

## Intelligenza artificiale e costituzionalismo: il modello europeo<sup>(\*)</sup>

Andrea PATRONI GRIFFI\*

**Sommario:** 1. Il nuovo mondo dell'intelligenza artificiale: oltre "le due culture" 2. Le radici del modello europeo di regolazione dell'IA 3. Dal *corpus iuris* digitale all'AI Act: un costituzionalismo applicato 4. Gli Stati Uniti e l'ascesa del "parastato digitale" 5. Per una sovranità digitale europea: condizioni minime per una cornice condivisa

### 1. Il nuovo mondo dell'intelligenza artificiale: oltre "le due culture"

L'intelligenza artificiale può essere descritta come un nuovo mondo<sup>1</sup>, che mette alla prova le categorie giuridiche tradizionali e impone di ripensare confini, sovranità, responsabilità e garanzie. Le vecchie categorie non bastano più; le nuove non sono ancora scritte. È qui che il costituzionalismo è chiamato a misurarsi, anche a livello europeo, con la sfida di governare l'algoritmo senza erigere barriere anacronistiche all'innovazione, ma senza smarrire la bussola dei diritti fondamentali<sup>2</sup>.

La metafora del "nuovo mondo" coglie una trasformazione profonda dello spazio e delle coordinate entro cui il diritto opera, di fronte a una rivoluzione tecnologica che mette in discussione, in modo inedito, lo stesso rapporto tra l'essere umano e la macchina<sup>3</sup>. Nel "nuovo mondo" della società digitale le categorie tradizionali non vanno abbandonate, devono però essere messe alla prova, e talvolta ripensate, al fine di potersi orientare in una realtà diversa, nella quale emergono sfide nuove e si ridefiniscono i confini dell'esperienza giuridica<sup>4</sup>.

I "confini" dell'intelligenza artificiale sono, per l'appunto, quanto mai mobili. Talvolta sembrano annullarsi, perché l'azione algoritmica attraversa istantaneamente territori e ordinamenti. In realtà, più spesso, si spostano, nel senso che i luoghi decisivi non coincidono più con la sede del decisore, ma con

---

<sup>(\*)</sup> Il contributo riprende e sviluppa, con integrazioni e note, la relazione tenuta alla *Settimana della Scienza Italia-Cina*, Pechino, 13 novembre 2025

\* Professore ordinario di Diritto costituzionale e pubblico, Università di Napoli Federico II.

<sup>1</sup> Tra i primi a utilizzare in Italia l'espressione A. D'Aloia (cur.), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2021.

<sup>2</sup> Sul tema si segnala, di recente, nella letteratura sempre più ampia, F. Balaguer Callejón, *La costituzione dell'algoritmo*, Milano, 2023; H. W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021; G. Di Cosimo, *Processi democratici e tecnologie digitali*, Torino, 2023; F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Napoli, 2022; M. Proietti, A. Venanzoni, *La sovranità digitale tra sicurezza nazionale e ordine costituzionale*, Pisa, 2023 e, se si vuole, A. Patroni Griffi (cur.), *Bioetica, diritti e intelligenza artificiale*, Sesto San Giovanni, 2023.

<sup>3</sup> Di "machina sapiens" parla N. Cristianini, *Machina sapiens. L'algoritmo che ci ha rubato il segreto della conoscenza*, Bologna, 2024. Nella prospettiva della filosofia teoretica, da ultimo, si segnala E. Mazzarella, *Critica della ragione digitale*, Roma, 2026. Il dibattito, in realtà, è anche precedente all'avvento dell'intelligenza artificiale: J. Offray de La Mettrie, *L'uomo macchina*, trad. it. di F. Polidori, Sesto San Giovanni, 2015; H. Jonas, *Dalla fede antica all'uomo tecnologico*, Bologna, 2001; e, in ambito giuridico, V. Frosini, *Cibernetica, diritto e società*, Milano, 1968, ried. open access, Roma, 2023.

<sup>4</sup> Cfr., in particolare, F. Balaguer Callejón, *La costituzione dell'algoritmo*, cit.; C. Casonato, *Per un'intelligenza artificiale costituzionalmente orientata*, in A. D'Aloia (cur.), *Intelligenza artificiale e diritto*, cit.; G. Mobilio, *La coregolazione delle nuove tecnologie, tra rischi e tutela dei diritti fondamentali*, in *Osservatorio sulle fonti*, 1/2024.

l'architettura tecnica, con la filiera dei dati<sup>5</sup>, con l'infrastruttura che rende possibile la decisione. Sovente, infine, si sovrappongono, perché in un'unica operazione convivono più livelli: pubblico e privato<sup>6</sup>, nazionale e sovranazionale, mercato, che dovrebbe essere libero, e sovranità statale, libertà e controllo, doveri diritti<sup>7</sup>.

Le questioni sono enormi e complesse, ma è possibile ridurle almeno a due piani fondamentali.

Il primo è quello della responsabilità, anzi delle responsabilità, da declinare al plurale. Esse riguardano l'intera filiera: chi progetta e addestra i modelli, chi li integra, chi li alimenta di dati, e chi decide di impiegarli, e in che modo. La responsabilità, a ben vedere, resta umana e istituzionale, in quanto, per l'appunto, "si sceglie" di affidare la decisione all'algoritmo. La questione, allora, è rendere sempre giuridicamente leggibile questa catena (ma fino a che punto è possibile farlo?). Si tratta di definire doveri, controlli e imputazioni, e prevedere anche divieti quando risultino necessari. Sennonché quando l'esito nasce da sistemi complessi, l'opacità tecnica rischia di tradursi in opacità giuridica. E, in una democrazia costituzionale, l'opacità ha sempre un costo, in quanto rischia di indebolire le tutele a danno spesso dei soggetti più deboli ed esposti.

