Regolazione e innovazione tecnologica nell' "ordinamento della rete"

Oreste Pollicino*

DRAFT

Sommario: 1. Introduzione e struttura del percorso di indagine. 2 Coordinate della ricerca e una guida per la lettura. 2.1 Assenza di potere: la promessa tradita. 2.2. Limitazione del potere. 2.3. Separazione tra poteri. 2.4 Base giuridica rilevante e fonti del diritto: forma e sostanza del diritto costituzionale europeo 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 irresistibile 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 e un nuovo equilibrio tra regolazione e innovazione tecnologica. – 8. Protezione dei dati e regolamentazione dell'algoritmo. – 8.1 Il passaggio da una dimensione (esclusivamente) assiologico-sostanziale a una (anche) di matrice procedurale: coordinate teoriche e applicative. – 9 Libertà di espressione online, moderazione dei contenuti e algoritmo. – 9.1. Le coordinate costituzionali. – 9.2. Dalla Direttiva e-Commerce alla nuova stagione regolativa (DSA) della moderazione dei contenuti in rete. – 9.3 (Segue) L'algoritmo nel DSA. – 10. Dall'algoritmo all'intelligenza artificiale: il magistero dell'Artificial Intelligence Act. – 10.1 Il nuovo Regolamento europeo sull'intelligenza artificiale: gli elementi portanti del nuovo sistema di regolazione. – 10.2. L'esplosione dell'intelligenza generativa e i nuovi rischi per stato di diritto e democrazia: alcune definizioni di base. 10.3 L'AI Act allo specchio: supera il test del costituzionalismo europeo? 11. Prospettive evolutive del modello di regolazione del digitale in Europa.

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

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

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

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 grande 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 algoritmo? 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 (AIA), 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.

Questa la struttura che si propone di seguire.

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,

---

[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.

[4] Nel significato kantiano di self-governance, caratteristica che non ha invece l'automazione.

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].

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

[5] J. P. BARLOW, *A Declaration of the Independence of Cyberspace*, Davos, 8 febbraio 1996.

[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 cronologico (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.

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 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.

---

[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, Instituzioni, 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.
[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. GOLDSMIT - 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.

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 – 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 guardate 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.

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?

---

[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.

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].

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

---

[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.

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].

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

---

[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)

[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, AIA), GU L, 2024/1689.

[27] AI Act, art. 7.

[28] "Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato III aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati nell'allegato III; b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali, e tale rischio è equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III."

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?

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 il merito di tale regolazione, avendo spesso un carattere verticale, sarà di competenza di studiosi, volta per volta, di diritto d'autore, protezione dati, audiovisivo e, per l'appunto, intelligenza artificiale, al contrario, la scelta della fonte da utilizzare e ancor prima l'identificazione della base giuridica, nei Trattati dell'Unione, più idonea per identificare la competenza di quest'ultima a legiferare in merito, è evidentemente un tema 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)*"[30].

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 in tema di riavvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri, che hanno per oggetto l'instaurazione e il funzionamento del mercato interno. 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[31] e dal Regolamento sulla trasparenza della pubblicità politica[32], 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.

---

[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] 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".

[31] 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.

[32] 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.

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 in materia di mercato unico. Disposizione che, evidentemente e inevitabilmente, 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, è sempre più evidente come mercato unico e stato di diritto non possano che essere due facce della stessa medaglia nel processo di integrazione europea, e, ovviamente, non solo con riferimento alla dimensione digitale. Basti riprende quanto affermato da Andrea Simoncini sul punto, quando ha ricordato che "*la disciplina della tecnologia digitale all'interno dell'Unione europea nasce originariamente connotata da quelli che sono spesso definiti come twin objectives (obiettivi gemelli), anch'essi tipici del modello europeo: da un lato, favorire lo sviluppo del mercato unico delle nuove tecnologie, considerato un fattore trainante della crescita economica e del benessere sociale; dall'altro, per la crescente pervasività di questi sistemi tecnici e la loro connessione con la sfera delle libertà fondamentali, garantire un elevato livello di protezione dei diritti individuali e collettivi*"[33].
Con riferimento alla seconda questione accennata, ossia la corretta identificazione delle fonti di diritto derivato di natura vincolante per realizzare l'obiettivo della disciplina legislativa prevista, vi è stata una discrepanza tra forma e sostanza nella scelta tra una direttiva di armonizzazione (massima o minima) e un regolamento che dovrebbe tendere all'uniformità. Questo scollamento è emerso particolarmente nella stagione di regolazione evocata, con specifico riferimento al GDPR e all'AI Act. In altre parole, le normative proposte dalla Commissione e successivamente approvate dai co-legislatori dell'Unione come regolamenti si sono spesso rivelate, a causa dell'elevato numero di clausole aperte, delle vere e proprie "direttive mascherate". Queste normative hanno richiesto (come nel caso del GDPR) e richiederanno (come nel caso del recente AI Act) un recepimento interno. In pratica, pur essendo formalmente regolamenti, necessitano di un adeguamento dell'ordinamento statale al regime previsto dalla fonte dell'Unione attraverso l'adozione di una legislazione nazionale. Evidente, quindi, il rischio di frammentazione e di mancata realizzazione dell'obiettivo dell'uniformità esplicitamente dichiarato dal legislatore dell'Unione nel motivare il passaggio dalla direttiva al regolamento, come nel caso della disciplina adottata in materia di protezione dei dati personali.

1.5 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

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

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"[34].
Al contrario, come si è fatto notare in uno studio di dieci anni fa[35], 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 national law, in which not only a global approach, but also a transnational one risks proving not to be fully adequate*"[36].
Sempre rispetto alla prospettiva spaziale qui rilevante, sull'altra sponda dell'Atlantico, non sono mancate alcune spinte giurisprudenziali volte a fare emergere come, al di là di dove si trovi la base informatica dei nuovi poteri digitali, se quest'ultimi forniscono i loro servizi anche nei confronti del mercato digitale europeo, devono sottostare alla normativa, e, quindi, al sistema valoriale, proprio delle tradizioni costituzionali comuni del vecchio continente. Ovviamente tale giurisprudenza ha un *humus*, e non poteva essere diversamente, diverso da quello che ha caratterizzato la giurisprudenza statunitense che ha reagito alla prospettiva anarcoide prima descritta. Se il terreno privilegiato di quest'ultima non poteva che essere la protezione della libertà di espressione, la giurisprudenza rilevante di Lussemburgo si concentra, e anche in questo caso (visto il diverso paradigma assiologico che caratterizza le due sponde dell'Atlantico) sulla protezione dei dati personali, considerato il Primo emendamento del costituzionalismo europeo.[37]
In questo particolare settore, la giurisprudenza della Corte di giustizia ha segnato un'evoluzione che rappresenta, oltre al chiaro primato che la privacy sembra vantare al cospetto di altri diritti tutelati, e, in teoria, pari-ordinati, l'idea che, al di là della dematerializzazione dei trattamenti di dati, i diritti degli individui e i confini territoriali "posti a loro tutela" possiedono ancora un rilievo.
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*[38]. 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

---

[34] 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.
[35] 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.
[36] *Ibidem*, 347.
[37] B. PETKOVA, *Privacy as Europe's first Amendment,* in *European Law Journal*, fasc. 25, 2, 2019, p. 140 ss.
[38] 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.

nella direttiva 95/46/CE[39]. La Corte di giustizia ha così anticipato il GDPR[40], 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 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". [41] 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 due *imperi digitali*, gli Stati Uniti e l'Unione europea[42].

Si dirà tra un momento del rischio di un *Bruxelles effect reloaded* per quanto riguarda la regolazione dell'intelligenza artificiale; tali riflessioni, però fanno emergere come, territorio, spazio e sovranità sono categorie vive e vegete nel contesto digitale. Nessuno scardinamento, ma caso mai, come si anticipava, una rimodulazione.

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*[43] in cui la Corte di Giustizia ha annullato la direttiva in materia di *data retention*[44] del 2006, perché in contrasto con la Carta dei diritti fondamentali. Infatti, secondo i giudici di Lussemburgo, "tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente". Qui si è ben oltre la questione dell'identificazione della legge applicabile, essendo il tema rilevante "tecnicamente" territoriale, a dimostrazione che anche questa categoria fondamentale del diritto costituzionale è, come si diceva, viva e vegeta nel cyberspazio, a dispetto dei tentativi di immaginare uno spazio virtuale con (non) regole e categorie autonome rispetto al mondo analogico.

Più recentemente, a questo proposito, si è posto il tema dell'effetto extraterritoriale di alcune normative europee (con l'*humus* assiologico sostanziale di riferimento che, ovviamente, si portano dietro) e, in particolare del GDPR e, assai recentemente, dell'AI Act.

---

[39] 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.

[40] 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.

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

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

[43] 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.

[44] 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.

Al di là di quanto si dirà nella seconda parte di questo scritto su come tali due normative non solo a democratizzare [45], ma anche costituzionalizzare "il fattore algoritmico", va in questa sede fatta una precisazione circa il cd. Bruxelles effect[46], derivante dalla presunta – e in certi casi effettiva – capacità del modello normativo e valoriale europeo in tema di regolazione del digitale di essere esportato in altre aree regionali quale parametro di riferimento per legislazioni settoriali. A questo proposito, se tale meccanismo di *legal traplants*[47] ha funzionato in parte per il GDPR, in quanto si trattava di un esercizio di massimizzazione della tutela di un diritto fondamentale, rischia di non funzionare per l'AI Act, poiché, in questo caso, non vi è un diritto fondamentale specifico da tutelare, ma si propone un modello di regolazione, fondato sui valori comuni europei come lo stato di diritto. Si fa particolare riferimento, almeno secondo l'impostazione della Commissione europea, a una visione che guarda principalmente al mercato e alla sicurezza, rispetto all'immissione all'interno del mercato unico europeo dell'*output* finale dei modelli di intelligenza artificiale.
Si tratta, dunque, di uno dei possibili modelli di regolazione, accanto a tanti altri alternativi che sono più rispondenti ai valori locali di altre aree regionali, a cominciare – con tutte le dovute differenze – da Stati Uniti e Cina. Aree regionali che non sono disposte, come è successo per il GDPR, a subire il *Bruxelles effect*, anche con riguardo alla regolamentazione dell'intelligenza artificiale. Il che vuol dire non agire solo di rimessa, come è capitato l'appunto con il GDPR per alcuni Stati degli USA (per esempio, la California[48]) e con un'operazione di *macquillage* molto più formale che sostanziale per la Cina[49], ma, al contrario, promuovere un modello, per forza di cosa alternativo, essendo assai diverso l'*humus* costituzionale di riferimento.
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.

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

---

[45] DE GREGORIO, *Democratising online content moderation: A constitutional framework*, cit.
[46] A. BRADFORD, *The Brussels effect : how the European Union rules the world*, Oxford University Press, Oxford, 2020.
[47] R. SACCO, *Legal Formants: A Dynamic Approach to Comparative Law*, in *The American Journal of Comparative Law*, fasc. 39, 1, 1991, p. 1-34.
[48] CA Civ Code § 1798.192 (2023) (California Consumer Privacy Act of 2018).
[49] Personal Information Protection Law of the People's Republic of China, passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021.
[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/la-lettera/12-2023-liberta-di-ricerca-e-intelligenza-artificiale/la-sfida-dell-intelligenza-artificiale.

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.

Riconoscendo, infatti, che molti dei rischi relativi all'IA sono intrinsecamente di natura internazionale e, quindi, possono essere affrontati in modo adeguato solo attraverso la cooperazione internazionale, la Dichiarazione contiene l'impegno, preso dai paesi partecipanti, a lavorare insieme in modo "inclusivo", allo scopo di realizzare un paradigma tecnologico antropocentrico e fondato su una IA affidabile, responsabile e sicura. Inoltre, la Dichiarazione promuove l'obiettivo di incentivare una maggiore trasparenza da parte degli attori privati impegnati nel mercato dell'IA.

Sotto il profilo sostanziale, inoltre, la Dichiarazione chiarisce tre punti fondamentali: in primo luogo – di fondamentale interesse per lo sviluppo economico globale – che l'IA sia affidabile e trasparente, a prescindere dal soggetto che la metta a disposizione degli utenti o da chi ne faccia uso; in secondo luogo, che il *focus* preminente debba essere sulle misure tecnologiche volte ad assicurare un'IA affidabile e che solo in via secondaria occorra intervenire attraverso la definizione di regole normative o comportamentali; in terzo luogo, che la predisposizione di idonee garanzie tecnologiche spetti sostanzialmente agli operatori e fornitori dei servizi di IA[54]. In altre parole, la Dichiarazione di Bletchley sembra porsi in un'ottica focalizzata *in primis* sull'attenta valutazione e implementazione di adeguati accorgimenti tecnici e solo *in secundis* sull'adozione di misure legislative e regolative.

Risale, tra l'altro, al medesimo periodo in cui veniva adottata la Dichiarazione di Bletchley la pubblicazione negli Stati Uniti di un ordine esecutivo (*Executive Order*, EO) del Presidente Joe Biden dedicato, precisamente, all'implementazione di nuovi standard per la sicurezza di sistemi di IA, alla protezione del diritto alla privacy dei cittadini statunitensi, alla promozione dei diritti civili e del principio di uguaglianza, alla tutela dei diritti dei consumatori e dei lavoratori, nonché alla promozione di innovazione e competizione nel mercato dell'IA[55]. Come sottolineato da Pizzetti[56], l'EO statunitense si caratterizza per il fatto di essere stato adottato a valle di una lunga attività di messa a punto che ha visto la partecipazione diretta delle imprese leader del settore, al fine di promuovere una strategia condivisa tra attori pubblici e privati nella promozione di un'innovazione tecnologica responsabile. In tal senso, l'approccio seguito dal Presidente degli Stati Uniti appare essere pienamente coerente con la Dichiarazione di Bletchley – forse ancor più di quello cristallizzato, a livello euro-unitario, nell'AI Act.

Se l'Unione, con l'AI Act, sembra mirare allo sviluppo di un quadro legislativo unitario per l'IA a livello orizzontale, direttamente applicabile in tutti gli Stati Membri, l'EO rivela una diversa scelta: quella di fondare la propria azione, prima che sull'adozione a livello federale di un atto legislativo sull'IA, direttamente sul potere esecutivo del Presidente, con l'obiettivo specifico di incentivare da parte dei diversi dipartimenti dell'esecutivo la formulazione di standard, linee guida, buone pratiche e regolamentazioni di comune accordo con l'industria stessa. Tale modello statunitense sembra, invero, porre il rischio dell'emergere di standard diversi a seconda del settore di intervento – del resto, l'approccio "per settori" ha da lungo caratterizzato la strategia degli USA in

---

[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/.

[56] PIZZETTI, *Attenzione, il mondo sceglie un approccio diverso da quello UE*, cit.

materia di IA – ma evita, d'altro canto, le criticità con riferimento all'AIA, relative alla mancanza di una sufficiente flessibilità[57].

Occorre, peraltro, sottolineare come l'EO di Biden, sebbene rappresenti la reazione più rilevante all'avanzamento delle tecnologie di IA nel contesto statunitense, non è l'unica iniziativa che si è avuta al di là dell'Oceano. In effetti, la questione della regolamentazione dell'IA è stata affrontata da numerosi stati federati, i quali hanno provveduto ad adottare propri atti legislativi in tale settore[58]. Inoltre, è da segnalare, a livello federale, l'avvio e la prosecuzione di lavori interni al Congresso da parte di una commissione di senatori *bipartisan*, impegnati, in particolare, nella predisposizione di linee guida e azioni legislative in materia di IA. Tra l'altro, una delle maggiori preoccupazioni sollevate dalla commissione si riferisce precisamente al potenziale impatto dell'IA nel contesto di processi democratici ed elezioni[59].

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[60].

