di determinati sistemi di riconoscimento biometrici, sistemi di *social scoring*, sistemi che utilizzino tecniche subliminali per condizionare le scelte di persone o gruppi di persone con l'effetto o rischio di provocare loro un danno⁸⁹. Non

⁸⁷ G. FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit., 121-122.

⁸⁸ Come per la definizione di IA, la Commissione Europea ha, altresì, adottato linee guida in merito agli usi c.d "proibiti". Cfr. Commissione Europea, *Approval of the content of the draft Communication from the Commission – Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, 4 febbraio 2025.

⁸⁹ AI Act, art. 5.

si tratta di divieti assoluti: sono, infatti, previste delle eccezioni, con un potenziale piuttosto allarmante quanto allo standard di tutela dei diritti fondamentali coinvolti, in particolare con riguardo alle garanzie riservate al contesto e alle modalità con cui tali utilizzi di IA verranno messi in pratica⁹⁰.

Al secondo “livello”⁹¹, l’AI Act classifica come ad alto rischio i sistemi di IA impiegati in settori sensibili, come biometria, infrastrutture critiche, istruzione, occupazione, servizi essenziali, attività di contrasto, gestione delle frontiere e giustizia. Questa categoria è centrale nel regolamento, poiché prevede obblighi stringenti, tra cui una valutazione del rischio ex ante prima dell’immissione sul mercato, per prevenire violazioni dei diritti fondamentali.

L’obiettivo è mitigare i rischi legati a tecnologie con impatti significativi sulla privacy, la protezione dei dati e la non discriminazione, soprattutto in contesti critici come la sorveglianza biometrica⁹², la giustizia e i servizi sanitari. Tuttavia, la regolazione di questi sistemi solleva interrogativi sull’effettiva capacità di bilanciare sicurezza, innovazione e tutela dei diritti umani nel contesto europeo⁹³,

Il terzo livello è rappresentato da alcuni sistemi di IA che presentano un rischio minimo a cui si applicano, in particolare, obblighi di trasparenza meno onerosi rispetto a quanto richiesto per i sistemi c.d. ad alto rischio. È il caso, ad esempio, dei *deep fake* o dei contenuti

⁹⁰ Sulle conseguenze di tale scelta e i rischi per i diritti fondamentali, si veda F. PAOLUCCI, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, SSRN Scholarly Paper, Rochester, 2024.

⁹¹ AI Act, art. 6 e Allegato III.

⁹² Si veda a riguardo F. PAOLUCCI, *Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights*, in *Verfassungsblog*, 2024.

⁹³ Di conseguenza, il Regolamento stabilisce misure obbligatorie per garantire che qualsiasi interferenza con i diritti costituzionali sia giustificata, proporzionata e minimizzata, al fine di evitare collisioni con i livelli di tutela dei diritti fondamentali previsti dal costituzionalismo europeo. L’obiettivo ultimo di tali disposizioni è quello di garantire che l’innovazione tecnologica non avvenga a scapito della sicurezza giuridica e del rispetto delle libertà fondamentali, garantendo un equilibrio tra progresso tecnologico e protezione dei diritti. In merito alla (finta) alternativa tra innovazione e tutela dei diritti, si faccia riferimento a A. BRADFORD, *The False Choice Between Digital Regulation and Innovation*, SSRN Scholarly Paper, Rochester, 2024.

generati da *chatbots*, che presentano un rischio di personificazione e di conseguente confusione tra umano e IA.

Infine, ultimo, ma non meno importante, è il quarto livello che, essendo composto da filtri IA di raccomandazione di contenuti⁹⁴ e da filtri *spam* impiegati nella gestione della posta elettronica, si caratterizza per l'assenza di una specifica regolazione a riguardo.

L'AI Act si concentra sugli obblighi di trasparenza per i sistemi a rischio limitato, ma non chiarisce come garantire una reale *accountability* nella loro integrazione nei processi democratici. Un caso emblematico è quello dei *deepfake*, spesso usati per amplificare discriminazioni di genere, in particolare contro le donne. Nonostante il loro potenziale dannoso⁹⁵, il regolamento li classifica come a basso rischio, imponendo solo l'obbligo di etichettarli come tali – un requisito facilmente aggirabile da chi intende manipolare la realtà⁹⁶.

Inoltre, manca una chiara attribuzione di responsabilità per l'uso dell'IA in campagne elettorali o nella gestione dei dati personali per fini politici. Senza un quadro normativo più solido, l'IA rischia di diventare un agente opaco, influenzando processi decisionali senza trasparenza né controllo effettivo, con possibili conseguenze sulla fiducia nei sistemi democratici.⁹⁷

8.2. L'esplosione dell'intelligenza generativa ed i nuovi rischi per stato di diritto e democrazia: alcune definizioni di base

Un discorso a parte meritano poi i cosiddetti modelli di IA per finalità generativa (*general purpose AI*, GPAI)⁹⁸, comunemente noti anche

⁹⁴ Quelli che, per intenderci, sono utilizzati dalle piattaforme per scegliere i contenuti che vengono mostrati agli utenti. Si consenta il riferimento a O. POLLICINO- P. DUNN, *Intelligenza Artificiale e Disinformazione*, Milano, 2024.

