INTELLIGENZA ARTIFICIALE E PIATTAFORME DIGITALI: OPPORTUNITÀ E RISCHI ALLA LUCE DEL RECENTE QUADRO REGOLATORIO*

di Bianca Nicla Romano**

Sommario. 1. Delimitazione del campo di indagine. – 2. Le Piattaforme digitali e il contesto in cui matura la relativa regolamentazione europea. – 3. Il *Digital Services Act* e il *Digital Market Act*. – 4. L'IA e le piattaforme digitali. – 5. Gli atti di *soft law* sull'interazione tra DMA, DSA e GDPR. – 6. Le recenti novità nel panorama nazionale: la legge italiana sull'Intelligenza Artificiale. Cenni. – 7. Riflessioni conclusive.

1. Delimitazione del campo di indagine. L'attuale realtà economico-sociale è il frutto di importanti e radicali trasformazioni determinate, negli ultimi anni, dal contributo dello sviluppo tecnologico: ci troviamo, infatti, nell'ormai sempre più consolidato contesto di quella che viene definita «transizione digitale», nell'ambito della quale si sono realizzate molteplici innovazioni che, in ragione del loro notevole impatto sulle manifestazioni della vita quotidiana, sono state (e sono tuttora) oggetto di particolare attenzione da parte degli studiosi delle materie giuridiche, dell'economia e dell'amministrazione.

Tale realtà è stata agevolata in particolare dall'emergenza pandemica, durante la quale *Internet* ha svolto un ruolo determinante rispetto alla tutela di diritti fondamentali quali quello alla salute, all'istruzione e al lavoro[1]. Ciò ha contribuito a modificare anche la sfera della libertà personale[2], attraverso spazi di *open networks*[3] che, gradualmente, hanno dato vita a una vera e propria coesistenza tra la realtà analogica e quella digitale, perché «l'ambiente in cui l'uomo ormai è immerso è in gran parte di tipo informatico e siamo, dunque, innanzi ad un nuovo umanesimo digitale»[4].

Nell'ambito di queste innovazioni – tra le quali si annovera, ovviamente, tutto il processo di digitalizzazione dell'attività amministrativa – particolare interesse lo hanno suscitato la

---

* *Sottoposto a referaggio.*

** Già Ricercatrice di Diritto amministrativo e pubblico – Università di Napoli Parthenope.

[1] Internet è stato definito «il più grande esperimento di anarchia della storia», cfr. E. Schmidt, J. Cohen, *La nuova era digitale. La sfida del futuro per cittadini, imprese e nazioni*, tr. it., Milano, 2013, XI. Si veda anche T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *DIRINF,* 2020, 483; G. De Minico, *Internet e le sue fonti*, in *Osservatorio sulle fonti*, 2013.

[2] Così M. Luciani, *Ogni cosa al suo posto*, Milano, 2023, 68.

[3] Cfr. T.E. Frosini, *Il Costituzionalismo nella Società tecnologica*, in *Consulta* online, 25 maggio 2020, 4 ss.

[4] M. Tiberii, *La regolamentazione Consob sulla raccolta di fondi* online*: l'*equity *e il* lending crowdfunding, in *Amministrativ@mente.it,* 1, 2022, 138-157.

Issn 2421-0528

blockchain[5], l'*e-commerce*, gli *smart contracts*[6], ma anche i *social media,* le problematiche ad essi connesse in termini di *cybersecurity* e di tutela dei dati e le piattaforme *on line,* queste ultime in considerazione non solo della notevole e predominante loro espansione, ma anche dell'impatto che pure su di esse ha avuto e può avere l'Intelligenza Artificiale (IA) con i suoi sistemi.

Questi ultimi nascono grazie ai dati che la stessa Intelligenza Artificiale riceve sotto forma di *input* i quali, a loro volta, ne generano di ulteriori, in un meccanismo potenzialmente infinito[7]; l'utilizzo dei dati rende possibili, ad esempio, tra le tante opportunità, non solo varie tipologie di transazioni, ma anche l'adempimento delle obbligazioni dedotte in contratto, in quanto si tratta di attività che possono essere governate da un sistema di *IA* che, mediante un algoritmo operante con un meccanismo di causa-effetto[8], garantisce l'esito dell'operazione, scongiurando il contenzioso e generando, così, fiducia tra gli utenti. L'algoritmo consente, dunque, di controllare variabili quali l'avveramento delle condizioni eventualmente inserite nel regolamento contrattuale[9].

Ma, a fronte dell'innegabile vantaggio che può derivare dalla rapidità e dal presunto alto livello di sicurezza offerto dal sistema, sorgono, cionondimeno, dubbi in merito alla natura contrattuale di accordi conclusi in tal modo (gli *smart contracts,* appunto); questi, infatti, caratterizzandosi per avere una struttura di protocolli informatici che riproducono ed

---

[5] La *blockchain*, descritta, in maniera un po' suggestiva, anche come «macchina della verità» o «protocollo di Dio», rappresenta una delle tecnologie più recenti e dibattute in tema di trasformazione digitale, in grado di dar vita ad una rivoluzione paragonabile e forse superiore a quella dell'avvento del *web*, tanto che viene vista come la seconda era di *Internet*, con il potenziale di cambiare radicalmente la moderna economia digitale. Si veda M. J. Casey, P. Vigna, *La macchina della verità. La* blockchain *è il futuro di ogni cosa*, Milano, 2018 (in cui si sostiene, infatti, che la *blockchain* possa contribuire a modificare il sistema di controllo e gestione dell'informazione divenendo un sistema distribuito nel quale le persone, i componenti essenziali della società globale, possano decidere in che modo debbano essere gestiti i propri dati). Essa può essere definita come una piattaforma virtuale al cui interno i soggetti iscritti condividono pubblicamente dati e informazioni, contribuendo anche alla loro verificazione e validazione, e può essere applicata a molteplici ambiti – dal campo finanziario, all'*audit* interno delle imprese, alla certificazione delle identità digitali, agli *smart contracts*, alla prevenzione del rischio corruzione – in quanto consente la creazione e la gestione di un *database* decentralizzato, ovvero una rete *peer-to-peer* che memorizza un registro delle transazioni, condiviso tra tutti i partecipanti (detti «nodi»). In tale registro vengono annotate, in modo ordinato e sequenziale, le operazioni compiute da ciascuno: in pratica, si tratta di una rete decentralizzata in cui i dati vengono raccolti non in un unico posto, ma in singoli «nodi», ognuno dei quali è una copia di un singolo *set* di dati. Raggiunto un certo numero di transazioni approvate viene formato un nuovo «blocco» crittografato che, a sua volta, sarà successivamente concatenato e bloccato insieme ad altri formando, in tal modo, una storia cronologica degli eventi che vive su ogni nodo del sistema. Chiunque può diventare un «nodo» e partecipare alla *blockchain* installandola sul proprio *server*, avendo, in tal modo, libero accesso alla rete e possibilità di verifica esatta di cosa accada. La criptazione del blocco e l'apposizione ad esso di una marca temporale al momento della sua chiusura conferiscono la sicurezza necessaria per il funzionamento del database che si viene a creare. Sul tema, *ex multis*, N. Attico, Blockchain*, guida all'ecosistema. Tecnologia,* business, *società*, Milano, 2018; M. Matassa, Blockchain *e pubblica amministrazione: stato dell'arte e prospettive*, in *Ist. Federalismo*, 3, 2021, 803-838; I. Francucci, *Trasparenza,* blockchain *e gestione dei rifiuti*, in *Diritto Amministrativo*, 1, 2024, 273 ss.

[6] Sugli *smart contracts,* o *self executing contracts, blockchain contracts o digital contracts* cfr. D. Di Sabato, *Gli* smart contracts: robot *che gestiscono il rischio contrattuale*, in *Contr. impr.*, 2, 2017, 378 ss.

[7] Si pensi, ad esempio, alla possibilità di utilizzare la tecnologia *blockchain* nell'ambito della gestione delle informazioni ambientali in vista di una semplificazione nel trattamento delle stesse, anche al fine di garantire maggiore trasparenza all'accesso per i richiedenti. Si vedano, sul tema, A. Micello, *La tecnologia blockchain al servizio della gestione delle informazioni ambientali: verso un "*Blockchained Green Public Procurement*"?*, in *Riv. quadrim. dir. amb.*, 3, 2018, 83-108; F. Calisai, *Intelligenza artificiale e ambiente,* in *Giustizia Civile*, fasc. 4, 1° aprile 2021, 898.

[8] Il meccanismo di causa - effetto cui si fa riferimento è quello «*if-then*», per cui, ad esempio, alla ricezione del pagamento consegue la consegna del bene o la concessione di una licenza d'uso. Cfr. S. Crisci, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm.*, 10, 2018, 1787 ss.

[9] Si parla, al riguardo, dell'inserimento di *trigger point.*

eseguono meccanicamente i termini di un accordo, rendono piuttosto difficile riuscire a riconoscere la natura negoziale ad un'operazione in cui manca la componente volontaria. A ciò si aggiunga, inoltre, che è anche possibile che si determinino delle «zone grigie di "irresponsabilità" e vuoti di tutela»[10] in caso di danni subiti dagli utilizzatori, conseguenti, magari, a un malfunzionamento della catena e del *software* in generale e causate proprio dalla eccessiva rigidità delle piattaforme, oltre che dalla impossibilità di modificare le informazioni ivi inserite, sebbene sia proprio la rigidità a garantire un maggior livello di sicurezza.

L'Intelligenza Artificiale, a ben vedere, ha, dunque, assunto una notevole rilevanza che si estende alle strategie commerciali, tanto quanto alla gestione dei rapporti economici e, infine, ai processi decisionali, nonostante, va detto, continuino a persistere notevoli perplessità con riguardo alla chiarezza e alla liceità delle modalità di funzionamento dei sistemi algoritmici che ne sono alla base e che derivano dalla ancora rilevabile difficoltà (se non proprio dalla impossibilità) di intervenire sulla discrezionalità che li connota e che, purtroppo, finisce con il contrapporre una certa opacità alla loro intrinseca versatilità[11].

Alla luce del quadro regolatorio che si è venuto a delineare negli ultimi anni e di cui si fornirà, di seguito, una breve analisi, lo scritto intende, dunque, soffermarsi sui vantaggi e le opportunità che può determinare l'Intelligenza Artificiale applicata alle piattaforme digitali, evidenziando, al contempo, i rischi che, tuttavia, ne possono derivare e che assumono un fondamentale rilievo in ragione del fatto che, spesso, sono sottovalutati perché ignorati dagli stessi utenti delle piattaforme.

Tali rischi sono, tra gli altri, connessi alla problematica della gestione dei dati acquisiti dalle piattaforme digitali sotto il profilo della *privacy* e che, pure a fronte della stretta regolamentazione contenuta nel *General Data Protection Regulation* (GDPR[12]), sono, purtroppo, esposti, spesso, a un trattamento non sempre corretto da parte dei titolari, ovvero i gestori delle piattaforme stesse.

I dati, invero, con l'affermarsi dei mercati digitali e dei *Big Data*, dei sistemi di profilazione e dei modelli predittivi utilizzati dai principali attori dell'economia digitale, sono ormai divenuti una risorsa estremamente preziosa, in relazione alla quale l'autorizzazione al trattamento non risulta più orientata alla salvaguardia di un valore intrinseco e non negoziabile, quale la riservatezza dell'informazione personale, ma tende, piuttosto, a divenire funzionale al suo sfruttamento economico. Infatti, la disponibilità e il valore economico di essi non appartengono più al soggetto cui si riferiscono, bensì, in via esclusiva, all'operatore economico che ne ha ottenuto il consenso alla raccolta e al trattamento[13]. E anche se il consenso a tale trattamento viene spontaneamente fornito dal titolare del dato stesso, non si

---

[10] F. Calisai, *Intelligenza artificiale e ambiente,* ult. cit., 900.

[11] M. L. Borgese, *La duplice radice dell'Intelligenza Artificiale: fra le esigenze di innovazione e la tutela dei più fragili,* su *https.www.medialaws.eurivista*, *Rivista di diritto dei* media, 1, 2024.