L'altro piano riguarda il confine tra pubblico e privato. Nel nuovo spazio digitale, alcuni attori privati esercitano, di fatto, funzioni che somigliano a quelle pubbliche, senza disporre della medesima legittimazione e senza essere sottoposti alle stesse forme di controllo e responsabilità. È una nuova edizione di un tema antico – il rapporto tra impresa e Stato – ma con manifestazioni del tutto inedite, perché passa attraverso infrastrutture informative e regole di accesso che riorganizzano la vita sociale e politica in tensione con la democrazia costituzionale<sup>8</sup>. Qui il costituzionalismo è chiamato a misurarsi anche con poteri privati capaci di incidere su libertà ed eguaglianza con un'intensità che, nel caso delle *big tech*, può perfino eccedere quella delle decisioni pubbliche assunte dagli Stati. Ecco perché l'IA non è solo una tecnologia o una nuova rivoluzione industriale. È un punto di pressione sul lessico fondamentale del diritto, soprattutto nella prospettiva della tradizione costituzionale europea del secondo dopoguerra.

Parlare di "nuovo mondo" significa, in definitiva, prendere sul serio le sfide poste dall'intelligenza artificiale: quali mappe servono, oggi, perché il diritto, le Costituzioni pluraliste continuino a svolgere la loro funzione di garanzia?

L'intelligenza artificiale non può essere ridotta a una mera *techné*, lasciata al solo dominio di scienziati, ricerca e imprese. Essa è ormai un *tòpos* politico e sociale: un "luogo" nel quale si ridisegnano i comportamenti umani, poteri e aspettative, e sul quale può prendere forma una società davvero nuova e non una versione semplicemente "aggiornata" delle precedenti.

*Ubi societas, ibi ius* afferma l'antico brocardo, che spesso viene ricordato anche nelle prime lezioni di diritto, ad indicare che il diritto origina dalla società e che con la società deve mantenere costante contatto: questo è ancor più vero in quella che viene denominata come società digitale<sup>9</sup>. Se anche in questa nuova società il diritto, inteso in senso oggettivo, deve essere funzionale soprattutto alla garanzia dei diritti in senso soggettivo, tale compito potrà essere davvero assolto, di fronte alle sfide dell'algoritmo, allargando il dialogo multidisciplinare tra i saperi e realizzando un'imprescindibile alleanza tra le due culture, umanistica e scientifica.

I dilemmi etici e le questioni giuridiche non possono essere affrontati restando prigionieri delle "due culture" di cui al libro di Snow del 1959<sup>10</sup>. Occorre superare steccati tra scienze e umanesimo, per evitare regole cieche o obsolete. Il giurista, come il filosofo, deve conoscere almeno l'essenziale della

<sup>5</sup> S. Calzolaio, *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, 1/2021.

<sup>6</sup> L. Torchia, *Poteri pubblici e poteri privati nel mondo digitale*, in *Il Mulino*, 1/2024; G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 4/2022.

<sup>7</sup> G. Pino, *Il costituzionalismo dei diritti. Struttura e limiti del costituzionalismo contemporaneo*, Bologna, 2017.

<sup>8</sup> Cfr. F. Balaguer Callejón, *Intelligenza artificiale e cultura costituzionale*, in *lceonline*, n. spec., 2/2023; A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Riv. di filosofia del diritto*, 1/2019.

<sup>9</sup> E. Di Carpegna Brivio, A. Sancino (cur.), *La democrazia della società digitale. Tensioni e opportunità*, Torino, 2023; E. Celeste, *Digital Constitutionalism. The Role of Internet Bills of Rights*, Abingdon-New York, 2022.

<sup>10</sup> C. P. Snow, *The Two Cultures and the Scientific Revolution*, Cambridge, 1959.

tecnologia che intende governare, altrimenti rischia di normare ciò che non comprende, cristallizzando in norma l'errore o l'irrilevanza.

## 2. Le radici del modello europeo di regolazione dell'IA

Se l'intelligenza artificiale è, come visto, un "nuovo mondo", risulta evidente come sia decisivo, sul piano normativo, individuare il luogo istituzionale in cui costruire regole comuni e, prima ancora, la grammatica valoriale e politica che quelle regole devono esprimere.

Oggi, per quanto auspicabile, un governo globale dell'IA appare ancora largamente utopico e supera l'oggetto di questo lavoro<sup>11</sup>. Sul piano sovranazionale europeo, invece, un modello regolativo è non solo necessario, ma già concretamente delineato in profili essenziali, come si vedrà.

L'Unione europea, infatti, non è soltanto un livello normativo "aggiuntivo" rispetto agli ordinamenti nazionali. È, invece, l'espressione giuridica di una società pluralista che, pur nella diversità delle identità nazionali, ha maturato una cultura comune e un metodo di integrazione<sup>12</sup>. È, perciò, il contesto più naturale per una disciplina dell'algoritmo che si traduca in *standard* condivisi e in garanzie effettive.

Le radici di questa scelta non sono contingenti. Esse affondano nella tradizione del costituzionalismo europeo del secondo dopoguerra e nella sua idea di fondo: la funzione primaria delle Costituzioni è limitare il potere, non solo quello pubblico ma anche quello privato, e assicurare che il mercato non degeneri in dominio oligopolistico e che i diritti, soprattutto dei più vulnerabili, restino concretamente garantiti<sup>13</sup>.

