LUISS

Corso di laurea in Giurisprudenza

Cattedra di Diritto Amministrativo

La regolazione dell'intelligenza artificiale nel quadro normativo nazionale ed europeo

Prof. Aristide Police

RELATORE

Prof.ssa Silvia De Nitto

CORRELATORE

Alessandro De Mascellis
Matr. 161913

CANDIDATO

Anno Accademico 2023/2024

Indice

INTRODUZIONE

Con l'avvento dell'Era digitale, spinta dall'Intelligenza Artificiale (IA) e dall'Internet delle Cose ("*Internet of Things*") quali tecnologie trainanti, il rapporto tra Stato e tecnologia è mutato profondamente: per la prima volta le tecnologie non rappresentano solo l'oggetto della regolazione, ma una componente essenziale del funzionamento stesso dello Stato. Nello Stato digitale, le funzioni pubbliche si trasformano, i servizi (dalla sicurezza alla giustizia) si dematerializzano e le regole che legittimano il potere vengono riscritte.

In questo contesto di profondi mutamenti, l'IA si distingue come il paradigma emergente dell'Era digitale, sollecitando la riflessione giuridica circa l'opportunità e le modalità di una sua regolamentazione. Regolare l'IA si rivela però un compito arduo, tanto sul piano tecnico quanto su quello propriamente giuridico.

In primo luogo, il fenomeno presenta contorni sfumati: la prima difficoltà che incontra il giurista è proprio definire cosa sia l'"intelligenza artificiale", identificare l'oggetto della regolazione. Il campo coinvolge una molteplicità di prospettive scientifiche – dall'informatica alla matematica, dalla linguistica alle scienze cognitive e persino alla filosofia – riflettendo la natura multidisciplinare dell'IA. Ne consegue che qualsivoglia tentativo di inquadramento normativo debba necessariamente interagire con il sapere specialistico *extra*-giuridico, di natura eminentemente tecnica. Ne deriva un oggetto regolatorio sfuggente, un "bersaglio mobile" in continua evoluzione,[1] che rende arduo stabilire regole chiare e *future-proof*, a "prova di futuro".

In secondo luogo, le caratteristiche proprie dei sistemi di IA pongono sfide inedite al regolatore. Gli algoritmi di apprendimento automatico introducono elementi di complessità tali da mettere in crisi gli schemi normativi tradizionali. Si pensi alla natura *general-purpose* di gran parte dei moderni sistemi di IA, capaci di adattarsi a contesti applicativi eterogenei: le medesime architetture algoritmiche possono essere impiegate in settori disparati, con impatti variabili sui diritti fondamentali degli individui. Si consideri

[1] *Cfr.* Andrea Bertolini, *Intelligenza artificiale e responsabilità civile: Problema, sistema, funzioni* (Bologna: Il Mulino, 2025).

altresì la natura *data-driven* dell'IA: l'ingente volume di *Big Data* necessario per l'addestramento dei modelli algoritmici solleva questioni attinenti alla tutela dei dati personali e della *privacy* e si pone in tensione con i principi sanciti dal GDPR. La regolazione dell'IA interroga molteplici aree del diritto, *inter alia*: la tutela dei dati personali, la disciplina della responsabilità civile e penale, la tutela della proprietà intellettuale.

Di fronte a tale complessità, qualsiasi analisi giuridica del fenomeno non può che partire dalla definizione del taglio metodologico adottato e del perimetro dell'analisi stessa. Questa tesi adotta, per quanto possibile, un approccio multidisciplinare, situando la regolazione dell'IA all'interno dell'evoluzione dello Stato regolatore. Il lavoro guarda quindi al diritto pubblico e al diritto amministrativo, dedicando i primi due capitoli all'analisi giuridico-sociologica dello Stato digitale e dello Stato regolatore, nonché alla funzione della regolazione in generale; gli ultimi due capitoli all'analisi della normativa vigente, nonché della definizione dell'architettura di *governance* dell'IA a livello nazionale ed europeo.[2] Esulano dall'ambito di questa trattazione riflessioni sull'impatto dell'intelligenza artificiale sulla disciplina della responsabilità civile e penale, sulla tutela del diritto d'autore, sulla protezione dei dati personali e sui rapporti tra AI Act e GDPR, sebbene siano presenti numerosi rimandi e digressioni nel corso del lavoro dedicate al tema dei dati.

Sul piano strutturale, la tesi si articola quindi in quattro capitoli, seguendo un percorso argomentativo che, muovendo da alcune premesse concettuali, conduce all'analisi della normativa nazionale ed europea in materia di intelligenza artificiale.

Il primo capitolo è dedicato al nuovo paradigma dello Stato digitale e fornisce alcune nozioni tecniche di base sull'IA. Si esamina come la rivoluzione digitale abbia inciso sulle funzioni statali e sull'ordinamento e si affronta la "questione definitoria" legata alla nozione di "intelligenza artificiale", illustrandone l'evoluzione storica e le diverse definizioni offerte dalla letteratura scientifica.

Il secondo capitolo concentra l'attenzione sulle *rationes*, gli obiettivi e le strategie che sottendono la regolazione dell'IA, con particolare riferimento all'approccio seguito

[2] Sebbene non venga sviluppata un'analisi dettagliata delle procedure di *enforcement* delineate dall'AI Act, pure rilevanti. La trattazione si concentra esclusivamente sull'architettura istituzionale di *governance*.

in ambito europeo. Viene pertanto affrontato il tema della "corsa alla regolazione" in atto negli ultimi anni, motivata, da un lato, dall'urgenza di governare i rischi intrinseci all'IA – *bias* algoritmici, opacità decisionale e impatti sociali– e, dall'altro, dalla volontà dell'Unione Europea di mantenere il suo ruolo di "regolatore globale egemone". In questo contesto, si procede a una ricognizione degli strumenti regolatori a disposizione, distinguendo tra strumenti di *hard* e *soft law*. Viene poi approfondito il costrutto teorico della regolazione "cibernetica" e l'idea di un *regulatory mix* che, integrando differenti modalità di intervento – diritto positivo, dinamiche di mercato, norme sociali e architetture tecnologiche – consenta di governare l'IA nell'ecosistema digitale. Il capitolo analizza il quadro normativo europeo in materia digitale nel quale si inserisce l'AI Act, ripercorrendo l'*iter* che dalla Proposta di regolamento della Commissione Europea nel 2021 ha condotto all'approvazione del Regolamento sull'intelligenza artificiale nel 2023, e mettendo in luce i punti salienti del dibattito che ha accompagnato l'adozione di questa legislazione pionieristica.

Il terzo capitolo è dedicato all'analisi dell'AI Act, attraverso la lente del modello europeo di regolazione del rischio digitale. Si illustrano l'ambito di applicazione del Regolamento e il suo carattere orizzontale, per poi approfondire il *risk-based approach* seguito dal legislatore europeo: i sistemi di IA sono classificati in categorie di rischio (inaccettabile, alto, limitato, minimo), cui si collegano diversi e gradati obblighi e divieti. In particolare, il capitolo esamina le pratiche vietate, i requisiti imposti ai sistemi ad alto rischio, le misure di trasparenza previste per taluni sistemi di IA e la disciplina speciale prevista per i sistemi di IA "per finalità generali".

Il quarto e ultimo capitolo è dedicato alla *governance* dell'intelligenza artificiale. Si procede a esaminare l'architettura istituzionale di *governance* come delineata dall'AI Act, articolata su una duplice dimensione, sovranazionale e nazionale. S'intravede quindi, sullo sfondo, un tema di fondamentale importanza: il modo in cui il quadro di *governance* introdotto dall'AI Act si integrerà e si coordinerà con la pletora di autorità amministrative indipendenti già esistenti a livello nazionale, istituzionalmente preposte alla vigilanza dei mercati e alla tutela dei diritti fondamentali, tra cui, *in primis*, il Garante per la protezione dei dati personali. Al fine di conferire concretezza all'analisi, si propone quindi l'analisi di un caso di studio: nelle more dell'entrata in vigore dell'AI Act, si sono registrati in Italia interventi puntuali da parte del Garante su taluni sistemi di IA generativa. Nello

specifico, i provvedimenti adottati nei confronti del *chatbot* ChatGPT costituiscono un utile *case study* per approfondire la portata e i limiti di tali interventi, e per derivare preziose indicazioni circa il ruolo che le autorità nazionali saranno chiamate a svolgere nell'*enforcement* del Regolamento europeo. Per ultimo, il capitolo analizza il disegno di legge n. 1146/2024, attualmente in discussione al Senato. Di tale proposta legislativa si valutano i contenuti, con particolare riguardo ai principi generali introdotti, alle misure settoriali delineate e al modello di *governance* proposto, evidenziandone le eventuali criticità e interrogandosi sulla sua compatibilità con il quadro normativo europeo.

I. L'ERA DIGITALE E L'INTELLIGENZA ARTIFICIALE

1. Lo Stato digitale e le disruptive technologies

Sin dagli esordi dello Stato moderno, intorno all'innovazione tecnologica si sono generate molte speranze, ma anche e soprattutto timori e scetticismo. Non stupisce, dunque, che alla diffusione di nuove applicazioni tecnologiche si sia sempre accompagnata la mano dello Stato, nella forma dell'intervento pubblico e di una più o meno intensa attività regolatoria.[3] È noto come l'evoluzione dei processi industriali tra il XVIII e XIX secolo abbia portato all'introduzione delle prime normative in materia di salute e sicurezza sul lavoro; ancora, con la seconda rivoluzione industriale, le nuove tecnologie per la produzione energetica e il genio ingegneristico stimolarono nuove ondate di regolamentazione, in particolare nei settori strategici dei trasporti e delle telecomunicazioni. La terza rivoluzione industriale, nell'attraversare il XX secolo, si caratterizzò per lo straordinario progresso conosciuto nei campi della biotecnologia, dell'energia nucleare, dell'informatica e dell'elettronica, per citarne alcuni. È questo il periodo storico in cui ci si inizia a interrogare sui rischi che le nuove tecnologie pongono all'ambiente e alla salute, ma è anche il periodo in cui la regolazione si inizia a occupare degli aspetti etici legati allo sviluppo inarrestabile della tecnica.[4]

Con l'avvento di quella che è stata definita "la quarta rivoluzione industriale",[5] il rapporto tra Stato e nuove tecnologie è mutato sensibilmente: per la prima volta, le tecnologie digitali non rappresentano solo l'oggetto della regolazione, ma diventano una componente fondamentale del funzionamento dello Stato. L'attività pubblica ne risulta

---

[3] Luisa Torchia, *Lo Stato digitale* (Bologna: Il Mulino, 2023), 17.

[4] Julia Black e Andrew Murray, "Regulating AI and Machine Learning: Setting the Regulatory Agenda," *European Journal of Law and Technology* 10, n. 3 (dicembre 2019): 1-2, https://www.ejlt.org/index.php/ejlt/article/view/722/980.

[5] Il termine è stato coniato da Klaus Schwab, fondatore del World Economic Forum, per riferirsi alla rivoluzione tecnologica in corso, ritenuta in grado di confondere "i confini tra la sfera fisica, digitale e biologica". Le tecnologie considerate alla base della quarta rivoluzione industriale sono principalmente l'Intelligenza Artificiale e i dispositivi cd. *smart* nell'Internet delle Cose (*Internet of Things* o *IoT*). Philip Ross e Kasia Maynard, "Towards a 4th Industrial Revolution," *Intelligent Buildings International* 13, n. 3 (marzo 2021): 159-161, doi:10.1080/17508975.2021.1873625. Sul tema, di grande interesse l'analisi di Floridi sulla c.d. *Fourth Revolution*, *cfr.* Luciano Floridi, *La rivoluzione dell'informazione* (Torino: Codice edizioni, 2012).

profondamente trasformata: dalla sicurezza ai servizi pubblici, dalla pianificazione del territorio all'amministrazione della giustizia; le funzioni pubbliche si riorganizzano e le regole che legittimano e disciplinano l'esercizio del potere vengono riscritte.[6] È dunque lo Stato stesso a "convertirsi" al digitale, ad aprirsi alle sfide e alle opportunità del cyberspazio.[7]

La digitalizzazione delle funzioni pubbliche ha avuto importanti riflessi anche nell'ordinamento italiano: si pensi alla firma digitale, alla posta elettronica certificata, agli sportelli telematici della pubblica amministrazione.[8] Più in generale, si pensi al Codice dell'Amministrazione Digitale (CAD), con il quale ha fatto il suo ingresso nel nostro ordinamento l'idea di "squisito sapore costituzionalistico" di una cittadinanza digitale:[9] a cittadini e imprese sono così riconosciuti i diritti relativi all'identità digitale e al domicilio digitale, all'accesso a servizi pubblici online, alla partecipazione attiva ai procedimenti amministrativi in formato elettronico e alla possibilità di effettuare pagamenti online.[10]

Come immaginabile, il processo di digitalizzazione non interessa la sola dimensione nazionale. La Bussola Digitale 2030 è il documento con cui la Commissione Europea ha fissato gli obiettivi per il "decennio digitale",[11] tracciando la strada da seguire per giungere a una completa digitalizzazione della vita democratica e garantire l'interoperabilità a tutti i livelli di governo e tra i servizi pubblici.[12] Il modello ispiratore è quello del c.d. *eGovernment*, più precisamente nella forma di *government as a platform*

---

[6] Torchia, *Lo Stato Digitale*, 19.

[7] Pasquale Costanzo, "Lo 'Stato digitale': considerazioni introduttive," relazione presentata al *Convegno annuale dell'Associazione "Gruppo di Pisa"*, Genova, 18 giugno 2021, 9, https://gruppodipisa.it/images/convegni/2021_Convegno_Genova/Pasquale_Costanzo_-_Relazione_introduttiva.pdf.

[8] Lorenzo Casini, "Il futuro dello Stato (digitale)," *Rivista trimestrale di diritto pubblico* 2 (aprile 2024): 436. Per una trattazione puntuale di questi aspetti l'autore rimanda al già citato Torchia, *Lo Stato digitale*, e Barbara Marchetti, "L'amministrazione digitale," in *Enciclopedia del diritto. Vol. III - Le funzioni amministrative*, a cura di Bernardo Giorgio Mattarella e Margherita Ramajoli (Milano: Giuffrè, 2022), 75-109.

[9] Costanzo, "Lo 'Stato digitale'," 3-4.

[10] D.lgs. n. 82/2005, *Codice dell'Amministrazione Digitale,* artt. 3-9, Sezione II, Capo I.

[11] Commissione Europea, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final.

[12] Barbara Boschetti, "La transizione della pubblica amministrazione verso il modello *Government as a platform*," in *L'amministrazione pubblica nell'era digitale*, a cura di Angelo Lalli (Torino: Giappichelli, 2022), 2-3.

(GaaP), e rappresenta un punto cardinale della transizione digitale europea.[13] La pubblica amministrazione è così chiamata a svolgere un ruolo di primaria importanza nella promozione dell'innovazione e nella tutela dei diritti digitali, nel rispetto dei principi costituzionali ed europei.

Per concentrarsi sulla regolazione e la *governance* delle tecnologie digitali, nello specifico dell'Intelligenza Artificiale (IA), questo lavoro tratterà solo incidentalmente il tema, comunque attualissimo, dell'amministrazione digitale.[14] A ogni modo, il riferimento alla rilevanza costituzionale delle recenti acquisizioni normative non è casuale: le nuove tecnologie trasformano lo Stato in profondità, ne cambiano la fisionomia e ne ridiscutono gli elementi costitutivi (popolo, territorio e sovranità). Rivoluzionano le modalità di esercizio delle funzioni legislative, giudiziarie ed esecutivo-amministrative; mettono in crisi i confini; producono non trascurabili effetti sulla vita delle persone, costituiscono un rischio per i loro diritti fondamentali, in particolare per il diritto alla protezione dei dati personali.[15]

Il c.d. "Stato digitale" appare dunque caratterizzato sotto un doppio profilo: da un lato, l'applicazione delle nuove tecnologie porta a una riarticolazione degli apparati e delle funzioni pubbliche; dall'altro, lo sviluppo tecnologico impatta sui mercati, ridefinisce i rapporti economici e sociali, impone la ricerca di nuovi presidi a tutela dei diritti fondamentali e fa emergere la necessità di una nuova regolazione pubblica.[16]

Non è un caso che le tecnologie protagoniste della quarta rivoluzione industriale siano sovente dette "trasformative", o, sottolineandone il carattere radicale,

---

[13] Boschetti, "La transizione della pubblica amministrazione," 3. Per una definizione di GaaP, l'autrice rimanda a R. Pope: "The term 'Government as a Platform' is used to refer to the whole ecosystem of shared APIs and components, open-standards and canonical datasets, as well as the services built on top of them and governance processes that (hopefully) keep the wider system safe and accountable". Richard Pope, *Playbook: Government as a Platform* (Cambridge, MA: Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 2019), 6.
https://ash.harvard.edu/wp-content/uploads/2024/02/293091_hvd_ash_gvmnt_as_platform_v2.pdf

[14] Per un approfondimento sul tema, *cfr*. Angelo Lalli, a cura di, *L'amministrazione pubblica nell'era digitale* (Torino: Giappichelli, 2022). Per una disamina su quella che è stata definita "amministrazione algoritmica" e l'impiego dell'Intelligenza Artificiale da parte della pubblica amministrazione, si rimanda a Aristide Police, "Scelta discrezionale e decisione algoritmica," in *Il diritto nell'era digitale: persona, mercato, amministrazione, giustizia*, a cura di Rosaria Giordano, Andrea Panzarola, Aristide Police, Stefano Preziosi e Massimo Proto (Milano: Giuffrè, 2022), 493–504.

[15] Casini, "Il futuro dello Stato," 438-439.

[16] Torchia, *Lo Stato Digitale*, 19.

"*disruptive*",[17] per tali intendendosi quelle tecnologie in grado di rivoluzionare l'economia, la società e – si è detto – le istituzioni.

Storicamente, Internet è stato un perfetto esempio di tecnologia "*disruptive*"; non solo, la storia della sua (mancata?) regolazione ben illustra le conseguenze negative cui si va incontro quando chi è chiamato a regolare la tecnologia resta inerte. La regolazione della rete, soprattutto nei primi anni del suo sviluppo, fu in larga parte affidata a enti non-statali, che si occuparono di definirne gli standard tecnici e i meccanismi di funzionamento. Con l'adozione del modello *open source* per i protocolli di rete TCP/IP e il rilascio dei protocolli software WWW da parte del CERN nel 1993, la convinzione più diffusa al tempo, forse ingenua, era che il mercato avrebbe regolato da sé la nascente tecnologia.[18] Nel corso degli anni '90, il dibattito tra accademici e cybernauti (o *netizens*, cittadini della Rete, ricorrendo alla terminologia dell'epoca) sull'opportunità di regolare il fenomeno vide una forte contrapposizione tra i sostenitori di due principali posizioni.[19] Sotto la prima – e più risalente – posizione si riunirono tutti coloro che, rifacendosi a idee di matrice libertaria e anarchica, si espressero in senso fortemente contrario a ogni tentativo di regolazione della Rete da parte degli Stati nazionali. Il documento che più e meglio di tutti raccoglie le rivendicazioni dei cyber-libertari è la cosiddetta *Dichiarazione di Indipendenza del Cyberspazio*, presentata al World Economic Forum di Davos nel 1996 e scritta da John Perry Barlow, co-fondatore dell'*Electronic Frontier Foundation* (EFF), una delle primissime fondazioni attive in difesa dei diritti e delle libertà digitali.[20] I sostenitori di Barlow, oltre ad argomentare su una supposta mancanza di legittimità che avrebbe inficiato da principio ogni tipo di intervento statale sul cyberspazio,[21]

---

[17] Per un quadro generale sulle sfide regolatorie poste dalle tecnologie "*disruptive*", *vedi* Araz Taeihagh, M. Ramesh e Michael Howlett, "Assessing the Regulatory Challenges of Emerging Disruptive Technologies," *Regulation and Governance* 15, n. 4 (marzo 2021): 1009–1019, doi:10.1111/rego.12392.

[18] Black e Murray, "Regulating AI and Machine Learning," 4. I principali enti non-statali che si occuparono di definire gli standard tecnici della Rete furono il *World Wide Web Consortium* (W3C), l'*Internet Engineering Taskforce* (IETF) e l'*Internet Corporationfor Assigned Names and Numbers* (ICAAN).

[19] Black e Murray, 6.

[20] Vittorio Bertola e Stefano Quintarelli, *Internet fatta a pezzi: Sovranità digitale, nazionalismi e big tech* (Torino: Bollati Boringhieri, 2023), 30. Per consultare il celebre manifesto di Barlow: John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation* (febbraio 1996), https://www.eff.org/cyberspace-independence.

[21] Sul punto, *cfr.* David R. Johnson e David G. Post, "Law and Borders - the Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367-1402.

confidavano in una forma di *self-regulation* e auto-governo degli spazi digitali da parte della stessa comunità dei cittadini della Rete. I c.d. *digital realist*, di converso, avevano intuito come, in assenza di interventi statali a tutela dei naviganti, la regolazione avrebbe finito per esser di fatto delegata a coloro che scrivevano il codice alla base del funzionamento della Rete, nonché agli organismi privati che detenevano il controllo dei punti di accesso alla stessa.[22] Un modello di regolazione "contrattualistica", ben lontano dal sogno libertario, che presto avrebbe portato alla nascita di vere e proprie monarchie digitali.[23]

A ben vedere, il *boom* di nuovi utenti registrato su Internet alla fine del XX secolo non avvenne in una totale assenza di regole, ma fu incentivato e reso possibile dalla prima normativa con cui si tentò di regolamentare la circolazione dei contenuti in Rete.[24] Con il *Telecommunications Act* americano del 1996,[25] grazie a quanto disposto alla *section* 230, i fornitori di servizi Internet vengono esonerati da ogni responsabilità, civile e penale, per l'eventuale illiceità dei contenuti trasmessi dagli utenti sulle loro piattaforme. Analogamente, l'utente non è ritenuto responsabile per i contenuti inseriti in rete da terzi (altri utenti o fornitori). Il limite all'operatività di questo generale principio di esenzione dalle responsabilità è rappresentato dall'ipotesi in cui il fornitore sia a conoscenza dell'esistenza di contenuti illegali sulla sua piattaforma; in tal caso, vi è l'obbligo di bloccarli e/o rimuoverli.

Questo criterio risultò fondamentale per consentire la nascita delle grandi piattaforme di distribuzione di contenuti generati dagli utenti,[26] al punto che in letteratura

---

[22] Black e Murray, "Regulating AI and Machine Learning," 6. Per approfondire quest'orientamento, I due autori rimandano a Henry H. Perritt Jr., "Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism," *Berkeley Technology Law Journal* 12, n. 2 (settembre 1997): 413-438, doi:10.15779/Z38N08W. *Cfr. anche* Lawrence Lessig, *Code: And Other Laws of Cyberspace* (New York: Basic Books, 1999).

[23] Bertola e Quintarelli, *Internet fatta a pezzi*, 133.

[24] Bertola e Quintarelli, 36.

[25] Stati Uniti, *Telecommunications Act of 1996*, Pub. L. No. 104-104, 110 Stat. 56 (1996).

[26] Bertola e Quintarelli, *Internet fatta a pezzi*, 36-37. Per meglio comunicare la portata innovativa del principio sancito dalla *section* 230, gli autori riportano l'esempio di YouTube: un simile servizio sarebbe stato inconcepibile all'interno di un diverso contesto normativo. La piattaforma sarebbe stata costretta a un'impraticabile opera di revisione per ogni singolo video caricato, al solo fine di non vedersi attribuita la responsabilità legale per eventuali contenuti illeciti.

ci si è riferiti alla *section* 230 come alle "ventisei parole che hanno creato l'Internet".[27] Un simile approccio fu seguito anche dall'Unione Europea, che nel 2000, con la Direttiva E-Commerce,[28] stabilì un'analoga esenzione di responsabilità per i fornitori di servizi, graduandola però diversamente a seconda dell'attività svolta da questi ultimi (puro trasporto di dati o *mere conduit*, ospitalità dei contenuti o *hosting*, velocizzazione della distribuzione di dati o *caching*). Nell'ottica di realizzare un mercato unico digitale europeo, la direttiva sancì poi un altro principio fondamentale, *id est* il "principio del paese di origine": un contenuto considerato legale in un paese membro può essere distribuito in tutti gli altri paesi, restando soggetto alla sola giurisdizione della nazione in cui è ospitato.[29]

In Europa e negli Stati Uniti, dunque, un quadro regolatorio – seppur minimale – vi fu. Anzi, fu proprio sulla scorta di quanto previsto dal *Telecommunications Act* che le *start up* americane, sottratte alla disciplina al tempo prevista per le *utilities*, riuscirono a svilupparsi e trasformarsi in soggetti verticalmente integrati, operando sempre più come oligopolisti e conoscendo una crescita economica senza precedenti nella storia del mondo.[30] Diversi fattori lo hanno reso possibile: diversamente dalle infrastrutture di rete "tradizionali", come le reti per l'energia elettrica, per il gas o per l'acqua, i fornitori di servizi digitali possono utilizzare Internet senza dover corrispondere compensi ad alcun gestore, e sono spesso proprio i fornitori di servizi a valle i proprietari dei server e delle infrastrutture su cui tali servizi vengono ospitati; in secondo luogo, il mercato di riferimento dei servizi digitali è un mercato di dimensione globale, che tendenzialmente prescinde da barriere fisiche e nazionali.[31] Sembra dunque essersi realizzato lo scenario paventato dai c.d. realisti digitali: lo scarno impianto regolatorio che gli Stati (segnatamente, gli Stati occidentali) hanno costruito intorno a Internet, ha fatto sì che

---

[27] L'espressione è stata utilizzata per la prima volta da Kosseff, che ha poi così titolato l'opera in cui ricostruisce la storia della legislazione americana che ha accompagnato la nascita di Internet. *Vedi* Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Ithaca: Cornell University Press, 2019).

[28] Unione Europea, Direttiva 2000/31/CE (*Direttiva sul commercio elettronico*), GUUE L 178 del 17 luglio 2000.

[29] Bertola e Quintarelli, *Internet fatta a pezzi*, 37.

[30] Torchia, *Lo Stato Digitale*, 23.

[31] Torchia, 24. Che i mercati digitali prescindano sempre e comunque dalle barriere che delimitano i mercati "*off-line*" non è sempre vero, e anzi lo è sempre meno. Possono esistere barriere tecniche, economiche, giuridiche e di prodotto. Sul tema, si rimanda al già citato Bertola e Quintarelli, *Internet fatta a pezzi*.

questa transitasse da rete aperta e decentralizzata a un sistema di telecomunicazione in gran parte concentrato nelle mani di pochi oligopolisti (*Big Tech*).[32]

Con il termine "Stato digitale" la letteratura non fa riferimento al solo Stato nazionale nella sua versione contemporanea, nell'accezione che si è avuto modo di illustrare sin dalle prime battute di questo paragrafo, ma anche agli "Stati digitali": [33] le piattaforme gestite dalle *Big Tech* hanno infatti raggiunto un tale livello di estensione e complessità che è stato per queste naturale dotarsi di un sistema di regole e funzioni che ricorda un vero e proprio ordinamento giuridico. Più correttamente, i sistemi normativi autonomi sorti spontaneamente sulle piattaforme digitali sono stati definiti *private legal system*.[34]

Si ricordi, poi, il monito di Cassese sul rapporto ambivalente tra la tecnologia di Internet e lo Stato democratico.[35] La Rete offre l'opportunità di rafforzare la partecipazione alla vita democratica e l'organizzazione della vita politica attraverso la c.d. "democrazia elettronica",[36] ma al tempo stesso facilita fenomeni quali la diffusione di notizie false, l'influenza della propaganda straniera, la creazione di "bolle" ideologiche e la polarizzazione del dibattito pubblico. In questo contesto, desta l'attenzione del regolatore non solo il ruolo delle *Big Tech* come *gatekeeper* dei mercati digitali, capaci di neutralizzare la concorrenza delle imprese minori attraverso acquisizioni strategiche e pratiche anticoncorrenziali, ma anche e soprattutto come "meccanismi di controllo dell'informazione", in grado di controllare e persino interrompere i flussi informativi, condizionare i processi democratici e comprimere la libertà di espressione.[37]

---

[32] Bertola e Quintarelli, *Internet fatta a pezzi*, 51.

[33] Torchia, *Lo Stato Digitale*, 23.

[34] Sul tema, *cfr.* Chris Reed e Andrew Murray, *Rethinking the Jurisprudence of Cyberspace* (Cheltenham: Edward Elgar, 2020), 109-120. Per alcuni esempi concreti, *vedi* Thomas Schultz, "Private Legal Systems: What Cyberspace Might Teach Legal Theorists," *Yale Journal of Law & Technology* 10, n. 151 (gennaio 2007): 151-193.

[35] *Cfr.* Sabino Cassese, *La democrazia e i suoi limiti*, 2ª ed. (Milano: Mondadori, 2018).

[36] Questa nuova forma di democrazia è stata definita anche "virtuale", "digitale", "continua" o ancora "nuova democrazia di massa". Così Tommaso Edoardo Frosini, "L'Ordine giuridico del digitale," in *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce (Torino: Giappichelli, 2023), 35-42.

[37] Emily B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge: Cambridge University Press, 2015), 116-171.

Con le considerazioni sino a qui svolte si è, per un verso, tentato di fornire una definizione di Stato digitale (e Stati digitali), per altro, si è fatto cenno ad alcune tappe fondamentali nella storia di Internet e della c.d. società dell'informazione.[38] Più di tutto, poi, si è cercato di mettere in luce il rapporto tra regolazione e nuove tecnologie, ricorrendo all'esempio paradigmatico della Rete.

Proprio come Internet, l'Intelligenza Artificiale è considerata una *disruptive technology,* ma il parallelismo non deve indurre in errore: l'IA non ha ancora raggiunto uno stadio di maturità tecnologica paragonabile a quello delle altre tecnologie dell'informazione e della comunicazione; le sue implicazioni per la società e gli ordinamenti giuridici non sono ancora stimabili con precisione.[39] La letteratura giuridica ha più volte sottolineato il carattere "rivoluzionario" di questa tecnologia,[40] l'inadeguatezza delle norme vigenti nel regolare macchine "all'evidenza diverse da tutte le altre",[41] e persino il rischio che a subire la "*disruption*" sia, in ultima analisi, la regolamentazione giuridica stessa, ben potendo i metodi e gli strumenti giuridici tradizionali venir condannati all'obsolescenza e all'inefficacia.[42]

Nel corso di questo lavoro ci si interrogherà quindi sull'*an*, sul *quantum* e sul *quomodo* della regolazione dell'IA.[43] Prima di procedere, tuttavia, appare necessaria una digressione riguardo le due dimensioni fondamentali in cui si sviluppa lo Stato digitale: il dato e l'algoritmo.

---

[38] Con il termine "società dell'informazione", in sociologia, si fa riferimento a quella società contraddistinta dall'utilizzo diffuso delle nuove tecnologie dell'informazione e della comunicazione (ICT) da parte dei suoi componenti. Viene così definito quel modello sociale che è storicamente succeduto alla società post-industriale. *Cfr.* Yoneji Masuda, *The Information Society as Post-Industrial Society* (Tokyo: World Future Society, 1980).

[39] Alessandro Pajno et al., "AI: Profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista," *BioLaw Journal - Rivista di BioDiritto*, n. 3 (novembre 2019): 207, doi:10.15168/2284-4503-449.

[40] Filippo Donati, "Quale disciplina per l'intelligenza artificiale?" in *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce (Torino: Giappichelli, 2023), 45-46.

[41] Carmela Salazar, "Umano, troppo umano. O no? Robot, androidi e cyborg nel 'mondo del diritto' (prime notazioni)," *BioLaw Journal - Rivista di BioDiritto*, n. 1 (maggio 2014): 257, doi:10.15168/2284-4503-21.

[42] Giuseppe Mobilio, "L'intelligenza artificiale e i rischi di una 'disruption' della regolamentazione giuridica," *BioLaw Journal - Rivista di BioDiritto*, n. 2 (luglio 2020): 401-424, doi:10.15168/2284-4503-669.

[43] Sul tema, in particolare, *vedi* capitolo II, paragrafo 1.

1.1. L'età degli algoritmi: automazione e predizione

La società dell'informazione sta oggi attraversando un importante fase di transizione. La dimensione globale della Rete ha consentito la proliferazione dei dati e dei mezzi di comunicazione, aprendo la strada alla c.d. "età degli algoritmi", il nuovo stadio evolutivo della società digitale. A partire dai dati, l'algoritmo è in grado di trasformare l'enorme mole di informazioni disponibile in conoscenza operativa, sfruttando processi automatizzati.[44] Per una migliore comprensione dell'impatto che hanno avuto – e avranno – gli algoritmi sugli ordinamenti giuridici, è necessario tracciare una distinzione tra decisione e predizione algoritmica.

Tradizionalmente, il programmatore di un algoritmo applica rigorose regole sintattiche e strutture di dati al fine di ottenere dalla macchina lo svolgimento automatico di un'azione desiderata. Per farlo, chi "scrive codice" adotta il c.d. pensiero computazionale: attraverso un lavoro di astrazione, dovrà scomporre l'algoritmo in sotto-programmi sempre più piccoli, ciascuno a sua volta composto da sotto-routine e ulteriori procedure.[45] Questo modo di operare ha consentito, attraverso il codice, la digitalizzazione della conoscenza e l'implementazione della decisione algoritmica in contesti istituzionali e nella pubblica amministrazione. Si tratta di algoritmi che si limitano a eseguire compiti predeterminati applicando le regole proprie del loro programma, tornando utili per la digitalizzazione della burocrazia e l'automazione dei procedimenti amministrativi.[46] Diversamente, la predizione algoritmica si caratterizza per l'impiego di modelli di analisi statistica in grado di individuare *pattern* e ricorrenze nei dati disponibili, così da formulare, sulla base di questi, previsioni e inferenze sul futuro. Il modello statistico, per giunta, non dev'essere necessariamente prestabilito dal programmatore, ben potendo la macchina determinarlo da sé attraverso l'apprendimento

---

[44] Martin Hilbert, "Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective," *Dialogues in Clinical Neuroscience* 22, n. 2 (giugno 2020): 193, doi:10.31887/DCNS.2020.22.2/mhilbert.

[45] *Cfr.* Karl Beecher, *Computational Thinking: A Beginner's Guide to Problem-Solving and Programming* (Swindon: BCS, The Chartered Institute for IT, 2017).

[46] Una prima riflessione sul tema nasce dal lavoro di Mark Bovens e Stavros Zouridis, "From Street-Level to System-Level Bureaucracies: How Information and Communication Technology is Transforming Administrative Discretion and Constitutional Control," *Public Administration Review* 62, n. 2 (dicembre 2002): 174-184.

automatico.[47] Come si vedrà, gli algoritmi predittivi e i modelli statistici, così come gli algoritmi di apprendimento automatico, sono alla base del funzionamento dell'intelligenza artificiale e pongono oggi le più significative sfide regolatorie.[48]

Con la distinzione qui proposta si vuole sottolineare come il diverso impiego che si fa dell'algoritmo comporti rischi differenti, domandando quindi un differenziato intervento regolatorio. Una breve digressione su come il diritto amministrativo nazionale ha reagito all'avvento della società digitale aiuterà a illustrare quanto sostenuto.

Nel già menzionato Codice dell'Amministrazione Digitale, all'art. 2, comma 1,[49] si rinviene un primo richiamo normativo all'esigenza di attuare una piena digitalizzazione delle funzioni amministrative, da perseguire tramite l'adozione delle tecnologie dell'informazione e della comunicazione. Il comma in esame è stato ritenuto espressione della finalità generale del Codice.[50] L'obiettivo dell'amministrazione digitale, in Italia, è stato quindi perseguito combinando più "forme della giuridicità": da un lato, attraverso la volontà del legislatore, cristallizzatasi nella disciplina prevista dal CAD; dall'altro, grazie agli interventi dell'Agenzia per l'Italia Digitale (AgId), che a vario titolo potremmo qualificare come "regolatori".[51] La prima forma di regolazione è rappresentata dal Piano triennale per l'informatica nella pubblica amministrazione, strumento di programmazione dal carattere sostanzialmente regolatorio, con cui l'AgId indirizza il processo di digitalizzazione della PA e fissa i principi operativi che andranno garantiti nella fornitura di servizi digitali.[52] Un'altra forma di regolazione, per così dire "tecnica", si realizza tramite le "Linee guida" periodicamente aggiornate dall'AgId; si tratta in

---

[47] Marc Schuilenburg e Rik Peeters, a cura di, *The Algorithmic Society: Technology, Power, and Knowledge* (Londra: Routledge, 2020), 4. Per la definizione di apprendimento automatico, *vedi* paragrafo 2.

[48] Per un chiarimento sulla definizione di intelligenza artificiale e alcuni cenni sul dibattito in corso nella letteratura scientifica (la c.d. "questione definitoria"), *vedi* paragrafo 2.

[49] «Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti le tecnologie dell'informazione e della comunicazione».

[50] Edoardo Chiti, "Doppio volto: il diritto amministrativo alla prova dell'amministrazione digitale e algoritmica," in *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, a cura di Angelo Lalli (Torino: Giappichelli, 2024), 84.

[51] Chiti, 83.

[52] Il Piano è previsto all'art. 14-*bis*, comma 2, lett. b) del CAD. La sua elaborazione è affidata ad AgId in collaborazione con il Dipartimento per la trasformazione digitale. Il programma dev'essere poi approvato dal Presidente del Consiglio o da Ministro delegato entro il 30 settembre di ogni anno.

questo caso di una regolazione flessibile, che si atteggia più che altro come strumento di ricognizione dello stato dell'arte raggiunto dalla tecnologia, riflettendo scelte di carattere puramente tecnico.[53] Da ultimo, non può ignorarsi come l'intera materia sia governata, sul piano informatico, proprio dall'algoritmo, dal "codice" con cui sono programmati i servizi digitali.[54]

Questa sommaria esposizione della normativa nazionale sull'amministrazione digitale restituisce un quadro piuttosto positivo: il diritto amministrativo si è mostrato preparato nel cogliere le opportunità offerte dalla digitalizzazione, più di quanto lo sia stata, in concreto, la pubblica amministrazione stessa. Sono state messe in campo diverse tecniche regolatorie e un quadro istituzionale di *governance*,[55] affidando le scelte tecniche al regolatore amministrativo e gettando così le fondamenta per il c.d. cyberspazio pubblico.[56]

Decisamente più frammentata, invece, la cornice regolatoria venuta a costruirsi intorno alla c.d. amministrazione algoritmica.[57] Con tale termine, si fa riferimento a quell'amministrazione non solo digitalizzata, ma in grado di impiegare, nell'esercizio delle sue funzioni, algoritmi predittivi e intelligenza artificiale. L'utilizzo dell'IA da parte della pubblica amministrazione ha posto numerosi interrogativi, cui i tradizionali principi di diritto amministrativo e le tecniche regolatorie "classiche" hanno potuto fornire risposte soltanto parziali; si aggiunga che l'adozione di detti algoritmi da parte delle amministrazioni ha costituito un fenomeno spontaneo, con effetti talvolta dirompenti. A tal proposito, si è parlato di un quadro segnato da "'pieni' e 'vuoti' regolatori",[58] in cui l'individuazione di "elementi di minima garanzia" è stata affidata, per lungo tempo, alla

---

[53] Le "Linee guida" sono disciplinate dall'art.14-*bis*, comma 2, lett. a) del CAD, in cui è previsto che spetta ad AgId la funzione di "emanazione di Linee guida contenenti regole, standard e guide tecniche, nonché di indirizzo, vigilanza e controllo sull'attuazione e sul rispetto delle norme di cui al presente Codice, anche attraverso l'adozione di atti amministrativi generali, in materia di agenda digitale, digitalizzazione della pubblica amministrazione, sicurezza informatica, interoperabilità e cooperazione applicativa tra sistemi informatici pubblici e quelli dell'Unione europea".

[54] Chiti, "Doppio volto," 83.

[55] Per la ricostruzione del quadro normativo e regolatorio posto dal CAD, *vedi* Bruno Carotti, "L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice," *Giornale di diritto amministrativo* 23, n. 1 (gennaio 2017): 7-18

[56] Chiti, "Doppio volto," 87

[57] La distinzione tra "amministrazione digitale" e "amministrazione algoritmica" è ripresa da Marchetti, "L'amministrazione digitale," 75-109.

[58] Così Chiti, "Doppio volto," 88

giurisprudenza del Consiglio di Stato.[59] Sebbene ancora manchi una disciplina articolata dell'uso dell'intelligenza artificiale nell'esercizio delle funzioni amministrative, in tempi recenti si sono registrati importanti progressi verso questa direzione e importanti indicazioni sono giunte soprattutto dalla normativa europea.

A ogni modo, l'utilizzo dell'intelligenza artificiale da parte delle pubbliche amministrazioni è già una realtà. Questo è vero non solo per le autorità indipendenti, ma anche, più in generale, per le amministrazioni centrali e per gli enti territoriali (si pensi alle esperienze di *smart cities*).[60] È una realtà anche nelle imprese e sui mercati: si pensi alle macchine a guida autonoma, ai sistemi in grado di offrire consulenza legale o finanziaria, agli algoritmi di *data analysis*.[61] I "nuovi" algoritmi introducono elementi di complessità che sfidano i tradizionali assetti normativi, non soltanto – come si è visto – nel diritto amministrativo. Senza pretesa di esaustività, si intende qui illustrarne alcuni tra i più rilevanti.

Un primo elemento di complessità è legato alla constatazione che i sistemi d'intelligenza artificiale sono assai raramente il "prodotto unico" (*one-off product*) di una singola organizzazione, rappresentando piuttosto l'esito di un lungo ciclo produttivo (c.d. "*AI life-cycle"*) che inizia con la raccolta e la categorizzazione dei dati destinati allo sviluppo del sistema e coinvolge una pluralità di attori. Ciò solleva questioni rilevanti sulle responsabilità da attribuire nelle diverse fasi del ciclo produttivo, nonché sulla definizione dell'ambito di applicazione di interventi normativi e regolatori in materia.[62]

Un secondo elemento di complessità risiede nel carattere *general-purpose* della maggior parte dei sistemi di IA. Con tale espressione si fa riferimento alla capacità di uno stesso sistema di adattarsi a diversi scenari e applicazioni, potenzialmente anche molto distanti tra loro, con implicazioni differenti per le persone e gli individui a seconda del

---

[59] L'espressione è tratta da Consiglio di Stato, sez. VI, sent. 13 dicembre 2019, n. 8472. Per una disamina completa sul contributo della giurisprudenza del Consiglio di Stato sul tema della decisione algoritmica della pubblica amministrazione, si rinvia al già citato Police, "Scelta discrezionale e decisione algoritmica".

[60] Per alcuni esempi e un'analisi delle tendenze in corso, compresa quella delle *smart cities*, *vedi* Edoardo Chiti, Barbara Marchetti e Nicoletta Rangone, "L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali," *BioLaw Journal - Rivista di BioDiritto*, n. 2 (luglio 2022): 489-507, doi:10.15168/2284-4503-2351.

[61] Georg Borges e Christoph Sorge, a cura di, *Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech* (Cham: Springer, 2022).