[12] Regolamento (UE) 2016/679, relativo al trattamento dei dati personali, nonché alla libera circolazione di essi, la cui entrata in vigore, com'è noto, ha abrogato la prima normativa in materia di tutela dei dati personali dell'individuo risalente alla Direttiva 95/46/CE sulla protezione dei dati personali che aveva avuto l'intento di ravvicinare le legislazioni nazionali in tema di *data protection*, a seguito dell'aumento dei flussi transfrontalieri di dati personali tra operatori economici pubblici e privati derivante dal funzionamento del Mercato unico. Sia consentito un rinvio a B.N. Romano, *In the Era of AI: Exploring New Frontiers in Cybercrime and Safeguarding Personal and Health data,* su *Corti Supreme e Salute,* 1, 2024, 461 ss.

[13] Nella precedente disciplina in materia, contenuta dapprima nella L. 675/1996 e poi nel Codice della privacy del 2003, invece, i dati personali erano considerati inalienabili e non negoziabili proprio perché inerenti al diritto fondamentale della persona alla riservatezza, per cui la tutela ad esso predisposta prevedeva non solo un'autorità garante (il Garante per la *privacy*, appunto), ma anche un rigido sistema di autorizzazione al trattamento e un sistema di prescrizioni e sanzioni anche di carattere penale (per il reato di trattamento illecito di dati personali). Si veda C. Contessa, *Il potere pubblico al tempo dei Big Data,* in C. Contessa, P. Del Vecchio (a cura di), *Testo unico dei servizi media Audiovisivi Radiotelevisivi (TUSMAR) commentato articolo per articolo,* Piacenza, 2021.

può non rilevare che una tale evoluzione rappresenti comunque una forma di «arretramento dell'ambito dei diritti inviolabili (anche di matrice sociale) e del sistema di regole posto a loro tutela, a tutto vantaggio dei diritti proprietari di matrice economica»[14].
L'analisi si concentrerà, pertanto, in particolare, sul rapporto tra la regolamentazione europea delle piattaforme digitali – segnatamente, il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA) – e la disciplina dell'Intelligenza Artificiale contenuta nell'*AI Act*, che introduce un approccio basato sulla valutazione del rischio e sulla classificazione dei sistemi di IA. Tale quadro regolatorio sarà esaminato alla luce non solo del GDPR, ma anche delle recenti Linee guida europee relative sia alle pratiche vietate di Intelligenza Artificiale, sia ai rapporti tra DSA, DMA e GDPR, riservando un cenno pure alla legge italiana che - anch'essa di recente - è stata emanata sull'Intelligenza Artificiale, ovvero la l.n. 132/2025.
Lo scopo è verificare se e in che misura il quadro regolatorio europeo che sta via via sempre più consolidandosi sia in grado di assicurare un equilibrio effettivo tra innovazione tecnologica e tutela dei diritti fondamentali, garantendo che l'impiego dell'Intelligenza Artificiale nelle piattaforme digitali avvenga in modo trasparente, responsabile e conforme ai principi dello Stato di diritto. In particolare, l'analisi intende valutare la capacità delle «nuove» normative di offrire strumenti idonei a governare i rischi derivanti dall'uso dell'IA – quali la manipolazione algoritmica, la profilazione e l'opacità decisionale – puntando alla costruzione di un sistema di *governance* digitale europeo unitario e coerente, senza, tuttavia, ostacolare le opportunità di sviluppo e competitività che essa può generare nel mercato digitale europeo.

2. Le Piattaforme digitali e il contesto in cui matura la relativa regolamentazione europea. È necessario, preliminarmente, intendersi su cosa siano le piattaforme digitali (*online*) e precisare che non sempre gli utenti ne conoscono effettivamente la realtà e, di conseguenza, cosa l'IA renda possibile all'interno del loro contesto, in quanto sono prevalentemente attratti dalle opportunità ad esse legati finendo, per tale motivo, con il sottovalutare gli effetti negativi che possono derivarne.
Le suddette piattaforme sono, a ben vedere, ambienti virtuali progettati per facilitare l'interazione, lo scambio di informazioni e le transazioni tra gli utenti; negli ultimi decenni esse sono divenute il fulcro di molte attività sociali, economiche e culturali, tanto da riuscire ad estendere la propria presenza in settori molteplici che vanno dall'*e-commerce*, ai *social media*, ma anche all'informazione e ai servizi finanziari. Tra le più note figurano, ad esempio, i *social network*, i *marketplace*, le piattaforme di *streaming*: tutte hanno in comune il pregio di avere trasformato il modo in cui le persone comunicano, consumano contenuti e prodotti e, persino, lavorano[15].
Riuscire a darne una definizione univoca, in realtà, non è, però, semplice[16], a causa della versatilità che le connota e che ne favorisce un ampio impiego in svariati ambiti settoriali (dai trasporti, alla compravendita di beni, al mercato del lavoro) nei quali è, pertanto, possibile

[14] *Idem,* 7.
[15] In tema di piattaforme digitali e loro regolazione si vedano, *ex multis,* O. Lobel, *The Law of the Platform*, in *Minnesota Law Review*, 2016; P. Akman, *Regulating competition in digital platform markets: a critical assessment of the framework and approach of the EU digital markets act*, in *European law review*, 1, 2022; R. Niro, *Piattaforme digitali e libertà di espressione fra autoregolamentazione e corregolazione: note ri-costruttive*, in *Osservatorio sulle fonti*, 3, 2021; M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale,* in *Gruppo di Pisa,* 2, 2021; M. Santaniello, *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics,* 3, 2021; E. Cremona, *Fonti private e legittimazione democratica nell'età della tecnologia,* in *DPCE online*, 2021, spec., 1236 s.
[16] Anche la stessa Commissione Europea ha incontrato difficoltà nel definire il termine piattaforma nella comunicazione sul mercato unico digitale *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final (6.5.2015).

percepire gli effetti del cd. *platformization process*[17]. È, tuttavia, chiaro che esse hanno potuto, in breve tempo, trasformare radicalmente non solo i mercati, ma anche le imprese che producono beni e servizi e le relative transazioni, lanciando sfide ai più tradizionali modelli di *business* e agli stessi legislatori e regolatori, grazie al potere via via sempre maggiore che hanno potuto acquisire, con effetti inevitabili sul mercato in genere, oltre che con riguardo alla tutela dei consumatori. Questi ultimi, in qualità di utenti, hanno inevitabilmente fornito ad esse dati propri[18] che, come detto, rappresentano una vera e propria «risorsa economica strategica, al pari del capitale o del lavoro»[19], in quanto consentono di addestrare gli algoritmi e, dunque, di personalizzare le offerte e finanche di anticipare le decisioni di mercato.

Dunque, fungendo da intermediari digitali, le piattaforme hanno dato vita a un nuovo modello di *business*[20] in cui sono in grado di collegare domanda e offerta e in cui consumatori e fornitori possono interagire e scambiare valore senza la necessità di intermediari tradizionali, in uno spazio di interazione di due o più gruppi omogenei di utenti che, grazie al carattere della bilateralità (*two-sided*) o della multilateralità (*multi-sided*) delle piattaforme stesse, intessono relazioni di scambio, ma anche di interdipendenza, secondo modalità e procedure di natura contrattuale[21].

Tale modello, sebbene sia abbastanza recente, ha, ciononostante, comportato la formazione di un vasto potere di mercato che, se, da un lato, costituisce un dato economico considerato ormai per acquisito, ha, dall'altro, dato vita a problematiche di varia natura connesse alla tutela della concorrenza nei mercati digitali e al contrasto alle posizioni di monopolio.

Infatti, la maggior parte delle piattaforme è caratterizzata dall'offerta integrata di una molteplicità di servizi e dalla sua rapida espansione; in esse, oltre all'esistenza di effetti di rete[22], sono presenti dei meccanismi che, di fatto, rinforzano la posizione oligopolistica delle grandi imprese del digitale (*Big Tech*) che già operano nel mercato, quali *Amazon, Microsoft, Google, Apple, Meta*. Tra questi meccanismi si evidenziano, tanto per citarne alcuni, l'utilizzo strategico dei dati, ma anche gli *switching costs* – che sono i costi che un consumatore deve

---

[17] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche,* in *Giornale di diritto amministrativo*, 1, 1° gennaio 2023, 116.

[18] L. Ammannati, *Verso un diritto delle piattaforme digitali?,* in *Federalismi.it*, 7, 2019, 2.

[19] M. Rubino de Ritis, *Intelligenza artificiale e mercato: dalla guerra al possibile equilibrio,* in *giustiziacivile.com,* 17.6.2025, che evidenzia che, al contempo, i dati rappresentano anche una «barriera all'ingresso potentissima», perché quanto maggiori sono i volumi che se ne possiedono, tanto più si riesce ad offrire servizi migliori, rapidi e più predittivi.

[20] Quello della *platform economy* è un tema che investe diversi settori; essendo la dottrina molto vasta si rinvia, a mero titolo esemplificativo, a: L. Ammannati, *Verso un diritto delle piattaforme digitali?,* cit.; S, Martinelli, Platform economy *e responsabilità delle piattaforme di intermediazione*, in S. Orlando, G. Capaldo (a cura di), *Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale*, Yearbook 2022 Juridical Observatory on Digital Innovation, Roma, 2022; A. Manganelli, A. Perrucci, *Servizi di pagamento e finanziari. L'impatto delle grandi piattaforme digitali, fra innovazioni tecnologiche ed evoluzione normativa,* in *Analisi Giuridica dell'Economia*, 1, 2025, 243-265; G. Toscano, *La tutela del lavoro nel giogo delle piattaforme digitali: sfide e prospettive,* in *Il diritto del mercato del lavoro*, 1, 2025; L. Parona, Addressing the interplay between competition law and data protection law in the digital economy through administrative cooperation: The CJEU judgement in the 'Meta Platforms' case, in *Italian Journal of Public Law,* 1, 2024, 239-265.

[21] Questa è la definizione che è possibile trarre dal *Public consultation on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy*, del Settembre 2015, documento con il quale è stata aperta la consultazione sul tema delle piattaforme. In esso si è fatto riferimento alla piattaforma come all'impresa che opera su mercati "bilaterali" (*two – sided market*) o" multilaterali" (*multi - sided markets*) in quanto, «grazie alla tecnologia, sono in grado di mettere in contatto un vasto numero di compratori e venditori». Cfr. L. Ammannati, *Verso un diritto delle piattaforme digitali?,* in *Federalismi.it*, 7, 2019, 3.

[22] Sulla configurazione «a rete» del sistema dei poteri pubblici di vigilanza e di controllo nel *Digital Services Act*, cfr. L. Torchia, *Poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Riv. trim. dir. pubbl.*, 2022, 4, 1101 ss.

sostenere quando intende cambiare fornitori di un certo bene o servizio – e i *behavioral biases* – ovvero le possibili distorsioni comportamentali. Essi determinano l'effetto di ostacolare lo spostamento degli utenti medesimi e di creare delle vere e proprie «barriere all'entrata» grazie alle quali le *Big Tech* riescono a non subire la pressione concorrenziale sui singoli servizi offerti[23].

A dire il vero, i suddetti meccanismi non sono stati percepiti come problematiche nell'immediato, con la conseguenza che le piattaforme *online* hanno potuto avvantaggiarsi per lungo tempo di politiche che, solo in seguito, sono state definite «troppo permissive, tanto negli Stati Uniti, quanto in Europa»[24]. Esse, in altri termini, sono divenute, veri e propri attori sovrastatali che hanno potuto acquisire uno smisurato potere agevolati non solo dalla apparente e pretesa libertà del *cyber*spazio, ma anche dal fatto che, per lungo tempo, i legislatori, nella convinzione di voler promuovere l'innovazione tecnologica, hanno lasciato ampi spazi di autoregolazione e di mercato. Proprio perché detengono risorse di tipo informativo tali da consentire di influenzare scelte individuali e collettive[25], essi, dunque, non si sono limitati a fornire servizi, ma hanno assunto il ruolo di vere e proprie "autorità di fatto", imponendo regole privatistiche e di procedure di *enforcement* (esecuzione) al di fuori di un controllo effettivo da parte di organi pubblici.

Pertanto, se, in un primo momento, si è manifestato un certo entusiasmo rispetto alla creazione di nuovi mercati da parte delle piattaforme digitali, anche in ragione del graduale e affascinante imporsi delle applicazioni tecnologiche, lo stesso entusiasmo si è, nel tempo, ridimensionato perché si è compresa la necessità di dover regolamentare tale nuovo mercato, per contrastare questi veri e propri oligopoli, a favore di operatori già affermati che, sfruttando la loro posizione predominante, sono riusciti ad "inglobare" iniziative economiche potenzialmente concorrenti con essi[26], grazie anche all'applicazione di prezzi anticoncorrenziali, come è accaduto, ad esempio, per le *transaction platforms* (di cui si è a lungo sottovalutato il rischio[27]).