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'AIA 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 rilevanze 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, si proverà a riflettere su quali, agli albori del web, siano state le ragioni che hanno definito, laddove internet è nato (gli Stati Uniti), un iniziale equilibrio tra innovazione tecnologica e (mancata) regolazione, per, poi, provare a ricostruire cause ed effetti del cambio di passo, con riferimento specifico all'Unione europea in termini di (iper?) regolazione. Si guarderà alle varie stagioni rilevanti in questo contesto,

---

[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] Si pensi, ad esempio, alla California che ha elaborato diverse proposte, tra cui la *Generative artificial intelligence: training data transparency* (AB-2013), la *Safe and Secure Innovation for Frontier Artificial Intelligence Models Act* (SB-1047) e la *California AI Transparency Act* (SB-942), già approvate dal Senato e dall'Assemblea ad agosto 2024. Sulla stessa linea, si pone il Colorado, dove sono entrati in vigore nella primavera/estate del 2024, il *Candidate Election Deepfake Disclosures* (HB24-1147) e il *Consumer Protections for Artificial Intelligence* (SB24-205). Per una dettagliata analisi della regolamentazione statale in materia di IA, si rimanda a *US state-by-state AI legislation snapshot*, *BCLP - Bryan Cave Leighton Paisner*, 2024, https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html .

[59] U. PERANO, *Bipartisan group of senators unveil long-awaited guidance on AI bills*, *POLITICO*, 2024, https://www.politico.com/live-updates/2024/05/15/congress/schumers-roadmap-on-ai-bills-00157828.

[60] 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/.

dal liberismo al costituzionalismo digitale e a come le politiche di regolazione si siano modificate in reazione al mutato assetto tecnologico e valoriale.
Tali processi trasformativi saranno esaminati guardando quale bussola di orientamento, da una parte, alla crescente emarginazione del "fattore umano" nel funzionamento delle nuove tecnologie digitali e, dall'altra, all'ascesa inarrestabile del "fattore algoritmico", per cercare di comprendere quali siano state le scelte di politica del diritto che il costituzionalismo europeo ha provato a suggerire in reazione a dette, rispettivamente, emarginazione e ascesa. Infine, si proverà a guardare attraverso la nuova frontiera del laboratorio tecnologico cui il fattore umano sembra – a volte soltanto apparentemente[61] – scomparire in maniera totale, ossia l'ecosistema dell'intelligenza artificiale, specie di carattere generativo, fortemente distinta dalla semplice automazione algoritmica. In particolare, ci si chiederà se lo sforzo regolatorio, assai ambizioso e recente dell'Unione confluito nell'AI Act, sia in linea con la bussola valoriale del costituzionalismo europeo. Le riflessioni finali saranno dedicate a identificare gli elementi fondamentali di quella che sembra essere la base portante del tentativo di conciliare innovazione e regolazione, con particolare riguardo alla protezione dei diritti fondamentali, nell'ultima frontiera che sta caratterizzando l'evoluzione (o involuzione) dell'ordinamento della rete in Europa. Il riferimento, in particolare, è alla cd. co-regolamentazione, quale terza via tra *hard* e *soft law* e alle politiche di regolazione fondate sulla gestione del rischio.

2. 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[62] e coloro che hanno contestato i presupposti normativi e descrittivi di questa tesi[63]. 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[64]), il legislatore

[61] Proletari digitali completo io questa nota
[62] D.R. JOHNSON- D. POST, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review,* fasc. 48, 5, 1996, 1371 ss.
[63] J.L. GOLDSMITH, *Against Cyberanarchy,* in *University of Chicago Law Review*, fasc. 65, 4, 1199 ss.
[64] 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*

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 si andava celebrando al cospetto dell'avvento di Internet[65]. 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[66], 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[67], costituì il risultato di una mozione *bipartisan* per evitare questo paradosso, ben visibile nella sentenza *Stratton Oakmont v. Prodigy*[68] 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[69]. 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*" [70]. Non solo questa opzione avrebbe reso 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

---

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".

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

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

[67] 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.

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

[69] 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.

[70] 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).

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[71]. 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[72]). L'espansione della *content moderation* a contenuti "politici o religiosi" generalmente protetti dal Primo Emendamento[73] ha portato parte della dottrina[74] 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*[75], 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*[76], 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[77], 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 sulla proibizione della censura sui social networks, ha cercato – nella opinione di maggioranza – di tutelare l'interpretazione tradizionale della Sezione 230[78].

Secondo l'orientamento della Corte Suprema[79], 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

---

[71] 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.

[72] 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.

[73] 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)*).

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

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

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

[77] 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).

[78] "*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).

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

espressione, tutelata nell'ordinamento statunitense dal Primo emendamento. Il riconoscimento di questa copertura costituzionale apre, come si è fatto notare[80] 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.

Sull'onda emotiva delle vicende che hanno interessato tempo addietro Donald Trump, le leggi adottate da Texas e Florida sono così finite al vaglio della Corte suprema in relazione alle previsioni che, tra le altre, sanzionavano le piattaforme che avessero rimosso account riconducibili a candidati a cariche politiche o loro manifestazioni di pensiero. Un modo per evitare che la libertà di moderazione delle piattaforme potesse degenerare in arbitrio o un limite inaccettabile alla loro libertà di espressione? Questo il grande interrogativo al centro della sentenza della Corte suprema, che ha esaminato i due casi congiuntamente nel tentativo di superare anche le divisioni tra le corti d'appello federali, che avevano raggiunto esiti opposti nell'*iter* di impugnazione delle due leggi. E, anche volendo considerare il quadro di contenuti disponibili su una piattaforma per effetto delle attività di moderazione compiute dal relativo gestore come un prodotto autonomo tutelato della libertà di espressione di quest'ultimo, quest'esito è compatibile con la visione sottostante alla Section 230, cristallizzata intorno all'assenza di un ruolo editoriale?

Se la sentenza si occupa del primo aspetto, essa non scioglie il secondo nodo, non affrontato direttamente, del resto, nell'ambito di una causa incentrata sulla compatibilità con il Primo emendamento delle sole leggi impugnate.

Difficile, d'altronde, come si è cercato di approfondire altrove, dare una risposta *tranchant* al dilemma appena evidenziato. È certamente vero, da una parte, che dall'epoca in cui è stata scritta la Section 230 sono passati quasi venti anni, più di un secolo nel "mondo dei bit". Ed è altrettanto vero che i soggetti che all'epoca erano immaginati quali destinatari dell'immunità in questione sono lontani parenti degli assai più potenti e sofisticati operatori privati di oggi. D'altra parte, quella normativa non è solo figlia dei suoi tempi, quindi di un internet agli albori assai differente dal contesto digitale che oggi conosciamo, ma è, sotto un profilo più generale, strettamente connessa alle radici liberali del costituzionalismo americano. Non è facile, dunque, pensare a una modifica di questa legislazione senza alterare lo spirito fondativo proprio di quelle radici.

D'altronde, non si può non aggiungere che parecchie perplessità circa la capacità della Sezione 230 di reggere ancora una volta all'urto della richiesta di una sua revisione (o aggiornamento), anche alla luce della trasfigurazione degli attori rilevanti che si è provato a fare emergere in precedenza. Basti ricordare quanto affermato da Justice Elena Kagan (ed il tema della separazione dei poteri anche nel contesto digitale è cruciale come si è evidenziato in apertura) quando, durante l'*hearing* delle parti[81], nel caso appena richiamato, ha ricordato che la revisione della normativa oggetto di giudizio sarebbe, caso mai, un compito del Congresso, anche perché "w*e're a court, we really don't know about these things*", Kagan ha poi sentito il bisogno di aggiungere, onde chiarire ogni dubbio in merito, che "*these are not like the nine greatest experts on the internet.*"

---

[80] 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

[81] 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.

2.1 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"

Quest'idea che si potrebbe definire di "liberismo digitale" è facilmente migrata da una sponda all'altra dell'Atlantico. Infatti, anche l'Europa si è dotata, seppure alcuni anni dopo, di un quadro di regole animato dalla preoccupazione di non rendere il modello di *business* dei "prestatori di servizi della società dell'informazione", come definiti dalla normativa che si citerà subito dopo, economicamente sconveniente. In altre parole, l'obiettivo della normativa iniziale era quello di favorire, attraverso un esercizio di minimalismo regolatorio, la crescita del commercio elettronico[82] e, quindi, alimentare il vento di innovazione tecnologica che quest'ultimo portava con sé.

Come correttamente osservato da Giovanni De Gregorio, i segni di questa fase di "liberismo digitale" si possono riscontrare in due importanti testi legislativi di quegli anni[83]: la Direttiva 95/46/CE[84], ovverosia la direttiva sulla protezione dei dati personali, e la Direttiva 2000/31/CE[85], cosiddetta "direttiva e-Commerce", volta alla regolamentazione del commercio elettronico.

La Direttiva sulla protezione dei dati personali, del resto, precedeva di diversi anni la Carta dei diritti fondamentali dell'Unione europea (CDFUE), la quale, nel porre le fondamenta della sistematica della tutela dei diritti umani nel contesto dell'Unione, avrebbe espressamente riconosciuto e dato rilevanza, per così dire, 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"[86]), sia al diritto alla protezione dei dati personali ("Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"[87]).

Anche alla luce di tale prospettiva storica, si comprende perché la normativa contenuta nella direttiva 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. Così, la normativa si focalizzava prevalentemente sulla natura funzionale della protezione dei dati personali nel contesto del corretto funzionamento del mercato interno. Del resto, la stessa denominazione della direttiva del 1995 faceva riferimento alla "libera circolazione di tali dati", rimandando, quindi, di fatto alle tradizionali quattro libertà di circolazione (di beni, di servizi, di capitali, di persone) che hanno caratterizzato fin dalle sue origini la natura economica dell'Unione[88].

Tale approccio della direttiva 95/46/CE emergeva del resto anche dallo stesso art. 1, il quale, nel richiedere che gli Stati membri garantissero "la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali"[89], sottolineava, tuttavia, in modo esplicito la finalità di garantire la massima mobilità possibile di questi ultimi, stabilendo il divieto per gli stati membri di restringere o vietare la libera

---

[82] G. DE GREGORIO, *Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society*, Cambridge University Press, Cambridge, 2022.

[83] 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.

[84] 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.

[85] 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.

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

[87] *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".

[88] 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.

[89] Direttiva 95/46/CE, art. 1(1).

circolazione dei dati personali tra gli stessi stati per motivi connessi alla tutela dei suddetti diritti e libertà fondamentali[90]. In altre parole, da un lato si richiedeva l'adozione di misure volte a proteggere gli interessi, costituzionalmente rilevanti, degli individui; dall'altro lato, si sottolineava come tali garanzie "minime" fossero necessarie al fine di rendere più agevole il movimento, economicamente rilevante, dei dati personali. Ancora più esplicito, in tal senso, il considerando 7 della Direttiva, il quale giustificava tra l'altro l'adozione di quest'ultima sottolineando che

> "*il divario nei livelli di tutela dei diritti e delle libertà personali, in particolare della vita privata, garantiti negli Stati membri relativamente al trattamento di dati personali può impedire la trasmissione dei dati stessi fra territori degli Stati membri e che tale divario può pertanto costituire un ostacolo all'esercizio di una serie di attività economiche su scala comunitaria, falsare la concorrenza e ostacolare, nell'adempimento dei loro compiti, le amministrazioni che intervengono nell'applicazione del diritto comunitario"*[91].

Anche la direttiva e-Commerce, la quale, a differenza della Direttiva 95/46/CE, è ancora in vigore al giorno d'oggi, è in gran parte orientata a promuovere e favorire lo sviluppo di un mercato elettronico interno a vantaggio degli interessi economici dell'Unione. Anche in questo caso, la Direttiva mira a una armonizzazione a livello europeo delle regole concernenti tale tipologia di mercato, al fine precipuo di limitare gli ostacoli di carattere legislativo al buon funzionamento delle nuove *agorà* digitali. Tra l'altro, particolare rilievo nel quadro della direttiva era ricoperto dalla specifica disciplina concernente le responsabilità per i fornitori di servizi di intermediazione digitale.

Lo specifico quadro giuridico istituito in tale settore dalla Direttiva e-Commerce verrà meglio descritto più sotto, quando si parlerà delle innovazioni introdotte dal Digital Services Act in tale settore. Basti qui segnalare che il regime istituito dalla menzionata direttiva si caratterizzava per uno spiccato approccio di favore agli interessi dei *provider*, i quali solo in ben definiti e ristretti casi potevano essere chiamati a rispondere per l'utilizzo dei loro servizi per finalità illecite. Seguendo il modello degli Stati Uniti, il legislatore dell'Unione mirava in sostanza a proteggere i fornitori di servizi digitali, il cui modello di *business* era a quei tempi ancora agli inizi, da un eccesso di responsabilità giuridiche che avrebbero potuto soffocarne la libertà di iniziativa economica e, di conseguenza, ostacolare grandemente l'avanzamento tecnologico all'interno del Vecchio Continente. Appare di tutta evidenza come il quadro normativo europeo e statunitense, così brevemente tratteggiato, risponda a un contesto ben preciso, in cui vi era terreno fertile, affinché il cyberspazio diventasse luogo di realizzazione della metafora del libero mercato delle idee. In quello scenario di grande concorrenza tra comunità virtuali, era inevitabile che la premura dei legislatori fosse quella di mantenere al minimo la pressione regolamentare, confidando nella capacità intrinseca del cyberspazio di "autoregolarsi" offrendo spazi alternativi tra loro in grado di affermarsi e legittimarsi.
In questo contesto, a regnare sovrano, è il diritto della concorrenza, quale unico strumento *ex post* di intervento sulle concentrazioni di potere economico che, gradualmente ed inevitabilmente, andavano a formarsi. Lo scenario rilevante è, per l'appunto, quello del mercato e la libertà rilevante è quella dell'iniziativa economica e dei suoi limiti.

3. Le ragioni di una metamorfosi e l'ascesa irresistibile del "fattore algoritmico"

Di lì a qualche anno, vi sarebbe stato un profondo cambio di paradigma tanto sotto il profilo tecnologico quanto, conseguentemente, sotto quello relativo alle tecniche di regolazione.

---

[90] *Ibidem*, art. 1(2).
[91] *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".

Con riguardo, in particolare, al primo profilo evocato, si sarebbe assistito ad una metamorfosi dei nuovi soggetti dell'era digitale da attori economici in veri e propri poteri privati e, quindi, come si vedrà, la disciplina antitrust avrebbe mostrato la sua inadeguatezza. Si è compreso che l'obiettivo di realizzare un libero mercato delle idee, alla base del minimalismo regolamentare descritto nella prima fase dello sviluppo dell'ordinamento della rete, non poteva essere raggiunto soltanto puntando sulla capacità auto-correttiva di detto mercato. Questo, lungi dall'essere libero, si rivelava sempre più soggetto a incrostazioni monopolistiche o oligopolistiche da parte di grandi soggetti privati, rendendo inadeguato un intervento ex post da parte della disciplina antitrust. Questo anche a causa del cambio di paradigma prima evocato, di cui bisogna adesso indagarne le ragioni.
Più precisamente, perché, in un determinato momento storico, i soggetti che esercitano iniziativa economica nel cyberspace si sono trasformati in veri e propri poteri privati in competizione con i poteri pubblici?
Per provare a fornire una risposta adeguata, bisogna fare un passo indietro di qualche decennio e ricordare chi, per primo, alla fine del secolo scorso[92], aveva in tempi non sospetti evidenziato una prima trasformazione, o meglio, un primo passaggio assai rilevante.
Il riferimento è 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. Ad avviso di Lessig, la modalità di regolazione più adatta alle peculiarità del cyberspazio è quella che vede le norme giuridiche agire indirettamente, incidendo sull'architettura del cyberspazio onde consentire alla tecnica di farsi essa stessa strumento di esecuzione di norme di condotta. La riflessione di Lessig ha colto alcuni aspetti centrali nel dibattito sulla regolamentazione del cyberspazio. Quello più rilevante ai nostri fini è, partendo dalla centralità del ruolo della tecnica per un'efficace regolamentazione, il fatto che vi fosse in corso un passaggio nelle decisioni fondamentali su tale regolamentazione dal legislatore all'informatico, all'esperto in grado di decodificare il codice. Come è stato evidenziato[93], on è, forse, casuale che le prime disposizioni dettate dai legislatori in materia abbiano interessato il ruolo degli intermediari, nella consapevolezza della centralità del ruolo tecnico? All'epoca, questo ruolo era ancora scevro da connotazioni oligopolistiche e, dunque, risparmiato da una disciplina che si estendesse sul versante della concorrenza, rispetto alle operazioni che coinvolgono un intervento sulle attività e condotte degli utenti. Oggi si assiste ad una sorta di "*code reloaded*", alla luce di quella metamorfosi prima evocata degli intermediari digitali da attori economici a veri e propri poteri privati in competizione con quelli pubblici. Infatti, da una parte, tali soggetti sono parenti alla lontana di quelli che sono stati (non) regolati dalla disciplina europea nella prima stagione, sopra descritta, di liberismo digitale. Sono diventanti – ed è stato un crescendo direttamente proporzionale all'accelerazione della rivoluzione digitale – assai meno neutri, assai meno passivi, ma molto più sofisticati e molto più in grado – pur non assumendo il ruolo di editori tradizionali – di incidere sui contenuti ospitati nei loro spazi virtuali.
Dall'altra parte, se Lessig aveva ben intuito e descritto un primo passaggio dal decisore politico all'esperto di informatica, qualche anno dopo, a partire dal decennio scorso, il consolidamento, da una parte, dei nuovi poteri privati digitali a seguito della trasfigurazione prima evocata e, dall'altra parte, l'ascesa del fattore algoritmico hanno ulteriormente spostato la sede, la modalità e il "momento" della decisione.
Si tratta di un passaggio che non va sottovalutato e che si caratterizza per un doppio livello: il primo è costituito dalla delega da parte degli attori pubblici ad operatori (poteri) privati di operazioni di bilanciamento tra diritti. Basti pensare ad uno degli effetti della codificazione giurisprudenziale del