[62] Lilian Edwards, *Regulating AI in Europe: Four Problems and Four Solutions* (Ada Lovelace Institute, 2022), 6, https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/.

contesto in cui il sistema entra in funzione. Un *software* di riconoscimento facciale, ad esempio, potrebbe essere utilizzato sia per l'autenticazione del personale all'ingresso di una struttura penitenziaria, sia per monitorare i clienti di un'attività commerciale, in un caso con finalità di sorveglianza, nell'altro con finalità pubblicitaria. È evidente come questo renda impossibile in astratto una valutazione d'impatto di tali sistemi, prescindendo dal considerare il settore ove in concreto saranno implementati.[63]

A un terzo e ulteriore elemento si è poi già fatto cenno, indirettamente, nel corso di questa trattazione. Chi è chiamato a normare e regolare l'intelligenza artificiale non può trascurare il rapporto simbiotico che lega le tecnologie della società digitale nell'*Internet of Things* (IoT). Del termine si è fatto largo uso in letteratura per riferirsi a quel paradigma emergente della società dell'informazione che ha reso possibile la comunicazione tra dispositivi elettronici e sensori attraverso Internet, consentendo lo scambio e la trasmissione di dati tra dispositivi c.d. *smart*. I dispositivi "intelligenti" sono capaci di percepire l'ambiente attraverso sensori, elaborare flussi di dati in tempo reale e regolare il proprio comportamento di conseguenza, impiegando a tal scopo gli algoritmi predittivi e l'intelligenza artificiale.[64] L'IA si è dunque sviluppata parallelamente alla gigantesca infrastruttura di dati globale resa possibile (e disponibile) dalla Rete; di questa si "nutre" e, al tempo stesso, la alimenta, anche grazie ai dati generati dagli artefatti. [65] Distinguere le due dimensioni sarebbe oggi impossibile.

Proprio perché basa il suo funzionamento sui dati e sugli algoritmi – in particolare, predittivi e di apprendimento automatico – l'intelligenza artificiale impone di rivedere l'assunto secondo cui la tecnologia sarebbe intrinsecamente "neutrale", dotata esclusivamente di una funzione strumentale e che, di conseguenza, non necessiti di una regolamentazione specifica.[66] L'argomento è stato a più riprese utilizzato per giustificare

---

[63] Edwards, 6-7

[64] Per una visione completa dell'IoT, le sue applicazioni e i possibili impatti sulla società, *cfr.* Sachin Kumar, Prayag Tiwari e Mikhail Zymbler, "Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review," *Journal of Big Data* 6, n. 111 (dicembre 2019), doi:10.1186/s40537-019-0268-2.

[65] Così Maria Grazia Peluso, *Intelligenza artificiale e tutela dei dati: Prospettive critiche e possibili benefici per una governance efficace* (Milano: Giuffrè, 2023), 47. Sul punto l'autrice rimanda a Douglas Heaven, a cura di, *Macchine che pensano. La nuova era dell'intelligenza artificiale*, tradotto da Valeria Lucia Gili (Bari: Edizioni Dedalo, 2018), 37.

[66] Mobilio, "L'intelligenza artificiale", 406.

una certa diffidenza verso la regolamentazione giuridica dell'intelligenza artificiale,[67] al punto che anche per l'IA può parlarsi di una "pretesa anarchica", per certi versi analoga a quella di Barlow e dei cyber-libertari all'indomani della diffusione della Rete negli anni 90'.[68] Non solo: l'impiego dell'intelligenza artificiale è talvolta incoraggiato in sostituzione del fattore umano nei processi decisionali, sull'assunto che questa, diversamente dall'uomo, non sarebbe condizionata da esperienze personali e costrutti valoriali, e dunque deciderebbe in maniera "neutrale".[69]

Tali affermazioni sembrerebbero il frutto di un fraintendimento. In primo luogo, è il funzionamento stesso degli algoritmi a contraddire questa pretesa di neutralità: questi non si limitano a riflettere passivamente la realtà, rispecchiando piuttosto le scelte e la visione del mondo dei loro programmatori. Il risultato restituito dalla macchina è sempre un risultato condizionato dal "peso attribuito ai singoli parametri inseriti", dalle "formule classificanti", e dalle "procedure" selezionate da chi ne ha scritto il codice.[70]

Per l'intelligenza artificiale, poi, questo è ancor più vero: gli algoritmi alla base del suo funzionamento non si limitano a svolgere calcoli matematici e operazioni computazionali su richiesta, seguendo il tradizionale schema *input-output*, ma realizzano, come si è detto, l'apprendimento automatico, conferendo alla macchina la capacità di apprendere dai dati immessi nel sistema e dai propri stessi risultati. Nello schema tradizionale *input-output*, consegnare all'algoritmo dati di cattiva qualità in *input* genera un errore "occasionale" in *output*.[71] Addestrare l'IA su dati di cattiva qualità ha conseguenze ben più significative: vuol dire compromettere il processo di apprendimento stesso, condannando il sistema a un "*bias* permanente".[72] In presenza di "cattivi" dati, la

---

[67] Mobilio, 406

[68] Pajno et al., "AI: Profili giuridici," 207.

[69] Peluso, *Intelligenza artificiale*, 43.

[70] Così Agata C. Amato Mangiameli, "Algoritmi e big data. Dalla carta sulla robotica," *Rivista di filosofia del diritto* 1 (giugno 2019): 109, doi:10.4477/93369.

[71] Giuseppe D'Acquisto, "Qualità dei dati e Intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati," in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti (Torino: Giappichelli, 2018), 266.

[72] D'Acquisto, 266.

correttezza formale dell'algoritmo è insufficiente a garantire la correttezza dell'*output*.[73] L'effetto in questione è noto in informatica come "*garbage in, garbage out*".[74]

Anche i dati "buoni", in ogni caso, non possono dirsi neutrali. Un dato ben potrebbe essere oggettivo – che riflette correttamente la realtà delle cose – e non neutrale al tempo stesso. A mero titolo di esempio: è un fatto oggettivo che alcune categorie di persone, a causa di una storia di discriminazione passata e presente, siano oggi sotto rappresentate in alcune professioni, in particolare nei ruoli dirigenziali.[75] I dati cristallizzano questa situazione di fatto, ma restano insensibili al contesto. L'algoritmo in cui tali dati sono inseriti, poi, operando mediante modelli statistici, tenderà a conservare e riprodurre lo "stato del mondo" così come descritto nel *dataset*, perpetuando nel futuro le ingiustizie del passato.[76] Persino *il* dato, singolarmente considerato, difficilmente può dirsi neutrale: questo è sì espressione della realtà, ma in forma semplificata e tradotta in formato computabile, secondo le scelte di chi lo ha reso interpretabile dalla macchina.[77]

Nel corso di questo paragrafo si è evidenziato come gli algoritmi riflettano i *bias* dei loro programmatori; nell'intelligenza artificiale il problema si pone sotto una prospettiva del tutto inedita. I sistemi di IA, grazie all'apprendimento automatico, possono sviluppare comportamenti imprevisti e difficilmente indagabili, che non

---

[73] D'Acquisto, 267.

[74] L'espressione è da sempre molto popolare nel campo dell'informatica. Charles Babbage, inventore del primo calcolatore programmabile, fa riferimento all'effetto *garbage in, garbage out* nel suo libro di memorie: "On two occasions I have been asked, 'Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?' ... I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question." Charles Babbage, *Passages from the Life of a Philosopher* (Londra: Longman and Co., 1864), 67.
Il tema gode di rinnovato interesse oggi, con riferimento all'intelligenza artificiale e agli algoritmi di apprendimento automatico. *Cfr*. Giuseppe Francesco Italiano, "Le sfide interdisciplinari dell'intelligenza artificiale," *Analisi Giuridica dell'Economia* 1 (giugno 2019): 13, doi:10.1433/94541.

[75] Può dunque dirsi che il dato non è mai neutrale perché è la realtà delle cose, anzitutto, a non esserlo. Un esempio di quanto si afferma è fornito da Torchia, *Lo Stato Digitale*, 142: "È un dato oggettivo che prima del 1963 non ci fossero donne magistrato ... È stata necessaria prima una sentenza della Corte costituzionale nel 1960 e poi un'apposita legge nel 1963 per consentire alle donne di accedere alla magistratura. Ed è sempre un dato oggettivo che in magistratura i ruoli apicali siano coperti in misura più ampia da uomini: ma poiché il principale criterio di avanzamento di carriera è l'anzianità, è evidente che ... la ridotta presenza [delle donne] nei ruoli apicali dipende più dal fattore tempo che non da minori capacità. Se però si utilizzasse un algoritmo per ... proiettare nel futuro le caratteristiche attuali della dirigenza, si finirebbe per ... riprodurre una politica di reclutamento e di avanzamento storicamente condizionata, che alla luce della Costituzione meriterebbe di essere, invece, profondamente innovata".

[76] Torchia, 141-143.

[77] Peluso, *Intelligenza artificiale*, 44.

necessariamente figuravano nelle intenzioni dei loro creatori.[78] L'autonomia decisionale di questi sistemi solleva questioni tuttora irrisolte in tema di responsabilità giuridica: se una decisione presa dall'IA causa un danno, chi è chiamato a risponderne? Le normative sulla responsabilità civile e penale si sono sviluppate in un contesto tecnologico radicalmente diverso da quello attuale; la tenuta dei criteri dell'intenzionalità e della colpa, presenti "virtualmente in ogni settore della legge", è oggi seriamente minacciata dall'intelligenza artificiale.[79]

L'ultimo profilo di criticità cui si intende qui fare riferimento riguarda l'interpretabilità e la trasparenza degli algoritmi. Indissolubilmente legato al tema della responsabilità giuridica, vi è infatti il c.d. "*black box effect*". In termini essenziali, la maggior parte degli algoritmi di intelligenza artificiale può essere paragonata a una "scatola chiusa" per via della sua opacità:[80] diversamente dagli algoritmi tradizionali, quando entra in gioco l'apprendimento automatico possiamo avere una chiara comprensione delle informazioni che forniamo all'algoritmo (*input*) e di quelle che esso restituisce (*output*), ma una conoscenza solo vaga, o persino nulla, del processo con cui la macchina ha elaborato l'*input* e calcolato l'*output*.[81] Uno dei primi studi dell'effetto *black box* dal punto di vista regolatorio è il celebre "*The Black Box Society*", 2015, di Frank Pasquale.[82] Sebbene il volume abbia aperto la strada alla riflessione accademica sul tema, negli anni successivi si sono registrati pochi progressi nella definizione di

---

[78] Alberto Marchetti Spaccamela e Fabrizio Silvestri, "Trasparenza e interpretabilità delle decisioni dei sistemi di Intelligenza Artificiale," in *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, a cura di Angelo Lalli (Torino: Giappichelli, 2024), 163.

[79] *Cfr.* Yavar Bathaee, "The Artificial Intelligence Black Box and the Failure of Intent and Causation," *Harvard Journal of Law & Technology* 31, n. 2 (marzo 2018): 889-938. Per esigenze di esposizione, questo lavoro si concentrerà sulla regolazione e la *governance* dell'AI, pur riconoscendo che la questione della responsabilità giuridica per i danni causati dai sistemi di intelligenza artificiale rappresenta da tempo uno dei temi più dibattuti in letteratura. Tra gli altri, *si vedano* Guido Alpa, a cura di, *Diritto e intelligenza artificiale* (Pisa: Pacini Giuridica, 2020); Salvatore Aleo, a cura di, *Evoluzione scientifica e profili di responsabilità: neuroscienze, intelligenza artificiale, tutela della persona e modelli di responsabilità* (Pisa: Pacini Giuridica, 2022); Ugo Ruffolo, Andrea Amidei ed Enrico Al Mureden, "La responsabilità," in *XXVI lezioni di diritto dell'intelligenza artificiale*, a cura di Ugo Ruffolo (Torino: Giappichelli, 2021), 131-184.

[80] Donati, "Quale disciplina per l'intelligenza artificiale?," 47.

[81] Stefano Quintarelli, *Intelligenza artificiale: Cos'è davvero, come funziona, che effetti avrà* (Torino: Bollati Boringhieri, 2020), 97.

[82] *Cfr.* Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

strategie regolatorie per affrontare il problema dell'opacità degli algoritmi.[83] L'elaborazione di un'efficace approccio regolatorio, anche mediante l'adozione di soluzioni tecniche innovative, appare non più rinviabile: la "spiegabilità" dei sistemi di IA è un nodo cruciale nella regolamentazione del fenomeno. Poter comprendere in modo chiaro il funzionamento della macchina e, ancor di più, come questa sia giunta a una decisione, costituisce un presupposto essenziale per instaurare fiducia nello strumento e verificare che stia agendo in modo equo, etico e legale.[84] I concetti di spiegabilità e responsabilità si mostrano dunque intimamente intrecciati: in assenza di un'adeguata comprensione del "come" la macchina abbia assunto una determinata decisione, attribuirne la responsabilità appare compito estremamente arduo.[85]

L'esigenza di garantire la trasparenza dei sistemi di IA è stata percepita anche dal legislatore europeo, come testimonia l'art. 13 del Regolamento (UE) 2024/1689 (AI Act)[86], che prevede che i sistemi di IA ad alto rischio siano progettati e sviluppati in modo da garantire un funzionamento "sufficientemente trasparente", tale da consentire ai *deployer* di interpretarne gli *output*. Il tipo e il livello di trasparenza in questione, inoltre, dovrà consentire a fornitori e *deployer* il rispetto degli ulteriori obblighi che il Regolamento pone a loro carico.[87] Il tema della trasparenza e della spiegabilità degli algoritmi, poi, assume rilievo anche alla luce di quanto previsto dall'art. 22 del Regolamento Europeo sulla protezione dei dati personali (GDPR),[88] che sancisce il diritto dell'interessato di "non essere sottoposto a una decisione basata unicamente sul

---

[83] Black e Murray, "Regulating AI and Machine Learning," 4.
[84] Marchetti Spaccamela e Silvestri, "Trasparenza e interpretabilità delle decisioni," 164.
[85] Marchetti Spaccamela e Silvestri, 168.
[86] Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (*Regolamento sull'intelligenza artificiale*), GUUE L, 12 luglio 2024.
[87] Regolamento (UE) 2024/1689, art. 13, par. 1: "I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del deployer di cui alla sezione 3."
[88] 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 e alla libera circolazione di tali dati (*GDPR*), GUUE L 119, 4 maggio 2016.

trattamento automatizzato".[89] Sebbene lo stesso articolo ponga a tale diritto alcune eccezioni, al ricorrere di due particolari ipotesi all'interessato dovranno essere garantite in ogni caso alcune tutele essenziali: "il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".

Sul testo dell'AI Act si tornerà in seguito;[90] quanto all'art. 22 del GDPR, basti qui accennare al fatto che questa disposizione ha indotto autorevole dottrina ha teorizzare l'esistenza di un vero e proprio "diritto alla spiegazione" in presenza di decisioni automatizzate.[91]

1.2. Big Data e Data economy

Il termine "*Big Data*" è di non agevole definizione. L'espressione è stata diversamente declinata in letteratura, venendo a ogni modo sempre riferita a quei fenomeni di natura sociologica di cui si è fatta menzione nel cominciare questo lavoro: società dell'informazione, quarta rivoluzione industriale e rivoluzione digitale.[92] Il dato, *rectius* i dati, costituiscono una delle dimensioni fondamentali dello Stato digitale; attraverso Internet, si è detto, questi hanno conosciuto un processo di crescita esponenziale apparentemente inarrestabile. Gran parte degli oggetti di uso quotidiano sono oggi "intelligenti": interagiscono tra loro e con gli utenti, assorbono informazioni dall'ambiente e le scambiano in Rete in tempo reale, per poi tradurle in innovative applicazioni pratiche.[93] Non più soltanto computer e *smartphone*: ad alimentare il flusso di dati *on-line* vi sono dispositivi di ogni tipo, dagli *smartwatch* indossabili alla domotica,

---

[89] Regolamento (UE) 2016/679, art. 22, par. 1: "L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona".

[90] *Vedi* capitolo III.

[91] Del resto, come evidenziato da Peluso: "Se non fosse possibile comprendere la logica sottostante allo specifico *output* ... sarebbe ... complesso un intervento umano ... parimenti complesso appare l'esercizio del diritto di contestare la decisione automatizzata dal momento che di essa non è possibile conoscere la *ratio* ma solo l'esito." Peluso, *Intelligenza artificiale*, 208.

[92] *Si veda* per tutti Aleksei V. Bogoviz, a cura di, *Big Data in Information Society and Digital Economy* (Cham: Springer, 2023).

[93] Arianna Maceratini, "Dall'Internet of Things alle Smart Roads. Riflessioni informatico-giuridiche su strade intelligenti, veicoli automatici e connessi," *Rivista elettronica di diritto economia e management*, n. 3 (gennaio 2019): 72.

passando per i dispositivi di navigazione assistita.[94] È all'interno di questa architettura, nell'*Internet of Things*, che anche grazie all'intelligenza artificiale si è sviluppato un "nuovo modello di produzione della conoscenza". I dati trattati da questo nuovo modello possono essere di diverso tipo: dati personali, dati estratti da beni immateriali, dati-misura di fenomeni naturali e umani.[95]

Nel 2001, nel tentativo di spiegare e gestire il fenomeno dei *Big Data*, Douglas Laney ha elaborato il celebre modello "tridimensionale" di *data management*. Il processo di crescita conosciuto dai dati nella società dell'informazione, in particolare ai tempi dell'*e-commerce*, viene analizzato dallo studioso nelle sue tre principali dimensioni, le c.d. "3 V": Volume, Velocità e Varietà.[96] Quanto al volume, è di tutta evidenza l'aumento quantitativo del flusso di informazioni in Rete: i dati sono oggi prodotti da sorgenti eterogenee, quali i canali di comunicazione e di commercio elettronico, nonché da dispositivi e sensori connessi all'IoT. Parallelamente, si assiste a un incremento esponenziale della velocità con cui queste informazioni sono prodotte, scambiate, "stoccate" e gestite dalle aziende che operano nel digitale. Per ultimo, dall'eterogeneità delle fonti di informazione discende la varietà dei dati (immagini, video, testo, etc.).[97] Sul punto, si noti che la diversità tra i formati con cui l'informazione è rappresentata in Rete ha costituito per lungo tempo un fattore di rallentamento del trattamento e dell'elaborazione dei dati. Come Laney aveva correttamente previsto, grazie all'intelligenza artificiale e alla capacità inferenziale dei moderni algoritmi – in grado di mettere in relazione dati non strutturati e semi strutturati – il problema è stato in larga parte risolto.[98]

---

[94] Michele Iaselli, "Privacy e nuove tecnologie," in *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, a cura di Michele Iaselli (Milano: Altalex, 2016), 153.

[95] Andrea Ottolia, *Big Data e innovazione computazionale* (Torino: Giappichelli, 2017), 8-9.

[96] *Cfr.* Doug Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety* (Stamford, CT: META Group, 2001).

[97] Giovanni De Gregorio e Raffaele Torino, "Privacy, protezione dei dati personali e big data," in *Privacy digitale: Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di Emilio Tosi (Milano: Giuffrè, 2019), 455.

[98] L'attenzione, in passato, era rivolta soprattutto ai c.d. dati strutturati*,* informazioni conservate in *database* organizzati secondo schemi rigidi. L'incremento delle capacità di analisi dovuto all'impiego di algoritmi predittivi e modelli statistici consente oggi di sfruttare anche i dati non strutturati*,* ossia quei dati che non seguono alcuno schema predefinito. La rivoluzione dei *Big Data* si sostanzia proprio in questo. De Gregorio e Torino, 455

Più di recente, nel tentativo di definire i *Big Data*, in letteratura si è proposto di prendere in considerazione le "nuove" dimensioni del dato, aggiungendo ulteriori "V" al modello di Laney. Il principale pregio di queste proposte sta proprio nell'attenzione posta sulla *Big Data analytics*, e cioè sull'applicazione dell'IA predittiva e dei modelli statistici ai dati. È grazie all'intelligenza artificiale, infatti, che è oggi possibile trasformare i dati in Valore (quarta "V"), informativo ed economico.[99] Il *focus*, dunque, si sposta dall'aspetto quantitativo (su cui si concentrava il modello tridimensionale delle "3 V") a quello qualitativo.[100] In questo contesto, estendendo la lente d'indagine all'intelligenza artificiale, rileva anche la Veridicità del dato (quinta "V"). Si è visto come il dato di qualità consenta di scongiurare l'effetto "*garbage in*, *garbage out*", riducendo l'incertezza nei risultati degli algoritmi, compresi quelli di *data analysis*; diversamente dagli altri, l'attributo della veridicità non indica una qualità intrinseca del fenomeno dei *Big Data*, ma è da ricollegarsi piuttosto alle esigenze di regolazione circa la qualità dei dati, il cui controllo è reso sempre più complesso dalla velocità con cui sono generati e dall'eterogeneità delle fonti di produzione.[101]

L'impiego dell'intelligenza artificiale ha quindi spostato l'attenzione dal dato in sé alle tecniche che consentono di ricavarlo e valorizzarlo. L'eco di questo spostamento, per altro, è riscontrabile anche nella definizione di *Big Data* fornita dal regolatore europeo, segnatamente dallo *European Data Protection Supervisor* (EDPS):

> Big Data refers to the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions. Big data relies not only on the increasing ability of technology to support the collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data.[102]

---

[99] Antonio Perrucci, "Dai Big Data all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche," *Analisi Giuridica dell'Economia* 1 (giugno 2019): 69, doi:10.1433/94545. L'autore riporta la definizione di *Big Data* elaborata da De Mauro, Greco e Grimaldi: "Big Data sono l'asset di informazioni caratterizzato da un volume, una velocità ed una varietà tali da richieder specifiche tecnologie e metodi analitici per la trasformazione in valore." Andrea De Mauro, Marco Greco e Michele Grimaldi, "A Formal Definition of Big Data Based on Its Essential Features," *Library Review* 65, n. 3 (marzo 2016): 122, doi:10.1108/LR-06-2015-0061.

[100] De Gregorio e Torino, "Privacy, protezione dei dati personali e big data," 455-456.

[101] Peluso, *Intelligenza artificiale,* 25.

[102] European Data Protection Supervisor, *Opinion 7/2015: Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability*, 19 novembre 2015.

Alla luce di quanto sin ora esposto, si condivide qui la definizione di *Big Data* elaborata da De Gregorio e Torino: ponendo l'accento sulle capacità inferenziali dell'IA, i due autori sostengono sia possibile utilizzare il termine per riferirsi a "un insieme di dati e procedure finalizzate ad ottenere 'informazioni da informazioni'".[103] Tra le sopracitate procedure sono di particolare interesse quelle di "*data mining*", termine traducibile in italiano come "estrazione di dati" o "attività estrattiva di dati".[104] Diversamente dai metodi tradizionali di analisi, attraverso il *data mining* gli algoritmi individuano *pattern* e relazioni statistiche in un *set* di dati (solitamente "grezzi", o non strutturati); il processo di scoperta di schemi utili viene automatizzato, e l'insieme delle relazioni scoperte viene chiamato "modello". Il modello, poi, potrà successivamente essere utilizzato per automatizzare a sua volta processi di classificazione di altre attività di interesse, prevedere esiti futuri e stimare il valore di variabili non osservate.[105]

Può forse intuirsi, allora, perché i dati siano oggi considerati un "*input* fondamentale dell'intero sistema economico",[106] al punto da essere stati definiti il "nuovo petrolio".[107] La metafora ha riscosso un grande successo e la sua attrattività è da ricercarsi nel fatto che, similmente a un combustibile fossile digitale, i dati sono "estratti" dalla rete e destinati a fare da "carburante" ai sistemi di intelligenza artificiale.[108] A ben vedere, la grande disponibilità di dati sul Web è proprio ciò che ha reso possibile l'IA per come la conosciamo oggi: una tecnologia *data-driven*, il cui comportamento "intelligente" è da attribuirsi in larga parte alla capacità degli algoritmi predittivi di scoprire regolarità statistiche nei loro *dataset*.[109] Ma i dati, al di là dell'impiego che può esserne fatto per

---

[103] De Gregorio e Torino, "Privacy, protezione dei dati personali e big data," 458.
[104] Giuseppe Contissa, *Information Technology for the Law* (Torino: Giappichelli, 2017), 106.
[105] Enza Pellecchia, "Privacy, decisioni automatizzate e algoritmi," in *Privacy digitale: Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di Emilio Tosi (Milano: Giuffrè, 2019), 422.
[106] Peluso, *Intelligenza artificiale,* 48.
[107] La metafora gode di grandissima notorietà ed è spesso riportata negli articoli di stampa internazionale che si occupano della materia. Viene generalmente attribuita al matematico Clive Humby. *Cfr.* Charles Arthur, "Tech Giants May Be Huge, but Nothing Matches Big Data," *The Guardian*, 23 agosto 2013, https://www.theguardian.com/technology/2013/aug/23/tech-giants-data.
[108] Roberta Angelini, "Intelligenza artificiale e governance. Alcune riflessioni di sistema," in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti (Torino: Giappichelli, 2018), 296.
[109] Come si avrà modo di illustrare nei paragrafi 2 e 2.1 di questo capitolo, l'approccio "basato sui dati" costituì un vero e proprio cambio di paradigma nella storia dell'intelligenza artificiale. Il *paper*-manifesto

"addestrare" i sistemi di intelligenza artificiale, sono anche un prodotto in sé, un efficace strumento d'analisi dotato di valore proprio.[110] Si pensi alla maggior parte dei servizi digitali "gratuitamente" disponibili in Rete: la vera occasione di guadagno per i fornitori è da ricercarsi nella raccolta e nello sfruttamento dei dati degli utenti, al fine di permettere la realizzazione di pubblicità mirata.[111]

Il valore economico del dato, quindi, non starebbe solo nell'essere "nutrimento" della macchina, ma anche nella possibilità che questa lo trasformi in conoscenza operativa. L'algoritmo opera sulle "tracce umane" lasciate dai naviganti in Rete elaborandole attraverso la "profilazione", una tecnica di trattamento dei dati personali volta a ricostruire il profilo individuale degli utenti. L'algoritmo è in grado di classificare gli utilizzatori del servizio, prendendo in considerazione la loro attitudine al consumo, la capacità di spesa, le preferenze e gli interessi, per poi raggrupparli in *clusters* tramite l'incrocio e l'associazione dei dati con quanto dedotto in precedenza dal sistema.[112] Tale tecnica si è rivelata particolarmente efficace non solo in ambito commerciale, aprendo la strada alla pubblicità mirata e all'offerta di servizi personalizzati ai naviganti *on-line*, ma anche nella realizzazione di campagne di *microtargeting* politico.[113]

---

dei ricercatori di Google "L'irragionevole efficacia dei dati", pubblicato nel 2009, formalizzò per la prima volta la "nuova ricetta" dell'AI, lodando le potenzialità dei *Big Data* nella creazione delle macchine intelligenti e codificando molte delle pratiche innovative che si stavano diffondendo nel settore. *Cfr.* Alon Halevy, Peter Norvig e Fernando Pereira, "The Unreasonable Effectiveness of Data," *IEEE Intelligent Systems* 24, n. 2 (marzo 2009): 8-12, doi:10.1109/MIS.2009.36.
Guardando all'oggi, è interessante notare come tutte le più recenti applicazioni di intelligenza artificiale che richiedono modelli statistici di linguaggio funzionino bene solo quando i dati usati per l'addestramento eccedono il miliardo di parole, da cui lo slogan "La vita inizia a un miliardo di esempi". Per una ricostruzione storica sul cambio di paradigma verificatosi nel campo dell'intelligenza artificiale, *vedi* Nello Cristianini, *La scorciatoia: Come le macchine sono diventate intelligenti senza pensare in modo umano* (Bologna: Il Mulino, 2023).

[110] Peluso, *Intelligenza artificiale,* 48.

[111] Alberto De Franceschi, "Il 'pagamento' mediante dati personali," in *I dati personali nel diritto europeo*, a cura di Vincenzo Cuffaro, Roberto D'Orazio e Vincenzo Ricciuto (Torino: Giappichelli, 2019), 1397.

[112] Alberto M. Gambino, "Piattaforme, IA e data sharing: premessa," in *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce (Torino: Giappichelli, 2023), 77.

[113] Per un approfondimento sull'impatto delle tecniche di profilazione sui processi politici, si rimanda a Torchia, *Lo Stato Digitale*, 37-39.

Ecco spiegato come il "dato profilato" sia diventato il bene economico per eccellenza dell'ecosistema digitale,[114] nonostante venga ricavato – quasi sempre – in maniera indiretta, rappresentando "un'esternalità" derivante dall'accesso degli utenti a servizi digitali gratuiti, come i *social network* e i motori di ricerca.[115] È bene ribadire che questo modello di *business* non si basa sull'acquisizione dei dati personali di un singolo utente, ma anzi trova la sua forza economica nei grandi numeri, nell'aggregazione di dati riconducibili a un ampissimo gruppo di utilizzatori.[116] Il paragone con il petrolio, sebbene suggestivo, appare comunque imperfetto: i dati non si consumano con il loro utilizzo, e anzi il loro valore aggiunto è dato proprio dalla capacità di analizzare *dataset* in continua crescita e sempre disponibili.[117] A ciò si aggiunga che in dottrina non sono mancati parallelismi tra i dati e i beni pubblici: l'informazione incapsulata nel dato, in quanto bene "osservabile", potrebbe considerarsi bene non escludibile, consumabile congiuntamente e dunque non rivale.[118]

Emerge dunque, alla luce di quanto si è avuto modo di illustrare, la duplice dimensione del dato personale: da un lato, *asset* economico fondamentale della nuova *data-driven economy*, dall'altro, in virtù del suo collegamento all'individuo, oggetto di tutela.[119] Del resto, se il diritto alla privacy e la tutela dei dati personali sono oggi riconosciuti come diritti fondamentali dell'individuo lo si deve in primo luogo

---

[114] La "metafora biologica" dell'ecosistema digitale è da attribuirsi a Fransman, 2010, che la impiega per descrivere il fenomeno di convergenza delle tecnologie e dei mercati dell'informazione e della comunicazione. *Vedi* Martin Fransman, *The New ICT Ecosystem: Implications for Policy and Regulation* (Cambridge: Cambridge University Press, 2010).
Prendendo le mosse da questo contributo, nonché da alcune pionieristiche relazioni dell'Autorità per le Garanzie nelle Comunicazioni (AGCom) al Parlamento italiano, Perrucci propone un'aggiornata ricostruzione teorica del fenomeno. Un ecosistema digitale "avanzato", che tiene conto del ruolo delle nuove tecnologie (*big data*, algoritmi, intelligenza artificiale e *blockchain*) e della pluralità di soggetti che vi interagiscono, includendo tra questi ultimi le Istituzioni (Parlamento e Governo, Autorità amministrative indipendenti e Giustizia Amministrativa). *Vedi* Perrucci, "Dai Big Data all'ecosistema digitale".

[115] Antonio Nicita, "Il dato profilato nella prospettiva economica tra privacy, propertization, secrecy," in *I dati personali nel diritto europeo*, a cura di Vincenzo Cuffaro, Roberto D'Orazio e Vincenzo Ricciuto (Torino: Giappichelli, 2019), 1169.

[116] Gambino, "Piattaforme, IA e data sharing," 80.

[117] Filomena Maggino e Gabriele Cicerchia, "Algoritmi, etica e diritto," *Il diritto dell'informazione e dell'informatica* 35, n. 6 (2019): 1161.

[118] Nicita, "Il dato profilato nella prospettiva economica," 1166-1167; Per alcune criticità legate a tale qualificazione *cfr.* Peluso, *Intelligenza artificiale*, 50.

[119] De Gregorio e Torino, "Privacy, protezione dei dati personali e big data," 459.

all'evoluzione normativa comunitaria. Come evidenziato in letteratura, in Europa il diritto alla privacy, pur partendo dall'influenza americana del *right to be alone*, ha conosciuto un'evoluzione autonoma verso la fine del XX secolo,[120] anche sulla spinta delle sfide poste dalle nuove tecnologie. La capacità degli algoritmi di trattare grandi quantità di dati in modo automatizzato ha reso insufficiente la tradizionale impostazione negativa del diritto alla riservatezza, richiedendo una tutela aggiuntiva estesa ai dati personali:[121] il diritto del soggetto di esercitare un controllo, attivo, sui dati che a lui si riferiscono, dall'accesso alla rettifica.[122] Con l'entrata in vigore del Trattato di Lisbona, nel 2009, viene riconosciuta la natura vincolante della Carta di Nizza, i cui articoli 7 e 8, congiuntamente all'art. 16 del TFUE, forniscono la base della tutela costituzionale del rispetto della vita privata e familiare e della protezione dei dati personali nell'Unione Europea.[123]

La tensione tra il dato come *asset* economico e il dato personale come oggetto di tutela è riscontrabile, per altro, sin dalle prime comunicazioni con cui la Commissione Europea si è occupata del digitale. La Strategia per il Mercato Unico Digitale, inaugurata nel 2015 dalla Commissione, ha individuato il più importante presupposto per il funzionamento di un'economia digitale all'interno dell'Unione: la rimozione delle barriere digitali che non esistono nel Mercato Unico "fisico". Il perseguimento di un tale obiettivo non può che passare attraverso una regolazione innovativa che tenga conto delle caratteristiche specifiche del digitale.[124] Il Mercato Unico Digitale, dunque, nelle parole

---

[120] Sull'evoluzione storica del diritto alla privacy nel contesto europeo si rimanda a Sergio Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali* (Padova: Cedam, 2006).

[121] De Gregorio e Torino, "Privacy, protezione dei dati personali e big data," 460.

[122] Giusella Finocchiaro, *Intelligenza artificiale. Quali regole?* (Bologna: Il Mulino, 2024), 72. Sul punto l'autrice cita efficacemente Rodotà, il quale definiva la protezione dei dati personali una "libertà positiva".

[123] De Gregorio e Torino, 461-462. Come riportato dai due autori, la giurisprudenza della Corte di Giustizia ha assunto un ruolo fondamentale nel processo di consolidazione costituzionale del diritto alla tutela dei dati, riconoscendone l'autonomia per la prima volta nel caso *Promusicae*: : "Tuttavia, occorre rilevare che nella controversia in relazione alla quale il giudice del rinvio ha sollevato tale questione risulta coinvolto, oltre ai due suddetti diritti, anche un altro diritto fondamentale, vale a dire quello che garantisce la tutela dei dati personali e, quindi, della vita privata" (punto 63). Corte di Giustizia dell'Unione Europea, causa C-275/06, *Promusicae*, ECLI:EU:C:2008:54.

[124] Mirela Mărcuţ, *Crystalizing the EU Digital Policy: An Exploration into the Digital Single Market* (Cham: Springer, 2017), 52.

della Commissione, da un lato dovrà "costruire l'economia dei dati",[125] eliminando gli ostacoli tecnici e normativi che ne impediscono la fioritura e assicurando l'interoperabilità e la portabilità dei dati tra i servizi, dall'altro, dovrà garantire "un livello elevato di protezione dei consumatori e dei dati personali".[126] Questa duplice finalità caratterizza anche i successivi interventi normativi del legislatore europeo, compreso il GDPR, che della Strategia per il Mercato Unico Digitale rappresenta una tappa fondamentale. Già dall'art. 1 il Regolamento palesa la sua "duplice anima",[127] con un riferimento espresso al raggiungimento di due obiettivi: garantire la protezione delle persone fisiche rispetto al trattamento dei dati personali e, al tempo stesso, assicurare la libera circolazione degli stessi.[128] Il considerando n. 4 chiarisce poi che il diritto alla protezione dei dati personali non è assoluto, ma deve essere contemperato con gli altri diritti fondamentali, in ottemperanza al principio di proporzionalità e alla luce della sua funzione sociale.[129]

Sebbene il GDPR sia generalmente considerato in dottrina una normativa avanzatissima, ambiziosa e meritoria, il modello del consenso al trattamento dei dati personali introdotto dal Regolamento del 2016 ha mostrato nel tempo diverse criticità, in particolare con riguardo all'efficacia sostanziale della tutela preposta. A tal proposito, il modello del consenso è stato definito, ricorrendo a un'elegante metafora, un "vaso di cristallo fragile e dal contenuto eterodeterminato".[130] Un vaso che, ad avviso di chi scrive, rischia di creparsi ulteriormente a contatto con l'intelligenza artificiale. Nonostante l'IA non sia mai esplicitamente menzionata nel GDPR, infatti, diverse disposizioni del

---

[125] Commissione Europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, 15.
[126] Commissione Europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, 3.
[127] Peluso, *Intelligenza artificiale*, 90.
[128] Regolamento (UE) 2016/679, art. 1: "1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".
[129] Peluso, *Intelligenza artificiale*, 92.
[130] Bruno Carotti, "La politica europea sul digitale: ancora molto rumore," *Rivista trimestrale di diritto pubblico* 72, n. 4 (2022): 999. L'autore sottolinea come il consenso sia spesso prestato dall'interessato "in modo inconsapevole e quasi automatico", mentre "la lettura delle privacy policy è pressoché impossibile: il numero di pagine da leggere per comprendere le principali applicazioni in uso dagli utenti è stato valutato in un milione".

Regolamento risultano applicabili alle nuove tecnologie, e parte di quanto disposto è oggi messo in discussione dal modo in cui l'intelligenza artificiale ha reso possibile trattare i dati personali. Si registra una tensione tra i principi posti dal GDPR, tra cui la limitazione delle finalità del trattamento, la minimizzazione dei dati, le limitazioni alle decisioni automatizzate, e il potenziale offerto dai sistemi di IA e dalla *big data analytics*.[131] Un ulteriore elemento di complessità, poi, è oggi rappresentato dall'AI Act: i profili di convergenza tra i due regolamenti sono molteplici e il loro rapporto è ancora in attesa di essere indagato a fondo dalla dottrina e dalle autorità di regolazione di settore. Sebbene l'art. 2, paragrafo 7 dell'AI Act ribadisca che "il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento" e che quest'ultimo lascia impregiudicato quanto previsto dal GDPR,[132] il rischio che la nuova normativa possa trovare difficoltà applicative in sede di individuazione delle basi legali necessarie a giustificare il trattamento di dati personali, sia nella fase di allenamento delle tecnologie di IA che nelle fasi della loro utilizzazione, sembrerebbe ancora non del tutto scongiurato.[133]

La presente trattazione non si concentrerà sul tema, pur rilevantissimo, del delicato rapporto tra GDPR e AI Act, sebbene si avrà modo di accennare a diversi profili d'interesse al riguardo. Al momento, basti sottolineare come il legislatore europeo abbia mostrato, negli ultimi anni e successivamente al GDPR, una sempre maggiore attenzione alla dimensione economica del dato e all'indissolubile rapporto che lo lega all'intelligenza artificiale, tecnologia *data-driven* per eccellenza.

---

[131] STOA - Panel for the Future of Science and Technology, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence* (Bruxelles: European Parliamentary Research Service, giugno 2020), II. Per una puntuale analisi, precedente all'*AI Act*, delle sfide poste dall'AI alla disciplina della protezione dei dati personali, *vedi* Franco Pizzetti, "La protezione dei dati personali e la sfida dell'Intelligenza Artificiale," in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti (Torino: Giappichelli, 2018), 5-187.

[132] Regolamento (UE) 2024/1689, art. 2, par. 7: "Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento".

[133] Franco Pizzetti, "AI, in Europa troppe regole? Pizzetti: 'Ecco i nodi da chiarire'," *Agenda Digitale*, 23 settembre 2024, https://www.agendadigitale.eu/sicurezza/privacy/ai-in-europa-troppe-regole-pizzetti-ecco-i-nodi-da-chiarire/.

Quanto si afferma emerge con chiarezza dalla Strategia Europea per i Dati del 2020,[134] che ha posto le basi per una *data-driven economy* competitiva a livello internazionale. Il *focus* della strategia sta proprio nell'accelerazione dei processi di transizione digitale, tramite il potenziamento dell'*e-commerce*, lo sviluppo di *database* pubblici, la promozione della *data literacy* e il miglioramento delle infrastrutture tecnologiche.[135] Del medesimo anno è poi il Libro Bianco sull'Intelligenza Artificiale,[136] con il quale la Commissione sottolinea come l'IA rappresenti una delle applicazioni più rilevanti della *data economy*, in un contesto che vede l'Europa in una posizione di debolezza rispetto ai principali attori internazionali per quanto riguarda le applicazioni destinate ai consumatori e le piattaforme online, debolezza che si traduce in uno svantaggio competitivo nell'accesso ai dati.[137] È tuttavia proprio il Libro Bianco a far notare come la crescita esponenziale dei dati ("nuova ondata di dati" o *Data Wave*) rappresenti un'importante opportunità per l'Unione Europea di farsi spazio nella *data economy* e affermarsi come *leader* del settore.[138] Da ultimo, è nel contesto della Strategia per i Dati che si inseriscono due recenti regolamenti intersettoriali: il *Data Governance Act* (Regolamento (UE) 2022/868) e il *Data Act* (Regolamento (UE) 2023/2854).[139] Mentre il *Data Act st*abilisce norme armonizzate per garantire un accesso equo ai dati e il loro utilizzo nell'ambito dell'IoT, rimuovendo le barriere che ostacolano il funzionamento del mercato unico, il *Data Governance Act* costituisce un tassello fondamentale del mosaico regolatorio europeo del digitale, ponendosi come punto di contatto tra la regolazione dell'economia dei dati, dell'intelligenza artificiale e delle

---

[134] Commissione Europea, *Una strategia europea per i dati*, COM(2020) 66 final.
[135] Peluso, *Intelligenza artificiale*, 76-78.
[136] Commissione Europea, *Libro Bianco sull'intelligenza artificiale: Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final. Da ora in avanti anche "Libro Bianco".
[137] Commissione Europea, *Libro Bianco*, 4.
[138] Commissione Europea, *Libro Bianco*, 4-5. Il quadro tracciato dalla Commissione non è negativo. Questa si mostra piuttosto ottimista riguardo le capacità europee di cogliere le potenzialità della *data economy*, evidenziando come l'Unione sia *leader* mondiale dell'elettronica a basso consumo, e allo stesso tempo all'avanguardia sul *quantum computing*, grazie all'alto livello accademico della ricerca sul campo.
[139] 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*), GUUE L 152, 3 giugno 2022. 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*), GUUE L, 22 dicembre 2023.

piattaforme online.[140] Il principio ispiratore del Regolamento è la *data monetization,* e può essere riassunto nell'espressione "dati uguale valore economico".[141] È con questo tassello finale, dunque, che il modello europeo di regolazione dei dati giunge alla sua versione più aggiornata: una regolazione a finalità plurima, che da un lato guarda all'interno, realizzando il mercato unico per i dati, dall'altro all'esterno, tentando di recuperare un posizionamento europeo nel mercato mondiale delle tecnologie digitali.[142]

Una nota conclusiva: come emerso nel corso di questa trattazione, difficilmente l'analisi del fenomeno dei *Big Data* potrebbe ignorare la connessione che intercorre tra dati e algoritmi o tra dati e piattaforme digitali. Un così intimo legame non poteva, parimenti, essere ignorato dal legislatore europeo. La logica dietro i numerosi interventi dell'Unione sul digitale, il "*fil rouge*" che collega i principali strumenti regolatori europei, è da ricercarsi proprio nella sequenza dato-algoritmo-piattaforma: il *Data Act* e il *Data Governance Act* si concentrano sulla circolazione e il riutilizzo dei dati; l'AI Act, insieme al GDPR, disciplina l'utilizzo e la messa in commercio degli algoritmi, garantendone la compatibilità con i diritti fondamentali europei; il *Digital Markets Act* (DMA) e il *Digital Services Act* (DSA) regolano le piattaforme, tutelando il funzionamento del mercato e gli interessi dei terzi.[143] Sebbene gli ultimi due regolamenti esulino dall'oggetto del presente lavoro, attraverso il loro richiamo si vuole sottolineare come la strategia europea rappresenti un modello complesso, senz'altro perfettibile, eppure coerente e integrato.