Le distorsioni alla concorrenza nei mercati digitali e i plurimi pregiudizi per gli utenti hanno, dunque, rivelato l'insufficienza di un approccio basato esclusivamente su meccanismi di *self-regulation* di origine privata[28]. Ne è conseguito che la tendenza degli attori protagonisti di questo ecosistema digitale a dotarsi «di un diritto de-territorializzato, sganciato da istituzioni politiche e meccanismi di rappresentanza democratica»[29] e reso possibile dal fatto che le istituzioni politiche non sono state in grado di corrispondere i traffici economici globali conseguenti al progresso economico, ha indotto la dottrina giuspubblicistica ad interrogarsi sull'enorme potere da essi acquisito in qualità di soggetti privati che hanno contribuito alla

---

[23] G. Bruzzone, *Verso il Digital Markets Act: obiettivi, strumenti e architettura istituzionale*, in *Rivista della Regolazione dei Mercati*, n. 2, 2021.

[24] G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche,* ult. cit. 117.

[25] M. Santaniello, *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics,* 3, 2021, 587-588.

[26] È il caso dell'acquisizione delle piattaforme *WhatsApp* e *Instagram* da parte di *Facebook*. Attualmente fanno entrambe parte dell'ecosistema più ampio di *Meta Piattaforme*, che ha sostituito *Facebook* e che comprende sia quest'ultima piattaforma che *Instagram*, *Messenger* e la crescente gamma di tecnologie VR e AR.

[27] È il caso di *Amazon, transaction platform* che, nata come semplice intermediaria, ha finito rapidamente con l'identificarsi con il mercato stesso, gestendo in autonomia domanda e offerta, sia dal lato degli utenti commerciali che da quello dei consumatori finali.

[28] Così G. Buttarelli, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche,* cit., 120.

[29] E. Cremona, *Fonti private e legittimazione democratica nell'età della tecnologia,* cit. 1236. Si veda, al riguardo, S. Rodotà, *Il mondo della rete. Quali diritti e quali vincoli*, Bari, 2014; Id., *Una Costituzione per Internet*, in *Politica del diritto*, 2010, 3, 337 ss.

nascita di nuovi beni di interesse generale[30].
Non potendocisi, però, soffermare sull'ampio dibattito che è maturato sul tema, ci si limita ad evidenziare che la medesima dottrina ha, da tempo, riconosciuto che, per riuscire a combinare la tutela dei diritti fondamentali con la produzione privata del diritto nell'era digitale, è necessaria una *co-regulation,* che rappresenta una forma di regolazione frutto della integrazione delle fonti pubbliche con quelle private dei protagonisti della rete, in cui possano, dunque, trovare composizione strumenti e interessi tanto pubblici quanto privati e che possa dar vita alla cd. *lex informatica*[31] in maniera più adeguata di quanto sia possibile attraverso non solo la *de-* o *self-regulation* ma anche la regolazione classica (o etero-regolazione)[32].
Il risultato di tale integrazione è ravvisabile proprio nelle recenti regolazioni del *Digital Services*

[30] Si vedano, *ex multis,* G. De Minico*, Regole. Comando e consenso,* Torino, 2005*;* Id. *Internet e le sue fonti,* in *Osservatorio sulle fonti,* 2013, 5-6*;* Id.*, Antiche libertà e nuova frontiera digitale,* Torino, 2016; O. Lobel*, The Law of the Platform, in Minnesota Law Review, 2016, 101*, e spec. par. IV*, From Code as Law to Platform as Regulation,* 142 ss.; T.E. Frosini, Internet *come ordinamento giuridico*, in *Percorsi costituzionali*, 2014, 1, 13 ss.; Id., in *Dir. Inf.*, 2020; A. Simoncini, *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa, M. Bassini (a cura di), *Diritti e libertà in internet*, Firenze, 2017, 19 ss.; E. Cremona, *Fonti private e legittimazione democratica nell'età della tecnologia,* in *DPCE online,* 2021, spec., 1236 ss.; M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *Gruppo di Pisa*, 2/2021, 168; E. Bruti Liberati, *Poteri privati e nuova regolazione pubblica,* in *Diritto pubblico*, fascicolo 1, gennaio-aprile 2023, 285-301.

[31] *Lex informatica* (J. R. Reidenberg, *Lex Informatica*: *The Formulation of Information Policy Rules through Technology*, in *76 Tex. L. Rev.* 553 (1997-1998), 7), così come *code of law (*L. Lessig, *Code: And Other Laws Of Cyberspace*, 1999), sono espressioni che risalgono agli anni Novanta attraverso le quali si è inteso fare riferimento, appunto, al codice regolatore del *cyber*-spazio. Si rinvia a L. Ammannati, *Verso un diritto delle piattaforme digitali?,* cit., 4. T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Dir. Inf.*, 2020, 482, definisce diritto spontaneo la *lex informatica*, nella quale, grazie alla *co-regulation,* vengono ad integrarsi «le poche ed essenziali leggi statali ed europee […] con una politica di *self-regulation* da parte degli utenti di *internet*». Inoltre ritiene che la *lex informatica,* proprio perché consente una integrazione tra fonti pubbliche e fonti private dei protagonisti della rete, può leggersi ispirata al principio di sussidiarietà, in quanto «la *co-regulation* dello Stato può venire in sussidio alla *self-regulation* degli utenti, quando questi la evocano ovvero quando la necessitano».

[32] La *de-* o *self-regulation* comporterebbe, infatti, in prospettiva, una sorta di «indifferenza giuridica» nei confronti dei diritti coinvolti dall'economia digitale, indifferenza non auspicabile per la varietà e il tenore di tali diritti. La regolazione classica (o etero-regolazione), invece, trattandosi di una regolazione esclusivamente pubblicistica, si scontrerebbe inevitabilmente con la ormai riconosciuta «crisi» della legge come esclusivo strumento di normazione che, tra l'altro, in tale contesto, risulta anche difficilmente conciliabile con la dimensione globale, la tecnicità e la velocità del fenomeno digitale. Si veda E. Cremona, *Fonti private e legittimazione democratica nell'età della tecnologia*, cit., 1263 ed anche G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *BioLaw Journal - Rivista di BioDiritto*, 2, 2020, 411-415. G. De Minico, *Internet e le sue fonti,* cit.*,* 9, sostiene che con la *co-regulation* «si ripropone l'antico e mai sopito conflitto tra autorità e libertà, uno scontro in cui si consuma da un lato, il tentativo di un ordinamento di aprirsi ai privati senza rinunciare a ideare il progetto politico-regolatorio, di cui conserva la responsabilità ultima; dall'altro, l'accettazione da parte dei privati di un metodo ispirato al *self-restraint*, il prezzo da pagare per l'imperatività e la generalità delle proprie regole, altrimenti volontarie e relative».

Act (DSA)[33] e del *Digital Markets Act (*DMA)[34], contenuti all'interno del *Digital Services Act Package*[35], del dicembre del 2020, attraverso il quale la Commissione europea ha fornito la disciplina necessaria a soddisfare alcune importanti esigenze: quella di garantire il buon funzionamento dei mercati, mantenendo un contesto economico aperto e concorrenziale; quella di prevenire lo sfruttamento iniquo del potere conseguito; e quella di regolamentare sia l'impatto potenziale delle condotte delle piattaforme sull'accesso all'informazione e sul condizionamento dei comportamenti individuali, sia il ruolo che le piattaforme possono svolgere ai fini della rimozione dei contenuti illeciti o dannosi sul *web*.

Al DSA e al DMA, aventi lo scopo di fornire – con i dovuti distinguo che verranno evidenziati – una disciplina organica per i servizi digitali e di stabilire le condizioni di competitività tra gli operatori all'interno dei mercati, si aggiungono (ma, in tale sede, non ci si soffermerà) il *Data Governance Act* (DGA)[36], che stabilisce le modalità e i termini per un riutilizzo dei dati oggetto di diritti di terzi o detenuti da enti pubblici[37]; e il *Data Act*[38], che, in

[33] 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). Tale Regolamento consta di 156 Considerando e di 93 articoli. Pubblicato il 27 ottobre 2022, la sua applicazione è stata divisa in due fasi: dal 25 agosto 2023 è stato applicato solo alle piattaforme *online* molto grandi e ai motori di ricerca molto grandi; mentre dal 17 febbraio 2024 è stato applicato anche alle altre piattaforme. Entro tale ultima data gli Stati hanno dovuto nominare i loro coordinatori per i servizi digitali. Sul tema si vedano, *ex multis,* F. Casolari, *Il "*Digital Services Act" *e la costituzionalizzazione dello spazio digitale europeo*, in *Giurisprudenza italiana*, 2, 2024, 462-465; M. C. Girardi, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, in *Federalismi.it,* 17, 2024; G. De Minico, *Nuova tecnica per nuove diseguaglianze.* Case law: *Disciplina Telecomunicazioni,* Digital Services Act *e Neurodiritti,* in *Federalismi.it,* 6, 2024, 1-22; I. De Vivo, *Il potere d'opinione delle piattaforme* -online*: quale ruolo del "*regulatory turn*" europeo nell'oligopolio informativo digitale?*, in *Federalismi.it*, 2, 2024, 45-75.

[34] 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). Esso consta di 109 Considerando e di 54 articoli ed è entrato in vigore il 7 marzo 2024. Sul DMA si vedano, *ex multis,* J. Moscianese, O. Pollicino (a cura di), *Concorrenza e regolamentazione nei mercati digitali. Lo stato dell'arte dopo l'entrata in vigore del Digital Market Act,* Giappichelli, 2024; G. Contaldi, *Il DMA* ("Digital Markets Act") *può contribuire alla protezione dei dati degli utenti online?*, in *Diritti umani e diritto internazionale*, 1/2023, 77-93. Sul DMA si vedano, *ex multis*, F. Sporta Caputi, "Gatekeeper", *abuso di posizione dominante ed efficacia preventiva dei presidi comportamentali e organizzativi introdotti dal* "Digital Market Act" *e dal* "Digital Service Act", in *AIDA*, 2023, pp. 39-101; M. Libertini, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Rivista trimestrale di diritto pubblico*, 4/2022, 1069-1083; P. Dunn, *Il* Digital Markets Act*: tra logiche concorrenziali e istanze costituzionali*, in *Diritti comparati*, 17 Febbraio 2022.

[35] Emanato nell'ambito della *European Strategy for data* (COM/2020/66); si tratta della Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni dal titolo *Una strategia europea per i dati* del 19.2.2020, pubblicata dalla Commissione al fine di rendere possibile a tutti, in egual misura, la transizione digitale.

[36] Regolamento (UE) 2022/868, entrato in vigore nel giugno 2022. Il DGA è diventato pienamente applicabile il 24 settembre 2023; esso riguarda la messa a disposizione dei dati del settore pubblico sulla base di tre pilastri: il riutilizzo dei dati pubblici, qualora tali dati siano oggetto di diritti di terzi; la condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma; il consenso all'utilizzo di dati personali con l'aiuto di un intermediario per la condivisione dei dati personali, e il consenso all'utilizzo dei dati per scopi altruistici. Rappresenta un importante impianto normativo rispetto al funzionamento dello Spazio comune europeo dei dati, già prefigurato nella Comunicazione della Commissione UE del 19 febbraio 2020 e richiamato nel considerando 2 del DGA. Diversamente dal momento in cui il GDPR è diventato efficace e pienamente applicabile, il *Data Governance Act* non dispone degli obblighi di adeguamento nell'immediato, ma offre delle opportunità per tutti coloro che vogliano accedere alla *data economy* utilizzando i dati (personali e non personali) che legittimamente detengono.

[37] Il DGA fissa, inoltre, tra le altre, le condizioni per i servizi di intermediazione nella condivisione dei dati tra imprese.

[38] Regolamento (UE) 2023/2854, entrato in vigore l'11 gennaio 2024 e pienamente applicabile dal 12 settembre 2025, che contiene la disciplina sul dovere di diligenza delle imprese ai fini della sostenibilità, volta a promuovere un comportamento aziendale sostenibile e responsabile. Esso ha lo scopo di regolare l'utilizzo e l'accesso ai dati

una prospettiva complementare al DGA, si pone l'obiettivo di ampliare la platea dei soggetti che hanno accesso alle informazioni: insieme a quest'ultimo esso si inserisce nella più ampia strategia europea per il mercato unico dei dati, in «dialogo» costante con il GDPR.