Nel tempo, la cultura comune dell'Unione si è condensata in un patrimonio di principi – dignità, libertà, eguaglianza, Stato di diritto – che orientano l'intera produzione normativa. La stessa centralità della persona, in una dimensione, al contempo, fisica e spirituale, viene intesa come nucleo non negoziabile della tradizione costituzionale europea e diventa ragione ultima per comprendere perché l'Unione non è restata silente di fronte alle sfide dell'intelligenza artificiale e ha provato a fondare uno spazio di "sovranità digitale europea"<sup>14</sup>. In questa prospettiva, l'IA non è un tema settoriale del mercato interno, ma una prova generale dell'identità europea. Diviene cartina al tornasole dell'integrazione, perché chiama in causa il modo in cui una comunità politica intende porsi di fronte a questa straordinaria sfida non meramente tecnologica. E l'integrazione diventa metodo di governo dei rischi globali senza arretrare sui valori comuni, a partire per l'appunto dalla centralità della persona.

Una tale impostazione emerge con particolare evidenza nell'AI Act, quando afferma, in modo esplicito, che il quadro normativo deve essere sviluppato in conformità ai valori dell'Unione e ai diritti fondamentali e che, come prerequisito, l'IA deve essere una "tecnologia antropocentrica". E aggiunge una proposizione densa, che si erge a criterio generale: l'IA "dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere umano" (*considerando n. 6*).

Il tema vero, dunque, non è quello di porre "barriere" alla tecnologia in sé, ma quello di evitare che l'innovazione produca diseguaglianze intollerabili, alimenti discriminazioni, svuoti gli spazi della privacy, e condizioni la formazione di un pensiero davvero libero e plurale, senza il quale non è possibile una democrazia *pluralista*<sup>15</sup>.

---

<sup>11</sup> Per un'analisi critica delle più rilevanti elaborazioni dottrinarie ascrivibili al c.d. costituzionalismo globale, cfr. O. Caramaschi, *Il costituzionalismo globale: teorie e prospettive*, Torino, 2022.

<sup>12</sup> A. Patroni Griffi (cur.), *E pluribus unum: le identità in Europa*, in *Diritto pubblico europeo rassegna online*, n. spec. 1/2024.

<sup>13</sup> Di recente, L. Di Majo, *La vulnerabilità degli utenti in rete*, in *BioLaw*, 1/2024 e i diversi contributi sulla "vulnerabilità tecnologica" in A. Patroni Griffi (cur.), *Vulnerabili. Questioni giuridiche, dilemmi bioetici*, Sesto San Giovanni, 2025, p. 591 ss.

<sup>14</sup> G. Tiberi, *L'irresistibile ascesa della sovranità digitale europea*, in G. Ferri (cur.), *Diritto costituzionale e nuove tecnologie*, Napoli, 2022.

<sup>15</sup> P. Dunn, *Intelligenza artificiale e democrazia: opportunità e rischi di disinformazione e discriminazione*, Milano, 2024; T. E. Frosini, *Liberté, égalité, Internet*, Napoli, 2015; M. Manetti, *Regolare Internet*, in *MediaLaws*, 2/2020, p. 35 ss.; M. C. Girardi, *Libertà e limiti della comunicazione nello spazio pubblico digitale*, in *Federalismi.it*, 17/2024; M. E. Bucalo, *La libertà di espressione in rete fra content moderation dei social network e regolazione dell'Unione europea*, in *Dirittifondamentali.it*, 3/2022.

Un tale irrinunciabile presupposto richiede un quadro di regole capace di fissare contorni e limiti, mediante bilanciamenti ragionevoli tra diritti e interessi contrapposti, tra politica e mercato, tra società civile e comunità<sup>16</sup>. Non si pone, dunque, a livello di Unione europea la questione dell'*an*, del se regolare, quanto quella del *quomodo*, del come regolare e con quali strumenti, nella consapevolezza che una regolazione, nel caso di una tecnologia così pervasiva, non è nemica dell'innovazione, ma in qualche modo condizione per preservare lo stesso modello liberale.

Certo, la regolazione deve essere insieme duttile e ferma. Duttile, perché la tecnica evolve e non si lascia irrigidire in schemi statici. Ferma, perché alcuni rischi non sono negoziabili quando incidono su dignità, libertà e uguaglianza. Questa idea – elasticità degli strumenti e rigidità dei principi – è la cifra di una razionalità intimamente costituzionale, che mira a governare l'algoritmo senza consegnarlo a mere logiche mercantili.

La dottrina più recente ha descritto questo passaggio come l'emersione di un vero costituzionalismo digitale<sup>17</sup>: un costituzionalismo chiamato a misurarsi non solo con il potere pubblico, ma anche con poteri privati, in grado di strutturare spazi di vita e infrastrutture decisive per la libertà.

In questa chiave, l'AI Act si colloca come punto di arrivo di una traiettoria europea che, già prima dell'IA, ha tentato di riportare il digitale entro il perimetro della responsabilità pubblica e tutela effettiva dei diritti.

Su queste basi si innesta, dunque, la scelta europea di un modello regolatorio specifico, che non è neutrale – né voleva esserlo – ma è coerente con questa storia e con questi valori.

### 3. Dal “corpus iuris digitale” all'AI Act: un costituzionalismo applicato

Il regolamento europeo sull'Intelligenza Artificiale (AI Act), approvato nel 2024<sup>18</sup>, non nasce nel vuoto; rappresenta, invece, la tappa più recente di una strategia regolatoria con cui l'Unione ha progressivamente ricondotto lo spazio digitale dentro un perimetro pubblico di garanzie. In un certo modo, esso rappresenta l'ultimo approdo di una traiettoria culturale e giuridica, affonda le sue radici più profonde non solo nella Carta dei diritti fondamentali dell'Unione europea ma, a ben vedere, direttamente nella tradizione del costituzionalismo europeo del secondo dopoguerra.

