RIVISTA
AIC ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI

Rivista N°: 2/2025
DATA PUBBLICAZIONE: 08/04/2025

AUTORE: Oreste Pollicino*

REGOLAZIONE E INNOVAZIONE TECNOLOGICA NELL'"ORDINAMENTO DELLA RETE"**

Sommario: 1. Introduzione e struttura del percorso di indagine. – 2. Coordinate della ricerca. I dilemmi della regolazione digitale nel quadro del costituzionalismo contemporaneo. – 2.1. Assenza di potere, la promessa tradita. – 2.2. Limitazione del potere. – 2.3. Separazione dei poteri. – 2.4. Base giuridica rilevante e fonti del diritto: forma e sostanza del diritto costituzionale europeo. – 2.5. La rilevanza della dimensione spaziale nel contesto digitale e la migrazione unidirezionale di idee costituzionali: un Bruxelles effect reloaded*? – 3. L'illusione anarcoide delle origini. La promozione dell'innovazione prevale sulle ragioni della regolazione. La prospettiva statunitense. – 3.1. La prospettiva europea: la Direttiva* e-Commerce *e la "direttiva madre" in tema di protezione dati quali emblema della prima stagione (nel bilanciamento tra innovazione e regolazione) di "liberismo digitale". – 4. Le ragioni di una metamorfosi e l'ascesa inarrestabile del "fattore algoritmico". – 5. Il consolidamento della società algoritmica e gli effetti sulle politiche di regolazione (giurisprudenziale e normativa). – 6. 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. – 7. 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? – 7.1. Protezione dati e regolamentazione dell'algoritmo. – 7.2. Il passaggio da una dimensione (esclusivamente) assiologico-sostanziale ad una (anche) di matrice procedurale: coordinate teoriche e applicative. – 8. Libertà di espressione online, moderazione dei contenuti e algoritmo. – 8.1. Le coordinate costituzionali. – 8.2. Dalla Direttiva* e-Commerce *alla nuova stagione regolativa (DSA) della moderazione dei contenuti in rete. – 8.3. (Segue) L'algoritmo nel DSA. – 9. Dall'algoritmo all'intelligenza artificiale: il magistero dell'*Artificial Intelligence Act*. – 10. Il nuovo Regolamento europeo sull'intelligenza artificiale: gli elementi portanti del nuovo sistema di regolazione. – 10.1. L'esplosione dell'intelligenza generativa ed i nuovi rischi per stato di diritto e democrazia: alcune definizioni di base. – 10.2. L'*AI Act *allo specchio: supera il test del costituzionalismo europeo? – 11. Riflessioni conclusive: quale futuro per il modello di regolazione del digitale in Europa?*

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

** Relazione al Convegno AIC "La libertà di manifestazione del pensiero", Salerno, 15-16 novembre 2024, pubblicata ai sensi dell'art. 4 del Regolamento della Rivista.

L'Associazione Italiana dei Costituzionalisti è iscritta al Registro Operatori della Comunicazione dal 9.10.2013, n. 23897. La Rivista AIC è inclusa nella classe A delle Riviste scientifiche dell'Area 12 - Scienze giuridiche. ISSN: 2039-8298 (on-line). Direttore responsabile: prof. Renato Balduzzi — Direttori: prof. Andrea Pertici (coord.), prof.ssa Benedetta Liberali, prof.ssa Lucia Scaffardi, prof.ssa Giusi Sorrenti.

1. Introduzione e struttura del percorso di indagine

Quali sono oggi i temi più rilevanti per la riflessione costituzionalistica a proposito dei processi evolutivi (o involutivi) dei modelli di regolazione del digitale, con particolare (ma non esclusivo) riferimento all'*humus* privilegiato caratterizzato dal costituzionalismo europeo? Può essere regolato il futuro? O, in altri termini, quali le insidie di una particolare processo di regolazione che è costretto a regolamentare, per l'appunto, qualcosa che nel migliore dei casi (se esiste) ha un dinamismo accelerato e in certi casi è solo prevedibile e non esistente, come per definizione è il caso del *novum* tecnologico[1]? Esiste davvero un dilemma esistenziale tra promozione dell'innovazione tecnologica e regolazione[2]? E, in caso di risposta affermativa, il modello europeo che sta emergendo negli ultimi anni per tentare di trovare un equilibrio tra le due istanze sopra evocate (forse solo apparentemente) in contrapposizione è, per un verso, coerente con i valori alla base del costituzionalismo europeo e, per altro verso, in grado di far sì che la fortezza regolamentare europea sia non solo inespugnabile ma anche in grado, quando necessario, di attivare i ponti levatoi di interconnessione con i modelli di regolazione – per forza di cosa concorrenti – di altre aree regionale del globo? Quali le ragioni della trasfigurazione in corso delle grandi piattaforme tecnologiche da "semplici" attori economici a veri e propri poteri privati spesso in competizione con quelli pubblici? È proporzionale e adeguata la trasformazione dello strumentario regolamentare europeo per fare fronte a tale trasfigurazione? Ed ancora, quali sono le nuove sfide che pone l'emersione (ed esplosione) dell'intelligenza generale di tipo generativo? Perché richiede una reazione regolamentare, ma anche una cornice costituzionale di contenimento, differente rispetto a quelle che hanno caratterizzato la reazione all'emersione del fattore "algoritmico"? E quale la differenza – in termine di principi costituzionali in gioco – tra automazione, alla base della stagione dell'algoritmo, e autonomia e inferenza e predittività[3], che, integrate, costituiscono le caratteristiche essenziali del nuovo ecosistema digitale costituito dall'intelligenza artificiale? In questo contesto, l'Artificial Intelligence Act (AI Act), recentemente adottato dell'Unione europea e che tenta – in maniera anche ambiziosa – di regolamentare tale nuovo ecosistema, è conforme alle coordinate essenziali del costituzionalismo europeo? E quali, infine, le prospettive evolutive del modello di regolazione del digitale in Europa?

Sono queste alcune delle domande di ricerca cui si proverà a rispondere, in modo – per forza di cose – non esaustivo in queste pagine che costituiscono l'avvio di un *working in progress*, meglio un cantiere, anche con riferimento alla citazione della letteratura rilevante di taglio costituzionalistico, sempre più ampia, variegata e interessante.

L'analisi che segue si propone di seguire la seguente struttura.

---

[1] M. E. PRICE, *The Newness of New Technology*, in *Cardozo Law Review*, fasc. 22, 2001, p. 1885.

[2] Da ultimo tale dilemma è messo in discussione con argomenti abbastanza efficaci da A. Bradford, *The False Choice Between Digital Regulation and Innovation*, aggiornato al marzo 2024 e visualizzabile on line https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=5567&context=faculty_scholarship

[3] Vedi ora le dense riflessioni contenute nel volume, F. FABRIZZI-L. DURST, *Controllo e predittività. Le nuove frontiere del costituzionalismo nell'era dell'algoritmo*, Editoriale Scientifica, Napoli, 2024.

Si guarderanno, innanzitutto, le più evidenti epifanie della rilevanza costituzionalistica dei processi di accelerazione tecnologica, da una parte, e della reazione regolatoria, dall'altra. Ci si concentrerà, in particolare, su alcuni scenari che sembrano essere rilevanti con riferimento alle classiche categorie o strumentario concettuale del diritto costituzionale. Più specificamente, si guarderà al rapporto tra potere e tecnologica che emerge in almeno in quattro declinazioni: a) assenza di potere (par 2.1), b) limitazione di potere (par 2.2.), c) separazione tra poteri (par 2.3); d) rapporto tra potere ed effetto extraterritoriale del modello di regolazione digitale in Europa (par. 2.5). Ci si concentrerà, sempre con riguardo a quello strumento concettuale prima evocato, anche sulle torsioni che sembrano riguardare fonti del diritto e base giuridica rilevante per la legislazione dell'Unione (par. 2.4). Si procederà, quindi, con un percorso di analisi di matrice diacronica per provare a comprendere quali siano le ragioni che hanno portato a un passaggio da una fase di liberismo digitale ad una di cd. «costituzionalismo digitale», dedicando, con particolare riferimento a quest' ultima locuzione, qualche riflessione aggiuntiva in modo da provare a riempire di un minimo significato (e utilità) quella che potrebbe sembrare soltanto un'etichetta (parr. 3, 4, 5, 6, 7). Si guarderà, quindi, alla fase tecnologica della automazione per comprendere come la normativa europea abbia provato a reagire alle nuove sfide poste dall'ascesa del «fattore algoritmico», tanto in riferimento alla protezione dati (par. 8), quanto alla libertà di espressione e moderazione dei contenuti (par. 9). Infine, si guarderà, da una parte, alla discontinuità, dal punto di vista dell'innovazione tecnologica, spesso non messa del tutto a fuoco, tra la stagione dell'*automazione* algoritmica e quella dell'*autonomia*[4] che caratterizza, invece, il tratto dominante dell'intelligenza artificiale di carattere generativo e, dall'altra parte, alla apparente mancata discontinuità con riguardo ai modelli di regolazione che si si sarebbe invece attesa rispetto allo scatto, appena evocato, in termini tecnologici, con una serie di implicazioni problematiche rispetto alla bussola dei principi caratterizzanti il costituzionalismo europeo, ad iniziare dal rispetto della *rule of law* (par. 10). Le riflessioni conclusive saranno dedicate a una breve analisi del presente e del futuro tentativo europeo di trovare una conciliazione tra innovazione e tutela dei diritti, vale a dire la cd. legislazione sulla gestione del rischio e la possibile terza via tra *self regulation* e *hard regulation* costituita dalla cd. co-regolamentazione (par. 11).

2. Coordinate della ricerca. I dilemmi della regolazione digitale nel quadro del costituzionalismo contemporaneo

2.1. Assenza di potere, la promessa tradita

Davos, 1997, World Economic Forum. «Governi del Mondo, stanchi giganti di carne e di acciaio, io vengo dal Cyberspazio, nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo»[5].

[4] Nel significato kantiano di self-governance, caratteristica che non ha invece l'automazione.
[5] J. P. BARLOW, *A Declaration of the Independence of Cyberspace*, Davos, 8 febbraio 1996.

Se ci fosse ancora qualche dubbio su come venisse concepito "l'ordinamento della rete" dai padri della stessa nel periodo fondativo del web, questo passaggio della Dichiarazione di indipendenza del Cyberspace di Barlow potrebbe essere utile per dissiparlo.

Si tratta di un ordinamento, o meglio di un nuovo immaginato ordine virtuale, che, per riprendere i due corni del pendolo – oggetto privilegiato di questa ricerca – regolazione vs innovazione, è allergico a qualsiasi tipo di regolazione[6] e in cui, dall'altra parte, l'innovazione è dirompente[7]. Infatti, quest'ultima è caratterizzata da una discontinuità assoluta rispetto all'ordinamento statale non solo per il distacco e la separazione spazio-temporale da quest'ultimo, ma anche per la valenza rivoluzionaria che viene attribuita alla comunità della rete, che sarebbe in grado di autoregolarsi senza alcun filtro delle istituzioni, dei poteri pubblici e delle formazioni sociali di carattere intermedio caratterizzanti l'*humus* strutturale dell'ordinamento giuridico inteso in senso romaniano.[8] Su questo Barlow è molto chiaro nella sua dichiarazione di intenti: «non abbiamo un governo eletto, né è probabile che ne avremo uno, quindi vi parlo con l'unica autorità con cui la libertà stessa parla sempre. Dichiaro che lo spazio sociale globale che stiamo costruendo è naturalmente indipendente dalle tirannie che cercate di imporci. Non avete alcun diritto morale di governarci, né possedete alcun metodo di coercizione che abbiamo reale motivo di temere. I governi derivano i loro giusti poteri dal consenso dei governati. Non avete né richiesto, né ricevuto il nostro. Non vi abbiamo invitato. Non ci conoscete, né conoscete il nostro mondo. Il cyberspazio non rientra nei vostri confini […]». Difficile descrivere meglio la grande promessa (diremmo illusione oggi, ma fin troppo facile etichettare *ex post*) intravista padri del web alle sue origini: un nuovo orizzonte di libertà, in primo luogo dal controllo statale. La promessa di un internet che alle sue origini è percepito dai nuovi pionieri

---

[6] In tempi non sospetti Natalino Irti aveva fatto emergere, con riferimento alle dinamiche evolutive (od involutive) del mercato globale, come quest'ultimo fosse capace di autoregolarsi e, dunque, di regolare gli esseri umani che agiscono al suo interno. Per un'attenta riflessione sul pensiero di Irti, e più in generale, vd. N. IRTI, *L'ordine giuridico del mercato*, Laterza, Roma-Bari, 2003.