[92] L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.
[93] M. BASSINI, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali,* Aracne, Roma 2019.

diritto all'oblio avvenuta, come notissimo, dalla decisione della Corte di giustizia, già richiamata, nel caso *Google Spain*. Di fatto, in quell'occasione, i giudici di Lussemburgo hanno affidato ad un motore di ricerca, operatore/potere privato, il compito di operare quel delicato bilanciamento tra diritto ad essere dimenticato da parte di un utente e diritto ad essere informati in capo alla maggioranza degli internauti. Un'operazione che dovrebbe essere di esclusiva attribuzione di un'autorità giurisdizionale o para-giurisdizionale e la cui delega, quasi in bianco, ad un operatore privato, senza, come si dirà successivamente, le adeguate garanzie procedimentali, non può fare altro che amplificarne il potere.
Il secondo livello è costituito da un'ulteriore sub-delega: i poteri privati, ma anche quelli pubblici[94], affidano sempre più spesso all'algoritmo il compito di operare l'assunzione di decisioni di grande delicatezza e impatto sociale[95]. È evidente che i sistemi molto più complessi di intelligenza artificiale di natura generativa, che saranno esaminati successivamente e distinti dal "semplice" fattore algoritmico, abbiano ulteriormente amplificato e reso visibile questo processo di delega[96]. Come è stato esattamente notato a questo proposito, "*These systems are increasingly called to make decisions that, de facto, are based on (technological) standards embedded in their design, not necessarily aligned with legal standards or the protection of public interest. Indeed, the threats of "algocracy" do not only question the role of humans, or the protection of fundamental rights, but also the role of the rule of law*"[97].
Vi è un altro aspetto che va evidenziato con riguardo a come l'intuizione, agli albori di Internet, di Lessig possa essere rimodulata nella stagione dell'automazione, seguendo quell'idea di *code reloaded* prima richiamata. Oggi, di fatto, l'architettura tecnologica non è soltanto la struttura portante che costituisce l'*humus* infrastrutturale fortemente interconnesso alla cornice giuridica della rete, ma la stessa architettura, riplasmata dal potere trasformativo dell'intelligenza artificiale, è essa stessa creatrice di regole. Come ha correttamente fatto emergere Giovanni De Gregorio parlando di *normative power* dell'intelligenza artificiale[98], i nuovi modelli di apprendimento automatico non sono solo più soltanto semplici strumenti di esecuzione basati su istruzioni e standard predefiniti, ma, attraverso un continuo processo di apprendimento e di adattamento della loro funzione attraverso l'esperienza e l'allenamento, esercitano un ruolo para-normativo. Ad esempio, la rimozione di contenuti online non è solo il risultato degli standard comunitari dei social media o del design delle tecnologie algoritmiche, ma anche della capacità dell'intelligenza artificiale di definire e, successivamente, decidere cosa considerare, per esempio, un contenuto disinformativo o un discorso d'odio e, solo dopo, rimuovere quel contenuto. Considerazioni simili si estendono al settore pubblico. La sorveglianza digitale sottolinea come le macchine calcolino certi gradi di rischio e poi segnalino alcuni casi alle forze dell'ordine. Le decisioni si basano non solo sui dati archiviati dalle autorità di polizia o sugli standard tecnici, ma anche su un insieme di norme tecniche auto-generate che valutano i rischi cambiando e adattandosi nel tempo. In questo contesto può forse dirsi che si è perfezionato

---

[94] Sul punto si veda E. LONGO, *Giustizia digitale e Costituzione: Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, Franco Angeli Edizioni, Milano, 2023.
[95] Si pensi al Regno Unito, dove il machine learning è stato impiegato per l'attribuzione di valutazioni in ambito scolastico (si veda H. SMITH, *Algorithmic bias: should students pay the price?*, in *AI & Society*, fasc. 35, 4, 2020, p. 1077-1078), o all'Olanda, dove le autorità fiscali hanno utilizzato un algoritmo per individuare le frodi nel settore dell'assistenza all'infanzia, generando una discriminazione per i gruppi etnici "non occidentali" (sul punto, M. HEIKKILÄ, *Dutch scandal serves as a warning for Europe over risks of using algorithms*, *POLITICO*, 2022 https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/). Il caso più celebre è senz'altro quello del COMPAS statunitense, che calcola la probabilità di recidiva di un reato e, conseguentemente, influenza le decisioni dei giudici in ambito penale (A. Z. HUQ, *Racial equity in algorithmic criminal justice*, in *Duke Law Journal*, fasc. 68, 6, 2019, p. 1043–1134).
[96] 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/.
[97] G. DE GREGORIO, *The Normative Power of Artificial Intelligence*, in *Indiana Journal of Global Legal Studies*, fasc. 30, 2, 2023, p. 55-80.
[98] *Ibidem.*

un passaggio che sembra rilevante per gli studi di diritto costituzionale in questo ambito: da *code is law* a *code as source of law.*

4. 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[99], l'attuale contesto storico è dominato dall'avvenuta affermazione di una "società algoritmica", caratterizzata segnatamente da due fattori. Da un lato, quest'ultima si fonda, per l'appunto, sull'accresciuto rilievo dello strumento dell'algoritmo, anche grazie allo straordinario patrimonio di dati ormai a disposizione di attori pubblici e, soprattutto, privati. Dall'altro lato, si tratta di una società che si caratterizza anche per l'emersione di nuovi rilevanti attori, per l'appunto, privati nello scenario globale. Le cosiddette "*big tech*", o le "compagnie del digitale", come osservato da Luciano Violante, riadattando al nuovo contesto globale il potere di fatto detenuto dalle "Compagnie delle Indie", 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[100].

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[101] 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.

---

[99] 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.
[100] 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".
[101] Per una lucida analisi, LONGO, *Giustizia digitale e Costituzione: Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, cit.

5. 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

Alla luce di tali mutamenti sociali, non stupisce che l'Unione abbia scelto di rispondere attraverso un attento ripensamento delle proprie strategie regolatorie. Il mutamento dell'orientamento dell'Unione quale reazione alle trasformazioni, prima descritte, del paradigma tecnologico si è, peraltro, avuto per gradi. La prima vera protagonista è stata, in tal senso, la Corte di giustizia dell'Unione europea. A partire dagli anni 2010, infatti, i giudici di Lussemburgo avviavano una corrente giurisprudenziale orientata a far fronte all'inerzia del legislatore europeo e allo stesso tempo a fare della Unione una fortezza in materia di dati personali (a volte senza i necessari ponti levatoi di interconnessione per assicurare un *enforcement* e una cooperazione adeguati).

Si tratta di un punto importante che non può essere liquidato in poche righe, perché va a toccare una delle caratteristiche essenziali del costituzionalismo europeo rispetto a quello statunitense, vale a dire la possibilità di servirsi dell'arma (nucleare?) dell'applicazione orizzontale dei diritti fondamentali, quale reazione a due mutamenti prima descritti: la trasfigurazione degli operatori digitali in poteri privati e l'ascesa inarrestabile del fattore algoritmico, ovvero dell'automazione che si nutre di una quantità spropositata di dati.

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"[102]. È fondamentale a questo proposito differenziare l'analisi quanto meno in una prospettiva transatlantica, Infatti, Wu sottovaluta, come vedremo, la creatività e l'audacia della Corte di giustizia dell'Unione europea nel "trasformare" per via interpretativa (*melius*: manipolativa) disposizioni dei trattati chiaramente pensate esclusivamente nei confronti degli Stati membri in strumenti direttamente azionabili dai singoli, con un effetto diretto orizzontale neanche immaginato dagli Stati membri al momento della sottoscrizione degli stessi trattati.

Così come è eccessivamente ottimista quanto sostiene a questo riguardo Robert Alexy[103], 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).

Il problema è che tale assunto, convincente da un punto di vista teorico, passando dall'"olimpo" dei filosofi all'"arena" dello *ius dicere*, rischia di non superare il test del diritto comparato. Le scelte delle corti costituzionali e supreme possono divergere su questo aspetto, in base al paradigma costituzionale al quale esse si ispirano, che fa da architrave, da humus assiologico e culturale.

Concentrandosi sulla prospettiva europea, si fa evidentemente riferimento alla possibilità di riconoscere effetti orizzontali alle "nostre" Carte dei diritti nei confronti dei soggetti privati, così facendo leva sulla dottrina della *Drittwirkung* di estrazione tedesca, edificata nel celebre caso *Lüth-Urteil*[104].

Dal canto suo, la Corte di giustizia ha, infatti, dimostrato di essere in grado di attribuire tale efficacia a disposizioni chiave dei Trattati istitutivi, anche per quelle che avevano chiaramente come destinatari esclusivi gli Stati membri.

---

[102] T. WU, *La maledizione dei giganti: un manifesto per la concorrenza e la democrazia*, Il Mulino, Bologna, 2021, p. 10.
[103] R. ALEXY, *Teoria dei diritti fondamentali*, Il Mulino, Bologna, 2012, p. 570-571.
[104] BVerfGE, 7, 198, 15 gennaio 1958.

Basti pensare alla decisione D*efrenne II* [105], che ha attribuito efficacia diretta orizzontale ad una disposizione del trattato (il vecchio art. 119 TCE, oggi trasposto nell'art. 157 TFUE, in tema di parità retributiva tra uomini e donne), che si rivolgeva esclusivamente agli Stati membri nel richiedere ai poteri legislativi interni di adottare le discipline a livello nazionale più idonee per garantire effettività, e, quindi, giustiziabilità negli ordinamenti giuridici nazionali al diritto alla parità retributiva tra i sessi per uno stesso lavoro (o per uno equivalente).
È stata la Corte di giustizia ad interpretare assai creativamente il portato di tale disposizione, attribuendole, in evidente contrasto con il tenore letterale della stessa, un effetto diretto orizzontale. In tale scenario, relativamente all'attribuzione di effettività al principio, fino ad allora soltanto proclamato, di parità retributiva tra uomo e donna, la sentenza *Defrenne II* ha la stessa rilevanza che la decisione *Costa c. Enel*[106] può vantare in riferimento al concetto di superiorità del diritto dell'Unione sul diritto interno e la sentenza *Simmenthal*[107] a proposito della nozione di *effetto utile* quale predicato imprescindibile del diritto europeo. Da lì in poi, non sono mancati i casi di applicazione orizzontale di principi generali del diritto dell'Unione[108] e, con una giurisprudenza non sempre cristallina, anche di alcuni articoli della Carta dei diritti fondamentali[109].
Vi è, però, una caratteristica peculiare, in questo contesto, che caratterizza la reazione della Corte di giustizia rispetto all'emersione di un potere digitale. In quegli anni, tale potere non veniva contrastato né da un legislatore di ispirazione neo-liberale, quanto alla (non) regolazione dei soggetti digitali, come si è provato a descrivere in precedenza, né da un legislatore semplicemente inerte, come nel caso dei lunghissimi tempi di gestazione che hanno portato all'adozione, nel 2016, del GDPR.
In particolare, tale caratteristica risiede, come si è cercato di dimostrare altrove, in una surrettizia e sicuramente non esplicitata applicazione orizzontale degli articoli 7 e 8 della Carta dei diritti fondamentali, in materia, rispettivamente, di tutela della vita personale e protezione dei dati. Questo si è manifestato nella giurisprudenza tra il 2014 e il 2015, nell'*enforcement* della privacy digitale nei confronti dell'emergente potere algoritmico[110].
Le decisioni rilevanti, che, peraltro, sono state già ampiamente richiamate in precedenza, meritano in questa sede un approfondimento specifico sotto la prospettiva appena menzionata, perché scandiscono i tempi di un processo di costruzione di una fortezza europea in tema di protezione dati, a tutela dell'emergente potere digitale privato, ma con non poche controindicazioni che dovranno essere approfondite.

---

[105] 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.
[106] C. giust. CE 15 luglio 1964, *Flaminio Costa c. ENEL*, causa 6/64.
[107] C. giust. CE 9 marzo 1978, *Amministrazione delle Finanze dello Stato c. Simmenthal SpA*, causa 106/77.
[108] *ex multis* C. giust. CE 5 febbraio 1963, *Van Gend en Loos c. Amministrazione olandese delle imposte*, causa 26/62; C. giust. CE 21 giugno 1974, *Reyners c. Stato belga*, causa 2/74; C. giust. CE 3 dicembre 1974, *Van Binsbergen c. Bestuur van de Bedrijfsvereniging voor de Metaalnijverheid*, causa 33/74; C. giust. CE 4 dicembre 1974, *Van Duyn c. Home Office*, causa 41/74.
[109] C. giust. UE 17 aprile 2018, *Egenberger*, causa C-414/16; C. giust. UE 6 novembre 2018, *Bauer*, causa C-569/16; C. giust. UE 6 novembre 2018, *Max-Planck-Gesellschaft zur Förderung der Wissenschaften*, causa C-684/16 C. giust. UE 11 settembre 2018, *IR c. JQ*, causa C-68/17; C. giust. UE 22 gennaio 2019, *Cresco Investigation*, causa C-193/17; C. giust. UE 14 maggio 2019, *CCOO*, causa C-55/18. V. E. FRANTZIOU, *The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle*, in *The Cambridge yearbook of European legal studies*, fasc. 22, 2020, p. 208-232; V. PICCONE, O. POLLICINO (a cura di), *La Carta dei Diritti Fondamentali dell'Unione Europea. Efficacia ed effettività*, Editoriale Scientifica, Napoli, 2018.
[110] 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.