Viene qui, in qualche modo trasposta nel digitale, la funzione tipica delle democrazie costituzionali: limitare il potere e rendere effettiva la tutela dei diritti, anche quando il potere è esercitato da attori privati e in forme opache. È questo il senso, già “costituzionale”, del *corpus iuris* europeo del digitale, volendosi evitare che il mercato degeneri in dominio oligopolistico e assicurare che diritti e libertà, soprattutto dei più vulnerabili, restino concretamente garantiti.

L'AI Act costruisce un quadro armonizzato europeo per l'IA, con una dichiarata proiezione su diritti fondamentali, democrazia e Stato di diritto, che si comprende bene solo se lo si colloca accanto a una più ampia regolazione europea, che vive in alcuni atti fondamentali, che hanno progressivamente “costituzionalizzato”, se è possibile dire così, lo spazio tecnologico.

Il GDPR, *General Data Protection Regulation*, “costituzionalizza” a livello europeo la protezione dati come architrave della tutela della persona<sup>19</sup>. Il DSA, il *Digital Services Act*, sposta l'asse dalla

<sup>16</sup> Per una posizione interessante sul tema, v. G. De Minico, *Libertà virtuali. Costituzione e mercato*, Torino, 2024.

<sup>17</sup> O. Pollicino, *Costituzionalismo digitale. Pensare la democrazia al tempo dell'IA*, Bologna, 2025.

<sup>18</sup> Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Tra i commenti all'AI Act, v. M. Finck, *The EU Artificial Intelligence Act: A Commentary*, Oxford, 2025; L. C. Hueso, D. U. Galetta (eds.), *The European Union Artificial Intelligence Act. A Systematic Commentary*, Napoli, 2025; A. F. Uricchio, C. Calderola, *L'intelligenza artificiale tra regolazione e esperienze applicative. AI Act (regolamento UE) e disegno di legge governativo*, Bari, 2025.

<sup>19</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

mera responsabilità *post-illecito* a obblighi procedurali *ex ante* (trasparenza, reclami, accesso ai dati per ricerca), riaffermando un controllo pubblico su condizioni private di servizio<sup>20</sup>. Il DMA, il *Digital Markets Act* sui mercati equi e contendibili nel settore digitale, pone obblighi *ex ante* per i *gatekeeper*, come interoperabilità, portabilità, divieti di *self-preferencing* e interviene sull'architettura stessa del mercato nel quale le libertà digitali si esercitano<sup>21</sup>.

In questo quadro si collocano, inoltre, gli atti europei “dei dati”<sup>22</sup> e, sul versante democratico, il Regolamento sulla trasparenza e il targeting della pubblicità politica<sup>23</sup>, che assume la manipolazione informativa come rischio sistemico per l'integrità del confronto pubblico.

È in questa cornice complessiva che l'Unione può rivendicare di non abdicare allo spazio regolatorio pubblico, promuovendo condizioni effettive di esercizio dei diritti anche nella società digitale.

Il cuore tecnico-giuridico dell'AI Act è l'approccio *risk-based*<sup>24</sup>, che non è un mero esercizio classificatorio, ma una scelta di razionalità normativa che, nel linguaggio costituzionale, richiama principi come proporzionalità e ragionevolezza. Più alto è il rischio per i diritti e democrazia, più intensi devono essere vincoli e controlli.

In tal senso, l'AI Act, più che inaugurare un “costituzionalismo digitale” come forma altra, rappresenta un costituzionalismo applicato al digitale, che invero non esprime lo stesso concetto. Esso individua, nello specifico dell'AI Act, pratiche vietate, prevede una disciplina stringente per i sistemi ad alto rischio e introduce obblighi specifici per i modelli di IA per finalità generali, con particolare attenzione ai rischi sistemici.

Il primo livello è quello, ai sensi dell'articolo 5, delle pratiche vietate, a rischio inaccettabile. Qui l'approccio interdittivo è coerente con la protezione della dignità e dell'autodeterminazione della persona. Sono vietate pratiche che manipolano in modo occulto, che sfruttano vulnerabilità o che configurano forme di controllo incompatibili con la libertà personale.

In questo contesto va collocato il tema del *social scoring*. Nel testo dell'AI Act il divieto non colpisce una generica valutazione settoriale – ad esempio, creditizia – in quanto tale; riguarda, invece, sistemi che valutano o classificano persone sulla base del comportamento sociale o di caratteristiche personali che, in forza del “punteggio”, determinano trattamenti pregiudizievoli in contesti non correlati, oppure ingiustificati o sproporzionati. È un punto da formulare con precisione, per non confondere le pratiche vietate con applicazioni che, semmai, ricadono nell'alto rischio e richiedono presidi rafforzati.

Il secondo livello è quello dei sistemi ad alto rischio, ammessi ma solo dietro l'individuazione di attenta disciplina, che riguarda gestione del rischio, requisiti su dati e qualità, documentazione e tracciabilità, trasparenza verso gli utenti e soprattutto supervisione umana significativa. Qui si vede la traduzione normativa di un punto significativo per il costituzionalismo: l'automazione non può diventare un modo per dissolvere responsabilità e legalità. Anche quando la decisione “emerge” da un modello complesso, la responsabilità resta umana e istituzionale, e deve restare giuridicamente esigibile lungo l'intera filiera<sup>25</sup>.

---

<sup>20</sup> 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).

<sup>21</sup> 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).

<sup>22</sup> Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati) (Testo rilevante ai fini del SEE) e Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

<sup>23</sup> Regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al targeting della pubblicità politica.