[7] Interessante la riflessione di Massimo Luciani intorno a come, per definizione, l'invenzione costringa ad un ritardo logico prima che cronologico la regolazione giuridica che, al di là delle opzioni di politica del diritto e della dimensione valoriale sottostante, si trova, in un certo senso, a dover abdicare alla possibilità di intervento preventivo di preorientamento. «Il diritto si trova dunque in una condizione di logico ritardo. Logico, insisto, non semplicemente crono-logico (ciò che – pure – è evidente), perché il suo asse è spostato rispetto a quello del processo inventivo. E il diritto incontra anche la supplementare difficoltà di essere assoggettato, nei sistemi democratico-liberali, a limiti posti a presidio delle libertà. Da noi, ad esempio, una regolazione giuridica che pretendesse di ammettere le sole innovazioni dotate di senso (sociale) sarebbe in problematica armonia con la garanzia della libertà della ricerca scientifica apprestata dall'art. 33 Cost. In via di principio, dunque, il diritto è costretto a riconoscere una libertà innominata, riservandosi di regolarla quando ne emergerà, se ne emergerà, il senso. Così facendo, però, abdica all'esercizio dell'attività di regolazione preventiva, che è sempre quella più efficace nel dominio dei comportamenti giuridici, perché è la sola capace di orientarli»; M. LUCIANI, *Può il diritto disciplinare l'Intelligenza Artificiale? Una conversazione preliminare*, in *Bilancio Comunità Persona*, fasc. 2, 2023, p. 10 ss.

[8] S. ROMANO, *L'ordinamento giuridico*, Quodlibet, Macerata, 1918. Si veda per riflessioni interessanti sull'ordine giuridico caratterizzante il cyberspazio, T. E. FROSINI, *L'ordine giuridico del digitale*, in *Quaderni costituzionali*, fasc. 1, 2023, p. 377 ss. e A. STERPA *et al.*, *L'ordine giuridico dell'algoritmo: la funzione regolatrice del diritto e la funzione ordinatrice dell'algoritmo*, in *Nuovi Autoritarismi e Democrazie : Diritto, Istituzioni, Società*, fasc. 5, 2, 2023. Interessanti intuizioni anche nel volume di M. R. ALLEGRI, *Ubi Social, Ibi Ius: Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider*, FrancoAngeli, Milano, 2018.

della frontiera digitale[9], come immune da qualsiasi forma di regolazione statale o sovranazionale.

Come è stato giustamente fatto notare, in questa prospettiva, i poteri pubblici sono «l'altrove, impossibilitati a predicare la propria sovranità e a estendere l'enforcement delle norme giuridiche entro uno spazio idealizzato come territorio separato»[10].

Quasi trent' anni dopo è facile concludere come la storia abbia poi fatto emergere una realtà assai diversa da quella che si augurava Barlow.

E questo per almeno due ragioni. La prima è che gli stati nazione[11] hanno dimostrato di poter non solo regolamentare, ma anche "iper-regolare" il cyberspazio che – è bene sempre tenerlo a mente – prima ancora che di bit, è costituito da infrastrutture fisiche e cavi sottomarini e, quindi, da una dimensione "atomica", parte di quel mondo analogico nei cui confronti Barlow (auto)proclamava un'irrealistica indipendenza.

Si pensi a come ordinamenti non democratici siano stati in grado di creare dei *Great Firewall*, come nel caso cinese e, ultimamente, quello russo a seguito della invasione dell'Ucraina, in cui muraglie virtuali e strategie di disinformazione e di censura hanno prodotto lesioni assai reali e significative all'esercizio della libertà di espressione e al diritto di essere informati.

La seconda ragione consiste nel fatto che ciò che doveva essere, secondo la visione utopistica dei pionieri della nuova frontiera digitale, un nuovo mondo libero da condizionamenti e poteri forti, in cui la comunità di utenti avrebbe avuto la capacità di auto-regolarsi alla luce di una cornice valoriale di riferimento fondata sulla libertà della rete e nella rete, si è rivelato uno spazio che, lungi dal voler cavalcare le visioni – altrettanto nocive come quelle utopistiche – distopiche, per esempio di Morozov[12] e parzialmente anche di Zuboff[13], si è rivelato assai accessibile ai poteri privati che hanno sicuramente condizionato quel processo di auto-determinazione da parte degli utenti, che doveva essere la pietra angolare su cui costruire lo spazio immaginato dai pionieri del web.

Il quadro appena tratteggiato, evidentemente, chiama in causa argomenti e categorie proprie del diritto costituzionale per una serie di ragioni.

Più precisamente, dimostratasi tradita la promessa di un'assenza di potere (e di poteri) nel nuovo ordinamento della rete, si è trattato di fare i conti con questioni chiave alla base del costituzionalismo contemporaneo. In particolare – e saranno i punti su cui ci si concentrerà in questa prima parte dello scritto – la cornice del "costituzionalmente rilevante" del tema oggetto di indagine ha almeno le seguenti componenti. In primo luogo, la limitazione del potere. In secondo luogo, la separazione tra poteri. In terzo luogo, sul piano delle tecniche di regolazione

---

[9] Rispetto alla rilevanza dell'idea di frontiera, calata soprattutto nel contesto del modello costituzionale statunitense, v. il suggestivo studio di A. BURATTI, *La frontiera americana. Una interpretazione costituzionale,* Ombre corte, Roma, 2016.

[10] M. BASSINI, *Libertà di espressione e social network, tra nuovi «spazi pubblici» e «poteri privati». Spunti di comparazione*, in *MediaLaws*, fasc. 2, 2021, p. 86 ss.

[11] J. GOLDSMITH - T. WU, *Who Controls the Internet? Illusions of a Borderless World*, in *Computer and Telecommunications Law Review*, fasc. 13, 7, 2006.

[12] E. MOROZOV, *The Net Delusion. The Dark Side of Internet Freedom*, PublicAffairs, New York 1997.

[13] S. ZUBOFF, T*he Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

– tramontata la chimera della *self-regulation* – l'identificazione della fonte del diritto e della base giuridica rilevante ai fini del menzionato esercizio di regolazione. Infine, come si accennava, la rilevanza dell'elemento territoriale in un contesto solo apparentemente allergico alla dimensione spaziale e la possibile migrazione (con rischio di rigetto) di "idee costituzionali" legate alle opzioni di politica del diritto alla base della regolazione digitale. Tali componenti dovranno essere analizzate autonomamente.

2.2. Limitazione del potere

In primo luogo, guardando al processo di trasformazione o trasfigurazione delle grandi piattaforme digitali[14], che non sono più (soltanto) attori economici in senso stretto, ma anche, come si accennava in precedenza, veri e propri poteri privati in competizione – spesso – con i poteri pubblici[15], emerge la prima sfida per il costituzionalismo, al quale è imposto un esercizio di rinnovamento perché, proprio per mantenere fede alla sua missione originaria di limitazione del potere, è costretto a trovare nuove geometrie di azione. Nello specifico, il passaggio più rilevante sembra essere l'affiancamento, ad una geometria esclusivamente verticale del classico rapporto autorità *versus* libertà, di una nuova dimensione orizzontale, il cui obiettivo è trovare le leve e gli strumenti più adeguati a limitare e contenere il potere privato detenuto dalle grandi piattaforme informatiche.

Si tratta di trasformazioni che non possono non chiamare in causa, tra l'altro, il rapporto tra diritto costituzionale e altri regimi o settori giuridici, che per lungo tempo hanno monopolizzato lo strumentario (e il dibattito) relativo a quale tipo di *enforcement* sia più idoneo a limitare il crescente potere dei soggetti privati in ambito digitale. Il riferimento non può che essere, in primo luogo, al diritto *antitrust*, il quale non solo, per le ragioni menzionate, non è più l'unica leva (anzi, forse non è neanche quella più adeguata) per contrastare tale potere, ma che si sta, altresì, interrogando su una possibile alterazione del suo codice genetico, tradizionalmente legato a un approccio che prevede un intervento del suo strumentario rilevante *ex post*, successivamente alla messa in opera delle condotte vietate. Non è un caso che il *Digital Markets Act*[16] abbia di fatto sfatato il tabù dell'intervento solo *ex post* del diritto della concorrenza, prevedendo un quasi eretico (per alcuni), ma assai efficace (per quasi tutti), intervento della disciplina rilevante *ex ante*, proprio a causa delle nuove sfide che l'accrescimento del potere di tali piattaforme sta facendo emergere.

E, attenzione, non si tratta di un potere esclusivamente di carattere economico, ma di natura assai più pervasiva, che tocca il nucleo duro della tutela dei diritti fondamentali.

---

[14] O. POLLICINO *et al.*, *Un « diritto al digitale »?*, in L. VIOLANTE - A. PAJNO, *Biopolitica, pandemia e democrazia*, Il Mulino, Bologna, 2021.

[15] La dottrina statunitense ha parlato, per esempio, di una relazione «triangolare» (cittadini-pattaforme-stato) nella regolazione dello *speech*: J.M. BALKIN, *Free Speech is a Triangle*, *in Columbia Law Review*, 118, 7, 2018, p. 2011 ss.

[16] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali, DMA), GU L 265/1. Per un commento, si veda J. MOSCIANESE - O. POLLICINO, *Concorrenza e regolamentazione nei mercati digitali*, Giappichelli, Torino, 2024.

Una domanda, in questo contesto alla luce delle considerazioni appena svolte, sembra essere rilevante: vi è davvero una discontinuità rispetto ad ambiti apparentemente analoghi in cui soggetti privati e *corporations* hanno o hanno avuto in passato un ruolo determinate nella configurazione del campo da gioco rilevante?

Nessuno è così ingenuo da pensare che questa sia la prima volta in cui si sia posto il problema del rapporto tra diritto pubblico e poteri privati[17], né che sia la prima volta che soggetti privati, di fatto, regolino determinati mercati – si pensi alle federazioni sportive – con una tale influenza su un particolare settore economico da detenere, *de facto*, un potere sostanzialmente *lato sensu* politico. La discontinuità, e, quindi, la rilevanza del nuovo scenario, che sta prendendo sempre più forma nel contesto digitale sono provocate da due ordini di ragioni. La prima è di ordine quantitativo: la pervasività del processo di digitalizzazione, i meccanismi di automazione algoritmica[18] e l'enorme quantità di dati a disposizione per definire processi di profilazione e anche di anticipazione delle preferenze degli utenti hanno portato le grandi multinazionali operanti nel settore digitale ad una capacità di influenza di natura globale senza precedenti. La seconda novità è di ordine, se si può chiamare così, qualitativo. Infatti, non si è infatti mai assistito a ciò che sta avvenendo nel contesto digitale. Vale a dire che soggetti privati con una dominanza così significativa su un mercato assai particolare come quello delle idee – per parafrasare la leggendaria metafora del *free marketplac*e di Holmes (*Abrams v. United States* 250 US 616, 1919, 624 ss.) – siano in grado di condizionare in modo così efficace il dibattito pubblico. Più precisamente – ed è qui che risiede la significativa discontinuità di fondo rispetto al passato, per le grandi piattaforme – come è stato recentemente sostenuto, «*fostering a large community – similar to a public sphere – is key to the business model*»[19]. È, dunque, evidente la rilevanza più diretta per lo strumentario del diritto costituzionale, con un'immediata ricaduta sulla tutela dei diritti in gioco – ad iniziare dalla libertà di espressione, la quale risulta sempre più assoggettata a forme private, e spesso automatizzate, di moderazione[20].