***3. Il* Digital Services Act *e il* Digital Market Act.** L'intervento della Commissione attraverso il *Digital Services Act Package* ha consentito di aggiornare la disciplina, precedentemente vigente, contenuta nella Direttiva 2000/31/CE[39] relativa all'armonizzazione dell'attività di prestazione transfrontaliera di servizi digitali nel mercato unico europeo[40].

È nel *Digital Services Act* (DSA) che si è concretizzato tale aggiornamento; quest'ultimo è l'atto normativo avente, per l'appunto, l'obiettivo di contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo «norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo»[41].

Esso fa riferimento alle «piattaforme *online* molto grandi»[42] – cd. VLOPs, *very large online platforms* – individuabili dalla Commissione secondo un parametro quantitativo, corrispondente a un numero di destinatari attivi mensili medi del servizio nell'Unione pari o superiore a 45 milioni[43]; e ai motori di ricerca molto grandi - VLOSE, *Very large online search engines* - individuabili anche questi dalla Commissione, in base al numero di utenti da essi fornito.

Tra le VLOPs la Commissione europea ha incluso le piattaforme dei *social media* (come *Twitter*, *Instagram*, *LinkedIn*, *TikTok* e *Facebook*), ma anche quelle di condivisione di video e musica (come *YouTube* e *Spotify*), quelle di alcuni siti di viaggi *online* (come Airbnb) e altri mercati digitali come *Amazon Store*; mentre tra le VLOSE ha individuato *Bing* e *Google Search*.

Attraverso il DSA si è voluto contribuire al corretto funzionamento del mercato interno dei servizi intermediari e alla realizzazione di uno spazio digitale in cui non solo si attuano la prevenzione e la riduzione dei rischi di uso improprio delle piattaforme *online,* ma sono anche definite le responsabilità degli utenti, delle piattaforme e delle autorità pubbliche, riequilibrate

---

generati nell'Unione europea in tutti i settori economici, in modo che sia garantita l'equità nell'ambiente digitale e sia stimolato un mercato dei dati più accessibili a tutti, proteggendo, altresì, le piccole e medie imprese dalle clausole contrattuali abusive imposte dalle parti che si trovano in una posizione contrattuale significativamente più forte.

[39] 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")*. Essa era stata emanata allo scopo di «contribuire al buon funzionamento del mercato garantendo la libera circolazione dei servizi della società dell'informazione tra Stati membri» (art. 1, co. 1), ravvicinando, altresì, «talune norme nazionali sui servizi della società dell'informazione che interessano il mercato interno, lo stabilimento dei prestatori, le comunicazioni commerciali, i contratti per via elettronica, la responsabilità degli intermediari, i codici di condotta, la composizione extragiudiziaria delle controversie, i ricorso giurisdizionali e la cooperazione tra Stati membri» (art. 1, co. 2).

[40] Tale Direttive definiva le responsabilità e gli obblighi dei prestatori di servizi digitali, in particolare delle piattaforme *online*, sottolineando la necessità di stabilire obblighi in materia di informazione e responsabilità per i prestatori di servizi digitali, oltre che per contrastare i contenuti illegali *online*. Richiedeva, inoltre, l'istituzione di una vigilanza pubblica a livello nazionale e di Unione europea ed una cooperazione tra le autorità competenti delle varie giurisdizioni nell'applicazione del diritto, soprattutto per quanto riguarda le questioni transfrontaliere.

[41] Art. 1, par. 1.

[42] Attraverso l'acronimo, GAFAM si descrivono cinque delle più influenti e dominanti società di tecnologia multinazionali, e cioè: *Google, Apple, Facebook, Amazon* e *Microsoft*. Si veda, al riguardo, M. Barbano, *Verso un "antitrust" Italiano 4.0? I GAFAM e i "Big data" all'esame dell'Agcm*, in *Diritto del commercio internazionale*, 4, 2021, 957-987.

[43] Art. 33, par. 1.

in base ai valori europei.
Ponendosi come normativa complementare rispetto alla disciplina comunitaria in materia di protezione dei consumatori, di protezione dei dati personali e di riservatezza delle comunicazioni, il DSA può conferire maggiore sicurezza e apertura a tutti gli utenti; inoltre, puntando sulla crescita e la competitività del mercato digitale, può facilitare l'espansione delle piattaforme più piccole e delle *start-up*.
Il *Digital Markets Act* (DMA), invece, è la legge sui mercati digitali emanata allo scopo di accrescere e armonizzare le responsabilità delle piattaforme *online* e dei fornitori di servizi d'informazione, rafforzando il controllo sulle politiche di contenuto delle piattaforme e introducendo, altresì, regole per assicurare l'equità e la contendibilità dei mercati digitali.
A differenza del DSA, che si rivolge alle imprese che offrono «servizi di intermediazione» agli utenti europei - e, dunque, ai fornitori di accesso a *Internet*, ai servizi *cloud*, *marketplace, social network,* escluse le piattaforme per la messaggistica tra privati - il DMA si rivolge alle grandi piattaforme, ai cd. *gatekeeper,* ovvero ai fornitori di servizi che assumono un impatto significativo sul mercato interno[44], ovvero gestiscono un punto di accesso importante (c.d. *gateway*) per l'intermediazione tra utenti commerciali e consumatori finali[45], ovvero detengono una posizione consolidata e duratura nell'ambito delle proprie attività[46].
Emanato anch'esso, come il DSA, sulla base giuridica dell'art. 114 del TFUE, il DMA ha come oggetto specifico quello di «contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti *gatekeeper* (controllori dell'accesso) siano equi e contendibili in tutta l'Unione, a vantaggio degli utenti commerciali e degli utenti finali»[47]. Si applica, dunque, ai servizi di piattaforma di base forniti o offerti dai *gatekeeper* a utenti commerciali stabiliti nell'Unione o a utenti finali stabiliti o situati nell'Unione, a prescindere dal luogo di stabilimento o di residenza dei *gatekeeper* e dalla normativa altrimenti applicabile alla fornitura del servizio[48].
In definitiva, esso nasce dall'esigenza di disciplinare un mercato in cui un numero ridotto di grandi imprese fornisce servizi di piattaforma di base dotate di considerevole potere economico «che potrebbe qualificarle per essere designate come *gatekeeper*»[49], veri e propri cancelli di entrata fra aziende e utenti[50], in grado di controllare flussi informativi, interfacce e modalità di interazione economica.
Inoltre, persegue lo scopo di scongiurare il rischio di una frammentazione normativa fra gli Stati membri, favorendo il pieno sviluppo delle potenzialità delle piattaforme e affrontando, a livello europeo, le principali ripercussioni delle pratiche sleali e della scarsa contendibilità,

[44] Art. 3, par. 1, lett. *a)*.
[45] Art. 3, par. 1, lett. *b)*.
[46] Art. 3, par. 1, lett. *c)*.
[47] Art. 1, par. 1.
[48] Art. 1, par. 2. Non si applica, invece, ai mercati relativi alle reti di comunicazione elettronica (come le reti satellitari, le reti mobili e le fisse) e ai servizi di comunicazione elettronica che comprendono il servizio di accesso a *internet*, diversi da quelli relativi ai servizi di comunicazione interpersonale indipendenti dal numero.
[49] Cons. 3.
[50] I *gatekeeper* hanno la capacità di stabilire le regole di accesso per gli altri operatori e possono decidere i dati da condividere e le condizioni contrattuali da imporre che, spesso, non sono negoziabili. Il loro potere deriva sia dalla quota di mercato che dal controllo esclusivo delle interfacce tecnologiche, degli utenti e delle informazioni. Infatti, come evidenziato dallo stesso DMA, «la contendibilità è ridotta in particolare a causa dell'esistenza di barriere molto alte all'ingresso o all'uscita» (cons. 3) che si verificano a causa di effetti di rete, del rilievo strategico dell'utilizzo dei dati, della possibile presenza di *switching costs* ma anche di *behavioral biases*. La conseguenza che ne deriva è che le imprese minori, non avendo lo stesso potere, sono costrette a dipendere dalla piattaforma dominante per raggiungere il pubblico senza avere un «accesso paritario ai dati generati dalla loro stessa attività». Cfr. M. Rubino de Ritis, *Intelligenza artificiale e mercato: dalla guerra al possibile equilibrio,* cit.

sì che gli utenti finali e commerciali possano sfruttare pienamente i benefici dell'economia di piattaforma e dell'economia digitale in generale, in un ambiente, per l'appunto, equo e contendibile.
Gli obiettivi evidenziati sono coerenti con il DSA; tuttavia, quest'ultimo si occupa di questioni quali la responsabilità degli intermediari *online* per i contenuti di terze parti, la sicurezza degli utenti *online* o gli obblighi asimmetrici in materia di dovere di diligenza per i diversi fornitori di servizi della società dell'informazione, in funzione della natura dei rischi che tali servizi rappresentano per la società; il DMA, al contrario, affronta le problematiche relative agli squilibri economici, alle pratiche commerciali sleali dei *gatekeeper* e agli effetti negativi che ne conseguono, come, ad esempio, la minore contendibilità dei mercati delle piattaforme. In tal modo, esso integra il diritto vigente dell'UE e quello interno degli Stati membri in materia di concorrenza, contrastando le pratiche sleali dei *gatekeeper*, che non sono contemplate dalla disciplina della concorrenza dell'UE o che da essa non possono essere regolamentate in modo efficace[51].

4. L'IA e le piattaforme digitali. Nel delineato contesto, e, dunque, con specifico riferimento alle piattaforme digitali, grazie alla sua capacità di analizzare grandi quantità di dati, di comprendere i comportamenti degli utenti e di automatizzare numerose attività, l'IA consente alle piattaforme digitali di offrire contenuti personalizzati e suggerimenti mirati, di migliorare la sicurezza e l'efficienza operativa e di ottimizzare, al contempo, la gestione delle interazioni tra utenti, rendendo l'esperienza digitale più fluida e attraente[52].

---

[51] Infatti, a differenza delle norme *antitrust*, che riguardano la situazione di mercati specifici e intervengono in seguito al verificarsi di un comportamento restrittivo o abusivo, il DMA tende a ridurre al minimo *ex ante* gli effetti strutturali pregiudizievoli delle pratiche sleali, senza, tuttavia, limitare la possibilità di intervenire *ex post*, secondo la normativa europea e nazionale in materia di concorrenza. Cfr. A. L. Rum, *Le nuove frontiere della normativa sui servizi digitali nel mercato unico europeo: si rafforza la protezione dei diritti fondamentali degli utenti online con la garanzia pubblicistica delle* Authorities. *Il* Digital Services Act, in *Il Diritto amministrativo*, novembre 2024.