2. Definire l'IA: i confini sfumati dell'oggetto di regolazione

La prima difficoltà che incontra l'operatore del diritto che si avvicina al tema della *governance* dell'Intelligenza Artificiale è senz'altro rappresentata dall'ineludibile necessità di definire l'oggetto della regolazione.

---

[140] Antonio Iannuzzi, "I regolamenti intersettoriali per l'istituzione dei 'data spaces': Data Governance Act *e* Data Act," in *La regolazione europea della società digitale*, a cura di Franco Pizzetti (Torino: Giappichelli, 2024), 107 e 123.

[141] Iannuzzi, 108.

[142] Iannuzzi, 107.

[143] Nicola M.F. Faraone, "Chi prima arriva [forse non] primo alloggia: questioni aperte in tema di concorrenza e regolamentazione ex-ante nei mercati digitali," in *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce (Torino: Giappichelli, 2023), 114-115.

Cosa s'intende per "Intelligenza Artificiale" è infatti, sin dalle origini della materia, oggetto di intenso dibattito tra gli studiosi.[144] Il campo di ricerca è molto vasto e le possibili prospettive da cui affrontarlo sono molteplici.[145] La questione, del resto, coinvolge e interseca diversi ambiti del sapere, va oltre la scienza delle macchine, la matematica e la fisica; pone interrogativi la cui risposta va ricercata di volta in volta nella linguistica, nelle scienze cognitive, nel sapere filosofico.[146]

Elaborare una definizione esauriente dell'IA, inoltre, impone un'operazione di ancora maggiore difficoltà: interrogarsi su cosa sia l'intelligenza *non* artificiale, più specificamente su cosa sia e come si manifesti l'intelligenza *naturale*, nonché stabilire se questa sia o non sia attributo esclusivo dell'umanità. Sul punto, la riflessione filosofica può dirsi secolare, se non millenaria,[147] e ciò che rileva in questa sede è che all'epoca delle scienze cognitive contemporanee non esiste una definizione unica di intelligenza, ma piuttosto diverse descrizioni di un insieme di capacità che ne valorizzano la "natura multidimensionale"[148]. Nella felice metafora culinaria di Floridi, "comprensione, consapevolezza, acume, sensibilità, preoccupazioni, sensazioni, intuizioni, semantica, esperienza, bio-incorporazione, significato, persino saggezza" diventano tutti "ingredienti" che contribuiscono a creare l'intelligenza umana.[149]

---

[144] La paternità del termine è comunemente attribuita a John McCharty, autore, nel 1955, della celebre proposta di seminario estivo per la ricerca sull'intelligenza artificiale, poi tenutosi al Dartmouth College di Hannover. Il seminario fu organizzato allo scopo di riunire i maggiori esponenti della disciplina, al tempo ancora chiamata "simulazione computazionale", e prese le mosse a partire dalla "congettura che ogni aspetto dell'apprendimento, e qualsiasi altra caratteristica dell'intelligenza, possa in linea di principio essere descritto così precisamente da poter costruirci una macchina per simularlo". John McCarthy, Marvin L. Minsky, Nathaniel Rochester e Claude E. Shannon, "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 31 August 1955," *AI Magazine* 27, n. 4 (dicembre 2006): 12.

[145] Peluso, *Intelligenza artificiale*, 1.

[146] Michele Iaselli, "Le origini dell'IA, evoluzione e rapporti con il diritto," in *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli (Rimini: Maggioli, 2024), 13.

[147] De Anna evidenzia come già Platone, prima ancora del sillogismo aristotelico, tracciasse una differenza tra diversi tipi d'intelligenza: *nous*, la capacità di cogliere l'essenza delle cose, e *dianoia*, intesa come capacità di ragionamento deduttivo inferenziale. Gabriele De Anna, "Automi, responsabilità e diritto," *Rivista di filosofia del diritto, Journal of Legal Philosophy 1* (giugno 2019): 128, doi: 10.4477/93370. Sul punto, di grande interesse anche la figura di Cartesio, definito come "l'antesignano della scienza cognitiva e dell'Intelligenza Artificiale", *cfr.* Bruno G. Bara, *Il metodo della scienza cognitiva. Un approccio evolutivo allo studio della mente* (Torino: Bollati Boringhieri, 2000).

[148] Iaselli, "Origini dell'IA", 15.

[149] Luciano Floridi, *Etica dell'intelligenza artificiale: Sviluppi, opportunità, sfide* (Milano: Raffaello Cortina, 2022), 52.

La parola "intelligenza", dunque, nella filosofia delle menti appare "sfumata" e foriera di incertezze già nella sua accezione *naturale*, quando è riferita all'uomo e non alla macchina. Queste incertezze finiscono poi per aumentare di numero e intensità nel momento in cui si decide di accoppiarla all'aggettivo "artificiale*"*.

L'intelligenza, d'altronde, è comunemente attribuita agli esseri umani (o tutt'al più agli animali) e ciò finisce inevitabilmente per condizionare, sin da principio, il discorso intorno alle applicazioni di IA in termini antropomorfici.[150] Sempre più spesso si avvicendano nella sfera pubblica parole altisonanti: macchine intelligenti, algoritmi che *imparano*, robot che minacciano l'occupazione. Questa "irrefrenabile tendenza all'antropomorfizzazione" non è soltanto un "gioco delle etichette" o un'operazione commerciale, ma ha ragioni profonde, è figlia dei nostri limiti conoscitivi e ci porta a proiettare sulle macchine la migliore intelligenza a noi conosciuta, quella umana.[151] Questa operazione di proiezione, tuttavia, non è esente da rischi. A ben vedere, sono molte le parole utilizzate per descrivere i sistemi di intelligenza artificiale che appaiono suggestive e tutt'altro che neutre, contribuendo a sviluppare sul tema una narrazione personalizzante e mitizzante, che va oltre la semplice antropomorfizzazione e attinge direttamente dall'immaginario dell'occulto e del fantastico.[152]

Questo non deve stupire: l'idea che un "artificio" dell'uomo possa manifestare un comportamento intelligente, sino a giungere al punto di sfuggire al controllo del suo stesso creatore, è un archetipo ricorrente nel canone della letteratura occidentale e ha sempre goduto di grande fortuna; in tempi più recenti non sono mancate rielaborazioni in chiave contemporanea, con riferimenti al mondo della robotica e dell'intelligenza artificiale.[153]

---

[150] Finocchiaro, *Intelligenza artificiale*, 23.

[151] Amedeo Santosuosso, "Forum: Law and Artificial Intelligence. Questioni definitorie," *BioLaw Journal – Rivista di BioDiritto* 1 (marzo 2020): 470. In senso fortemente critico verso la rivoluzione digitale e l'antropomorfizzazione delle macchine, *cfr.* Éric Sadin*, Critica della ragione artificiale. Una difesa dell'umanità* (Roma: LUISS University Press, 2019).

[152] A titolo esemplificativo, si parla frequentemente, oltre che di "intelligenza": di "oracolo", per riferirsi ai sistemi di intelligenza artificiale che, interrogati dall'utente, forniscono risposte sulla base di dati che hanno elaborato; di "allucinazioni", con riferimento agli esiti errati delle elaborazioni del sistema; di "incantesimi", descrivendo quei *prompt* (*id est* inserzioni o *input* dell'utente) che consentono di aggirare le limitazioni e i divieti di ChatGPT e chatbot analoghi. Finocchiaro, *Intelligenza artificiale*, 23.

[153] Caselli trova un'espressione significativa di tale archetipo nel "paradigma dell'apprendista-stregone" e rinviene nella figura del *golem* della letteratura ebraica altomedievale una delle sue prime ricorrenze.

Al fine di sfrondare il campo di discussione da fraintendimenti, nel tentativo di impostare un dialogo che abbandoni retoriche suggestive e metafore mitologiche in favore di una terminologia tecnica e per quanto possibile "neutra", si è proposto di utilizzare il termine *Machine Learning* (ML) in luogo di "Intelligenza Artificiale".[154] Gran parte di ciò che oggi il dibattito pubblico e la pubblicità commerciale chiamano comunemente "IA", infatti, altro non è che il risvolto applicativo di algoritmi di *machine learning*.[155] L'impiego di questo termine ha l'indiscutibile merito di spogliare l'intelligenza artificiale di quell'abito di mistero e fascinazione di cui – con frequenza sempre maggiore negli ultimi anni – va vestendosi, riportando il discorso su un piano tecnico, forse meno suggestivo ma senz'altro più intelligibile.

Il *machine learning* è una branca dello studio dell'intelligenza artificiale,[156] un "termine ombrello" che include tutti quegli algoritmi in grado di formulare previsioni (ma anche descrizioni e prescrizioni) sulla base di un set di dati, solitamente di grandissime dimensioni.[157] La sua popolarità è tale che gli algoritmi di *machine learning* sono stati più volte definiti come la tecnologia chiave della quarta rivoluzione industriale, o "*Industry 4.0*", in grado di consentire l'analisi intelligente di dati e lo sviluppo di applicazioni pratiche a partire da questi.[158] Il termine, di evidente derivazione anglosassone, è spesso reso in lingua italiana con la traduzione non letterale di "apprendimento automatico", descrivendo quell'insieme di tecniche e metodi di allenamento che consentono alla macchina di apprendere in modo automatico, e cioè,

---

Antonio Caselli, "Dagli artifici dell'intelligenza all'Intelligenza Artificiale," in *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti (Torino: Giappichelli, 2018), 193. Su come il tema sia stato rielaborato nelle arti moderne e contemporanee, *vedi anche* Quintarelli, *Intelligenza artificiale*, 14-20.

[154] Finocchiaro, *Intelligenza artificiale*, 23.

[155] Michael I. Jordan, "Artificial Intelligence—The Revolution Hasn't Happened Yet," *Harvard Data Science Review* 1, n. 1 (luglio 2019), doi:10.1162/99608f92.f06c6e61.

[156] Per un'introduzione tecnica ma accessibile alle basi del *machine learning*, *vedi* Alexander Jung, *Machine Learning: The Basics* (Singapore: Springer, 2022). Il testo fornisce una panoramica completa e di settore sui principali concetti alla base del ML.

[157] James A. Nichols, Hsien W. Herbert Chan, e Matthew A. B. Baker, "Machine Learning: Applications of Artificial Intelligence to Imaging and Diagnosis," *Biophysical Reviews* 11, n. 1 (febbraio 2019): 111-118, https://doi.org/10.1007/s12551-018-0449-9.

[158] Iqbal H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science* 2, n. 160 (marzo 2021), doi:10.1007/s42979-021-00592-x. Sul rapport tra quarta rivoluzione industrial e AI, *cfr.*. Beata Ślusarczyk, "Industry 4.0—Are We Ready?," *Polish Journal of Management Studies* 17, n. 1 (giugno 2018): 232-248, doi:10.17512/pjms.2018.17.1.19.

ricorrendo a un'efficace semplificazione, senza richiedere una programmazione per singole strisce di comando.[159] La macchina diventa così in grado di compiere osservazioni e valutazioni, migliorando le proprie prestazioni nei compiti futuri.[160]

L'interesse giuridico per il tema dell'intelligenza artificiale si è principalmente soffermato proprio su detti algoritmi, con particolare attenzione al *deep learning* e alle reti neurali artificiali.[161] È questa infatti la tecnologia alla base di gran parte dei sistemi di IA con cui interagiamo ogni giorno, talvolta persino in maniera inconsapevole: si pensi agli algoritmi di raccomandazione che influenzano i contenuti che visualizziamo sui *social network* o che scelgono quali prodotti consigliarci sui mercati digitali, ai filtri anti-spam delle nostre caselle email, ai sistemi di navigazione GPS, ai programmi di traduzione automatica e di riconoscimento vocale, alle automobili a guida autonoma.[162] Sono poi sempre le reti neurali – e dunque il *machine learning* – alla base del

---

[159] Peluso, *Intelligenza artificiale,* 25.

[160] Contissa, *Information Technology for the Law*, 107.

[161] Peluso, *Intelligenza artificiale,* 25. Le reti neurali artificiali, come si vedrà, differiscono dai modelli di intelligenza artificiale "tradizionale" (sistemi esperti). Le reti non conoscono le regole, ma attraverso un algoritmo di apprendimento si modellano, così da comportarsi "come se" le conoscessero. Il loro funzionamento simula quello del cervello umano, replicandone l'organizzazione: i neuroni artificiali, in modo simile a quelli biologici, calcolano il segnale in uscita come funzione della differenza fra il prodotto dei segnali in entrata per i rispettivi "pesi sinaptici" e un valore di soglia prefissato. L'impiego di algoritmi di *backpropagation* rende possibile l'apprendimento attraverso la regolazione iterativa dei pesi sinaptici, che vengono ottimizzati per ridurre l'errore tra *output* previsto e reale. La conoscenza può quindi essere acquisita attraverso un processo *bottom-up*, e non necessita di essere immessa dall'esterno come avviene nei sistemi esperti. Il principale vantaggio fornito da una rete neurale rispetto a un sistema esperto è che, se la rete è abbastanza "robusta", è possibile inserire fra le variabili di *input* anche variabili che non hanno alcuna influenza sul fenomeno, o, viceversa, non inserire alcune variabili rilevanti; la rete è in grado di tollerare la mancanza di alcuni dati essenziali, così come è in grado di non prendere in esame (o prendere in esame nella misura dovuta) il dato non essenziale. Iaselli, "Origini dell'IA", 21-22. Quanto al *deep learning*, questo può essere considerato una sottocategoria delle reti neurali artificiali e prende il nome dall'utilizzo di reti neurali "profonde". Nel *deep learning* i neuroni artificiali sono organizzati in modo gerarchico, su diversi "livelli" (*layers*), molti dei quali nascosti. Si tratta dunque di un metodo di apprendimento attraverso più livelli di rappresentazione, ottenuti componendo moduli semplici ma non lineari, ciascuno dei quali trasforma la rappresentazione di un livello (partendo dall'*input* grezzo) in una rappresentazione a un livello superiore, leggermente più astratto. Componendo un numero sufficiente di tali trasformazioni, possono essere apprese funzioni estremamente complesse: il *deep learning* ha consentito enormi progressi nel riconoscimento vocale, nel riconoscimento di oggetti visivi e in molti altri ambiti, come la scoperta di farmaci e la genomica. Per un'introduzione ai metodi di apprendimento e all'architettura delle reti neurali dietro tale tecnologia, appare imprescindibile il riferimento a Yann LeCun, Yoshua Bengio e Geoffrey Hinton, "Deep Learning," *Nature* 521, n. 7553 (maggio 2015): 436-444, doi:10.1038/nature14539.

[162] Mobilio, "L'intelligenza artificiale", 402.

funzionamento dei *Large Language Model* (LLM),[163] di cui il *chatbot* noto come ChatGPT rappresenta oggi il più celebre applicativo software. A loro volta, i LLM sono classificabili come una tipologia di intelligenza artificiale generativa (GenAI), per tale intendendosi quell'IA che, a partire da grandi quantità di dati esistenti, utilizza la conoscenza per generare nuovi contenuti non espressamente programmati dagli sviluppatori del sistema, come immagini, musica e testo.[164]

Sebbene siano evidenti le ragioni che hanno portato la riflessione giuridica e le prime proposte regolatorie a concentrarsi sugli algoritmi di apprendimento automatico, è doveroso sottolineare che *machine learning* e *artificial intelligence* non sono termini interscambiabili. L'utilizzo del primo in luogo del secondo, ancor più se impiegato in un contesto di *drafting* normativo, può dare adito a ulteriori incertezze: il ML è un sottoinsieme dell'IA, ne rappresenta solo una piccola parte (sebbene importante) e non ne esaurisce la definizione.[165] Informatici e matematici, sin dagli albori della materia, hanno fatto ricorso all'ampio *genus* dell'intelligenza artificiale per riferirsi genericamente a tutto quanto veniva fatto rientrare nel campo della simulazione computazionale.[166] Esistono dunque diversi tipi di intelligenza artificiale, che usano diversi calcoli e algoritmi e le cui tecniche vanno al di là dell'apprendimento (proprio del *machine learning*), potendo configurarsi anche come rappresentazione (*representation*), regole (*rules*) e ricerca (*search*).[167]

---

[163] I *Large Language Model* sono modelli di intelligenza artificiale in grado, tra le altre cose, di riconoscere e generare testo. Sono addestrati su enormi set di dati, spesso milioni di gigabyte di testo (da qui il nome "Large"), e basano anch'essi il loro funzionamento sul machine learning, nello specifico sul *deep learning* e su di un tipo di rete neurale detta *transformer*. Tra le principali "famiglie" di LLM troviamo GPT di OpenAI, LLaMA di Meta e PaLM di Google, su cui si basano rispettivamente i chatbot ChatGPT, Meta AI e Bard. I recenti progressi compiuti dagli LLM che si basano sui *transformer* hanno notevolmente ampliato le loro capacità, rendendoli in grado di compiere operazioni di *problem-solving* e ragionamento sequenziale (*multi-step reasoning*). Shervin Minaee et al., "Large Language Models: A Survey," *arXiv*, n. arXiv:2402.06196 (febbraio 2024), https://arxiv.org/abs/2402.06196.

[164] L'intelligenza artificiale generativa è in grado di imitare la creatività umana, e rappresenta oggi uno strumento prezioso in diversi settori, tra cui il gioco, l'animazione e la progettazione di prodotti. Si è dimostrata particolarmente utile anche nel campo della ricerca biomedica, potendo essere addestrata per la scoperta di nuove molecole e il riconoscimento di sequenze di amminoacidi. Iaselli, "Origini dell'IA", 24-26.

[165] Hannah Ruschemeier, "AI as a Challenge for Legal Regulation – The Scope of Application of the Artificial Intelligence Act Proposal," *ERA Forum* 23 (gennaio 2023): 364.

[166] Margaret Boden, *L"intelligenza artificiale* (Bologna: Il Mulino, 2019), 22.

[167] K.R. Chowdhary, *Fundamentals of Artificial Intelligence* (Heidelberg: Springer, 2020), 9.

Se da un lato nelle discipline umanistiche si è fatta ampia critica del termine "intelligenza artificiale", considerato parziale quando non inesatto, dall'altro non può negarsi come l'intelligenza umana sia stata per lungo tempo (ed è ancora) il principale metro di paragone adottato da informatici e matematici per valutare l'intelligenza della macchina.[168] È celebre a tal proposito la citazione di Marvin Lee Minsky, tra i padri fondatori della disciplina, che nel 1968 definì l'IA come "*the science of making machines do things that would require intelligence if done by men*".[169]

Nel solco tracciato da Minsky seguirono numerosi e ulteriori tentativi di definire la materia, molti dei quali contraddistinti proprio dal paragone con l'intelligenza umana. Non sono per altro mancati contrasti: l'approccio di Minsky poggia sull'idea che una "comprensione degli oggetti richieda un computer capace di pensare come una persona"[170], immaginando sistemi in grado di simulare il funzionamento del cervello umano, quanto meno nella forma di imitazione; a questo orientamento si è da sempre contrapposto un approccio che potremmo definire razionalista, che rivendica l'impiego della logica formale, della matematica e dell'ingegneria e pone l'attenzione non tanto sull'imitazione del pensiero umano, quanto sul perseguimento di un *comportamento* razionale da parte della macchina.[171]

L'indirizzo razionalista, o logicista che dir si voglia, può essere definito come l'approccio tradizionale all'intelligenza artificiale, al punto da essersi guadagnato il nostalgico appellativo di "*Good Old-Fashioned AI"* (GOFAI).[172] L'IA, così come l'informatica, deriva dalla logica, principalmente dal ragionamento deduttivo, e cioè da quell'insieme di tecniche che a partire da una o più premesse iniziali consentono di derivare delle conseguenze.[173] Per eseguire un ragionamento deduttivo, è necessario che

---

[168] Ruschemeier, "AI as a Challenge for Legal Regulation," 365.

[169] La citazione è attestata da numerose fonti bibliografiche. Tra gli altri, vedi Tom Stonier, *Beyond Information: The Natural History of Intelligence* (Londra: Springer, 1992), 107.

[170] La citazione è riportata da Peluso, *Intelligenza artificiale,* 2. Sul punto l'autrice rimanda a Kevin Warwick, *Intelligenza artificiale. Le basi*, trad. Chiara Barattieri di San Pietro e Giuseppe Maugeri (Palermo: Dario Flaccovio Editore, 2015), 26.

[171] Stuart J. Russell e Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4ª ed. (Londra: Pearson, 2020), 1-2.

[172] John Haugeland, *Artificial Intelligence: The Very Idea* (Cambridge, MA: MIT Press, 1985), 113.

[173] Maurizio Gabbrielli, "Dalla logica al *deep learning*: una breve riflessione sull'intelligenza artificiale," in *XXVI lezioni di diritto dell'intelligenza artificiale*, a cura di Ugo Ruffolo (Torino: Giappichelli, 2021), 27.

le macchine siano programmate con regole predefinite, proprie del pensiero razionale, che poi applicheranno per manipolare la conoscenza espressa mediante simboli – da qui, l'ulteriore definizione di "intelligenza artificiale simbolica".[174] L'idea alla base è che il pensiero umano possa essere formalizzato attraverso linguaggi di logica formale, senza che sia necessario simularne il funzionamento biologico: si assume che i processi mentali, come il ragionamento, la pianificazione e il *problem-solving*, possano essere rappresentati e riprodotti mediante simboli e regole.[175] Dotarsi di un "sistema di simboli fisici" diventa quindi condizione necessaria e sufficiente per riprodurre l'agire intelligente.[176] È proprio dal modello simbolico, da questo approccio tradizionale, che nascono i primi *expert system* e le prime applicazioni di IA;[177] nella sua formulazione originaria, infatti, la definizione di GOFAI ideata da Haugeland esclude tutte quelle tecniche che puntano a ricostruire nelle macchine l'architettura cerebrale, come il percettrone, le reti neurali e il *machine learning*.

---

[174] Gabbrielli, 27.

[175] Haugeland ritiene che alla base di tutte le teorie GOFAI vi siano due enunciati: "1. Our ability to deal with things intelligently is due to our capacity to think about them reasonably (including subconscious thinking); 2. Our capacity to think about things reasonably amounts to a faculty for internal 'automatic' symbol manipulation". Haugeland, *Artificial Intelligence*, 113.

[176] Gli enunciati di Haugeland riecheggiano anche nelle parole di Simon e Newell: "A physical symbol system has the necessary and sufficient means for general intelligent action". Allen Newell e Herbert A. Simon, "Computer Science as Empirical Inquiry: Symbols and Search," *Communications of the ACM* 19, n. 3 (marzo 1976): 116, doi:10.1145/360018.360022.
Lo stesso può dirsi per il "presupposto psicologico" di Dreyfus: "The mind can be viewed as a device operating on bits of information according to formal rules." Hubert Dreyfus, *What Computers Still Can't Do* (New York: MIT Press, 1979), 157.

[177] I sistemi esperti, o *expert system*, sono sistemi informatici basati sulla conoscenza. Questa è contenuta in una determinata "base", generalmente espressa in un linguaggio formale ad alto livello, e cioè in linguaggio di programmazione "vicino" a quello usato nella comunicazione umana. Un motore inferenziale è poi in grado di interpretare il contenuto della base di conoscenza ed effettuare deduzioni logiche sulla base di quanto richiesto dall'utente, che interagisce col sistema attraverso un'interfaccia. È poi presente, oltre all'interfaccia utente, un'interfaccia per il programmatore, l'autore del programma che può aggiornare e modificare la base di conoscenza. Tali sistemi sono detti "esperti" in quanto in grado di simulare il ragionamento di un esperto umano; i loro principali attribuiti sono la trasparenza (è possibile ricostruire la linea di ragionamento inferenziale seguita dalla macchina), l'euristica (l'adozione, nella risoluzione di problemi, di strategie tipiche degli esperti umani) e la flessibilità (la possibilità di modificare la base di conoscenza). Iaselli, "Origini dell'IA", 18-20. Alla base del funzionamento di un sistema esperto vi è dunque la logica formale (IF/THEN) che, in un dato dominio finito, grazie a una serie di condizioni (IF), conclusioni (THEN) e regole per la risoluzione dei conflitti, permette alla macchina di agire in modo autonomo. Peluso, *Intelligenza artificiale*, 20.

Adottando una diversa lente d'indagine, nel tentativo di dar vita a una macchina intelligente, l'orientamento c.d. connessionista (o connettivista) prende il suo nome dalle connessioni neurali proprie del cervello umano: se l'obiettivo è riprodurre il comportamento intelligente dell'uomo, sarà imprescindibile lo studio e l'imitazione della struttura del cervello, delle cellule organiche di cui si compone e delle sinapsi.[178] Un tale approccio non può che basarsi, in parte, sulle evidenze empiriche emerse dallo studio della psicologia e dei processi cognitivi.[179] È proprio in questo campo di ricerca che si sviluppano le prime teorizzazioni delle reti neurali,[180] la cui unità computazionale è rappresentata dal neurone artificiale. Il modello delle reti neurali si presenta radicalmente diverso rispetto alla classica intelligenza artificiale simbolica: i neuroni artificiali senz'altro manipolano simboli, ma lo fanno localmente, in assenza di regole generali che descrivono come modificare la conoscenza.[181] Il focus viene spostato dai linguaggi di programmazione ai dati, che grazie all'architettura del sistema consentono alla macchina di imparare in modo autonomo – da qui, il nome di "intelligenza artificiale sub-simbolica".[182] È questo il modello di funzionamento che caratterizza gran parte della "nuova IA".[183]

La distinzione tra "vecchia" e "nuova" intelligenza artificiale[184] risulta efficace ai fini espositivi e consente di ricostruire la dialettica tra i due principali orientamenti in materia, ma si scontra con due importanti limiti. Il primo è che, se è vero che l'impostazione simbolica tradizionale storicamente precede quella connessionista, è anche vero che i fondamentali di entrambi i campi di ricerca si sono sviluppati per lo più

---

[178] Contissa, *Information Technology*, 149.
[179] Russel e Norvig, *Artificial Intelligence*, 2.
[180] A Marvin Minsky e Dean Edmonds si deve la realizzazione di SNARC (*Stochastic Neural Analog Reinforcement Calculator*) intorno al 1950, il primo computer basato su una rete neurale. Il lavoro è così rivoluzionario che, quando Minsky lo presenta alla commissione valutativa per il suo dottorato di ricerca, questa si dice scettica sul se sia possibile o meno considerarlo "matematica". Secondo quanto riferito, in quell'occasione von Neumann avrebbe esclamato: "Se non lo è adesso, lo sarà un giorno". Russel e Norvig, *Artificial Intelligence*, 17.
[181] Gabbrielli, "Dalla logica al *deep learning*," 27.
[182] Gabbrielli, 27.
[183] Floridi, *Etica dell'intelligenza artificiale*, 25.
[184] Floridi, 25.

parallelamente,[185] conoscendo nella successione storica degli eventi fortune alterne e battute d'arresto. Il secondo è che il "nuovo" non ha – nel contesto attuale – sostituito il "vecchio", e anzi entrambi gli approcci, pur partendo da diverse premesse, sono oggi usati congiuntamente, in modo integrato e interoperabile.[186] L'attenzione della ricerca è volta verso la creazione di sistemi misti,[187] mentre sempre più voci autorevoli argomentano sulla necessità di far dialogare i due approcci e giungere a un IA c.d. neuro-simbolica.[188]

Un'ulteriore specificazione si rende poi necessaria con riguardo all'approccio tradizionale. Nel corso degli anni, le riflessioni della scuola razionalista non si sono limitate alla GOFAI e alla logica formale, ma hanno mostrato una crescente apertura verso tecniche mutuate da altri ambiti disciplinari, come la statistica, la psicologia cognitiva, la teoria del controllo, l'economia, la cibernetica e persino il *machine learning* e le reti neurali artificiali.[189] È da attribuire a questo orientamento l'introduzione del concetto di "agente", inteso come "qualsiasi cosa che può essere vista come in grado di percepire il suo ambiente attraverso sensori e agire su di esso tramite attuatori";[190] un agente può dirsi razionale se è in grado di agire sull'ambiente conseguendo l'obiettivo desiderato.[191] Se il risultato dei passaggi di stato dell'ambiente in conseguenza all'azione dell'agente è un risultato desiderabile, allora può dirsi che l'agente è intelligente e in grado di fare "la cosa giusta".[192] Per la teoria degli agenti, dunque, l'intelligenza può essere definita come "la capacità di un sistema di agire in modo appropriato in un ambiente incerto, dove le azioni

---

[185] Risale al 1943 il primo modello di neurone artificiale elaborato da McCulloch e Pitts. Warren S. McCulloch e Walter H. Pitts, "A Logical Calculus of the Ideas Immanent in Nervous Activity," *The Bulletin of Mathematical Biophysics* 5 (1943): 115-133.

[186] Santosuosso, "Questioni definitorie," 472.

[187] Peluso, *Intelligenza artificiale*, 21.

[188] Di grande interesse la proposta di sviluppare una teoria unificata che congiunga i due orientamenti, applicando la riflessione di Kahneman sui "pensieri lenti e veloci" all'intelligenza artificiale. Grady Booch et al., "Thinking Fast and Slow in AI," *Proceedings of the AAAI Conference on Artificial Intelligence* 35, n. 17 (maggio 2021): 15042-46, doi:10.1609/aaai.v35i17.17765.
Vedi anche Daniel Kahneman, *Pensieri lenti e veloci*, trad. Laura Serra (Milano: Mondadori, 2020).

[189] *Cfr.* Stuart J. Russell e Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4ª ed. (Londra: Pearson, 2020). L'ultimo prezioso lavoro dei due autori rappresenta una delle rielaborazioni più recenti dell'approccio tradizionale all'AI.

[190] Russel e Norvig, *Artificial Intelligence*, 36.

[191] Si noti come l'impostazione di Russel e Norvig conservi la matrice "razionalista" spostando il focus dal funzionamento al comportamento dell'agente, che ben potrebbe operare anche attraverso un algoritmo di machine learning.

[192] Russel e Norvig, *Artificial Intelligence*, 39.

appropriate sono quelle che aumentano le probabilità di successo, e il successo è il raggiungimento di sotto-obiettivi comportamentali che supportano l'obiettivo finale del sistema".[193] È evidente che un comportamento volto a raggiungere determinati obiettivi assume senso solo in un ambiente controllabile e osservabile, solo così potrebbe valutarsi come "giusta" l'azione dell'agente.[194]

L'approccio c.d. "dell'agente razionale" all'IA ha prevalso a lungo nella storia della materia, al punto da essere talvolta indicato come il modello *standard*. Presenta infatti due principali vantaggi rispetto agli altri modelli. In primo luogo, è un approccio flessibile che si è mostrato in grado di tener conto di tutte le principali innovazioni del settore, diversamente del modello logicista puramente deduttivo. Secondo i suoi sostenitori, inoltre, lo standard di razionalità è matematicamente ben definito e generalizzabile, e ciò renderebbe possibile dimostrare quando e se un agente si comporta in modo razionale – operazione che risulta in gran parte impossibile nel momento in cui si adotta un approccio puramente connessionista, imitativo dei processi cognitivi umani.[195]

Il paradigma dell'agente razionale è di particolare interesse per il giurista: le più recenti definizioni elaborate dalla dottrina, nel tentativo di fissare una definizione normativa dell'IA e aprire la strada a un'efficace regolazione giuridica del fenomeno, ricorrono spesso all'idea di un agente in grado di agire sull'ambiente e raggiungere un dato obiettivo.[196]

Echi di questa tendenza sono riscontrabili anche nelle nozioni elaborate in seno alle Istituzioni europee. Un esempio, tra tutti, è quello fornito dalla definizione di IA elaborata nel 2018 dal c.d. *High Level Expert Group on AI* (*AI HLEG*):[197]

> Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve

---

[193] James S. Albus, "Outline for a Theory of Intelligence," *IEEE Transactions on Systems, Man, and Cybernetics* 21, n. 3 (maggio 1991): 474.
[194] Cristianini, *La scorciatoia,* 16-17
[195] Russel e Norvig, *Artificial Intelligence*, 39.
[196] Per una voce critica su questa tendenza, *vedi* Giovanni Romano, "Diritto, robotica e teoria dei giochi: riflessioni su una sinergia," in *Diritto e Intelligenza Artificiale*, a cura di Guido Alpa (Pisa: Pacini, 2020), 108.
[197] Sui lavori svolti dall'AI HLEG e il suo rilevante contributo alla dimensione etica dell'IA, *vedi* capitolo II, paragrafo 1.2.

> the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).[198]

La nozione coniata dall'AI HLEG può apparire forse elaborata, ma mira ad essere ampia e omnicomprensiva. Tradisce l'esigenza, propria del giurista, di dotarsi di una definizione normativa quanto più generale possibile, al fine di scongiurare vuoti di tutela e dubbi interpretativi.[199]

Persino un'analisi sommaria di quanto emerge *ex professo* dal campo di ricerca dell'IA, dunque, pare non fornire una soluzione univoca alla questione definitoria. A questo si aggiunga che tutte le teorie che si è avuto modo di illustrare fanno inevitabilmente ricorso al concetto di "intelligenza", che in precedenza si è volutamente tentato di lasciare sullo sfondo. Sembra quindi inevitabile imbattersi in una certa circolarità concettuale che lascia irrisolta la questione fondamentale:[200] è possibile definire l'intelligenza artificiale senza prima aver definito l'intelligenza umana?

È quasi ironico, oggi, constatare come già nel 1950 Alan Turing, annoverato tra i padri dell'informatica e tra le più brillanti menti matematiche del XX secolo, si fosse posto una simile domanda. Nel citatissimo "*Computer Machinery and Intelligence*", Turing giunge alla conclusione che interrogarsi sul se le macchine siano in grado di pensare sia cosa "troppo insignificante per meritare di essere discussa".[201] Stabilire una definizione comunemente accettata dei termini "macchina" e "pensare" è infatti compito di estrema difficoltà, già al tempo considerato potenzialmente infruttuoso.[202] Pertanto, nel

---

[198] High Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Scientific Disciplines* (2018), 7, https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.

[199] Peluso, *Intelligenza artificiale*, 7.

[200] Santosuosso, "Questioni definitorie," 471.

[201] Alan M. Turing, "Computing Machinery and Intelligence," *Mind* 59, n. 236 (ottobre 1950): 442, doi:10.1093/mind/LIX.236.433.

[202] Turing si dice convinto che per la fine del secolo l'uso delle parole e l'opinione pubblica dotta sarebbero cambiati così tanto che si sarebbe potuto parlare di macchine pensanti senza timore di esser contraddetti. Turing, "Computing Machinery", 442

suo lavoro, Turing propone di riformulare l'interrogativo in: "Esistono computer digitali concepibili che si comporterebbero bene nel gioco dell'imitazione?".[203]

Il gioco dell'imitazione, in lingua originale "*The Imitation Game"* (anche conosciuto come "Test di Turing"), rappresenta il cuore del sopracitato articolo ed è descritto estensivamente al suo interno. Nella sua versione originale, il gioco richiede tre partecipanti: un giudice, un uomo e una macchina. Al giudice sarà poi data la possibilità di comunicare a distanza con gli altri due giocatori, con la specificazione che potrà interrogarli esclusivamente attraverso un mezzo di comunicazione scritta, idealmente un monitor collegato a una tastiera. Per il giudice, lo scopo del gioco è quello di indovinare l'identità dei due interlocutori sulla base delle loro risposte; per la macchina, è quello di ingannare quanto più a lungo possibile il giudice "imitando" il comportamento umano; per il giocatore umano, lo scopo è aiutare per quanto possibile il giudice.[204] Se è impossibile rispondere alla domanda "Possono le macchine pensare?", è senz'altro empiricamente verificabile se una macchina sia in grado di superare il test di Turing.[205] Ancora una volta, a rilevare non è tanto se la macchina sia o meno intelligente com'è intelligente l'uomo, se questa sia o meno cosciente o dotata di intenzionalità,[206] quanto il suo comportamento.

Esistono dunque calcolatori digitali concepibili in grado di replicare il comportamento umano e ottenere buoni risultati nel gioco dell'imitazione? La risposta, per alcuni ricercatori, è che detti calcolatori non solo sono concepibili in astratto, ma potrebbero esistere già, qui e ora. GPT-4 e diversi altri LLM hanno buone probabilità di superare il test così come descritto nella sua formulazione originaria, e di sicuro lo hanno

---

[203] Turing, "Computing Machinery", 442

[204] Turing, "Computing Machinery", 433-435.

[205] Turing omette diversi dettagli su come il gioco dell'imitazione vada condotto in un contesto sperimentale. Diversa letteratura scientifica concorda nel ritenere che lo scopo della sua pubblicazione non fu mai quello di teorizzare un vero e proprio "test" da condurre in laboratorio, quanto rispondere agli scettici e sensibilizzare la popolazione, attraverso un esperimento mentale, sui risultati che da lì a pochi decenni ci si sarebbe potuti aspettare dall'intelligenza artificiale. *Cfr.* Bernardo Gonçalves, "The Turing Test is a Thought Experiment," *Minds & Machines* 33 (marzo 2023): 1-31, doi:10.1007/s11023-022-09616-8.

[206] La teoria dell'intenzionalità nega la possibilità che una macchina possa dirsi intelligente, pur esibendo un comportamento apparentemente qualificabile come tale. Alla macchina mancherebbe, per l'appunto, l'intenzionalità dell'azione. Uno dei primi e più noti esponenti della teoria dell'intenzionalità fu Searle, ideatore del celebre esperimento mentale della "stanza cinese". *Cfr*. John R. Searle, "Minds, Brains, and Programs," Behavioral and Brain Sciences 3, n. 3 (1980): 417-424, doi:10.1017/S0140525X00005756.

già superato nella percezione popolare, essendo attualmente in grado di ingannare diverse persone, quanto meno nelle conversazioni brevi.[207] Negli ultimi anni, piuttosto che tentare di replicare il gioco dell'imitazione, i ricercatori si sono concentrati sulla valutazione dei sistemi di IA attraverso test standardizzati progettati per le macchine, misurandone le prestazioni in relazione a capacità specifiche (abilità linguistiche, matematiche, di *problem solving* etc.).[208] OpenAI, il laboratorio di ricerca noto ai più per aver sviluppato ChatGPT, ha reso pubblici alcuni dei più impressionanti risultati raggiunti da GPT-4, uno dei loro modelli di linguaggio più avanzati, su una serie di parametri di valutazione. Tra i diversi test sottoposti alla macchina figura anche lo *Uniform Bar Exam*, il cui superamento è in molti Stati americani requisito necessario per ottenere l'abilitazione all'esercizio della professione forense; GPT-4 ha realizzato un punteggio che lo colloca nel 10% dei migliori candidati che hanno sostenuto l'esame.[209]

Al di là della questione terminologica, è sufficiente un'istantanea dello stato dell'arte per intuire le ragioni che impongono al giurista una seria riflessione sui rischi e le opportunità che si celano dietro i sistemi c.d. *AI-Powered*. Viviamo ormai pienamente in quella che è stata definita, anche nel corso di questa trattazione, la "Società dell'Algoritmo" (*Algorithmic Society*),[210] per tale intendendosi quella società in cui le tecnologie basate sugli algoritmi non solo prendono decisioni, ma sono anche in grado di portarle a termine.[211] L'intelligenza artificiale è una di queste tecnologie, fa parte del nostro presente e già da tempo ci conviviamo.[212] La sua natura di strumento "*general-purpose*" fa sì che possa essere adottata nei più svariati ambiti, generando benessere sociale e ricchezza economica; al tempo stesso, costituisce una seria minaccia per i diritti fondamentali della persona, dal diritto alla privacy al diritto di non-discriminazione, dal

---

[207] Celeste Biever, "The Easy Intelligence Tests That AI Chatbots Fail," *Nature* 619 (luglio 2023): 686, doi:10.1038/d41586-023-02361-7. Sui recenti tentativi di replicare in via sperimentale il Test di Turing per finalità di ricerca, *vedi anche* Gonçalves, "Turing Test", 2-5.

[208] Biever, "Easy Intelligence Tests," 687.

[209] Biever, "Easy Intelligence Tests," 688. Sul punto l'autrice rimanda allo studio in *preprint* condotto da OpenAI, oggi giunto alla sua sesta versione. *Cfr*. OpenAI, "GPT-4 Technical Report," *arXiv*, n. arXiv:2303.08774v6 (marzo 2024), https://arxiv.org/abs/2303.08774.

[210] Per una trattazione di natura sociologica sull'argomento, *cfr*. Schuilenburg e Peeters, *The Algorithmic Society*.

[211] Jack M. Balkin, "The Three Laws of Robotics in the Age of Big Data," *Ohio State Law Journal* 78, n. 5 (2017): 1219.

[212] Commissione Europea, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, 1.

diritto all'auto-determinazione al diritto alla salute.[213] Come tutte le tecnologie trasformative, l'IA solleva nuove e numerose questioni etiche e legali, interroga con urgenza il legislatore italiano ed europeo, nonché le autorità di regolazione nazionali e sovranazionali, affinché sia elaborato un quadro normativo di riferimento in grado di promuovere l'innovazione e al tempo stesso tutelare i diritti fondamentali.[214]

Senza pretesa di esaustività, in questo paragrafo si è tentato di ricostruire una panoramica dei principali sforzi profusi da filosofi e soprattutto *computer scientist* nel tentativo trans-disciplinare di definire l'intelligenza artificiale, sottolineando come il tema sia ancora oggi intensamente dibattuto. Sebbene la questione definitoria sia tutt'altro che chiusa, l'auspicio è che il giurista possa trarre, dall'analisi delle diverse prospettive illustrate, un insegnamento utile per cimentarsi nella costruzione di un efficace quadro regolatorio. Affinché ciò sia possibile, sarà forse necessario che il "cantiere" del diritto, come osserva Santosuosso, si apra a una "concezione molecolare ... relativista ... pluralista e policentrica .... dei fenomeni giuridici".[215]

---

[213] Nathalie Alisa Smuha, "From a 'Race to AI' to a 'Race to AI Regulation' - Regulatory Competition for Artificial Intelligence," *Law, Innovation and Technology* 13, n. 1 (2021): 3-4, doi:10.2139/ssrn.3501410.
[214] Commissione Europea, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, 3.
[215] Santosuosso, "Questioni definitorie," 472.