---

[17] P. BARILE, *Il soggetto privato nella Costituzione*, Cedam, Padova, 1953; C. M. BIANCA, *Le autorità private*, Jovenese, Napoli, 1977; M. BASSINI, *Internet e libertà di espressione: prospettive costituzionali e sovranazionali*, Aracne Editrice, Roma, 2019; M. BASSINI, *Fundamental rights and private enforcement in the digital age*, in *European Law Journal : Review of European Law in Context*, fasc. 25, 2, 2019, p. 182-197; M. MONTI, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e diritto*, 1, 2019; M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, fasc. 3, 2021, p. 739-760; F. COSTAMAGNA, *Diritti fondamentali e rapporti tra privati nell'ordinamento dell'Unione europea*, Giappichelli, Torino, 2022. Si veda anche il numero monografico 3/2022 di *Diritto Pubblico* dedicato, per l'appunto, a *Poteri privati* e, volendo, O. POLLICINO, *Potere digitale*, in M. CARTABIA - M. RUOTOLO (a cura di), *Potere e Costituzione*, in *Enciclopedia del Diritto*, V, Giuffrè, Milano, 2023.

[18] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Rivista di BioDiritto*, fasc. 1, 2019, p. 63 ss.

[19] M. POIARES MADURO - F. DE ABREU DUARTE, *Regulating Big Tech will take pluralism and institutions*, in *euronews.com*, 7 ottobre 2021. Non può essere qui oggetto di indagine specifico la questione della modalità di riproposizione delle condizioni e dei presupposti di una sfera pubblica funzionante, nell'accezione che ne dà Habermas (1991), nel contesto dell'ecosistema digitale, che però, evidentemente, merita un approfondimento in altra sede perché, evidentemente, si intreccia con la questione relativa alla concentrazione di potere detenuto da soggetti privati (che spesso però esercitano *de facto*, come si diceva, funzioni di natura para-costituzionale).

[20] P. DUNN, *Moderazione automatizzata e discriminazione algoritmica: il caso dell'hate speech*, in L. ABBA *et al., La Internet governance e le sfide della trasformazione digitale*, Editoriale scientifica, Napoli, 2022, p. 175 ss.; G. DE GREGORIO, *Democratising online content moderation: A constitutional framework*, in *The Computer Law and Security Report*, fasc. 36, 2020.

2.3. Separazione dei poteri

Accanto alla questione della limitazione del potere vi è però una seconda possibile prospettiva in grado di valorizzare il tema oggetto di indagine, quale terreno fertile per approfondire le trasformazioni di categorie e argomenti del diritto costituzionale.

In particolare, le questioni che attengono al rapporto tra innovazione e regolazione nell'ordinamento della rete sembrano costituire un laboratorio privilegiato per un recupero, accanto a quello di *bill of rights* (come emerge plasticamente dall'art. 16 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789), del concetto di costituzione quale *frame of government*, ossia di distribuzione ed equilibrio tra poteri. Non è, infatti, un mistero che la tecnologia digitale stia producendo un impatto significativo anche sui profili connessi alla separazione dei poteri, sia a livello nazionale che sovranazionale.

In particolare, da una parte, essa ha ulteriormente amplificato, come si è cercato di dimostrare altrove[21], quel fenomeno di *judicial globalization* descritto alla fine del secolo scorso da Slaughter[22], dall'altra ha necessitato di una profonda revisione, a dire il vero non sempre perfezionatasi, dell'apparato amministrativo statale[23].

Il tutto contribuisce a fare emergere in modo sempre più plastico la "solitudine" di un legislatore per lunghi tratti inerte rispetto alle accelerazioni spasmodiche della tecnologia. Un legislatore che viene sempre più messo all'angolo, insieme al principio di certezza del diritto e, se si vuole, alla necessaria legittimazione del circuito democratico rappresentativo, a favore di un assai audace attivismo giudiziario in cui il confine tra interpretazione creativa e manipolazione si va sempre più pericolosamente assottigliando. Dall'altra parte, deve anche riconoscersi che l'inerzia del potere legislativo non sempre è forzata ma, spesso, in qualche modo, volontaria. Quest'ultimo, infatti, pur di non rimanere perennemente indietro rispetto alle accelerazioni tecnologiche, preferisce rimanere inerte, delegando ai giudici la responsabilità di scelte, spesso tragiche[24]. Tali decisioni insistono su quelle operazioni di bilanciamento connesse ad una tecnologia che lungi dall'essere neutrale, sottintendendo una forte matrice assiologica-sostanziale. In questo contesto anche la Corte Suprema statunitense ha riconosciuto come «*the questions of whether, when, and how to regulate online entities, and in particular the social-media giants, are understandably on the front-burner of many legislatures and agencies. And those government actors will generally be better positioned than courts to respond to the emerging challenges social-media entities pose. But courts still have a necessary role in protecting those entities' rights of speech, as courts have historically protected traditional media's rights*»[25].

---

[21] O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Hart Publishing, Oxford, 2021, p. 184 ss.

[22] A.-M. SLAUGHTER, *Judicial Globalization*, in *Virginia Journal of International Law*, fasc. 40, 2000, p. 1103 ss.

[23] L. TORCHIA, *Lo Stato digitale: una introduzione*, Il Mulino, Bologna, 2023.

[24] G. CALABRESI - P.C. BOBBITT, *Tragic Choices*, W.W. Norton & Company, New York, 1978.

[25] *Moody v NetChoice, LLC and NetChoice, LLC v. Paxton*, 603 U.S. ___ (2024)

Il principio di separazione dei poteri è assai rilevante, specialmente con riferimento al livello privilegiato di produzione normativa in materia, ossia quello unionale, anche con riferimento ai rapporti tra, da una parte, i due co-legislatori dell'Unione e, dall'altra, la Commissione europea, cui spetta l'iniziativa legislativa.

Si faccia l'esempio dell'assai recentemente adottato, su cui si tornerà successivamente, Artificial Intelligence Act (AI Act)[26], vale a dire il regolamento con cui l'Unione ambisce, primo esperimento globale, a regolamentare in modo esaustivo e inevitabilmente *ex ante*, alcuni utilizzi (i più rischiosi) dei modelli di intelligenza artificiale. La Commissione europea, a norma del Regolamento[27] prima evocato, ha anche il compito, attraverso l'adozione di atti delegati[28], di aggiornare l'elenco dei sistemi di AI ritenuti ad alto rischio. Provando a non complicare il quadro con dettagli che hanno pure la loro rilevanza, il tema più significativo che sembra proporsi con riguardo al principio di separazione dei poteri è il seguente: l'aggiornamento di un insieme di usi e applicazioni di intelligenza artificiale, con la conseguente integrazione, in caso di emersione di nuove tipologie che presentano un rischio significativo, è una mera ricognizione tecnica che può essere delegata all'organo esecutivo dell'Unione o implica (visto che nessuna tecnologia, e tanto meno un ecosistema a sé come è l'intelligenza artificiale, può definirsi neutrale) delle scelte di natura assiologico-sostanziale che dovrebbero essere affidate all'organo legislativo all'interno del circuito democratico rappresentativo, per quanto azzoppato[29] dell'Unione? [30]

2.4. Base giuridica rilevante e fonti del diritto: forma e sostanza del diritto costituzionale europeo

È evidente che la questione appena evocata, che ha una dimensione ben più pregnante rispetto al tecnicismo apparente che potrebbe sembrare caratterizzarla, sia fortemente connessa a quella della identificazione della base giuridica, da una parte, e della fonte del diritto più adeguata, dall'altra, specie a livello europeo, per l'adozione della regolazione digitale. Ovviamente, mentre la regolamentazione sostanziale di queste materie – spesso di

---

[26] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale, AI Act), GU L, 2024/1689.

[27] AI Act, art. 7.

[28] AI Act, Art. 97.

[29] Per tutti si veda, J. H. H. WEILER, *Europe in crisis - on "political messianism", "legitimacy" and the "rule of law"*, in *Singapore journal of legal studies*, 2012, p. 248-268. Si consideri anche, I. PERNICE *et al.*, *Legitimacy issues of the European Union in the face of crisis: Dimitris Tsatsos in memoriam*, Nomos, Baden-Baden, 2017; V. A. SCHMIDT, *Europe's crisis of legitimacy: governing by rules and ruling by numbers in the Eurozone*, University Press, Oxford, 2020; C. SCHWEIGER, *Exploring the EU's legitimacy crisis : the dark heart of europe*, Edward Elgar Publishing, Northampton, 2016; W. SCHROEDER, *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation*, Hart Publishing, Oxford 2016.

[30] Non vi è dubbio vi sono nel trattato sul Funzionamento dell'Unione europea articoli che regolano la delega di potere, quali l'art. 290 TFUE e l'art. 97 come completato dal considerando 173, che introducono regole e limiti precisi al potere della Commissione, imponendole di consultare gli esperti designati dagli Stati membri e di coinvolgere attivamente il Parlamento e il Consiglio. Il dubbio però permane? Si tratta di salvaguardie sufficienti visto cosa vi è in gioco?

carattere settoriale – rientra nelle competenze degli studiosi di diritto d'autore, protezione dei dati, regolazione audiovisiva e, in particolare, intelligenza artificiale, la scelta della base giuridica più adeguata nei Trattati dell'Unione per determinare la competenza legislativa dell'UE è, invece, una questione di diritto costituzionale europeo. Come Andrea Morrone ha esattamente notato a riguardo, «il sistema di fonti normative è il riflesso dello specifico rapporto tra società civile e pubblici poteri (forma di stato) e del rapporto tra i poteri pubblici dello stato (forma di governo)»[31].

E non è soltanto un tema teorico.

Al di là di quanto si è detto, può essere sufficiente fare due esempi. Per quanto riguarda la base giuridica rilevante, l'Unione europea sembra aver pescato "il coniglio dal cilindro" nell'art. 114 TFUE che consente l'adozione di misure relative al riavvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri, che hanno per oggetto l'instaurazione e il funzionamento del mercato interno.[32]

A partire dal Regolamento generale per la protezione dei dati personali, il celeberrimo GDPR (2016), fino ad arrivare all'AI Act del 2024 che forse diventerà, per la sua quasi smodata ambizione regolatoria di una tecnologia in costante mutamento, ancor più celebre (non necessariamente in positivo), passando dall'European Media Freedom Act[33] e dal Regolamento sulla trasparenza della pubblicità politica[34], adottato nel tentativo di contrastare il fenomeno della dilagante disinformazione sul web specie nella stagione elettorale, la base giuridica rilevante è stata sempre identificata nell'articolo 114 TFUE, "asso piglia tutto" (non solo) nel settore digitale.

Due considerazioni rapide sul punto. In primo luogo, la forzatura è evidente. Le legislazioni che si sono ricordate sono sempre più legate, in via inevitabilmente incrementale, alla tutela dello stato di diritto e alla democrazia in ambito digitale, e quindi sempre più attratte dall'ambito di applicazione della bussola valoriale dell'art. 2 TUE. Previsione che, però, evidentemente non può essere utilizzata quale esclusiva base giuridica, e che, quindi, necessita della stampella di una disposizione già presente originariamente nel trattato di Roma, come quella appena ricordata (art. 114 TFUE), relativa all'armonizzazione delle legislazione statali

---

[31] A. MORRONE, *Fonti normative*, Il Mulino, Bologna, 2018, p. 15, così come ripreso da N. MACCABIANI, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, in *Osservatorio sulle fonti*, fasc. 3, 2022, secondo cui le modalità con cui è congegnato il sistema delle fonti del diritto non ha portata meramente formale e procedurale, bensì è «materia di diritto costituzionale».

[32] M. KELLERBAUER, *Article 114 TFEU*, in M. KELLERBAUER *ET AL.* (a cura di), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford University Press, 2019; A. ENGEL, *Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market*, in A. ENGEL *ET AL.* (a cura di), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights*, Springer Nature Switzerland, Cham, 2025, p. 13–28.