[52] In tema di IA si vedano, *ex multis*, F. Lorè, P. Musacchio, *Artificial Intelligence, tra profili di responsabilità e protezione dei dati personali: aspetti de jure condito e prospettive de jure condendo*, in *amministrativ@mente.it*, 1, 2024; G. Lo Sapio, *L'"Artificial Intelligence Act" e la prova di resistenza per la legalità*, in *Federalismi.it*, 16, 2024, 265-290; Id., *Intelligenza artificiale: rischi, modelli regolatori, metafore*, in *Federalismi.it*, 27, 2022, 232-258; D U. Galetta, *Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono,* in *Federalismi.it*, 12, 2023, 4-14; S. Zorzetto, *La metafora della IA: una giungla lessicale e foresta simbolica,* in *Notizie di Politeia*, 151, 2023, 179-185; S. Salardi - M. Saporiti, *Risposte ai commenti e nuove riflessioni,* in *Notizie di Politeia,* 151, 2023, 186-189; A. Alaimo, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?,* in *Federalismi.it*, 25/2023, 132-149; *Intelligenza artificiale, decisione politica e transizione ambientale: sfide e prospettive per il costituzionalismo*, in *www.federalismi.it*, 15/2023, 40-87; F. Pizzetti, *Con AI Verso la Società digitale,* in *Federalismi.it,* 23, 2023, 4-9; A. Simoncini, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti,* in *Rivista AIC,* 2, 2023; Id., *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, 4, 2019; M. Corti, *L'intelligenza artificiale nel decreto trasparenza e nella legge tedesca sull'ordinamento aziendale,* in *Federalismi.it*, 29, 2023, 162-170; L. Imberti, *Intelligenza artificiale e sindacato. Chi controlla i controllori artificiali?,* in *Federalismi.it*, 29, 2023, 191-201; L. M. Lucarelli Tonini, *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova proposta di* "ai liability directive", in *Diritto dell'Informazione e dell'Informatica* (Il), 2, 2023, 327; D. Chiappini, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea,* in *Rivista Italiana di Informatica e diritto,* 2, 2022, 95-108; N. Rangone, *Intelligenza artificiale e pubbliche amministrazioni: affrontare i numerosi rischi per trarne tutti i vantaggi*, in *BioLaw Journal. Rivista di biodiritto*, 2, 2022, 476 ss.; L. Corso, *Intelligenza collettiva, intelligenza artificiale e principio democratico,* in R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia,* Giuffrè, 2022, 443-459; D. Reinerset al., *The Combination of Artificial Intelligence and Extended Reality: A Systematic Review*, in *Frontiers in Virtual Reality*, 2, 2021; B. Caravita di Toritto, *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo (a cura di), *Intelligenza artificiale*, Milano, 2020, 451 ss.; F. Faini, *Intelligenza artificiale e diritto: le sfide giuridiche in ambito pubblico*, in *BioLaw Journal – Rivista di BioDiritto,* 1, 2019, 145-162; C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto,* 1, 2019, 177;

Essa rappresenta il metodo naturale di analisi dei *big data,* ovvero di quella enorme quantità di informazioni che, non potendo essere gestita dall'uomo attraverso le tradizionali metodologie di archiviazione e analisi, necessita dell'ausilio delle nuove tecnologie[53].
In altri termini, grazie all'IA è possibile determinare la prospettiva etico valoriale, gli stereotipi e *bias* nel processo di *gatekeeping*; infatti, gli algoritmi di *machine learning* rendono possibile suggerire contenuti, prodotti o servizi basati sul comportamento e sulle preferenze degli utenti (come accade, ad esempio, sulle piattaforme Netflix o Amazon); analizzare i dati per offrire annunci mirati e più efficaci; fornire supporto in tempo reale, rispondendo a domande comuni o guidando gli utenti; identificare i *pattern* nei comportamenti degli utenti per prevedere esigenze o *trend* futuri e, infine, monitorare i comportamenti per ridurre i tassi di abbandono (*churn rate*) [54].
Le istituzioni dell'UE mostrano grande attenzione per i settori dell'IA e dei mondi virtuali, nella prospettiva di riuscire a garantire che, pure grazie ad essa, i nuovi mercati digitali rimangano competitivi, contendibili ed equi.
A tal fine, ritengono necessario che siano tenuti in considerazione i rischi legati all'utilizzo dell'IA, sia quelli di natura individuale, sia quelli riferibili ai «pericoli per la società in generale e i danni individuali non materiali»[55], così come evidenziato dal Parlamento europeo nella *Relazione sull'Intelligenza Artificiale in un'era digitale*[56], in cui viene sottolineato che tali rischi potrebbero essere mitigati o eliminati grazie a «contromisure efficaci» che le stesse tecnologie dell'IA possono fornire.
Emerge, tuttavia, dalla Relazione che, «poiché l'IA è ancora nelle sue prime fasi di sviluppo in un contesto più ampio di tecnologie emergenti», non è possibile avere certezza circa il suo pieno potenziale né, tantomeno, conoscere *ex ante* tutti i rischi che da essa derivano. Pertanto, in considerazione dei notevoli «squilibri del potere di mercato», presenti nei mercati dei dati e nella vicina economia dell'IA, sarebbero necessarie una concorrenza leale e la rimozione degli ostacoli affinché le imprese *start-up* e le PMI possano competere e, di conseguenza, possano essere equamente distribuiti i potenziali vantaggi che l'Intelligenza Artificiale arreca in termini sia economici che sociali.
Al riguardo, appare, dunque, quantomai rilevante l'approvazione del DMA, il cui obiettivo è proprio quello di contribuire al corretto funzionamento del mercato interno, a vantaggio degli utenti commerciali e degli utenti finali, stabilendo, a livello europeo, una «serie mirata di obblighi giuridici armonizzati»[57] per garantire mercati digitali in cui non vengano adottate condizioni e pratiche commerciali diverse negli Stati membri a causa delle quali possano

S. Quintarelli, F. Corea, F. Fossa, A. Loreggia, S. Sapienza, *AI: profili etici. Una prospettiva etica sull'Intelligenza Artificiale: princìpi, diritti e raccomandazioni*, in *BioLaw Journal,* in *Rivista di BioDiritto*, 3, 2019, 193.
[53] G. Fasano, *L'intelligenza artificiale nella cura dell'interesse generale,* in *Giornale di diritto amministrativo*, 6, 2020, 715.
[54] I. De Vivo, *Il potere d'opinione delle piattaforme*-online*: quale ruolo del "*regulatory turn*" europeo nell'oligopolio informativo digitale?*, cit., 52. L'A. evidenzia che se la presenza degli algoritmi, invisibili ma non trasparenti, riesce a «mediare» la percezione del reale, essi non possono essere progettati e, successivamente, applicati senza che sia predisposta una forma di controllo e garanzia, perché ciò «significherebbe aprire la strada al tecnodeterminismo» in ragione del quale gli attori che li governano potrebbero non solo determinare essi stessi i valori degli individui e della società, ma anche, conseguenzialmente, dettare «arbitrariamente lo standard di protezione dei diritti e delle libertà a livello transnazionale secondo le logiche del capitalismo digitale». Dunque, è necessario che l'algoritmo sia trattato come oggetto di regolazione, per individuare i limiti costituzionali alle misure normative e all'intervento pubblico nell'autonomia privata; ed anche come strumento di regolazione o di co-regolazione.
[55] *Relazione sull'intelligenza artificiale in un'era digitale*, cit., p.to 97.
[56] Del 5.4.2022.
[57] Reg. (UE) 2022/1925, Cons. 8.

crearsi distorsioni nella concorrenza[58].
Per tale motivo, alla Commissione sono assegnati rilevanti poteri di ispezione e controllo del corretto funzionamento dei mercati digitali, vincolando le imprese o le associazioni di imprese private a garantire l'accesso, laddove ne venga fatta richiesta, anche agli «algoritmi» attraverso i quali viene implementata l'attività commerciale, pena l'irrogazione di un'ammenda nel caso in cui l'impresa attenzionata non garantisca l'accesso all'algoritmo[59].
Tale previsione conferma l'ipotesi di fondo per cui l'implementazione di strutture algoritmiche avanzate può alterare la concorrenza nei mercati digitali[60]: esse, infatti, avvantaggiano fortemente taluni *players* privati, determinando l'effetto di rendere il mercato «non contendibile» e di squilibrare il sistema competitivo continentale, sino al punto di poter costituire autentici «oligopoli digitali»[61].

Ma le problematiche sono anche di altra natura.
Com'è noto, in materia di IA è di recente entrato in vigore l'*AI Act*[62] che rappresenta la prima regolamentazione in materia e che conferma lo scopo perseguito, negli anni, dal Legislatore europeo, di voler promuovere l'adozione di un'Intelligenza Artificiale antropocentrica e affidabile, da utilizzarsi sostenendo l'innovazione ma, allo stesso tempo, garantendo un elevato livello di protezione dagli effetti nocivi che i suoi sistemi possono apportare alla salute, alla sicurezza, ai diritti fondamentali, alla democrazia e all'ambiente[63]. Anche tale atto è stato emanato al fine di evitare che normative nazionali divergenti possano determinare una frammentazione del mercato interno e diminuire la certezza del diritto, in merito, specificamente, allo sviluppo, all'importazione ed all'utilizzo di sistemi di IA, da cui possano, altresì, derivare ostacoli alla libera circolazione, all'innovazione, alla diffusione e all'adozione dei relativi sistemi di IA e dei prodotti e servizi nel mercato interno[64]. Una disciplina uniforme a livello transfrontaliero sull'utilizzo dell'IA, infatti, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, limitando il verificarsi dei rischi ad essa legati.
Il conseguimento degli obiettivi che *l'AI Act* persegue deve avvenire tramite un approccio normativo orizzontale all'IA, equilibrato e proporzionato, «che si limita ai requisiti minimi necessari per affrontare i rischi e i problemi ad essa collegati» senza ostacolare indebitamente lo sviluppo tecnologico[65]. Non deve, inoltre, essere aumentato in modo sproporzionato il costo dell'immissione sul mercato di soluzioni di IA, così come non devono essere create

[58] Il Considerando 7 del Reg. (UE) 2022/1925, in merito alla connessione tra strutture algoritmiche private e potenziale alterazione della concorrenza in materia di mercati digitali, evidenzia come i «*gatekeeper*, pur avendo tendenza ad adottare modelli commerciali e strutture algoritmiche globali o, quanto meno, paneuropei, possono adottare, e hanno in qualche caso adottato, condizioni e pratiche commerciali diverse in Stati membri diversi, il che può creare disparità tra le condizioni di concorrenza per gli utenti dei servizi di piattaforma di base forniti dai *gatekeeper*, a discapito dell'integrazione del mercato interno».
[59] Artt. 30-31 Reg. (UE) 2022/1925.
[60] M. Bevilacqua, *La regolazione* ex ante *delle piattaforme digitali nel nuovo* Digital Markets Act, in *Osservatorio sullo Stato digitale IRPA*, 20 ottobre 2022.
[61] Cfr. M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto Pubblico*, 3, 2021, 739 ss.
[62] Reg. (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).
[63] L'*AI* Act si inserisce nel contesto della c.d. strategia *A Europe fit for the digital age*, delineata dalla Commissione Europea; esso definisce i livelli di rischio associati all'impatto dei diversi sistemi di AI sulla vita delle persone e sui loro diritti.
[64] Reg. (UE) 2024/1689, cons. 3.
[65] Sia consentito un rinvio a B. N. Romano, *In the Era of AI: Exploring New Frontiers in Cybercrime and Safeguarding Personal and Health Data,* in *Corti Supreme e Salute*, 1, 2024, 461-488.

restrizioni inutili al commercio[66].
Specificamente in tema di rischi, con riguardo alle piattaforme digitali, l'*AI Act* prevede che i sistemi e i modelli di IA integrati in piattaforme *online* o motori di ricerca *online,* entrambi di dimensioni molto grandi, «sono soggetti al quadro di gestione dei rischi di cui al regolamento (UE) 2022/2065»[67] (ovvero al DSA).
In altri termini, esso responsabilizza i prestatori di tali piattaforme e motori di ricerca riguardo alla valutazione non solo dei potenziali rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'utilizzo dei rispettivi servizi, ma anche delle modalità attraverso cui la progettazione dei sistemi algoritmici impiegati nel servizio possono contribuire a tali rischi, imponendo loro, a tal fine, l'adozione di misure di attenuazione adeguate nel rispetto dei diritti fondamentali[68].