<sup>24</sup> Per un'analisi sistematica, articolo per articolo, sulla regolazione in base al rischio, nella sterminata letteratura, v., ad esempio, L. C. Hueso, D. U. Galetta (eds.), *The European Union Artificial Intelligence Act*, cit., p. 181 ss.; v. anche P. Dunn, G. De Gregorio, *AI Act, rischio e costituzionalismo digitale*, in *MediaLaws*, 22 aprile 2022; O. Pollicino, F. Paolucci, *AI Act e diritti fondamentali*, in *Civiltà delle macchine*, 2/2024.

<sup>25</sup> In ciascuna fase della stessa: progettazione, addestramento, integrazione, uso.

Il terzo livello riguarda i modelli di IA per finalità generali, spesso generativi, con possibili rischi sistemici, quali disinformazione, discriminazione, manipolazione etc. In questo ambito l'AI Act affida un ruolo importante a obblighi di trasparenza, di valutazione e di mitigazione dei rischi. La disciplina è affiancata da strumenti di coregolazione, in primo luogo i codici di pratica (CoP - Codes of Practice), sotto il coordinamento dell'AI Office (*Ufficio europeo per l'IA*), quale snodo centrale della governance e, in particolare, del coordinamento degli strumenti attuativi relativi ai modelli GPAI<sup>26</sup>.

Rispetto a una tale scala *risk based*, è bene ricordare che il rischio è una categoria per sua natura aperta e dinamica. Proprio per questo, la sua traduzione in pratiche amministrative, standard tecnici e codici di condotta richiede cautela. Concetti decisivi non possono essere assorbiti in un linguaggio esclusivamente tecnico, fino a perdere il loro contenuto sostanziale di garanzia dei diritti. In questa prospettiva si comprende anche il richiamo precedente al superamento delle “due culture”: l'attuazione di un modello basato sul rischio esige competenze miste e, soprattutto, un controllo pubblico effettivo sulle scelte che determinano, in concreto, il livello di tutela.

In quest'ottica, il principio di trasparenza assume la funzione di un vero presidio di “*due process*” nella società algoritmica. Al riguardo è stato sottolineato come il “principio di comprensibilità della tecnologia” è in qualche modo funzionale al “nuovo personalismo tecnologico”<sup>27</sup>. La straordinaria capacità “profilante” dell'IA che non pone etichette sulle cose, ma sulle persone, espone a rischi di discriminazioni sanitarie, sociali e culturali. Senza trasparenza e contestabilità, l'opacità tecnica rischia di diventare opacità giuridica. E l'opacità in una democrazia costituzionale colpisce soprattutto i soggetti più esposti.

La regolazione dei *deepfake*, in tal senso, è emblematica. L'AI Act impone obblighi di etichettatura e informazione, ma la dottrina segnala la tensione intrinseca tra l'obbligo di “dirsi *deepfake*” e la finalità tipica di chi intende ingannare<sup>28</sup>. Proprio per questo la trasparenza, da sola, non basta: deve innestarsi in filiere di responsabilità e in poteri pubblici effettivi di vigilanza e sanzione. Tutto ciò ad evitare che i modelli generativi diventino “macchine di influenza incontrollata”. È un approccio che, si vedrà, segna un punto di differenza, abbastanza netto, dal modello statunitense, dove queste misure sono invece, come noto, perlopiù volontarie.

La costruzione europea di garanzie non avviene, quindi, solo per divieti, ma soprattutto attraverso un “*data due process*”, cioè un insieme di obblighi procedurali che rendono verificabile il potere digitale e ne impediscono l'esercizio arbitrario. È la logica che attraversa GDPR, DSA, DMA e, con modalità proprie, l'AI Act. Ciò dovrebbe aiutare a “limitare”, se vogliamo dire così, i colossi del digitale non soltanto con enunciazioni valoriali, ma con procedimenti, accessi ai dati, auditing, trasparenze, reclami.

La credibilità del modello europeo cerca di passare anche per l'enforcement. L'AI Act prevede un regime sanzionatorio dissuasivo: per la violazione dei divieti (art. 5), sanzioni amministrative fino a 35 milioni di euro o al 7% del fatturato mondiale annuo; fino a 15 milioni o al 3% per altre violazioni rilevanti; e sanzioni ulteriori per informazioni inesatte o fuorvianti.

Il collegamento con il restante *corpus digitale* è evidente. Il DSA consente sanzioni fino al 6% del fatturato mondiale e il DMA fino al 10% (20% in caso di recidiva), con anche pagamenti periodici per imporre il rispetto degli obblighi. È una scelta che rende concreta l'idea di una regolazione ex ante e non meramente simbolica.

<sup>26</sup> Sui diversi strumenti normativi di cui all'AI Act, cfr. G. De Minico, *Le fonti del diritto: un'argine all'intelligenza artificiale*, in *Riv. AIC*, 3/2025.

<sup>27</sup> A. Simoncini, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, n. 2/2023. Sul punto fondamentale fu Consiglio di Stato, sez. VI, sent. 8 aprile 2019, n. 2270: “il meccanismo attraverso il quale si concretizza la decisione robotizzata (ovvero l'algoritmo) deve essere “conoscibile”, secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico”. E, ancora: “Tale conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti. Ciò al fine di poter verificare che gli esiti del procedimento robotizzato siano conformi alle prescrizioni e alle finalità stabilite dalla legge o dalla stessa amministrazione a monte di tale procedimento e affinché siano chiare – e conseguentemente sindacabili – le modalità e le regole in base alle quali esso è stato impostato”.

<sup>28</sup> M. E. Bucalo, *Intelligenza artificiale e deepfakes: le nuove frontiere della disinformazione e i possibili rimedi giuridici*, in *MediaLaws*, 2024.