Nel caso *Digital Rights Ireland*, i procedimenti di rinvio pregiudiziale sono stati avviati dall'Alta Corte d'Irlanda e dalla Corte costituzionale austriaca in relazione alle normative nazionali di recepimento della direttiva del 2006 sulla conservazione dei dati. Questa Direttiva permetteva alle autorità nazionali di raccogliere in modo intrusivo informazioni riguardanti molteplici aspetti della vita privata di coloro che avevano sottoscritto contratti per la fornitura di servizi di telecomunicazione. La Corte di giustizia, utilizzando la Carta quale parametro costituzionale rilevante – quello che era mancato in tutta la sua giurisprudenza precedente relativa alla tutela dei diritti fondamentali[111] che di fatto la Carta ha codificato – ha annullato, per la prima volta nella storia del processo di integrazione europea, un'intera legislazione di natura derivata, perché in contrasto con il *bill of rights* europeo.
La legislazione in questione, la Direttiva del 2006 prima menzionata, costituiva il prodotto di una reazione securitaria agli attacchi dell'11 settembre 2001, imbevuta di una logica di controllo preventivo. Essa aveva ritagliato alcune eccezioni relative alla protezione del diritto al rispetto della vita privata.
I giudici europei offrono un'analisi dettagliata degli aspetti critici della direttiva. Innanzitutto, si sottolinea che l'interferenza con il diritto fondamentale alla vita privata avrebbe potuto investire l'intera popolazione dell'Unione, senza distinzione alcuna e senza che rilevasse che una persona fosse o meno sottoposta a indagini per "reati gravi". Il semplice richiamo generico a "reati gravi" per giustificare una simile ingerenza è, inoltre, considerato inadeguato e, in quanto tale, incompatibile con il principio di proporzionalità. In aggiunta, la Corte sottolineò la mancanza di garanzie sostanziali e processuali. Su queste basi, i giudici di Lussemburgo concludono che l'interferenza nei diritti da parte della Direttiva è eccessivamente ampia per considerarsi rispettosa dei principi di necessità e proporzionalità[112].
In *Google Spain*, 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.
La Corte fonda, nuovamente, la propria decisione quasi esclusivamente sugli artt. 7 e 8 della Carta di Nizza, relegando al margine altre norme quali gli artt. 11, in materia di libertà di espressione, e 16, che tutela la libertà di iniziativa economica.
In particolare, tale applicazione piuttosto eterodossa dell'efficacia orizzontale dei diritti fondamentali consente alla Corte di Lussemburgo di applicare la disciplina della Direttiva anche ai gestori di motori di ricerca, fatti rientrare nella nozione di "titolari del trattamento", superando nel contempo, come si è avuto modo di anticipare in precedenza, l'eccezione relativa allo stabilimento estero degli stessi.
Si potrebbe sottolineare come, in *Digital Rights Ireland* e in *Google Spain*, la Corte si sia impegnata a proteggere, nei confronti dell'emergente potere digitale, in modo così "viscerale" la fortezza europea a tutela della privacy europea, da sottovalutare le conseguenze negative di un simile approccio. Da un lato, un ridimensionamento della protezione riservata ad altri valori di pari rilevanza costituzionale, inclusa la libertà di espressione; dall'altro lato, come si avrà modo di rilevare anche più avanti, la delega in bianco a un soggetto privato di operare quel bilanciamento tra diritti che dovrebbe esclusivamente caratterizzare il nucleo duro di funzioni giurisdizionali o para-giurisdizionali.

---

[111] C. giust. CE 14 maggio 1974, *Kohlen- und Baustoffgroßhandlung c. Commissione delle Comunità europee*, causa 4/73.
[112] C. giust. UE, Digital Rights Ireland, cit., § 65.

Schrems I segue a sua volta le linee tracciate da *Digital Rights Ireland* e *Google Spain*. Anche in questo caso, 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. Secondo i giudici di Lussemburgo la nozione di "livello di protezione adeguato" ai sensi dell'art. 25 è da interpretarsi con riferimento specifico agli artt. 7 e 8 della Carta di Nizza, di nuovo il prisma interpretativo che caratterizza l'intero impianto argomentativo della decisione.
È proprio grazie a tale prisma che la Corte è in grado di modificare lo standard relativo all'adeguatezza del livello di protezione in uno differente che sembra prevedere una qualche forma – mai richiesta dalla normativa rilevante – di equivalenza tra gli ordinamenti giuridici posti a confronto. Riferendosi alla *ratio* dell'art. 25, la Corte concluse che, anche se un livello di protezione adeguato non richiede necessariamente che i Paesi terzi adottassero standard identici a quelli dell'Unione Europea, un sistema di tutela "sostanzialmente equivalente" è comunque richiesto[113].
Un aspetto peculiare che caratterizza *Schrems I* è, innanzitutto, il fatto che, a differenza di *Digital Rights Ireland*, è in questo caso il sistema statunitense, e non un atto interno all'Unione, a costituire oggetto di un giudizio di conformità con gli artt. 7 e 8 della Carta di Nizza. Tale valutazione, del resto, è influenzata dallo scandalo che aveva colpito in quegli anni la *National Security Agency* (NSA) statunitense. *Schrems I*, inoltre, produsse a sua volta delle conseguenze anche al di là dell'Atlantico: in *ACLU v. Clapper*[114], la Corte d'Appello degli Stati Uniti per il Secondo Circuito concluse che la Sezione 215 del *USA Patriot Act* non autorizzava l'NSA a condurre una sorveglianza di massa e a raccogliere in modo massiccio metadati concernenti i cittadini. La migrazione di idee costituzionali in ambito digitale è spesso biunivoca.
Nel complesso, il dato fondamentale di *Schrems I* è dato dal fatto che la CGUE ha fondamentalmente riscritto i criteri rilevanti, sostituendo, attraverso un'interpretazione dell'art. 25 orientata alla tutela dei principi contenuti nella Carta di Nizza, il concetto di adeguatezza con quello di "equivalenza". Si tratta di una "manipolazione tramite interpretazione"[115] della normativa rilevante volta ad una surrettizia applicazione orizzontale della Carta ed alla costruzione, per via giudiziaria, di una fortezza europea a protezione della privacy digitale che esercita la sua sovranità anche nel cyberspace, quale reazione al rafforzamento del potere privato ed ascesa del fattore algoritmico
Si diceva che quella dell'applicazione orizzontale dei diritti fondamentali è una caratteristica identificativa del costituzionalismo europeo in quanto, per esempio, l'arsenale di diritto costituzionale d'Oltreoceano non disponeva della stessa arma. O meglio, per quanto riguarda l'applicazione dei

---

[113] 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".
[114] 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).
[115] O. POLLICINO, *Interpretation or manipulation? The Court of Justice sets a new right to digital privacy*, in *Federalismi.it*, fasc. 3, 2014.

diritti previsti dagli Emendamenti della Costituzione introdotti a partire dal 1791, e, con particolare riferimento al Primo emendamento, l'efficacia orizzontale (*inter privatos*) dello stesso è negata dall'applicazione della c.d. *state action doctrine*[116], in forza della quale le garanzie previste dai diritti sanciti dal *Bill of Rights* federale possono essere fatte valere soltanto nei confronti dei poteri pubblici e non dei privati.
La ragione alla base della resistenza all'accettazione di una generale efficacia orizzontale dei diritti previsti dalla Costituzione federale si spiega con il terreno culturale che fa da *humus* al costituzionalismo statunitense, il quale è basato sui valori di *liberty* e *individual freedom* che costituiscono il fondamento dell'autonomia privata.
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*". La domanda, con riguardo al nostro campo di indagine, nasce spontanea: una tale intrusione può essere considerata intollerabile anche quando siamo di fronte a poteri privati che *de facto* spesso esercitano funzioni di natura pubblicistica o para-costituzionale e, quindi, possono essere considerati *latu senso state actors*? La risposta della Corte suprema è abbastanza netta e conferma l'intollerabilità dell'intrusione. Nell'unica decisione di un certo rilievo assunta finora alle cronache[117], è stato escluso che un soggetto privato, per quando di dimensioni elefantiache come YouTube, possa essere considerato uno *state actor*.
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"[118]; al contrario, questi non sarebbero altro che soggetti privati che adottano decisioni relative alla *governance* del proprio spazio.
Il riferimento al governo dello spazio gestito dalle piattaforme, considerando l'invalicabilità dell'ostacolo rappresentato dal mancato superamento della *state action doctrine*, rappresenta il secondo tentativo del diritto costituzionale statunitense di essere più efficace nella delimitazione dell'emergente potere digitale. Anche questo tentativo, come vedremo, è stato sostanzialmente infruttuoso.
In particolare, si fa riferimento all'opzione interpretativa menzionata in apertura, che mira a equiparare gli spazi offerti dalle piattaforme digitali di social network alla categoria del public forum. Questo permetterebbe di applicare la *public forum doctrine*, la quale consente limitatissime interferenze con l'esercizio della libertà di espressione, perlopiù neutre rispetto ai contenuti, in luoghi come parchi, strade e piazze, considerati naturalmente destinati allo scambio di idee e opinioni tra individui.
Si è evidenziato in dottrina[119] come questa metafora ricorra spesso allo scopo di descrivere i social network, come la nuova pubblica piazza, tuttavia, è cosa ben diversa sottendervi una valenza normativa. La giurisprudenza statunitense, fino a oggi, ha avallato questa ricostruzione soltanto in presenza di account social utilizzati da *state officials*, ossia da soggetti che agiscono nella loro qualifica pubblicistica, allo scopo di ritenere misure quali il blocco o la rimozione di commenti

---

[116] 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.
[117] Corte d'appello federale degli Stati Uniti d'America per il Nono Circuito 26 febbraio 2020, *Prager University c. Google LLC,* n. 18-15712 (9th Cir. 2020).
[118] BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, cit. 22.
[119] BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, cit. 68.

effettivamente lesive della libertà di espressione degli utenti[120]. Vale la pena segnalare che la giurisprudenza non considera la natura proprietaria ostativa alla qualificazione pubblicistica, rilevando che ben possono esistere *designated public forum*, ossia spazi che "diventano", pur essendo privati, di natura sostanzialmente pubblica, coinvolti nel medesimo processo di metamorfosi che abbiamo visto caratterizzare i soggetti in gioco. Infine, alcune specificazioni rispetto al discorso dei *public officials* online (e alla loro facoltà di bloccare gli utenti) sono state fatte da parte della Corte Suprema, che ha delineato una serie di requisiti per identificare quando le condotte dei *public officials* siano inquadrabili come *state actions*[121].

Ritornando all'esame della reazione giurisprudenziale europea all'ascesa del fattore algoritmico, la Corte di giustizia, d'altra parte, è intervenuta anche sotto il profilo della responsabilità dei fornitori di servizi digitali per la commissione di attività o la diffusione di materiali illeciti: se, come menzionato sopra, la Direttiva e-Commerce si caratterizzava per l'adozione di un regime generalmente assolutorio di tali fornitori, prevedendo estese forme di esenzione da tali forme di responsabilità, i giudici di Lussemburgo, a partire dal 2010, cominciarono a dare un'interpretazione restrittiva della Direttiva, affermando che essa tutelava solamente quei *provider* la cui prestazione dei servizi assumeva un carattere "meramente tecnico, automatico e passivo"[122]. Scopo della Corte era, chiaramente, quello di adeguare l'obsolescente disciplina della Direttiva e-Commerce, ormai considerata troppo di favore nei confronti di attori che avevano acquisito un assai rilevante potere economico.

Sebbene le reazioni della Corte di Giustizia, motivate come si è accennato dalla necessità di adattare la normativa esistente al nuovo panorama socio-economico e tecnologico in modo tale da promuovere, anche nel contesto della società algoritmica, l'insieme dei valori fondamentali e democratici caratterizzanti l'*humus* costituzionale europeo, appaiano sicuramente comprensibili, sono, tuttavia, riscontrabili alcune significative controindicazioni relative alla stagione dell'"attivismo giudiziario" dei giudici di Lussemburgo. In particolare, almeno tre controindicazioni sembrano essere di particolare rilievo. La prima, di particolare evidenza, fa riferimento all'amplificazione di uno squilibrio, già evocato in apertura, in termini di separazione tra poteri, tra il versante giudiziario e quello politico-legislativo.

Se già dalla fine del secolo scorso si fa riferimento al fenomeno della *judicial globalization*[123] per fare emergere il ruolo crescente, fino a diventare preponderante, delle Corti nei rapporti (di forza) con potere legislativo ed esecutivo, ebbene tale ruolo, come si è avuto di sottolineare altrove[124], si è ulteriormente accresciuto nel contesto digitale. Questo per almeno due ragioni. La prima è dovuta all'inerzia del legislatore che è diventata cronica con riferimento a un ambito, come quello relativo alla regolazione del cyberspace, ad altissimo rischio di obsolescenza, in un circolo vizioso in cui potere legislativo ed esecutivo, pur di non rimanere perennemente indietro rispetto alle accelerazioni tecnologiche, preferiscono restare inerti. In questo modo, delegano ai giudici la responsabilità di

---

[120] 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.).

[121] 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).

[122] 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.

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

[124] POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, cit.

operazioni di bilanciamento connesse a una tecnologia che lungi dall'essere neutrale, sottintendendo una forte matrice assiologica-sostanziale.
La seconda ragione risiede, come si è avuto modo sottolineare *supra* commentando le prime pronunce giurisdizionali di corti statunitensi di reazione alla prospettiva anarcoide di un cyberspace immune dall'influenza dei poteri pubblici, in quell'esercizio di radicamento della giurisdizione, tipico del diritto di internet, che amplifica ulteriormente il ruolo delle Corti nell'ecosistema digitale.
Alla luce di queste considerazioni, e tornando allo scenario europeo, non sorprende che si sentisse l'esigenza di attenuare lo squilibrio menzionato in termini di separazione dei poteri. L'Unione Europea ha cercato di rispondere all'emersione dei nuovi poteri digitali e all'ascesa dell'algoritmo attraverso il processo legislativo democratico-rappresentativo, piuttosto che affidarsi esclusivamente all'attivismo giurisprudenziale, seppur ragionevole nel contesto descritto.
L'asimmetria appena riscontrata non è l'unico inconveniente della modalità espressiva di sovranità digitale a trazione giurisprudenziale. A ciò deve aggiungersi un processo di frammentazione anche a livello nazionale delle regole giurisprudenziali pensate per il singolo caso, con un nocumento significativo per il principio di certezza del diritto. Più precisamente, i giudici, sia europei che nazionali, nell'inerzia del legislatore che non interveniva sui modelli di esenzione (*melius*: limitazione) di responsabilità previsti dalla richiamata Direttiva 2000/31/CE, si sono esercitati nel coniare nuove ruoli e definizioni per gli *Internet service provider*: da quello attivo a quello passivo[125], passando per quello "sofisticato"[126], creando una moltitudine di nuove figure, a legislazione invariata, a cui corrispondevano diversi livelli di responsabilità per gli assai "cresciuti" e geneticamente modificati soggetti privati *gatekeeeper* dell'ecosistema digitale. Il tutto, ovviamente, in uno scenario caratterizzato da un significativo livello, come si accennava, di frammentazione giurisprudenziale e, conseguentemente, indebolimento del principio delle legittime aspettative.
Una terza controindicazione alla stagione di attivismo giurisprudenziale che si è descritta consiste in una conseguenza, sicuramente involontaria, ma assai rischiosa che emerge dalle decisioni che si sono commentate (in particolare, da *Google Spain*). Si fa riferimento a quella delega in bianco ad un operatore privato delle operazioni di bilanciamento assai delicate tra diritti fondamentali che si è prima richiamata.

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

Preso atto dell'improrogabilità di un intervento normativo per tutte le ragioni esposte nel paragrafo precedente, il legislatore dell'Unione ha deciso, a partire dalla metà degli anni 2010 e sempre più dagli inizi degli anni 2020, di riappropriarsi del ruolo di legislatore, temporaneamente assunto dalla Corte di giustizia, così avviando quello che è stata da più parti definita come la nuova stagione del "costituzionalismo digitale"[127] 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

---

[125] *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.
[126] Tribunale di Roma, sez. IX, 27 aprile 2016, n. 8437.
[127] 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.

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*[128] 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[129].

Proprio da questo punto di vista si comprende, allora, come la nuova stagione europea cui si è accennato si caratterizza per una volontà di riappropriazione, da parte del legislatore, del ruolo di *law maker*, per troppo tempo esercitato – specialmente in ambito digitale e per le ragioni che si sono prima identificate – dalla Corte di Giustizia dell'Unione.

Questa volta, il legislatore è ben consapevole, a differenza della prima fase degli anni 2000 caratterizzata da un liberismo digitale in cui regnava incontrastata l'antitrust, della necessità di una "iniezione" di una visione costituzionalmente orientata. Questo è diventato essenziale una volta che la metamorfosi dei soggetti privati da attori economici a poteri in senso stretto si è completata, per limitare l'influenza di questi poteri e prevenirne gli abusi.

I prossimi paragrafi investigheranno precisamente i momenti più salienti e le fonti di diritto più rilevanti di questa nuova stagione costituzionale dell'Unione, soffermandosi in particolare sulle strategie progressivamente adottate per contrastare le esternalità negative, seguendo l'impostazione e le conseguenti differenziazioni che si sono fatte nel primo paragrafo, dell'ascesa del fattore algoritmico, prima, (par. 6) e dell'intelligenza artificiale in senso stretto – che oltre alla automazione algoritmica, come vedremo, si fonda sui concetti di autonomia, deduzione, predizione e adattabilità –, dopo, (par.7), in termini di tutela dei valori democratici e dello stato di diritto.