In particolare, tali fornitori sono tenuti ad individuare e attenuare i rischi sistemici che possono derivare dalla diffusione di contenuti generati o manipolati artificialmente, sì che possa essere efficacemente attuato il reg. (UE) 2022/2065[69]. Essi devono, altresì, rimuovere, a richiesta dell'interessato, non solo i contenuti *online* ritenuti lesivi della propria reputazione, ma anche i contenuti identici o equivalenti ad altri già dichiarati illeciti da un giudice interno, al fine di bilanciare il controllo dei contenuti con la libertà di espressione degli individui[70].
Specificamente il DSA individua ben quattro categorie di rischi sistemici, che vanno dalla diffusione di contenuti illegali (come il materiale pedopornografico o forme illegali di incitamento all'odio) e lo svolgimento di attività illegali[71] alla progettazione dei sistemi algoritmici utilizzati dalle suddette piattaforme o motori di ricerca, o all'abuso dei loro servizi attraverso la presentazione di segnalazioni abusive o altri metodi per ostacolare la concorrenza. Tali rischi si estendono, inoltre, agli effetti negativi reali o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, nonché sulla sicurezza pubblica; infine, (si estendono) a quelli che possono derivare alla tutela della salute pubblica e dei minori dalla progettazione, dal funzionamento o dall'uso, anche mediante manipolazione, di piattaforme *online* e di motori di ricerca *online*[72].
Il Regolamento si sofferma, poi, anche sull' «abuso» che può realizzarsi sulle piattaforme *online* minando la fiducia e ledendo i diritti e gli interessi legittimi delle parti interessate attraverso una continua presentazione di contenuti manifestamente illegali o di segnalazioni o reclami manifestamente infondati; rispetto ad esso devono essere attuate garanzie adeguate, proporzionate ed efficaci, affinché siano rispettati i diritti e gli interessi legittimi di tutte le parti coinvolte[73].
Dal canto suo, l'*AI Act* fornisce una puntuale disciplina in merito ai rischi conseguenti alle

---

[66] Tale precisazione è in linea con la base giuridica della proposta di Regolamento, costituita innanzitutto dall'art. 114 TFUE, che prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno.
[67] Questo prevede il Reg. (UE) 2024/1689 al cons. 118.
[68] *Idem*.
[69] Reg. (UE) 2024/1689, cons. 120, che fa specificamente riferimento al rischio di impatti negativi effettivi o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, anche mediante la disinformazione.
[70] Corte di Giustizia, sent. 3 ottobre 2019, C.18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited.* Cfr. M. C. Girardi, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, cit., 162.
[71] Ad esempio, la vendita di prodotti o servizi vietati dal diritto dell'Unione o nazionale, compresi i prodotti pericolosi o contraffatti e gli animali commercializzati illegalmente.
[72] Le categorie di rischi sono specificate e definite puntualmente nei considerando da 80 a 82 del Reg. (UE) 2022/2065.
[73] Cons. 63.

pratiche vietate[74], tra cui rientrano la manipolazione comportamentale cognitiva di persone o gruppi vulnerabili specifici, la classificazione sociale e i sistemi di identificazione biometrica in tempo reale e a distanza, come il riconoscimento facciale attraverso *web scraping* non mirato. Quest'ultimo, in particolare, è finalizzato a estrarre dati da un sito *web* per poi raccoglierli in *database* o tabelle locali ed analizzarli per dedurre la razza o le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche e l'orientamento sessuale[75].
In altri termini è vietato l'utilizzo dei sistemi di IA per valutare o classificare le persone fisiche o i gruppi di esse per un certo periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali, al fine di evitare trattamenti pregiudizievoli o sfavorevoli in contesti sociali estranei a quelli in cui i dati sono stati originariamente generati o raccolti.
Sulle piattaforme digitali la *privacy* e la sicurezza dei dati risultano particolarmente esposte ai suddetti rischi: essi possono derivare proprio dalla raccolta eccessiva di dati grazie ai quali personalizzare l'esperienza dell'utente. Infatti, attraverso algoritmi avanzati è possibile creare una profilazione approfondita, ovvero la creazione di profili dettagliati degli utenti, anche riguardo a dati sensibili come preferenze personali, salute o orientamento politico; così come, grazie all'addestramento degli algoritmi su dati storici, è possibile la riproduzione di pregiudizi esistenti che, magari, vengono amplificati, con impatti negativi, su settori cruciali come il mercato del lavoro o l'accesso ai servizi.
Tali dati potrebbero, inoltre, essere usati in modi non etici, ad esempio per manipolare le scelte o indirizzare pubblicità mirata[76].
Le recenti Linee guida emanate dalla Commissione al fine di fornire orientamenti sulle pratiche vietate di Intelligenza Artificiale[77], nell'ottica di garantire l'applicazione coerente,

[74] Art. 5 Reg. (UE) 2024/1689. Tale norma disciplina quattro categorie di rischio, classificate in base alla gravità. Esse sono quelle di: rischio *inaccettabile*, relative a pratiche come la manipolazione dannosa, il punteggio sociale e la sorveglianza biometrica in tempo reale, vietate in quanto considerate una chiara minaccia per i diritti e la sicurezza delle persone; rischio *elevato*, relativo a sistemi che operano in settori critici come trasporti, istruzione, sanità, e nella gestione delle infrastrutture critiche e che richiedono severi requisiti di controllo umano e conformità, data la loro capacità di prendere decisioni che impattano direttamente le vite delle persone; rischio *limitato*, relativo a sistemi come i *chatbot* e le IA generative che possono simulare l'essere umano e per i quali l'*AI Act* impone, in particolare, obblighi di trasparenza, quale quello di informare gli utenti quando interagiscono con un'IA, per prevenire frodi e disinformazione; infine, rischio *minimo* o *nullo*, relativo alla maggior parte dei sistemi, come filtri *antispam* o giochi, in cui non sussistono rischi significativi, per cui non è prevista regolamentazione specifica.
[75] Reg. (UE) 2024/1689, art. 5, lett. b *bis*). È, in buona sostanza, vietato l'utilizzo dei sistemi di AI per valutare o classificare le persone fisiche o i gruppi di esse per un certo periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali al fine di evitare trattamenti pregiudizievoli o sfavorevoli in contesti sociali estranei a quelli in cui i dati sono stati originariamente generati o raccolti.
[76] Va segnalata, al riguardo, la recentissima pronuncia della Quarta Sezione della Corte di giustizia dell'Unione Europea del 4 ottobre 2024 - causa C-446/21 - avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dall'*Oberster Gerichtshof* (Corte suprema, Austria), con decisione del 23 giugno 2021, nel procedimento *Maximilian Schrems* contro *Meta Platforms Ireland Ltd*, già *Facebook Ireland Ltd*. La questione riguarda il trattamento asseritamente illecito dei dati personali da parte della piattaforma Meta; in tale occasione, la Corte ha precisato limiti stringenti all'uso dei dati per finalità pubblicitarie da parte delle piattaforme, sottolineando il valore fondamentale del principio di minimizzazione del trattamento (art. 5, par. 1, lett. c RGPD) e l'inammissibilità dell'uso indistinto di dati personali, specialmente se ricavabili da fonti terze. Le questioni sollevate in tale sentenza si riflettono anche sul piano dell'azione pubblica che faccia uso di IA, imponendo alle amministrazioni l'adozione di misure proporzionate, trasparenti e giustificate nel trattamento di dati, ispirate ad una logica di necessità, proporzionalità e rispetto della volontarietà del conferimento dei dati, in particolare quando si rischi di inferire categorie sensibili, partendo da dati apparentemente neutri.
[77] *Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/ 1689 (regolamento sull'IA)*, del 29 lugli 2025.

efficace e uniforme della legge sull'IA in tutta l'Unione europea, chiariscono[78] come tale disciplina si coordini, in particolare, con quella del Regolamento sui servizi digitali, definendo «complementari» i divieti contenuti nell'*AI Act* con quelli del DSA e facendo riferimento agli obblighi da questo introdotti volti a garantire trasparenza, sicurezza e responsabilità nella fornitura dei servizi intermediari.

In particolare, esse impongono ai fornitori di piattaforme *online* e motori di ricerca di evitare pratiche manipolative e di assicurare la tutela effettiva degli utenti[79], sottolineando, altresì, che le piattaforme di grandi dimensioni (VLOPs e VLOSEs) sono tenute a condurre valutazioni periodiche dei rischi sistemici derivanti dal funzionamento dei propri algoritmi di raccomandazione, pubblicità o moderazione dei contenuti, adottando misure per la loro mitigazione[80].

In questo contesto, tali *Linee guida*, ad avviso di chi scrive, contribuiscono a precisare il quadro, chiarendo, al contempo, che la gestione dei rischi algoritmici deve rispettare i principi di liceità, trasparenza e proporzionalità propri del GDPR, assicurando coerenza grazie alla complementarità tra i diversi strumenti regolatori. Pare evidente, inoltre, che si stiano sempre più rinforzando le basi affinché possa determinarsi un modello di *governance* algoritmica integrata, che responsabilizza tutti gli attori coinvolti ed in cui la prevenzione dei rischi e la protezione dei diritti fondamentali diventano pilastri comuni della regolazione europea delle piattaforme digitali. Tale disciplina assume, tra l'altro, una rilevanza ancora maggiore se si pensa che, precedentemente all'emanazione dell'*AI Act*, non esistevano norme di riferimento - a livello europeo e non solo - grazie alle quali fronteggiare i nuovi rischi conseguenti all'uso dell'Intelligenza Artificiale; così come non esistevano norme neanche relative alla raccolta, all'elaborazione, alla conservazione e all'utilizzo di dati tramite queste tecnologie e si continuava a fare riferimento a principi come quelli di limitazione delle finalità, di minimizzazione dei dati o del consenso contenuti in discipline molto datate e risalenti ad un'epoca in cui non solo le piattaforme, ma anche *Internet,* non erano così diffusi[81].

5. Gli atti di* soft law *sull'interazione tra DMA, DSA e GDPR. Ancora più recentemente sono state proposte Linee guida con riguardo all'interazione sia del DSA[82] che del DMA[83] con il GDPR: si tratta di atti di *soft law* ancora in fase di consultazione pubblica e, dunque, non definitivi, di cui, senza entrare puntualmente nel merito, si intende evidenziare gli aspetti salienti.

Specificamente, le *Guidelines 3/2025 on the interplay between the DSA and the GDPR* sono state adottate l'11 settembre 2025 dal Comitato europeo per la protezione dei dati (EDPB) e sono in consultazione pubblica fino al 31 ottobre 2025. L'obiettivo che si prefiggono è quello di fornire indicazioni concrete per garantire un'applicazione coerente tra la disciplina posta a tutela dei dati personali (GDPR) e quella relativa all'ecosistema *online* sicuro e trasparente (DSA), in modo che quest'ultima non deroghi alla prima. Le due discipline devono, dunque, operare in parallelo ed essere applicate in modo compatibile, evitando riduzioni del livello di

[78] Ai Cons. 139 e 140.

[79] In particolare, infatti, si intendono quali esempi di tecniche manipolative o ingannevoli ai sensi dell'art. 5, par. 1, lett. a), del regolamento sull'IA, qualora possano provocare danni significativi, i *dark patterns*, ovvero le interfacce progettate per indurre l'utente a scelte inconsapevoli, vietate dall'art. 25 del DSA.

[80] Tali previsioni si integrano con l'approccio dell'*AI Act*, che estende la logica della valutazione e prevenzione del rischio a ulteriori scenari applicativi (come *chatbot* e sistemi di IA generativa) che non sono coperti dal DSA.

[81] G. Mobilio, *L'Intelligenza Artificiale e i rischi di una «*disruption*» della regolamentazione giuridica,* in *BioLaw Journal*, n. 2, 2020, 422.

[82] *Guidelines 3/2025 on the interplay between the DSA and the GDPR*.

[83] *Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation*.

protezione, sì da fornire certezza giuridica ai fornitori di servizi intermediari (*hosting*[84], piattaforme *online*, motori di ricerca) e proteggere i diritti fondamentali degli utenti.
Tali Linee guida si concentrano su alcune disposizioni del DSA con un'interazione particolarmente intensa con il GDPR, per esempio relativamente alle misure per rilevare contenuti illegali[85] con possibili trattamenti di dati personali. In tali casi si prevede che i trattamenti relativi alla rimozione o disabilitazione di contenuti devono rispettare i principi del GDPR e fondarsi su basi giuridiche contenute in tale atto[86]. Inoltre, è raccomandata una valutazione d'impatto (DPIA) nei casi ad alto rischio ed in cui la rimozione o la disabilitazione di contenuti implichi trattamenti di dati personali. Ancora, con riferimento ai sistemi di segnalazione[87], è previsto che le piattaforme predispongano meccanismi di segnalazione di contenuti illegali e gestione dei reclami, limitando la raccolta dei dati personali allo stretto necessario e informando adeguatamente gli interessati.
Rientrano, inoltre, nel campo del GDPR anche le vietate interfacce ingannevoli (*dark patterns*)[88] se influenzano il comportamento degli utenti nel fornire dati personali; così come, a proposito dell'uso vietato di categorie particolari di dati per pubblicità basata su profilazione[89], si precisa[90] che la disciplina contenuta nel DSA[91] deve applicarsi senza pregiudicare (cioè senza derogare o entrare in conflitto con) le disposizioni del GDPR, in particolare con riferimento a quelle relative al diritto di opposizione, alle decisioni automatizzate, inclusa la profilazione, e alla necessità del consenso dell'interessato prima del