[33] Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media), GU L. 2024/1083. Per un'analisi della questione qui accennata si veda O. POLLICINO-F. PAOLUCCI, *Unveiling the Digital side of Journalism: Exploring the European Media Freedom Act's opportunities and challenges*, in *La Revue des Juristes de Sciences Po*, 1, 2024; E. LONGO, *Grounding media freedom in the EU: The legal basis of the EMFA*, in *Rivista Italiana Di Informatica e Diritto*, fasc. 7, 1, 2025, p. 14–14.

[34] Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al *targeting* della pubblicità politica, GU L. 2024/900.

in materia di mercato unico.[35] Disposizione che ha una forte vocazione economicistica, che non rispecchia del tutto l'orizzonte valoriale dell'ultima stagione di regolazione in tema di digitale, su cui si tornerà, e che ha come parametro di riferimento, come si diceva, (anche) il rispetto dello stato di diritto e della tutela dei diritti fondamentali in rete.

In secondo luogo, mercato unico e stato di diritto sono inscindibili nel processo di integrazione europea, anche oltre la dimensione digitale. Come osserva Andrea Simoncini,[36] la regolazione del digitale nell'UE nasce con due obiettivi gemelli: promuovere il mercato unico delle nuove tecnologie e garantire un'elevata protezione dei diritti fondamentali, data la crescente pervasività di questi sistemi. Un nodo cruciale ha riguardato la scelta tra direttiva e regolamento. Nonostante l'intento di uniformità, il GDPR e l'AI Act, pur formalmente regolamenti, funzionano spesso come "direttive mascherate" per l'alto numero di clausole aperte, richiedendo interventi nazionali di recepimento. Questo paradosso normativo rischia di vanificare l'obiettivo di armonizzazione, come già accaduto nella protezione dei dati personali.

2.5. La rilevanza della dimensione spaziale nel contesto digitale e la migrazione unidirezionale di idee costituzionali: un Bruxelles effect reloaded*?*

Le posizioni anarcoidi delle origini di internet legate al dogma della *self-regulation*, che saranno anche riprese più avanti, hanno ben presto lasciato spazio a visioni non ostili a una regolazione statale. Visioni che hanno conosciuto un più facile radicamento anche per effetto delle prime pronunce giurisprudenziali in cui, soprattutto negli Stati Uniti, si prendeva atto che le peculiarità del cyberspazio non fossero tali da distogliere le attività che vi prendevano corpo da qualsiasi regola di condotta che non fosse già stata introdotta dagli Stati per governare il "mondo della materia"[37].

Al contrario, come si è fatto notare in uno studio di dieci anni fa[38], è proprio la reazione delle corti statunitensi all'orientamento anarcoide prima evocato, attraverso l'esercizio di radicamento della propria giurisdizione in merito a casi aventi ad oggetto una disputa su Internet, a confermare che esistono "*adjudicators"*all'interno di uno spazio che si pensava fosse immune all'intervento dei pubblici poteri. Il che, si notava in quello studio, potrebbe fare emergere uno scenario alquanto paradossale nel quale «*the area of Internet law, for years considered the most emblematic expression of the limitations of national law in facing the challenges of globalisation, would, by contrast, prove to be one of the few fields of law still encapsulated in*

---

[35] Sul punto, si richiama anche l'*explanatory memorandum* pubblicato dalla Commissione Europea a corredo della Proposta sull'AI Act. Si veda Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, Brussels, 21 aprile 2021, §2.1.

[36] A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, fasc. 4, 2022, p. 1031-1049.

[37] V. U. KOHL, *Jurisdiction and the Internet,* University Press, Cambridge, 2009; D. J. SVANTESSON, *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford, 2017; J. HÖRNLE, *Internet Jurisdiction Law and Practice,* Oxford University Press, Oxford, 2020.

[38] O. POLLICINO- M. BASSINI, *The Law of the Internet between Globalization and Localization*, in M. MADURO *et al.*, *Transnational Law - Rethinking Law and Legal Thinking*, Cambridge University Press, Cambridge, 2014.

national law, in which not only a global approach, but also a transnational one risks proving not to be fully adequate»[39].

Oltre l'Atlantico, alcune decisioni giurisprudenziali hanno riaffermato che i poteri digitali, operando nel mercato europeo, devono rispettarne la normativa e i valori costituzionali. Questa prospettiva si distingue dall'approccio statunitense, focalizzato sulla libertà di espressione, mentre la giurisprudenza europea, riflettendo un diverso paradigma assiologico, privilegia la protezione dei dati personali, considerata il "Primo emendamento" del costituzionalismo europeo. D'altro canto, l'evoluzione giurisprudenziale dei giudici della Corte di Giustizia evidenzia il primato della *privacy* rispetto ad altri diritti e riafferma la rilevanza dei confini giuridici nella tutela individuale, nonostante la dematerializzazione dei dati.[40]

In questa particolare prospettiva, due "mosse" giurisprudenziali paiono essere indicative di questa attitudine: la prima sortita della Corte di giustizia degna di nota risale al celeberrimo caso *Google Spain*[41]. Questa sentenza non rileva tanto in questo momento per il suo contenuto sostanziale (l'applicazione a un motore di ricerca della disciplina sulla protezione dei dati in qualità di titolare del trattamento), quanto per il suo presupposto fondante: l'estensione a soggetti stabiliti al di fuori dall'Unione europea, che effettuano trattamenti di dati di individui residenti negli Stati membri, della applicazione della disciplina all'epoca racchiusa nella direttiva 95/46/CE[42]. La Corte di giustizia ha così anticipato il GDPR[43], che all'art. 3, par. 2, contiene ora una analoga previsione, volendo affermare con fermezza il principio per cui lo sfruttamento in chiave economica di dati personali di cittadini europei non può essere svincolato e distolto dal rispetto delle garanzie richieste dall'ordinamento dell'Unione, espressive del più elevato livello di tutela racchiuso, tra l'altro, negli artt. 7 e 8 della Carta dei diritti fondamentali e nell'art. 8 della CEDU. La sentenza *Google Spain* ha, così, segnato un punto di non ritorno, evidenziando la necessità che anche gli operatori con provenienza extra-UE si conformino alla normativa europea rilevante, che rispecchia la dimensione assiologica delle tradizioni costituzionali comuni degli Stati membri.

La questione dello spazio è, dunque, visceralmente connessa a quella della sovranità anche nell'ordinamento della rete. Come ha fatto emergere recentemente Luisa Torchia, «vi è

---

[39] *Ibidem*, 347.

[40] B. PETKOVA, ***Privacy as Europe's first Amendment,*** in *European Law Journal*, fasc. 25, 2, 2019, p. 140 ss.

[41] C. giust. UE 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/14. La letteratura in proposito è vastissima. Per una panoramica, si può richiamare la rassegna monografica ospitata da G. RESTA- V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google,* RomaTre-Press, Roma, 2015. Sulle conseguenze sul piano della tutela dei diritti umani, in E. FRANTZIOU, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, in *Human Rights Law Review*, fasc. 14, 4, 2014, 761 ss. Per una lettura in chiave statunitense della sentenza e del suo impatto, R. POST, *Data Privacy and Dignitary Privacy: Google Spain, the Right To Be Forgotten, and the Construction of the Public Sphere,* in *Duke Law Journal*, fasc. 67, 2018, p. 981 ss. nonché J. ROSEN, *The Right To Be Forgotten,* in *Atlantic,* July/August 2012. Per una prospettiva di più ampio respiro, ancorché precedente alla sentenza F. PIZZETTI, *Il caso del diritto all'oblio,* Giappichelli, Torino, 2012.

[42] Direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, n. 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L. 281/1995.

[43] Regolamento del Parlamento europeo e del Consiglio 27 aprile 2016, n. (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, GU L. 119/2016.

una crescente tendenza alla creazione di un nuovo tecno-nazionalismo, in nome del quale risuona lo slogan della sovranità digitale che ciascun ordinamento rivendica». E aggiunge «la sovranità digitale, rispetto alla nozione tradizionale di sovranità, presenta un carattere nuovo, perché viene invocata sia per assicurare la difesa contro interferenze esterne e, quindi, il controllo sul territorio (naturale e digitale) nazionale, sia, innovativamente, per espandere le regole di ciascun ordinamento, che seguono – per così dire – i cittadini di quell'ordinamento: per le regole sulla privacy sinora, e potenzialmente per la nuova regolazione europea in materia di mercati e servizi digitale e di intelligenza artificiale, gli obblighi imposti hanno una proiezione extraterritoriale». [44] Rispetto a tali sovranità digitali, Anu Bradford ha evidenziato come i conflitti regolatori in materia di diritti e libertà siano emersi principalmente nello "scontro" fra almeno due *imperi digitali*, gli Stati Uniti e l'Unione europea[45].La seconda stagione giurisprudenziale rilevante in questa sede – perché volta a dimostrare come lo spazio, e, più in particolare, il territorio siano ingredienti essenziali del potere anche nella sua dimensione digitale – è rappresentata dal caso *Digital Rights Ireland*[46] in cui la Corte di Giustizia ha annullato la direttiva in materia di *data retention*[47] del 2006, perché in contrasto con la Carta dei diritti fondamentali.[48]

Il caso *Digital Rights Ireland* ha riaffermato il ruolo centrale del territorio nel diritto digitale: la Corte di Giustizia ha annullato la direttiva sulla *data retention* del 2006 per incompatibilità con la Carta dei diritti fondamentali, rilevando l'assenza di un vincolo di conservazione dei dati nell'UE e quindi di un effettivo controllo indipendente. Ciò conferma che lo spazio giuridico resta essenziale anche nel cyberspazio, smentendo l'idea di un digitale autonomo dalle categorie del diritto costituzionale.

Più recentemente, il dibattito si è spostato sull'effetto extraterritoriale di normative come il GDPR e l'AI Act. Mentre il GDPR ha influenzato altri ordinamenti in quanto tutela un diritto fondamentale, il *Brussels effect* potrebbe non replicarsi per l'AI Act, che propone un modello regolatorio basato sullo stato di diritto e sulla sicurezza del mercato unico. A differenza del GDPR, l'AI Act incontra maggiore resistenza in altre aree regionali come Stati Uniti e Cina, che sviluppano modelli alternativi in base ai propri riferimenti costituzionali, senza adattarsi passivamente alla normativa europea.

Non è un caso, dunque, che si sia aperta una vera e propria corsa, o meglio rincorsa, alla regolazione con riguardo all'intelligenza artificiale. In particolare, è opportuno sottolineare in primo luogo come simili spinte si siano avute nel continente europeo non solo a livello di Unione, ma anche a livello di Consiglio d'Europa.[49]

---

[44] L. TORCHIA, *Poteri pubblici e poteri privati nel mondo digitale*, in *Il Mulino*, fasc. 1, 2024, p. 28.

[45] A. BRADFORD, *Digital Empires. The Global Battle to Regulate Technology*, Oxford, 2023.

[46] C. giust. UE 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, cause C-293/12 e C-594/128.

[47] Direttiva del Parlamento europeo e del Consiglio 15 marzo 2006, n. 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, GU L. 105/2006.

[48] M. BASSINI, *Data retention as a matter of constitutional law*, in E. KOSTA, I. KAMARA (a cura di), *Data retention in Europe and beyond*, 2025.

[49] F. P. LEVANTINO-F. PAOLUCCI, *Advancing the Protection of Fundamental Rights Through AI Regulation: How the EU and the Council of Europe are Shaping the Future*, SSRN Scholarly Paper, Rochester, NY, 2024.