⁹⁵ F. ROMERO MORENO, *Generative AI and deepfakes: a human rights approach to tackling harmful content*, in *International Review of Law, Computers & Technology*, 2024, 1-30.

⁹⁶ AI Act, art. 50(4).

⁹⁷ Di recente notizia è stata la scelta della Commissione Europea di ritirare la proposta di Direttiva sulla "*liability*", ovvero sulla responsabilità civile per i danni dell'IA, aprendo ancora una volta a importanti incertezze applicative.

⁹⁸ «The term *foundation model* was introduced by the Stanford Institute for Human Centered Artificial Intelligence in August 2021. That concept refers to a new machine learning paradigm in which one large model is pre-trained on a huge amount of data

come “modelli fondativi” (*foundation models*), la cui disciplina è stata, infine, introdotta nel Regolamento, a seguito di un travagliato dibattito istituzionale e anche ad uno stallo del processo legislativo avutosi nella primavera del 2022, quando è esploso il caso ChatGPT e con esso la questione relativa a come regolamentare la c.d. intelligenza generativa, su cui si tornerà tra un momento⁹⁹.

I modelli fondativi si caratterizzano per il fatto di essere in grado di assolvere a una pluralità di compiti di carattere, per l'appunto, generale, così da trovare potenziale applicazione in una molteplicità di contesti e situazioni differenti, secondo l'uso che se ne intenda fare. In altre parole, i modelli fondativi servono precisamente quale fondamento per il successivo sviluppo di applicativi di IA dediti a finalità più specifiche.

La portata generale di tali sistemi e, pertanto, l'impossibilità di determinare aprioristicamente quale sarà l'uso che ne sarà fatto, nonché quali effetti (positivi e/o negativi) ne potranno derivare, costituiscono una sfida assai significativa a livello regolatorio¹⁰⁰, a causa delle implicite difficoltà connesse al necessario temperamento tra i bisogni dello sviluppo tecnico e scientifico, oltre che del mercato, e quelli legati alla tutela di diritti fondamentali, degli interessi pubblici e dei valori costituzionali e democratici¹⁰¹. La difficoltà inerente alla regolazione dell'IA generativa si situa, dunque, nella sua versatilità e, a tratti, nella sua imprevedibilità, che lascia lo spazio a un vastissimo *carney* di potenziale, ma apre anche a rischi rispetto alla sua «messa a terra» in settori che hanno strettamente a che vedere con la tutela dei diritti fondamentali¹⁰².

(*broad data at scale*) and can be used for many downstream tasks and applications» (R. BOMMASANI *et al.*, *On the Opportunities and Risks of Foundation Models*, arXiv, 2022.)

⁹⁹ Vale la pena rammentare in questa sede la controversa sanzione dell'Autorità Garante per la Protezione dei Dati Personali italiana comminata nei confronti di OpenAI, e, successivamente, revocata e graduata. Si veda il provvedimento del 30 marzo 2023, n. 9870832, e successive modifiche.

¹⁰⁰ BOMMASANI *et al.*, *On the Opportunities and Risks of Foundation Models*, cit.

¹⁰¹ F. DONATI, *Intelligenza artificiale e diritti fondamentali nel regolamento sull'intelligenza artificiale*, in O. POLLICINO *et al.* (a cura di), *Il Regolamento europeo sull'intelligenza artificiale*, cit.

¹⁰² Esemplicativo della portata orizzontale delle problematiche individuate è la tutela del diritto d'autore, come bene evidenziano C. GEIGER-V. IAIA, in *Generative AI, Digital Constitutionalism and Copyright: Towards a Statutory Remuneration Right*

Il legislatore euro-unitario ha conseguentemente optato per l'inserimento, all'interno dell'AI Act, di un'apposita disciplina costruita su due livelli di rischio. Il primo livello concerne tutti i sistemi fondati su modelli di GPAI. Il secondo livello, invece, è relativo a quei modelli di GPAI che presentino "rischi sistemici" a livello dell'Unione¹⁰³, in quanto abbiano portata significativa all'interno dell'Unione stessa o implicino «effetti negativi effettivi e ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso»¹⁰⁴. Sono tali, in particolare, quei modelli che presentino "capacità di impatto elevato", ovvero sia «capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati»¹⁰⁵, da valutarsi «sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento»¹⁰⁶, fatta salva la possibilità per la Commissione di rendere decisioni (*ex officio* oppure a seguito di segnalazione qualificata del gruppo di esperti scientifici) con le quali vengano riconosciute simili capacità o impatto in altri modelli di GPAI¹⁰⁷.

Il rapporto tra i *modelli fondativi* e l'IA generativa è strettamente legato alle tensioni tra innovazione tecnologica e tutela dei diritti fondamentali nel contesto del costituzionalismo europeo. Questi modelli, grazie alla loro capacità di produrre grandi quantità di output testuali,

Grounded in Fundamental Rights, in *MediaLaws*, 2023, <https://www.medialaws.eu/generative-ai-digital-constitutionalism-and-copyright-towards-a-statutory-remuneration-right-grounded-in-fundamental-rights/>.