6.1 Protezione dati e regolamentazione dell'algoritmo

La nuova stagione della regolamentazione europea del digitale si è aperta con l'adozione, nel 2016, del Regolamento generale sulla protezione dei dati (*General Data Protection Regulation*, GDPR)[130] 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[131], si caratterizza, tuttavia, per una connotazione spiccatamente personalistica e un orientamento maggiormente attento alla stretta interrelazione tra

---

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

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

[130] 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.

[131] 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".

diritto alla privacy e diritto alla protezione dei dati, da un lato, e tutela della dignità umana[132]. 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"*[133].

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"[134], il GDPR, si è osservato, configura un approccio legislativo peculiare che, focalizzandosi sul principio di "responsabilizzazione" (*accountability*) del titolare del trattamento, richiede a quest'ultimo di attivarsi per la protezione dei diritti fondamentali dell'interessato. Infatti, la disciplina rilevante non si focalizza tanto sulla previsione di una serie di prescrizioni e obblighi, il rispetto dei quali consentirebbe al titolare del trattamento di proteggersi dall'inflizione di sanzioni legislative, piuttosto il GDPR prevede che siano gli stessi titolari a valutare l'entità dei rischi – in termini, ovviamente, di tutela della *privacy* e di protezione dei dati – che derivino dalle loro attività e, conseguentemente, ad adottare i necessari correttivi per mitigare tali rischi[135]. 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 disciplina 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[136].
La disciplina introdotta dal GDPR, peraltro, ha riflessi significativi nel contesto della regolamentazione dell'algoritmo e dei processi decisionali automatizzati sotto diversi profili. Del resto non potrebbe essere diversamente, perché l'algoritmo e i processi decisionali automatizzati si fondano su sistemi alimentati da ingenti e amplissime basi di dati.

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

---

[132] 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.
[133] GDPR, considerando 4.
[134] GDPR, art. 17.
[135] 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 Gisella 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.
[136] B. PETKOVA, *Privacy as Europe's first amendment*, in *European Law Journal*, fasc. 25, 2019, p. 140-154.

casi eccezionali[137], 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[138].

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 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[139].

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*)[140], 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

---

[137] 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".

[138] 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.

[139] *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*".

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

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[141]. In ogni caso, l'opinione ormai prevalente è quella che riconosce nell'articolo 22 quanto meno *in nuce*[142], un diritto dell'interessato alla "spiegazione" sottesa alla decisione presa: una conclusione, tra l'altro, supportata anche dal considerando 71 del Regolamento, il quale specifica esplicitamente che tali tipologie di trattamento dovrebbero essere subordinate

> "*a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione.*"

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[143] 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.

6.2 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)[144].

In questo senso, al di là della prospettiva legata alla migrazione, richiamata in apertura e nota come "Bruxelles effect", verso aree regionali differenti dall'*humus* costituzionale europeo, il GDPR ha, in realtà, contribuito a rendere ancora più inespugnabile dall'esterno la fortezza europea a difesa del paradigma valoriale prima richiamato, messo a rischio dall'amplificazione del potere digitale privato. Un tale esercizio di fortificazione è, del resto, comune a tutta una serie di normative di carattere verticale, per singoli settori di competenza, adottate in anni recenti: dalla disciplina di

---

[141] 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.

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

[143] 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.

[144] 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.

riforma del copyright[145] a quella dei servizi media audiovisivi[146], fino alla legislazione europea in materia di prevenzione terroristica[147].

Si tratta di quella che potrebbe essere considerata una prima fase di quella stagione che si è prima definita di costituzionalismo digitale e che si è aperta quale reazione del circuito politico-rappresentativo europeo allo strapotere giurisdizionale della stagione precedente, i cui percorsi e inconvenienti si sono descritti in precedenza.

Tale prima fase è accomunata, come si diceva, da una forte impostazione assiologico-sostanziale di matrice legislativa che ha, però, a sua volta, due inconvenienti di fondo, pur nella sua profonda coerenza con le radici costituzionali europee.

Il primo inconveniente consiste nel rischio di innescare un processo di frammentazione interna, a causa della moltitudine di discipline settoriali richiamate. Questo rischio è simile a quello osservato nella precedente fase di attivismo giudiziale, dove si applicavano regole diverse, anche in termini di modelli di responsabilità per le grandi piattaforme digitali, a seconda della specifica disciplina rilevante. Inoltre, gli Stati membri hanno un significativo margine di manovra, dato l'elevato numero di clausole aperte contenute nei regolamenti, che spesso si rivelano essere delle vere e proprie direttive mascherate.[148].

In questo senso, il GDPR, come si è anticipato anche in precedenza, è stato il primo di una serie di tentativi della Commissione europea, di cui anche la Proposta di Regolamento denominata *Artificial Intelligence Act* ne è testimonianza, di voler dare, attraverso l'etichetta del *nomen iuris* della fonte di riferimento (regolamento), l'illusione di voler ambire a una uniformità delle regole (una sorta di *common roof* europeo) che, in realtà, rischia di tramutarsi (proprio a causa delle clausole di flessibilità cui si faceva riferimento e, quindi, all'ampio margine di manovra, con annesso rischio di geometria variabile, in capo agli stati membri), in un esercizio di armonizzazione (tipico invece delle direttive) che, al massimo, può assicurare un *common floor*.

Il secondo inconveniente è rappresentato dal rischio che, puntando esclusivamente su una cornice valoriale di natura regionale, con caratteristiche peculiari, si tenti di disciplinare un ecosistema digitale che è, per definizione, transnazionale. Questo potrebbe portare a un isolamento radicale dell'Europa, priva di collegamenti con altri poli regionali rilevanti. Tale isolamento rischia di tradursi in un mancato *enforcement* delle regole europee e, più in generale, nell'amplificazione delle distanze con l'altra sponda dell'Atlantico. Ciò metterebbe a rischio la solidità del ponte transatlantico, la cui manutenzione è cruciale per contenere efficacemente il potere digitale privato, ormai consolidato, nel contesto del costituzionalismo moderno[149].

Tali inconvenienti hanno portato a una seconda fase, quella attuale e del futuro prossimo, del costituzionalismo digitale in Europa, che ha una trazione non (soltanto) assiologico-sostanziale, ma, se si può dire così, procedurale o procedimentale[150] e un campo di applicazione "orizzontale", non incentrato su singoli settori, ma trasversale, proprio per evitare quel processo di frammentazione prima menzionato.

---

[145] Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE, GU L. 130/2019.

[146] Direttiva del Parlamento europeo e del Consiglio 14 novembre 2018, n. (UE) 2018/1808, 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, in considerazione dell'evoluzione delle realtà del mercato, GU L. 303/2018.

[147] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online, GU L. 172/2021.

[148] DE GREGORIO, *Democratising online content moderation: A constitutional framework*, cit.

[149] 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.

[150] POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, cit.

Una nuova declinazione o rimodulazione cerca di risolvere le problematiche di opacità e mancata trasparenza che emergono frequentemente nei meccanismi algoritmici dei nuovi poteri. Questo avviene attraverso garanzie procedurali che compensano l'assenza di garanzie sostanziali comparabili a quelle dei rapporti con attori pubblici. Tuttavia, è importante notare che questa declinazione, pur concentrandosi maggiormente sulla dimensione procedurale rispetto alla precedente di natura esclusivamente assiologico-sostanziale, non deve essere confusa con una radicalizzazione di tale orientamento. Questo rischio potrebbe trasformare lo stato in quella che Forsthoff avrebbe chiamato "una macroamministrazione priva di capacità politica"[151] . 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"[152].

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[153], rischia di amplificare la possibilità di collisioni costituzionali e, quindi, di conflitti.

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

Tali salvaguardie possono supportare l'effettiva applicazione dei diritti sostanziali nei confronti dei nuovi attori privati emergenti e, allo stesso tempo, interagire con questi diritti per cercare di contenere lo strapotere algoritmico. Questo è particolarmente rilevante nell'ambito della ricerca sui big data e sulle violazioni della privacy.

Nell'ambito della ricerca sui big data e sulle violazioni della privacy (comprese quelle causate dall'uso di algoritmi predittivi), Crawford e Schultz[154] 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[155] di giusto processo, valori come l'accuratezza, l'equità, l'uguaglianza di *input*, la prevedibilità, la trasparenza, la razionalità e la partecipazione.

---

[151] BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, cit., spec. p. 747; M. BETZU, *Il costituzionalismo digitale: un abuso di denominazione*, in *Scritti in onore di Pietro Ciarlo*, Editoriale Scientifica, Napoli, 2022, vol. 1, p. 3–13.

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

[153] 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.

[154] 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.

[155] 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.

Citron[156] 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[157], 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.

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

7.1 Le coordinate costituzionali

Per comprendere le varie stagioni che, specie in ambito europeo, si sono susseguite con riferimento all'attività di moderazione dei contenuti on line è necessaria una, seppure sommaria e sintetica, disamina delle coordinate costituzionali di riferimento, in relazione alla tutela della libertà di espressione e ai limiti costituzionalmente ammessi a quest'ultima, in una prospettiva che non può non essere transatlantica. Come sempre accade, anche in questo caso, le opzioni di politica del diritto prescelte sono fortemente influenzate dall'*humus* valoriale che caratterizza gli ordinamenti in questione. Semplificando al massimo una questione che meriterebbe ben altro approfondimento, si potrebbe dire che se la parola chiave del costituzionalismo statunitense è "libertà", quella del costituzionalismo europeo, e non poteva non esserlo, è "dignità". Più precisamente, esiste una profonda frattura di fondo che oppone alla visione nordamericana incentrata sull'esaltazione del Primo emendamento, una rappresentazione squisitamente europea fondata sul predominio assiologico della protezione dei dati.

La libertà di espressione è stata interpretata da sempre nel diritto costituzionale statunitense come la stella polare, il diritto che segna la caratterizzazione di quell'ordinamento giuridico. Questo atteggiamento trova emersione nella cornice valoriale adottata dalla Corte Suprema, incline a esaltare, fin dalla prima pronuncia in materia, l'inedita dimensione libertaria del fenomeno *internet*. Da subito, agli occhi della Corte Suprema statunitense, *internet*, *the new free marketplace of ideas*, offre coordinate e spazi nuovi per l'esercizio della libertà di parola, ai quali occorre guardare attraverso lenti e categorie diverse da quelle che si applicano ai media tradizionali. Da qui la scelta, in *Reno v.*

[156] D. K. CITRON, *Technological due process*, in *Washington University Law Review*, fasc. 85, 6, 2008, p. 1249.
[157] CRAWFORD- SCHULTZ, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, cit.

ACLU[158], di mutuare dalla celebre *dissenting opinion* di Justice Holmes in *Abrams*[159] , l'utilizzo della metafora del *free marketplace of ideas*, la cui importazione nell'ordinamento europeo è stata la causa principale, come si dirà, delle questioni costituzionali sollevate dal consolidamento di nuovi attori privati, come anche dimostrato dal parziale fallimento del primo codice di condotta dell'Unione europea in tema di lotta alla disinformazione.

Rispetto all'assetto valoriale statunitense appena descritto, possiamo dire, semplificando, che tale libertà in Europa gioca la sua partita "alla pari" con altri diritti fondamentali e non gode di quella prevalenza assiologica che caratterizza la posizione e l'interpretazione del Primo emendamento nell'ordinamento statunitense.

Ci sono almeno due elementi che confermano questo quadro e sono rintracciabili entrambi all'interno del quadro convenzionale. Innanzitutto, l'art. 10 della Convenzione europea dei diritti dell'uomo, al suo secondo comma, prevede un qualcosa di assolutamente "irricevibile" per il costituzionalismo statunitense. Ovvero, la codificazione espressa, come del resto per tutte le altre libertà e diritti previsti dal medesimo testo convenzionale, di limiti e, quindi, di restrizioni alla stessa libertà, giustificate alla luce della stella polare del costituzionalismo europeo, ovvero il principio di responsabilità.

In secondo luogo, altro concetto sconosciuto al diritto costituzionale d'oltreoceano, la Convenzione (ma anche la Carta dei diritti fondamentali dell'Unione) prevede espressamente la possibilità dell'abuso del diritto[160], a conferma di quell'ottica di non assolutezza, bilanciamento e pari-ordinazione tra diritti, quali caratteristiche delle tradizioni costituzionali comuni europee. Proprio questa impostazione più moderata, che considera la libertà di espressione in modo analogo ad altri diritti pari-ordinati, ha permesso di gettare le fondamenta per interventi normativi più moderni; si pensi al GDPR[161] , alla direttiva *Copyright*[162], e alla revisione della Direttiva in tema di servizi media audiovisivi[163], e, in particolare, al DSA e AI Act, su cui sarà rivolta l'attenzione nei prossimi paragrafi, perché costituiscono il regime privilegiato in termini di moderazione dei contenuti.

7.2 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.
Come menzionato sopra, la Direttiva e-Commerce del 2000[164] introduceva, con riferimento al tema della regolamentazione della moderazione dei contenuti prodotti dagli utenti della rete, una disciplina di tendenziale favore per i fornitori di servizi di intermediazione. La normativa, infatti, introduceva

---

[158] *Reno c. Aclu* 521 U.S. 844 (1997), cit.
[159] *Abrams c. United States* 250 U.S. 616 (1919), cit. Si veda, nello specifico, la *dissenting opinion* di Holmes, pp. 624 ss.
[160] Art. 17 CEDU e art. 54 Carta dei diritti fondamentali dell'Unione europea.
[161] GDPR, cit.
[162] Direttiva sul diritto d'autore e sui diritti connessi nel mercato unico digitale, cit.
[163] 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.
[164] 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.

un regime di esenzione di responsabilità di tali attori, a fronte dell'utilizzo dei loro sistemi per la commissione di attività illecite e per il caricamento e/o la diffusione di contenuti illeciti in rete.

Scopo ultimo del legislatore dell'Unione, nel 2000 appare essere, in sostanza, quello di garantire che l'intermediario che agisca in buona fede sia protetto dal rischio di incorrere in sanzioni per attività illecite di terzi. Un'aspirazione chiaramente apprezzabile e certamente ragionevole, specialmente alle origini del web in cui gli intermediari erano assai più neutrali (rispetto al controllo dei contenuti) e meno sofisticati[165], alla luce della necessità di garantire agli stessi *provider* il godimento dei loro stessi diritti costituzionali, ivi inclusa la libertà di impresa e di iniziativa economica (articolo 16 della Carta dei diritti fondamentali dell'Unione europea). Complementare a questo, l'articolo 15(1) della Direttiva e-Commerce vieta agli Stati membri di imporre ai prestatori di servizi di intermediazione un obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate, né un obbligo generale di ricercare attivamente fatti o circostanze che indichino attività illecite. Come sottolineato dalla Corte di Giustizia, questa proibizione tutela non solo gli interessi economici dei *provider*, ma anche i diritti fondamentali degli utenti, come la riservatezza, la protezione dei dati e la libertà di espressione e informazione[166].

D'altra parte, come già menzionato sopra, il sistema inerentemente liberale introdotto dalla Direttiva e-Commerce ha suscitato dubbi crescenti alla luce, in particolare, del crescente potere degli intermediari digitali, direttamente proporzionale all'ascesa dell'evocato più volte "fattore algoritmico", portando prima la giurisprudenza e, in seguito, il legislatore dell'Unione a ripensare al quadro normativo di riferimento. In particolare, a partire dalla seconda metà degli anni 2010, l'Unione ha adottato una serie di misure legislative di settore volte a introdurre nuovi obblighi a carico dei *provider* – e soprattutto a carico dei fornitori di servizi di *hosting* – al fine di responsabilizzarli maggiormente, nell'ottica di contrastare condotte illecite in rete. Così, con la Direttiva (UE) 2018/1808[167], 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[168] 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[169] ha introdotto una specifica disciplina volta al contrasto dei contenuti terroristici online.

Intanto il fattore algoritmico ha giocato un crescente ruolo di protagonista nell'attività di moderazione dei contenuti.