Con riguardo al Consiglio d'Europa, il riferimento, già menzionato, è, in particolare, alla Convenzione quadro sull'intelligenza artificiale e sui diritti umani, la democrazia e la *rule of law*, approvata dal Comitato sull'Intelligenza Artificiale d'Europa (CAI) il 14 marzo 2024, adottata dal Comitato dei Ministri il 17 maggio 2024 e, infine, aperta alla firma da parte degli Stati contraenti a partire dal 5 settembre 2024[50]. A livello nazionale, un caso emblematico è rappresentato tra l'altro dallo schema di disegno di legge, recentemente approvato dal Consiglio dei Ministri della Repubblica italiana, recante disposizioni e delega al governo in materia di intelligenza artificiale[51].

Significative spinte in direzione di una maggiore regolamentazione delle tecnologie connesse all'IA si sono avute recentemente anche al di fuori dell'Europa e, in generale, nel contesto internazionale globale[52]. Con riferimento a tale aspetto, sembra opportuno richiamare in primo luogo l'adozione della cosiddetta Dichiarazione di Bletchley, risultato di un *summit* sull'IA tenutosi a inizio novembre 2023 e che ha visto la partecipazione di 28 Stati, oltre che dell'Unione europea[53]. La Dichiarazione rappresenta, in tal senso, un significativo passo avanti nel contesto della cooperazione internazionale in materia di *governance* dell'intelligenza artificiale.

In questo senso, la Dichiarazione di Bletchley riconosce la natura internazionale dei rischi dell'IA e promuove la cooperazione per un'IA affidabile, sicura e trasparente, con un focus sulla responsabilità degli operatori più che sulla regolamentazione normativa[54]. Parallelamente, negli Stati Uniti, la precedente amministrazione guida dal Pres. Biden mirava a creare nuovi standard per la sicurezza dell'IA, la tutela della privacy e la promozione di diritti civili e innovazione, attraverso una strategia condivisa tra pubblico e privato.[55] Strategia che, assieme a un nutrito gruppo di altri *executive orders* (EO) è stata del tutto rivista dall'amministrazione successiva guidata, invece, dal Pres. Trump, il quale, in uno dei suoi primi atti ha rescisso vari

[50] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CET Series n. [225], firmata a Vilnius il 5 settembre 2024, https://rm.coe.int/1680afae3c.

[51] Vedi, tra l'altro, M. BORGOBELLO, *DDL intelligenza artificiale: così l'Italia tutela la dignità delle persone*, in *Agenda Digitale*, 24 aprile 2024, https://www.agendadigitale.eu/cultura-digitale/ddl-intelligenza-artificiale-cosi-litalia-tutela-la-dignita-delle-persone/.

[52] M. LUCIANI, *La sfida dell'intelligenza artificiale*, 2023 https://www.associazionedeicostituzionalisti.it/it/lalettera/12-2023-liberta-di-ricerca-e-intelligenza-artificiale/la-sfida-dell-intelligenza-artificiale.

[53] «The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023», https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023, 1 novembre 2023.

[54] Vedi in tal senso F. PIZZETTI, *Attenzione, il mondo sceglie un approccio diverso da quello UE*, *Agenda Digitale*, 2023, https://www.agendadigitale.eu/sicurezza/privacy/ai-pizzetti-attenzione-il-mondo-sceglie-un-approccio-diverso-da-quello-ue/.

[55] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, 30 ottobre 2023. Si veda, sulle connessioni tra EO di Biden e Dichiarazione di Bletchley Park, N. A. SMUHA, *Biden, Bletchley, and the emerging international law of AI*, in *Verfassungsblog*, 2023, https://verfassungsblog.de/biden-bletchley-and-the-emerging-international-law-of-ai/.

EO, tra cui quello relativo all'IA.[56] In sostanza, l'approccio statunitense, ancora una volta, si smarca da quello europeo per una maggiore flessibilità che intende evitare rigidità normative.[57]

Oltre all'EO, diversi stati federati hanno comunque adottato proprie leggi sull'IA, mentre il Congresso lavora su linee guida bipartisan, con particolare attenzione all'impatto dell'IA sui processi democratici ed elettorali.

Sul piano internazionale, infine, appare importante fare un breve cenno anche alle strategie implementate dalla Repubblica popolare cinese, la quale, del resto, è da anni impegnata in una significativa stagione legislativa nel contesto digitale: essa si è recentemente dotata, *inter alia*, di un *Personal Information Protection Law* (PIPL), oltre che di una *Data Security Law* (DSL) e di una *Cybersecurity Law* (CSL). In agosto 2023, inoltre, la Cina ha adottato alcune significative misure *ad interim* dedicate esplicitamente alla regolazione di sistemi di IA generativa (*Interim Measures for the Management of Generative Artificial Intelligence Services*). Poi, tali misure sono state implementate dal *Basic security requirements for generative artificial intelligence service*, adottato il 29 febbraio 2024, il quale individua oltre 30 rischi di sicurezza specifici derivanti dallo sfruttamento dell'IA, tra cui la violazione del copyright, i *bias* algoritmici, ma anche la divulgazione di informazioni circa il sistema politico cinese e la sua storia[58].

In generale, appare chiaro che l'Unione è destinata a confrontarsi in modo significativo con le numerose spinte, provenienti dal panorama internazionale, concernenti la regolamentazione del fenomeno dell'IA. La sfida che sembra aprirsi, alla luce di quanto esplicitato nelle pagine che precedono, è quella relativa all'effettiva capacità del nuovo quadro normativo e, in particolare, dell'AI Act di rappresentare uno strumento competitivo, sotto il profilo costituzionale ed economico, per lo sviluppo di un mercato europeo dell'IA.

Il quadro appena tratteggiato può essere utile per evidenziare la rilevanza accresciuta della prospettiva costituzionalistica per un'azione anticipatoria e non soltanto reattiva riguardo sfide e dilemmi connessi al difficile equilibrio regolazione-innovazione nell'ordinamento della rete e derivanti la natura trasformativa della tecnologia digitale, ed, in particolare, dell'intelligenza artificiale.

Nelle pagine che seguiranno, adottando uno sguardo anche di taglio diacronico, questo lavoro analizzerà l'evoluzione della regolazione digitale, dal *laissez-faire* degli albori del web negli Stati Uniti all'(iper?) regolazione europea. Si esaminerà il passaggio dal liberismo al costituzionalismo digitale, valutando come la normativa abbia reagito ai cambiamenti tecnologici e valoriali. Particolare attenzione sarà dedicata alla marginalizzazione del "fattore umano" e all'ascesa del "fattore algoritmico", interrogandosi sulle risposte del costituzionalismo europeo.

---

[56] Executive Order, Initial Rescissions of Harmful Executive Orders and Actions, 20 gennaio 2025, https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/.

[57] Vedi, tra l'altro, D. Tobey *et al.*, *Secure, safe, and trustworthy: Common ground between the US AI Executive Order and the EU AI Act*, *DLA Piper*, 2023, https://www.dlapiper.com/en/insights/publications/ai-outlook/2023/secure-safe-and-trustworthy-common-ground.

[58] Center for Security and Emerging Technology, *Basic Safety Requirements for Generative Artificial Intelligence Services*, 2024, https://cset.georgetown.edu/publication/china-safety-requirements-for-generative-ai-final/.

L'intelligenza artificiale generativa, distinta dalla semplice automazione, sarà il banco di prova per valutare se l'AI Act sia coerente con i principi europei.

Infine, si esplorerà la co-regolamentazione come terza via tra *hard* e *soft law* e l'approccio basato sulla gestione del rischio, elementi chiave per bilanciare innovazione e tutela dei diritti fondamentali nell'evoluzione della rete in Europa.

3. L'illusione anarcoide delle origini. La promozione dell'innovazione prevale sulle ragioni della regolazione. La prospettiva statunitense.

Anche a causa dell'influenza delle posizioni sintetizzate nella Dichiarazione di Barlow, nelle riflessioni dei primissimi commentatori che hanno esplorato l'avvento del cyberspazio, compaiono riferimenti costanti alle difficoltà che una rete globale, in grado di connettere individui-utenti localizzati in ordinamenti giuridici diversi tra loro e con siti-comunità virtuali a loro volta riconducibili a sistemi giuridici variegati, poteva produrre rispetto alla pretesa di controllo delle attività e condotte su un territorio, tipico postulato della sovranità statuale.

Soprattutto nella dottrina statunitense, si è subito evidenziata una contrapposizione tra i sostenitori di una visione cyberanarcoide[59] e coloro che hanno contestato i presupposti normativi e descrittivi di questa tesi[60]. Le posizioni antitetiche alla *state regulation*, ispirate, forse, anche da un "pregiudizio libertario", che è incline a guardare con diffidenza all'assoggettamento a regolazione pubblicistica di fenomeni "nuovi", si fondavano sul riconoscimento di una pretesa superiorità dell'autoregolamentazione sul cyberspazio. Questa visione era suggestionata da alcune criticità ravvisate nell'applicazione alla rete di regole pensate per un mondo fatto di materia e fondato sulla delimitazione di confini territoriali (anche quale operazione idonea a sancire un limite all'efficacia spaziale di certe regole), fra cui, per esempio, l'incertezza che gli individui-utenti avrebbero patito nell'identificare le regole applicabili nei vari ambiti/siti in cui le loro condotte prendevano corpo (l'assenza della c.d. "*notice*").

Nel contesto di una diffidenza verso la regolazione e, in particolare, di marcata ostilità rispetto a una *content regulation* che potesse differenziare i contenuti legittimamente disponibili nella realtà virtuale da quelli accessibili nel mondo reale (del resto, dirà proprio la Corte suprema che non vi è prova di un maggior beneficio insito nella regolamentazione, rispetto a una sua assenza[61]), il legislatore statunitense ha optato per un paradigma destinato oggi a far discutere, racchiuso nella *Section* 230 del *Communications Decency Act*. La disposizione, tuttora in vigore, traduce in atto quel fervore libertario consacrato dal Primo emendamento che

---

[59] D.R. JOHNSON-D. POST, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review,* fasc. 48, 5, 1996, 1371 ss.

[60] J.L. GOLDSMITH, *Against Cyberanarchy,* in *University of Chicago Law Review*, fasc. 65, 4, 1199 ss.

[61] Corte Suprema federale degli Stati Uniti d'America 26 giugno 1997, *Reno c. Aclu*, in 521 U.S. 844 (1997): «*The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship*».

si andava celebrando al cospetto dell'avvento di Internet[62]. La norma esonera da responsabilità i prestatori di servizi per ogni atto di moderazione di contenuti di natura diffamatoria: sia che il prestatore di servizi abbia deciso di rimuovere un contenuto, sia che abbia scelto di mantenerlo disponibile, l'opzione prescelta non potrà generare alcuna responsabilità a suo carico, al di fuori di una serie di eccezioni particolari. Questa opzione di grande favore per i fornitori di servizi ha a proprio fondamento l'intento di evitare linee d'ombra nella qualificazione giuridica dei prestatori di servizi, sciogliendo il dilemma apparso all'attenzione della giurisprudenza statunitense tra una qualificazione di *distributors* o di *publishers*. Si è evidenziato come la scelta compiuta, che, peraltro, traduce un rafforzamento della stessa tutela prevista dal Primo emendamento[63], abbia trovato fondamento nell'opportunità di evitare che forme virtuose di moderazione e *policing* dei contenuti da parte di siti, che avessero implementato idonee misure a questo proposito, finissero per determinare l'applicazione di un regime, quello della responsabilità editoriale, eccessivamente penalizzante per soggetti formalmente estranei a un controllo sui contenuti. Come è stato sottolineato in letteratura, la *Section* 230 CDA, al centro, peraltro, di qualche (velleitario e poi sopito) tentativo di rivisitazione anche nel corso della presidenza Trump[64], costituì il risultato di una mozione *bipartisan* per evitare questo paradosso, ben visibile nella sentenza *Stratton Oakmont v. Prodigy*[65] della Corte suprema dello Stato di New York: il prodigarsi di una piattaforma per effettuare, in buona fede, *content policing* avrebbe potuto attrarre sul gestore di quel sito l'applicazione di uno standard di responsabilità più severo, come quello per gli editori-fornitori di contenuti[66]. La necessità di mantenere distinti gli standard di responsabilità derivava dall'esigenza di favorire il più possibile la diffusione di nuove "agorà virtuali", che potessero ospitare e rilanciare contenuti di terzi, anche creati dagli stessi individui-utenti. In questa prospettiva, equiparare le piattaforme ai creatori di contenuti avrebbe fortemente penalizzato il disegno di favorire l'esercizio della libertà di espressione nel cyberspazio. L'assenza di responsabilità editoriale in capo ai prestatori di servizi fu ritenuta la formula più funzionale a questo scopo. Del resto, l'imposizione di una responsabilità "diretta" per i contenuti pubblicati da terzi avrebbe fortemente scoraggiato il *business* delle piattaforme di condivisione di contenuti. Come la Corte d'Appello per il Quarto Circuito affermerà nel 1997 nel caso *Zeran*: «*The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems*»[67]. Non solo questa opzione avrebbe reso

---

[62] J. KOSSEFF, *The Twenty-Six Words That Created the Internet*, Cornell University Press, Ithaca-Londra, 2017.