¹⁰³ La nozione di rischio sistemico, come definita dall'AI Act all'Art. 3(1)(65), è legata all'individuazione di rischi associati ai modelli di intelligenza artificiale di tipo generativo, che comprendono la possibilità di effetti negativi rilevanti su settori critici come la salute pubblica, la sicurezza democratica e l'integrità delle infrastrutture. Il Cons. 110 evidenzia, altresì, che detti rischi possono verificarsi durante tutto il ciclo di vita del modello e possono essere amplificati dalle capacità del modello, dalla sua autonomia e dal suo eventuale utilizzo improprio. Inoltre, i rischi possono derivare da vulnerabilità, come la diffusione di contenuti falsi o discriminatori, l'uso di capacità cibernetiche offensive o la manipolazione di infrastrutture critiche.

¹⁰⁴ *Ibidem*.

¹⁰⁵ AI Act, art. 3(64).

¹⁰⁶ Ivi, art. 51(1)(a).

¹⁰⁷ Ivi, art. 51(1)(b). Su questo tema, S. WACHTER, *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, cit.

visivi o multimodali, rappresentano strumenti estremamente potenti per la generazione di contenuti. Come ha notato Dunn¹⁰⁸, l'IA generativa, caratterizzandosi precisamente per la sua capacità di produrre contenuti a partire da *input* esterni (solitamente testi scritti dall'utilizzatore), esiste in realtà già da tempo: le cosiddette «reti generative avversarie» (*generative adversarial networks*, GAN) sono state largamente utilizzate sin dal 2014 per creare contenuti, ivi inclusi, per esempio, i «filtri» di Instagram¹⁰⁹.

Tuttavia, al di là della classificazione per livelli di rischio e degli obblighi di trasparenza previsti dall'*AI Act*, resta aperta una questione più ampia: *come e da chi viene deciso l'inserimento di questi sistemi nei processi democratici?*¹¹⁰. L'integrazione dell'IA generativa nel dibattito politico, nell'informazione e nella formazione del consenso solleva interrogativi profondi sulla manipolazione dell'opinione pubblica e sull'impatto delle tecnologie predittive nei processi elettorali.

All'osservatore che sia cultore del diritto costituzionale può porsi, inoltre, un'ulteriore domanda, di per sé separata ma connessa a questi interrogativi e funzionale indirettamente anche alla loro soluzione: qual è lo statuto giuridico di questi contenuti? Come evidenziato da Bassini in un recente contributo¹¹¹, si tratta di stabilire se le creazioni di questi sistemi di intelligenza artificiale possano aspirare a una tutela costitu-

¹⁰⁸ DUNN, in POLLICINO-DUNN, *Intelligenza Artificiale e Disinformazione*, cit.

¹⁰⁹ Le GAN si caratterizzano per la cooperazione di due reti neurali, che vengono poste l'una contro l'altra. La prima rete neurale ha la funzione di produrre contenuti (per esempio immagini), mentre la seconda assolve al compito di determinare se i contenuti che le sono proposti sono reali oppure no. In tal modo, le due reti neurali si forniscono reciproci *feedback*, creando un circolo virtuoso attraverso il quale entrambe sono in grado di migliorare le proprie *performance*. Vedi Cambridge Consultants, *Use of AI in online content moderation*, 2019, 1–84, spec. p. 22; E. JONES, *Explainer: What Is a Foundation Model?*, in *Ada Lovelace Institute*, 17 July 2023, <https://www.adalovelaceinstitute.org/resource/foundation-models-explainer/>.

¹¹⁰ Come osserva il Report pubblicato dall'Ufficio dell'Alto Commissario per le Nazioni Unite (OHCHR), «*the proliferation of inaccurate internet content created with generative AI tools—whether disinformation or misinformation—may drown out or obscure evidence-based and fact-checked information online, broadly threatening individuals' and communities' right to access information*». OHCHR, «*Taxonomy of Human Rights Risks Connected to Generative AI*», United Nations Human Rights, 2024.

¹¹¹ M. BASSINI, *Speech without a speaker: a constitutional coverage for generative AI output?*, in corso di pubblicazione, 2025.

zionale come manifestazioni di pensiero; ciò non tanto per tutelare un “parlante” in questo caso assente (a meno di voler ricercare a ogni costo un agente umano cui imputare gli *output*), quanto per preservare la generazione di questi artefatti digitali da possibili interferenze dei legislatori destinate a tradursi in limitazioni contenutistiche, e cioè relative a quanto essi possono “dire” e “non dire”. Al tema, peraltro, è collegata l'ulteriore domanda sulla responsabilità degli sviluppatori o utilizzatori di questi sistemi rispetto alla moderazione dei contenuti generati artificialmente¹¹²: è ipotizzabile, per esempio, l'applicazione a questi operatori delle norme introdotte dal DSA per le piattaforme online o i motori di ricerca di grandi dimensioni? Regole che non soltanto dettano particolari meccanismi di responsabilità ma che, a ben vedere, estendono altresì misure di mitigazione del rischio a questi soggetti in virtù del loro impatto sulla sfera pubblica.