II. Regolare l'IA: motivazioni, obiettivi e strategie europee

1. Quale regolazione per l'IA?

Manca, in letteratura, una definizione univoca di "regolazione". Il termine è utilizzato per riferirsi a una "varietà di concezioni differenti",[216] venendo per altro impiegato in diversi contesti e ambiti di studio, dalle teorie economiche alla sociologia del diritto, passando per la scienza politica. Operando una sintesi essenziale, è possibile schematizzare le principali riflessioni prodotte dalla dottrina giuridica sul tema in quattro "livelli" di regolazione: la regolazione attraverso autorità amministrative indipendenti, agenzie governative o commissioni; gli atti intenzionali di controllo da parte dello Stato; gli atti intenzionali di controllo da parte dello Stato e dei soggetti non statali; gli atti non intenzionali di controllo da parte dello Stato e dei soggetti non statali.[217] Con particolare riguardo al contesto occidentale, poi, è celebre la nozione di "Stato regolatore" elaborata da Giandomenico Majone e Antonio La Spina, che hanno così definito quel modello di Stato che a partire dagli anni '70, e con incisività sempre maggiore dagli anni '80 in poi, ha progressivamente sostituito lo Stato c.d. interventista-keynesiano. Com'è noto, lo "Stato positivo", pianificatore, produttore di beni e servizi e fortemente interventista, basato per lo più sulla gestione discrezionale della domanda aggregata e un ampio ricorso a politiche redistributive, conobbe in quel giro d'anni una profonda crisi.[218] Il nuovo modello di Stato che venne ad affermarsi, di converso, vide come protagonista un soggetto pubblico – il regolatore, per l'appunto – dotato di poteri coercitivi, la cui attività principale è quella di modificare il contesto di azione di diversi attori (pubblici o privati) con l'obiettivo, implicito o esplicito che sia, di perseguire l'interesse pubblico. A tal fine, lo strumento adoperato dallo Stato regolatore non è, diversamente dal suo predecessore, l'intervento diretto nelle sfere di attività degli altri attori, ma la "statuizione esterna di regole". La "regolazione", dunque, assume una finalità duplice: garantire la possibilità e l'efficienza delle attività economiche, nonché prevenirne le possibili esternalità (inclusi i

---

[216] Karen Yeung, *Securing Compliance: A Principled Approach* (Oxford: Hart Publishing, 2004), 5.
[217] Ljupcho Grozdanovski e Jérôme De Cooman, "Forget the Facts, Aim for the Rights! On the Obsolescence of Empirical Knowledge in Defining the Risk/Rights-Based Approach to AI Regulation in the European Union," *Rutgers Computer and Technology Law Journal* 49, n. 2 (settembre 2023): 225.
[218] Antonio La Spina e Giandomenico Majone, *Lo Stato regolatore* (Bologna: Il Mulino, 2000), 15–17.

costi sociali), tramite la statuizione di regole di condotta e sanzioni, siano esse afflittive o premiali. [219]

Nell'ottica di un inquadramento generale, la definizione offerta da Majone e La Spina può essere ricondotta al primo dei quattro livelli di regolazione cui si è fatto riferimento; elemento essenziale dello Stato regolatore è infatti proprio l'istituzione di "autorità regolative indipendenti" (AR).[220] La natura giuridica delle AR appare di difficile collocazione, soprattutto se si opera una rigida separazione tra legislazione e amministrazione: se è indubbio che sia un atto legislativo a sancire gli obiettivi di interesse pubblico da perseguire, così come è sempre un atto legislativo a delegare alle autorità le competenze necessarie, a distinguere le AR è l'elevato grado di autonomia loro riconosciuto, anche rispetto all'esecutivo.[221] Quanto al tipo di regolazione in concreto esercitata dalle autorità, queste possono adottare norme generali di condotta, esercitare poteri amministrativi e poteri "quasi-giudiziari" (*adjudication*), talvolta a seguito di ricorso di un soggetto regolato avverso un provvedimento dell'AR stessa, talvolta nel ruolo di arbitro, mediatore o conciliatore tra privati in posizione di parità o tra utenti e fornitori di servizi essenziali.[222] In ultima analisi, un siffatto modo di intendere la regolazione ricorda, con i dovuti distinguo, l'accezione classica di *regulation* che si ritrova nella letteratura americana, ove il termine è sovente utilizzato per riferirsi specificatamente all'attività di regolazione svolta dalle *agencies* pubbliche.[223]

Per poter meglio indagare il ventaglio di "strumenti regolatori" a disposizione del potere pubblico, tuttavia, ai fini del presente lavoro s'intende adottare una concezione di regolazione di più ampio respiro, quale quella fornita dalla cibernetica. In questo campo,

---

[219] La Spina e Majone, 27.
[220] La Spina e Majone, 28.
[221] La Spina e Majone, 63-64. Non è possibile, in questa sede, fornire un'analisi approfondita delle Autorità Regolative Indipendenti, limitandosi a un breve richiamo. Per una panoramica completa, si rimanda a Marcello Clarich, *Autorità indipendenti: Bilancio e prospettive di un modello* (Bologna: Il Mulino, 2009). Sul tema della legittimazione delle AR, *vedi anche* Giandomenico Majone, "The Regulatory State and Its Legitimacy Problems," *West European Politics* 22, n. 1 (1999): 1–24, doi:10.1080/01402389908425284.
[222] La Spina e Majone, *Lo Stato regolatore*, 64.
[223] La Spina e Majone, 29-30. Sul punto gli autori richiamano la definizione di regolazione fornita da Philip Selznick: "un controllo prolungato e focalizzato, esercitato da una agency pubblica, su attività cui una comunità attribuisce una rilevanza sociale". Philip Selznick, "Focusing Organisational Research on Regulation," in *Regulatory Policy and the Social Sciences*, a cura di Roger G. Noll (Berkeley: University of California Press, 1985), 363.

il termine è impiegato per riferirsi a quei sistemi di controllo in grado di distinguere tra uno stato delle cose voluto e uno non voluto (*standard-setting*), monitorare lo stato attuale del sistema e le sue variazioni (*information-gathering*) e mettere in campo una serie di misure tali da cambiare lo stato del sistema sino al raggiungimento del risultato desiderato (*behaviour-modification*).[224]

Prendere le mosse da un'accezione ampia del termine consente, per altro, di tenere in dovuta considerazione quella che sembra essere una tendenza emergente nella dottrina che più di recente si è occupata della regolazione delle nuove tecnologie. A tal proposito, si è parlato di una vera e propria "nuova fenomenologia della regolazione": se da un lato si è assistito alla moltiplicazione delle autorità pubbliche dotate di potere normativo (e dunque, in senso lato, "regolativo"), dall'altro sono profondamente mutate le forme di esercizio di tale potere.[225] La regolazione di un settore di attività, oggi, può avvenire attraverso l'impiego di strumenti regolatori molto diversi tra loro. A mero titolo di esempio: agli operatori privati è comunemente riconosciuta una certa "capacità regolativa", dal momento che ben potrebbero questi dotarsi di un proprio sistema di regole, anche in assenza di regolazione pubblica; capacità regolativa è poi tradizionalmente attribuita alle scelte economico-finanziarie dello Stato, capaci di influenzare e regolare il mercato; financo la disciplina della responsabilità civile, orientando i comportamenti degli operatori privati, è in un certo senso considerabile uno strumento regolatorio.[226]

Proprio sul tema della regolazione delle nuove tecnologie, poi, particolarmente influente appare il contributo di Lawrence Lessig, cui si deve l'identificazione delle "quattro modalità di regolazione" che influenzano i comportamenti degli attori negli spazi reali e, soprattutto, virtuali: la legge, le norme sociali, il mercato e l'architettura del sistema.[227] Nel contesto del cyberspazio, come intuibile, l'architettura è costituita dal

---

[224] Karen Yeung, "Design for the Value of Regulation," in *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*, a cura di Jeroen van den Hoven, Pieter E. Vermaas e Ibo van de Poel (Dordrecht: Springer, 2015), 448-449. Per una voce critica su un tale modo di intendere la regolazione, *vedi* La Spina e Majone, *Lo Stato regolatore*, 24-25.

[225] Andrea Simoncini, "Verso la regolamentazione della intelligenza artificiale. Dimensioni e governo," *BioLaw Journal - Rivista di BioDiritto*, n. 2 (giugno 2021): 411.

[226] Simoncini, 411.

[227] Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* 113, n. 2 (dicembre 1999): 507-508.

"codice", e cioè da "*software* e *hardware,* che definiscono il cyberspazio per quello che è" e disegnano l'"insieme di vincoli su come ci si può comportare".[228] La lezione fondamentale di Lessig potrebbe quindi essere riassunta nella celebre affermazione *"Code is law"*.[229] Le quattro modalità di regolazione indicate non vanno comunque intese come rigidamente distinte: queste si influenzano reciprocamente, non sono mutualmente esclusive e ben possono operare simultaneamente e dinamicamente anche all'interno dello stesso ambito di applicazione.[230] Come già emerso nel dibattito accademico e scientifico che ha accompagnato la diffusione di Internet, le *disruptive technologies* obbligano le autorità pubbliche a rivedere le modalità classiche di regolazione,[231] a prendere in considerazione la totalità degli strumenti regolatori e ad adottare un approccio alla regolazione che, impiegando un termine suggestivo, si vuol qui definire "multimodale".[232]

1.1. La "corsa alla regolazione": motivazioni e obiettivi

Una volta chiarito quale definizione di "regolazione" si intende adottare in questa sede, occorre interrogarsi sul *se* questa sia necessaria nel caso dell'intelligenza artificiale e, in ipotesi affermativa, quali siano le principali ragioni a supporto di un intervento regolatorio. Nel cominciare questo lavoro si è riportato un esempio di mancata (o meglio, insufficiente) regolazione di tecnologia storicamente considerata *disruptive* quale Internet;[233] si è poi fornita una veloce panoramica di alcune delle principali sfide che i

---

[228] Lessig, 509.

[229] Sul tema si rimanda anche a Lawrence Lessig, *Code: and Other Laws of Cyberspace* (New York: Basic Books, 1999).

[230] È proprio Lessig a chiarire che: "*though I have described these four modalities as distinct, obviously they do not operate independently … Norms will affect which objects get traded in the market … the market will affect the plasticity, or malleability, of architecture … architectures will affect what norms are likely to develop … all three will influence what laws are possible*". Lessig, "The Law of the Horse," 511.

[231] Mobilio, "L'intelligenza artificiale", 416.

[232] La scelta del termine non è casuale. Nell'ambito dell'intelligenza artificiale, sono detti "multimodali" quei modelli di ML in grado di elaborare e integrare informazioni da più modalità o tipi di dati. Tali dati possono presentarsi in formato di testo, immagine, audio, video o, più genericamente attraverso un determinato tipo di *input* sensoriale. *Vedi* Paul Pu Liang, Amir Zadeh e Louis-Philippe Morency, "Foundations and Trends in Multimodal Machine Learning: Principles, Challenges, and Open Questions," *arXiv*, n. arXiv:2209.03430 (settembre 2022), https://arxiv.org/abs/2209.03430.

[233] *Vedi* capitolo I, paragrafo 1.

nuovi algoritmi pongono agli ordinamenti giuridici.[234] Per certi versi, il dibattitto intorno alla possibilità di regolare l'intelligenza artificiale non è così dissimile da quello che si accompagnò alla diffusione della Rete: se da un lato l'IA condivide con le *disruptive techonologies* diversi fattori di rischio che giustificherebbero interventi di *economic regulation* e *social regulation*,[235] dall'altro pone ai regolatori sfide del tutto inedite.

Un primo problema è rappresentato dalla natura *hi-tech* dell'intelligenza artificiale. Fatta eccezione per gli addetti ai lavori, gli attori sociali assai raramente possiedono conoscenze adeguate in merito al funzionamento delle nuove tecnologie e alle loro possibili applicazioni, il che si traduce in importanti asimmetrie informative tra gli attori coinvolti, sui mercati ma anche, più in generale, nei diversi livelli di società, incluso quello di governo.[236] A questo si aggiunga il problema della mancanza di trasparenza intrinseco ai sistemi di IA. Da un lato i segreti industriali, che bloccano l'accesso alle informazioni sui metodi impiegati nello sviluppo dei sistemi e i relativi risultati ottenuti, dall'altro il problema dei "blocchi costitutivi": quando più attori collaborano nella progettazione di componenti *hardware* e *software* è spesso difficile ottenere una conoscenza completa dell'origine e del funzionamento di tutte le parti del sistema.[237] Resta sullo sfondo, poi, il celebre problema della "*black box*", che caratterizza, come si è visto, gli algoritmi di apprendimento automatico.[238]

L'incredibile velocità con cui avanza il progresso tecnologico, nonché le trasformazioni sociali che questo porta con sé, obbligano poi i regolatori ad agire in un clima di costante incertezza. Le asimmetrie informative e l'imprevedibilità

---

[234] *Vedi* capitolo I, paragrafo 1.1.

[235] L'obiettivo dell'*economic regulation* è correggere i difetti interni al mercato, garantendo l'efficienza economica del sistema regolato. "Si tratterà quindi, di volta in volta, di prevenire il potere monopolistico o di controllarlo ... di specificare standards cui attenersi nell'offerta del servizio, di regolare l'ingresso di nuovi concorrenti ... di mantenere la concorrenza ... di migliorare la qualità dei prodotti ... di far diminuire o comunque fissare i loro prezzi". La *social regulation*, invece, mira a "correggere una vasta gamma di difetti di informazione ovvero di effetti collaterali o esternalità delle attività economiche, in campi quali la salute, l'ambiente, la sicurezza dei lavoratori, gli interessi dei consumatori". La Spina e Majone, *Lo Stato regolatore*, 39-40.

[236] Araz Taeihagh, M. Ramesh e Michael Howlett, "Assessing the Regulatory Challenges of Emerging Disruptive Technologies," *Regulation & Governance* 15 (marzo 2021): 1010, doi:10.1111/rego.12392.

[237] Wolfgang Hoffmann-Riem, "Artificial Intelligence as a Challenge for Law and Regulation," in *Regulating Artificial Intelligence*, a cura di Thomas Wischmeyer e Timo Rademacher (Cham: Springer, 2020), 17.

[238] *Vedi* capitolo I, paragrafo 1.1.

dell'evoluzione della tecnica comportano il rischio che le norme atte a regolare l'intelligenza artificiale si rivelino inefficaci: queste devono essere sì flessibili, così da non ostacolare le opportunità offerte dalla digitalizzazione, ma mai al punto da compromettere la capacità della norma di prevenire o mitigare i rischi.[239]

Un ulteriore sfida regolatoria è rappresentata dalla dimensione transnazionale delle *Big Tech*. Le grandi aziende tecnologiche globali percepiscono le differenze tra i quadri normativi nazionali come una minaccia ai loro modelli di *business*, e pertanto sfruttano diverse opportunità al fine di eludere regole il cui rispetto ritengono eccessivamente oneroso. Nel contesto normativo europeo, un'innovativa soluzione regolatoria al problema è stata fornita dall'art. 3 del GDPR.[240] Nel definire l'ambito territoriale del Regolamento, il par. 1 stabilisce che questo si applica "al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione". Il par. 2, poi, sancisce due ulteriori condizioni al verificarsi delle quali il GDPR si applica anche "al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione".[241] A tal proposito, si è parlato in dottrina di un rivoluzionario ambito di applicazione "extra-territoriale" o "a-territoriale" del Regolamento.[242] Come si vedrà nel corso del terzo capitolo di questa trattazione, il legislatore europeo ha percorso una simile strada anche nel nuovo AI Act.[243]

Le tecnologie dirompenti producono effetti diversi su diversi segmenti della società; ciò che per i grandi investitori e le *Big Tech* rappresenta un'importante occasione di guadagno, per i dipendenti delle imprese "*disrupted*" e per le categorie vulnerabili

---

[239] Hoffmann-Riem, "Artificial Intelligence as a Challenge for Law and Regulation," 14.

[240] Hoffmann-Riem, 15-16

[241] Regolamento (UE) 2016/679, art. 3, par. 2: "Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione."

[242] *Si veda*, tra gli altri, Merlin Gömann, "The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement," *Common Market Law Review* 54, n. 2 (aprile 2017): 567–590, doi:10.54648/COLA2017035.

[243] *Vedi* capitolo III, paragrafo 1.

rischia di tradursi in una serie di conseguenze negative,[244] tra cui la polarizzazione dell'occupazione, la stagnazione salariale per i lavoratori con competenze medio-basse e un accesso sempre più limitato a posti di lavoro di qualità.[245] Si è poi già fatta menzione dei rischi, per così dire, di "sistema" posti dall'intelligenza artificiale: la trasversalità dei settori in cui può essere impiegata, da soggetti pubblici o privati che siano, rende particolarmente complessa la gestione delle conseguenze di eventuali difetti di programmazione o malfunzionamenti, senza considerare i possibili usi illeciti cui si prestano i sistemi di IA. Ad essere in discussione non sono solo i diritti fondamentali, ma, più in generale, la tenuta dei principi democratici e dello Stato di diritto.[246]

Alla luce delle considerazioni sin qui svolte, la regolazione sembrerebbe non solo necessaria, ma lo strumento che più di tutti si è dimostrato in grado di rispondere a quel "dilemma amministrativo" che è il "governo del digitale": non solo un meccanismo di *command and control*, ma una funzione di equilibrio, capace di mediare tra la spinta all'innovazione tecnologica e le finalità sociali, tra il dinamismo del mercato e la protezione degli interessi collettivi.[247] Come argomentato da Smuha, è proprio attraverso un utilizzo consapevole delle diverse modalità delineate da Lessig che i governi internazionali potranno raggiungere tale equilibrio, sfruttando a pieno sia il "ruolo protettivo", sia il ruolo "abilitativo" della regolazione.[248]

A ben vedere, i maggiori paesi del mondo sembrerebbero piuttosto consapevoli dell'importanza strategica dell'intelligenza artificiale, al punto che negli ultimi anni si è

---

[244] Taeihagh, Ramesh e Howlett, "Assessing the Regulatory Challenges," 1011.

[245] Laura D. Tyson e John Zysman, "Automation, AI & Work," *Daedalus* 151, n. 2 (maggio 2022): 256. Per una panoramica completa sul complesso rapporto tra AI e lavoro, *vedi* Inka Knappertsbusch e Kai Gondlach, a cura di, *Work and AI 2030: Challenges and Strategies for Tomorrow's Work* (Wiesbaden: Springer, 2023).

[246] Si pensi a tutti quei casi in cui i sistemi di intelligenza artificiale decidono sulla concessione di un mutuo, selezionano i vincitori di un concorso pubblico o, ancora, sono adoperati nell'adozione di provvedimenti amministrativi e decisioni giudiziarie. Donati, "Quale disciplina per l'intelligenza artificiale?," 47.

[247] Bruno Carotti, "La politica europea sul digitale," 1001. Sulla definizione di "governo del digitale", o "*digital governance"*, si riporta poi quanto scritto da Floridi: "*Digital Governance is the practice of establishing and implementing policies, procedures and standards for the proper development, use and management of the infosphere. It is also a matter of convention and good coordination, sometimes neither moral nor immoral, neither legal nor illegal*". Luciano Floridi, "Soft Ethics, the Governance of the Digital and the General Data Protection Regulation," *Philosophical Transactions of the Royal Society A* 376, n. 2133 (novembre 2018): 3, doi:10.1098/rsta.2018.0081.

[248] Smuha, "From a 'Race to AI' to a 'Race to AI Regulation'," 5.

parlato di una vera e propria corsa allo sviluppo di applicazioni di IA ("*Race to AI*" o "*AI arms race"*).[249] Vincere questa competizione, per i principali attori internazionali, è considerata una priorità "esistenziale", non solo per affermarsi nel ruolo di *leader* sui mercati globali, ma anche e soprattutto per esigenze di sicurezza nazionale ed economica. In questo senso vanno lette le recenti strategie assunte da Cina, Stati Uniti e Unione Europea per accelerare e guidare lo sviluppo dei nuovi algoritmi.[250] Contemporaneamente, si è sostenuto, si sarebbe sviluppata una vera e propria competizione anche sotto un altro fronte, quello della regolazione dell'intelligenza artificiale ("*Race to AI regulation*").[251] Del resto è da tempo che la miglior dottrina evidenzia come la competizione internazionale non riguardi solo i produttori di beni e servizi (e dunque, delle nuove tecnologie), ma anche i regimi regolatori. La "competizione regolatoria" premierebbe proprio quei regimi "in cui le innovazioni istituzionali non restano indietro rispetto alle nuove scelte strategiche".[252] Potrebbe dirsi che l'idea economica del "*first-mover advantage*", secondo la quale le imprese che per prime ottengono il controllo di risorse produttive, lanciano un nuovo prodotto o servizio sul mercato acquisiscono un vantaggio competitivo, sembra oggi potersi traslare all'ambito normativo-regolatorio.[253]

In un contesto internazionale dominato dalla produzione tecnologica cinese e statunitense, la strategia europea è stata quella di "spostare il campo di gioco dalla

---

[249] Smuha, 3.

[250] Smuha, 3. L'autrice fa riferimento alle prime iniziative assunte in materia, tra cui il "*Next Generation AI Development Plan*" adottato dalla Cina nel 2017, la strategia europea delineata nella comunicazione della Commissione "*L'intelligenza artificiale per l'Europa"* del 2018, e l'*Executive Order No. 13859* del 2019, firmato dall'allora Presidente degli Stati Uniti Donald Trump.

[251] Smuha, "From a 'Race to AI' to a 'Race to AI Regulation'," 4-5.

[252] Giandomenico Majone, "From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance," *Journal of Public Policy* 17, n. 2 (maggio 1997): 139

[253] Smuha, "From a 'Race to AI' to a 'Race to AI Regulation'," 18. Per meglio illustrare cosa si intende per "*first-mover* advantage", l'autrice ricorre a un esempio: un Paese A decide di adottare un quadro regolatorio, prevedendo che siano garantiti determinati requisiti nei sistemi di AI sul mercato. Le imprese di un Paese B, per accedere al mercato del Paese A, dovranno conformarsi a tali regole, affrontando costi che le imprese del Paese A, che producono solo per il mercato interno, non devono sostenere. Per far fronte a questo svantaggio competitivo, è plausibile che le imprese del Paese B facciano pressione sul loro governo affinché adotti regole simili a quelle del Paese A. Il Paese B si troverà così a essere un "*rule-taker*", il Paese A sarà invece un "*rule-setter*". Mentre le imprese del Paese B si adattano al nuovo quadro regolatorio, le imprese del Paese A avranno già internalizzato i costi da tempo. Sul tema, *cfr. anche* Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 349.

tecnologia alle regole", nel tentativo di affermarsi come *leader* nella produzione normativa e porsi come modello di riferimento globale nella regolazione delle nuove tecnologie. Non potendo contare sulla titolarità di piattaforme digitali di rilievo, né tantomeno su processi produttivi competitivi in campo tecnologico, l'Unione Europea ha inseguito il c.d. "effetto Bruxelles" (*Brussels Effect*).[254] Con il termine, coniato e reso celebre dalla professoressa della Columbia Law School Anu Bradford, si fa riferimento alla capacità, mostrata dall'UE, di porsi sullo scacchiere internazionale come "potenza regolatoria globale".[255] Se l'obiettivo dichiarato della regolazione europea in materia digitale è stato a lungo quello di costruire un mercato unico interno, rimuovendo gli ostacoli agli scambi commerciali intra-unione, nel corso degli anni, lo sviluppo di un ambiente regolatorio armonizzato ha acquisito una crescente dimensione esterna, consacrando l'UE come regolatore egemone.[256]

Come si avrà modo di vedere più approfonditamente nella sezione di questo lavoro dedicata alla regolazione europea,[257] di recente le istituzioni europee sembrano aver assunto una sempre maggiore consapevolezza di questa influenza esterna. Non sorprende, dunque, che l'UE abbia partecipato con determinazione alla "corsa per la regolazione dell'IA". Così come non sorprende che, come accaduto in passato, la Commissione abbia ricoperto in questo processo un ruolo da assoluta protagonista. Come osservato da Majone, priva di poteri tradizionali come la tassazione o la spesa pubblica, la Commissione ha storicamente potuto ampliare la propria influenza e le proprie competenze sviluppando una sorta di "Stato regolatore puro".[258] Gli sforzi regolatori che ne sono derivati hanno così consentito all'Unione di presentarsi preparata alla sfida dell'intelligenza artificiale, potendo far affidamento su una preesistente e solida ossatura regolatoria.[259]

---

[254] Finocchiaro, *Intelligenza artificiale*, 109.
[255] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020), 7.
[256] Bradford, 7.
[257] *Vedi* paragrafi 2 e 3 del presente capitolo.
[258] Majone, "From the Positive to the Regulatory State," 150. *Vedi anche* Bradford, *The Brussels Effect,* 16-17.
[259] *Cfr.* Franco Pizzetti, "Introduzione alla regolazione europea della società digitale," in *La regolazione europea della società digitale*, a cura di Franco Pizzetti (Torino: Giappichelli, 2024).

1.2. La cassetta degli attrezzi

È adesso possibile fornire una panoramica degli strumenti che compongono la "*regulatory toolbox",* la "cassetta degli attrezzi" del regolatore. Come evidenziato da Simoncini, è possibile prendere in considerazione diverse "dimensioni" della regolazione, a seconda della prospettiva d'indagine che s'intende adottare.[260]

Con riguardo all'*efficacia* delle regole, la dottrina è solita distinguere tra *hard law* e *soft law*: la prima indica un sistema di regole dotato di piena obbligatorietà giuridica, la seconda è generalmente impiegata per riferirsi a regole non precettive.[261] Non collocabile tra le fonti primarie o secondarie del diritto, la *soft law* può considerarsi una fonte terziaria che si caratterizza per la presenza di contenuto normativo (inteso quindi a influenzare la condotta dei destinatari), sebbene giuridicamente non vincolante.[262] Nell'ambito dell'intelligenza artificiale, esempi di *soft law* possono considerarsi le numerose iniziative assunte dalle istituzioni internazionali e sovranazionali nel tentativo di promuovere codici etici, dichiarazioni di principi e norme valoriali. Sebbene il "dibattito etico" abbia accompagnato l'IA sin dalla nascita, dal 2016 in poi si è assistito a una proliferazione di linee guida e carte etiche senza precedenti; si è parlato, in letteratura, di una vera e propria "*Rush to ethics*", una corsa, o meglio una fretta, a dotarsi di un'intelligenza artificiale etica.[263]

Sono da leggersi in questo contesto le diverse iniziative assunte dall'Unione Europea in materia, a partire dalla comunicazione della Commissione di aprile 2018, "L'intelligenza artificiale per l'Europa",[264] e di dicembre dello stesso anno, con il "Piano coordinato sull'intelligenza artificiale".[265] Viene così delineato dalla Commissione uno

---

[260] Simoncini, "Verso la regolamentazione della intelligenza artificiale," 412.
[261] Simoncini, 412.
[262] La Spina e Majone, *Lo Stato regolatore*, 87.
[263] Vasiliki Koniakou, "From the 'Rush to Ethics' to the 'Race for Governance' in Artificial Intelligence," *Information Systems Frontiers* 25, n. 1 (febbraio 2023): 75, doi:10.1007/s10796-022-10300-6. Uno dei primi documenti internazionali a trattare da un punto di vista etico il tema dell'intelligenza artificiale può essere considerata la celebre "Convenzione 108". *Vedi* Consiglio d'Europa, *Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, 28 gennaio 1981, ETS n. 108.
[264] Commissione Europea, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final.
[265] Commissione Europea, *Piano coordinato sull'intelligenza artificiale*, COM(2018) 795 final.

dei principi fondamentali dell'IA *made in Europe*: l'etica *by design*, vale a dire garantita sin dal momento della progettazione.[266]

Un passo importante del cammino europeo per un IA etica è poi rappresentato dall'istituzione del già citato Gruppo di esperti di alto livello sull'intelligenza artificiale, o AI HLEG. Tra le principali attività del gruppo vi è stata la redazione, nel 2019, delle *Ethics guidelines for trustworthy AI* ("Orientamenti etici per un'IA affidabile"),[267] testo che aveva l'obiettivo di promuovere un'intelligenza artificiale in grado di garantire, per tutto il ciclo di vita del sistema, i principi di legalità, eticità e robustezza.[268] È all'interno di questo documento che il gruppo di esperti declina quattro principi etici fondamentali – a loro volta ricavati dalla Carta dei diritti fondamentali dell'Unione Europea – che saranno poi ripresi all'interno dei Considerando 7 e 27 dell'AI Act: presenza dell'autonomia e della sorveglianza umana, prevenzione dei danni, equità ed esplicabilità della decisione algoritmica.[269] Principi analoghi si ritrovano anche nella Raccomandazione del Consiglio OCSE sull'intelligenza artificiale del 2019 (oggi disponibile nella sua versione aggiornata al 2024).[270] Il documento, che costituisce il primo *standard* intergovernativo sull'IA, persegue diversi scopi: la promozione di ricerca e sviluppo nel campo dell''automazione, la creazione di un ecosistema digitale per l'IA

---

[266] Valentina Grazia Sapuppo, "Etica ed IA," in *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli (Rimini: Maggioli, 2024), 113.

[267] High Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 8 aprile 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[268] Sapuppo, "Etica ed IA," 114.

[269] Sapuppo, 115. Regolamento (UE) 2024/1689, Considerando 7: "Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire regole comuni per i sistemi di IA ad alto rischio. Tali regole dovrebbero essere coerenti con la Carta, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Dovrebbero inoltre tenere conto della dichiarazione europea sui diritti e i principi digitali per il decennio digitale e degli orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG)."
Regolamento (UE) 2024/1689, Considerando 27: "Sebbene l'approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un'IA affidabile del 2019 elaborati dall'AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che sono intesi a contribuire a garantire che l'IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. ..."

[270] OCSE, *Raccomandazione del Consiglio sui principi sull'intelligenza artificiale*, 22 maggio 2019, https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

nonché la cooperazione internazionale in materia.[271] Fondamentale, per gli orientamenti etici europei, è infine il ruolo rivestito dal già citato "Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia", con il quale la Commissione, nel 2020, getta le fondamenta per la costruzione del nuovo quadro normativo strategico per l'intelligenza artificiale.[272]

Cambiando lente d'analisi, passando dall'*efficacia* delle regole ai *soggetti* che le adottano, si condivide la tripartizione proposta da Simoncini, che distingue: forme di "etero-regolazione pubblica", per tali intendendosi le regole poste dalle autorità pubbliche; forme di "auto-regolazione privata", o *self-regulation*, dunque sistemi di regole stabiliti dagli stessi destinatari della regolazione; forme ibride di *co-regulation*, categoria cui è possibile ricondurre tutte quelle tecniche di regolazione "mista", a metà strada tra gli estremi dell'etero-regolazione pubblica e dell'auto-regolazione privata.[273]

Quanto alla *self-regulation*, si segnala in letteratura una certa confusione semantica sul tema. Il termine è talvolta impiegato per riferirsi, genericamente, alla *soft law*; talvolta all'adozione unilaterale di *standard* da parte di imprese; talvolta ad accordi bilaterali tra governo e regolati.[274] Se per auto-regolazione s'intende la fissazione di regole da parte dei destinatari della regolazione, del resto, è stato fatto notare come questa, oltre che volontaria, ben potrebbe essere delegata dallo Stato, soggetta ad approvazione da parte del potere pubblico, o persino obbligata sotto minaccia di sanzione.[275] Nel tentativo di fare chiarezza, torna qui utile la tripartizione sopracitata: ai fini del presente lavoro si considererà *self-regulation* soltanto l'adozione volontaria di regole da parte di soggetti privati; le altre forme di auto-regolazione elencate si caratterizzano infatti tutte per una qualche forma di intervento del potere pubblico, e appaiono pertanto meglio ascrivibili alla categoria della *co-regulation*.[276] Possono quindi dirsi forme di *self-regulation* le

---

[271] Pajno et al., "AI: Profili giuridici," 207-208.
[272] Commissione Europea, *Libro Bianco sull'intelligenza artificiale: Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final.
[273] Simoncini, "Verso la regolamentazione della intelligenza artificiale," 412.
[274] Julia Black, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World," *Current Legal Problems* 54, n. 1 (dicembre 2001): 121, doi:10.1093/clp/54.1.103.
[275] Black, 118.
[276] A partire dall'analisi di Black, giunge a considerazioni analoghe Mobilio, "L'intelligenza artificiale", 414.

dichiarazioni sui principi etici, l'istituzione di comitati etici interni e i vari fenomeni associativi promossi dalle grandi aziende del digitale, tra cui si segnala la *Partnership on Artificial Intelligence* avviata da IBM, Google/DeepMind, Facebook, Amazon, Apple e Microsoft nel 2016.[277]

Quanto agli spazi della co-regolazione, anche qui è possibile ritrovare in letteratura diverse definizioni del fenomeno. A titolo di mero esempio, è stata ricondotta alla categoria della *co-regulation* l'attività "quasi" giurisdizionale esercitata dalle autorità indipendenti, come i pareri o le autorizzazioni generali emesse dalle Autorità di protezione dei dati personali.[278] La *co-regulation* è poi lo strumento regolatorio più impiegato per la definizione di *standard* tecnici a livello nazionale e sovranazionale.[279] L'approccio seguito è detto *multistakeholder*, basato sul coinvolgimento di attori pubblici e privati, e mira a includere tutti quei soggetti che rivestono un ruolo chiave nello sviluppo delle nuove tecnologie.[280] Nell'elaborazione di *standard* e norme tecniche, di primaria importanza è poi il ruolo svolto dagli organi internazionali di standardizzazione tecnica, come la *International Organization for Standardization* (ISO), la *International Electrotechnical Commission* (IEC), lo *European Committee for Standardization* (CEN) e lo *European Committee for Electrotechnical Standardization* (CENELEC).[281]

Un caso particolare è poi costituito dal GDPR. Sebbene, trattandosi di regolamento dell'Unione Europea, questo sia pacificamente qualificabile come *hard law*, alcuni autori sottolineano come l'approccio seguito dall'UE in materia di protezione di dati si differenzi dalle forme tradizionali di *command and control*, configurandosi piuttosto

---

[277] Mobilio, 409. L'autore cita una moltitudine di dichiarazioni di principi etici pubblicate dalle *Big Tech*, cui si rimanda. A questo panorama si possono aggiungere, guardando ai più recenti sviluppi nell'ambito dell'intelligenza artificiale, la "Carta" di OpenAI e le iniziative di Anthropic, in particolar modo la "*Claude Constitution*", uno dei più innovativi progetti di *AI ethics by design*. Anthropic è attualmente impegnata nel tentativo di "orientare costituzionalmente" *Claude,* il proprio modello di linguaggio, integrando nel processo di addestramento diversi testi costituzionali, tra cui la Dichiarazione Universale dei Diritti Umani. Per la "Carta" di OpenAi *consulta*: https://openai.com/charter/. Per la "*Claude Constitution*", *consulta*: https://www.anthropic.com/news/claudes-constitution.

[278] Simoncini, "Verso la regolamentazione della intelligenza artificiale," 412-413.

[279] Mobilio, "L'intelligenza artificiale", 411.

[280] Pajno et al., "AI: Profili giuridici," 209.

[281] Mobilio, "L'intelligenza artificiale", 412. Sul tema della co-regolazione e l'elaborazione della norma tecnica, l'autore rimanda a Antonio Iannuzzi, *Il diritto capovolto: Regolazione a contenuto tecnico-scientifico e Costituzione* (Napoli: Editoriale Scientifica, 2018).

come un modello regolatorio *bottom-up*.[282] Il GDPR, infatti, non stabilisce una specifica modalità per conformarsi ai requisiti indicati come obbligatori, ma delega a titolari e responsabili del trattamento l'onere di valutare il rischio che tale trattamento pone ai diritti e alle libertà degli interessati (*risk assessment*) e di adottare, di conseguenza, tutte le misure tecniche e organizzative necessarie a garantire un livello di sicurezza adeguato (*risk mitigation*).[283]

L'ultima dimensione della regolazione è rappresentata dal *contenuto* delle regole.[284] A tal riguardo, si è visto come la lezione di Lessig abbia aperto la strada a un approccio regolatorio innovativo, che guarda direttamente all'architettura profonda dietro il funzionamento delle nuove tecnologie. La tecnologia non più solo come obiettivo della regolazione, ma come strumento attraverso cui regolare.[285] Un siffatto approccio è generalmente indicato col nome di "*regulation by design*", in quanto aspira all'integrazione degli obiettivi regolatori a partire dalla progettazione, dal *design* stesso dei sistemi tecnologici.[286] La regolazione *by design* obbliga i progettisti a garantire che il loro sistema soddisfi specifici requisiti legali. I progettisti, a loro volta, rispettano tale regola trasformando i requisiti legali in requisiti tecnici, incorporando i contenuti della regola nel codice.[287] Il termine nasce intorno agli anni '70, quando i tecnici dell'Internet iniziarono a integrare protocolli di sicurezza e meccanismi di tutela della privacy direttamente nell'architettura della Rete.[288] Spostandoci all'oggi, anche il legislatore europeo sembra aver compreso "la valenza 'normativa' del codice":[289] ne è un esempio

---

[282] Grozdanovski e De Cooman, "Forget the Facts," 291.

[283] Grozdanovski e De Cooman, 290. Sul tema, *cfr*. Irene Kamara, "Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation 'Mandate,'" *European Journal of Law and Technology* 8, n. 1 (marzo 2017), https://ejlt.org/index.php/ejlt/article/view/545/725.

[284] Simoncini, "Verso la regolamentazione della intelligenza artificiale," 412.

[285] Sulla differenza tra "*Technology as a Regulatory Target*" e "*Technology as a Regulatory Tool*", *vedi* Roger Brownsword e Karen Yeung, a cura di, *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Oxford: Hart Publishing, 2008).

[286] Robert Mahari e Alex Pentland, "Regulation by Design: A New Paradigm for Regulating AI Systems," in *Digital Single Market and Artificial Intelligence: AI Act and Intellectual Property in the Digital Transition*, a cura di Mario Franzosi, Oreste Pollicino e Gianluca Campus (Roma: Aracne, 2024), 432.

[287] Marco Almada, "Regulation by Design and the Governance of Technological Futures," *European Journal of Risk Regulation* 14, n. 4 (maggio 2023): 697-698, doi:10.1017/err.2023.37.

[288] Mahari e Pentland, "Regulation by Design," 433.

[289] Mobilio, "L'intelligenza artificiale", 417.

l'art. 25 del GDPR, che sancisce il principio della c.d. "*privacy by design*" e "*by default"*, la protezione dei dati garantita sin dalla progettazione dei sistemi tecnologici e per impostazione predefinita.[290]

Generalmente, si ritiene che un'efficiente regolazione *by design* richieda la sussistenza di tre presupposti fondamentali: un chiaro consenso sugli obiettivi che s'intende raggiungere attraverso la regolazione, l'implementazione di una metrica con la quale misurare il successo dell'intervento regolatorio, e, dal momento che un tale tipo di regolazione fa largo affidamento sugli sviluppatori delle tecnologie regolate, l'esistenza di meccanismi di *audit* per instaurare un continuo dialogo con questi ultimi.[291]

Sembra auspicabile che le regole con cui si andrà a governare l'intelligenza artificiale tengano conto, nel loro contenuto, della dimensione essenziale del *code*. I sistemi di IA, per altro, sono dinamici, possono essere ottimizzati per il raggiungimento di diversi obiettivi e aggiornati sulla base di nuovi dati, il che li renderebbe, in linea teorica, perfetti candidati per una *regulation by design*.[292]

Nel terminare questo capitolo, si vogliono avanzare dei brevi rilievi conclusivi su come i diversi "attrezzi" della regolazione siano stati impiegati dal regolatore europeo nel campo dell'intelligenza artificiale, e con quali effetti. Cominciando dall'ultimo degli strumenti analizzati, premesso che sul punto la letteratura appare ancora insufficiente e si attendono ulteriori sviluppi, potrebbe argomentarsi che l'AI Act realizzi un modello di *regulation by design,* quanto meno nella disciplina tracciata per i sistemi di IA ad alto rischio.[293] La sezione 2 del capo terzo individua i requisiti che tali sistemi devono rispettare, "tenendo conto delle loro previste finalità nonché dello stato dell'arte generalmente riconosciuto in materia di IA e di tecnologie correlate all'IA".[294] L'argomento sarà ripreso nel trattare in dettaglio la disciplina dell'AI Act.[295] Sul punto,

---

[290] Mahari e Pentland, "Regulation by Design," 433. Tale affermazione sembra trovare diversi riscontri in dottrina. *Vedi*, tra tutti, Kostina Prifti, Jessica Morley, Claudio Novelli e Luciano Floridi, "Regulation by Design: Features, Practices, Limitations, and Governance Implications," *Minds & Machines* 34, n. 2 (maggio 2024): 2, doi:10.1007/s11023-024-09675-z.

[291] Mahari e Pentland, "Regulation by Design," 436-439.

[292] Mahari e Pentland, "Regulation by Design," 432.

[293] Sebbene il lavoro non si concentri sull'analisi dell'AI Act, tali conclusioni sembrano essere condivise da Prifti et al., "Regulation by Design," 2.

[294] Regolamento (UE) 2024/1689, art. 8, par. 1.

[295] *Vedi* capitolo III, paragrafo 3.2.

basti notare quanto previsto dall'articolo 15 in tema di accuratezza, robustezza e cybersicurezza dei sistemi. Non solo questi aspetti devono essere garantiti nella progettazione tecnica dell'IA e durante l'intero "ciclo di vita" dei sistemi: l'articolo 15 si spinge oltre, stabilendo che "per affrontare gli aspetti tecnici relativi alla misurazione degli adeguati livelli di accuratezza e robustezza ... la Commissione, in cooperazione con le parti interessate e le organizzazioni competenti ... incoraggia, ove opportuno, lo sviluppo di parametri di riferimento e metodologie di misurazione".[296]

Quanto alla *soft law*, alle diverse forme di auto-regolazione e co-regolazione, si è visto come questi strumenti siano stati impiegati, dal 2016 in poi, nel tentativo di sviluppare un'etica dell'intelligenza artificiale. I limiti di questo tipo di interventi furono subito evidenti alla dottrina del tempo. Si deve a Floridi una prima analisi critica delle conseguenze negative derivanti dalla proliferazione di principi, documenti e carte etiche; questi mise in luce alcune pratiche di "malcostume" diffuse tra gli attori del settore digitale, coniando, per una in particolare, il celebre termine di "*bluewashing*".[297] Si insinuò dunque il dubbio, tra le pagine degli studiosi, che l'eccessiva attenzione per la dimensione etica stesse in realtà causando una "ritirata" del diritto e della regolazione, in favore di forme meno incisive di *soft governance*.[298]

Sebbene la *self-regulation* presenti alcuni innegabili vantaggi, come l'ottenimento di una facile legittimazione da parte dei suoi destinatari, una maggiore agilità e consapevolezza dei problemi che affronta, non può ignorarsi come questa si riveli "spesso strutturalmente inadeguata a tenere in conto i costi diffusi che ... [un'] attività economica ... scarica su soggetti esterni ai governi privati",[299] o meglio, citando Torchia, "esterni agli Stati digitali".[300] Nel campo dell'intelligenza artificiale, poi, non si riscontrano ancora quelle caratteristiche necessarie affinché la *soft governance* funzioni, come la presenza di

---

[296] Regolamento (UE) 2024/1689, art. 15, par. 2. Sarebbe quindi prevista una metrica per la misurazione degli obiettivi regolatori, come vorrebbe una *regulation by design* efficiente.

[297] Se il *greenwashing* si riferisce a comportamenti che mirano a sembrare più ecologici di quanto non lo siano realmente, il *bluewashing* indica l'uso delll'etica digitale come mera "decorazione" cosmetica, senza alcun impegno sostanziale. Il blu richiama simbolicamente il mondo digitale. Per una panoramica completa sulle pratiche di sfruttamento dell'etica a fini commerciali, *vedi* Luciano Floridi, "Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical," *Philosophy and Technology* 32, n. 2 (maggio 2019): 185–193, doi:10.1007/s13347-019-00354-x.

[298] Black e Murray, "Regulating AI and Machine Learning," 8.

[299] La Spina e Majone, *Lo Stato regolatore*, 83.

[300] Il riferimento è sempre a Torchia, *Lo Stato digitale*.

norme di buon comportamento consolidate ed enti collettivi di licenza.[301] Quanto ai documenti di *soft law* provenienti dalle istituzioni sovranazionali e internazionali, sebbene le iniziative siano state accolte in dottrina come lodevoli, la varietà di principi e dichiarazioni, l'uso di un linguaggio spesso vago, la frammentarietà delle iniziative assunte e il carattere settoriale delle linee guida ne hanno spesso compromesso l'efficacia pratica.[302]

Alle soglie del 2021, una disciplina unificata in materia appariva ormai come una necessità indifferibile.