Sul piano interno, piace, infine, accennare alla legge italiana 23 settembre 2025, n. 132, che si inserisce come legge di principi e deleghe, di raccordo nazionale e di declinazione settoriale, in coerenza dichiarata con l'impianto europeo<sup>29</sup>.

#### 4. Gli Stati Uniti e l'ascesa del "parastato digitale"

Sul versante opposto al *corpus*, europeo e nazionale degli Stati membri dell'Unione, gli Stati Uniti non appaiono avere ad oggi un *corpus* federale organico paragonabile all'AI Act<sup>30</sup>.

La governance dell'IA è più frammentata e flessibile. Ci si affida a interventi settoriali, all'azione delle agenzie sulla base di leggi esistenti, e a strumenti volontari. Il NIST AI Risk Management Framework, ad esempio, è esplicitamente pensato per uso volontario<sup>31</sup>.

L'orientamento statunitense è quello sostanzialmente di favorire la *leadership* tecnologica, di ridurre vincoli regolatori e di affidare gran parte della *governance* all'autoregolazione delle imprese e a linee guida settoriali a realizzare una sorta di eteronomia tecnologica, confermando un'impostazione meno incline a un vincolo generale *ex ante*.

La radice profonda di questo divario è culturale e costituzionale. La centralità del Primo Emendamento e di un assoluto *freedom of speech*, la metafora del *free marketplace of ideas* hanno storicamente orientato la regolazione del digitale, con una diffidenza strutturale verso interventi pubblici che possano essere letti come limitazione della libertà di espressione.

Il fatto è che l'emersione di poteri privati smisurati, spesso riconducibili anche a singole persone fisiche, sposta l'ago della sovranità e rende la politica "soccumbente". La rete, da promessa libertaria, si è trasformata infatti in un ambiente dominato da pochi attori capaci di influenzare mercato, dibattito democratico e tutela dei diritti. Non si tratta più di meri operatori economici. Sono emersi dei veri e propri poteri digitali che esercitano funzioni quasi parastatali, in concorrenza con le autorità pubbliche<sup>32</sup>.

La concentrazione di potere nelle mani di poche persone finisce per incidere sul baricentro stesso della sovranità. Ne deriva il rischio strutturale che la politica arretri, mentre piattaforme e infrastrutture digitali esercitano, di fatto, funzioni di regolazione e indirizzo con effetti pubblicistici, senza corrispondente legittimazione democratica e senza adeguate forme di responsabilità. In una democrazia pluralista, questo slittamento non può e non deve essere considerato come un esito "neutro" del progresso tecnologico. Di questo l'Unione europea mostra consapevolezza, molto più degli USA.

L'osservatorio tecnologico-digitale mostra una territorialità nuova, immateriale e reticolare. È un territorio "senza confini" in cui dati, piattaforme e reti sociali generano spazi di influenza che attraversano ordinamenti, e nei quali si ripropongono, in forma inedita, categorie classiche come sovranità e giurisdizione.

Se il diritto pubblico arretra, la sovranità digitale viene ad essere esercitata, di fatto, da soggetti privati come potere sostanzialmente assoluto.

Per questo la questione della "giurisdizione sui dati" e della territorialità normativa nel *cloud* e nell'IA deve essere ricostruita come rivendicazione della competenza pubblica indipendentemente dall'allocazione fisica dei dati o dalla sede delle big tech: altrimenti il digitale rischia di riportarci, paradossalmente, a forme precostituzionali di potere.

---

<sup>29</sup> F. Paolucci, *La legge italiana sull'intelligenza artificiale: attuazione nazionale dell'AI Act e primi nodi applicativi*, in *Quaderni costituzionali*, 4/2025.

<sup>30</sup> Per un'analisi sistematica, molto completa, da ultimo, M. Hu, *AI Law and Policy*, New York, 2025. Per una comparazione USA-UE, O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete*, in *Rivista AIC*, 2/2025.

<sup>31</sup> Su cui, F. K. Cameron, *NIST's AI Risk Management Framework plants a flag in the AI debate*, in *Brookings*, 2023.

<sup>32</sup> Sui pericoli del capitalismo ai tempi delle big tech, sempre fondamentale, S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019. Di "Stati privati" e "capitalismo delle piattaforme" parla A. Venanzoni, *Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*, in *MediaLaws*, 3/2020; Id., *Cyber-costituzionalismo: la società digitale tra silicolonizzazione, capitalismo delle piattaforme e reazioni costituzionali*, in *Rivista italiana di informatica e diritto*, 1/2020.

In controtelaio si comprende anche una possibile ragione del diverso atteggiamento statunitense, che non ha adottato, almeno finora, una cornice federale organica e vincolante sull'IA. Questo orientamento non è soltanto espressione di una tradizione giuridica più diffidente verso l'intervento pubblico; può apparire anche come una scelta di opportunità strategica, volta a preservare la *leadership* tecnologica e la competitività delle grandi piattaforme. In tale scenario, la linea di confine tra interesse pubblico e interesse privato tende incredibilmente ad assottigliarsi, quasi ad annullarsi.

In alcune fasi – e ciò in verità appare particolarmente evidente nell'orizzonte dell'amministrazione Trump – si è rafforzata una convergenza tra priorità governative e priorità delle *big tech*<sup>33</sup>. Deregolazione, riduzione dei vincoli, fiducia nella *governance* di mercato e negli standard volontari diventano espressione prepotente di fortissimi interessi privati, piuttosto che configurarsi come mera conseguenza della diversa cultura giuridica d'oltreoceano. Ne risulta un modello nel quale il potere privato può espandersi in un ambito scarsamente vincolato, mentre la risposta pubblica si concentra più su incentivi, partnership e strumenti flessibili ed evita sistematicamente obblighi *ex ante* e sanzioni strutturali.