L'*AI Act*, pur regolando alcuni aspetti della trasparenza e del rischio sistemico, non affronta in modo esaustivo i meccanismi di controllo necessari per garantire un uso etico e trasparente di questi strumenti, né si diffonde sullo statuto giuridico dei contenuti artificialmente generati. Il rischio è che l'uso massiccio dell'IA generativa possa erodere la fiducia nei processi democratici, rendendo urgente una riflessione più ampia su come bilanciare innovazione e salvaguardia dei principi democratici. Questo sarà l'oggetto dell'analisi nel prossimo paragrafo.

8.3. *L'AI Act allo specchio: supera il test del costituzionalismo europeo?*

Le premesse su cui poggia l'Act erano portatrici di soluzioni volte a ridurre l'asimmetria regolativa che caratterizza l'industria del digitale rispetto ad altri settori. A differenza di prodotti regolati con autorizzazioni preventive e test di sicurezza – come nel settore automobilistico – l'IA è stata lanciata senza obblighi simili, come dimostra il caso di OpenAI nel 2023. Quando la Commissione ha proposto il regolamento nel 2021, l'obiettivo principale era garantire la sicurezza del prodotto nel mercato unico, basandosi sull'art. 114 TFUE, come si diceva. Tuttavia, l'approccio iniziale si è rivelato riduttivo: mancava una visione

¹¹² *Ibidem.*

sistemica della tutela dei diritti fondamentali, lacuna che il Parlamento europeo ha cercato di colmare in fase di revisione.

Questo peccato originale ha portato a un testo che cerca di conciliare sicurezza e innovazione con il rispetto dei diritti umani, ma risulta un compromesso tra esigenze di mercato e stato di diritto, nonché tra governi nazionali e Parlamento europeo. Di conseguenza, emergono due livelli di frammentazione.

Il primo riguarda l'applicazione del regolamento a livello nazionale: come accaduto con il GDPR, l'ampiezza delle clausole potrebbe tradursi in 27 interpretazioni diverse, generando divergenze tra gli Stati membri.¹¹³ Il secondo deriva dalla vaghezza di concetti chiave, come la valutazione del rischio sistemico nella valutazione d'impatto sui diritti fondamentali. L'assenza di definizioni precise ha richiesto l'adozione di linee guida successive, creando incertezza normativa. Emblematico è il caso delle linee guida sugli usi proibiti, pubblicate dopo l'entrata in vigore delle disposizioni corrispondenti, aumentando il rischio di applicazioni incoerenti – con conseguenti, eventuali e futuri, interventi giurisprudenziali frammentati da parte della Corte di Giustizia e dei giudici nazionali.

Sempre guardando al test del costituzionalismo europeo, una delle più significative criticità dell'AI Act è la deliberata esclusione delle applicazioni militari e delle tecnologie di intelligenza artificiale utilizzate per scopi non professionali¹¹⁴. Questo vuoto normativo è particolarmente preoccupante, poiché lascia ampi settori di applicazione dell'IA senza un'adeguata regolamentazione, esponendoli a potenziali abusi anche di potere, rafforzando i pochi Stati Membri che possono svi-

¹¹³ Art. 5 par. 3. A questo proposito va detto che l'AI Act – che rischia di tramutarsi in una direttiva mascherata, come in parte è stato per il GDPR, in ragione dell'altissimo numero di clausole aperte che attribuiscono un significativo margine di manovra agli Stati – lascia a questi ultimi anche la scelta circa l'autorità, amministrativa o giurisdizionale, cui demandare l'autorizzazione del riconoscimento biometrico. Cfr. F. Paolucci, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, cit.

¹¹⁴ Art. 2 del Regolamento. Il tema dell'esclusione della regolazione di detto settore e le criticità connesse a tale scelta sono state anche messe in evidenza da M. Draghi, in M. DRAGHI, *The future of European competitiveness, European Commission*, 2024, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en.

luppate tecnologie di IA nel settore bellico, paradossalmente proprio in un periodo in cui il settore in questione dovrebbe essere quello tra i più armonizzati, a causa della persistente aggressione russa in Ucraina e delle implicazioni belliche che ne derivano. Si aggiunga che la mancanza di supervisione in questo ambito contrasta con l'approccio rigoroso adottato per le applicazioni civili, creando un pericoloso doppio standard¹¹⁵.

Addentrandoci nel cuore del Regolamento, uno degli aspetti più controversi è senz'altro il già accennato affidamento all'autovalutazione da parte dei *deployer* di IA. Il regolamento impone ai *deployer* di condurre valutazioni dei rischi sui propri sistemi, sollevando preoccupazioni riguardo a potenziali conflitti di interesse¹¹⁶. L'autovalutazione, senza un'adeguata supervisione indipendente, potrebbe portare a una sottostima dei rischi, riducendo l'efficacia delle misure di tutela¹¹⁷. Questo aspetto è critico specie per i sistemi di IA ad alto rischio, dove l'*enforcement* dovrà giocare un ruolo rilevante per portare ad arginare gravi conseguenze per i diritti fondamentali degli utenti. L'assenza di *auditor* indipendenti o di organismi di verifica obbligatori per i sistemi di IA ad alto rischio mina la credibilità delle salvaguardie previste. Anche se il regolamento prevede misure dettagliate per la gestione dei rischi, queste possono risultare inefficaci se non supportate da un controllo adeguato e indipendente¹¹⁸. La creazione di un quadro normativo che si basa principalmente, e quasi paradossalmente, sull'autoregolamentazione riduce la capacità dell'UE di garantire che i sistemi di IA operino in conformità con i più alti standard di sicurezza ed etica e

¹¹⁵ F. PALMIOTTO, *The AI Act Roller Coaster: How Fundamental Rights Protection Evolved in the EU Legislative Process*, Rochester, 2024.