2. Il quadro normativo europeo sul digitale

Sin dagli inizi degli anni 2000 appaiono evidenti gli sforzi profusi dall'Unione Europea nel tentativo di dotarsi di una disciplina organica della società digitale. Nel cominciare questa trattazione con alcuni cenni essenziali alla storia di Internet, si è avuto modo di illustrare il contributo apportato dalla Direttiva E-commerce (sulla falsariga della statunitense *section 230*) nell'indirizzare lo sviluppo della Rete.[303] Testimonianza di un tale, lungimirante, impegno legislativo è contenuta anche nei "Piani d'azione" "*eEurope* 2002"[304] e "*eEurope* 2005",[305] orientati alla promozione della connettività Internet nel territorio dell'Unione, nonché alla traduzione di questa connettività "in un aumento della produttività economica e in un aumento della qualità e dell'accessibilità dei servizi a profitto di tutti i cittadini europei".[306] Un ulteriore, fondamentale passaggio è poi rappresentato dall'adozione, nel 2010, dell'Agenda digitale europea,[307] strategia decennale che per prima ha riconosciuto il ruolo centrale rivestito dalle tecnologie dell'informazione e della comunicazione nel perseguimento degli obiettivi comunitari.[308]

---

[301] Black e Murray, "Regulating AI and Machine Learning," 8.
[302] Koniakou, "From the 'Rush to Ethics,'" 77. Ma anche Alessandro Pajno, "Forum: Law and Artificial Intelligence," *BioLaw Journal – Rivista di BioDiritto* 1 (marzo 2020): 490, doi:10.15168/2284-4503-538.
[303] *Vedi* capitolo I, paragrafo 1.
[304] Commissione Europea, *eEurope 2002: Impatto e priorità*, COM(2001) 140 def.
[305] Commissione Europea, *eEurope 2005: una società dell'informazione per tutti*, COM(2002) 263 def.
[306] I piani sono menzionati come primo esempio dell'interesse europeo verso il digitale da Antonio Iannuzzi, "Le fonti del diritto dell'Unione europea per la disciplina della società digitale," in *La regolazione europea della società digitale*, a cura di Franco Pizzetti (Torino: Giappichelli, 2024), 9.
[307] Commissione Europea, *Un'agenda digitale europea*, COM(2010) 245 def.
[308] Iannuzzi, "Le fonti del diritto dell'Unione europea," 10.

Aggiornata e ampliata nel 2015 dalla già citata Strategia per il Mercato Unico Digitale, l'Agenda ha indicato i tre pilastri fondamentali attorno ai quali si sono concentrati gli sforzi strategici dell'Unione: garantire un migliore accesso ai beni e servizi digitali per cittadini e imprese; creare un contesto favorevole e parità di condizioni per le reti digitali avanzate e i servizi innovativi; massimizzare il potenziale di crescita dell'economia digitale.[309] È nel solco tracciato dall'Agenda Digitale che nel 2016 viene adottato, come si è visto, il Regolamento generale sulla protezione dei dati, definito, con efficacia evocativa, "la pietra d'angolo della disciplina europea sui dati e le tecnologie digitali incentrata sulla persona".[310] Ed è proprio accanto alla stella polare del GDPR che si inizia a popolare una costellazione di atti normativi di settore: il Regolamento sulla portabilità dei servizi digitali;[311] il Regolamento sui blocchi geografici,[312] mirato a eliminare le discriminazioni ingiustificate basate sulla nazionalità o sul luogo di residenza; il Regolamento sulla libera circolazione dei dati non personali,[313] che consente alle imprese e alle amministrazioni pubbliche di archiviare e trattare dati non personali ovunque scelgano; il Regolamento sulla cybersicurezza,[314] che rafforza l'Agenzia dell'Unione Europea per la cybersicurezza e istituisce un quadro per la certificazione della sicurezza informatica di prodotti e servizi; la Direttiva sull'apertura dei dati,[315] che definisce norme comuni per la creazione di un mercato europeo per i dati posseduti dai governi.

---

[309] Commissione Europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final.
[310] Iannuzzi, "Le fonti del diritto dell'Unione europea," 10.
[311] Regolamento (UE) 2017/1128 del Parlamento Europeo e del Consiglio, del 14 giugno 2017, relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno, GUUE L 168, 30 giugno 2017.
[312] Regolamento (UE) 2018/302 del Parlamento Europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE, GUUE L 60 I, 2 marzo 2018.
[313] Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea, GUUE L 303, 28 novembre 2018.
[314] Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione Europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (*Regolamento sulla cibersicurezza*), GUUE L 151, 7 giugno 2019.
[315] Direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, GUUE L 172, 26 giugno 2019.

Alla luce di questa sommaria ricognizione di fonti normative, emerge con chiarezza lo sforzo dell'Unione – a dire il vero pionieristico – atto a dotarsi di regole per la società digitale. È a partire dal 2020, tuttavia, che il modello regolatorio europeo sembra vestirsi di una nuova consapevolezza.

Si pone, in questa nuova fase, anzitutto un tema di diritto pubblico: l'avvento dell'era digitale ha portato alla nascita di un potere sovrano di natura inedita, difficilmente inquadrabile nella tradizionale distinzione tra pubblico e privato, e che si caratterizza soprattutto per la sua natura eminentemente *tecnica*.[316] Le tecnologie digitali, nonché le infrastrutture sulle quali operano, sono per larghissima parte gestite e possedute da soggetti privati. Sono proprio le *Big Tech* ad assumere gran parte delle decisioni che riguardano il funzionamento e le specifiche tecniche dietro tecnologie di uso quotidiano quali il *cloud computing*, le piattaforme di *e-commerce* e i *social network*.[317] È questo il potere degli Stati "privati" digitali, di cui si è avuto modo di parlare diffusamente nel corso di questo lavoro.[318] L'interferenza di attori stranieri nella vita politica ed economica degli Stati Membri, poi, sebbene rappresenti una minaccia per certi versi già nota, ha assunto con l'evolversi della tecnologia forme e modalità inedite, ed è oggi condotta attraverso attività che spaziano dalle campagne di *disinformation* e *misinformation* online ai cyber-attacchi alle infrastrutture critiche che fanno largo affidamento sul digitale.[319]

Vi è poi il grande tema della competizione tra modelli non solo economici, ma anche, si è detto, normativi e regolamentari proposti dai maggiori attori internazionali coinvolti nella corsa al cyberspazio.[320] Il modello delineato dall'Unione Europea per la regolazione del digitale è stato definito "*rights-driven model*":[321] un approccio "guidato" dai diritti della persona, che riconosce a questa una posizione centrale e che si traduce, sul piano normativo, in strumenti di tutela dei diritti fondamentali e in un elevato livello

---

[316] Andrea Simoncini, "Sovranità e potere nell'era digitale," in *Diritti e libertà in Internet*, a cura di Tommaso Edoardo Frosini, Oreste Pollicino, Ernesto Apa e Marco Bassini (Milano: Mondadori Education, 2017), 20.

[317] Nathalie A. Smuha, "Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective," in *European Sovereignty: The Legal Dimension*, a cura di Gavin Barrett, Peter-Christian Müller-Graff, Jean-Philippe Rageade e Viktor Vadász (Cham: Springer, 2024), 136.

[318] *Vedi* capitolo I, paragrafo 1.

[319] Smuha, "Digital Sovereignty in the European Union," 138-139.

[320] *Vedi* capitolo II, paragrafo 1.1.

[321] Sul tema si rimanda a Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 105–145.

di protezione dei dati personali. Si tratta di un modello alternativo rispetto a quello seguito dai principali *competitor* dell'Unione nel settore delle nuove tecnologie, segnatamente Cina e Stati Uniti.[322] La cultura normativa statunitense riflette una visione ottimistica della tecnologia, seguendo un approccio "*market-driven*", guidato dal mercato. Alcuni degli elementi caratterizzanti questo modello regolatorio possono essere individuati nella tutela della libertà di espressione, nel mantenimento di forti incentivi all'innovazione e in un'ampia fiducia nella capacità autoregolatrice del mercato.[323] La matrice ideologica alla base di un simile approccio sarebbe da rintracciarsi, secondo parte della letteratura, nell'influenza culturale sortita dalle pretese cyber-libertarie e tecno-ottimiste radicate negli ambenti delle *Big Tech* e nei principali poli d'innovazione tecnologica internazionale.[324] Segnando una distanza ancora più marcata dal modello europeo, l'approccio cinese si caratterizza, di converso, per l'impiego diffuso delle nuove tecnologie in ottica di consolidazione del potere statale sui mercati. Adottando un modello "*state-driven*", la tecnologia diventa poi strumento di propaganda e sorveglianza di massa, realizzando l'"autoritarismo digitale" attraverso l'incisivo controllo del governo sulle grandi imprese *tech* nazionali.[325]

Un'ultima considerazione si rende necessaria sul tema della competizione internazionale: il tessuto economico europeo si contraddistingue per la presenza di una moltitudine di piccole e medie imprese, ancor di più nel settore delle nuove tecnologie; il fenomeno delle *Big Tech*, dunque, è oggi tratto distintivo delle economie americana e cinese.[326] Se è vero che "il cyberspazio è governato da chi ha accesso ai dati",[327] appare evidente il vantaggio strategico con cui Cina e Stati Uniti si accingono a disegnare lo spazio digitale globale, orientandone i valori e il *code*.

---

[322] A definire Cina e Stati Uniti "*competitor*" dell'Unione è proprio la Commissione Europea. Commissione Europea, *Una strategia europea per i dati*, COM(2020) 66 final, 19 febbraio 2020.
[323] Bradford, *Digital Empires*, 34-68.
[324] Bradford, 33-40. Per un riferimento sul tecno-ottimismo in ambito culturale e politico, si rimanda al "Manifesto Tecno-ottimista" dell'informatico e imprenditore statunitense Marc Andreessen. Marc Andreessen, "The Techno-Optimist Manifesto," *Andreessen Horowitz*, 16 ottobre 2023, https://a16z.com/the-techno-optimist-manifesto/.
[325] Bradford, *Digital Empires*, 69-104.
[326] Iannuzzi, "Le fonti del diritto dell'Unione europea," 18. Volgendo lo sguardo alla *leadership* globale nel settore digitale, emerge una netta preminenza di aziende con sede negli USA o in Cina. Fanno eccezione alcune realtà europee, come la piattaforma svedese di *streaming* musicale *Spotify*. 8
[327] Iannuzzi, 16.

Non desta sorpresa, allora, che nel discorso politico europeo si sia iniziato a discutere con incisività sempre maggiore di "sovranità europea" e, per quanto rileva in questa sede, di "sovranità digitale".[328] Il termine, come spesso accade quando il diritto è chiamato a occuparsi dell'innovazione tecnologica, si presta a molteplici letture e interpretazioni. Adottando una prospettiva squisitamente giuridica, la sovranità europea richiama alla mente l'autonomia dell'ordinamento giuridico dell'Unione. Sin dal celebre caso Costa contro ENEL, la Corte di Giustizia dell'Unione Europea (CGUE) ha riconosciuto la natura sovrana dell'ordinamento comunitario,[329] fonte autonoma di diritto nonché "ordinamento giuridico dotato della capacità di operare come un sistema auto-referenziale di norme, al contempo coerente e completo".[330]

Ricostruire una definizione tecnico-giuridica della "sovranità digitale", di converso, appare operazione ben più complessa. Ciò nonostante, il termine ha trovato largo impiego in una pluralità di documenti e dichiarazioni politiche nell'Unione e nei suoi Stati Membri. Primo tra tutti, si segnala il documento sugli "Orientamenti politici per la prossima Commissione Europea 2019-2024", con il quale l'allora candidata alla presidenza della Commissione, Ursula von der Leyen, ha gettato le basi del programma sul digitale di quella che da lì a breve sarebbe stata la nuova Commissione Europea: il perseguimento di "un'Europa più ambiziosa nello sfruttare le opportunità dell'era digitale in un contesto che garantisca la sicurezza e rispetti l'etica" e la necessità di "conseguire una sovranità tecnologica in alcuni settori tecnologici fondamentali", preso atto del ritardo che sconta l'economia europea nel settore delle nuove tecnologie.[331] In questa direzione sono da leggersi i successivi strumenti messi in campo dall'UE per affrontare le sfide della transizione digitale: la seconda strategia digitale quinquennale, Plasmare il

---

[328] Smuha, "Digital Sovereignty in the European Union," 130-132. Sul tema della sovranità digitale, imprescindibile il riferimento a Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy & Technology* 33 (agosto 2020): 369-378, doi:10.1007/s13347-020-00423-6

[329] Corte di Giustizia dell'Unione Europea, causa 6/64, *Costa contro ENEL*, ECLI:EU:C:1964:66.

[330] Smuha, "Digital Sovereignty in the European Union," 127-128. L'autrice fa riferimento alla capacità dell'UE di legiferare (Parlamento Europeo e Consiglio), giudicare (CGUE e tribunali nazionali), regolamentare (Commissione Europea e agenzie) e far rispettare il diritto dell'Unione (Commissione Europea e autorità nazionali).

[331] Ursula von der Leyen, *Orientamenti politici per la prossima Commissione europea 2019-2024* (Lussemburgo: Ufficio delle pubblicazioni dell'Unione Europea, 2020), 13, doi:10.2775/688283.

futuro digitale dell'Europa (2020);[332] il già citato Libro Bianco sull'intelligenza artificiale (2020);[333] la Bussola per il digitale 2030 (2021), strumento decennale volto a concretizzare le ambizioni di sovranità tecnologica europea entro il 2030;[334] la Strategia europea per i dati (2020), documento politico di riferimento per le misure politiche e gli investimenti a sostegno dell'economia dei dati sino al 2025.[335]

Alla fissazione di obiettivi strategici da parte della Commissione si è accompagnata un'intensa attività normativa del legislatore europeo, attraverso l'adozione di regolamenti che interessano tutte le dimensioni del digitale e che, nel loro complesso, seguono la sequenza "dato-algoritmo-piattaforma".[336]

Si è avuto modo di illustrare come l'attuale disciplina europea dei dati sia volta a favorirne la circolazione e il riutilizzo in un contesto di fiducia e sicurezza. È in tale ambito che si colloca il Regolamento (UE) 2022/868, *Data Governance Act* (DGA). Il Regolamento introduce strumenti per supervisionare il riutilizzo di dati pubblici e protetti, una disciplina specifica per la figura degli "intermediari di dati", e la promozione, tra le altre cose, della condivisione dei dati per motivi altruistici (cd. "altruismo dei dati").[337] Nel suo ambito di applicazione ricadono sia i dati pubblici sia i dati personali, con conseguente applicabilità, per questi ultimi, delle garanzie offerte dal GDPR. Al DGA si affianca poi il più recente Regolamento (UE) 2023/2854, *Data Act* (DA), approvato il 27 novembre 2023 e in vigore dall'11 gennaio 2024. Le sue disposizioni saranno applicabili a partire dal 12 settembre 2025. Il *Data Act*, tradotto in lingua italiana come "Legge europea sui Dati", introduce norme armonizzate per l'accesso equo ai dati e il loro utilizzo, con l'obiettivo di rendere l'Unione *leader* della *data economy*, sfruttando il potenziale

---

[332] Commissione Europea, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final.
[333] Commissione Europea, *Libro Bianco sull'intelligenza artificiale: Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final.
[334] Commissione Europea, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final.
[335] Commissione Europea, *Una strategia europea per i dati*, COM(2020) 66 final.
[336] *Vedi* capitolo I, paragrafo 1.2.
[337] 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*), GUUE L 152, 3 giugno 2022.

offerto dalla quantità sempre crescente di dati industriali e di dati prodotti dai dispositivi IoT.[338]

Sul fronte delle piattaforme digitali, l'approccio europeo appare da un lato volto a tutelare i diritti degli utenti, dall'altro a garantire un mercato digitale equo e contendibile. In tal senso, i Regolamenti (UE) 2022/1925 e 2022/2065, rispettivamente *Digital Markets Act* (DMA) e *Digital Services Act* (DSA), approvati dal Parlamento Europeo in rapida successione il 14 settembre e il 19 ottobre 2022.[339] Mentre il DSA traccia una disciplina organica per la responsabilità dei fornitori di servizi digitali e per la rimozione dei contenuti illeciti *online*, il DMA integra la normativa europea sulla concorrenza, introducendo una serie di obblighi e divieti per i c.d. *gatekeeper*, imprese che forniscono "servizi di piattaforma di base", designate in base a criteri oggettivi individuati dal regolamento stesso.[340]

All'analisi dell'AI Act, il Regolamento con cui si è provveduto a disciplinare, infine, la dimensione dell'algoritmo, sarà dedicato il presente capitolo. Prima, appare doveroso un breve accenno a un'altra dimensione fondamentale dello spazio digitale: la sicurezza cibernetica. Si segnala, a tal riguardo, l'approvazione, il 10 novembre 2022, della Direttiva NIS2 (*Network and Information System Security*),[341] che abroga la precedente Direttiva NIS in ragione degli sviluppi raggiunti dallo stato dell'arte nel

---

[338] 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*), GUUE L, 22 dicembre 2023.

[339] 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*), GUUE L 265, 12 ottobre 2022. 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*), GUUE L 277, 27 ottobre 2022.

[340] Regolamento (UE) 2022/1925, art. 3, par. 1: Un'impresa è designata come gatekeeper se: a) ha un impatto significativo sul mercato interno; b) fornisce un servizio di piattaforma di base che costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali; e c) detiene una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisisca siffatta posizione nel prossimo futuro.

[341] Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (*Direttiva NIS 2*), GUUE L 333, 27 dicembre 2022.

campo della sicurezza informatica.[342] L'obiettivo della direttiva è quello di ravvicinare ulteriormente le legislazioni degli Stati membri al fine di stabilire un livello comune elevato di cybersicurezza nell'Unione Europea, così da migliorare il funzionamento del mercato interno. Sempre nell'ottica di garantire la resilienza operativa dei sistemi informatici e di rete, con specifico riguardo al settore finanziario, si colloca per ultimo il Regolamento (UE) 2022/2554, *Digital Operational Resilience Act* (DORA),[343] del 14 dicembre 2022, che introduce in tale ambito una serie di obblighi specifici per gli operatori di settore.

Alla luce dei più recenti sviluppi normativi, il concetto di sovranità digitale sembra quindi potersi intendere come la capacità dell'Unione, dei suoi cittadini e degli operatori economici di esercitare un controllo sulla direzione, o meglio sul "destino", dello sviluppo delle nuove tecnologie nel territorio europeo, nonché sulle infrastrutture che in concreto rendono tali tecnologie operative.[344]

3. Dalla Proposta di Regolamento all'approvazione dell'AI Act

Già nel Libro Bianco del 2020 la Commissione Europea sottolineava come, in assenza di un quadro normativo europeo comune sull'intelligenza artificiale, vi sarebbe stato il rischio di una frammentazione del mercato interno. Non solo: sebbene la normativa europea in materia di diritti fondamentali, protezione dei dati e protezione dei consumatori fosse applicabile sin dal principio a sviluppatori e utilizzatori dell'IA, nulla garantiva che questa sarebbe stata sufficiente a far fronte ai rischi specifici posti dalle macchine intelligenti.[345] Sebbene nel testo, poi, la Commissione ribadisca di aver accolto con favore il lavoro svolto dall'AI HLEG,[346] per la prima volta sembra emergere a livello

---

[342] Per questa ricostruzione sommaria del quadro normativo europeo sul digitale si è fatto riferimento al già citato Iannuzzi, "Le fonti del diritto dell'Unione europea", cui si rimanda per una panoramica completa.
[343] Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011, GUUE L 333, 27 dicembre 2022.
[344] Smuha, "Digital Sovereignty in the European Union," 131-132. La definizione fornita dall'autrice fa eco a quella di Larsen in Benjamin Cedric Larsen, "The Geopolitics of AI and the Rise of Digital Sovereignty," *Brookings*, 8 dicembre 2022, https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.
[345] Commissione Europea, *Libro Bianco*, 11.
[346] Sull'AI HLEG, *vedi* capitolo II, paragrafo 1.2.

istituzionale la consapevolezza che accanto a strumenti di *soft law* e orientamenti etici non vincolanti sia necessario affiancare strumenti tradizionali di *hard law*, al fine garantire la certezza del diritto e la creazione di "un ecosistema di fiducia".[347]

Non è un caso, dunque, che il 19 febbraio 2020 la Commissione abbia avviato una consultazione pubblica online per raccogliere pareri e opinioni degli *stakeholder* sul Libro Bianco, registrando un generale consenso per l'adozione di una normativa nuova in materia di IA.[348] Delle considerazioni avanzate dai portatori di interessi si è poi tenuto conto nell'elaborazione della Proposta definitiva di regolamento, pubblicata nell'aprile del 2021.[349]

La Proposta si distingue per due elementi di novità: l'allontanamento, come si è detto, da principi etici incerti in favore dell'impiego di uno strumento di *hard law*; l'adozione di un regolamento in assenza di leggi nazionali sull'IA o di approcci divergenti tra gli Stati membri.[350] Del resto, ciò appare coerente con quelli che sono gli obiettivi dichiarati nella Relazione di accompagnamento alla Proposta: (i) assicurare che i sistemi di intelligenza artificiale, immessi sul mercato dell'Unione o utilizzati al suo interno, siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali; (ii) garantire la certezza del diritto, così da favorire gli investimenti e promuovere l'innovazione; (iii) migliorare la *governance* e assicurare un'applicazione efficace della normativa esistente; (iv) facilitare lo sviluppo di un mercato unico per applicazioni di intelligenza artificiale che siano lecite, sicure e affidabili, prevenendo al contempo il rischio di frammentazione del mercato.[351] Il "tipico" obiettivo di armonizzazione sovente perseguito dai regolamenti dell'UE è dunque qui sostituito da un obiettivo strategico-industriale. Si osserva poi, come già accaduto con il GDPR, una tensione tra due differenti finalità: la tutela dei diritti fondamentali dei cittadini europei e la promozione degli

---

[347] Commissione Europea, *Libro Bianco*, 3.

[348] Commissione Europea, *Proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale*, COM(2021) 206 final, 8. Da ora in avanti anche "Proposta di regolamento".

[349] Elena Mandarà, "Il Regolamento UE sull'intelligenza artificiale," in *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli (Rimini: Maggioli, 2024), 48–49.

[350] Alessandro Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (L'Aia: T.M.C. Asser Press, 2022), 166–167.

[351] Commissione Europea, *Proposta di regolamento*, 3.

interessi del mercato interno.[352] Quanto al rapporto tra i due diversi obiettivi, è stato evidenziato in letteratura come, stando al contenuto della Relazione, la regolazione del mercato non avvenga "'nel rispetto 'dei' diritti fondamentali, bensì 'per', o meglio, 'attraverso' il prisma dei diritti fondamentali".[353] La certezza del diritto, nonché la creazione di un ecosistema di fiducia, non può che passare dalla garanzia di uno *standard* di tutela elevato e uniforme dei diritti riconosciuti dalla Carta di Nizza,[354] in tutto il territorio dell'Unione.[355]

L'attenzione per i diritti fondamentali non pregiudica, in ogni caso, la scelta della base giuridica della Proposta di regolamento, individuata correttamente dalla Commissione nell'art. 114 TFUE,[356] e ulteriormente integrata dal riferimento all'art. 16 TFUE.[357] Si è dunque scelto di seguire l'*iter* previsto dalla procedura legislativa ordinaria. L'intervento regolatorio, del resto, è strumentale a garantire l'integrità del mercato interno, e difficilmente si sarebbe potuto agire diversamente.[358] È di tutta evidenza, infatti, che se ciascuno Stato membro avesse proceduto unilateralmente a disciplinare l'intelligenza artificiale, eventuali restrizioni nazionali avrebbero finito col violare il principio di libera circolazione dei servizi e dei prodotti nel territorio dell'Unione.[359]

---

[352] Mantelero, *Beyond Data*, 167.

[353] Così Cristina Schepisi, "Brevi note sulla 'dimensione europea' della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti," in *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce (Torino: Giappichelli, 2023), 61.

[354] Carta dei Diritti Fondamentali dell'Unione Europea*,* GUUE C 326, 26 ottobre 2012.

[355] Schepisi, "Brevi note," 61.

[356] Trattato sul Funzionamento dell'Unione Europea, GUUE C 326, 26 ottobre 2012, art. 114, par. 1: " ... Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale, adottano le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno".

[357] Trattato sul Funzionamento dell'Unione Europea, art. 16: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti …".

[358] Schepisi, "Brevi note," 71.

[359] Schepisi, 56.

Individuata la base giuridica, la Commissione rinviene nel regolamento l'atto giuridico più idoneo a perseguire gli obiettivi sopra delineati.[360] In ossequio all'art. 288 TFUE,[361] l'applicabilità diretta del regolamento appare come il migliore strumento normativo disponibile per affrontare la frammentazione giuridica e promuovere lo sviluppo di un mercato unico per i sistemi di IA.[362] Una scelta che, a ben vedere, si iscrive nel solco tracciato dalle più recenti iniziative normative europee in ambito digitale – *ex multis*, il GDPR, il *Data Governance Act*, il *Digital Markets Act* e il *Digital Services Act*.[363] Non si deve, tuttavia, cadere nell'errore di ritenere che il principio di diretta applicabilità del regolamento europeo comporti, come automatismo, l'efficacia diretta di tutte le norme in esso contenute. Per l'AI Act è vero piuttosto il contrario: il margine di discrezionalità lasciato agli Stati membri è tutt'altro che trascurabile, in particolare riguardo l'organizzazione del sistema di *governance* da predisporre a livello nazionale, le funzioni di controllo e le sanzioni,[364] come si avrà modo di approfondire in seguito.[365]

La versione definitiva della Proposta, infine, è stata sottoposta a una valutazione d'impatto, volta a vagliare diverse opzioni strategiche e individuare il miglior grado di intervento normativo.[366] Se l'obiettivo è assicurare il buon funzionamento del mercato unico, ci si è chiesti quale fosse la strada migliore per raggiungerlo. Si è quindi optato per una regolazione orizzontale, in alternativa a uno strumento legislativo verticale che avrebbe previsto una disciplina specifica per i diversi settori in cui i sistemi di intelligenza artificiale sono suscettibili di applicazione, o a una regolazione puntuale rivolta a ciascun prodotto *AI powered*.[367] Il modello regolatorio proposto dalla Commissione, viceversa, riguarda sì tutti i sistemi di IA (da qui, il carattere orizzontale), ma introduce in capo a produttori, *deployer* e utilizzatori divieti, obblighi e adempimenti procedurali

---

[360] Commissione Europea, *Proposta di regolamento*, 7.
[361] Trattato sul Funzionamento dell'Unione Europea, art. 288, secondo comma: "Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri".
[362] Commissione Europea, *Proposta di regolamento*, 7-8.
[363] Schepisi, "Brevi note," 71.
[364] Schepisi, "Brevi note," 71-72.
[365] Sull'approccio regolatorio perseguito dall'AI Act, *vedi* capitolo III.
[366] Commissione Europea, *Proposta di regolamento*, 10.
[367] Schepisi, "Brevi note," 56.

diversamente gradati in base al livello di rischio che tali sistemi pongono ai diritti fondamentali.[368]

La scelta di un approccio c.d. *risk-based* era suggerita, per altro, già dal Libro Bianco sull'Intelligenza Artificiale. Il documento ribadiva la necessità di un quadro normativo che, preso atto della capacità dell'IA di generare danni tanto materiali quanto immateriali, si concentrasse primariamente sulla riduzione al minimo dei diversi rischi di danno potenziale.[369] Nell'adottare espressamente un modello d'intervento basato sul rischio, la Proposta appare quindi coerente con il documento programmatico che l'ha preceduta. La Commissione Europea, inoltre, motiva tale scelta evidenziando la natura *future-proof* e *innovation-friendly* di un simile approccio, concepito per intervenire solo laddove strettamente necessario nel rispetto del principio di proporzionalità.[370]

In linea con tale impostazione, la Proposta delinea una vera e propria tassonomia del rischio. Contestualmente alla presentazione dell'atto, la Commissione ha infatti diffuso – sebbene non attraverso canali ufficiali, bensì durante seminari e *workshop* – una grafica piramidale volta a illustrare la logica sottesa al modello regolatorio prescelto.[371] La piramide concettuale categorizza i sistemi di IA in base ai diversi livelli di rischio che questi pongono in concreto per i diritti fondamentali, distinguendo tra: "rischio inaccettabile", categoria in cui ricadono le applicazioni di IA che, nella prospettiva della Commissione, dovrebbero essere vietate, salve specifiche eccezioni puntualmente delineate; "alto rischio", per i sistemi connotati da un significativo potenziale di danno, cui è dedicato gran parte del complesso e articolato *corpus* di disposizioni contenute nella Proposta; "rischio limitato", sistemi per i quali si prevedono requisiti regolamentari modesti, incentrati principalmente su obblighi di trasparenza; "rischio minimo o nullo", in cui ricadono le applicazioni di IA giudicate prive di rischio o connotate da un rischio trascurabile, e che sono conseguentemente esentate da ogni obbligo.[372]

---

[368] Schepisi, 54.
[369] Commissione Europea, *Libro Bianco*, 11-12.
[370] Commissione Europea, *Proposta di regolamento*, 3.
[371] Theodore Christakis e Theodoros Karathanasis, "Tools for Navigating the EU AI Act: (2) Visualisation Pyramid," *HAL Open Science*, n. hal-04845277f (marzo 2024):4, https://hal.univ-grenoble-alpes.fr/hal-04845277v1.
[372] Christakis e Karathanasis, 4-5.

Alla luce di quanto sin ora considerato, è possibile così riassumere i tratti salienti della Proposta del 2021: uno strumento legislativo orizzontale, orientato alla promozione dell'innovazione e al funzionamento del mercato interno, dotato di efficacia diretta; un approccio basato sui diritti fondamentali (*rights-driven*) e calibrato su diversi livelli di rischio (*risk-based*), e che non può che comportare, nella costruzione di una tassonomia del rischio, un bilanciamento *ex ante* tra i diritti fondamentali e gli interessi del mercato unico, nonché tra i diversi diritti fondamentali tra loro.[373]

Così formulata, la Proposta è quindi passata all'esame dei co-legislatori. Durante l'esame del Consiglio, la difficoltà nel conciliare le posizioni dei diversi Starti membri ha portato alla produzione di numerosi testi di compromesso, per poi giungere alla versione finale di bozza il 6 dicembre 2022.[374] La posizione negoziale del Parlamento Europeo è stata adottata sei mesi dopo, il 14 giugno 2023, con la pubblicazione del testo emendato. Le modifiche apportate al testo hanno riguardato, tra le altre cose, la regolamentazione dei c.d. "modelli di fondazione" (*foundation model*s).[375] Per *foundation models*, in letteratura scientifica, si è soliti intendere qui modelli di apprendimento automatico *deep learning* addestrati su enormi quantità di dati, tali da permetterne l'utilizzo in una pluralità di contesti applicativi. [376] L'intelligenza artificiale generativa, e in particolare i *Large Language Models*,[377] sono comunemente definiti modelli di fondazione.[378]

L'interesse del Parlamento Europeo verso questo tipo di modelli è da ricollegarsi ad alcuni eventi di rilievo verificatisi durante la procedura di negoziazione, primo tra tutti, per impatto, la messa in commercio di ChatGPT nel novembre 2022.[379] L'architettura

---

[373] Schepisi, "Brevi note," 67.
[374] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 49.
[375] Mandarà, 49.
[376] Il termine "*foundation models"* è stato utilizzato per la prima volta nel 2021 dal *Center for Research on Foundation Models* dello *Stanford Institute for Human-Centered Artificial Intelligence* nel rapporto *On the Opportunities and Risks of Foundation Models*. Questo studio ha evidenziato una tendenza emergente nel campo del *machine learning*: l'uso predominante di poche architetture di *deep learning* per lo sviluppo di diversi sistemi di IA. I modelli di fondazione sono quindi definiti come sistemi di *machine learning* addestrati su enormi quantità di dati, capaci di svolgere una vasta gamma di compiti. Center for Research on Foundation Models, "On the Opportunities and Risks of Foundation Models," *arXiv*, n. arXiv:2108.07258 (agosto 2021), https://arxiv.org/abs/2108.07258.
[377] Per una definizione di LLM, *vedi* nota 163.
[378] Più correttamente, sovente i modelli di fondazione rappresentano l'architettura alla base dei sistemi di IA generativa.
[379] Christakis e Karathanasis, "Tools for Navigating the EU AI Act," 5.

GPT, alla base del funzionamento del celebre *chatbot*, rappresenta infatti un esempio paradigmatico di modello di fondazione. Sul punto, preme sottolineare come la versione definitiva dell'AI Act, a ogni modo, non presenti alcun riferimento ai modelli di fondazione. Il testo fa riferimento unicamente ai "modelli di IA per finalità generali" (*general purpose AI models*) e ai "sistemi di IA per finalità generali" (*general purpose AI systems*), sebbene la definizione normativa dei primi sembri ricalcare, in larga parte, proprio le principali caratteristiche dei modelli di fondazione (tra cui l'addestramento con grandi quantità di dati su larga scala e il grado significativo di generalità).[380] A tali modifiche si è accompagnata l'introduzione di una nuova categoria di rischio, non contemplata dalla Proposta della Commissione: il c.d. "rischio sistemico", di cui si tratterà in seguito.[381]

Gli interventi del Parlamento, poi, si sono distinti soprattutto per una spiccata attenzione al tema dei diritti fondamentali. Si segnala, a tal riguardo, la proposta di introdurre l'obbligo per i fornitori dei sistemi di IA ad "alto rischio" di effettuare una valutazione d'impatto sui diritti fondamentali, sebbene nel testo definitivo del Regolamento la portata di detto obbligo appaia sensibilmente ridimensionata.[382]

Si è infine aperta la fase dei c.d. "triloghi", i negoziati interistituzionali tra Consiglio, Commissione e Parlamento. Al termine di un anno segnato dal succedersi di confronti serrati, le istituzioni dell'Unione hanno raggiunto un accordo politico il 9 dicembre 2023.[383] L'*iter* si è quindi concluso con l'approvazione formale del testo definitivo da parte di tutti gli Stati membri il 2 febbraio 2024, e il successivo voto in seduta plenaria del Parlamento Europeo il 24 marzo 2024.[384] Con la pubblicazione in Gazzetta Ufficiale il 2 luglio 2024 e l'entrata in vigore del Regolamento il successivo 2 agosto 2024,[385] l'UE si è dotata di uno strumento normativo unico nel suo genere, il cui

---

[380] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 91.
[381] *Vedi* capitolo III, paragrafi 2 e 3.4.
[382] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 49.
[383] Luca Tremolada, "AI Act, tutto quello che sappiamo finora e qualche considerazione," *Il Sole 24 Ore*, 16 dicembre 2023, https://www.infodata.ilsole24ore.com/2023/12/16/ai-act-tutto-quello-che-sappiamo-finora-e-qualche-considerazione/
[384] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 50.
[385] Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (*Regolamento sull'intelligenza artificiale*), GUUE L, 12 luglio 2024.

impatto resta tuttavia da verificare. Il Regolamento europeo sull'intelligenza artificiale conosce soltanto adesso la sua fase applicativa, e la sfida del futuro sarà tradurre i principi e le disposizioni normative in prassi operativa. L'esito di questa partita regolatoria, in larga parte, dipenderà dalla tenuta del nuovo sistema di *governance* alla prova dell'evoluzione tecnologica.

III. LA GESTIONE DEL RISCHIO E LA CLASSIFICAZIONE DEI SISTEMI DI IA NELL'AI ACT

1. L'ambito di applicazione dell'AI Act

Nel corso del lungo *iter* conclusosi con l'approvazione del testo definitivo dell'AI Act, diversi sforzi sono stati dedicati alla ricerca di una puntuale definizione normativa per l'intelligenza artificiale. Il punto è di primaria importanza: definire l'oggetto della regolazione è essenziale per delimitare l'ambito di applicazione materiale del Regolamento; di converso, la definizione normativa non può non tenere conto degli obiettivi perseguiti dall'intervento regolatorio.[386]

Le sfide affrontate dal legislatore europeo sono, come si è visto, esemplificative delle difficoltà che s'incontrano nel regolare le nuove tecnologie.[387] Una definizione troppo generica può essere foriera di dubbi interpretativi, se poi questa dovesse dimostrarsi troppo ampia nel suo momento applicativo, si corre anche il rischio di una sovra-regolamentazione del settore.[388] Una nozione di IA che si concentri eccessivamente su tecnicismi e aspetti di dettaglio, d'altro canto, presenta più di una criticità. Si pensi a una disciplina dedicata, in via esclusiva, alla regolazione del *machine learning*: produttori e fornitori di IA potrebbero optare per algoritmi di diversa natura, così da evitare di essere soggetti agli obblighi prescritti.[389] In un tale scenario, gli approcci *rule-based*, i sistemi esperti e l'intelligenza artificiale simbolica finirebbero per essere favoriti, a discapito dell'innovazione e di approcci sub-simbolici rivelatisi particolarmente efficienti in diversi contesti.[390]

---

[386] Ruschemeier, "AI as a Challenge for Legal Regulation," 366.
[387] Ruschemeier, 364.
[388] Schepisi, "Brevi note," 58.
[389] Andrea Renda e Alex Engler, "What's in a Name? Getting the Definition of Artificial Intelligence Right in the EU's AI Act," *CEPS Explainer* (febbraio 2023): 2, https://www.ceps.eu/ceps-publications/whats-in-a-name/.
[390] Sul tema dei diversi approcci all'intelligenza artificiale, *vedi* capitolo I, paragrafo 2. Di diverso avviso e a favore di una definizione normativa di IA che includa solo il *machine learning*, e in particolare l'*unpredictable machine learning, si veda* Patrick Grady, "The AI Act Should Be Technology-Neutral," *Center for Data Innovation* (febbraio 2023), https://www2.datainnovation.org/2023-ai-act-technology-neutral.pdf. Ad avviso di chi scrive, tuttavia, l'articolo presenterebbe un'incongruenza: sebbene si sostenga

Una possibile soluzione a tale dilemma, ad avviso di certa letteratura, sarebbe quella di costruire un quadro normativo *techonology neutral*: il legislatore dovrebbe evitare di fare distinzioni tra le diverse tecnologie, a meno che tali distinzioni non siano funzionali all'obiettivo che s'intende perseguire con l'intervento regolatorio.[391] Parte considerevole della dottrina si mostra, poi, fortemente critica nei confronti di quelle proposte legislative che si concentrano esclusivamente sulla disciplina di specifiche configurazioni tecniche.[392] Nel documento *Better Regulation Toolbox*, pubblicato dalla Commissione Europea nel 2021, si afferma che "[la legislazione europea] dovrebbe puntare alla neutralità tecnologica e cercare di evitare di concentrarsi ["*lock-in"*] su una specifica soluzione tecnologica o tecnica".[393] Tra i vantaggi che la Commissione attribuisce a un siffatto tipo di regolazione, quello di essere flessibile e "a prova di futuro" (*future-proof*).[394] Alla luce della vasta – e raramente concorde – produzione dottrinale sul tema, la neutralità tecnologica da un lato consentirebbe al potere pubblico di astenersi dall'individuare il vincitore della competizione tecnologica, lasciando libero spazio alla concorrenza e all'innovazione; dall'altro, scongiurerebbe l'obsolescenza della normativa e degli interventi regolatori.[395] Una definizione ampia di IA, in definitiva, consentirebbe di includere approcci e algoritmi innovativi d'intelligenza artificiale, in un settore caratterizzato da rapidi progressi evolutivi.[396]

Si è detto sulla difficoltà di rintracciare una definizione di "Intelligenza Artificiale" condivisa dalla comunità scientifica.[397] Nell'AI Act, il legislatore europeo rinuncia a

---

la necessità di un approccio regolatorio *technology neutral,* si suggerisce una regolazione dedicata esclusivamente a un tipo di algoritmi specifici, contraddicendo di fatto l'assunto iniziale.

[391] Lyria Bennett Moses, "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target," *Law, Innovation and Technology* 5, n. 1 (2013): 15, doi:10.5235/17579961.5.1.1.

[392] *Si veda*, tra gli altri Philipp Hacker, Andreas Engel e Marco Mauer, "Regulating ChatGPT and Other Large Generative AI Models," in *FAccT '23: The 2023 ACM Conference on Fairness, Accountability, and Transparency* (New York: Association for Computing Machinery, 2023), 1112–1123.

[393] Commissione Europea, *Better Regulation Toolbox* (2023), 174.

[394] Commissione Europea, *Better Regulation Toolbox*, 174.

[395] Un'efficace ricognizione della dottrina sul tema è presente nel *working paper* di Marco Almada, "Two Dogmas of Technology-Neutral Regulation," *SSRN* (settembre 2024), doi:10.2139/ssrn.4953377. Per una voce critica sul principio di neutralità tecnologica, imprescindibile il riferimento a Brad A. Greenberg, "Rethinking Technology Neutrality," *Minnesota Law Review* 100 (marzo 2016): 1495–1562.

[396] Renda e Engler, "What's in a Name?," 2-3.

[397] *Vedi* capitolo I, paragrafo 2.

definire l'intelligenza artificiale in sé, limitandosi a fornire, all'art. 3, la definizione di "sistema di IA":[398] "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'*input* che riceve come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".[399] I criteri in base ai quali individuare un sistema di IA, dunque, sembrerebbero essere l'autonomia, l'adattabilità e la capacità inferenziale.[400] Un chiarimento interpretativo è poi fornito dal Considerando 12: per autonomia deve intendersi "un certo grado di autonomia di azione rispetto al coinvolgimento umano" o la "capacità di funzionare senza l'intervento umano"; l'adattabilità si riferisce alle "capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso"; quanto alla capacità inferenziale, infine, si fa riferimento "al processo di ottenimento degli *output*, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da *input* o dati".[401]

La nozione di "sistema di IA" dell'art. 3 ha, in primo luogo, l'indubbio merito di allinearsi a quella fornita, sul piano internazionale, dall'Organizzazione per la cooperazione e lo sviluppo economico.[402] È discusso, invece, se l'approccio seguito dal legislatore europeo possa definirsi o meno *technology neutral*, considerando che il termine non fa la sua apparizione nel testo del Regolamento.[403] Si tratta, in ogni caso, di una definizione piuttosto inclusiva: le tecniche di inferenza di un sistema di IA comprendono infatti sia "approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi", sia "approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione

---

[398] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 51.
[399] Regolamento (UE) 2024/1689, art. 3, par. 1, n.1.
[400] Tervel Bobev, "Defining AI in the AI Act: Pin the Tail on the System," *KU Leuven CiTiP Blog*, 2 aprile 2024, https://www.law.kuleuven.be/citip/blog/defining-ai-in-the-ai-act-pin-the-tail-on-the-system/.
[401] Regolamento (UE) 2024/1689, considerando 12.
[402] Bobev, "Defining AI in the AI Act".
[403] Almada, "Two Dogmas of Technology-Neutral Regulation," 3-4. Come sottolineato dall'autore, l'unico riferimento alla neutralità tecnologica è presente al Considerando 119 del Regolamento, che riguarda però l'interpretazione del *Digital Services Act*.

simbolica ...".[404] Stando alla lettera del Considerando 12, in altre parole, rispetterebbero il requisito della "capacità inferenziale" sia le inferenze di tipo induttivo che deduttivo, sia gli approcci di *machine learning* sia i tradizionali sistemi esperti.[405] L'elencazione delle tecniche fornita dal Considerando, per altro, non ha carattere esaustivo, e nulla impedisce che in futuro, in ambito applicativo, non si ritengano sistemi di IA ai fini del regolamento anche sistemi che adottano approcci statistici e di stima bayesiana. Proprio questi, nell'Allegato I della Proposta della Commissione, erano indicati quale "terza via" all'IA, accanto al *machine learning* e agli approcci basati sulla conoscenza.[406] Allo stesso tempo, la definizione prospettata dalla Commissione ha sollevato diverse perplessità ed è stata infine abbandonata dal testo definitivo, poiché suscettibile di attrarre nel perimetro regolatorio gran parte dei *software* esistenti.[407] Tale preoccupazione non è condivisa da tutta la letteratura: occorre ricordare che non tutti i sistemi di IA sono soggetti agli obblighi imposti dal Regolamento. L'AI Act, si è visto, adotta un approccio basato sul rischio, e a un ambito di applicazione esteso non corrisponde necessariamente un fenomeno di *over-regulation*.[408]

Permangono, tuttavia, alcune incertezze interpretative. Il Considerando 12 fa riferimento ai "livelli di autonomia variabili" che può presentare un sistema, ma non fornisce un'indicazione chiara circa la soglia minima d'autonomia necessaria rispetto all'intervento umano.[409] L'autonomia, poi, implicherebbe di per sé una certa capacità di adattamento. Non si comprende allora perché l'art. 3 sembri considerare l'adattamento alla stregua di un requisito opzionale, nel prevedere che un sistema "possa" (o meno?) presentare adattamento dopo la sua diffusione.[410] In questo contesto, la capacità

---

[404] Regolamento (UE) 2024/1689, considerando 12.
[405] Una nota terminologica: la versione in lingua italiana dell'art. 3 dell'AI Act definisce un sistema di IA come sistema che "*deduce*" dagli *input* ricevuti come generare diversi *output.* Come chiarito dal Considerando 12 e dalla versione in lingua inglese del Regolamento, però, dovrebbe più correttamente parlarsi di un sistema che "inferisce", dal momento che alla base del suo funzionamento ben potrebbe esserci sia un approccio di tipo logico-deduttivo, sia un approccio di tipo "induttivo", quale è il *machine learning* adoperato in fase di *training*.
[406] Bobev, "Defining AI in the AI Act".
[407] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 52-53.
[408] Renda e Engler, "What's in a Name?," 3-4.
[409] Bobev, "Defining AI in the AI Act".
[410] Bobev, "Defining AI in the AI Act".

inferenziale si distingue come l'unico requisito veramente dirimente per l'identificazione di un sistema di IA.