Più precisamente, per comprendere quando l'automazione incontra (e influenza) la libertà di espressione, basterebbe osservare attentamente come fluisce l'informazione online alla luce dei processi di moderazione dei contenuti propri delle piattaforme digitali. Infatti, per organizzare e moderare innumerevoli contenuti ogni giorno, le piattaforme si affidano anche a meccanismi di automazione per decidere se rimuovere contenuti o segnalare alcune espressioni ai moderatori umani. Il risultato di tale delega algoritmica appare problematico per lo stato di diritto da diverse prospettive.

---

[165]E-Commerce Directive, considerando 42.

[166]CGUE, causa C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, sentenza del 24 novembre 2011, para. 50-52: "Per di più, gli effetti di detta ingiunzione non si limiterebbero al FAI [fornitore di accesso ad Internet, *NdR*] coinvolto, poiché il sistema di filtraggio controverso è idoneo a ledere anche i diritti fondamentali dei clienti di tale FAI, ossia il loro diritto alla tutela dei dati personali e la loro libertà di ricevere o di comunicare informazioni, diritti, questi ultimi, tutelati dagli artt. 8 e 11 della Carta. Da un lato, infatti, è pacifico che l'ingiunzione di predisporre il sistema di filtraggio controverso implicherebbe un'analisi sistematica di tutti i contenuti, nonché la raccolta e l'identificazione degli indirizzi IP degli utenti all'origine dell'invio dei contenuti illeciti sulla rete, indirizzi che costituiscono dati personali protetti, in quanto consentono di identificare in modo preciso i suddetti utenti. Dall'altro, detta ingiunzione rischierebbe di ledere la libertà di informazione, poiché tale sistema potrebbe non essere in grado di distinguere adeguatamente tra un contenuto lecito ed un contenuto illecito, sicché il suo impiego potrebbe produrre il risultato di bloccare comunicazioni aventi un contenuto lecito". Allo stesso modo, vedi CGUE, causa C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*, sentenza del 16 febbraio 2012, para. 48-50.

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

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

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

In primo luogo, i sistemi di intelligenza artificiale contribuiscono a identificare il livello di protezione dei diritti fondamentali, stabilendo di fatto uno standard privato di tutela nell'ambiente digitale. In secondo luogo, vi è anche un problema di prevedibilità e certezza giuridica, poiché tali determinazioni automatiche offuscano le linee di confine tra standard pubblici e privati. Questo ci porta al terzo punto: la mancanza di trasparenza e responsabilità nella decisione riguardante i limiti da apportare all'esercizio della libertà di espressione online. [170]

Proprio alla luce di tali nuove insidie, nel 2022, con l'approvazione del già menzionato *Digital Services Act*[171], 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)[172]. 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[173] e, quindi, andare direttamente a intervenire su uno degli aspetti caratterizzanti la società algoritmica.

Il pacchetto DSA/DMA si caratterizza peraltro, come anticipato, per una trazione non (soltanto) assiologico-sostanziale, ma anche per una dimensione intrinsecamente procedurale o procedimentale ed un campo di applicazione "orizzontale" Si è già anticipato che, in tal senso, il pacchetto costituisce una nuova declinazione del costituzionalismo digitale, una nuova stagione rispetto al paradigma del GDPR, che tenta di risolvere le problematiche in termini di opacità che emergono frequentemente nei meccanismi algoritmici propri dei nuovi poteri, attraverso la predisposizione soprattutto di garanzie procedurali[174].

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"[175].

Occorre tuttavia specificare che tale sistema di obblighi si caratterizza per il fatto di essere basato su un approccio asimmetrico, nel senso che non tutti gli intermediari sono soggetti alle stesse regole. Nello specifico, il DSA prevede quattro livelli di obblighi:

- Ad applicazione "universale", previsti cioè per qualsiasi tipo di *provider* di servizi di intermediazione;
- Obblighi "base", cui sono tenuti solamente gli *hosting provider*;
- Obblighi "avanzati", applicabili a quella sottocategoria di *hosting provider* che il DSA identifica come "piattaforme online", ovverosia quei "serviz[i] di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico" e che, quindi, non si limitano a ospitare i contenuti ma sono orientati alla disseminazione degli stessi;
- Obblighi "speciali", rivolti a quelle specifiche categorie di piattaforme online che raggiungano dimensioni tali da essere riconosciute come piattaforme online o motori di ricerca "molto grandi" (rispettivamente, VLOP e VLOSE)

---

[170] 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.

[171] 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.

[172] Regolamento sui mercati digitali, cit.

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

[174] Volendo, ora, O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, pp. 569–594.

[175] DSA, Capo III.

Sebbene non sia in questa sede possibile ripercorrere esaustivamente il plesso di nuovi obblighi introdotti dal Regolamento, è possibile identificare almeno tre linee direttrici che orientano l'azione della nuova normativa.

In primo luogo, il DSA mira a promuovere forme di trasparenza aggiuntive in termini di pratiche di moderazione e organizzazione dei contenuti: così, a puro titolo di esempio, oltre a prevedere tutta una serie di obblighi concernenti la periodica pubblicazione di relazioni sullo svolgimento di tali pratiche[176], l'articolo 14 – facente parte della categoria di obblighi aventi applicazione "universale" – fissa regole specifiche relative alla pubblicazione ed *enforcement* dei termini e delle condizioni di utilizzo dei servizi; mentre l'articolo 17 prevede che tutti gli *hosting provider* forniscano "a tutti i destinatari del servizio interessati una motivazione chiara e specifica per le … restrizioni imposte a motivo del fatto che le informazioni fornite dal destinatario del servizio costituiscono contenuti illegali o sono incompatibili con le proprie condizioni generali".

In secondo luogo, il DSA introduce – come già accennato sopra – alcune importanti garanzie di carattere procedurale a tutela degli utenti stessi della rete. Del resto, in tal senso, le menzionate norme in materia di trasparenza rappresentano esse stesse delle precondizioni essenziali all'esercizio da parte dei destinatari dei propri diritti e, pertanto, rappresentano esse stesse delle garanzie procedurali. D'altro canto, a tali norme il DSA aggiunge tutta una serie di ulteriori obblighi inclusa, per esempio, la necessità di prevedere – per gestori di piattaforme online e di piattaforme online e motori di ricerca molto grandi – un sistema interno di gestione dei reclami per permettere agli utenti di contestare le decisioni precedentemente prese dalla piattaforma.

In terzo luogo, il Regolamento (UE) 2022/2065, presa coscienza dei rischi cui internet apre in termini di circolazione di contenuti illeciti e di realizzazione di condotte illecite o dannose, prevede alcuni doveri in capo ai *provider* orientati a una maggiore responsabilizzazione degli stessi in termini di riduzione di tali rischi. Se, dunque, il sistema di esenzione dalla responsabilità per fatto di terzi come elaborato dalla Direttiva e-Commerce è rimasto tuttora in piedi, i fornitori di servizi intermediari sono tuttavia soggetti a importanti forme di responsabilità – amministrativa – per fatto proprio laddove non rispettino le nuove regole di diligenza del DSA. Occorre innanzitutto ricordare, in questo senso, l'articolo 16 il quale impone agli *hosting provider* la predisposizione di un meccanismo di "segnalazione e azione" che consenta agli utenti di indicare loro "la presenza nel loro servizio di informazioni specifiche che tale persona o ente ritiene costituiscano contenuti illegali": segnalazione che, in sostanza, ha l'effetto di impedire al *provider* di avvalersi dell'esenzione da responsabilità per contenuti ti terzi in quanto, chiaramente, non sarà a questo punto più nella possibilità di argomentare di non essere "effettivamente a conoscenza delle attività o dei contenuti illegali"[177]. Ancora, gli *hosting provider* sono tenuti a informare le autorità giudiziarie in caso vengano a conoscenza di "informazioni che fanno sospettare che sia stato commesso, si stia commettendo o probabilmente sarà commesso un reato che comporta una minaccia per la vita o la sicurezza di una o più persone"[178], mentre le sole piattaforme online sono tenute ad adottare alcune misure di contrasto agli abusi da parte degli utenti dei loro servizi, quali per esempio la sospensione di destinatari che ripetutamente forniscano contenuti manifestamente illegali[179].

Peraltro, con riferimento a questo terzo plesso di obblighi, di particolare rilievo appare essere la previsione, agli articoli 34 e 35 di un meccanismo di valutazione e attenuazione dei rischi sistemici derivanti dalla fornitura di piattaforme online e motori di ricerca di dimensioni molto grandi. In particolare, i *provider* di tali servizi sono tenuti a valutare, e conseguentemente ad elaborare sistemi di mitigazione adeguati, l'entità dei rischi sistemici connessi a:

a. la diffusione di contenuti illegali tramite i loro servizi;
b. eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali sanciti nella Carta dei diritti fondamentali dell'Unione europea, in particolare i diritti fondamentali

[176] DSA, artt. 15, 24, 39.
[177] *Ibidem*, art. 6.
[178] *Ibidem*, art. 18(1).
[179] *Ibidem*, art. 23(1).

alla dignità umana, al rispetto della vita privata e familiare, alla tutela dei dati personali, alla libertà di espressione e di informazione, inclusi la libertà e il pluralismo dei media, e alla non discriminazione, al rispetto dei diritti del minore, così come all'elevata tutela dei consumatori;

c. eventuali effetti negativi, attuali o prevedibili, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica;
d. qualsiasi effetto negativo, attuale o prevedibile, in relazione alla violenza di genere, alla protezione della salute pubblica e dei minori e alle gravi conseguenze negative per il benessere fisico e mentale della persona[180].

L'obbligo per i fornitori di VLOP e VLOSE rappresenta, verosimilmente, uno degli aspetti centrali all'interno dell'intero sistema del DSA con riferimento a quel processo di adeguamento – e "costituzionalizzazione" – delle forme del potere esercitate dai grandi protagonisti globali del mercato digitale all'interno della società algoritmica.

7.3 (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. Infatti, al giorno d'oggi, i sistemi di moderazione e di cura dei contenuti sono prevalentemente amministrati in modo automatico, attraverso il ricorso a sistemi di IA capaci, tra le altre cose, di operare da filtro per contrastare la presenza di materiali illeciti, di raccogliere i dati e le informazioni relative agli utenti, al fine di meglio strutturare la presentazione e l'organizzazione dei contenuti secondo le loro preferenze, nonché, di ridurre la visibilità o de-monetizzare le informazioni che possano essere in qualche modo dannose.

Se il GDPR, in particolare all'articolo 22, si focalizza soprattutto sulla necessità di tutelare la dignità dell'interessato a fronte di processi decisionali automatizzati e di forme di profilazione condotte attraverso l'uso dell'algoritmo, il DSA associa a questa finalità quella di "imbrigliare" il potenziale del potere computazionale dei *provider* e dei loro sistemi algoritmici, allo scopo di promuovere gli interessi e i valori democratici dell'Unione stessa. Tale doppia interpretazione delle tecnologie dell'automazione, quali sfide per la tutela di diritti fondamentali individuali e al tempo stesso quali *asset* per la promozione di valori democratici, emerge icasticamente dalla disciplina del summenzionato meccanismo di valutazione e attenuazione dei rischi sistemici connessi alla previsione di piattaforme online e di motori di ricerca di dimensioni molto grandi.

Difatti, l'articolo 35(1) del Regolamento (UE) 2022/2065 prevede, da un lato, che gli strumenti di mitigazione di tali rischi possano includere, tra l'altro, "la sperimentazione e l'adeguamento dei loro sistemi algoritmici, compresi i loro sistemi di raccomandazione" e, dall'altro lato, che, nell'adottare qualsivoglia meccanismo di attenuazione di rischi, i *provider* abbiano cura che tali misure siano "ragionevoli, proporzionate ed efficaci, adattate ai rischi sistemici specifici individuati … prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali". Emerge, in sostanza, una consapevolezza da parte del legislatore euro-unitario della necessità di fare affidamento su sistemi algoritmici per il governo dello spazio digitale e per limitare la diffusione di materiale illecito, anche e soprattutto a fronte delle attuali dimensioni del flusso informazionale digitale. D'altro canto, a tale consapevolezza se ne associa un'altra corrispondente alle preoccupazioni – già evidenti nel GDPR – che l'uso di quei sistemi fa emergere in termini di tutela della dignità umana, dell'autodeterminazione informazionale, della *privacy*, della protezione dei dati personali e della libertà di espressione e di informazione.

In linea con questo secondo aspetto, il tema dell'utilizzo di sistemi decisionali automatizzati rientra in una pluralità di ulteriori norme relative alla tutela degli interessi individuali dei destinatari dei servizi. In particolare, ponendosi in continuità con lo stesso GDPR, il DSA prevede alcune norme finalizzate a garantire un seppur minimo livello di intervento umano a fronte del ricorso all'algoritmo

[180] *Ibidem*, art. 34(1).

per scopi di moderazione dei contenuti, oltre che un certo grado di trasparenza con riferimento all'utilizzo di tali sistemi.

Il già menzionato articolo 14, relativo alle regole concernenti la predisposizione di termini e condizioni di utilizzo, prevede, per esempio, che le informazioni rese agli utenti riguardino, tra l'altro, "le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti, compresi il processo decisionale algoritmico e la verifica umana". Inoltre, ai sensi dell'articolo 15, le relazioni per la trasparenza devono specificare, con riferimento all'utilizzo di strumenti automatizzati, "la descrizione qualitativa, la descrizione delle finalità precise, gli indicatori di accuratezza e il possibile tasso di errore degli strumenti automatizzati utilizzati nel perseguimento di tali scopi e le eventuali garanzie applicate". Allo stesso modo, con riferimento alla motivazione che gli *hosting provider* di piattaforme online devono offrire ai destinatari dei servizi ogniqualvolta li sottopongano a misure sanzionatorie, il DSA specifica che tale motivazione deve indicare "informazioni sugli strumenti automatizzati usati per adottare la decisione, ivi compresa l'informazione che indichi se la decisione sia stata adottata in merito a contenuti individuati o identificati per mezzo di strumenti automatizzati"[181], mentre ai gestori di piattaforme online è richiesto di assicurare che il sistema interno di gestione dei reclami si concluda con decisioni "prese con la supervisione di personale adeguatamente qualificato e non avvalendosi esclusivamente di strumenti automatizzati"[182].

Il DSA, dunque, si caratterizza per il fatto di trasporre, nel contesto della moderazione dei contenuti in rete, gli stessi principi costituzionali che sono di fatto stati espressi dal GDPR con riferimento processi decisionali automatizzati. Ciò avviene alla luce della consapevolezza dell'iniezione algoritmica che tale moderazione ha avuto negli ultimi anni, oltre che della necessità di promuoverne un uso coerente con i valori democratici dell'Unione, a fronte dell'ormai insuperabile necessità assoluta di tali strumenti. In questo senso, è possibile cogliere nel DSA un passaggio ulteriore del "costituzionalismo digitale" dell'Unione stessa, orientato verso un sempre più equilibrato bilanciamento tra rischi e vantaggi dell'automazione[183].

In sintesi, uno dei principali contributi della legislazione appena evocata è l'istituzione di un nuovo quadro normativo per la moderazione dei contenuti. Questo quadro, come è stato giustamente notato[184], crea "*a semi-constitutional structure that defines the meta-procedural framework for governing digital platform content moderation actions*". La struttura include, ad esempio, disposizioni riguardanti la notifica e l'obbligo di motivare determinate decisioni riguardanti, ad esempio, la rimozione di contenuti, la disabilitazione dell'accesso ai contenuti o la retrocessione di contenuti (*notice and take action*),[185] l'istituzione di un sistema interno di gestione dei reclami che consente agli utenti di presentare reclami elettronicamente e gratuitamente contro una decisione presa dal fornitore,[186] ma anche la creazione di un sistema di risoluzione delle controversie extragiudiziale in grado di offrire un rimedio accessibile,[187] alternativo a quello, espressamente garantito, di accesso alla giustizia[188].