[84] Dal termine inglese *to host,* che significa «ospitare», l'*hosting* è l'allocazione di un sito o di un'applicazione su un *server* nel *web*, tramite cui si forniscono ai professionisti gli strumenti necessari affinché il proprio sito sia visibile in rete. Cfr. A. Palmieri, *Profili giuridici delle piattaforme digitali. Tutela degli utenti commerciali e dei titolari di siti web aziendali*, Torino, 2019. Va evidenziato che, negli anni, si è formata una nutrita giurisprudenza, in particolare con riguardo al regime di responsabilità che deve essere applicato in merito alle cosiddette piattaforme di *hosting*. Tali piattaforme hanno permesso la diffusione di massa di qualsiasi tipo di contenuto grazie al ruolo centrale raggiunto in relazione agli accessi degli utenti e allo scambio di informazioni in rete. Al riguardo si segnala la sentenza n. 1208/2023, emanata dal Tribunale di Milano, nella causa *Snaitech* + altri c. *Facebook* Ireland *Limited* n. 31458/2020 e riguardante la condotta illecita di *Facebook* sulla mancata rimozione di profili con contenuti evidentemente diffamatori. Il giudice, attraverso di essa, si è pronunciato sull'obbligo generale in capo alle piattaforme *social* (nello specifico, *Facebook*) di rimuovere i contenuti che vengono segnalati dagli utenti come diffamatori. La società *Facebook* è stata, infatti, qualificata come un ISP (*Internet Service Provider*) - nello specifico quale *hosting provider* - in quanto la sua attività si limiterebbe a «immagazzinare» informazioni senza mantenere un ruolo prettamente attivo nella condivisione delle stesse. Cfr. A. Zurzolo, *La nuova frontiera della regolazione delle piattaforme digitali: le sanzioni contro Google e Meta,* in *Diritto Mercato Tecnologia*, 22 febbraio 2023.
[85] 2.1. *Voluntary own-initiative investigations and legal compliance in relation to illegal content (Article 7 DSA*), in cui, richiamando gli articoli da 4 a 6 del DSA - che stabiliscono esenzioni di responsabilità per i fornitori di servizi di semplice trasmissione, memorizzazione temporanea e *hosting* che consentono la trasmissione e/o l'archiviazione di informazioni, a determinate condizioni - si porta l'esempio di un fornitore di servizi di *hosting* che non abbia effettiva conoscenza di contenuti illegali e, per quanto riguarda le richieste di risarcimento danni, non sia a conoscenza di fatti o circostanze dai quali risulti evidente l'illegalità dei contenuti. Tale soggetto non è considerato responsabile dei danni subiti dai destinatari del servizio o da terzi a seguito della memorizzazione (compresa la diffusione, nel caso in cui il fornitore sia una piattaforma online) di tali contenuti illegali.
[86] Ovvero l'art. 6(1)(c) o (f) GDPR) e, se i trattamenti sono automatizzati, si devono considerare le regole dell'art. 22 GDPR.
[87] 2.2 *Processing of personal data in notice and action mechanisms and in internal complaint-handling systems* (Articles 16, 17, 20, and 23 del DSA).
[88] 2.3 *Deceptive design patterns* (art. 25 DSA).
[89] Contenuto nell'art. 26 del DSA che impone regole di trasparenza ai fornitori di piattaforme *online* in materia di pubblicità e vieta loro di mostrare annunci agli utenti basati sulla profilazione che utilizzi categorie particolari di dati personali di cui all'art. 9, par. 1, del GDPR (come dati relativi alla salute, all'origine etnica, alle convinzioni religiose, ecc.).
[90] 2.4 *Advertising transparency and prohibition of presenting advertisements based on profiling using special categories of data (Article 26).*
[91] E cioè il cons. 68.

trattamento dei dati personali per fini di pubblicità mirata[92]. Sono, altresì, previsti sistemi di verifica dell'età dei minori che non implichino identificazioni univoche o memorizzazioni permanenti dei dati[93].

Tali Linee guida, infine, contengono la raccomandazione alle autorità di protezione dei dati di partecipare alla redazione dei codici di condotta previsti dal DSA per garantire coerenza con quelli del GDPR[94], prevedendo, altresì, una cooperazione obbligatoria e continua tra la Commissione europea, i Digital Services Coordinators e le autorità per la protezione dei dati, al fine di evitare conflitti di competenza e violazioni del principio del *ne bis in idem*.

Per quanto riguarda, invece, le *Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation*, queste sono state adottate il 9 ottobre 2025, elaborate dal medesimo EDPB con la Commissione europea e anch'esse in versione ancora non definitiva. Contengono i primi orientamenti congiunti, in linea con la Strategia 2024-2027 e con gli obiettivi della recente dichiarazione di Helsinki relativi alla semplificazione della conformità al GDPR e sono finalizzate a promuovere contemporaneamente trasparenza, libertà di scelta e tutela dei diritti fondamentali degli utenti, attraverso l'interazione tra il GDPR e il DMA, che, come detto, mira a garantire mercati digitali equi e aperti, intervenendo sulle pratiche anticoncorrenziali dei grandi operatori *online* (i *gatekeeper*).

Uno dei punti centrali affrontati dalle Linee guida riguarda il consenso degli utenti[95]: i *gatekeeper* non possono combinare o riutilizzare i dati personali raccolti attraverso servizi diversi senza aver ottenuto un consenso esplicito e informato, in linea con quanto previsto dal GDPR. Inoltre, gli utenti devono poter disporre di un'alternativa «meno personalizzata ma equivalente», in modo da non essere penalizzati se decidono di non prestare il consenso.

Altro aspetto cruciale concerne, poi, la distribuzione di applicazioni e *store* digitali[96]: infatti, le piattaforme sono tenute a consentire l'installazione e l'uso di *app* di terze parti, garantendo comunque la piena osservanza delle norme in materia di protezione dei dati personali.

Le Linee guida ribadiscono, poi, l'importanza del diritto alla portabilità dei dati[97], che viene rafforzato e ampliato rispetto a quanto già previsto dal GDPR grazie alla possibilità, per gli utenti (o terze parti da loro autorizzate) di trasferire agevolmente i propri dati tra diversi servizi digitali, favorendo, così, la concorrenza e la libertà di scelta. In materia di accesso ai dati[98] esse obbligano i *gatekeeper* a condividere determinate informazioni con imprese commerciali o motori di ricerca concorrenti, ma soltanto qualora tali dati siano anonimizzati o vi sia un consenso esplicito degli utenti interessati: in tal modo si viene a bilanciare l'apertura dei mercati digitali con le garanzie di riservatezza e sicurezza dei dati.

Infine, anche queste Linee guida, come le altre, sottolineano l'esigenza di una stretta cooperazione tra le autorità competenti, per cui la Commissione europea, responsabile dell'attuazione del DMA, e le autorità garanti per la protezione dei dati, incaricate dell'attuazione del GDPR, devono coordinare le rispettive azioni per garantire un'applicazione coerente delle norme e prevenire conflitti di competenza o duplicazioni sanzionatorie.

---

[92] Parimenti, è previsto che l'art. 26 DSA non incide sulle norme della Direttiva *ePrivacy* relative alla memorizzazione di informazioni nei dispositivi terminali degli utenti (come *cookie* o *tracker*) e all'accesso alle informazioni ivi conservate.

[93] 2.6 *Protection of minors (Article 28)*.

[94] 2.8 *Codes of conduct, including for online advertising (Articles 45, 46 and 47), and their relationship with codes of conduct under Article 40 GDPR*.

[95] 5.4 *Mechanism(s) enabling access to end-user's personal data*, par. 160 che fa riferimento all'art. 5 del DMA (Obblighi dei *gatekeeper*).

[96] 3 *Distribution of software application stores and software applications (Article 6(4) DMA)*.

[97] 4. *Right to data portability of end users and third parties authorised by end users (Article 6(9) DMA)*.

[98] 5. *Right to data access of business users and authorised third parties (Article 6(10) DMA)*.

Dall'analisi effettuata si conferma, a parere di chi scrive, una tendenza sempre più marcata verso l'integrazione dei diversi strumenti di *governance* del digitale. Tale aspetto non può che costituire un'evoluzione significativa, in quanto segna il passaggio da un approccio settoriale e frammentato a un tentativo di costruzione di un diritto digitale unitario, fondato su principi comuni di trasparenza, proporzionalità e responsabilità. Tuttavia, non va negato il timore che l'interazione tra le suddette fonti europee possa dar vita a una complessità regolatoria crescente, che finisca col tradursi in difficoltà applicative e in una possibile sovrapposizione di competenze tra autorità di controllo. Laddove, invece, in questo quadro, l'obiettivo del Legislatore deve essere, piuttosto, quello di garantire coerenza e certezza del diritto data la continua trasformazione del contesto, evitando che l'espansione delle regole digitali freni la capacità di innovazione e dia vita ad un «labirinto normativo» anziché ad un ecosistema chiaro e accessibile.

6. Le recenti novità nel panorama nazionale: la legge italiana sull'Intelligenza Artificiale. Cenni. Da ultimo, merita qualche cenno la recentissima legge nazionale in tema di Intelligenza Artificiale e di trattamento dei dati nei mercati digitali, ovvero la l. n. 132/2025, contenente *Disposizioni e deleghe al Governo in materia di Intelligenza Artificiale*.

Va detto che l'Italia è stata il primo Stato membro a dotarsene, anche al fine di disciplinarne l'utilizzo da parte della Pubblica Amministrazione, la cui attività e i cui rapporti con i cittadini, in conseguenza di tali evoluzioni, si sono trasformati in maniera radicale. Al riguardo, la legge prevede, infatti, che le pubbliche amministrazioni utilizzino l'Intelligenza Artificiale «allo scopo di incrementare l'efficienza della propria attività, di ridurre i tempi di definizione dei procedimenti e di aumentare la qualità e la quantità dei servizi erogati ai cittadini e alle imprese, assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo»[99]. La norma prevede, altresì, che tale utilizzo sia finalizzato a fornire un supporto all'attività decisionale, senza sostituire l'autonomia e la responsabilità umana, che restano in capo al funzionario competente, rimettendo alle amministrazioni l'adozione di misure tecniche, organizzative e formative, e avvalendosi, per tutti gli adempimenti previsti dalla legge, delle risorse già disponibili.

Così posta la disciplina pare volere, dunque, legittimare l'uso dell'IA al fine di favorire la «buona amministrazione», nel rispetto dei principi di legalità, imparzialità, trasparenza e partecipazione, tentando, altresì, di superare le profonde criticità che si sono palesate (e continuano a palesarsi) nei processi di implementazione, e tenendo conto delle nuove dinamiche sociali oltre che delle conseguenziali nuove modalità di esercizio del potere pubblico.

Ciononostante, tali criticità, ad avviso di chi scrive, potrebbero non essere superate nel breve periodo, perché la conoscenza dei sistemi e delle potenzialità dell'IA non è ancora tale da consentirne un utilizzo disinvolto, che limiti (o, addirittura, escluda) conseguenze in termini di responsabilità e che renda le amministrazioni capaci di adottare le misure tecniche richieste dalla legge, per di più avvalendosi delle risorse, innanzitutto umane, già a disposizione delle amministrazioni. Si ravvisa, in altri termini, la necessità che si perfezionino e si consolidino maggiormente le conoscenze in materia di Intelligenza Artificiale sì da poterne consentire un utilizzo responsabile.

Ad ogni buon conto, la legge – composta da 28 articoli ed entrata in vigore il 10 ottobre 2025 – intende fornire una cornice normativa nazionale sull'Intelligenza Artificiale che apra un complesso dialogo con il Regolamento europeo dell'*AI Act*, di cui recepisce i principi, senza, tuttavia, prevedere nuovi obblighi. Al contempo, essa introduce una disciplina specifica per

[99] Art. 14, co. 1, l. n. 132/2025.

settori chiave con l'obiettivo dichiarato di promuovere uno sviluppo dell'IA sicuro, affidabile, trasparente e rispettoso della dignità umana, in una dimensione antropocentrica, garantendo la vigilanza sui rischi economici e sociali e sull'impatto sui diritti fondamentali dell'Intelligenza Artificiale stessa[100].

Il Legislatore ha precisato che l'uso dei sistemi ad essa relativi deve svolgersi nel pieno rispetto del metodo democratico che caratterizza la vita istituzionale e politica, nonché dei principi di autonomia e sussidiarietà che regolano l'azione delle istituzioni territoriali, e che non può in alcun modo essere compromessa la libertà del dibattito democratico che deve restare immune da interferenze illecite o manipolazioni algoritmiche[101].