Quanto all'ambito di applicazione territoriale del Regolamento, l'approccio scelto dal legislatore europeo sembra seguire, per certi versi, quanto già sperimentato con il GDPR.[411] Si è fatto riferimento alla scelta rivoluzionaria di conferire al Regolamento generale sulla protezione dei dati un ambito di applicazione c.d. "a-territoriale".[412] Tale decisione è coerente con le aspirazioni di sovranità digitale dell'Unione, ma anche e soprattutto con la necessità di assicurare una protezione effettiva ai diritti fondamentali dei cittadini europei, considerata la natura immateriale e transfrontaliera dello spazio digitale. L'art. 2 dell'AI Act prevede quindi che il regolamento si applica "ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo",[413] nonché ai loro rappresentanti autorizzati. Parimenti, il Regolamento si applica ai *deployer* dei sistemi di IA che hanno il loro stabilimento o sono situati nell'UE.[414] Ma l'intento del legislatore emerge con ancora maggiore evidenza dalla previsione secondo cui il Regolamento trova applicazione anche nei confronti di fornitori e *deployer* stabiliti o situati in paesi terzi, qualora l'*output* generato dal sistema sia utilizzato all'interno dell'Unione.[415] Ad assumere rilievo, dunque, non è tanto il luogo in cui è situato il fornitore né quello in cui si trova l'utente, bensì la localizzazione del sistema di IA e il luogo in cui il suo *output* è utilizzato. Si configura così un tentativo di regolazione indiretta delle attività di soggetti giuridici stranieri.[416]

Nell'ambito di applicazione soggettivo del Regolamento ricadono le figure dei "fornitori" e "*deployer*" di sistemi di IA, ma anche gli importatori e i distributori di tali sistemi, nonché i fabbricanti di prodotti che immettono sul mercato o mettono in servizio

---

[411] Ruschemeier, "AI as a Challenge for Legal Regulation," 371.
[412] Il riferimento va sempre a Merlin Gömann, "The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement," *Common Market Law Review* 54, n. 2 (aprile 2017): 567–590, doi:10.54648/COLA2017035.
[413] Regolamento (UE) 2024/1689, art. 2, par. 1, lett. a).
[414] Regolamento (UE) 2024/1689, art. 2, par. 1, lett. b).
[415] Regolamento (UE) 2024/1689, art. 2, par. 1, lett. c).
[416] Ruschemeier, "AI as a Challenge for Legal Regulation," 371.

un sistema di IA insieme al loro prodotto, con il loro nome o marchio. Quanto alla figura del fornitore, si rileva come la sua definizione abbia sollevato diverse criticità già durante l'elaborazione della Proposta legislativa. Gli *stakeholder* lamentavano che una nozione eccessivamente ampia di "fornitore" avrebbe potuto comportare l'applicazione indiscriminata dei medesimi obblighi a soggetti diversi, a vario titolo coinvolti nello sviluppo di un sistema di IA.[417] Si è dunque spinto per una distinzione puntuale delle responsabilità dei soggetti parte della c.d. *AI supply chain*, di modo da garantire che gli obblighi previsti dal Regolamento gravino solo su chi si trova nella posizione effettiva di poterli adempiere.[418]

Le istanze degli *stakeholder* sono state accolte solo parzialmente, e nella versione definitiva del Regolamento la nozione di fornitore resta piuttosto generica. Questi è infatti definito come la persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che sviluppa o fa sviluppare un sistema di IA o un modello di IA per finalità generali, lo immette sul mercato o lo mette in servizio con il proprio nome o marchio, a titolo oneroso o gratuito.[419] Quanto alla peculiare figura del *deployer*, con detto termine s'intende, ai fini del regolamento, la persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la propria autorità, ad esclusione dell'utilizzo nel corso di attività personali non professionali.[420] L'importatore è invece definito come il soggetto, ubicato o stabilito nell'Unione Europea, che per primo immette sul mercato un sistema di IA recante il nome o il marchio di un produttore extra-UE. Tale definizione pone quindi l'accento sull'origine extra-comunitaria del sistema.[421] Il distributore, infine, costituisce una figura residuale: una persona fisica o giuridica nella

---

[417] Nikos Th. Nikolinakos, *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act* (Cham: Springer, 2023), 522.

[418] Nikolinakos, *EU Policy and Legal Framework for Artificial Intelligence*, 528.

[419] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 3: "«fornitore»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito".

[420] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 4: "«*deployer*»: una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale".

[421] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 6: "«importatore»: una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo".

catena di approvvigionamento, *diversa dal fornitore o dall'importatore*, che mette a disposizione un sistema di IA sul mercato dell'Unione.[422]

L'AI Act trova applicazione anche nei confronti delle "persone interessate che si trovano nell'Unione".[423] La disposizione risulta piuttosto oscura, dal momento che, diversamente dagli altri soggetti menzionati, l'art. 3 non fornisce alcuna definizione di "persone interessate". In fase di elaborazione del testo, il Parlamento Europeo aveva proposto di utilizzare la diversa nozione di "persone danneggiate", in conseguenza dell'impatto negativo di un sistema di IA sulla salute, la sicurezza o i diritti fondamentali.[424] L'attuale formulazione appare meno chiara, ma sembra riflettere l'intento di garantire una tutela più inclusiva.

Le disposizioni del Regolamento, a ogni modo, non si applicano ai sistemi di IA messi sul mercato esclusivamente per scopi militari, di difesa o di sicurezza nazionale, né all'utilizzo di *output* (di sistemi non immessi nel mercato interno) per i medesimi scopi.[425] Come altra esenzione rilevante, si segnala per ultimo quella prevista per sistemi, modelli o *output* sviluppati e messi in servizio per scopi di ricerca e sviluppo.[426]

2. Il risk-based approach

Come anticipato dalla Proposta legislativa della Commissione, l'AI Act segue un approccio regolatorio orizzontale e "a strati", gradando gli obblighi prescritti in funzione del rischio posto da ciascun sistema di IA.[427] Tale impostazione trova una prima esplicitazione all'interno del Considerando 26, dove si ribadisce che, al fine di stabilire regole proporzionate ed efficaci per l'intelligenza artificiale, è "opportuno avvalersi di un approccio basato sul rischio".[428] La regolamentazione del rischio, lungi dal rappresentare una novità nel panorama giuridico europeo, è spesso oggetto di atti normativi in materia

---

[422] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 7: "«distributore»: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione".
[423] Regolamento (UE) 2024/1689, art. 2, par. 1, lett. g).
[424] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 57.
[425] Regolamento (UE) 2024/1689, art. 2, par. 3.
[426] Regolamento (UE) 2024/1689, art. 2, par. 8. Non rientrano nell'esclusione, tuttavia, le c.d. "prove in condizioni reali".
[427] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 57.
[428] Regolamento (UE) 2024/1689, considerando 26.

di *welfare*, salute e ambiente, nonché, con frequenza sempre maggiore dalla seconda metà del 2010, tratto caratteristico del quadro normativo europeo sul digitale.[429]

Sotto il profilo definitorio, all'art. 3 del Regolamento il "rischio" è definito come "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso".[430] Significativamente, una simile nozione di rischio la si ritrova anche nel Regolamento (UE) 2017/745 sui dispositivi medici,[431] ed è, adottando una prospettiva d'insieme, coincidente con quanto stabilito nel *New Legislative Framework* (NLF), il quadro armonizzato di riferimento per la regolamentazione dei prodotti nel mercato interno, di cui l'AI Act è da considerarsi parte integrante.[432]

Per esigenze espositive, nell'illustrare gli obblighi che l'AI Act pone a carico degli operatori dei diversi sistemi di IA, appare utile ricorrere alla già menzionata "piramide del rischio". Lo schema elaborato dalla Commissione ha natura divulgativa e non certo tecnico-giuridica, eppure fornisce un'efficace chiave di lettura, un *iter* logico ben definito che porta a distinguere tra sistemi: (i) a rischio inaccettabile, e pertanto vietati; (ii) ad alto rischio, soggetti a specifici obblighi; (iii) a rischio limitato, sottoposti per lo più a obblighi di trasparenza; e (iv) a rischio minimo o nullo. All'interno di questa categorizzazione, parte della dottrina suggerisce di aggiungere la nozione di "rischio sistemico", in conseguenza di quanto previsto per i modelli di IA per finalità generali all'art. 51.[433]

Adottando la lente del giurista e volgendo lo sguardo direttamente al testo del Regolamento, al Capo II troviamo elencate le "pratiche di IA vietate", espressione dalla portata più ampia rispetto alla categoria, invero affine, dei "sistemi a rischio inaccettabile". Il Capo III definisce il regime applicabile ai sistemi di IA qualificati come

---

[429] Erik Longo, "La disciplina del rischio digitale," in *La regolazione europea della società digitale*, a cura di Franco Pizzetti (Torino: Giappichelli, 2024), 72. Sul come l'intera attività normativa europea sul digitale sia definita in termini di regolazione del rischio, l'autore rimanda ad Alberto Alemanno, "The Past, Present and Future of Risk Regulation," *European Journal of Risk Regulation* 8, n. 1 (marzo 2017): 1–3, doi:10.1017/err.2017.4.

[430] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 2.

[431] Così Longo, "La disciplina del rischio digitale," 73. Regolamento (UE) 2017/745 del Parlamento Europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio, GUUE L 117, 5 maggio 2017.

[432] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 57.

[433] Il riferimento è sempre a Christakis e Karathanasis, "Tools for Navigating the EU AI Act". Sui modelli di IA per finalità generali, *vedi* paragrafo 3.4.

ad alto rischio, mentre il Capo IV si concentra in modo specifico sugli obblighi di trasparenza gravanti sui fornitori e sui *deployer* di taluni sistemi di IA. Il Capo V traccia una disciplina per i modelli di IA per finalità generali e, in particolare, per quei modelli che pongono un rischio sistemico.

Esaurita la disamina degli obblighi previsti per le diverse categorie di sistemi, si procederà a svolgere alcune considerazioni critiche in merito al modello di *governance* emergente dall'AI Act.

3. La classificazione dei sistemi di IA

3.1. Le pratiche vietate

Si è visto come il modello regolatorio *risk-based* postuli un bilanciamento *ex ante* tra i diritti fondamentali e le esigenze del mercato unico, nonché una valutazione sui diversi diritti fondamentali che vengono in rilievo. L'art. 5 del Regolamento dunque, alla luce di una siffatta valutazione, fornisce un elenco di pratiche vietate in ragione della loro incompatibilità assoluta con i valori fondanti dell'UE. Tale elenco, in ogni caso, non esclude l'operatività di ulteriori divieti, laddove una specifica pratica di IA violi altre disposizioni di diritto dell'Unione.[434] In ragione del rischio inaccettabile associato ai sistemi che impiegano simili pratiche, i divieti di cui all'art. 5 trovano applicazione già a partire dal 2 febbraio 2025, congiuntamente alle disposizioni generali del Capo I.[435]

La prima pratica vietata è l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che impiegano tecniche subliminali ovvero tecniche volutamente manipolative o ingannevoli.[436] Tali tecniche devono avere lo scopo o l'effetto di distorcere materialmente il comportamento di una persona (o di un gruppo di persone). Sul punto, si noti che il ricorso a tecniche subliminali o manipolative *per se* non è sufficiente a fondare il divieto, e il legislatore europeo ha inteso ancorarlo a un criterio oggettivo. Allo stato attuale, infatti, le conoscenze scientifiche non consentono di stabilire con precisione quando un comportamento possa dirsi "distorto"; il divieto si applica quindi alle sole ipotesi in cui sia stata pregiudicata in modo considerevole la capacità di

[434] Regolamento (UE) 2024/1689, art. 5, par. 8.
[435] Regolamento (UE) 2024/1689, art. 113.
[436] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. a).

una persona di prendere una decisione informata, inducendola ad assumere una determinazione che, altrimenti, non avrebbe preso.[437] Ulteriore requisito richiesto è che tale decisione provochi, o possa ragionevolmente provocare, un danno significativo alla persona che l'ha assunta, ad altra persona o a un gruppo di individui.[438]

Quanto alle tecniche subliminali, il Considerando 29 fornisce alcuni esempi pratici, tra cui "stimoli audio, grafici e video che le persone non sono in grado di percepire ... che sovvertono o pregiudicano l'autonomia, il processo decisionale o la libera scelta di una persona". Tale effetto, prosegue il Considerando, potrebbe essere amplificato dall'impiego di interfacce cervello-macchina o dalla realtà virtuale.[439] Ciò nonostante, la dottrina ha spesso criticato l'assenza di una definizione sufficientemente chiara di "tecniche subliminali" ai fini del Regolamento. Stando alla lettera dell'art. 5, le tecniche subliminali oggetto di divieto sono quelle che "agiscono senza che una persona ne sia consapevole". Ciò che è subliminale, tuttavia, è tale proprio in quanto agisce in assenza di consapevolezza, e la specificazione non sembra contribuire in alcun modo a delimitare l'ambito applicativo della norma.[440] Una persona, poi, ben potrebbe essere messa a conoscenza dell'esistenza di uno stimolo sensoriale che non è in grado di percepire, ma ignorare del tutto come questo agisca e che influenza avrà sulla sua capacità decisionale.[441]

Per le tecniche manipolative o ingannevoli, l'operatività del divieto sembrerebbe scattare allorquando queste siano *volutamente* utilizzate per distorcere il comportamento di una persona o un gruppo di persone. Parte della dottrina evidenzia come la necessità di provare l'intenzionalità della manipolazione rischi di compromettere l'efficacia della

---

[437] Rostam J. Neuwirth, "Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)," *Computer Law & Security Review* 48 (aprile 2023), doi:10.1016/j.clsr.2023.105798.

[438] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. a).

[439] Regolamento (UE) 2024/1689, considerando 29.

[440] Donatella Casaburo e Lorenzo Gugliotta, "The EU AI Act Proposal(s): Manipulative and Exploitative AI Practices," *KU Leuven CiTiP Blog*, 22 settembre 2023, https://www.law.kuleuven.be/citip/blog/the-eu-ai-act-proposals-manipulative-and-exploitative-ai-practices/.

[441] Matija Franklin, Philip Moreira Tomei e Rebecca Gorman, "Vague Concepts in the EU AI Act Will Not Protect Citizens from AI Manipulation," *OECD.AI Policy Observatory*, 7 settembre 2023, https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions. Il Considerando 29, sebbene non abbia valore prescrittivo, sembra prendere in considerazione questa possibilità nel considerare subliminali le tecniche sia quando chi utilizza il sistema non ne è consapevole, sia quando, seppur consapevole, "non è in grado di controllarle o resistervi o possa evitare l'inganno".

norma, risultando particolarmente arduo accertare le reali intenzioni di sviluppatori e *deployer* di sistemi di IA.[442]

Alcuni commentatori, poi, hanno ritenuto insufficiente il riferimento alla distorsione materiale del comportamento di una persona o di un gruppo di persone, suggerendo di estendere il divieto anche a quelle tecniche di IA in grado di distorcere o modificare le preferenze personali. È indubbio che gran parte dei sistemi di IA, in particolare gli algoritmi di raccomandazione che operano sui *social network* e nei mercati digitali, influenzino i contenuti proposti e, di riflesso, il comportamento degli utenti.[443] Ad avviso di chi scrive, il pregio della scelta operata dall'AI Act risiede tuttavia proprio nell'aver tentato di ancorare il divieto a un elemento oggettivo, rispetto alla più complessa prova dell'influenza che può avere un sistema di IA sulle preferenze individuali e sui processi psichici interni di una persona.

Perché operi il divieto è infine necessario, si è detto, che la distorsione del comportamento provochi o possa provocare un danno significativo. Il Considerando 29 chiarisce che "non è necessario che il fornitore o il *deployer* abbiano l'intento di provocare un danno significativo, purché ... derivi da pratiche manipolative o di sfruttamento consentite dall'IA".[444] Resta, tuttavia, l'ambiguità della nozione di "danno significativo", mancando criteri interpretativi sufficientemente chiari per valutare la gravità del danno cagionato o potenzialmente cagionabile dal sistema.[445]

La lett. b) dell'art. 5 dell'AI Act sancisce l'ulteriore divieto di immettere sul mercato, mettere in servizio o utilizzare sistemi di IA che sfruttino le vulnerabilità legate all'età, alla disabilità o a una particolare situazione sociale o economica di una persona fisica o di uno specifico gruppo di persone.[446] Tale ipotesi appare parzialmente sovrapponibile alla prima, richiedendosi anche in questo caso l'obiettivo o l'effetto di distorcere materialmente il comportamento in modo tale da provocare, o poter ragionevolmente provocare, un danno significativo. La differenza tra le due ipotesi risiede nel fatto che, in presenza di un sistema in grado di sfruttare le vulnerabilità di un soggetto,

---

[442] Nikolinakos, *EU Policy and Legal Framework for Artificial Intelligence*, 376.
[443] Franklin, Moreira Tomei e Gorman, "Vague Concepts in the EU AI Act."
[444] Regolamento (UE) 2024/1689, considerando 29.
[445] Casaburo e Gugliotta, "The EU AI Act Proposal(s)."
[446] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. b).

non è necessario che la tecnica impiegata sia qualificabile come subliminale, manipolativa o ingannevole.[447]

Rientrano nelle pratiche vietate anche i sistemi di IA c.d. di *social scoring*, per tali intendendosi quei sistemi che consentono la valutazione o la classificazione delle persone fisiche o di un gruppo di persone sulla base del loro comportamento sociale, delle caratteristiche personali o della loro personalità, sia che tali caratteristiche siano note, sia che vengano inferite o previste dal sistema stesso.[448] La preoccupazione del legislatore europeo verso tali sistemi, secondo alcuni commentatori, sarebbe stata alimentata dalla diffusione che questi stanno conoscendo in contesti extra-europei, in particolare in Cina.[449] A ciò si aggiunga l'allarme destato dalla vastità delle tecniche utilizzabili, al giorno d'oggi, per la raccolta e l'elaborazione di dati personali: l'impiego di dati generati dai dispositivi IoT per la valutazione e classificazione di individui solleva inquietanti scenari di controllo tecnologico.[450]

Perché il sistema sia considerato vietato secondo il Regolamento, è necessario dunque che produca un "punteggio sociale". La disposizione tace sulla forma tecnica che tale punteggio dovrebbe avere: l'elemento determinante è che consenta la classificazione o la valutazione delle persone, cui dovrà collegarsi una differenziazione nel loro trattamento.[451] Il divieto, infatti, è operativo solo al verificarsi di una o di entrambe le conseguenze di cui alla lett. c) dell'art. 5: (i) un trattamento pregiudizievole o sfavorevole in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; (ii) un trattamento pregiudizievole, ingiustificato o sproporzionato rispetto al comportamento sociale tenuto dalle persone e alla sua gravità.[452]

La formulazione letterale di tale disposizione non è delle più felici e le criticità interpretative che potrebbero emergere in futuro sono molteplici. Appare difficile stabilire quando il "contesto sociale" in cui i dati sono raccolti possa dirsi "non collegato" a quello

---

[447] Casaburo e Gugliotta, "The EU AI Act Proposal(s)."
[448] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. c).
[449] Neuwirth, "Prohibited Artificial Intelligence Practices".
[450] Uroš Ćemalović, "Prohibited Artificial Intelligence Practices According to Article 5 of the European Union's Regulation on AI - Between the 'Too Late' and the 'Not Enough,'" *International Journal of Law and Information Technology* 32, n. 1 (dicembre 2024):6, doi:10.1093/ijlit/eaae023.
[451] Ćemalović, "Prohibited Artificial Intelligence Practices," 6-7.
[452] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. c).

in cui la valutazione/classificazione è impiegata, così come i criteri di "proporzionalità" del trattamento e "gravità" del comportamento sociali appaiono vaghi e potenzialmente soggetti a interpretazioni discordanti.[453]

La lett. d) dell'art. 5 statuisce il divieto di immissione sul mercato, messa in servizio o utilizzo di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche, al fine di valutare o prevedere il rischio che una persona commetta un reato.[454] L'ipotesi delineata alla lettera d) presenta alcune analogie con il *social scoring*. Entrambe le categorie di sistemi vietati compiono una categorizzazione degli individui: mentre il *social scoring* elabora un "punteggio sociale", i sistemi di valutazione del rischio producono una stima della probabilità che una persona compia condotte criminose. L'elemento comune risiede nella segmentazione della popolazione in almeno due categorie, di cui una è qui definita come "a rischio".[455] Come emerso durante la fase di consultazione per la Proposta della Commissione, tali sistemi rischiano anzitutto di violare il principio di presunzione di innocenza, richiamato proprio dal Considerando 42.[456] Non solo: come tutti i sistemi di IA, anche questi strumenti non sono immuni al rischio di *bias* nel *data set* o nell'algoritmo.

Il divieto, in ogni caso, trova applicazione soltanto per quei sistemi che fondano la loro valutazione unicamente sulla profilazione della persona o sulla valutazione dei tratti e delle caratteristiche della personalità.[457] I dati in ingresso sarebbero dunque rappresentati, per lo più, da modelli comportamentali e profili psicologici individuali. Dal momento che si tratta di informazioni sensibili che riguardano la sfera privata dell'individuo, la disposizione in esame andrà interpretata compatibilmente con quanto già previsto dal GDPR.[458] Non si tratta però di un divieto assoluto, ed è anzi contemplata un'eccezione di rilevante portata: la norma non si applica ai sistemi di IA utilizzati "a sostegno della valutazione umana", qualora l'oggetto della valutazione sia il

[453] Ćemalović, "Prohibited Artificial Intelligence Practices," 7.
[454] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. d).
[455] Ćemalović, "Prohibited Artificial Intelligence Practices," 7-8.
[456] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 68.
[457] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. d).
[458] Ćemalović, "Prohibited Artificial Intelligence Practices," 8-9.

coinvolgimento di una persona in un'attività criminosa, e a patto che ci si basi su fatti oggettivi già conosciuti e verificabili.[459]

Il timore che l'IA possa accrescere il senso di sorveglianza di massa e ledere i diritti fondamentali dei cittadini europei – segnatamente il diritto alla vita privata –[460] ha portato a includere, nell'elenco fornito dall'art. 5, il divieto di sistemi di IA deputati alla creazione o all'ampliamento di banche dati di riconoscimento facciale, qualora tale processo si realizzi mediante "*scraping*"[461] non mirato di immagini facciali reperite in Rete o captate da filmati di telecamere a circuito chiuso ("*CCTV footage*").[462] Internet e le telecamere a circuito chiuso rappresentano indubbiamente le fonti di approvvigionamento dati più comunemente impiegate per alimentare le banche dati di riconoscimento facciale; restano, tuttavia, numerose e ulteriori modalità di "alimentazione" non espressamente menzionate dalla disposizione. La scelta di non includerle nel divieto rischia di minare, in futuro, l'effettività della norma.[463]

Alla lettera f) dell'art. 5 vi è poi il divieto di immettere sul mercato, mettere in servizio o utilizzare di sistemi di IA per inferire le emozioni di una persona fisica sul luogo di lavoro e negli istituti di istruzione.[464] Manca, nel testo del Regolamento, una definizione normativa di "emozioni". Il Considerando 18 chiarisce che la nozione fa riferimento a "emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento", ma sarebbero da escludersi "stati fisici, quali dolore o affaticamento", così come la "semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti", a meno che non siano a loro volta impiegati per inferire emozioni.[465] Il divieto, si è visto, è limitato

---

[459] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. d).
[460] Regolamento (UE) 2024/1689, considerando 43.
[461] Il *web scraping* è una tecnica che utilizza software (*crawler* o *bot*) per estrarre automaticamente dati specifici da pagine web, trasformandoli in dati strutturati (*database*, tabelle) per l'analisi. A differenza dei *crawler* dei motori di ricerca come Google, che raccolgono informazioni per indicizzare in modo automatico pagine di un sito, il *web scraping* consente l'estrazione di informazioni di ogni tipo dalle pagine web stesse, come dati personali, dati di contatto, *email*, numeri di telefono, URL. Andrea Fumagalli, "Web Scraping: Cos'è, perché si usa e come difendersi da 'intrusioni' indesiderate," *Agenda Digitale*, 23 aprile 2021, https://www.agendadigitale.eu/sicurezza/web-scraping-cose-perche-si-usa-e-come-difendersi-da-intrusioni-indesiderate/.
[462] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. e).
[463] Ćemalović, "Prohibited Artificial Intelligence Practices," 9-10.
[464] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. f).
[465] Regolamento (UE) 2024/1689, considerando 18.

all'ambito del luogo di lavoro e degli istituti di istruzione; i sistemi di IA destinati a esser utilizzati per il riconoscimento delle emozioni in settori diversi da quelli contemplati dalla norma, pertanto, saranno soggetti agli obblighi previsti per i sistemi ad alto rischio.[466] Se da un lato sembra potersi dire che il legislatore europeo abbia inteso tutelare i soggetti vulnerabili in contesti caratterizzati da una rilevante asimmetria di potere (datore di lavoro/dipendente; docente/discente),[467] dall'altro, restano esclusi dall'ambito applicativo del divieto numerosi altri contesti pubblici (spazi urbani non privati, trasporti, uffici amministrativi e giudiziari).[468] Anche per questo divieto, infine, è prevista una significativa eccezione, laddove il sistema di inferenza delle emozioni sia destinato a essere messo in funzione (o immesso sul mercato) per motivi medici o di sicurezza.[469]

La lett. g) dell'art. 5 proibisce l'immissione sul mercato, la messa in servizio e l'uso dei "sistemi di categorizzazione biometrica" che classificano le persone fisiche sulla base dei loro dati biometrici, qualora tali dati siano impiegati per trarre deduzioni o inferenze su determinate caratteristiche personali: la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale della persona.[470] Per "dati biometrici", ai fini dell'AI Act, devono intendersi quei dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica.[471] Non sono invece qualificabili come "sistemi di categorizzazione biometrica" quei sistemi di IA accessori ad altri servizi commerciali, il cui impiego è strettamente necessario per ragioni tecniche oggettive: si pensi ai filtri utilizzati sui mercati digitali o sui *social network*, che classificano caratteristiche personali dell'utente per visualizzare in anteprima la vestibilità di prodotti da acquistare.[472] Il divieto non si applica alle operazioni di "etichettatura o filtraggio" di *dataset* biometrici acquisiti legalmente nel settore delle attività di contrasto. Per beneficiare della deroga, i *dataset*

---

[466] Regolamento (UE) 2024/1689, Allegato III, punto 1, lett. c).
[467] Regolamento (UE) 2024/1689, considerando 44.
[468] Ćemalović, "Prohibited Artificial Intelligence Practices," 10-11.
[469] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. f).
[470] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. g). Il Considerando 16 cita anche altre caratteristiche personali come i tatuaggi, l'appartenenza a una minoranza, la lingua parlata. A ogni modo, tali caratteristiche non figurano nell'elenco dell'art. 5, che è da ritenersi tassativo.
[471] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 34. In linea con quanto indicato al Considerando 14, la nozione è da considerarsi analoga a quella fornita *ex* GDPR.
[472] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 67. Così si deduce dal Regolamento (UE) 2024/1689, art. 3, par. 1, n. 40.

devono quindi soddisfare due condizioni cumulative: in primo luogo, devono essere stati acquisiti legalmente; in secondo luogo, devono essere impiegati esclusivamente "nel settore delle attività di contrasto", e cioè per quelle attività svolte dalle autorità di contrasto ai fini di prevenzione, indagine, accertamento, perseguimento di reati o esecuzione di sanzioni penali.[473] Sono invece da considerarsi ad alto rischio – e non soggetti a divieto – i sistemi che compiono categorizzazione biometrica "in base ad attributi o caratteristiche sensibili protette basati sulla deduzione di tali attributi o caratteristiche".[474]

La pratica vietata di cui all'art. 5, lett. h) ha rappresentato, nel corso dell'*iter* di approvazione del Regolamento, il punto su cui si sono registrate le più importanti differenze di vedute tra Consiglio e Parlamento europeo.[475] Il divieto riguarda l'uso di sistemi di identificazione biometrica remota "in tempo reale", in spazi accessibili al pubblico e ai fini di attività di contrasto.[476] La *ratio* dietro tale divieto sarebbe da ricercarsi nel carattere particolarmente invasivo di tali sistemi, potenzialmente lesivo del diritto al rispetto della vita privata. L'identificazione in tempo reale, poi, genera nel cittadino un senso di costante sorveglianza, scoraggiando indirettamente l'esercizio della libertà di riunione e di altri diritti fondamentali.[477] Sebbene il Parlamento avesse proposto il divieto totale di tali sistemi, la formulazione adottata nel testo finale è più affine alla posizione del Consiglio, dal momento che è lasciato agli Stati membri un ampio margine di discrezionalità nell'attuazione della norma.[478]

In ogni caso, qualora ciò sia strettamente necessario, l'identificazione biometrica in tempo reale negli spazi accessibili al pubblico è consentita per il perseguimento di alcuni obiettivi, tassativamente individuati dalla norma: (i) ricerca mirata di vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale, nonché la ricerca di persone scomparse; (ii) prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità delle persone fisiche, o di un attacco terroristico; (iii) localizzazione o identificazione di persona sospetta di aver commesso un reato per il quale è possibile

---

[473] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 46.
[474] Regolamento (UE) 2024/1689, Allegato III, punto 1, lett. b).
[475] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 65.
[476] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. h).
[477] Regolamento (UE) 2024/1689, considerando 32.
[478] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 65-66.

disporre mandato d'arresto europeo, ai soli fini di indagine, esercizio dell'azione penale o esecuzione di una sanzione penale.[479]

In tutte le ipotesi sopracitate, l'impego di tali sistemi è comunque subordinato al rigoroso rispetto di alcune tutele procedurali. Elemento centrale della procedura delineata al par. 2 dell'art. 5 è la necessità, per le autorità di contrasto, di ottenere un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente designata dallo Stato membro in cui s'intende usare il sistema.[480] Tale autorizzazione, da richiedersi con istanza motivata e nel rispetto delle normative nazionali di attuazione, può essere concessa solo previo accertamento della sussistenza dei requisiti di necessità e proporzionalità rispetto agli obiettivi di cui al paragrafo 1, primo comma, lettera h), e dovrà attestare che l'utilizzo del sistema di identificazione sia limitato, dal punto di vista temporale e geografico, a quanto strettamente necessario.[481] È prevista una deroga in caso di urgenza debitamente giustificata, sebbene anche in tali circostanze eccezionali l'autorizzazione successiva dovrà essere richiesta senza ritardo, e comunque entro 24 ore dal primo utilizzo.[482] In ogni caso, è ribadito il divieto di adottare decisioni che producano effetti giuridici negativi su una persona, quando fondate unicamente sul risultato generato dai sistemi di identificazione biometrica. Viene così salvaguardato il ruolo centrale della valutazione umana nel processo decisionale.[483]

È infine previsto, per ogni uso del sistema, un duplice obbligo di notifica: alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati.[484]

Come si è detto, la disciplina della fase procedurale per il rilascio dell'autorizzazione preventiva è rimessa in larga misura agli Stati membri, che godono di un apprezzabile margine di discrezionalità nello stabilire le regole di richiesta, rilascio ed esercizio delle autorizzazioni.[485] Si è poi previsto, in aggiunta, che ogni Stato membro possa decidere in primo luogo se autorizzare o meno l'impiego di tali sistemi – in tutte o

---

[479] Regolamento (UE) 2024/1689, art. 5, par. 1, lett. h).
[480] Regolamento (UE) 2024/1689, art. 5, par. 3.
[481] Regolamento (UE) 2024/1689, art. 5, par. 3, secondo comma.
[482] Regolamento (UE) 2024/1689, art. 5, par. 3.
[483] Regolamento (UE) 2024/1689, art. 5, par. 3, secondo comma.
[484] Regolamento (UE) 2024/1689, art. 5, par. 4.
[485] Regolamento (UE) 2024/1689, art. 5, par. 5.

solo in alcune delle ipotesi tipizzate dall'art. 5 dell'AI Act – nonché introdurre, nel rispetto del diritto dell'UE, disposizioni più restrittive anche per i sistemi di identificazione biometrica remota *non* in tempo reale (classificati come ad alto rischio).[486]

3.2. I sistemi di IA ad alto rischio

L'articolo 6 dell'AI Act definisce le regole di classificazione dei sistemi di intelligenza artificiale "ad alto rischio". L'identificazione di detti sistemi rappresenta un passaggio di fondamentale importanza, dal momento che, come si è avuto modo di illustrare,[487] è proprio per i sistemi ad alto rischio che trova applicazione la maggior parte degli obblighi prescritti dal Regolamento. È possibile distinguere, a tal proposito, due categorie.

La prima categoria comprende tutti i sistemi che soddisfano entrambe le condizioni di cui al par. 1 dell'art. 6, e cioè: (i) la destinazione d'uso quale componente di sicurezza di un prodotto, o quale prodotto autonomo, disciplinato dalla normativa di armonizzazione dell'UE di cui all'Allegato I dell'AI Act; (ii) la previsione, nella medesima normativa di armonizzazione, dell'obbligo di una valutazione di conformità da parte di terzi per il prodotto che incorpora il sistema di IA quale componente di sicurezza, ovvero per il sistema di IA stesso in quanto prodotto autonomo, anteriormente all'immissione sul mercato o alla messa in servizio all'interno dell'UE.[488] Quanto all'Allegato I, è incluso al suo interno un elenco di oltre trenta direttive e regolamenti settoriali dedicati alla disciplina di diverse categorie merceologiche, quali giocattoli, veicoli, aeromobili civili, ascensori, apparecchiature radio e dispositivi medici.[489]

In aggiunta a quanto previsto dal par. 1 dell'art. 6, la seconda categoria di sistemi ad alto rischio ricomprende tutti i sistemi individuati dall'Allegato III.[490] Allo stato attuale, l'Allegato elenca otto settori di utilizzo, all'interno dei quali sono specificamente individuati i sistemi di IA ad alto rischio. A titolo di mero esempio, tra i settori è possibile

---

[486] Regolamento (UE) 2024/1689, Allegato III, punto 1, lett. a).
[487] *Vedi* paragrafo 2.
[488] Regolamento (UE) 2024/1689, art. 6, par. 1.
[489] Martin Braun, Anne Vallery e Itsiq Benizri, "What Are High-Risk Artificial Intelligence Systems Within the Meaning of the European Union's Artificial Intelligence Act and What Requirements Apply to Them?," *The Global Regulatory Developments Journal* 1, n. 6 (novembre 2024): 430.
[490] Regolamento (UE) 2024/1689, art. 6, par. 2.

menzionare la biometria, le infrastrutture critiche, l'istruzione e la formazione professionale, l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo.[491] In linea con l'esigenza di garantire uno strumento regolatorio flessibile e *future-proof*, è da accogliersi con favore la previsione espressa del potere della Commissione di modificare e integrare il predetto Allegato III, adeguandolo all'evoluzione tecnologica e ai rischi di volta in volta posti dai nuovi sistemi. L'esercizio di tale potere di modifica è subordinato al verificarsi di due condizioni: in primo luogo, il sistema di IA deve essere destinato a operare in uno dei settori previsti dall'Allegato III; in secondo luogo, il sistema deve presentare un rischio di danno per la salute o la sicurezza delle persone, ovvero di impatto negativo sui diritti fondamentali, equivalente o superiore a quello presentato dai sistemi già inclusi in elenco.[492] Specularmente, alla Commissione è riconosciuto il potere di rimuovere sistemi di IA dall'Allegato, qualora questi non pongano più rischi significativi e la soppressione della voce in elenco non riduca il livello generale di protezione della salute, della sicurezza e dei diritti fondamentali.[493]

La regola generale, dunque, è che l'inclusione di un sistema nell'Allegato III ne comporti la classificazione *ipso facto* come ad alto rischio. È tuttavia contemplata una deroga: i sistemi possono non essere considerati ad alto rischio qualora non presentino, in concreto, un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali degli individui, incluso il rischio di influenzare materialmente l'esito dei processi decisionali.[494] La deroga non trova però applicazione qualora il sistema di IA

---

[491] Regolamento (UE) 2024/1689, Allegato III. Le altre categorie sono: "accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi"; "attività di contrasto, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso"; "migrazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso"; "amministrazione della giustizia e processi democratici".

[492] Regolamento (UE) 2024/1689, art. 7, par. 1. La verifica della sussistenza di quest'ultimo requisito richiede una valutazione complessa e multifattoriale, che deve tenere conto di una serie di criteri indicati al paragrafo immediatamente successivo.

[493] Regolamento (UE) 2024/1689, art. 7, par. 3.

[494] Regolamento (UE) 2024/1689, art. 6, par. 3. In particolare, il sistema non sarà classificato ad alto rischio qualora sia destinato a una delle seguenti pratiche: (i) eseguire un compito procedurale limitato; (i) migliorare il risultato di un'attività umana precedentemente completata; (iii) rilevare schemi decisionali o deviazioni da schemi decisionali precedenti, senza sostituire o influenzare la valutazione umana precedentemente svolta in assenza di un'adeguata revisione; (iv) svolgere un compito preparatorio per una valutazione rilevante ai fini dei casi d'uso elencati come ad alto rischio. Anche in questo caso alla Commissione è riconosciuto il potere di modificare le ipotesi nelle quali è possibile escludere che il sistema sia qualificato come ad alto rischio, sebbene presente nell'elenco dell'Allegato III.

realizzi un'attività di profilazione di persone fisiche.[495] Sul punto, è interessante rilevare come la "profilazione" nell'AI Act sia definita mediante rinvio all'art. 4, punto 4, del GDPR;[496] la portata particolarmente ampia della nozione di "profilazione" *ex* GDPR, di fatto, limita significativamente la possibilità di invocare l'esenzione, ogniqualvolta siano impiegate forme di trattamento automatizzato di dati personali per valutare aspetti relativi a una persona fisica.

La distinzione tra le due categorie di sistemi ad alto rischio rileva soprattutto con riferimento alla data dalla quale inizieranno ad applicarsi gli obblighi previsti dal Regolamento: 2 agosto 2026 quelli indicati nell'Allegato III, un anno dopo (2 agosto 2027) per tutti gli altri.[497]

Qualora un fornitore dovesse ritenere che un sistema di IA di cui all'Allegato III non sia ad alto rischio, dovrà documentarne la valutazione prima che sia immesso sul mercato o messo in servizio. In ogni caso, questi è comunque tenuto, *ex* art. 49, a rispettare l'obbligo di registrazione nella banca dati dell'UE per i sistemi di IA ad alto rischio. Così come, su richiesta delle autorità nazionali competenti, sarà tenuto a mettere a disposizione la documentazione relativa alla valutazione.[498]

3.2.1. I requisiti dei sistemi di IA ad alto rischio

La Sezione 2 del Capo III dell'AI Act individua i requisiti che i sistemi di IA ad alto rischio devono rispettare per essere immessi nel mercato interno. Si è accennato, nel corso del precedente capitolo, a come sembri configurarsi un modello di "*regulation by design*", argomento che sembra trovare conferma all'articolo 8, laddove è imposto ai sistemi di IA il rispetto dei requisiti di cui alla Sezione 2 "tenendo conto delle loro previste finalità nonché dello stato dell'arte generalmente riconosciuto in materia di IA e di tecnologie

---

[495] Regolamento (UE) 2024/1689, art. 6, par. 3, ultimo comma.

[496] Regolamento (UE) 2016/679, art. 4, par. 1, n. 4: «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

[497] Regolamento (UE) 2024/1689, art. 113.

[498] Regolamento (UE) 2024/1689, art. 6, par. 4.

correlate".[499] Novità centrale, in tale contesto, è la previsione dell'obbligo per i fornitori di istituire, attuare, documentare e mantenere un sistema di gestione dei rischi ("*Risk Management System*", RMS).[500] Il Regolamento non fornisce una definizione espressa di cosa sia un sistema di gestione dei rischi, ma individua, all'art.9, gli *step* in cui questo dovrà articolarsi. Alla luce di quanto disposto, la letteratura specialistica ritiene che facciano parte del sistema sia il "processo" di gestione del rischio",[501] sia le "procedure di prova".[502] In linea con quanto previsto per il sistema di gestione della qualità di cui all'articolo 17, paragrafo 1,[503] è quindi possibile intendere il RMS come un sistema strutturato di politiche, procedure e istruzioni.[504]

Quanto al processo, questo si configura come iterativo e continuo, pianificato ed eseguito durante l'intero ciclo di vita del sistema e sottoposto a costante aggiornamento e revisione.[505] Tra gli obiettivi perseguiti vi sono: l'identificazione dei rischi noti e ragionevolmente prevedibili che il sistema, quando utilizzato conformemente alla sua finalità, può porre alla salute, alla sicurezza o ai diritti fondamentali; l'adozione di misure opportune ad attenuarli o eliminarli; la stima e la valutazione dei rischi che possono emergere dal sistema, sia in ipotesi di uso conforme alla finalità, sia in condizioni d'uso improprio ragionevolmente prevedibili; la valutazione degli ulteriori rischi emersi durante la fase di monitoraggio successiva all'immissione sul mercato.[506]

---

[499] Regolamento (UE) 2024/1689, art. 8. Come si è detto, tali conclusioni sembrano essere condivise da Prifti et al., "Regulation by Design," 2. Sulla stessa linea, sebbene il lavoro sia dedicato all'analisi della Proposta di Regolamento della Commissione e non alla sua versione definitiva, si rimanda al già citato Almada, "Regulation by Design".