Infine, si aggiunga – nel quadro della cornice di indagine, che si è finora concentrata sull'ascesa del fattore algoritmico e sulla sua crescente prevalenza rispetto a quello umano (ancora presente, a differenza di quanto accade in quel particolare processo di automazione che è costituito

---

[181] *Ibidem*, art. 17(3)(c).
[182] *Ibidem*, art. 20(6).
[183] 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.
[184] O. PEREZ - N. WIMER, *Algorithmic Constitutionalism*, in A. GOLIA - G. TEUBNER, *Indiana Journal of Global Legal Studies*, fasc. 30, 2, 2023.
[185] DSA, art. 17(1).
[186] *Ibidem*, art. 20 (1).
[187] *Ibidem*, art. 21.
[188] Il DSA, diversamente quanto accade per l'AI Act, chiarisce che il destinatario del servizio può avviare, in qualsiasi momento, un procedimento per contestare la decisione assunta dal fornitore di piattaforme online davanti a un organo giurisdizionale, in conformità al diritto applicabile (DSA, art. 21 (1)).

dall'intelligenza artificiale in senso stretto) – che, nell'esercizio di scrittura del DSA, si è cercato di salvaguardare la presenza, seppur evidentemente accessoria, del principio personalistico.

Il DSA richiede ai *providers* di piattaforme online di garantire che le decisioni prese dal sistema interno di gestione dei reclami "siano adottate sotto la supervisione di personale adeguatamente qualificato e non esclusivamente tramite mezzi automatizzati" e che i destinatari del servizio possano comunicare direttamente e rapidamente con il fornitore in modo *user-friendly*, senza affidarsi esclusivamente a strumenti automatizzati[189]. I *providers* sono, inoltre, tenuti a includere informazioni sull'uso di mezzi automatizzati nelle notifiche inviate agli utenti[190].

Ancora più chiaro al riguardo l'art. 42 del DSA che, solo in riferimento alle *Very Large Platforms* (*because size matters*) impone a queste ultime, di indicare chiaramente "le risorse umane dedicate dal fornitore alla moderazione dei contenuti in relazione al servizio offerto nell'Unione". Un tale obbligo non avrebbe senso con riferimento ai servizi offerti dai modelli di intelligenza artificiale di carattere generativo. Ed è una delle differenze sostanziali tra automazione, che caratterizza la stagione della combinazione tra algoritmo e dati, e autonomia, elemento distintivo di quell'ecosistema digitale – non di una semplice tecnologia, lo si ribadisce – costituito dall'intelligenza artificiale, alla cui analisi saranno dedicati i prossimi paragrafi.

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

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

In effetti, se, come si è detto, il GDPR ha introdotto per primo una fondamentale previsione in tema di soggezione a decisioni prese secondo modalità automatizzate, lo stesso sembra, peraltro, trattare tale fattispecie come un'ipotesi, per così dire, "residuale", a fronte del tradizionale trattamento umano dei dati. Inoltre, come è stato osservato da Giusella Finocchiaro, il GDPR manca di tener conto delle applicazioni di intelligenza artificiale fondate sui *big data* e, dunque, manca di considerare il sempre più rilevante fenomeno dei trattamenti di dati di massa[191].

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[192]. 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*.

---

[189] DSA, art. 20(6) and art. 12(1).

[190] DSA, art. 16 (6).

[191] 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.

[192] 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.

La cybersociety è il terzo tipo di società, frutto della modernizzazione della società digitale, per effetto delle molteplici, interconnesse e alluvionali applicazioni del digitale. Noi costituiamo la cybersociety, la alimentiamo attraverso le nostre relazioni digitali e viviamo al suo interno. Si tratta dell'evoluzione della società digitale, determinata dallo sviluppo della tecnologia digitale: l'autoapprendimento, i sistemi di controllo autonomo, la cooperazione tra uomo e macchina, il supercomputing. Nella società digitale prevale il network, nella cybersociety prevale l'automazione. La cybersociety ha tutte le caratteristiche della società digitale, potenziate dagli sviluppi di quella tecnologia[193].

L'effetto di tali importanti trasformazioni si intravedono, peraltro, già nelle più recenti legislazioni dell'Unione in materia. Come si è avuto modo di illustrare sopra, il DSA è un esempio particolarmente significativo in tal senso. Esso, infatti, da un lato, riconosce l'ineluttabilità dell'automazione nell'ambito della moderazione dei contenuti online e, conseguentemente, l'inevitabilità di un trattamento massivo dei dati concernenti gli utenti e i contenuti da loro postati e, dall'altro lato, cerca di orientare l'utilizzo di quegli strumenti tecnologici al fine di promuovere il perseguimento degli interessi costituzionali e democratici dell'Unione.

D'altra parte, un ulteriore aspetto di particolare rilievo, che già emerge dalla riportata citazione di Violante, concerne il progressivo passaggio da un approccio all'automazione fondato sull'"algoritmo" a una prospettiva sempre più fondata sull'"intelligenza artificiale". 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[194] –, 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[195]. 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[196]. La definizione che l'AI Act dà di intelligenza artificiale, che sarà esaminata nel paragrafo successivo, sembra confermare le caratteristiche appena evidenziate in quanto si fonda, alla luce del meccanismo di apprendimento automatico, sui concetti di autonomia, adattabilità e capacità di deduzione e predizione.

In effetti, all'interno del panorama scientifico-tecnologico caratterizzante l'IA, con particolare riferimento all'intelligenza artificiale di natura generativa, si sta progressivamente affermando l'utilizzo di sistemi di *machine learning* e, addirittura, di *deep learning*, i quali, fondandosi su basi statistiche piuttosto che su basi logico-formali, presentano l'indubbio vantaggio di un ben più elevato grado di efficienza ed efficacia, ma sollevano, nel contempo, nuove e importanti sfide che toccano l'essenza dello stato di diritto e sono connessi alla trasparenza degli stessi processi decisionali e ai rischi connessi all'errore, nonché quelli relativi alla possibilità di forme di discriminazione; ma anche

---

[193] VIOLANTE, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, cit.
[194] Cons. Stato, Sez. III, sentenza del 25 novembre 2020, n. 7891, paragrafo 9.1 in diritto.
[195] 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.
[196] *Ibidem*.

sfide derivanti paradossalmente dal crescente grado di sofisticatezza degli stessi sistemi di intelligenza artificiale: si pensi, in tal senso, al fenomeno dei *deep-fake*, contenuti sintetici o comunque manipolati, caratterizzati da un elevato grado di verosimiglianza.

Il rapporto tra intelligenza artificiale e disinformazione sarà oggetto di una specifica sezione conclusiva, dopo aver però prima guardato a qual è stata la reazione dell'Unione, in termini di regolazione, al mutamento di paradigma tecnologico dall'algoritmo all'intelligenza artificiale in senso stretto, specialmente di carattere generativo. Un mutamento che chiaramente porta con se, come anticipato in apertura, un'ulteriore emarginazione del fattore umano, con tutte le implicazioni per le democrazie costituzionali che hanno quale base portante il principio personalistico.

8.1 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, prima della scorsa estate, del più volte del Regolamento sull'intelligenza artificiale[197]. 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[198].
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 virtu*ali"[199].

Ritorna l'elemento caratterizzante l'intelligenza artificiale che, fondandosi per lo più su sistemi di *machine learning*, si caratterizza per la capacità di elaborare autonomamente regole di inferenza a partire dai dati utilizzati per operare un esercizio di "addomesticamento" degli stessi. Quindi, capacità computazionale, forza di calcolo, quantità di dati a disposizione, autonomia nella capacità di inferire decisioni da *input* ricevuti e capacità predittiva sono gli elementi caratterizzanti il nuovo ecosistema digitale dell'intelligenza artificiale. L'accelerazione in termini di innovazione, inutile ribadirlo, è fenomenale. Non si ha a che fare esclusivamente con automazione algoritmica, che non implica l'assenza di partecipazione e programmazione umane, ma con una nuova autonomia che, come ricordato nel considerando 12 dell'AI Act, si caratterizza per "un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano". Ovviamente, anche il potenziale di rischio è direttamente proporzionale a tale capacità di discontinuità con lo *status quo* in termini tecnologici e per questo l'Unione europea ha tentato di adottare un modello di regolazione assai ambizioso, attraverso il già più volte evocato Artificial Intelligence Act. Non è questa la sede per un esame puntuale della disciplina. In continuità con il

---

[197] Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale, cit.

[198] 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.

[199] AIA, art. 3(1). Interessante notare che nella proposta normativa della Commissione europea, che precede il cataclisma prodotto dall'esplosione dell'AI di tipo generativo, la definizione di intelligenza artificiale faceva ancora riferimento ad una supervisione umana. Riferimento scomparso invece nella definizione presente nel testo finale che ha dovuto essere di fatto parzialmente riscritto, a cominciare dai profili definitori, proprio a causa del cataclisma prima evocato.

percorso adottato con riguardo alle reazioni del costituzionalismo europeo in risposta alle nuove sfide poste dal processo incrementale di automazione, con conseguente ascesa del fattore algoritmico ed emarginazione di quello umano, si tenterà ora una valutazione della risposta europea alla stagione tecnologica – quella dell'intelligenza artificiale – in cui tale processo sembra essersi perfezionato. In particolare, dopo un brevissimo riferimento al meccanismo sottostante l'esercizio della regolazione che caratterizza l'AI Act, si guarderà al modello più dirompente, sotto il profilo dell'innovazione tecnologica, di intelligenza artificiale, ovvero a quella di natura generativa. Anche nel caso dell'AI Act, tra l'altro, il tentativo di contemperare interessi e finalità talora contrapposte – esigenze dello sviluppo tecnologico e del mercato, da un lato, ed esigenze di tutela di principi e valori democratici, dall'altro – è stato declinato attraverso il ricorso a un approccio basato sul rischio: attraverso, cioè, una categorizzazione di differenti livelli di rischio associati alle applicazioni di IA, cui corrisponde specularmente una graduazione della severità dei regimi giuridici applicabili.

Come si è avuto modo di osservare altrove[200], 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[201].

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*. 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[202]. 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[203].

Il secondo livello è costituito, invece, dai sistemi di IA categorizzati come "ad alto rischio", individuati sulla base della normativa vigente in materia di sicurezza dei prodotti ovvero sulla base dell'Allegato III dello stesso Regolamento[204], il quale include in particolare i seguenti settori: biometria; infrastrutture critiche; istruzione e formazione professionale; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; attività di contrasto; migrazione, asilo e gestione del controllo delle frontiere; amministrazione della giustizia e processi democratici. Tale categoria di rischio rappresenta, peraltro, la più rilevante nell'economia dell'intero Regolamento, in quanto ad essa è dedicata la maggioranza delle disposizioni normative volte a prevedere tutta una serie di

---

[200] DE GREGORIO -DUNN, *The European risk-based approaches: Connecting constitutional dots in the digital age*, cit.
[201] FINOCCHIARO, *Intelligenza artificiale. Quali Regole*, cit. pp. 121-122.
[202] AIA, art. 5.
[203] 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.
[204] AIA, art. 6.

obblighi, specie con riferimento ad una valutazione del rischio *ex ante*, da effettuare prima dell'immissione del prodotto sul mercato, per provare a prevenire i rischi connessi all'uso di sistemi di intelligenza artificiale applicati ad aree assai sensibili. Questo processo deve essere condotto prima che il sistema venga introdotto sul mercato ed è finalizzato a identificare e mitigare eventuali rischi che possano compromettere il rispetto dei diritti fondamentali sanciti dal quadro costituzionale europeo, tra cui il diritto alla *privacy*, alla protezione dei dati e il diritto alla non discriminazione. In tale contesto, è particolarmente importante considerare che i sistemi di intelligenza artificiale applicati ad aree sensibili – come la sorveglianza biometrica,[205] la giustizia e i servizi sanitari – possono avere impatti significativi su diritti umani essenziali[206].

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[207] e da filtri *spam* impiegati nella gestione della posta elettronica, si caratterizza per l'assenza di una specifica regolazione a riguardo.

La classificazione del rischio, dunque, adotta un approccio doppio: in parte si focalizza sugli usi di IA che possono essere considerati maggiormente rischiosi per gli individui, in altra parte, invece, si focalizza sulla "tipologia" di IA, senza badare particolarmente al contesto in cui viene utilizzata. In altre parole, il Regolamento, per i casi non percepiti come particolarmente rischiosi, si concentra principalmente sugli obblighi di trasparenza e sulla mitigazione dei rischi sistemici, ma trascura di fornire indicazioni su come garantire una vera *accountability* nell'integrazione di tali sistemi nei processi democratici. Un caso emblematico è quello dei *deepfake*, una pratica odiosa spesso utilizzata per amplificare le discriminazioni di genere, in particolare contro le donne. Nonostante i gravi danni che l'uso dei *deepfake* può causare alle vittime, l'AI Act classifica questa tecnologia come a "rischio limitato", sottoponendola solo agli obblighi di trasparenza. Ad esempio, detti obblighi consisteranno nell'inserire la dicitura "*deepfake*" nella presentazione del contenuto[208]. È chiaramente controintuitivo che chiunque voglia generare un contenuto tale da mistificare una realtà relativa a una persona o una notizia vada a rispettare detto obbligo. Tuttavia, è evidente che le conseguenze per le vittime dei *deepfake* siano molto rilevanti. E per "vittime" non si intende solo la persona la cui immagine viene distorta, ma anche tutti coloro che potrebbero essere ingannati da informazioni false trasmesse tramite video manipolati[209].

Inoltre, non è chiaro chi debba assumersi la responsabilità ultima per l'uso di questi sistemi in contesti delicati come le campagne elettorali o la gestione dei dati personali dei cittadini, spesso raccolti e analizzati da IA per fini politici. Senza un quadro giuridico solido che affronti questi aspetti, il rischio è che l'intelligenza artificiale possa diventare un agente opaco, capace di influenzare indirettamente decisioni critiche senza una chiara attribuzione di responsabilità.

---

[205] 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.

[206] 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.

[207] 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.

[208] AIA, art. 50(4).

[209] 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.

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

Un discorso a parte meritano poi i cosiddetti modelli di IA per finalità generativa (*general purpose AI*, GPAI)[210], 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 essa la questione relativa a come regolamentare la c.d. intelligenza generativa, su cui si tornerà tra un momento[211].

I modelli fondativi prima richiamati 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 un'assai significativa sfida a livello regolatorio[212], a causa delle implicite difficoltà connesse alla necessaria contemperazione 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[213]. 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[214].

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[215], in quanto abbiano portata 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"[216]. Sono tali,

---

[210] "*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.)

[211] 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.

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

[213] . DONATI, *Intelligenza artificiale e diritti fondamentali nel regolamento sull'intelligenza artificiale*, in O. Pollcino, F:Donati, G. Finocchiaro, F. Paoulcci, Il Regolamento europeo sull'intelligenza artificiale. Analisi, criticità e prospettive, Giuffrè, in corso di pubblicazione

[214] Esemplificativo della portata orizzontale delle problematiche individuate è la tutela del diritto d'autore, come bene evidenziano C. GEIGER E V. IAIA, in *Generative AI, Digital Constitutionalism and Copyright: Towards a Statutory Remuneration Right Grounded in Fundamental Rights*, *MediaLaws*, 2023, https://www.medialaws.eu/generative-ai-digital-constitutionalism-and-copyright-towards-a-statutory-remuneration-right-grounded-in-fundamental-rights/.

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

[216] Come si menzionava *supra,* il Cons. 110 specifica che "In particolare, gli approcci internazionali hanno finora rilevato la necessità di prestare attenzione ai rischi derivanti da potenziali usi impropri intenzionali o da involontari problemi di controllo relativi all'allineamento con l'intento umano; […] alle capacità informatiche offensive, come le modalità per

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"[217], da valutarsi "sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento"[218], 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[219].

A questo punto può essere più chiaro il rapporto tra modelli fondativi e l'ultima frontiera dell'intelligenza artificiale – la cui capacità di innovazione è direttamente proporzionale alla possibilità di collisione con il livello di tutela dei diritti fondamentali proprio del costituzionalismo europeo – , ovvero la già richiamata AI di matrice generativa.

I modelli fondativi, infatti, sono generalmente capaci di produrre grandi quantità di *output*. In tal senso, essi rappresentano strumenti particolarmente efficienti ed efficaci ai fini della generazione di contenuti (testi, immagini, video, audio), siano essi unimodali ovvero multimodali. Di conseguenza, tali modelli presentano significative potenzialità ai fini della loro applicazione in termini di IA "generativa" (*generative AI*).

Come ha notato Pietro Dunn[220], l'IA generativa, caratterizzandosi precisamente per la sua capacità di generare contenuti a partire da *output* 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 produrre contenuti, ivi inclusi, per esempio, i "filtri" di Instagram[221].