La risposta europea a questa sfida non può che essere profondamente diversa. E passa, come visto, attraverso un organico apparato normativo regolatorio su cui si cerca di innestarsi, a garantire effettività, la stessa giurisprudenza eurounitaria.

La nota sequenza Digital Rights Ireland, Google Spain, Schrems I e Schrems II è decisiva perché consolida la Carta dei diritti come parametro di controllo e costruisce una chiara forma di "giurisdizione sui flussi"<sup>34</sup>. Nel digitale non si giudica la tecnologia in astratto, ma si valutano gli ecosistemi giuridici che accolgono i dati e rendono possibile l'esercizio del potere. In Google Spain, in particolare, la Corte applica in modo incisivo i diritti fondamentali anche verso soggetti privati, mostrando come la tutela dei diritti, nello spazio digitale, assuma inevitabilmente anche una dimensione "orizzontale". Resta tuttavia essenziale calibrare con equilibrio strumenti sostanziali e procedurali, evitando sia l'inerzia sia l'ipertrofia normativa.

Il rischio che poteri privati si autoproclamino "sovrani" della rete è reale e, in una prospettiva europea, non può che essere respinto. La sovranità digitale dell'Unione tende infatti a configurarsi come una giurisdizione sui flussi, non priva di confini, ma capace di far valere i propri valori anche oltre la mera territorialità fisica, ricostruendo una territorialità normativa indipendente dall'allocatione dei dati e dalla sede delle big tech.

In questo senso, il cuore del modello europeo è la costruzione di un'architettura regolatoria di razionalità intimamente costituzionale, fondata sulla consapevolezza che l'IA, se abbandonata a logiche esclusivamente mercantili, può erodere trasparenza, non discriminazione, pluralismo informativo e, in definitiva, la libertà di autodeterminazione della persona, che è presupposto essenziale della democrazia pluralista.

## 5. Per una sovranità digitale europea: condizioni minime per una cornice condivisa

In definitiva, la questione non è soltanto *che cosa* regolare, ma come rendere effettiva la scelta regolatoria, la capacità di trasformare il disegno normativo in garanzie effettive. L'AI Act, insieme al più ampio *corpus* europeo sul digitale, ha introdotto una disciplina importante, che si basa, come visto, su responsabilità, trasparenza e anche controllo, ma la verifica decisiva si gioca sul piano dell'attuazione e dell'effettività, e quindi anche su standard tecnici coerenti con i principi, misure concrete di audit e di controllo, coordinamento tra autorità, e un *enforcement* che sia chiaro e realmente dissuasivo.

<sup>33</sup> Basterebbe citare Executive Order n. 14179, del 23 gennaio 2025, "Removing Barriers to American Leadership in Artificial Intelligence", in *The White House*, 23 gennaio 2025.

<sup>34</sup> G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Il diritto dell'informazione e dell'informatica*, 4(5)/2015, p. 779 ss.

Senza questa dimensione operativa, la regolazione rischia di rimanere un discorso alto, ma privo di presa sulla realtà, soprattutto in un contesto nel quale la velocità dell'innovazione e la concentrazione del potere tecnologico privato tendono a precedere l'intervento pubblico.

Non basta disporre di buone regole se, nei casi più delicati, prevalgono inerzie. La tutela dei diritti non può nemmeno scaricarsi interamente sul contenzioso giudiziario e quindi al momento patologico della violazione delle regole. È necessaria, invece, una capacità pubblica stabile di intervento, che renda la garanzia dei diritti tempestiva, verificabile e non meramente eventuale.

In conclusione, ciò che spesso viene definito "effetto Bruxelles"<sup>35</sup> può essere letto, come una forma di sovranità normativa che l'Unione cerca di perseguire in campo digitale attraverso la via regolatoria. Una "sovranità" che, per struttura del mercato e per forza di attrazione dello spazio europeo, possiede una naturale vocazione extraterritoriale. La regola europea tende, infatti, a proiettarsi oltre confine, perché condiziona, di fatto, l'accesso a uno spazio economico e sociale di "appetite" dimensioni globali.

Sarebbe però riduttivo identificare la "sovranità digitale" soltanto con la capacità di produrre norme.

Il primo strumento di una reale "sovranità digitale" si dovrebbe porre, indipendentemente dal piano regolatorio, su piano di una capacità di autonomia strategica nel settore. Cioè, la predisposizione di condizioni politiche ed economiche, di competenze, di infrastrutture in senso lato, che consentano alle imprese europee di essere protagoniste nella competizione sull'intelligenza artificiale, dalla quale dipendono non solo quote di mercato, ma anche posizionamento geopolitico e capacità di indirizzo tecnologico.

Oltre il piano strettamente regolatorio, dove l'Unione, come visto, si è mossa con tempestività e coerenza rispetto alla propria tradizione valoriale, occorre, soprattutto, non sottovalutare che disciplinare un mercato digitale, dominato da grandi piattaforme non europee, significa affrontare una vera prova politica.

Le frizioni transatlantiche sulle regole digitali e le prime applicazioni incisive degli strumenti europei mostrano che la norma, da sola, non basta. Essa presuppone istituzioni solide e, in ultima analisi, una capacità di tenuta politica nella "sfida globale" con potenze economiche e tecnologiche come Stati Uniti e Cina<sup>36</sup>. In assenza di tale sostegno, la sovranità regolatoria rischia di restare forte nei testi, ma fragile negli effetti.