[63] Recentemente, E. GOLDMAN, *Why Section 230 Is Better Than the First Amendment*, in *Notre Dame Law Review Reflection*, fasc. 95, 1, 2019, 33 ss.

[64] V. J. MATHEWS, *Trump vs. Twitter*, in *Verfassungsblog*, 30 maggio 2020; G. DE GREGORIO- R. RADU, *Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech,* in *medialaws.eu,* 6 giugno 2020.

[65] Corte Suprema di New York 24 maggio 1995, *Stratton Oakmont c. Prodigy*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995).

[66] Solo pochi anni prima, in realtà, la Corte distrettuale degli Stati Uniti d'America per il distretto meridionale di New York, nel caso 29 ottobre 1991, *Cubby, Inc. c. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), era parsa assecondare una qualificazione come *distributor* delle piattaforme online, immaginando un parallelismo al livello di controllo dei contenuti tipico di edicole, biblioteche e librerie.

[67] Corte d'appello federale degli Stati Uniti d'America per il Quarto Circuito 2 ottobre 1997, *Zeran c. America Online, Inc.*, 129 F. 3d 327 (4th Cir. 1997).

fortemente sconveniente un'attività come quella dei fornitori di servizi, ma, altresì, avrebbe comportato conseguenze poco desiderabili sul piano della libertà di espressione, sottoponendo la libera circolazione di contenuti online al vaglio inevitabilmente preventivo (teso a evitare una responsabilità per contenuti illeciti) delle piattaforme. In questo modo, si sarebbe delineato un quadro tutt'altro che favorevole alla realizzazione di un *marketplace of ideas* digitale[68]. Naturalmente, il margine di intervento delle piattaforme è rimasto intatto, nella fase successiva legata alla scelta di moderare contenuti: la differenza fondamentale si colloca, tuttavia, nell'assenza di vincoli legislativi che lasciano così "liberi" i prestatori di servizi di agire (verosimilmente, in un senso maggiormente conforme allo spirito del Primo emendamento[69]). L'espansione della *content moderation* a contenuti "politici o religiosi" generalmente protetti dal Primo Emendamento[70] ha portato parte della dottrina[71] a mettere in dubbio che questa evoluzione della Sezione 230 sia in linea con l'intento del legislatore del 1996.

Ebbene, tuttavia, le basi portanti, prima descritte, a fondamento della Sezione 230 sembrano oggi non avere più un supporto granitico. Gli indizi di questo cambio di prospettiva sembrano essere confermati dal caso *Gonzalez c. Google*[72], dove la Corte Suprema ha, sostanzialmente, deciso di non decidere. Infatti, in una sentenza di appena tre pagine, la Corte non si è pronunciata sull'applicabilità della Sezione 230, ritenendo che, oltre alla piena sovrapponibilità della questione a quella decisa nel caso *Twitter, Inc. c. Taamneh*[73], la domanda di risarcimento del danno non risultava «plausibile» in considerazione dell'assenza di adeguate allegazioni da parte dei ricorrenti. È coerente con questo cambio di prospettiva anche una recente sentenza pronunciata dal Terzo Circuito[74], dove si è chiarito che la Sezione 230 offre un'immunità alle piattaforme digitali limitatamente all'attività realizzata da terzi (*third-party speech*), ma non rispetto al proprio contenuto espressivo.

Da ultimo, tale "impostazione" della Sezione 230 è stata riaffermata nella sentenza *Moody v NetChoice, LLC and NetChoice, LLC v. Paxton* che, pur rimandando la questione ai circuiti federali per quanto riguarda le "*facial challenges*" delle legislazioni di Texas e Florida

---

[68] Rispetto alla inidoneità di questa metafora a rappresentare efficacemente il mondo di Internet, soprattutto a fronte della sua «piattaformizzazione» sia consentito il rinvio a A. MORELLI- O. POLLICINO, *Le metafore della Rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto,* in *Rivista AIC,* fasc. 1, 2018, 1 ss.; O. POLLICINO, *Fake News, Internet and Metaphors (to Be Handled Carefully*), in *Italian Journal of Public Law,* fasc. 9, 1, 2017, 1 ss.

[69] V. G. BOGNETTI, *La libertà d'espressione nella giurisprudenza nord-americana: contributo allo studio dei processi dell'interpretazione giuridica*, Istituto Editoriale Cisalpino, Milano, 1958; F. ABRAMS, *The Soul of the First Amendment: Why Freedom of Speech Matters*, Yale University Press, New Haven, 2017.

[70] Come sottolineato dal Justice Thomas: «*But from the beginning, courts have held that §230(c)(1) protects the exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content*» Statement of Justice Thomas respecting the denial of certiorari, *Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 16 (2020)*).

[71] A. CANDEUB, E. VOLOKH, *Interpreting 47 U.S.C. Sec. 230(c)(2)*, 1 *Journal of Free Speech Law*, 2021.

[72] Corte Suprema federale degli Stati Uniti d'America 18 maggio 2023, *Reynaldo Gonzalez, et al., Petitioners c. Google LLC*, in 598 U. S. (2023).

[73] Corte Suprema federale degli Stati Uniti d'America 18 maggio 2023, *Twitter, Inc., Petitioner c. Mehier Taamneh, et al.*, in 598 U. S. (2023).

[74] Corte d'appello federale degli Stati Uniti d'America per il Terzo Circuito 27 agosto 2024, *Tawainna Anderson c. Tiktok, Inc.; Bytedance, Inc.*, 22 F. 3d 3061 (3rd Cir. 2024).

sulla proibizione della censura sui social networks, ha cercato – nella opinione di maggioranza – di tutelare l'interpretazione tradizionale della Sezione 230[75].

Secondo l'orientamento della Corte Suprema[76], l'organizzazione algoritmica dei contenuti costituisce una forma di espressione per le piattaforme e, conseguentemente, tale attività non rientra nel perimetro di esenzione di cui alla Sezione 230. Più precisamente, secondo i giudici, quando le piattaforme sociali come Facebook o YouTube scelgono quali contenuti di terzi rimuovere in base ai loro termini di servizio o alle loro linee guida, fanno ciò nell'esercizio della propria libertà di espressione, tutelata nell'ordinamento statunitense dal Primo emendamento. Il riconoscimento di questa copertura costituzionale apre, come si è fatto notare[77] a conseguenze assai importanti, in un'epoca contrassegnata, da una parte, da campagne di disinformazione e conflitti transnazionali nei quali la propaganda gioca un ruolo strategico e, dall'altra, dalla trasformazione, che si è spesso evocata in queste pagine, delle grandi piattaforme digitali.

Le leggi di Texas e Florida, nate sulla scia delle controversie legate a Donald Trump, sono state esaminate dalla Corte Suprema per valutare se sanzionare la rimozione di account politici dalle piattaforme fosse una tutela contro l'arbitrio o una limitazione alla libertà di espressione delle stesse. Il verdetto ha cercato di risolvere il contrasto tra le corti d'appello, ma ha evitato il nodo cruciale: la compatibilità di questa visione con la Section 230, che esclude un ruolo editoriale delle piattaforme.

Dunque, anche alla luce dell'attuale assetto alla guida degli Stati Uniti, sarà necessario osservare lo sviluppo del dibattito, anche con riguardo alla libertà d'espressione: la Section 230, figlia di un'epoca in cui il web era agli albori, è ancora adeguata alla realtà delle attuali piattaforme dominanti? La sua revisione potrebbe alterare principi fondativi del costituzionalismo americano. Tuttavia, come ricordato da Justice Kagan, spetta al Congresso e non alla Corte ridefinire questa normativa, data la complessità della materia e l'evoluzione del digitale[78].

3.1. La prospettiva europea: la Direttiva e-Commerce *e la "direttiva madre" in tema di protezione dati quali emblema della prima stagione (nel bilanciamento tra innovazione e regolazione) di "liberismo digitale"*

L'idea di un *liberismo digitale* ha attraversato l'Atlantico e, sebbene l'Europa l'abbia adottata con qualche anno di ritardo, ha portato alla definizione di un quadro normativo volto

---

[75] «*But this Court has many times held, in many contexts, that it is no job for government to decide what counts as the right balance of private expression—to «un-bias» what it thinks biased, rather than to leave such judgments to speakers and their audiences. That principle works for social-media platforms as it does for others*». *Moody v. NetChoice, LLC and NetChoice, LLC v. Paxton*, 603 U.S. ___ (2024).

[76] Corte Suprema federale degli Stati Uniti d'America 1 luglio 2024, *Moody c. NetChoice, LLC*., 603 U. S. (2024).

[77] M. BASSINI *et al.*, *Il Primo Emendamento USA tutela le piattaforme la attribuisce loro un ruolo editoriale*, in *Il Sole 24 Ore*, 2024, in https://www.ilsole24ore.com/art/il-primo-emendamento-usa-tutela-piattaforme-e-da-loro-ruolo-editoriale-AFmB0MiC?refresh_ce=1

[78] A. ROBERTSON, *The Supreme Court is deciding the future of the internet, and it acted like it*, *The Verge*, 2023 https://www.theverge.com/2023/2/21/23608949/supreme-court-section-230-gonzalez-google-youtube-algorithm-oral-arguments.

a evitare che il modello di business dei "prestatori di servizi della società dell'informazione" diventasse economicamente insostenibile. L'approccio iniziale, improntato a un minimalismo regolatorio, mirava a favorire lo sviluppo dell'*e-commerce* e a stimolare l'innovazione tecnologica. [79]

Come già osservato in letteratura, i segni distintivi di questa fase si possono riscontrare in due testi legislativi fondamentali:[80] la Direttiva 95/46/CE,[81] che regola la protezione dei dati personali, e la Direttiva 2000/31/CE[82], nota come "Direttiva e-Commerce". La prima, adottata anni prima della Carta dei diritti fondamentali dell'Unione europea, ha gettato le basi per il successivo riconoscimento costituzionale sia al diritto alla riservatezza («Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni»[83]), sia al diritto alla protezione dei dati personali («Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano»[84]).

Osservando, quindi, il dato storico, ben si comprende perché la normativa contenuta nelle direttive menzionate non si caratterizzasse ancora per quella dimensione inerentemente costituzionalistica, orientata alla tutela di *privacy* e *data protection*, quali valori democratici e fondamentali, che avrebbe caratterizzato la successiva legislazione in materia, quanto, piuttosto, per una dimensione economica.[85]

Più precisamente, la normativa si concentrava sulla funzione della *data protection* nel favorire e garantire il corretto funzionamento del mercato interno, più che sulla tutela della privacy come valore fondamentale. Non a caso, il titolo stesso della direttiva richiamava la "libera circolazione" dei dati, ricollegandosi alle quattro libertà economiche dell'Unione.[86]

Questa impostazione emerge chiaramente dall'art. 1, che imponeva agli Stati membri di tutelare i diritti fondamentali, in particolare la vita privata, ma al contempo vietava restrizioni alla circolazione dei dati per motivi di protezione individuale. Si delineava così un equilibrio tra garanzie minime per gli individui e la necessità di favorire la mobilità economica dei dati. Il considerando 7 della Direttiva rafforzava questa visione, sottolineando che la mancanza di

---

[79] G. De Gregorio, *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, Cambridge University Press, Cambridge, 2022.