A latere della classificazione di genere, inoltre, una discussione che è scarsamente considerata dall'AI Act, a parte i richiami ivi effettuati, è l'ambito di applicazione in cui inserire detti sistemi di IA. Il discorso varrebbe in generale per tutti quanti i sistemi, ma in special modo per quelli di IA generativa. In altre parole, a parte la divisione di rischio sistemico e non rischio, e a parte gli obblighi di trasparenza, chi e come si decide l'integrazione di questi sistemi nel grande nucleo del processo democratico?

La questione dell'integrazione dei sistemi di IA generativa nei meccanismi democratici va ben oltre la semplice classificazione di rischio. Essa tocca profondamente temi come l'impatto sulle

---

consentire la scoperta, lo sfruttamento o l'uso operativo delle vulnerabilità; agli effetti dell'interazione e dell'uso di strumenti, compresa, ad esempio, la capacità di controllare i sistemi fisici e di interferire con infrastrutture critiche; ai rischi derivanti da modelli che realizzano copie di sé stessi o "autoreplicanti" o che addestrano altri modelli; […] all'agevolazione della disinformazione o alla violazione della vita privata con minacce ai valori democratici e ai diritti umani; al rischio che un particolare evento possa provocare una reazione a catena con notevoli effetti negativi che potrebbero interessare fino a un'intera città, un intero settore o un'intera comunità".

[217] AIA, art. 3(64).

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

[219] *Ibidem*, art. 51(1)(b). Come ci anticipava, gli articoli 51 e 52 dell'AI Act distinguono tra modelli di intelligenza artificiale a uso generale e quelli con rischi sistemici. Un modello è considerato a rischio sistemico quando la quantità di calcolo cumulativa utilizzata per il suo addestramento, misurata in operazioni a virgola mobile (FLOPS), supera la soglia di 10^25. Tuttavia, il fornitore ha la possibilità di dimostrare che il sistema non presenta tali rischi. Il problema principale risiede nel fatto che l'ampio ricorso all'autocertificazione può, da un lato, sovraccaricare i *deployer* di responsabilità e, dall'altro, se non accompagnato da un'applicazione robusta e armonizzata del Regolamento, rischia di portare a una mancata o insufficiente attuazione delle norme. Ciò potrebbe favorire l'esclusione di alcuni obblighi previsti dall'AI Act sulla base dell'autodichiarazione dei fornitori. 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*, in *Yale Journal of Law and Technology*, fasc. 26, 3, 2024.

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

[221] 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/.

decisioni politiche, la manipolazione dell'opinione pubblica e il ruolo che questi sistemi possono giocare nella formazione del consenso[222]. La crescente autonomia di tali tecnologie solleva interrogativi cruciali su come i processi decisionali democratici possano essere influenzati o distorti dall'uso massiccio di intelligenze artificiali in ambiti sensibili come la comunicazione politica, l'informazione e persino l'analisi predittiva per fini elettorali.

Il processo decisionale su chi e come possa integrare l'IA nel tessuto democratico non è sufficientemente regolamentato, come vedremo nel paragrafo che segue, dall'AI Act. Il regolamento lascia aperti molti interrogativi su quali meccanismi di controllo debbano essere implementati per garantire che queste tecnologie siano utilizzate in modo etico e trasparente, soprattutto considerando che molte IA generative possono produrre contenuti che influenzano direttamente l'opinione pubblica, potenzialmente erodendo la fiducia nei processi democratici.

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

L'AI Act, a bene vedere, è innanzitutto l'espressione, sotto il profilo della regolamentazione, di un grande ripensamento rispetto ad una delle grandi asimmetrie regolative che caratterizzano l'industria del digitale rispetto a qualsiasi altra industria. Nessuna licenza, nessun obbligo di pubblicare dei test di sicurezza, nessuna autorizzazione preventiva per Sam Altman quando, nel 2023, ha lanciato sul mercato Open AI, come sarebbe stato obbligatorio per un nuovo prodotto in qualsiasi altra industria, basti pensare a quella automobilistica. Ben prima che ChaptCPT rilevasse al mondo qual è il potenziale di autonomia dell'intelligenza generale di carattere generativo, quando nel 2021 la Commissione europea ha adottato la sua proposta di un regolamento sull'intelligenza artificiale, l'esecutivo dell'Unione aveva in mente di ridurre tale asimmetria regolativa attraverso una legislazione si concentrasse sulla sicurezza del prodotto. Non è, dunque, una coincidenza che l'AI Act si fondi sulla base giuridica, prima richiamata, dell'art. 114 TFUE, in tema di riavvicinamento delle legislazioni nazionali nel contesto del mercato unico. La prima preoccupazione, ragionevole, è stata, perciò, adottare una legislazione che assicurasse che l'*output* di intelligenza artificiale che ha accesso al mercato europeo fosse un prodotto sicuro. Non si è però subito compreso che, nella regolamentazione del nuovo ecosistema digitale, era quantomeno riduttivo guardare soltanto al profilo della sicurezza del prodotto, pur a fronte della sua imprevedibilità e del suo potenziale di rischio, sebbene sia vero anche che si era in una fase precedente l'esplosione dell'intelligenza artificiale di tipo generativo. In particolare, mancava una visione sistemica relativa alla protezione dei diritti fondamentali e su questo il Parlamento europea ha fatto quello che ha potuto in sede di revisione legislativa. Sta proprio qui quello che potremmo definire il peccato originale dell'AI Act: un fine iniziale, e conseguenzialmente un linguaggio, che si concentra eccessivamente sulla sicurezza del prodotto e lascia, invece, troppo spesso sullo sfondo le questioni collegate alla tutela dei diritti fondamentali[223]. In altre parole, l'AI Act incarna pienamente una tensione tutta europea, cercando di conciliare mercato e stato di diritto, l'innovazione tecnologica e la sicurezza dei sistemi di intelligenza artificiale con il rispetto dei diritti umani e dei valori fondamentali sanciti dal costituzionalismo europeo[224]. Per molti il risultato finale è un testo di compromesso, non solo tra le due esigenze che si

---

[222] 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.

[223] M. ALMADA- N. PETIT, *The EU AI Act: a medley of product safety and fundamental rights?*, SSRN Scholarly Paper, Rochester, 2023. Sul punto, si consideri anche DONATI, *Intelligenza artificiale e diritti fondamentali nel regolamento sull'intelligenza artificiale*, cit. v

[224] In questo senso, l'AI Act sembra aver fatto un passo in avanti rispetto al Consiglio d'Europa, che, invece, ha pubblicato una Convenzione quadro che troverà applicazione solo per gli stati firmatari che impone dei principi senza, tuttavia, dettagliare, come evidenziano 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, 2024.

sono richiamate ma anche, evidentemente, tra la volontà dei governi nazionali riuniti nel Consiglio dei Ministri dell'Unione e il Parlamento europeo, che rischia di alimentare due livelli di frammentazione. Il primo è stato richiamato in apertura. Così come è capitato per il GDPR, vi è una discordanza tra etichetta (Regolamento) e ampiezza di moltissime clausole che necessiteranno di un recepimento da parte degli Stati membri, come nel caso delle direttive. Non dovrebbe stupire se tra qualche tempo avremo ventisette normative in parte differenti, esattamente come è avvenuta per il "recepimento" nazionale del GDPR.

Il secondo rischio è diretta conseguenza della scrittura dell'AI Act, che definisce, a maglie larghe e spesso non univoche, alcuni concetti come, per esempio, quello di valutazione del rischio sistemico alla base della valutazione di impatto sui diritti fondamentali cui si accennerà tra poco. Non potrà che essere la Corte di giustizia (ma anche i giudici nazionali) ad attribuire un significato meno equivoco a tali concetti, sulla base di una giurisprudenza per forza di cose rapsodica, in quanto fondata sui diversi casi e contesti fattuali che si presenteranno.

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[225]. 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[226].

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[227]. L'autovalutazione, senza un'adeguata supervisione indipendente, potrebbe portare a una sottostima dei rischi, riducendo l'efficacia delle misure di tutela[228]. 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[229]. La creazione di un quadro normativo che si basa principalmente, e quasi paradossalmente, sull'autoregolamentazione riduce la capacità dell'UE di garantire che i sistemi di IA operino in conformità con i più alti standard di sicurezza ed etica e ripropone, ancora una volta, vecchi meccanismi, che sembrano appartenere a un'altra epoca della regolazione digitale.

---

[225] 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.

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

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

[228] 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.

[229] 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.

Un esempio di questo problema si trova nell'uso della Fundamental Rights Impact Assessment (FRIA)[230]. Secondo l'AI Act, il FRIA è uno strumento chiave per valutare l'impatto dei sistemi di IA ad alto rischio sui diritti fondamentali[231]. 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[232].

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)[233]. 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[234], 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.

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[235]. La speranza è ovviamente che la scelta degli Stati ricada sull'autorità giurisdizionale, per ovvie ragioni di effettività della protezione dei diritti in gioco e imparzialità dell'organismo di controllo. Rimane certo l'amaro in bocca pensando che, in un momento in cui l'Unione europea sta affrontando la sfida cruciale dello stato di diritto (anche) al suo interno, non abbia preso una netta posizione a favore dell'unica opzione (quella dell'accertamento giurisdizionale) che, in casi come questi in cui sono in gioco i diritti personalissimi, è la sola conforme alle radici del costituzionalismo europeo.

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[236]) 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 IA[237], questa spiegazione risulta spesso superficiale,

---

[230] AIA, art. 27.

[231] 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/.

[232] AIA, art. 27(3).

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

[234] 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.

[235] Art. 5 par. 3

[236] 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.

[237] AIA, art. 86.

mancando della trasparenza necessaria per consentire agli individui di contestare efficacemente tali decisioni. Come osservato da De Gregorio e Demková[238], 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[239]. 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[240].

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[241].

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. L'implementazione di meccanismi di sorveglianza indipendenti, *audit* obbligatori e responsabilità legale chiara dovranno essere rafforzati, soprattutto per quei sistemi di IA che operano in settori ad alto rischio e con potenziali ripercussioni significative sui diritti e le libertà fondamentali. L'introduzione del diritto a una "spiegazione significativa" delle decisioni automatizzate è senza dubbio un passo avanti, ma risulta insufficiente se non accompagnata da procedure chiare e trasparenti che permettano agli individui di comprendere appieno come le decisioni sono state prese e quali dati sono stati utilizzati. Questo aspetto è fondamentale per garantire che i sistemi di IA operino in modo equo e responsabile.

L'esclusione delle applicazioni militari, la definizione ristretta di IA, l'affidamento eccessivo all'autovalutazione e la carente protezione degli individui impattati dalle decisioni automatizzate rappresentano criticità che devono essere affrontate con urgenza, specie dal punto di vista del diritto costituzionale. 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[242]. Paradossalmente, si creerebbe uno scenario

---

[238] 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.

[239] 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.

[240] 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.

[241] 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.

[242] 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. Dove, *inter alia,* si afferma che c'è una certa confusione nella definizione dei ruoli e delle responsabilità tra "*provider*" e "*deployer*", il che rende difficile attribuire responsabilità in caso di violazioni dei diritti. Questa ambiguità si riflette anche nel rapporto tra le figure del titolare e del responsabile del trattamento dei dati personali, già presenti nel GDPR, e quelle del produttore e del fornitore

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).

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

Le mosse dell'Unione sembrano definire nuovi scenari nelle risposte alle sfide poste dal digitale. Come già sottolineato, piuttosto che ricorrere a un esercizio di autoregolamentazione guidata da un neoliberalismo digitale, da misure illiberali o da un approccio focalizzato sulla definizione di regole tecniche che riflettano regole costituzionali[243], 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*[244].

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[245]. 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[246]. Seppur in modo diverso, anche l'AI Act si colloca in un tale quadro di maggior responsabilizzazione, considerando il ruolo delle piattaforme digitali quali fornitori e utilizzatori di sistemi di IA, come nel caso dei *deep fake*.

Similmente, l'Unione sembra essersi concentrata sulla costruzione di un approccio collaborativo in cui attori pubblici e privati lavorano insieme per sviluppare e implementare norme e politiche. Come osservato, "la premessa da cui deriva l'idea della co-regolazione è che la tecnologia digitale sia caratterizzata da un *mix* tale di complessità specialistica e rapidità evolutiva che in molti casi solo i

---

introdotte dall'AI Act. Inoltre, l'uso del riconoscimento biometrico è regolamentato in modo ambiguo. L'AI Act vieta l'uso di sistemi di identificazione biometrica in tempo reale da parte delle forze dell'ordine in spazi pubblici, salvo alcune eccezioni, mentre l'uso "*ex post*" è considerato ad alto rischio. Tuttavia, la distinzione tra questi due usi è poco chiara e l'autorizzazione dipende da un'autorità che può essere amministrativa o giudiziaria, senza una preferenza chiara per quest'ultima, che sarebbe più garante dell'imparzialità. Infine, ci sono difficoltà pratiche nell'applicazione di alcuni divieti e obblighi. Ad esempio, il divieto di utilizzo del riconoscimento emotivo in ambito lavorativo ed educativo è vago e non è chiaro se le attività di *recruiting* rientrino in questi ambiti. Anche l'obbligo di trasparenza è ambiguo, poiché non informa gli individui circa la possibilità di utilizzare i sistemi emotivi o di categorizzazione biometrica per indagare su reati.

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

[244] 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.

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

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

destinatari stessi delle norme sono in possesso delle conoscenze necessarie a svolgere il compito normativo"[247].

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[248], 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 Digital Services Act 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[249]. 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[250]. Il Digital Services Act 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[251].

In questo contesto, come stabilito dal Digital Services Act, 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[252]. Tali codici possono svolgere un ruolo fondamentale non solo nel dettagliare meglio gli obblighi derivanti dal Digital Services Act, ma dovrebbero anche essere considerati come misure di attenuazione del rischio, attuate dalle piattaforme digitali designate come *very large* per affrontare i rischi sistemici, compresa la disinformazione. Di conseguenza, i codici di condotta non sono solo strumenti di autoregolamentazione, ma piuttosto strumenti di co-regolamentazione che trovano la loro base nell'accordo volontario tra attori pubblici e privati, ma anche in una normativa. Come sottolineato dal Digital Services 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 Digital Services Act[253]. 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

---

[247] 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.

[248] 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.

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

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

[251] DSA, Considerando 104.

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

[253] *Ibidem.*

problematici dell'autoregolazione, come assai lucidamente individuato da Luisa Torchia. "*L'autoregolazione ha assunto i caratteri tipici degli strumenti di limitazione del potere (quale che sia la natura del potere): la determinazione di regole e principi generali, il controllo sul rispetto di quelle regole, la costruzione di apparati tendenzialmente indipendenti, chiamati a risolvere eventuali controversie. Si finisce per mimare così il potere pubblico, ivi compreso un embrione di principio di divisioni dei poteri, anche se tutte le funzioni — la determinazione delle regole, il controllo sul loro rispetto e la funzione giustiziale — sono strutturate e rimangono all'interno della piattaforma*"[254].
Tuttavia, il Codice di buone pratiche non è ancora diventato un Codice di condotta, come definito dal Digital Services Act. 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[255]. 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 Digital Services Act[256]. 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[257].
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,[258] 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[259]. Seppur restino domande costituzionali relativamente a un potenziale eccesso di regolamentazione e alle forzature delle basi giuridiche dell'UE a tal fine, lo sviluppo di una strategia di questo tipo può collegarsi alla necessità per il costituzionalismo europeo di rigettare approcci neoliberali o eccessivamente restrittivi, concentrandosi piuttosto sul bilanciamento, non solo tra diritti, ma tra le opzioni di regolazione (del presente, ma anche del futuro) che si è cercato di fare emergere nelle pagine che precedono

---

[254] L. TORCHIA, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista Trimestrale di Diritto Pubblico*, fasc. 4, 2022
[255] I. NENADIC *et al.*, *Structural indicators to assess effectiveness of the EU's Code of Practice on Disinformation*, Working Paper, 2023.
[256] DSA, art. 40.
[257] 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.
[258] Garante per la protezione dei dati personali, fascicolo n. 112, provvedimento del 30 marzo 2023, cit.
[259] DRAGHI, *The future of European competitiveness*, cit.