[500] Regolamento (UE) 2024/1689, art. 9. A dire il vero, l'art. 9 non indica chi sia il destinatario dell'obbligo, ma è possibile ricavarlo dall'art. 18. Non è chiaro cosa si intenda esattamente per "istituire", "attuare", "documentare" e "mantere" un sistema di gestione dei rischi. Jonas Schuett propone alcune definizioni. Un sistema di gestione del rischio sarebbe: "istituito", quando sono creati e approvati i documenti obbligatori previsti dal Regolamento da parte dei decisori competenti; "implementato", quando applicato e compreso dai soggetti coinvolti; "documentato", se esiste una documentazione scritta e organizzata di istruzioni e procedure, da esporre su rischista alle autorità competenti; "mantennuto", se è periodicamente rivisto e aggiornato. Jonas Schuett, "Risk Management in the Artificial Intelligence Act," *European Journal of Risk Regulation* 15 n. 2 (agosto 2024): 374, doi:10.1017/err.2023.1.

[501] Regolamento (UE) 2024/1689, art. 9, paragrafi da 2 a 5.

[502] Regolamento (UE) 2024/1689, art. 9, paragrafi da 6 a 8.

[503] Regolamento (UE) 2024/1689, art. 17, par. 1.

[504] Schuett, "Risk Management in the Artificial Intelligence Act," 374.

[505] Regolamento (UE) 2024/1689, art. 9, par. 2.

[506] Braun, Vallery e Benizri, "What Are High-Risk Artificial Intelligence Systems?," 429. Regolamento (UE) 2024/1689, art. 9, par. 2, lettere a), b), c) e d).

Quanto alle procedure di prova, la loro finalità è, da un lato, quella di individuare le misure di gestione del rischio più appropriate, dall'altro, quella di garantire che il sistema agisca conformemente alla sua finalità e rispetti tutti i requisiti di cui alla Sezione 2 del Regolamento.[507] Diversamente dal processo di gestione dei rischi, la cui durata deve estendersi all'intero ciclo di vita del sistema, è interessante notare come le prove siano previste soltanto con riguardo alla fase di sviluppo. Queste potranno avvenire "in qualsiasi momento", ma dovranno essere in ogni caso anteriori all'immissione sul mercato o alla messa in servizio.[508] L'intento del legislatore europeo di realizzare un modello di regolazione *by design* sembra emergere con ancora più chiarezza, poi, dalla previsione che le prove siano condotte "sulla base di metriche e soglie probabilistiche" precedentemente definite.[509] La fissazione di metriche appropriate, in ogni caso, dipende dalla tipologia di sistema e dal contesto di utilizzo, e non può che segnalarsi, allo stato attuale, l'assenza di *best practices* consolidate.[510]

Nell'impossibilità di rintracciare una definizione di rischio nel testo del Regolamento, appare opportuno anche in questo caso fare riferimento alla nozione impiegata nel *New Legislative Framework*.[511] In ogni caso, i rischi individuati e affrontanti dal sistema di gestione non dovranno essere tutti i rischi astrattamente posti da un sistema di IA, bensì soltanto quelli che i fornitori possono ragionevolmente attenuare o eliminare in fase di sviluppo o progettazione, o fornendo informazioni tecniche adeguate.[512] La disciplina del RMS evidenzia come l'approccio basato sul rischio – lungi dal limitarsi alla "piramide del rischio" sottesa alla classificazione dei sistemi di IA – pervada trasversalmente l'intera architettura regolatoria del Regolamento. Riflessi del modello regolatorio *risk-based* sono infatti rintracciabili in più di una

[507] Regolamento (UE) 2024/1689, art. 9, par. 5.
[508] Regolamento (UE) 2024/1689, art. 9, par. 8.
[509] Regolamento (UE) 2024/1689, art. 9, par. 8. Si è detto di come l'implementazione di una metrica con la quale misurare il successo dell'intervento regolatorio rappresenti uno dei presupposti essenziali per un'efficiente *regulation by design*. *Vedi* capitolo II, paragrafo 1.2.
[510] Schuett, "Risk Management in the Artificial Intelligence Act," 379.
[511] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 73.
[512] Regolamento (UE) 2024/1689, art. 9, par. 3.

disposizione del testo, tra cui, a titolo di mero esempio, la procedura per la gestione di sistemi di IA che presentano un rischio a livello nazionale *ex* articolo 79.[513]

L'AI Act riconosce poi il ruolo essenziale svolto dai dati nel garantire il funzionamento sicuro dei sistemi di IA e la prevenzione di discriminazioni vietate dal diritto dell'Unione.[514] L'articolo 10 sancisce gli obblighi da rispettare in materia di qualità dei dati e *data governance* per i sistemi di IA ad alto rischio, sia che si tratti di *set* di dati di addestramento, sia che si tratti di *set* di dati di convalida e prova.[515] Con riferimento alle pratiche di *governance* e gestione ivi prescritte, queste dovranno essere "adeguate alla finalità del sistema" e riguardare, tra le altre cose: scelte di progettazione pertinenti, processi di raccolta dei dati appropriati, operazioni di trattamento pertinenti ai fini della preparazione dei dati (*e.g.* annotazione, etichettatura, pulizia, aggiornamento, arricchimento, aggregazione), esami per la valutazione delle possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate, nonché misure adeguate per individuare, prevenire e attenuare tali distorsioni.[516]

I *dataset* di addestramento, convalida e prova devono inoltre possedere specifici requisiti qualitativi: essere "pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista"; ove applicabile, possedere "proprietà statistiche appropriate" riferibili alle persone o ai gruppi di persone rispetto ai quali il sistema è destinato a essere utilizzato; infine, tener conto

---

[513] Longo, "La disciplina del rischio digitale," 74.

[514] Regolamento (UE) 2024/1689, considerando 67: "Dati di alta qualità e l'accesso a dati di alta qualità svolgono un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione … ". Sui rischi di discriminazione legati all'utilizzo di dati di cattiva qualità, *vedi* capitolo I, paragrafo 1.1.

[515] Regolamento (UE) 2024/1689, art. 10, par. 2. Le definizioni di "dati di addestramento", "dati di convalida" e "dati di prova" sono fornite all'art. 3, nn. 29), 30) e 32) del Regolamento: dati di addestramento, e cioè "i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere"; dati di convalida, "utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine tra l'altro di evitare lo scarso (*underfitting*) o l'eccessivo (*overfitting*) adattamento ai dati di addestramento"; dati di prova, "utilizzati per fornire una valutazione indipendente del sistema di IA al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio".

[516] Regolamento (UE) 2024/1689, art. 10, par. 2.

delle caratteristiche proprie dell'ambito "geografico, contestuale, comportamentale o funzionale" in cui il sistema entrerà in funzione.[517] Con riguardo a tali requisiti, si segnala che non sembrano del tutto scongiurate le criticità evidenziate dagli *stakeholder* nel corso dell'*iter* di approvazione del Regolamento: le nozioni di "pertinenza" e "rappresentatività" rischiano di rivelarsi eccessivamente vaghe, soggette a variare in funzione del contesto e del tempo; un *dataset* esente da errori e completo, poi, appare di difficile se non impossibile realizzazione, particolarmente nel caso in cui siano impiegate, ai fini dell'addestramento, enormi quantità di dati.[518] È per altro fatto notorio, per gli operatori del settore, che in determinate circostanze l'addestramento con *dataset* parzialmente erronei o incompleti può risultare addirittura auspicabile, al fine di aumentare la robustezza del sistema e migliorarne le capacità di gestione di *input* imperfetti o lacunosi.[519]

Al par. 5 dell'art. 10 è infine disciplinato il trattamento, da parte dei fornitori, di categorie particolari di dati personali *ex* art. 9 del GDPR. Tali dati possono essere trattati solo nella misura in cui ciò sia "strettamente necessario a garantire il rilevamento e la correzione delle distorsioni" dei sistemi di IA ad alto rischio, a condizione che sia garantito il rispetto di tutte le condizioni elencate dalla disposizione.[520]

È poi previsto che i sistemi, lungo tutto il loro ciclo di vita, siano accompagnati da apposita documentazione tecnica aggiornata, redatta in forma chiara e comprensibile e predisposta anteriormente all'immissione sul mercato o alla messa in servizio.[521] Al fine di dimostrare che il sistema rispetta tutti i requisiti previsti dalla normativa, l'Allegato IV indica il contenuto minimo che tale documentazione dovrà contenere.[522] Sul punto, si

---

[517] Regolamento (UE) 2024/1689, art. 10, par. 3-4.
[518] Nikolinakos, *EU Policy and Legal Framework for Artificial Intelligence*, 460.
[519] Nikolinakos, 460.
[520] Regolamento (UE) 2024/1689, art. 10, par. 5.
[521] Regolamento (UE) 2024/1689, art. 11, par. 1.
[522] Regolamento (UE) 2024/1689, Allegato IV. La documentazione dovrà includere, tra le altre cose: una descrizione dettagliata del sistema di IA, dei suoi componenti e del processo di sviluppo; le informazioni relative al monitoraggio, al funzionamento e al controllo del sistema; una descrizione dell'adeguatezza delle metriche di prestazione; una descrizione dettagliata del sistema di gestione dei rischi *ex* art. 9; l'elenco delle modifiche pertinenti apportate dal fornitore durante il ciclo di vita del sistema; un elenco delle norme armonizzate applicate; una copia della dichiarazione di conformità; e, infine, una descrizione dettagliata del sistema di valutazione delle prestazioni del sistema dopo l'immissione sul mercato.

segnala che è stato previsto, anche in questo caso, uno strumento di flessibilità atto a garantire l'adeguamento della normativa allo sviluppo tecnologico: la Commissione potrà pertanto modificare il testo dell'Allegato, prevedendo l'inclusione di ulteriori informazioni necessarie.[523]

Allo scopo di assicurare la tracciabilità, poi, i sistemi di IA ad alto rischio dovranno garantire, a livello tecnico, la registrazione automatica degli eventi ("*log*") lungo l'intero ciclo di vita.[524] Diverse le ragioni sottese all'obbligo di registrazione: individuare i soggetti responsabili in caso di danni, facilitare lo svolgimento di *audit* esterni, consentire al fornitore di provare la conformità del suo sistema ai requisiti prescritti dal Regolamento.[525] Sui fornitori ricade poi l'obbligo di conservazione dei *log* per un periodo adeguato alla finalità perseguita dalla macchina e, in ogni caso, non inferiore a sei mesi.[526]

Nel corso del primo capitolo di questa trattazione si è discusso di come una delle principali criticità dell'intelligenza artificiale sia l'opacità intrinseca degli algoritmi di apprendimento automatico (c.d. *black box effect*). Tale criticità risulta aggravata, si è detto, dalla presenza di segreti industriali che impediscono l'accesso alle informazioni relative ai metodi impiegati nello sviluppo dei sistemi, dalla frammentazione di competenze e conoscenze dovuta al coinvolgimento di più attori nella catena di approvvigionamento, nonché dalla natura *hi-tech* e dalla complessità della tecnologia in esame.[527] Nel tentativo di ovviare a questo problema, l'articolo 13 prevede che i sistemi di IA ad alto rischio siano progettati e sviluppati in modo tale che il loro funzionamento sia sufficientemente trasparente, consentendo ai *deployer* – i soggetti che utilizzano il sistema sotto la propria autorità – una corretta interpretazione dell'*output* e un utilizzo adeguato del sistema. Perché il livello di trasparenza possa dirsi sufficientemente adeguato, poi, questo dovrà essere tale da consentire a fornitori e *deployer* il rispetto di tutti gli obblighi posti dal Regolamento.[528] A tal fine, i sistemi ad alto rischio dovranno essere accompagnati da delle istruzioni per l'uso, rese disponibili in formato digitale o

---

[523] Regolamento (UE) 2024/1689, art. 11, par. 3.
[524] Regolamento (UE) 2024/1689, art. 12, par. 1-2.
[525] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 78.
[526] Regolamento (UE) 2024/1689, art. 19.
[527] Per una breve panoramica sulle principali sfide regolatorie poste dall'intelligenza artificiale, *vedi* capitolo I, paragrafo 1.1.
[528] Regolamento (UE) 2024/1689, art. 13, par. 1.

analogico, e comprensive di informazioni "concise, complete, corrette e chiare ... pertinenti, accessibili e comprensibili".[529]

Nell'analizzare il testo della Proposta di regolamento, alcuni commentatori avevano sottolineato come il requisito della trasparenza avrebbe potuto condurre a due diverse letture interpretative: seguendo una lettura restrittiva, nel prescrivere l'obbligo di fornire al *deployer* istruzioni concernenti l'interpretazione dell'*output* del sistema, la norma farebbe riferimento a semplici indicazioni quali l'avvertimento circa la presenza di potenziali *bias* del sistema. Un'interpretazione estensiva, viceversa, obbligherebbe i fornitori a esplicitare il *modus operandi* attraverso il quale il sistema perviene ai propri risultati, aprendo uno spiraglio sulla *black box* algoritmica.[530] A ogni modo, la formulazione adottata nella versione definitiva dell'art. 13 sembra concedere ai fornitori un ampio margine di discrezionalità nella scelta dei mezzi tecnici e delle modalità con cui adempiere ai suddetti obblighi. Tale flessibilità rischia, tuttavia, di perpetuare prassi di sub-ottimali, offrendo una visione solo parziale della logica di funzionamento sottesa al sistema di IA.[531]

L'approccio all'intelligenza artificiale seguito dal legislatore europeo è sovente definito "antropocentrico", e trova una sua importante espressione nel requisito della sorveglianza umana. Già l'AI HLEG, nei suoi Orientamenti Etici, aveva ribadito la necessità di garantire il rispetto dell'autonomia e della capacità decisionale degli utenti che interagiscono con sistemi di IA.[532] Riprendendo le parole della Commissione, "l'intelligenza artificiale non è fine a se stessa, ma è uno strumento a servizio delle persone che ha come fine ultimo quello di migliorare il benessere degli esseri umani".[533] In linea con tale visione, l'art. 14 prevede l'obbligo di dotare i sistemi di IA ad alto rischio di interfacce uomo-macchina adeguate, volte a consentire un'effettiva supervisione

---

[529] Regolamento (UE) 2024/1689, art. 13, par. 2. Come prescritto al paragrafo 3, "le istruzioni per l'uso contengono almeno le informazioni seguenti: a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato; b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio ... ".

[530] Madalina Busuioc, Deirdre Curtin e Marco Almada, "Reclaiming Transparency: Contesting the Logics of Secrecy Within the AI Act," *European Law Open* 2 (2023): 92, doi:10.1017/elo.2022.47.

[531] Busuioc, Curtin e Almada, 92.

[532] AI HLEG, *Ethics Guidelines for Trustworthy AI*, 12.

[533] Commissione Europea, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final, 2.

umana durante l'utilizzo.[534] L'obiettivo è sempre quello di prevenire e minimizzare i rischi per la salute, la sicurezza e i diritti fondamentali, sia in condizioni di uso conforme alla finalità prevista, sia in scenari di uso improprio ragionevolmente prevedibili.[535] In ogni caso, le misure di sorveglianza previste dall'articolo 14 dovranno rispettare il principio di proporzionalità, adattandosi ai rischi, al livello di autonomia del sistema e al contesto in cui questo è utilizzato.[536] Laddove tecnicamente fattibile, tali misure dovranno essere individuate anteriormente all'immissione sul mercato del sistema e integrate nel sistema *by design*, sin dalla progettazione. In alternativa, dovranno poter essere implementate dal *deployer*.[537]

Ove opportuno, e nel rispetto del principio di proporzionalità, i soggetti incaricati di svolgere le operazioni di sorveglianza dovranno: essere posti nelle condizioni di comprendere le capacità e i limiti del sistema di IA, nonché di monitorarne il funzionamento al fine di individuare e correggere anomalie, disfunzioni e prestazioni inattese; essere consapevoli del rischio di "*automation bias*", ossia della tendenza umana, nei processi decisionali, a riporre eccessiva fiducia nell'*output* generato dal sistema; interpretare correttamente l'*output*, ed eventualmente ignorarlo, annullarlo o ribaltarlo; intervenire attivamente sul funzionamento del sistema, sino a interromperlo se vi è la necessità.[538]

Per ultimo, i sistemi di IA ad alto rischio devono garantire il mantenimento di un livello adeguato di accuratezza, robustezza e cybersicurezza durante tutto il loro ciclo di vita.[539] La Commissione Europea è incaricata di promuovere lo sviluppo di parametri di riferimento ("*benchmark*") e metodologie di misurazione volti a concretizzare e standardizzare la valutazione di tali requisiti. I livelli di accuratezza – e le "metriche di

---

[534] Regolamento (UE) 2024/1689, art. 14, par. 1.
[535] Regolamento (UE) 2024/1689, art. 14, par. 2.
[536] Regolamento (UE) 2024/1689, art. 14, par. 3. Sempre in ottica di proporzionalità, si noti che l'articolo 14, paragrafo 5 sancisce la necessità di misure di sorveglianza umana rafforzate nel caso di sistemi di identificazione biometrica remota.
[537] Regolamento (UE) 2024/1689, art. 14, par. 3.
[538] Regolamento (UE) 2024/1689, art. 14, par. 4.
[539] Regolamento (UE) 2024/1689, art. 15, par. 1.

accuratezza pertinenti" – devono poi essere inclusi nelle istruzioni per l'uso del sistema.[540]

I sistemi di IA ad alto rischio devono essere resilienti, per quanto possibile, a errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso è destinato ad agire;[541] nonché a tentativi da parte di terzi non autorizzati di modificarne l'uso, gli *output* o le prestazioni.

3.3. Gli obblighi di trasparenza

In linea con quanto emerso nel corso dei lavori svolti dall'AI HLEG,[542] l'AI Act dedica alla trasparenza diverse disposizioni normative. Appare doveroso precisare che, a differenza di quanto si è detto in merito alla celebre "piramide del rischio", il testo normativo non fa alcuna menzione dei c.d. "sistemi a rischio limitato", per tali intendendosi quei sistemi che sarebbero soggetti ai soli obblighi di trasparenza.

Il Regolamento contempla, da un lato, obblighi di trasparenza incombenti solo sui fornitori di sistemi ad alto rischio (art. 13), dall'altro, introduce un diverso e ulteriore *set* di obblighi di trasparenza incombenti sia sui fornitori, sia sui *deployer* di determinati sistemi di IA (art. 50). Si tratta, per lo più, di obblighi posti a tutela del pubblico e delle persone fisiche che interagiscono direttamente con i suddetti sistemi. Ne consegue che un sistema di IA classificato come ad alto rischio ben potrebbe essere soggetto, cumulativamente, sia agli obblighi di trasparenza *ex* art. 13, sia a quelli *ex* art. 50; solo i sistemi non classificabili come ad alto rischio, ma al tempo stesso ricompresi nelle fattispecie elencate all'art. 50, saranno sottoposti esclusivamente agli obblighi di

---

[540] Regolamento (UE) 2024/1689, art. 15, par. 2-3.

[541] Regolamento (UE) 2024/1689, art. 15, par. 4. Nel corso di questa trattazione si è discusso dei rischi posti dagli algoritmi di apprendimento automatico, nonché di come l'addestramento su dati di cattiva qualità comporti un errore sistemico e non occasionale (*vedi* capitolo I, paragrafo 1.1). Non sorprende, dunque, l'attenzione rivolta dal legislatore europeo ai sistemi che continuano ad apprendere dopo l'immissione sul mercato. Tali sistemi devono essere sviluppati in modo da eliminare o ridurre, per quanto possibile, il rischio che *output* potenzialmente distorti ("*biased*") possano influenzare i dati di ingresso per operazioni future, innescando circoli viziosi di auto-amplificazione dei *bias*.

[542] A mero titolo di esempio, l'AI HLEG descrive la trasparenza come "*closely linked with the principle of explicability*". AI HLEG, *Ethics Guidelines for Trustworthy AI*, 18.

trasparenza verso il pubblico.[543] Ciò premesso, si può adesso tentare un'analisi critica degli obblighi d trasparenza sanciti dall'articolo 50.

Qualora un sistema di IA sia destinato a interagire direttamente con le persone fisiche, è anzitutto previsto l'obbligo, a carico dei fornitori, di progettarlo e svilupparlo in modo tale che tali persone siano informate del fatto di stare interagendo con una macchina. È prevista una deroga qualora, tenuto conto del contesto, ciò risulti di per sé evidente dal punto di vista di una persona ragionevolmente informata, attenta e avveduta.[544] I fornitori di sistemi di IA generativa, inclusi i modelli GPAI, hanno poi l'obbligo di garantire che gli *output* del sistema – contenuti audio, immagini, video o testi sintetici – siano marcati in un formato leggibile meccanicamente ("*machine-readable"*) e rilevabili come generati o manipolati artificialmente.[545] Trattasi di *labeling*, o "etichettatura", dei risultati generati dall'intelligenza artificiale, al fine di garantire la consapevolezza dell'utenza rispetto alla natura artificiale di tali contenuti.

Quanto agli obblighi gravanti sui *deployer*: nel caso di sistemi di IA in grado di creare "*deepfake*"[546], questi sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente; lo stesso può dirsi per i *deployer* di sistemi che generano contenuti testuali, qualora i testi siano pubblicati ai fini di informazione su questioni di pubblico interesse, *e.g.* articoli giornalistici scritti tramite l'ausilio di *Large Language Models*.[547]

In ogni caso, nessuno degli obblighi di *labeling* summenzionati trova applicazione nell'ipotesi in cui l'utilizzo dei sistemi di IA e dei relativi *output* sia autorizzato dalla legge per finalità di accertamento, prevenzione, indagine e perseguimento di reati.[548]

Si intende ora mettere in luce alcune criticità in merito all'effettività e alla tenuta futura delle disposizioni esaminate. Le tecniche di *labeling* attualmente più diffuse (*watermarking*, *digital fingerprinting*, metadati crittografati) presentano, infatti,

---

[543] Così emerge dalla lettura dell'art. 50, par. 6 del Regolamento.
[544] Regolamento (UE) 2024/1689, art. 50, par. 1.
[545] Regolamento (UE) 2024/1689, art. 50, par. 2.
[546] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 60: "«deep fake»: un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona".
[547] Regolamento (UE) 2024/1689, art. 50, par. 4.
[548] Regolamento (UE) 2024/1689, art. 50, par. 1, 2 e 4.

importanti limiti.[549] I *watermark*, sia visibili che invisibili, non sono a prova di manomissione, e anzi possono essere rimossi con facilità, specialmente in contesti in cui gli attori cercano attivamente di evitarne il rilevamento.[550] A ciò si aggiunge la mancanza, allo stato attuale, di *standard* tecnici di riferimento: ogni azienda può utilizzare approcci diversi di *watermarking* in base ai propri modelli proprietari, rendendo così complessa la verifica della natura artificiale di contenuti provenienti da diverse piattaforme.[551] È pur vero che, nel caso dei fornitori di IA generativa, l'obbligo di trasparenza impone di adottare "soluzioni tecniche ... efficaci, interoperabili, solide e affidabili nella misura in cui ciò sia tecnicamente possibile ... ".[552] L'effettività di tale obbligo dipenderà dunque, in larga parte, dagli *standard* tecnici fissati a livello europeo e dai Codici di buone pratiche che saranno adottati dalla Commissione.

L'enfasi normativa sull'etichettatura dei contenuti generati da IA non garantisce, in ogni caso, la repressione di fenomeni quali la disinformazione, la violazione del diritto d'autore e la diffusione di *deepfake*, dal momento che a tali fenomeni possono contribuire, del pari, contenuti prodotti da esseri umani.[553]

Distinguere un contenuto umano da un contenuto *AI-generated*, per altro, non è sempre agevole, in particolare in contesti in cui l'intelligenza artificiale svolge un ruolo per così dire "ausiliario", sotto la direzione e la sorveglianza di *creator* umani. Il Regolamento sembra prendere in considerazione tale possibilità e prevede alcune deroghe agli obblighi di trasparenza *ex* art. 50. L'obbligo di *labeling* a carico dei fornitori di sistemi di IA generativa non si applica qualora i sistemi svolgano una funzione meramente assistenziale di "*editing standard*", o comunque non modifichino in modo sostanziale i dati di ingresso (*input*) forniti dal *deployer* – sebbene rimanga poco chiaro quali siano i confini tra una modifica sostanziale e una mera assistenza all'*editing*.[554] Analogamente, per i *deployer* è previsto un alleggerimento dell'obbligo di informazione nel caso in cui il *deepfake* sia impiegato in opere artistiche, creative, satiriche o fittizie, di modo da non

---

[549] Justyna Lisinska e Daniel Castro, "Why AI-Generated Content Labeling Mandates Fall Short," *Center for Data Innovation* (dicembre 2024), https://www2.datainnovation.org/2024-ai-watermarking.pdf.
[550] Lisinska e Castro, 5-6.
[551] Lisinska e Castro, 5-6.
[552] Regolamento (UE) 2024/1689, art. 50, par. 2.
[553] Lisinska e Castro, "Why AI-Generated Content Labeling Mandates Fall Short," 6-7.
[554] Regolamento (UE) 2024/1689, art. 50, par. 2.

comprometterne il godimento.[555] Quanto ai testi destinati a informare il pubblico, l'obbligo renderne nota la natura artificiale è escluso se il contenuto ha subito un processo di revisione umana e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione.[556]

A conclusione di questa breve ricognizione degli obblighi di trasparenza, appare opportuno menzionare come l'articolo in esame imponga anche, ai *deployer* dei sistemi di riconoscimento delle emozioni e di categorizzazione biometrica, l'obbligo di informare le persone fisiche che vi sono esposte in merito al funzionamento del sistema, nonché di trattare i dati personali in conformità con il GDPR.[557]

3.4. I modelli di IA per finalità generali

L'AI Act dedica alcune disposizioni specifiche ai modelli di IA per finalità generali (GPAI). Con il termine, il Regolamento fa riferimento a quei modelli di IA – spesso addestrati con grandi quantità di dati mediante autosupervisone su larga scala – che presentano una "generalità significativa", e sono pertanto in grado di svolgere un'ampia gamma di compiti distinti. Qualità specifica di tali modelli, anzitutto, è quella di poter essere a loro volta integrati da altri fornitori in una varietà di sistemi e applicazioni a valle.[558]

Per i fornitori di modelli GPAI trovano applicazione una serie di obblighi specifici, tra cui la redazione e l'aggiornamento costante della documentazione tecnica, da tenersi a disposizione delle autorità competenti e dell'Ufficio per l'IA.[559] Il contenuto minimo della documentazione è fornito all'Allegato XI dell'AI Act e include, *inter alia*, una descrizione generale del modello e le informazioni sulle modalità di integrazione nei sistemi a valle.[560] La documentazione dovrà quindi essere accessibile anche a quei fornitori che intendano integrare modelli GPAI nei propri sistemi, ferma restando la tutela della proprietà intellettuale, dei segreti commerciali e delle informazioni commerciali

---

[555] Regolamento (UE) 2024/1689, art. 50, par. 4, primo comma.
[556] Regolamento (UE) 2024/1689, art. 50, par. 4, secondo coma.
[557] Regolamento (UE) 2024/1689, art. 50, par. 3.
[558] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 63.
[559] Regolamento (UE) 2024/1689, art. 53, par. 1, lett. a). Sull'Ufficio per l'IA e l'architettura di governance dell'AI Act, *vedi* capitolo IV, paragrafo 1.
[560] Regolamento (UE) 2024/1689, Allegato XI.

riservate secondo il diritto dell'Unione.[561] Il legislatore europeo sembra mostrare un particolare *favor* nei confronti dei modelli GPAI *open source* rilasciati con licenza libera, i cui fornitori sono sollevati dagli obblighi di documentazione tecnica.[562] Tenuto conto delle ingenti quantità di dati impiegate nello sviluppo dei modelli per finalità generali, si è infine previsto l'ulteriore obbligo, per tutti i fornitori, di pubblicare una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento, adottando un modulo che sarà loro fornito dall'Ufficio per l'IA.[563]

Ulteriori e più gravosi obblighi sono invece previsti nel caso in cui un modello di IA per finalità generali sia classificato come a "rischio sistemico". Si tratta di un rischio specifico legato alle "capacità di impatto elevato" di tali modelli, in grado di impattare in modo significativo sul mercato dell'Unione o produrre effetti negativi sui diritti fondamentali o sulla società tutta.[564] Gli effetti prodotti da un modello GPAI, infatti, sono potenzialmente idonei a propagarsi su larga scala e per l'intera catena del valore.[565] La classificazione di un modello GPAI come "a rischio sistemico" è quindi subordinata all'accertamento di una capacità di impatto levato, che può avvenire: (i) sulla base di strumenti tecnici e metodologie appropriate, in base a una valutazione del rischio compiuta dal fornitore;[566] (ii) in virtù di una decisione della Commissione Europea, *ex*

---

[561] Regolamento (UE) 2024/1689, art. 53, par. 1, lett. b).

[562] Regolamento (UE) 2024/1689, art. 53, par. 2. Un esempio è rappresentato da Le Platform, libreria di servizi di IA e LLM open source sviluppata da Mistral AI, startup francese con sede a Parigi, celebre per consentire la modifica financo dei pesi dei suoi modelli. La *ratio* di questa esenzione sembra risiedere nel fatto che, per tali sistemi, i dati rilevanti sono già resi pubblicamente accessibili. *Le Platform* è accessibile a https://mistral.ai/en/products/la-plateforme.

[563] Regolamento (UE) 2024/1689, art. 53, par. 1, lett. d).

[564] Per una tassonomia completa dei rischi sistemici, si rimanda a Risto Uuk et al., "A Taxonomy of Systemic Risks from General-Purpose AI," *SSRN* (novembre 2024), doi:10.2139/ssrn.5030173.

[565] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 65.

[566] Se un modello di IA per finalità generali presenta un rischio sistemico (*soddisfa la condizione di cui all'art. 51, par. 1, lett. a)*), il fornitore informa la Commissione entro due settimane dal momento in cui ne viene a conoscenza. Se la Commissione viene a conoscenza di un modello di IA per finalità generali che presenta rischi sistemici di cui non è stata informata, può in ogni caso decidere in autonomia di designarlo come modello con rischio sistemico.

Il fornitore di un modello di IA per finalità generali con rischio sistemico può presentare, unitamente alla sua notifica, argomentazioni sufficientemente fondate per dimostrare che, in via eccezionale, il modello di IA per finalità generali non presenta, a causa delle sue caratteristiche specifiche in concreto, rischi sistemici e non dovrebbe essere pertanto classificato come tale. Così è previsto dal Regolamento (UE) 2024/1689, art. 52, par. 1-2.

officio o a seguito di segnalazione qualificata del Gruppo di esperti scientifici.[567] È poi prevista una presunzione legale di capacità di impatto elevato qualora "la quantità cumulativa di calcolo" utilizzata per l'addestramento del modello, misurata in operazioni in virgola mobile, sia superiore a 10^25.[568]

Alla Commissione è comunque riconosciuto il potere di adottare atti delegati per modificare i criteri di classificazione di un sistema di IA come a rischio sistemico *ex* art. 51, nonché per integrare parametri di riferimento e gli indicatori di rischio alla luce degli sviluppi tecnologici.[569] Può argomentarsi che tale strumento di flessibilità normativa sia destinato ad assumere una sempre maggiore rilevanza in futuro. Si pensi alla presunzione di capacità di impatto elevato nei casi in cui il calcolo computazionale impiegato per l'addestramento del modello superi la soglia di 10^25 FLOP. Con il progressivo incremento della potenza di calcolo disponibile, è plausibile che tale parametro possa in futuro rivelarsi eccessivamente restrittivo. Contrariamente e al tempo stesso, l'evoluzione delle tecniche di addestramento dei modelli di IA consentono già oggi una riduzione significativa del fabbisogno computazionale necessario a ottenere prestazioni elevate. In particolare, la c.d. *knowledge distillation* consente di sviluppare modelli di dimensioni ridotte, in grado di garantire risultati comparabili a quelli prodotti da modelli più grandi e onerosi, ma con una maggiore efficienza in termini di risorse impiegate.[570]

I fornitori di modelli con rischio sistemico hanno l'obbligo di effettuare una valutazione delle loro tecnologie in conformità con protocolli e strumenti standardizzati e aggiornati allo stato dell'arte, anche mediante *adversarial testing*.[571] Dovranno quindi valutare e attenuare i rischi sistemici potenzialmente derivanti dallo sviluppo, dall'immissione sul mercato o dall'utilizzo dei modelli con rischio sistemico a livello

---

[567] Regolamento (UE) 2024/1689, art. 51, par. 1. In ogni caso il fornitore può chiedere una nuova valutazione alla Commissione, qualora il sistema sia stato designato come con rischio sistemico *ex officio*.
[568] Regolamento (UE) 2024/1689, art. 51, par. 2.
[569] Regolamento (UE) 2024/1689, art. 51, par. 3.
[570] La *knowledge distillation* è un processo di trasferimento della conoscenza da un modello più grande e complesso ("*teacher*") a un modello più piccolo ed efficiente ("*student*"). Questo avviene attraverso un addestramento supervisionato in cui il modello *student* apprende a riprodurre le previsioni o le rappresentazioni interne del modello *teacher*, riducendo la differenza tra i propri *output* e quelli del modello originale. Per un approfondimento di settore, imprescindibile il riferimento a Geoffrey Hinton, Oriol Vinyals e Jeff Dean, "Distilling the Knowledge in a Neural Network," *arXiv*, n. arXiv:1503.02531 (marzo 2015), https://arxiv.org/abs/1503.02531.
[571] Regolamento (UE) 2024/1689, art. 51, par. 1, lett. a).

dell'Unione.[572] Incombe altresì, a carico dei fornitori, l'obbligo di riferire, senza indebito ritardo all'Ufficio per l'IA e alle autorità nazionali competenti, le informazioni relative agli incidenti gravi verificatisi e alle misure correttive adottate.[573] Per ultimo, i fornitori sono tenuti ad assicurare un livello adeguato di protezione della cybersicurezza, sia del modello, sia della infrastruttura fisica che lo rende operativo.[574]

[572] Regolamento (UE) 2024/1689, art. 51, par. 1, lett. b).
[573] Regolamento (UE) 2024/1689, art. 51, par. 1, lett. c).
[574] Regolamento (UE) 2024/1689, art. 51, par. 1, lett. d).

IV. LA GOVERNANCE DELL'IA: TRA UNIONE EUROPEA E ORDINAMENTO NAZIONALE

1. L'architettura di governance nell'AI Act

L'AI Act istituisce un'innovativa e complessa architettura di *governance* strutturata su due livelli, nazionale e sovranazionale, al fine di garantire un'efficace e uniforme attuazione del Regolamento. Di seguito si tenterà una ricognizione dei ruoli e delle funzioni attribuite ai nuovi organismi di *governance* dell'IA, delle procedure che coinvolgono i soggetti regolati e di alcune criticità emerse dalla più recente riflessione dottrinale.

1.1. Le autorità sovranazionali

La prima autorità di governance prevista dall'AI Act è l'Ufficio europeo per l'IA ("*AI Office*"),[575] istituito in seno alla Commissione Europea e parte della struttura amministrativa del Direttorato generale per le reti di comunicazione, i contenuti e le tecnologie (DG CNET).[576] Questo si presenta come organismo di coordinamento centrale a livello europeo, collaborando strettamente sia con le autorità nazionali di *governance* dell'IA sia con la più ampia comunità di esperti (scientifici, dell'industria e della società civile) per combinare competenze interdisciplinari e valutare gli sviluppi, i potenziali benefici e i rischi dei sistemi di IA.

L'Ufficio svolge specifiche funzioni in ottica di attuazione del Regolamento, tra cui la prestazione di supporto tecnico-scientifico. A tal riguardo, sviluppa strumenti, metodologie e parametri di riferimento per la valutazione delle capacità dei modelli di IA per finalità generali e l'individuazione del rischio sistemico;[577] supporta l'attuazione delle norme sulle pratiche di IA vietate e sui sistemi di IA ad alto rischio, anche facilitando lo

[575] Regolamento (UE) 2024/1689, art. 64.
[576] Commissione Europea, *Decisione del 24 gennaio 2024, che istituisce l'Ufficio Europeo per l'Intelligenza Artificiale*, C(2024) 390 final.
[577] Commissione Europea, C(2024) 390 final, art. 3, par. 1, lett. a).

scambio di informazioni e la collaborazione tra le autorità nazionali;[578] agevola e monitora l'elaborazione di codici di buone pratiche e di codici di condotta a livello UE.[579]

In termini di *enforcement*, l'Ufficio può svolgere indagini su possibili violazioni delle norme sui modelli di IA per finalità generale.[580] Presta poi assistenza normativa alla Commissione nell'elaborazione di diversi atti normativi: prepara decisioni, atti di esecuzione o atti delegati, nonché orientamenti e linee guida a sostegno dell'attuazione del Regolamento;[581] indirizza alla Commissione richieste di normazione e valutazioni delle norme esistenti;[582] fornisce sostegno tecnico e consulenza per l'istituzione di *regulatory sandboxes*, spazi di sperimentazione normativa.[583]

Più in generale, favorisce lo sviluppo e la diffusione di un IA affidabile, cooperando a tal fine con gli *stakeholder*, la Commissione, gli organi e gli organismi europei nonché gli attori internazionali coinvolti.[584] Fornisce inoltre il segretariato al Consiglio per l'IA e supporto amministrativo al Forum consultivo e al Gruppo di esperti scientifici indipendenti, fungendo da motore amministrativo dell'intero impianto di *governance*.[585]

Secondo la migliore dottrina, sebbene centrale nell'architettura di *governance*, l'Ufficio presenterebbe diverse criticità strutturali. Anzitutto, è bene ribadire che questo opera sotto la direzione amministrativa e regolamentare della Commissione, e, in quanto parte del DG CNET, dovrà rispettarne i piani di gestione.[586] Né il testo del Regolamento né la decisione della Commissione con cui è stato istituito dedicano disposizioni alla struttura organizzativa dell'Ufficio, a come garantirne la competenza tecnica o l'autonomia operativa. Tale autonomia operativa appare ulteriormente limitata dalle competenze attribuite ad altri organi e organismi europei, dal momento che mancano

---

[578] Commissione Europea, C(2024) 390 final, art. 3, par. 1, lett. f).
[579] Commissione Europea, C(2024) 390 final, art. 3, par. 2, lett. i).
[580] Commissione Europea, C(2024) 390 final, art. 3, par. 1, lett. d).
[581] Commissione Europea, C(2024) 390 final, art. 3, par. 2, lett. a) e c).
[582] Commissione Europea, C(2024) 390 final, art. 3, par. 2, lett. d).
[583] Commissione Europea, C(2024) 390 final, art. 3, par. 1, lett. e).
[584] Commissione Europea, C(2024) 390 final, artt. 4, 5, 6 e 7.
[585] Commissione Europea, C(2024) 390 final, art. 3, par. 2, lett. h).
[586] Claudio Novelli, Philipp Hacker, Jessica Morley, Jarle Trondal e Luciano Floridi, "A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities," *European Journal of Risk Regulation* (2024): 10-12, doi:10.1017/err.2024.57.

indicazioni in merito ai meccanismi di coordinamento e alla gestione dei conflitti in ipotesi di sovrapposizioni di competenze.[587]

Infine, sebbene l'Ufficio non abbia il potere di adottare decisioni vincolanti, non può ignorarsi come questo influenzi il contenuto delle decisioni e degli atti delegati della Commissione; da qui, la necessità che operi secondo un meccanismo di funzionamento trasparente, in grado di renderne conoscibili ed evidenti gli apporti. Col tempo, potrebbe dunque emergere l'esigenza di dotare l'Ufficio di maggiore autonomia e di personalità giuridica. Una delle possibili soluzioni, sebbene radicale, sarebbe quella di rivedere l'intero quadro istituzionale dell'AI Act, spingendo per una maggiore decentralizzazione e caratterizzandolo come un'Agenzia europea.[588]

Il Consiglio per l'IA ("*European Artificial Intelligence Board*", o EAIB) è l'organo collegiale incaricato di fornire consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del Regolamento.[589] È concepito sul modello di altri *board* europei (*e.g.* l'EDPB del GDPR), come piattaforma di confronto fra autorità nazionali, con funzioni consultive e di indirizzo, nonché di supporto all'armonizzazione. Il Consiglio è composto da un rappresentante designato per ciascuno Stato membro, con mandato triennale rinnovabile una sola volta. È prevista la partecipazione ai lavori dell'Ufficio per l'IA, senza diritto di voto, e del Garante europeo della protezione dei dati (EDPS), in qualità di osservatore. A seconda dei temi trattati, poi, possono essere invitati ai lavori anche altri organismi nazionali o dell'Unione competenti per materia.[590]

Tra i compiti del Consiglio rientrano: formulare raccomandazioni e pareri scritti su qualsiasi questione relativa all'attuazione del regolamento;[591] contribuire

---

[587] Novelli et al., "A Robust Governance for the AI Act," 12-13.
[588] Novelli et al., 21.
[589] Regolamento (UE) 2024/1689, art. 66.
[590] Regolamento (UE) 2024/1689, art. 65, par. 2.
[591] Regolamento (UE) 2024/1689, art. 66, par. 1, lett. e). Raccomandazioni e pareri saranno forniti, tra l'altro: "i) sull'elaborazione e l'applicazione di codici di condotta e codici di buone pratiche ... ; ii) sulla valutazione e il riesame del ... regolamento ... , anche per quanto riguarda la comunicazione di incidenti gravi ... , ... il funzionamento della banca dati dell'UE ... , la preparazione degli atti delegati o di esecuzione ... ; iii) sulle specifiche tecniche o sulle norme esistenti relative ai requisiti [dei sistemi di IA ad alto rischio ... ; iv) sull'uso delle norme armonizzate ... ; v) sulle tendenze, quali la competitività globale europea nell'IA, l'adozione dell'IA nell'Unione e lo sviluppo di competenze digitali; vi) sulle tendenze relative

all'armonizzazione delle pratiche amministrative negli Stati membri;[592] contribuire al coordinamento tra le autorità nazionali, nonché alla condivisione delle conoscenze tecniche e delle migliori pratiche in materia di IA.[593]

Appare opportuno evidenziare una differenza significativa con quanto previsto per l'EDPB nel quadro normativo europeo, all'articolo 65 del GPDR.[594] Il Consiglio per l'IA, diversamente dall'EDPB, non ha il potere di adottare decisioni vincolanti sulle controversie sorte tra le autorità nazionali di controllo. Questa scelta potrebbe indebolire la coerenza complessiva del sistema di *governance*: qualora un'autorità nazionale dovesse interpretare le norme del Regolamento in maniera divergente rispetto a quanto accade negli altri Stati membri, il Consiglio non potrà correggerne la rotta adottando decisioni vincolanti. Ipotizzare un simile scenario non sembra così difficile: si è visto come la disciplina d'attuazione del divieto di sistemi di identificazione biometrica remota in tempo reale lasci ampi spazi di discrezionalità agli Stati membri,[595] potendo variare significativamente tra paesi più attenti alle libertà civili e altri più inclini a giustificare l'impiego di tali sistemi per ragioni di sicurezza.[596]

Il rapporto tra Ufficio e Consiglio per l'IA, infine, sembra caratterizzarsi in termini di supporto reciproco. Pur in presenza di aree in cui le funzioni delle due autorità sembrano sovrapporsi, queste svolgono ruoli distinti: il primo fornisce supporto all'organo esecutivo dell'UE e ne esegue le decisioni vincolanti, il secondo garantisce la coordinazione e la rappresentanza degli Stati membri, mantenendo un grado di indipendenza maggiore rispetto alle istituzioni europee.[597]

All'art. 68 dell'AI Act è poi prevista l'istituzione di un Gruppo scientifico di esperti indipendenti ("*Scientific panel*"), con compiti di supporto all'Ufficio per l'IA nelle attività di *enforcement*.[598] Si tratta di un *panel* di esperti nominati dalla Commissione Europea,

---

all'evoluzione ... delle catene del valore dell'IA ... ; vii) sull'eventuale necessità di modificare l'Allegato III ... e sull'eventuale necessità di una possibile revisione dell'articolo 5 ...".