¹¹⁶ È il caso sopra menzionato della valutazione concessa al *deployer* relativa all'assenza di «alto rischio» di un sistema di IA.

¹¹⁷ Sul punto, estensivamente, WACHTER, *Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond*, cit.

¹¹⁸ Molto complesso è il quadro della *governance* dell'AI Act che, a differenza di DSA e di DMA, oltre al naturale accentramento nella Commissione, prevede la nazionalizzazione di alcune misure di *enforcement* che danno molte responsabilità agli Stati Membri nell'individuazione delle Autorità che giocheranno un ruolo essenziale per l'applicazione del Regolamento.

ripropone, ancora una volta, vecchi meccanismi, che sembrano appartenere a un'altra epoca della regolazione digitale.

Un esempio di questo problema si trova nell'uso della Fundamental Rights Impact Assessment (FRIA)¹¹⁹. Secondo l'AI Act, il FRIA è uno strumento chiave per valutare l'impatto dei sistemi di IA ad alto rischio sui diritti fondamentali¹²⁰. Tuttavia, nonostante l'ambizione di tutelare i diritti fondamentali, il FRIA si basa su una metodologia di autovalutazione. Gli attori pubblici e privati incaricati dell'implementazione dei sistemi di IA sono tenuti a condurre questa valutazione e a segnalare i rischi individuati alle autorità di vigilanza del mercato, ma senza che sia previsto un intervento esterno obbligatorio, salva la comunicazione che il *deployer* deve effettuare all'Autorità di Sorveglianza del Mercato¹²¹.

Il FRIA, che dovrebbe identificare e mitigare i rischi per i diritti fondamentali, soffre di carenze strutturali simili ad altre valutazioni dell'impatto, come il Data Protection Impact Assessment (DPIA) previsto dal GDPR e le valutazioni del rischio nel Digital Services Act (DSA)¹²². Senza un adeguato livello di *enforcement* e armonizzazione, il rischio è che queste valutazioni diventino meri esercizi burocratici, che duplicano i controlli che le aziende sono tenute a fare¹²³, senza una reale considerazione dei rischi complessi e in evoluzione posti dai sistemi autonomi di IA. Inoltre, il FRIA deve affrontare le sfide legate all'autonomia dei sistemi di IA. La natura autonoma e auto-apprendente delle IA, specie quelle generative, rende difficile per gli implementatori anticipare tutti i rischi potenziali e adattare le salvaguardie in modo adeguato. Questa mancanza di supervisione esterna obbligatoria aumenta il rischio che i diritti fondamentali non siano adeguatamente

¹¹⁹ AI Act, art. 27.

¹²⁰ G. DE GREGORIO *et al.*, *Compliance through Assessing Fundamental Rights: Insights at the Intersections of the European AI Act and the Corporate Sustainability Due Diligence Directive*, *MediaLaws*, 2024, <https://www.medialaws.eu/compliance-through-assessing-fundamental-rights-insights-at-the-intersections-of-the-european-ai-act-and-the-corporate-sustainability-due-diligence-directive/>.

¹²¹ AI Act, art. 27(3).

¹²² P. CHIARA- F. GALLI, *Normative Considerations on Impact Assessments in EU Digital Policy*, in *MediaLaws*, 1, 2024.

¹²³ Sul rischio di replica tra FRIA e DPIA in capo al *deployer*, PAOLUCCI, *Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights*, cit.

protetti, soprattutto in settori ad alto rischio come la sanità, la giustizia e la sorveglianza biometrica.

Più in generale, su questo punto, è proprio con particolare riferimento alla questione dell'accesso alla giustizia e all'esigenza di rimedi giurisdizionali effettivi (di fatto, la triangolazione tra art. 47 della Carta e articoli 2 e 19 TFEU su cui la giurisprudenza della Corte di giustizia sta fondando la sua giurisprudenza più recente sulla tutela dello stato di diritto¹²⁴) che sembrano emergere i profili più delicati dell'AI Act. Quest'ultimo, infatti, non offre meccanismi di accesso ai rimedi adeguati alle persone impattate dalle decisioni automatizzate prese dai sistemi di IA. Sebbene sia introdotto un diritto a una spiegazione delle decisioni basate su IA¹²⁵, questa spiegazione risulta spesso superficiale, mancando della trasparenza necessaria per consentire agli individui di contestare efficacemente tali decisioni. Come è stato evidenziato¹²⁶, l'accesso a rimedi legali efficaci e a una giustizia sostanziale è un aspetto centrale per garantire la tutela dei diritti fondamentali nell'era digitale. Tuttavia, la promessa del diritto a una "spiegazione significativa" delle decisioni prese dai sistemi di IA, benché innovativa, risulta inefficace senza un accesso reale e concreto a procedure di giustizia che permettano alle persone di contestare le decisioni e di ottenere un risarcimento adeguato¹²⁷. Senza la possibilità di un *due process* chiaro e ben delineato, si rischia di creare una situazione in cui le decisioni algoritmiche operano in una sorta di vuoto giuridico, con le persone che subiscono danni senza possibilità di ricorrere a strumenti di tutela *ad hoc*, che possano rendere l'accesso