Specificamente sul tema della protezione dei dati personali, la disciplina sembra voler dar vita ad una integrazione «funzionale» con il GDPR, trasformando i principi di protezione della *privacy* in un solido fondamento per uno sviluppo responsabile dell'Intelligenza Artificiale. Infatti, il comma 2 dell'art. 4 richiede che i sistemi di IA garantiscano «il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità al diritto dell'Unione europea in materia di dati personali». Mentre il co. 3 della stessa norma prevede l'obbligo di spiegabilità dei medesimi sistemi, il quale si aggiunge alla richiesta di informazioni chiare sul trattamento dei dati già prevista nel GDPR, affinché possa essere garantita all'utente «la conoscibilità dei relativi rischi e il diritto di opporsi ai trattamenti autorizzati dei propri dati personali». In tal modo si intravede una forma di rafforzamento della trasparenza in quanto essa non si limita ai soli dati trattati, ma si estende anche ai meccanismi decisionali dell'IA. Inoltre, l'art. 3, co. 2, richiede che lo sviluppo di sistemi e di modelli (di Intelligenza Artificiale) per finalità generali avvenga «su dati e tramite processi di cui devono essere garantite e vigilate la correttezza, l'attendibilità, la sicurezza, la qualità, l'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati».

Puntuale attenzione è, poi, dedicata ai dati sensibili o «particolari»[102], quali quelli relativi alla salute, ai minori, o ai dati trattati in ambito lavorativo; mentre con riguardo alla ricerca e alla sperimentazione sono introdotte disposizioni che permettono l'uso dei dati (anche «particolari») in forma anonimizzata, pseudonimizzata o sintetica, nei casi di interesse pubblico, a condizione che siano rispettate le garanzie previste e che sia data informativa agli interessati o al Garante per la *privacy*.

A ben vedere, il Legislatore punta, dunque, ad una lettura di tale legge coordinata sia con il GDPR che con l'*AI Act* al fine di rafforzare la tutela degli interessati e responsabilizzare i titolari del trattamento.

Con riguardo, specificamente, alle piattaforme, è contemplato il richiamo a quelle di *e-procurement* delle amministrazioni pubbliche[103], che lo Stato e le altre autorità pubbliche devono indirizzare affinché possano scegliere fornitori di sistemi e di modelli di Intelligenza Artificiale privilegiando «soluzioni che garantiscono la localizzazione e l'elaborazione dei dati strategici presso data center posti nel territorio nazionale, le cui procedure di disaster recovery e *business continuity* siano implementate in data center posti nel territorio nazionale, nonché modelli in grado di assicurare elevati standard in termini di sicurezza e trasparenza nelle modalità di addestramento e di sviluppo di applicazioni basate sull'Intelligenza Artificiale generativa, nel rispetto della normativa sulla concorrenza e dei principi di non discriminazione e proporzionalità». In altri termini, con tale norma, il Legislatore intende,

[100] Art. 1, l. n. 132/2025.
[101] Ai sensi dell'art. 3, co. 4.
[102] Che il GDPR definisce all'art. 9, recante *Trattamento di categorie particolari di dati personali*.
[103] All'art. 5, co. 1, lett. *d)*.

dunque, orientare la Pubblica Amministrazione verso un uso dell'IA che, oltre che sicuro e trasparente, sia anche territorialmente controllabile, ponendo, in tal modo, le basi per una «sovranità digitale pubblica» grazie alla quale proteggere i dati strategici favorendo, al contempo, lo sviluppo tecnologico interno, ma sempre e comunque nel rispetto delle regole europee.

Nonostante lambisca gran parte delle problematiche inerenti l'uso dell'IA (con riguardo a molteplici settori, dal lavoro alla sanità, dalla pubblica amministrazione alla giustizia), va, tuttavia, detto che la l.n. 132/2025 contiene comunque delle imprecisioni che, probabilmente, sono anche il frutto della «rapidità» con la quale è stata emanata. Certo è ancora troppo acerba per potere già avere prodotto risultati, ciononostante non si può sottacere il timore che le numerose deleghe legislative che contiene possano finire con il frammentare il panorama normativo, compromettendo, di tal guisa, la creazione di un contesto in cui, grazie alla certezza del diritto, sia possibile attrarre e favorire la crescita di nuove realtà tecnologiche.

7. Riflessioni conclusive. Le considerazioni svolte consentono di trarre alcune riflessioni di carattere generale, volte a delineare le prospettive che il diritto europeo e nazionale sono oggi chiamati ad affrontare. Le sfide poste dall'Intelligenza Artificiale e dalla regolazione dei mercati digitali assumono una portata sistemica che travalica i singoli interventi legislativi: quanto è emerso dalla analizzata disciplina che, via via, va sempre più implementandosi (grazie anche alle *Linee guida*) e che si è arricchita, sul piano nazionale, di una legge specifica sull'IA, denota una parte di non poco rilievo nell'ambito di un processo – che, in realtà, si prefigura molto più ampio – di adattamento del diritto ai mutamenti tecnologici e sociali in atto. Sono, infatti, ancora tante le problematiche determinate dall'IA e che restano in parte sconosciute o senza una risposta concreta e chiara per gli utenti che utilizzano le piattaforme digitali.

Si tratta di questioni che mettono in discussione non soltanto la tenuta delle categorie giuridiche tradizionali, ma anche la capacità stessa delle istituzioni di governare in modo democratico e trasparente i processi di automazione.

Tuttavia, il quadro normativo che, nel giro di poco tempo, si sta consolidando, denota una particolare attenzione da parte delle istituzioni europee rispetto alla garanzia, in generale, di una maggiore tutela ai diritti degli utenti *online*, contro lo sviluppo di possibili fenomeni degenerativi.

Emerge, inoltre, che l'obiettivo prioritario che si intende conseguire è quello di creare una disciplina uniforme per tutti gli Stati membri, al fine di evitare che normative nazionali divergenti possano determinare una frammentazione del mercato interno e diminuire la certezza del diritto, in merito alle tematiche specificamente affrontate. Per quanto riguarda l'*AI Act*, in particolare, tali tematiche attengono allo sviluppo, all'importazione e all'utilizzo di sistemi di IA, da cui possano, altresì, derivare ostacoli alla libera circolazione, all'innovazione, alla diffusione e all'adozione dei sistemi relativi e dei prodotti e servizi nel mercato interno[104].

L'armonizzazione appare, dunque, essenziale non solo per favorire la competitività e l'innovazione, ma anche per garantire che la trasformazione digitale avvenga nel pieno rispetto dei valori democratici, della trasparenza e della centralità della persona.

Una disciplina uniforme a livello transfrontaliero, anche e in particolare sull'utilizzo dell'IA, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, limitando il verificarsi dei rischi ad essa legati - sia materiali che immateriali, compreso il pregiudizio fisico, psicologico, sociale o economico - e che

[104] Reg. (UE) 2024/1689, rec. 3.

possono pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione.

In questa prospettiva, appare chiara l'urgenza di rafforzare il ruolo delle amministrazioni pubbliche come garanti dei diritti fondamentali anche nell'ambiente digitale, attraverso un'amministrazione responsabile, trasparente e tecnicamente competente. Esse sono chiamate a operare secondo un nuovo paradigma, in cui l'efficienza algoritmica deve essere bilanciata da presìdi giuridici capaci di assicurare l'effettività delle tutele e la legalità dell'azione pubblica.

Al più volte dichiarato fine di garantire trasparenza ed equità nella gestione dei contenuti e tutelare maggiormente i diritti in rete, l'Unione europea ha, dunque, tentato di attuare un *costituzionalismo digitale*[105], attraverso l'emanazione di atti che vanno dal GDPR – fra tutti il più risalente[106] – ai più recenti DSA e DMA e *AI Act*, grazie ai quali sottoporre le piattaforme *online* a un controllo democratico, mediante strumenti di regolazione *ex ante*[107].

In particolare, *l'AI Act* prevede espressamente un collegamento con il GDPR[108], del quale richiama i principi fondamentali e, specificamente il considerando 47, che prevede che «per ovviare all'opacità che può rendere alcuni sistemi di IA incomprensibili o troppo complessi per le persone fisiche, è opportuno imporre un certo grado di trasparenza per i sistemi di IA ad alto rischio. Gli utenti dovrebbero poter interpretare gli output del sistema e utilizzarlo in modo adeguato […]». Del resto, il principio di trasparenza viene esteso espressamente non solo al trattamento dei dati personali ma all'intero funzionamento del sistema.

In definitiva, se, da un lato, il principio di trasparenza appare essenziale non solo rispetto al trattamento dei dati personali, ma anche rispetto all'intero funzionamento del sistema stesso, dall'altro lato è necessario che, per garantire la tutela del diritto fondamentale alla protezione dei dati personali e la loro libera circolazione all'interno dell'Unione europea, le regole sull'IA siano armonizzate con quelle sulla *data protection* e sulla circolazione dei dati personali, anche dal punto di vista economico[109].

Il nesso tra Intelligenza Artificiale e protezione dei dati personali si conferma, dunque, il terreno privilegiato sul quale si misura la compatibilità tra efficienza tecnologica e garanzie dello Stato di diritto.

Così come si conferma pure la necessità della componente umana nei processi decisionali compiuti ed elaborati dal sistema artificiale e che abbiano un profondo impatto sulla *privacy* e/o sulla salute e l'integrità fisica e necessitino di un successivo controllo o di una ratifica.

Si rafforza sempre più, pertanto, la convinzione che non può che restare in capo all'individuo il potere – e il diritto – di comprendere, controllare e contestare le scelte operate dagli algoritmi, scongiurando il pericolo dell'opacità (c.d. «effetto scatola nera»)[110] tipico dei processi decisionali ad essi affidati, affinché il progresso tecnologico non si traduca in un arretramento delle garanzie dello Stato di diritto, ma ne diventi, al contrario, il più moderno strumento di attuazione.

---

[105] In merito al costituzionalismo digitale si rinvia a O. Pollicino, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quad. cost.*, 3, 2023, 569 ss.

[106] Regolamento UE 679/2016.

[107] M. C. Girardi, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, cit., 156.

[108] Come previsto al punto 1.2 della *Relazione di accompagnamento al Regolamento del Parlamento europeo e del Consiglio* che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, del 21 aprile 2021.

[109] Cfr. L. M. Lucarelli Tonini, *L'IA tra trasparenza e nuovi profili di responsabilità: la nuova proposta di* "ai liability directive", cit., 336.

[110] F. Calisai, *Intelligenza artificiale e ambiente*, cit., 903.

Abstract. L'applicazione dell'IA nelle piattaforme digitali rappresenta una rivoluzione che rende possibili numerose opportunità ma che pone anche rischi significativi. Essa, infatti, attraverso processi automatizzati, contribuisce a migliorare l'esperienza degli utenti e a facilitare attività come il commercio elettronico e i contratti intelligenti. Tuttavia, questi progressi sono accompagnati da rischi legati non solo alla rigidità dei sistemi di IA – che può portare a errori o danneggiare gli utenti per l'assenza di un'intenzionalità umana diretta – ma pure alla difficoltà di tutelare la *privacy* e i dati, poiché le piattaforme, grazie anche all'IA, ne elaborano grandi quantità attraverso modalità che potrebbero non essere conformi a normative rigorose come quella del GDPR. Il presente contributo affronta tali aspetti e ne esamina le relative implicazioni alla luce del recente quadro regolatorio che si è venuto a delineare (e che si è ultimamente arricchito anche della l.n. 132/2025 sull'IA) e che sembra orientato alla costruzione di un ecosistema digitale improntato a trasparenza, equità e tutela dei diritti fondamentali, nel tentativo di bilanciare le esigenze di innovazione e competitività con quelle di salvaguardia della persona.

Abstract. The application of AI within digital platforms represents a revolution that enables numerous opportunities but also poses significant risks. Indeed, through automated processes it helps to improve the user experience and facilitate *Act*ivities such as e-commerce and smart contr*act*s. However, these advances are accompanied by risks related to the rigidity of AI systems – which may lead to errors or harm users due to the absence of direct human intent – but also related to challenges in protecting privacy and personal data, as platforms, thanks in part to AI, process vast amounts of information in ways that may not fully comply with strict regulations such as the GDPR.
This paper addresses these issues and examines their implications in light of the recent regulatory framework that has emerged (and which has recently been supplemented by Law l. no. 132/2025 on AI), which appears to be oriented toward building a digital ecosystem grounded in transparency, fairness, and the protection of fundamental rights, in an attempt to balance the needs of innovation and competitiveness with those of safeguarding the individual.

Parole chiave. Intelligenza artificiale – Piattaforme digitali – Protezione dei dati e *Privacy*.

Key words. Artificial Intelligence – Digital Platforms – Data Protection and Privacy.