[80] G. De Gregorio, *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law*, fasc. 19, 1, 2021, p. 41–70.

[81] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 1995/281.

[82] 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»), GU L 2000/178.

[83] Carta dei diritti fondamentali dell'Unione europea del 18 dicembre 2000, G.U. 2000/C 364/01, art. 7.

[84] *Ibidem*, art. 8 (1). La norma, ai paragrafi 2-3, continua: «2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[85] De Gregorio, *The rise of digital constitutionalism in the European Union*, cit., 48; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Hart, Oxford, 2021, pp. 110-111.

[86] *Ibidem*, art. 1(2).

uniformità tra gli Stati membri avrebbe ostacolato la trasmissione dei dati, falsando la concorrenza e limitando l'efficacia dell'applicazione del diritto comunitario.[87]

Un'impostazione simile caratterizzava, altresì, la Direttiva *e-Commerce*, che di fatto è ancora in vigore, volta a facilitare lo sviluppo del mercato digitale interno riducendo le barriere legislative. Particolare attenzione era rivolta alla responsabilità degli intermediari digitali, che godevano di un regime giuridico favorevole: i provider potevano essere ritenuti responsabili solo in casi eccezionali e ben definiti, per evitare che un eccesso di obblighi giuridici soffocasse il nascente settore digitale.

Seguendo il modello statunitense, l'Unione da principio ha dunque privilegiato la tutela dell'iniziativa economica digitale, in un contesto in cui il cyberspazio era visto come una nuova frontiera del libero mercato delle idee. In questa fase, la regolazione minimale si basava sulla convinzione che la competizione tra comunità virtuali e la capacità del web di autoregolarsi avrebbero favorito l'innovazione, limitando la necessità di interventi normativi restrittivi.

4. Le ragioni di una metamorfosi e l'ascesa inarrestabile del "fattore algoritmico"

Di lì a poco, il paradigma regolatorio sarebbe cambiato radicalmente, riflettendo l'evoluzione tecnologica. Le grandi piattaforme digitali si sono trasformate da attori economici a *poteri privati*, rivelando l'inadeguatezza della disciplina antitrust. Il minimalismo regolamentare, fondato sull'idea di un mercato delle idee autoregolato, si è scontrato con la realtà di monopoli e oligopoli digitali, rendendo insufficiente un intervento *ex post*.

Ma perché il cyberspazio ha visto l'ascesa di questi poteri privati in competizione con quelli pubblici? Per comprenderlo, occorre guardare indietro e analizzare le prime trasformazioni che, già alla fine del secolo scorso, segnalavano questo cambiamento. [88]

Anzitutto, occorre fare riferimento a Lawrence Lessig, il quale ha evidenziato come la regolamentazione di condotte individuali, in un contesto come il cyberspazio, potesse svolgersi in modo appagante soltanto previa considerazione della intrinseca peculiarità di questa tecnologia, ossia della sua architettura, o meglio il suo *code. «Code is law»*, nelle parole di Lessig, indica la capacità di diverse matrici (tra cui le norme giuridiche) di incidere sulla regolamentazione delle condotte individuali, contribuendo sia direttamente sia indirettamente a dettare regole di condotta. Ebbene, se inizialmente, il potere decisionale si è spostato dal legislatore agli esperti informatici, con le prime normative che riconoscevano il ruolo centrale degli intermediari digitali, con la trasformazione delle grandi piattaforme in veri e propri "poteri privati" e l'ascesa del "fattore algoritmico", il processo di regolazione ha subito un ulteriore cambiamento.[89]

Da un lato, si è assistito alla delega agli attori privati di decisioni fondamentali sul bilanciamento tra diritti, come nel caso *Google Spain*, in cui la Corte di Giustizia ha affidato ai

---

[87] *Ibidem*, considerando 7. Dello stesso tenore il considerando 9, che sottolineava come, a seguito della direttiva, «gli Stati membri non potranno più ostacolare la libera circolazione tra loro di dati personali per ragioni inerenti alla tutela dei diritti e delle libertà delle persone fisiche, segnatamente del diritto alla vita privata».

[88] L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

[89] M. BASSINI, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali,* Aracne, Roma 2019.

motori di ricerca la valutazione delle richieste di diritto all'oblio. Dall'altro, questa delega si è estesa agli algoritmi stessi,[90] ai quali sempre più spesso viene demandata l'assunzione di decisioni con impatti rilevanti sulla società, dalla moderazione dei contenuti online alla sorveglianza digitale.[91]

Oggi, con l'IA generativa, l'architettura tecnologica non si limita più a eseguire istruzioni predefinite, ma definisce autonomamente criteri e regole, adattandosi e trasformandosi nel tempo. Non si tratta più solo di un'infrastruttura che facilita l'applicazione delle norme giuridiche, ma di un vero e proprio sistema che genera standard normativi propri, come ha notato De Gregorio parlando di *normative power* dell'intelligenza artificiale[92]. In questo scenario, il passaggio da *code is law* a *code as source of law* segna una nuova sfida per il diritto costituzionale, ponendo interrogativi sulla tenuta dello Stato di diritto di fronte a un potere tecnologico sempre più autonomo.[93]

5. 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 costringimenti statali, si è posta un'esigenza di regolazione coerente con le 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 Balkin[94], l'attuale contesto storico è dominato dall'avvenuta affermazione di una «società algoritmica», caratterizzata segnatamente da due fattori.

---

[90] Sul punto si veda E. Longo, *Giustizia digitale e Costituzione: Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, Franco Angeli Edizioni, Milano, 2023.

[91] C. Hill, Dutch judge causes storm by using ChatGPT for fact checking in judgment, 8 agosto 2024, https://legaltechnology.com/2024/08/08/dutch-judge-causes-storm-by-using-chatgpt-for-fact-checking-in-judgment/.

[92] G. De Gregorio, *The Normative Power of Artificial Intelligence*, in *Indiana Journal of Global Legal Studies*, fasc. 30, 2, 2023, p. 55–80.

[93] F. Paolucci, *From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights*, SSRN Scholarly Paper, Rochester, NY, 2024.

[94] 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, p. 1149.

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", ovverosia 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 insieme[95].

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 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 giustizia[96] 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.

6. 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*,

---

[95] L. VIOLANTE, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *Rivista di BioDiritto*, fasc. 1, 2022, p. 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».

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

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, 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»[97]. 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 Alexy[98], 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. [99]

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*, [100] dove l'art. 119 TCE (oggi art. 157 TFUE) sulla parità retributiva è stato reinterpretato per essere immediatamente applicabile nei rapporti tra privati. Questa sentenza ha avuto un impatto paragonabile a *Costa c. Enel*[101] per la supremazia del diritto UE e *Simmenthal*[102] 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

---

[97] T. WU, *La maledizione dei giganti: un manifesto per la concorrenza e la democrazia*, Il Mulino, Bologna, 2021, p. 10.

[98] R. ALEXY, *Teoria dei diritti fondamentali*, Il Mulino, Bologna, 2012, p. 570-571.

[99] BVerfGE, 7, 198, 15 gennaio 1958.

[100] 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 arret Defrenne. L'égalité de rétribution des travailleurs masculins e des travailleurs féminin*, in *Cahiers droit européen*, 1977, p. 180 ss.; W. VAN GERVEN, *Contribution dell'arret defrenne au development du droit comunitarie,* in *Cahiers droit européen*, 1977, p. 131 ss.; G. CATALANO SGROSSO, *Il principio della parità di trattamento tra lavoratori e lavoratrici nel diritto comunitario*, in *Rivista di diritto europeo*, 1979, p. 245 ss.

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

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

applicato in modo surrettizio gli artt. 7 e 8 della Carta dei diritti fondamentali, [103] rafforzando la tutela della privacy e della protezione dei dati nei confronti delle grandi piattaforme, anticipando la regolazione poi formalizzata con il GDPR[104].

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.

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 terzi. [105]

---

[103] 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, Editoriale Scientifica, Napoli, 2018, 264 ss.

[104] 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, Editoriale Scientifica, Napoli, 2018, 264 ss.

[105] 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».

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*,[106] che 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*».[107] 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»[108]; al contrario, questi non sarebbero altro che soggetti privati che adottano decisioni relative alla *governance* del proprio spazio.[109]

La metafora dei social network come nuova piazza pubblica è spesso evocata, ma assume un significato ben diverso quando implica conseguenze normative[110]. La giurisprudenza statunitense ha riconosciuto questa dimensione solo per gli *state officials*, considerando il blocco di utenti come una potenziale violazione del Primo Emendamento[111]. Inoltre, ha

---

[106] 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).

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

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

[109] BASSINI, *Libertà di espressione e social network, tra nuovi «spazi pubblici» e «poteri privati». Spunti di comparazione*, cit. 68.

[110] 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-Ratcliff c. Garnier*, in 601 U.S. 205 (2024).

[111] 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.).

chiarito che spazi privati possono acquisire una natura pubblica come *designated public forums*, trasformandosi in luoghi di espressione soggetti a vincoli costituzionali. [112]

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 crescente. [113]

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*[114] ha amplificato il ruolo delle Corti rispetto a legislativo ed esecutivo, aggravato dall'accelerazione 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.[115]

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 procedimentali. 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.

7. 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,

---

[112] 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-Ratcliff c. Garnier*, in 601 U.S. 205 (2024).

[113] 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.

[114] A. SLAUGHTER, *Judicial Globalization*, in *Virginia Journal of International Law*, fasc. 40, 2000, p. 1103 ss.

[115] *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.

temporaneamente assunto dalla Corte di giustizia, così avviando quello che è stata da più parti definita come la nuova stagione del "costituzionalismo digitale"[116] in Europa.

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*[117] 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 liberale[118].

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.

7.1. Protezione dati e regolamentazione dell'algoritmo

---

[116] G. De Gregorio, *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, Cambridge University Press, Cambridge, 2022; 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*, Routledge, Londra, 2022, p. 77-87; A. J. Golia, *Critique of digital constitutionalism: Deconstruction and reconstruction from a societal perspective*, in *Global Constitutionalism*, 2023, p. 1–31.

[117] Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, cit.

[118] F. de A. Duarte *et al.*, *Perspectives on digital constitutionalism*, in B. Brożek *et al.*, *Research Handbook on Law and Technology*, Elgar, Northampton, 2023.

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)[119] 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 contemperamento tra gli interessi economici alla libera circolazione dei dati e la tutela dei valori democratici e costituzionali[120], 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 umana[121]. 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 contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica»[122].

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"[123], 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

---

[119] 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.

[120] 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».

[121] 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, p. 307-312.

[122] GDPR, considerando 4.

[123] GDPR, art. 17.

tutela della *privacy* e di protezione dei dati – che derivino dalle loro attività e, conseguentemente, ad adottare i necessari correttivi per mitigare tali rischi[124]. Il Regolamento in questione ha, così, segnato un'evoluzione strutturale nell'approccio euro-unitario alla tutela dei 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'Unione[125].

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 eccezionali[126], 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 umana[127].

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

---

[124] 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, p. 473-500, spec. pp. 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*, Il Mulino, Bologna 2024, spec. p. 85.

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

[126] 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».

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

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 dignità[128].

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, ideologico, 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*)[129], ovverosia all'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 GDPR[130]. In ogni caso, l'opinione ormai prevalente è quella che riconosce nell'articolo 22 quanto meno *in nuce*[131], un diritto dell'interessato alla "spiegazione" sottesa alla decisione presa.[132] Una tale

---

[128] *Ibidem*., p. 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*».

[129] F. PASQUALE, *The black box society: the secret algorithms that control money and information*, Harvard University Press, Cambridge, Mass. - London, 2015.

[130] 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. pp. 3-4.

[131] FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit., spec. p. 83.