¹²⁴ C. giust. UE 27 febbraio 2018, *Associação Sindical dos Juizes Portugueses c. Tribunal de Contas*, causa C-64/16. Più di recente, C. giust. UE 16 febbraio 2022, *Ungheria c. Parlamento e Consiglio*, causa C-156/21, e C. giust. UE 16 febbraio 2022, *Polonia c. Parlamento e Consiglio*, C-157/21. Per analizzare i recenti sviluppi, si veda C. giust. UE 26 aprile 2024, *Parlamento europeo c. Commissione europea*, causa C-225/24.

¹²⁵ AI Act, art. 86.

¹²⁶ G. DE GREGORIO- S. DEMKOVA, *The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe*, 2024.

¹²⁷ Sulle criticità già contenute nell'art. 22 del GDPR, che conteneva un simile e molto discusso diritto alla spiegazione, F. PALMIOTTO, *When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis*, in *German Law Journal*, fasc. 25, 2, 2024, 210-236.

alla giustizia più efficace: promessa che dovrebbe essere mantenuta in forza dell'Art. 47 della Carta¹²⁸.

L'AI Act, infatti, introduce importanti obblighi di trasparenza, ma non fornisce garanzie sufficienti per quanto riguarda la responsabilità legale dei fornitori di IA o dei soggetti che utilizzano tali sistemi in contesti critici, come la giustizia, la salute o la pubblica amministrazione. Attualmente, l'AI Act non stabilisce con sufficiente chiarezza chi debba essere ritenuto responsabile nei casi in cui un sistema di IA prenda una decisione che viola i diritti fondamentali di un individuo. Ad esempio, nei casi di discriminazione legata a sistemi di selezione automatizzata del personale o di concessione di crediti, è cruciale che vi sia un soggetto responsabile identificabile, che possa essere chiamato a rispondere delle conseguenze di tali decisioni¹²⁹.

Un elemento chiave, pertanto, sarà la futura evoluzione dell'AI Act per includere non solo obblighi di trasparenza, ma anche norme più solide che garantiscano l'accesso alla giustizia e un reale *due process* per coloro che subiscono decisioni negative da parte dei sistemi di IA. Se queste problematiche non verranno risolte, l'AI Act rischia di non raggiungere i suoi ambiziosi obiettivi di protezione dei diritti fondamentali e di *governance* etica dell'intelligenza artificiale, e, addirittura, di rappresentare un passo indietro rispetto ad altri regolamenti dedicati alla regolazione dello spazio digitale, come il DSA¹³⁰. Paradossalmente, si creerebbe uno scenario normativo in cui, in risposta ad una sfida di matrice tecnologica più complessa – autonomia e non solo automazione, nei termini che si sono più volte richiamati –, ci sarebbe una reazione legislativa meno garantista nella stagione dell'autonomia

¹²⁸ F. PAOLUCCI, *Due process of Artificial Intelligence: a challenge for the protection of fundamental rights*, in G. Campus, et al. (ed.) *Digital Single Market and Artificial Intelligence*, Roma, 2024, 499-513.

¹²⁹ Questa è la reale sfida che il legislatore europeo dovrà affrontare: «*the establishment of a new general model for liability for losses caused by artificial intelligence applications that goes beyond the minimum harmonisation approach embraced in the proposal for a regulation and the proposal for a directive*», in G. FINOCCHIARO, *The regulation of artificial intelligence*, in *AI & SOCIETY*, 2023.

¹³⁰ Per un'attenta analisi di questo tema, si può fare riferimento alle considerazioni presenti in O. POLLICINO, F. PAOLUCCI, *AI Act e diritti fondamentali*, in *Civiltà della Macchine*, fasc. 2, 2024, 53-57.

di quella che ha caratterizzato la reazione alla stagione dell'automazione (algoritmica).

9. *Riflessioni conclusive: quale futuro per il modello di regolazione del digitale in Europa?*

Le mosse dell'Unione sembrano definire nuovi scenari nelle risposte alle sfide poste dal digitale. Come già sottolineato, piuttosto che ricorrere a un esercizio di autoregolamentazione guidata da un neoliberalismo digitale, da misure illiberali o da un approccio focalizzato sulla definizione di regole tecniche che riflettano regole costituzionali¹³¹, la strategia europea ha messo in luce la necessità di bilanciare, da un lato, il rispetto dei diritti in una società democratica e, dall'altro, di assicurare che il mercato europeo possa adattarsi alle trasformazioni globali nel settore digitale e competere in questo ambito. Questo approccio di rottura, che ha portato a una nuova stagione per il costituzionalismo digitale europeo, non definisce un semplice passaggio da una fase di *self-regulation* a una di *hard regulation*, ma piuttosto contribuisce a riconoscere il ruolo di meccanismi che possano assicurare maggiore collaborazione come rappresentato dall'espansione della regolazione del rischio e dei processi di *co-regulation*¹³².