Proprio per questo, se l'Unione vuole restare fedele alla propria anima costituzionale, deve rafforzare la propria integrazione politica, così da sostenere con effettività, anche sul piano esterno, l'impianto di trasparenza, responsabilità e tutela dei diritti che ha scelto per governare il mercato digitale.

Vi è spazio per semplificazioni tecnico-normative, oggi da più parti richieste, quando siano davvero utili. Ma senza retrocedere sui presidi necessari a rendere l'algoritmo, e il potere delle grandi piattaforme, compatibile con diritti e democrazia.

In questo quadro, la vocazione europea non è costruire una "fortezza" normativa, ma proporre un metodo, dove i diritti siano la bussola e il rischio il criterio operativo, con istituzioni capaci di garantire effettività. È così che l'Europa può aspirare a essere ponte tra paradigmi differenti, come quello cinese e statunitense, non per neutralità, ma perché capace di trasformare i propri valori in regole e regole in strumenti di controllo che funzionano.

Se questa è la posta in gioco, i modelli posti in Cina e USA, con semplificazione estrema e come tale parziale, sono chiari. Da un lato, un controllo pubblico pervasivo che può degenerare in regressione autoritaria; dall'altro, un *laissez-faire* che, dietro la retorica dell'innovazione, rischia di "chiudere" la sfera digitale a oligopoli privati e a una eteronomia tecnologica difficilmente reversibile.

In ultima analisi, il confronto tra modelli mette in luce una distanza non solo regolatoria, ma anche culturale tra l'approccio europeo e quello statunitense; e, al tempo stesso, rende evidente la necessità di costruire un ponte.

---

<sup>35</sup> A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020.

<sup>36</sup> S. Aceto di Capriglia, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e cinese. Uno studio comparato*, in *Federalismi.it*, 9/2024.

La sfida è planetaria: Europa, Stati Uniti e Cina incarnano tre paradigmi che non possono limitarsi a competere, ma devono aprire canali di dialogo politico, economico e culturale, evitando logiche di contrapposizione fondate sulla forza. L'alternativa, peraltro, è la frammentazione normativa, che si traduce in un rischio sistemico. In assenza di standard almeno parzialmente interoperabili, l'IA diventa un moltiplicatore di asimmetrie e un terreno di conflitto economico destinato a riflettersi sul piano politico. Per questo occorre un dialogo capace di fissare un nucleo minimo di principi comuni: sicurezza, responsabilità, divieto delle pratiche manifestamente lesive dei diritti fondamentali, pur nel rispetto dei diversi contesti, e trasparenza dei modelli generativi nei contesti più sensibili.

La prospettiva europea, in definitiva, nei limiti di forza del vecchio continente, riesce a indicare le linee di un percorso chiaro: disciplinare l'algoritmo senza demonizzarlo né arretrare rispetto alla responsabilità pubblica; promuovere l'innovazione in forme pienamente compatibili con le libertà fondamentali, l'eguaglianza e la democrazia; creare, con realismo, le condizioni essenziali di una governance multilaterale capace di assicurare che l'intelligenza artificiale rimanga uno strumento di progresso umano, e non un moltiplicatore di conflitti e disuguaglianze.

---

## Abstract

*L'intelligenza artificiale costituisce una sfida alle categorie giuridiche tradizionali anche nella prospettiva del costituzionalismo europeo. In tale ambito, l'Unione europea ha progressivamente definito un modello regolatorio che, pur non esente da rigidità e da margini di semplificazione, resta ancorato alla centralità della persona e alla tutela dei diritti. Muovendo dal più ampio corpus iuris europeo del digitale, sino all'AI Act, viene ricostruito un itinerario normativo nel quale l'approccio risk-based assume il significato di una forma di "costituzionalismo applicato al digitale". Il modello europeo viene messo a confronto con l'approccio prevalente negli Stati Uniti, caratterizzato da una regolazione assente o frammentata, orientata al mercato e alla salvaguardia di veri e propri parastati digitali privati. La specificità europea consiste, al riguardo, non solo nell'approccio regolatorio, ma anche nel tentativo di sottoporre i poteri tecnologici a una grammatica pubblicistica fatta di controlli e garanzie. Pur tra difficoltà e pressioni derivanti dalla competizione globale, il modello europeo viene in rilievo come possibile criterio ordinante per la conciliazione tra innovazione, diritti fondamentali e garanzie democratiche, nonché come base per l'elaborazione di principi minimi condivisi nella nascente governance globale dell'intelligenza artificiale.*

**Parole chiave:** AI Act; costituzionalismo digitale; sovranità digitale europea; diritti fondamentali; regolazione dell'intelligenza artificiale

\*

*Artificial intelligence constitutes a challenge to traditional legal categories, including from the perspective of European constitutionalism. Within this framework, the European Union has progressively developed a regulatory model which, although not exempt from rigidities and still marked by margins for simplification, remains anchored in the centrality of the person and in the protection of rights. Moving from the broader European corpus iuris of the digital sphere to the AI Act, the article reconstructs a regulatory trajectory in which the risk-based approach acquires the meaning of a form of "constitutionalism applied to the digital domain". The European model is then compared with the prevailing approach in the United States, characterised by absent or fragmented regulation, market-oriented logic, and the safeguarding of veritable private digital quasi-states. In this respect, the specificity of the European model lies not only in its regulatory approach, but also in its attempt to subject technological powers to a public-law grammar shaped by controls and guarantees. Despite the difficulties and the pressures arising from global competition, the European model emerges as a possible ordering criterion for reconciling innovation, fundamental rights, and democratic guarantees, as well as a basis for the elaboration of shared minimum principles within the emerging global governance of artificial intelligence.*

**Key words:** AI Act; digital constitutionalism; European digital sovereignty; fundamental rights; regulation of artificial intelligence