[132] Cfr. Cons. 71, GDPR.

direzione è stata recentemente ribadita dalla CGUE che, interpretando l'Art. 22 GDPR, ha stabilito per gli interessati il diritto a ricevere "informazioni signitificative 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 signitificative 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 tale interessato al fine di ottenerne un risultato determinato, come un profilo di solvibilità».[133]

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'algoritmo[134] 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.

7.2. 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)[135].

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 potere 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

---

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

[134] Sul punto si pensi alla importante della 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.

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

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.[136]

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»[137].

Un esempio può, forse, aiutare a fare emergere il valore aggiunto, almeno potenziale, che i meccanismi di garanzia procedimentale possono 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 Internet[138], 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

---

[136] 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.

[137] M. ZALNIERIUTE, *Technology and the Courts: Artificial Intelligence and Judicial Impartiality*, SSRN Scholarly Paper, Social Science Research Network, Rochester, NY, 2021.

[138] 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, p. 302–319.

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 Schultz[139] hanno sottolineato la necessità di inquadrare una forma di «*procedural data due process*». L'applicazione di una tale forma di procedura tecnologica avrebbe anche un impatto sui diritti di natura sostanziale, poiché essa dovrebbe preservare, in conformità con il modello di Redish e Marshal[140] di giusto processo, valori come l'accuratezza, l'equità, l'uguaglianza di *input*, la prevedibilità, la trasparenza, la razionalità e la partecipazione.

Citron[141] 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 Schultz[142], 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 fortezza europea meno isolata e più dialogante, evitando l'imperialismo digitale del "*Bruxelles effect*". Tale dimensione, e il principio del *due process* applicato alla sfera digitale, non sono affatto estranei al costituzionalismo statunitense.

8. Libertà di espressione online, moderazione dei contenuti e algoritmo

8.1. Le coordinate costituzionali

---

[139] 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, p. 93.

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

[141] D. K. CITRON, *Technological due process*, in *Washington University Law Review*, fasc. 85, 6, 2008, p. 1249.

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

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*[143], nella celebre *dissenting opinion* di Justice Holmes in *Abrams*[144] , 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. [145] Questo principio rafforza un approccio regolativo che privilegia il bilanciamento tra diritti, favorendo la costruzione di un quadro normativo più articolato.

Questa impostazione ha reso possibile l'adozione di interventi legislativi come il GDPR[146], la direttiva *Copyright*[147], e la revisione della Direttiva in tema di servizi media audiovisivi[148], 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.

8.2. 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 2000[149] 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

---

[143] *Reno c. Aclu* 521 U.S. 844 (1997), cit.

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

[145] Art. 17 CEDU e art. 54 Carta dei diritti fondamentali dell'Unione europea.

[146] GDPR, cit.

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

[148] 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.

[149] 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.

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 quadro.[150] Così, con la Direttiva (UE) 2018/1808[151], 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) 2019/790[152] ha innovato la materia del diritto d'autore per adeguare la normativa di settore alle nuove sfide di internet; mentre, il Regolamento (UE) 2021/784[153] 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.[154] 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*[155], 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)[156]. 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 concorrenza. Come è stato sottolineato fin dagli inizi, scopo ultimo era (ed è) quello di «addomesticare» i giganti del mercato digitale[157] 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

---

[150] E-Commerce Directive, considerando 42.

[151] Direttiva sui servizi di media audiovisivi, cit.

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

[153] Regolamento relativo al contrasto della diffusione di contenuti terroristici online, cit.

[154] O. POLLICINO- G. DE GREGORIO, *Constitutional Law in the Algorithmic Society*, in H.-W. MICKLITZ *et al.*, *Constitutional Challenges in the Algorithmic Society*, Cambridge University Press, Cambridge, 2021.

[155] 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.

[156] Regolamento sui mercati digitali, cit.

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

termini di opacità che emergono frequentemente nei meccanismi algoritmici propri dei nuovi poteri, attraverso la predisposizione soprattutto di garanzie procedurali[158].

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»[159].

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). [160] 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 della Direttiva *e-Commerce*, ma prevedendo sanzioni amministrative per la mancata osservanza delle nuove regole di diligenza. [161]

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). [162] 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.

8.3. (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). [163]

---

[158] Volendo, ora, O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, pp. 569–594.
[159] DSA, Capo III.
[160] DSA, artt. 15, 24, 39.
[161] *Ibidem*, art. 23(1).
[162] DSA, artt. 15, 24, 39.
[163] *Ibidem*, art. 17(3)(c).

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 extragiudiziali. Inoltre, il DSA preserva un principio personalistico, richiedendo alle piattaforme di garantire un'interazione umana nei processi decisionali e nei canali di comunicazione con gli utenti. [164]

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.

9. 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 applicazioni di intelligenza artificiale fondate sui *big data* e, dunque, manca di considerare il sempre più rilevante fenomeno dei trattamenti di dati di massa[165].

---

[164] 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 approaches: Connecting constitutional dots in the digital age*, cit.

[165] 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. FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit., pp. 86-87.

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 tecnologico[166]. 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»[167].

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 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 Stato[168] –, 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'allenamento[169]. 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 decisioni[170]. La definizione che l'AI Act dà di intelligenza artificiale, che sarà esaminata nel paragrafo

---

[166] 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, pp. 87–106.

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

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

[169] 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, pp. 1–39.

[170] *Ibidem*.

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.

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.

10. 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 artificiale[171]. 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 Commissione[172].

Il nuovo Regolamento contiene al suo interno una definizione del concetto stesso di intelligenza artificiale, che, essendo stata elaborata 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»[173].

---

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

[172] 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.

[173] 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

La definizione di IA contenuta nel Regolamento riprende quella già elaborata dall'Organizzazzione per la Cooperazione e lo Sviluppo Economico (OECD)[174]. A differenza dall'approcio "controfattuale" proposto da Floridi,[175] 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.[176] 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 rispetto alla distinzione tra sistemi di intelligenza artificiale e software tradizionali avanzati.[177]

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,[178] 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

---

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.

[174] 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.

[175] 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*, Oxford University Press, 2023.

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

[177] 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.

[178] 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.

strategie elusive, con aziende che classificano i propri prodotti come software tradizionali per evitare gli oneri normativi.

Come si è avuto modo di osservare altrove[179], l'AI Act si caratterizza per l'adozione di un approccio basato su un rischio radicalmente diverso 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 regolati[180].

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 della 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 Regolamento.[181] 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 danno[182]. Non 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 pratica[183].

Al secondo "livello", [184] 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

---

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

[180] FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit. pp. 121-122.

[181] Come per la definizione di IA, la Commissione Europea ha, altresì, adottatto 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.

[182] AI Act, art. 5.

[183] 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.

[184] AI Act, art. 6 e Allegato III.

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 biometrica,[185] 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 europeo. [186]

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 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 contenuti[187] 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 dannoso [188], 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 realtà. [189]

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.[190]

---

[185] 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.

[186] 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.

[187] 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*, Bocconi University Press, Milano, 2024.

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

[189] AI Act, art. 50(4).

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

10.1. 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)[191], comunemente noti anche 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 momento[192].

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 regolatorio[193], a causa delle implicite difficoltà connesse al necessario contemperamento 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 democratici[194]. 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 *carnet* 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 fondamentali[195].

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'Unione[196], in quanto abbiano portata

---

[191] «*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 (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.)

[192] 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.

[193] BOMMASANI *et al.*, *On the Opportunities and Risks of Foundation Models*, cit.

[194] 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.

[195] Esemplificativo 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 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/.

[196] 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

significativa all'interno dell'Unione stessa o implichino «effetti negativi effettivi e ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso»[197]. Sono tali, in particolare, quei modelli che presentino "capacità di impatto elevato", ovverosia «capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati»[198], da valutarsi «sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento»[199], 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 GPAI[200].

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, visivi o multimodali, rappresentano strumenti estremamente potenti per la generazione di contenuti. Come ha notato Dunn[201], 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 Instagram[202].

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?***[203] 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

---

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.

[197] *Id*.

[198] AI Act, art. 3(64).

[199] *Ibidem*, art. 51(1)(a).

[200] *Ibidem*, 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.

[201] DUNN, in POLLICINO-DUNN, *Intelligenza Artificiale e Disinformazione*, cit.

[202] 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, pp. 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/.

[203] 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.

anche alla loro soluzione: qual è lo statuto giuridico di questi contenuti? Come evidenziato da Bassini in un recente contributo[204], si tratta di stabilire se le creazioni di questi sistemi di intelligenza artificiale possano aspirare a una tutela costituzionale 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 artificialmente[205]: 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.

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

Le premesse su cui poggi l'Act erano portatici 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 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

---

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

[205] *Ibidem.*

divergenze tra gli Stati membri.[206] 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 professionali[207]. 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 sviluppare 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 standard[208].

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 interesse[209]. L'autovalutazione, senza un'adeguata supervisione indipendente, potrebbe portare a una sottostima dei rischi, riducendo l'efficacia delle misure di tutela[210]. 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 indipendente[211]. La creazione

---

[206] 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.

[207] 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.

[208] F. PALMIOTTO, *The AI Act Roller Coaster: How Fundamental Rights Protection Evolved in the EU Legislative Process*, SSRN Scholarly Paper, Rochester, 2024.

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

[210] 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.

[211] 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.

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 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)[212]. Secondo l'AI Act, il FRIA è uno strumento chiave per valutare l'impatto dei sistemi di IA ad alto rischio sui diritti fondamentali[213]. 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 Mercato[214].

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)[215]. 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 fare[216], 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 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 diritto[217]) 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

---

[212] AI Act, art. 27.

[213] 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/.

[214] AI Act, art. 27(3).

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

[216] 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.

[217] C. giust. UE 27 febbraio 2018, *Associação Sindical dos Juízes 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.

IA[218], questa spiegazione risulta spesso superficiale, mancando della trasparenza necessaria per consentire agli individui di contestare efficacemente tali decisioni. Come è stato evidenziato[219], 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 adeguato[220]. 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 alla giustizia più efficace: promessa che dovrebbe essere mantenuta in forza dell'Art. 47 della Carta[221].

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 decisioni[222].

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 DSA[223]. 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 di quella che ha caratterizzato la reazione alla stagione dell'automazione (algoritmica).

---

[218] AI Act, art. 86.

[219] G. De Gregorio- S. Demkova, *The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe*, SSRN Scholarly Paper, Rochester, 2024.

[220] 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, pp. 210–236.

[221] 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*, Aracne, Roma, 2024, pp. 499–513.

[222] 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.

[223] 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, pp. 53-57.

11. 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 costituzionali[224], 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*[225].

L'approccio basato sul rischio, infatti, permette di porre al centro non tanto regole rigide quanto obblighi di identificazione, valutazione e gestione dei rischi specifici[226]. 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 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 misure[227]. 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

---

[224] PEREZ- WIMER, *Algorithmic Constitutionalism*, cit.

[225] R. GELLERT, *The risk-based approach to data protection*, Oxford University Press, 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.

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

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

evolutiva che in molti casi solo i destinatari stessi delle norme sono in possesso delle conoscenze necessarie a svolgere il compito normativo»[228].

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 privati[229], 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 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 paradigmatico[230]. 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 illiberali[231]. 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 grandi[232].

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 sistemici[233]. 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

---

[228] 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.

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

[230] POLLICINO - DUNN, *Intelligenza Artificiale e Disinformazione*, cit.

[231] C. T. MARSDEN, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge, 2011.

[232] DSA, Considerando 104.

[233] *Ibidem*, art. 45(1).

privati, ma anche in una normativa. Come sottolineato dal DSA Act, 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 DSA[234]. 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 Torchia[235].

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 contenuti[236]. 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 DSA[237]. 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 politica[238].

In un tale contesto, l'approccio dell'Unione sembra sempre più distinguersi 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,[239] 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 europei[240]. Seppur restino domande

---

[234] *Ibidem.*

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

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

[237] DSA, art. 40.

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

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

[240] DRAGHI, *The future of European competitiveness*, cit.

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.