L'approccio basato sul rischio, infatti, permette di porre al centro non tanto regole rigide quanto obblighi di identificazione, valutazione e gestione dei rischi specifici¹³³. Questo modello si sta affermando come un'alternativa più flessibile e adattabile rispetto alle tradizionali forme di regolamentazione, in quanto consente ai regolatori di concentrare risorse e attenzioni sulle aree di maggiore criticità, riducendo al contempo il carico normativo nelle situazioni meno rischiose. Se il GDPR aveva già contribuito a spostare il focus dell'Unione verso

¹³¹ PEREZ-WIMER, *Algorithmic Constitutionalism*, cit.

¹³² R. GELLERT, *The risk-based approach to data protection*, Oxford, 2020; Z. EFRONI, *The Digital Services Act: risk-based regulation of online platforms*, *Internet Policy Review*, 2021, <https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606>.

¹³³ J. BLACK, R. BALDWIN, *When risk-based regulation aims low: Approaches and challenges*, in *Regulation & Governance*, fasc. 6, 1, 2012, 2–22.

una regolamentazione del rischio, il Digital Services Act, piuttosto che imporre esclusivamente obblighi e garanzie procedurali, ha rafforzato tale approccio, rendendo maggiormente responsabili le *very large online platforms*, tramite obblighi di valutazione del rischio e conseguenti misure di attenuazione e mantenendo, al contempo, il controllo sulla valutazione di tali misure¹³⁴. Seppur in modo diverso, anche l'AI Act si colloca in un tale quadro di maggior responsabilizzazione, considerando il ruolo delle piattaforme digitali quali fornitori e utilizzatori di sistemi di IA, come nel caso dei *deep fake*.

Similmente, l'Unione sembra essersi concentrata sulla costruzione di un approccio collaborativo in cui attori pubblici e privati lavorano insieme per sviluppare e implementare norme e politiche. Come osservato, «la premessa da cui deriva l'idea della co-regolazione è che la tecnologia digitale sia caratterizzata da un *mix* tale di complessità specialistica e rapidità evolutiva che in molti casi solo i destinatari stessi delle norme sono in possesso delle conoscenze necessarie a svolgere il compito normativo»¹³⁵.

L'emergente modello di regolamentazione dell'Unione, come sottolineato dal GDPR, dal Digital Services Act e dall'Artificial Intelligence Act, evidenzia il ruolo dei codici di condotta nella definizione di un sistema di dialogo tra attori pubblici e privati¹³⁶, tendendo quindi a superare i limiti di un approccio di *enforcement* di natura principalmente verticale, che ha già dimostrato i suoi limiti, tanto da richiedere nuove regole al fine di affrontare le sfide poste dal digitale. Nel caso del Digital Services Act, la co-regolamentazione si concretizza principalmente attraverso codici di condotta volontari, che consentono alle piattaforme di lavorare con le istituzioni europee per sviluppare misure personalizzate in base ai rischi specifici che affrontano. Questi codici non sono semplici linee guida, ma strumenti flessibili che possono rendere maggiormente specifici obblighi generali e più prevedibili le

¹³⁴ EFRONI, *The Digital Services Act: risk-based regulation of online platforms*, cit.

¹³⁵ SIMONCINI, *La co-regolazione delle piattaforme digitali*, cit. Sul tema si veda inoltre, G. MOBILIO, *La co-regolazione delle nuove tecnologie, tra rischi e tutela dei diritti fondamentali*, in *Osservatorio sulle fonti*, fasc. 1, 2024.

¹³⁶ N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, in *Osservatorio sulle fonti*, fasc. 3, 2022, 55-91.

conseguenze di potenziali violazioni. Non è un caso, infatti, che il DSA valuti negativamente la decisione delle piattaforme di non prender parte a tali esercizi di co-regolamentazione, che, seppur volontari, rappresentano degli elementi centrali del paradigma europeo di regolamentazione del digitale.

Il caso delle politiche sulla disinformazione costituisce un esempio paradigmatico¹³⁷. Concentrandosi qui sulle questioni relative alla co-regolamentazione, il codice di buone pratiche rafforzato sulla disinformazione rappresenta un tentativo di mediazione tra istanze neoliberali e illiberali¹³⁸. Il DSA svolge un importante ruolo anche in questo caso sottolineando la natura ancora volontaria dei codici di condotta, ma riconoscendo il ruolo della co-regolamentazione come misura di mitigazione per contrastare i contenuti considerati dannosi ma non di per sé illegittimi (*harmful but non illegal*) come nel caso della disinformazione. In questo caso, i codici di condotta mirano a svolgere un ruolo importante nella lotta contro l'amplificazione delle notizie false e possono essere considerati un'adeguata misura di mitigazione del rischio da parte delle piattaforme online di dimensioni molto grandi¹³⁹.

In questo contesto, come stabilito dal DSA, la Commissione e il Comitato europeo per i servizi digitali hanno il ruolo di incoraggiare e facilitare l'elaborazione di codici di condotta volontari, tenendo conto in particolare delle sfide specifiche legate alla lotta contro i diversi tipi di contenuti illegali e i rischi sistemici¹⁴⁰. Tali codici possono svolgere un ruolo fondamentale non solo nel dettagliare meglio gli obblighi derivanti dal DSA, ma dovrebbero anche essere considerati come misure di attenuazione del rischio, attuate dalle piattaforme digitali designate come *very large* per affrontare i rischi sistemici, compresa la disinformazione. Di conseguenza, i codici di condotta non sono solo strumenti di autoregolamentazione, ma piuttosto strumenti di co-regolamentazione che trovano la loro base nell'accordo volontario tra attori pubblici e privati, ma anche in una normativa. Come sottolineato dal DSA Act,

¹³⁷ O. POLLICINO, DUNN, *Intelligenza Artificiale e Disinformazione*, cit.

¹³⁸ C.T. MARSDEN, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge, 2011.

¹³⁹ DSA, Considerando 104.

¹⁴⁰ Ivi, art. 45(1).

il rifiuto di partecipare a tale processo senza adeguate spiegazioni da parte delle piattaforme può essere preso in considerazione dalla Commissione nel valutare se queste abbiano violato gli obblighi introdotti dal DSA¹⁴¹. Anche se la partecipazione al Codice non garantisce in automatico il rispetto delle garanzie e degli obblighi che si applicano alle piattaforme, questo sistema non solo rende maggiormente responsabili le piattaforme nel contrasto alla disinformazione, ma riduce anche la loro discrezionalità nella moderazione dei contenuti. In altre parole, l'idea di tali codici è superare uno degli aspetti più problematici dell'autoregolazione, come assai lucidamente individuato da Luisa Torchia¹⁴².

Tuttavia, il Codice di buone pratiche non è ancora diventato un Codice di condotta, come definito dal DSA. Nonostante sia stato adottato per far fronte al fallimento del primo tentativo di auto-regolamentazione del 2018, il codice rappresenta ancora un meccanismo volontario che aspira a diventare un codice di condotta e, quindi, una misura di co-regolamentazione. Al momento, tale valutazione da parte della Commissione sembra solo rimandata, anche se risulta importante sottolineare come l'ambito stesso di applicazione del codice potrebbe essere messo in discussione dall'ampliamento delle politiche europee in materia di piattaforme online e moderazione dei contenuti¹⁴³. Alcune parti del Codice tendono a sovrapporsi agli obblighi giuridici che sono stati introdotti dalla legislazione europea dopo la sua adozione. Ad esempio, l'accesso a fini di ricerca ai dati detenuti dalle piattaforme online, nel Codice, si sovrappone al quadro giuridico introdotto dal DSA¹⁴⁴. Analogamente, è probabile che le norme del codice in materia di pubblicità politica soddisfino l'obbligo che sarà introdotto dal regolamento sulla trasparenza della pubblicità politica¹⁴⁵.

In un tale contesto, l'approccio dell'Unione sembra sempre più di-

¹⁴¹ *Ibidem*.

¹⁴² L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista Trimestrale di Diritto Pubblico*, fasc. 4, 2022

¹⁴³ I. NENADIC *et al.*, *Structural indicators to assess effectiveness of the EU's Code of Practice on Disinformation*, Working Paper, 2023.

¹⁴⁴ DSA, art. 40.

¹⁴⁵ Regolamento relativo alla trasparenza e al *targeting* della pubblicità politica, cit. Per un quadro più ampio sul rapporto tra disinformazione e IA nel contesto delle elezioni politiche, si consideri O. POLLICINO, P. DUNN, *Disinformazione e intelligenza*

stinguersi a livello globale. La regolamentazione del rischio e la co-regolamentazione contribuiscono ad avvicinare gli attori pubblici al loro obiettivo di rendere maggiormente effettive le politiche pubbliche negli spazi digitali, aumentando al contempo la reattività degli attori privati all'attuazione dei propri obblighi e l'accettazione di potenziali sanzioni. In effetti, un maggiore dialogo con le autorità di regolamentazione nella fase di applicazione avrebbe potuto aiutare a mitigare misure sproporzionate quale, ad esempio, la sospensione temporanea di ChatGPT da parte del Garante per la protezione dei dati personali,¹⁴⁶ nonché a rendere maggiormente coerente e attrattivo il mercato interno, che non sembra portare a un cambiamento di rotta per quanto riguarda lo sviluppo di prodotti e servizi digitali europei¹⁴⁷. Seppur restino domande costituzionali relativamente a un potenziale eccesso di regolamentazione e alle forzature delle basi giuridiche dell'UE a tal fine, lo sviluppo di una strategia di questo tipo può collegarsi alla necessità per il costituzionalismo europeo di rigettare approcci neoliberali o eccessivamente restrittivi, concentrandosi piuttosto sul bilanciamento, non solo tra diritti, ma tra le opzioni di regolazione (del presente, ma anche del futuro) che si è cercato di fare emergere nelle pagine che precedono.

artificiale nell'anno delle global elections: rischi (ed opportunità), in *Federalismi.it*, fasc. 12, 2024.

¹⁴⁶ Garante per la protezione dei dati personali, fascicolo n. 112, provvedimento del 30 marzo 2023, cit.

¹⁴⁷ DRAGHI, *The future of European competitiveness*, cit.