[592] Regolamento (UE) 2024/1689, art. 66, par. 1, lett. d).

[593] Regolamento (UE) 2024/1689, art. 66, par. 1, lett. a).

[594] Regolamento (UE) 2016/679, art. 65, par. 1.

[595] *Vedi* capitolo III, paragrafo 3.1.

[596] Novelli et al., "A Robust Governance for the AI Act," 16.

[597] Novelli et al., 16.

[598] Regolamento (UE) 2024/1689, art. 68, par. 1.

scelti sulla base delle loro competenze scientifiche o tecniche nel settore dell'IA. Diversamente dal Consiglio, dunque, il Gruppo scientifico non rappresenta gli Stati membri, ma l'eccellenza scientifica indipendente.[599] In particolare, il supporto e la consulenza del *Panel* potranno essere richiesti per la segnalazione dei possibili rischi sistemici, per la classificazione di sistemi e modelli di IA per finalità generali, o anche per assistere il lavoro delle autorità di vigilanza del mercato.[600] Qualora si renda necessario, la Commissione garantisce agli Stati membri l'accesso tempestivo al Gruppo di esperti indipendenti.[601] Gli esperti scientifici sono tenuti a esercitare le loro funzioni con imparzialità e obiettività, e garantiscono la riservatezza delle informazioni e dei dati ottenuti durante lo svolgimento del lavoro.[602]

Il Forum consultivo, invece, è un forum *multi-stakeholder* composto da rappresentanti dell'industria, delle *start*-up, delle PMI, dell'accademia e della società civile, incaricato di fornire consulenza e competenze tecniche al Consiglio per l'IA e alla Commissione, anche mediante l'elaborazione di pareri, raccomandazioni e contributi scritti.[603] La coesistenza di tre distinti organismi di *governance* a livello sovranazionale – Consiglio, Forum consultivo e Gruppo di esperti – con composizioni e competenze parzialmente sovrapponibili, è stata notata dai commentatori, che paventano possibili inefficienze e problemi di coordinamento. Ad aver animato il legislatore sembra esserci l'idea che ciascun organismo sia portatore di un punto di vista diverso, e che tutti contribuiscano a garantire una piena attuazione del Regolamento: l'interesse degli Stati membri nel Consiglio, quello "lobbistico" nel Forum e il punto di vista tecnico-scientifico indipendente nel Gruppo di esperti.[604]

---

[599] Regolamento (UE) 2024/1689, art. 68, par.2: "Il gruppo di esperti scientifici è composto da esperti selezionati dalla Commissione sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'IA necessarie per lo svolgimento dei compiti di cui al paragrafo 3 ed è in grado di dimostrare di soddisfare tutte le condizioni seguenti: a) possesso di particolari conoscenze e capacità nonché competenze scientifiche o tecniche nel settore dell'IA; b) indipendenza da qualsiasi fornitore di sistemi di IA o di modelli di IA per finalità generali; c) capacità di svolgere attività in modo diligente, accurato e obiettivo. La Commissione, in consultazione con il consiglio per l'IA, determina il numero di esperti del gruppo in funzione delle esigenze richieste e garantisce un'equa rappresentanza di genere e geografica".

[600] Regolamento (UE) 2024/1689, art. 68, par. 3, lett. a) e b).

[601] Regolamento (UE) 2024/1689, art. 69.

[602] Regolamento (UE) 2024/1689, art. 68, par. 4.

[603] Regolamento (UE) 2024/1689, art. 67, par. 1, 2 e 3.

[604] Novelli et al., "A Robust Governance for the AI Act," 15.

1.2. Le autorità nazionali competenti: notifica e vigilanza del mercato

A livello nazionale, ogni Stato membro è tenuto a garantire l'operatività di apposite autorità nazionali competenti, che avranno il compito di assicurare l'attuazione e l'applicazione dell'AI Act, esercitando i loro poteri in modo indipendente e imparziale.[605] Queste dovranno disporre di adeguate risorse tecniche, finanziarie e umane, e la Commissione ne agevola la cooperazione e lo scambio di esperienze.[606] Ai sensi dell'art. 70, ciascuno Stato deve istituire o designare almeno un'autorità di vigilanza del mercato e un'autorità di notifica.[607] Alla Commissione andrà poi notificato quale autorità di vigilanza del mercato funge da punto di contatto unico ai fini del Regolamento, di modo che possa essere inserita nell'elenco dei punti di contatto disponibili al pubblico.[608]

Le autorità di notifica sono gli organismi nazionali preposti a valutare, designare e notificare gli organismi di valutazione della conformità (c.d. organismi notificati) che eseguiranno le verifiche di conformità dei sistemi di IA ad alto rischio.[609] In pratica, l'autorità di notifica riceve le candidature, *rectius* domande di notifica, di organismi nazionali che intendono svolgere il ruolo di organismo notificato ai fini del Regolamento, e ne verifica il possesso di tutti i requisiti (competenze tecniche, imparzialità, indipendenza, risorse, *etc*.) anche tramite certificazioni di accreditamento nazionali.[610] Una volta accertata la conformità ai requisiti prescritti *ex* art. 31, l'autorità autorizza l'organismo di valutazione e lo notifica alla Commissione e agli altri Stati membri.[611] In assenza di obiezioni,[612] la Commissione procederà dunque ad attribuire un numero di identificazione unico all'organismo notificato, che sarà inserito in un apposito elenco disponibile al pubblico, insieme all'indicazione degli specifici sistemi di IA per i quali può procedere alla valutazione di conformità.[613] Gli organismi potranno ricevere la

---

[605] Regolamento (UE) 2024/1689, art. 70, par. 1.
[606] Regolamento (UE) 2024/1689, art. 70, par. 3.
[607] Regolamento (UE) 2024/1689, art. 70, par. 1.
[608] Regolamento (UE) 2024/1689, art. 70, par. 2.
[609] Regolamento (UE) 2024/1689, art. 28, par. 1.
[610] Regolamento (UE) 2024/1689, art. 29.
[611] Regolamento (UE) 2024/1689, art. 30, par. 1 e 2.
[612] Regolamento (UE) 2024/1689, art. 30, par. 5: "Se sono sollevate obiezioni, la Commissione avvia senza ritardo consultazioni con gli Stati membri pertinenti e l'organismo di valutazione della conformità. Tenutone debito conto, la Commissione decide se l'autorizzazione è giustificata ...".
[613] Regolamento (UE) 2024/1689, art. 35.

notifica anche da parte di autorità di più Stati membri.[614] Successivamente, all'autorità di notifica spetta il compito di sorvegliare sull'operato degli organismi notificati. Qualora l'autorità abbia motivo di ritenere che un organismo notificato non soddisfa più i requisiti *ex* art. 31 o sia inadempiente, questa potrà limitare, sospendere o ritirare la designazione.[615]

Quanto ai possibili profili di criticità emergenti dal punto di vista regolatorio, la letteratura ha esposto alcuni dubbi in merito al funzionamento degli organismi notificati. Si rileva, anzitutto, una mancanza di trasparenza organizzativa e operativa, ulteriormente aggravata dal frequente ricorso all'*outsourcing* delle attività di valutazione di conformità da parte degli organismi stessi.[616] Poco è detto dal Regolamento in merito al meccanismo di coordinamento tra gli organismi notificati *ex* art. 38, se non che questo dovrà essere garantito dalla Commissione. Un livello di coordinamento adeguato è però essenziale per non incorrere in difformità nazionali nell'interpretazione della disciplina di notifica e monitoraggio degli organismi notificati, al fine di prevenire pratiche c.d. di "*conformity shopping*".[617] Infine, sebbene sia previsto che gli organismi notificati debbano essere indipendenti dai fornitori di sistemi di IA per i quali svolgono valutazioni della conformità,[618] in assenza di indicazioni sufficientemente chiare su come garantire e valutare tale indipendenza si corre il rischio concreto di una c.d. "cattura del regolatore".[619]

Quanto alle autorità di vigilanza del mercato, l'art. 74 dell'AI Act estende l'ambito di applicazione del regolamento europeo sulla vigilanza del mercato e la conformità dei prodotti a tutti gli operatori e a tutti i sistemi soggetti alla disciplina dell'AI Act.[620] Le autorità di vigilanza del mercato istituite con regolamento (UE) 2019/1020 esercitano

---

[614] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 100.
[615] Regolamento (UE) 2024/1689, art. 36, par. 4. Analogo potere, per altro, spetta alla Commissione, *ex* art. 37.
[616] Sul tema, *si veda* Jean-Pierre Galland, "The Difficulties of Regulating Markets and Risks in Europe through Notified Bodies," *European Journal of Risk Regulation* 4, n. 3 (2013): 365–373.
[617] Novelli et al., "A Robust Governance for the AI Act," 18.
[618] Regolamento (UE) 2024/1689, art. 31, par. 4.
[619] Si rimanda a Aude Cefaliello e Miriam Kullmann, "Offering False Security: How the Draft Artificial Intelligence Act Undermines Fundamental Workers' Rights," *European Labour Law Journal* 13, n. 4 (dicembre 2022): 542–562, doi:10.1177/20319525221114474.
[620] Regolamento (UE) 2024/1689, art. 74.

dunque la loro attività di controllo anche verso operatori economici e sistemi di IA, così come definiti del Regolamento sull'intelligenza artificiale.[621] Sono poi individuate regole specifiche per la designazione dell'autorità di vigilanza del mercato competente per i sistemi di IA impiegati in alcuni settori o soggetti a norme armonizzate.[622] Di particolare interesse, inoltre, quanto previsto al par. 9 dell'art. 74: è riconosciuta all'EDPS la qualità di autorità di vigilanza del mercato per quanto concerne l'applicazione delle disposizioni dell'AI Act a istituzioni, organi e organismi dell'Unione.[623]

Alle autorità di vigilanza spettano importanti poteri ispettivi e di indagine: possono verificare la conformità dei sistemi di IA; hanno accesso, limitatamente a quanto necessario per l'adempimento delle loro funzioni, alla documentazione tecnica e ai *log*, ai *set* di dati utilizzati per l'addestramento, la convalida e la prova dei sistemi, nonché, laddove sussistano specifiche condizioni, al codice sorgente dei sistemi di IA ad alto rischio.[624] In ogni caso, queste garantiscono la massima riservatezza in merito alle informazioni ottenute nel corso della loro attività.[625]

Le autorità di vigilanza fungono quindi da primo baluardo nazionale nell'applicazione del Regolamento, pur operando all'interno di una complessa rete di cooperazione europea, supportata dall'Ufficio e dal Consiglio per l'IA. In tale contesto, è esplicitamente incoraggiato, di concerto con la Commissione, lo svolgimento di indagini congiunte tra autorità di diversi Stati membri, in particolare in relazione a sistemi di IA ad alto rischio che presentino un rischio grave di natura transfrontaliera.[626] Parallelamente, è prevista la collaborazione con l'Ufficio per l'IA in alcune ipotesi relative ai sistemi di IA per finalità generali o a determinati sistemi ad alto rischio basati su modelli di IA per finalità generali.[627] È poi prevista la cooperazione e il coordinamento

---

[621] Inoltre, comunicano annualmente alla Commissione e alle autorità garanti della concorrenza le informazioni rilevanti per il diritto della concorrenza, e riferiscono inoltre alla Commissione in merito a eventuali pratiche vietate verificatesi nel corso dell'anno. Regolamento (UE) 2024/1689, art. 74, par. 2.
[622] Mandarà, "Il Regolamento UE sull'intelligenza artificiale," 100.
[623] Regolamento (UE) 2024/1689, art. 74, par. 9.
[624] Regolamento (UE) 2024/1689, art. 74, par. 11, 12 e 13.
[625] Regolamento (UE) 2024/1689, art. 74, par. 14 e art. 78.
[626] Regolamento (UE) 2024/1689, art. 74, par. 11.
[627] Regolamento (UE) 2024/1689, art. 75. Sono previste tre diverse ipotesi di collaborazione. In particolare, nel caso in cui un sistema di IA si basi su un modello di IA per finalità generali, e sia il modello sia il sistema siano sviluppati dallo stesso fornitore, sarà l'Ufficio per l'IA a monitorare e supervisionare la conformità di tale sistema agli obblighi del Regolamento. Per svolgere i suoi compiti, l'Ufficio disporrà di

con alcune autorità di vigilanza di settore quando necessario. A tal riguardo, è opportuno evidenziare come permangano zone grigie e potenziali sovrapposizioni di competenze tra le diverse autorità coinvolte, elementi che potrebbero generare frizioni nella prassi applicativa.[628]

Obblighi di cooperazione sono previsti anche con le autorità nazionali che tutelano i diritti fondamentali, compreso il diritto alla non discriminazione, quali le autorità nazionali per la protezione dei dati.[629] A titolo di esempio, l'art. 77 riconosce a queste ultime il diritto di richiedere e ottenere accesso a tutta la documentazione prodotta ai sensi del Regolamento, in formato accessibile e comprensibile. Di ogni richiesta in tal senso sarà informata proprio l'autorità di vigilanza dello Stato membro interessato.[630]

Un'ultima considerazione: come visto, l'art. 70 consente agli Stati membri di istituire nuove autorità nazionali o, in alternativa, di indicarne di preesistenti quali autorità competenti ai fini dell'AI Act. In particolare, in alcuni Stati membri si è discusso in merito all'opportunità di designare, quale autorità di vigilanza del mercato, proprio l'autorità nazionale per la protezione dei dati (*Data Protection Authority*, o DPA).[631] È proprio l'EDPB, inoltre, ad aver sostenuto che i garanti nazionali potrebbero rappresentare la scelta naturale per le autorità di vigilanza del mercato contemplate dall'AI Act. Del resto, "le autorità di protezione dei dati hanno dimostrato ... di essere attori indispensabili nella

---

tutti i poteri di un'autorità di vigilanza del mercato. Qualora abbiano motivi sufficienti per ritenere che i sistemi di IA per finalità generali che possono essere utilizzati direttamente dai *deployer* per almeno una finalità classificata come ad alto rischio non siano conformi ai requisiti prescritti, le autorità di vigilanza del mercato cooperano con l'Ufficio per effettuare valutazioni della conformità e informano il Consiglio per l'IA e le altre autorità di vigilanza. Infine, qualora non sia in grado di concludere la propria indagine sul sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali, un'autorità di vigilanza del mercato può presentare una richiesta motivata all'Ufficio per l'IA, che garantirà l'accesso alle informazioni.

[628] Laura Pliauskaite e Isabelle Roccia, "Governance: EU and National Stakeholders," in *Top 10 Operational Impacts of the EU AI Act*, *IAPP* (settembre 2024): 48, https://iapp.org/media/pdf/resource_center/top_10_impacts_eu_ai_act.pdf.

[629] Novelli et al., "A Robust Governance for the AI Act," 19.

[630] Regolamento (UE) 2024/1689, art. 77.

[631] Florina Pop, Michaela Sullivan-Paul ed Elpida Longinidou, "Are Data Protection Authorities the New AI Market Surveillance Authorities?," *European Institute of Public Administration Blog*, 23 settembre 2024, https://www.eipa.eu/blog/are-data-protection-authorities-the-new-ai-market-surveillance-authorities/.

catena che porta alla diffusione sicura e orientata ai diritti dei sistemi di IA".[632] Appare opportuno sottolineare come le DPA abbiano storicamente svolto, sin dal principio, funzione di controllo sull'osservanza della normativa in materia di protezione dei dati anche in relazione ai sistemi di intelligenza artificiale, dal momento che il GDPR trova applicazione in riferimento a qualsiasi trattamento dei dati personali.[633] Designarle quali autorità di vigilanza del mercato ai fini dell'AI Act consentirebbe, per altro, di sfruttare gli assetti organizzativi esistenti e le conoscenze acquisite in materia di IA da tali autorità.[634] Esempio eloquente del ruolo rivestito dalle DPA nella *governance* dell'IA, ancor prima dell'entrata in vigore dell'AI Act, è fornito dall'intervento del Garante italiano nei confronti di ChatGPT. La vicenda rappresenta un caso di studio paradigmatico nel dibattito sulla regolamentazione dell'intelligenza artificiale, e pertanto se ne propone un'analisi al paragrafo che segue.

Un'altra strada percorribile dagli Stati membri, infine, potrebbe essere quella di istituire una sotto-sezione specializzata per l'IA all'interno delle autorità di vigilanza del mercato già esistenti. Attualmente, negli Stati dell'UE operano diverse autorità di vigilanza classificate per settore (*e.g.* dispositivi medici, prodotti da costruzione, veicoli a motore), e potrebbe essere loro concessa competenza esclusiva sulla vigilanza dei sistemi di IA impiegati nel settore di riferimento.[635] All'estremo opposto, uno Stato potrebbe optare per la creazione di un nuovo organismo centralizzato dedicato esclusivamente all'IA, sebbene ciò implichi costi e tempi maggiori.[636] Quale che sia la strada scelta dagli Stati dell'Unione, non può ignorarsi come questa eterogeneità di approcci – alla luce di quanto previsto dal Regolamento, tutti percorribili in linea teorica – possa generare importanti difformità tra i livelli nazionali di *governance*.[637]

---

[632] European Data Protection Board, *Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework* (2024), 3, https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf.

[633] Pop, Sullivan-Paul e Longinidou, "Are Data Protection Authorities the New AI Market Surveillance Authorities?"

[634] Novelli et al., "A Robust Governance for the AI Act," 4.

[635] Novelli et al., 19.

[636] Novelli et al., 3-4 e 19.

[637] Ad analoghe conclusioni sembra giungere Kasia Söderlund e Stefan Larsson, "Enforcement Design Patterns in EU Law: An Analysis of the AI Act," *Digital Society* 3 (luglio 2024): 1–21, doi:10.1007/s44206-024-00129-8, cui si rimanda per una panoramica completa sul tema dell'*enforcement* nell'AI Act.

2. I provvedimenti del Garante italiano: il "caso ChatGPT" e il "caso DeepSeek"

Il 30 marzo 2023, in Italia, l'autorità garante per la protezione dei dati personali (in seguito anche "l'Autorità", o "il Garante") ha emanato un provvedimento d'urgenza con cui ha imposto a OpenAI, società statunitense sviluppatrice e gestrice di ChatGPT, la "limitazione provvisoria del trattamento" dei dati personali degli interessati stabiliti nel territorio italiano.[638] L'intervento del Garante, oltre a costituire una decisione del tutto inedita nel panorama regolatorio europeo, rappresenta con efficacia il ruolo che possono assumere le autorità nazionali per la protezione dei dati nella regolazione dell'IA. Già da prima dell'entrata in vigore dell'AI Act, infatti, il Garante ha dimostrato come gli strumenti giuridici esistenti, *in primis* il GDPR, possano essere impiegati per tutelare i diritti fondamentali anche di fronte alla sfida dell'intelligenza artificiale. Il provvedimento ha conosciuto una vasta eco a livello internazionale, stimolando dibattito in merito al delicato equilibrio tra innovazione e tutela dei diritti fondamentali, tra coloro che auspicano la definizione di limiti etici e giuridici per l'IA e quanti paventano un rallentamento del progresso tecnologico in Italia e nell'Unione Europea.[639] Il "caso ChatGPT" costituisce un precedente rilevante altresì per aver incoraggiato un coordinamento a livello europeo in materia. In seguito al provvedimento italiano, l'EDPB ha istituito una *taskforce* di esperti europei su ChatGPT, al fine di promuovere la cooperazione e lo scambio di informazioni tra le DPA su eventuali iniziative per l'applicazione del GDPR.[640] Parallelamente, il Parlamento europeo ha emendato il testo dell'AI Act – al tempo in corso di approvazione – al fine di includervi i sistemi di IA per finalità generali.[641]

A distanza di quasi due anni, il 28 gennaio 2025, il Garante è tornato a occuparsi di IA generativa, intervenendo nei confronti di un nuovo sistema sul mercato europeo:

---

[638] Garante per la protezione dei dati personali, *Provvedimento n. 112*, 30 marzo 2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

[639] Gianluigi Maria Riva, "IA e Internet," in *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli (Rimini: Maggioli, 2024), 327.

[640] European Data Protection Board, *Report of the Work Undertaken by the ChatGPT Taskforce*, 23 maggio 2024,https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

[641] *Vedi* capitolo II, paragrafo 3.

DeepSeek, *chatbot* cinese che ha registrato una rapidissima diffusione, con milioni di *download* soltanto sul territorio italiano.[642] In difetto di rassicurazioni in merito alle modalità di trattamento dei dati da parte dei titolari, l'Autorità italiana ha preliminarmente inviato una richiesta di informazioni a *Hangzhou DeepSeek Artificial Intelligence* e *Beijing DeepSeek Artificial Intelligence*, le società che forniscono il servizio.[643] Successivamente, valutando la risposta delle società alla richiesta come "del tutto insufficiente", il Garante ha disposto, in via d'urgenza e con effetto immediato, la limitazione del trattamento dei dati degli utenti italiani.[644]

Sebbene l'istruttoria aperta nei confronti di *DeepSeek* sia ancora in corso e in attesa di definizione, entrambe le vicende offrono l'occasione per un'analisi dei rilievi giuridici alla base degli interventi del Garante, delle principali obiezioni sollevate dai commentatori della comunità legale e tecnologica, del possibile ruolo delle DPA nel *framework* regolatorio dell'intelligenza artificiale.

In seguito al Provvedimento n. 112 del 30 marzo, il discorso pubblico pare essersi concentrato intorno a due interrogativi: ci si è chiesti, per lo più, se l'intervento d'urgenza del Garante fosse necessario e, in caso di risposta affermativa, proporzionato.[645] Sul punto è stato ribadito, in letteratura, che la disciplina della protezione dei dati incrocia il diritto amministrativo ogni qual volta il Garante non opera nelle sue funzioni giurisdizionali.[646] Questi è infatti un'autorità amministrativa indipendente, istituita dalla legge n. 675 del 31 dicembre 1996 e disciplinata dal Codice in materia di protezione dei dati personali.[647]

---

[642] Alessandro Longo, "Privacy, faro su Deepseek: a rischio i dati di milioni di italiani," *Il Sole 24 Ore*, 28 gennaio 2025, https://www.ilsole24ore.com/art/il-garante-la-privacy-accende-faro-deepseek-e-apre-indagine-AGWUATbC.

[643] La richiesta di informazioni (prot. n. 10841/25) inviata dal Garante il 28 gennaio 2025 non risulta pubblicamente accessibile. Per un riferimento, *si veda* Garante per la protezione dei dati personali, "IA: il Garante privacy chiede informazioni a DeepSeek. Possibile rischio per i dati di milioni di persone in Italia," *Comunicato stampa*, 28 gennaio 2025, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10096856.

[644] Garante per la protezione dei dati personali, *Comunicato stampa*, 30 gennaio 2025, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10097450.

[645] Riva, "IA e Internet," 333.

[646] Riva, 334.

[647] D.lgs n. 196/2003, *Codice in materia di protezione dei dati personali*. Quanto al quadro normativo europeo, l'istituzione di un'autorità indipendente per la tutela dei dati personali è prevista all'art. 51 del GDPR. Per un riferimento *extra* GDPR, *si veda* anche *Carta dei Diritti Fondamentali dell'Unione Europea*, art. 8, comma 3.

Laddove espressione del potere amministrativo, l'attività del Garante dovrà pertanto trovare giustificazione e fondamento nella legge. Partendo dal dato normativo, dunque, è evidente come sia proprio il GDPR ad attribuire all'Autorità il potere di sorvegliare e assicurare l'applicazione del regolamento, di svolgere indagini e di monitorare "gli sviluppi che presentano un interesse ... in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali".[648] Quanto al contenuto del Provvedimento, occorre preliminarmente un chiarimento terminologico: sebbene nel dibattito pubblico e mediatico si sia parlato diffusamente di un "blocco" di ChatGPT, è bene sottolineare che il Garante si è limitato a disporre, in conformità con quanto previsto *ex* art. 58, par. 2, lett. f) del GDPR, la "misura della limitazione provvisoria del trattamento dei dati personali" degli utenti italiani.[649] La sospensione integrale del servizio in Italia, per tanto, sarebbe da ricondursi a una scelta di OpenAI. Ad avviso di chi scrive, tuttavia, appare difficile sostenere che il fornitore potesse in concreto adottare soluzioni alternative, soprattutto alla luce delle violazioni contestategli e della natura del servizio offerto.

Di concerto con la disposizione della limitazione del trattamento, il Garante ha poi aperto un'istruttoria nei confronti di OpenAI, invitando quest'ultima, entro 20 giorni dalla ricezione del Provvedimento, a comunicare le iniziative intraprese al fine di dare attuazione a quanto prescritto dall'Autorità e a fornire ogni elemento utile a giustificare le violazioni contestate, [650] di cui si dirà a breve. Anche in questo caso, l'invito del Garante trova conforto sicuro nel dato normativo, dal momento che il GDPR riconosce espressamente il potere delle autorità di controllo di "notificare al titolare del trattamento ... le presunte violazioni del ... regolamento",[651] di rivolgergli avvertimenti in merito alle violazioni,[652] nonché di "ingiungere al titolare ... di conformare i trattamenti alle

---

[648] Regolamento (UE) 2016/679, art. 57, par. 1, lett. a), h) e i).

[649] Elio Franco, "ChatGPT è il buco nero della privacy, il Garante ha fatto bene: ecco perché," *Cybersecurity360*, 3 aprile 2023, https://www.cybersecurity360.it/legal/privacy-dati-personali/chatgpt-e-il-buco-nero-della-privacy-il-garante-ha-fatto-bene-ecco-perche/.

[650] Garante, *Provvedimento n. 112*, 30 marzo 2023.

[651] Regolamento (UE) 2016/679, art. 58, par. 1, lett. d). Ma sembra rilevare, nel caso in esame, anche il potere del Garante di "ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti", di cui alla lett. a) del presente articolo.

[652] Regolamento (UE) 2016/679, art. 58, par. 2, lett. a) e b).

disposizioni del ... regolamento, se del caso, in una determinata maniera ed entro un determinato termine".[653]

In virtù dell'ambito di applicazione c.d. extraterritoriale del GDPR, art. 3, par. 2, poi, a nulla rileva che il servizio ChatGPT fosse offerto da un soggetto *extra*-UE al tempo privo di stabilimento sul territorio europeo, essendo in ogni caso contemplato il trattamento di dati personali di interessati nell'Unione.[654] Piuttosto, dal momento che OpenAI era priva di uno stabilimento nell'UE, il Garante italiano ha potuto agire di sua iniziativa, non trovando applicazione il meccanismo c.d. dello *one-stop-shop* (sportello unico) *ex.* artt. 56 e 60 del GDPR.[655] Come evidenziato dall'EDPB, a partire dal 15 febbraio 2024, in effetti, OpenAI si è dotata di uno stabilimento sul territorio dell'Unione (in Irlanda); pertanto, il meccanismo dello sportello unico troverà applicazione soltanto in riferimento a quelle procedure di trattamento dati successive a tale data, senza pregiudizio per le investigazioni e le istruttorie in corso concernenti presunte infrazioni del GDPR anteriori al 15 febbraio 2024. Tali investigazioni, inclusa quella del Garante italiano, continueranno senza pregiudizio alcuno, coordinate dalla *taskforce* dell'EDPB.[656]

Venendo alle violazioni contestate nel Provvedimento, in primo luogo il Garante rilevava l'assenza di qualsivoglia informativa, diretta agli utenti e agli interessati, in

---

[653] Regolamento (UE) 2016/679, art. 58, par. 2, lett. d).

[654] Regolamento (UE) 2016/679, art. 3, par. 2: "Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

[655] Regolamento (UE) 2016/679, artt. 56 e 50. Attraverso il principio dello sportello unico il GDPR mira all'armonizzazione delle norme europee in materia di protezione dei dati personali. Il meccanismo si applica se: (i) il titolare (o il responsabile) del trattamento opera in più Stati dell'Unione europea; (ii) il trattamento, pur effettuato da un titolare con stabilimento in un solo Stato dell'UE, incide in modo sostanziale sugli interessati residenti in più di uno Stato membro dell'Unione. In tali circostanze, l'autorità di controllo dello Stato membro ove è situato lo stabilimento del titolare (o responsabile) agisce in qualità di autorità di controllo capofila per le attività di trattamento transfrontaliero e per le relative indagini. Tale autorità è investita del potere di adottare decisioni vincolanti per le altre autorità coinvolte, ma è tenuta a cooperare con le altre autorità nei casi di maggiore rilevanza concernenti violazioni del Regolamento europeo sulla protezione dei dati personali e in ipotesi di contrasti tra le diverse autorità. L'argomento esula dall'ambito di questa trattazione, per tanto, si rimanda a "Exceptions to the One-Stop-Shop Rule of the GDPR," *GRUR International* 71, n. 1 (gennaio 2022): 64–81, doi:10.1093/grurint/ikab139

[656] EDPB, *Report of the Work Undertaken by the ChatGPT Taskforce*, 5.

merito alle modalità con cui i loro dati sarebbero stati raccolti e trattati tramite ChatGPT, in violazione degli obblighi di trasparenza di cui all'art. 13 del GDPR.[657] L'Autorità evidenziava altresì "l'assenza di idonea base giuridica in relazione alla raccolta dei dati personali e al loro trattamento per scopo di addestramento degli algoritmi sottesi al funzionamento di ChatGPT",[658] ritenendo non soddisfatta nessuna delle condizioni di liceità di cui all'art. 6 del Regolamento generale sulla protezione dei dati.[659] OpenAI, infatti, aveva erroneamente indicato quale base giuridica del trattamento quella prevista alla lettera b) dell'articolo sopracitato, e cioè che il trattamento fosse "necessario all'esecuzione di un contratto di cui l'interessato è parte". Tale indicazione, tuttavia, è apparsa al Garante insufficiente a giustificare l'utilizzo su larga scala di dati personali necessario per l'addestramento del modello di IA alla base del *chatbot*.[660] In aggiunta, il Garante ritiene "inesatto" il trattamento, dal momento che le informazioni fornite da ChatGPT non sempre corrispondono al dato reale.[661] Per ultimo, viene censurata l'assenza di qualsivoglia meccanismo di verifica dell'età degli utenti, in violazione di quanto previsto all'art. 8 del GDPR e nonostante i termini di servizio di OpenAI dichiarino che questo sia riservato esclusivamente ai maggiori di 13 anni.[662]

---

[657] Regolamento (UE) 2016/679, art. 13.

[658] Garante, *Provvedimento n. 112*, 30 marzo 2023.

[659] Regolamento (UE) 2016/679, art. 6, par. 1: "Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".

[660] Così si evince dal successivo provvedimento adottato dall'Autorità nei confronti di OpenAI. Garante per la protezione dei dati personali, *Provvedimento n. 114*, 11 aprile 2023, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702

[661] In violazione di quanto previsto *ex* art. 5, par. 1, lett. d) del GDPR.

[662] Regolamento (UE) 2016/679, art. 8, par. 1 e 2: "... per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale ... Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale ...".

Alla luce delle considerazioni sino a qui svolte, appaiono senz'altro convincenti le motivazioni che hanno portato il Garante a intervenire. Potrebbe certo argomentarsi in merito alla doverosità di tale intervento, nonché discutere sul se l'esercizio dei poteri correttivi costituisca un'attività discrezionale, oppure, di converso, se l'Autorità fosse obbligata a intervenire d'urgenza. In ogni caso, il Provvedimento appare legittimo sul piano normativo. Se quanto si sostiene è vero, tuttavia, non si comprende la ragione per cui le altre DPA europee non siano intervenute, analogamente al Garante italiano, d'urgenza. A tal riguardo, appaiono più che condivisibili le considerazioni avanzate da Rivera: "o lo spazio di valutazione discrezionale all'interno di un'attività cogente di vigilanza, controllo e intervento è particolarmente ampio da prevedere comportamenti incoerenti fra le stesse autorità europee, o l'una – l'italiana – o le altre sono in difetto". Delle due l'una: o il Garante ha "abusato" dei poteri discrezionali, o le DPA europee hanno omesso di esercitare i loro poteri quando era doveroso farlo.[663]

Per altro, in ragione dell'urgenza ravvisata dal Garante si è deciso di procedere nelle more dell'istruttoria aperta nei confronti di OpenAI, disponendo sin da subito la misura correttiva più "forte", *id est* la limitazione del trattamento. Di più: l'urgenza è stata ritenuta tale da non permettere neanche la convocazione in tempo utile dell'Autorità, e il presidente ha quindi adottato provvedimento urgente in sostituzione dell'organo.[664] Ammesso che una tale urgenza vi fosse, però, non si comprende per quale motivo il Garante abbia agito diversamente nell'analogo caso *DeepSeek*. Il *chatbot* cinese, infatti, presenta le medesime criticità che hanno stimolato l'intervento dell'Autorità su ChatGPT,[665] cui si aggiunge il "tema Cina", e cioè il fatto che i dati raccolti dal titolare

---

[663] Riva, "IA e Internet," 335.

[664] L'Autorità ritiene ricorrano i presupposti per l'applicazione dell'art. 5, comma 8, del Regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante, il quale prevede che "nei casi di particolare urgenza e di indifferibilità che non permettono la convocazione in tempo utile del Garante, il presidente può adottare i provvedimenti di competenza dell'organo, i quali cessano di avere efficacia sin dal momento della loro adozione se non sono ratificati dal Garante nella prima riunione utile, da convocarsi non oltre il trentesimo giorno". Garante, *Provvedimento n. 112*, 30 marzo 2023.

[665] In un'intervista rilasciata ad Agenda Digitale, il presidente dell'Autorità, Prof. Pasquale Stanzione, ha espresso preoccupazione per DeepSeek, "la stessa [preoccupazione] che avevamo maturato su ChatGPT due anni fa: bisogna sapere quali sono le fonti che hanno alimentato il chatbot, qual è la base giuridica su cui si è mosso e soprattutto evitare o comunque sapere che non ci siano fake news e bias." *Si veda* Massimo Borgobello, "DeepSeek, privacy zero: comincia in Italia lo scontro di diritti," *Agenda Digitale*, 30 gennaio 2025, https://www.agendadigitale.eu/sicurezza/privacy/deepseek-privacy-zero-in-italia-e-scontro-di-diritti/.

nell'ambito della fornitura del servizio sono conservati presso la Repubblica Popolare Cinese, in potenziale violazione di quanto previsto dall'art. 32 del GDPR in materia di sicurezza del trattamento.[666] Eppure, in quest'ultimo caso, il Garante sembra essersi mosso con maggiore cautela, dapprima inviando alle società cinesi titolari del trattamento una richiesta di informazioni,[667] e soltanto in seguito, dopo aver ritenuto la risposta da parte delle società insufficiente, disponendo la misura della limitazione del trattamento.[668]

In seguito al "caso ChatGPT", diversi commentatori (e persino alcuni rappresentati delle istituzioni) hanno osservato come il provvedimento dell'Autorità non abbia interessato le API[669] di OpenAI, circostanza che ha determinato la paradossale situazione per cui, durante il periodo di sospensione del servizio, rimanevano accessibili in Rete numerosi servizi basati sull'architettura GPT.[670] Invero, le motivazioni che hanno spinto l'Autorità a intervenire risultano astrattamente applicabili a una pluralità di altri sistemi di IA generativa, meritevoli di analogo scrutinio. Si pensi, *exempli gratia*, ai *chatbot* basati su LLM di diversi fornitori, quali Gemini di Google, Claude di Anthropic, Perplexity, Grok di XAi, o ancora, ai servizi di generazione immagini e video, tra cui DALL-E (sempre di OpenAI), Runway e Midjourney, solo per citarne alcuni. Replika, un altro *chatbot*, costituisce, al momento in cui si scrive, l'unica eccezione, essendo stato oggetto di analogo provvedimento di limitazione del trattamento dei dati da parte del Garante. [671]

Un'ulteriore considerazione s'impone in merito all'effettività dei provvedimenti del Garante. La sospensione di questi servizi limitatamente al territorio italiano può essere elusa dall'utenza mediante l'utilizzo di semplici reti private virtuali (VPN). Emblematico, a tal riguardo, il dato dichiarato da AtlasVPN: secondo il fornitore di servizi VPN, in Italia, a seguito della sospensione di ChatGPT, i *download* del suo applicativo *software*

---

[666] Regolamento (UE) 2016/679, art. 32.

[667] Garante, *Comunicato stampa*.

[668] Garante per la protezione dei dati personali, *Provvedimento n. 33*, 30 gennaio 2025, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10098477.

[669] *Application Programming Interface*. Si tratta di interfacce che consentono a diversi *software* di comunicare tra loro in modo strutturato e automatizzato, definendo regole e protocolli per l'accesso a determinate funzionalità o dati di un sistema.

[670] Riva, "IA e Internet," 337. L'autore segnala, in particolare, come, durante la sospensione del servizio, ChatGPT continuasse a essere accessibile come applicativo di Bing, motore di ricerca di Microsoft.

[671] Garante per la protezione dei dati personali, *Provvedimento n. 39*, 2 febbraio 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852214.

sarebbero aumentati di oltre il 400% rispetto alla media registrata nel mese di marzo.[672] La disponibilità di numerose API e modelli di IA per finalità generali (specialmente quando rilasciati con licenza *open source*) consente, inoltre, la proliferazione di servizi alternativi e la nascita di *competitor* in grado di affermarsi in tempi brevi sul mercato, rendendo potenzialmente inefficace un modello di vigilanza basato esclusivamente su interventi puntuali *ex post*. Il rischio è che le DPA si ritrovino coinvolte in un meccanismo di tipo "*whack-a-mole*" ("schiaccia la talpa"), in cui, per ogni intervento correttivo indirizzato a uno specifico fornitore, si assiste alla nascita e all'affermazione di una moltitudine di servizi analoghi.

Nel tentare un'analisi giuridica del fenomeno, non può tacersi in ogni caso la dimensione "politica" sottesa alla vicenda: posto che nessuna DPA è intervenuta nei confronti dei fornitori e dei servizi sopracitati, la questione si configura in termini di opportunità dell'azione, ovverosia se non fosse preferibile, rispetto all'intervento "solitario" del Garante italiano, un'azione coordinata tra le autorità europee sul settore dell'IA generativa.[673]

Nonostante le criticità evidenziate, non può negarsi come, quantomeno nel caso di ChatGPT, l'intervento del Garante abbia sortito importanti effetti. Le violazioni del GDPR contestate – concernenti, si è detto, gli obblighi informativi di trasparenza, l'assenza di una base giuridica idonea per il trattamento dei dati, l'inesattezza dei dati in *output*, l'assenza di misure di tutela dei minori e il mancato rispetto del principio di *privacy by design/by default* – avevano indotto l'Autorità a ritenere il trattamento dei dati eseguito da OpenAI in violazione degli artt. 5, 6, 8, 13 e 25 del GDPR.[674] A fronte di tali rilievi, la *no-profit* americana ha intrapreso azioni di adeguamento nel corso dell'aprile 2023, tra cui: la pubblicazione di una *privacy policy* per il trattamento dei dati finalizzato all'addestramento dei modelli; l'implementazione di strumenti per l'esercizio dei diritti degli interessati, incluso un *form* per l'opposizione e la cancellazione; l'individuazione

---

[672] Il dato è stato riportato da numerose testate giornalistiche e persino in alcuni commenti della dottrina sul tema. Si deve tuttavia rilevare che i dati originariamente pubblicati dal fornitore non risultano più accessibili *online*, e sono attualmente attestati soltanto da fonti secondarie. Considerata la diffusione di cui ha goduto la notizia e, di riflesso, la visibilità ottenuta dal servizio, si suggerisce una certa cautela nella sua valutazione.

[673] Riva, "IA e Internet," 336-337.

[674] Garante, *Provvedimento n. 112*, 30 marzo 2023.

del legittimo interesse ex art. 6, par. 1, lett. f) del GDPR quale base giuridica per il trattamento dei dati ai fini dell'addestramento del modello; l'introduzione di un meccanismo di *opt-out* per consentire agli utenti di sottrarre i propri dati all'addestramento; e, infine, l'attivazione di un meccanismo di *age-gate* per la verifica dell'età degli utenti, volto a impedire l'accesso al servizio da parte di minori di 13 anni e a raccogliere l'attestazione del consenso genitoriale per utenti di età compresa tra i 13 e i 17 anni.[675] Alla luce delle azioni intraprese dal titolare, l'Autorità, con provvedimento n. 114 dell'11 aprile 2023, ha quindi deliberato la sospensione del provvedimento n. 112/2023 di limitazione provvisoria del trattamento, consentendo così la ripresa del servizio ChatGPT in territorio italiano.[676]

In ogni caso, l'istruttoria aperta nei confronti di OpenAI è comunque proseguita, giungendo al termine il 2 novembre 2024. In tale data, con provvedimento n. 755, il Garante ha ingiunto alla società il pagamento della somma di 15 milioni di euro a titolo di sanzione amministrativa pecuniaria, in ragione delle violazioni accertate.[677] Non si intende, in questa sede, discutere la proporzionalità della sanzione irrogata, atteso che il GDPR, *ex* art. 83, paragrafo 1, prevede che le sanzioni amministrative siano "in ogni singolo caso effettive, proporzionate e dissuasive".[678] Piuttosto, si vogliono qui avanzare alcune considerazioni conclusive in merito a una contestazione in particolare. Ad avviso del Garante, il fatto che ChatGPT generi *output* inesatti ("non corrispondenti al dato reale") rappresenterebbe una violazione dell'art. 5, par. 1, lett. d) del regolamento, relativo al principio di esattezza dei dati personali. In base a tale principio, i dati personali oggetto

---

[675] OpenAI ha dichiarato di aver adottato tali iniziative nel corso dell'istruttoria. Le misure sono dettagliate in Garante per la protezione dei dati personali, *Provvedimento n. 755*, 2 novembre 2024, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085455.

[676] Garante, *Provvedimento n. 114*, 11 aprile 2023.

[677] Garante, *Provvedimento n. 755*, 2 novembre 2024. Si tratta di tutte violazioni "di natura non continuata" consumate in data anteriore al 15 febbraio 2024. Non potrebbe essere diversamente, dal momento che, come si è detto, a partire da tale data OpenAI dispone di uno stabilimento nel territorio dell'Unione, precisamente in Irlanda. Conseguentemente, in conformità all'art. 56, par. 1, GDPR, la competenza a conoscere delle violazioni successive al 15 febbraio, nonché di quelle anteriori aventi natura continuata o continuativa e quindi persistenti oltre tale data, si radica in capo all'autorità di controllo capofila irlandese. Si segnala, in ogni caso, che le contestazioni accertate nel Provvedimento n. 755 del 2024 riprendono sostanzialmente i rilievi già formulati nel provvedimento d'urgenza del marzo 2023, fatta eccezione per l'ulteriore e autonoma violazione, parimenti contestata, dell'art. 33 GDPR, relativa all'omessa notifica all'autorità garante di un evento di *data breach* occorso il 20 marzo 2023.

[678] Regolamento (UE) 2016/679, art. 83, par. 1.

del trattamento devono essere "esatti e, se necessario, aggiornati"; devono poi essere adottate "tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati". [679] L'Autorità sembra seguire una lettura eccessivamente formalistica di tale principio, che finisce per negare *de facto* la liceità di tutti i sistemi di IA generativa. Tali sistemi, inclusi gli LLM, non nascono, infatti, con la finalità di fornire informazioni fattualmente veritiere. Al contrario, la loro ragion d'essere risiede nella capacità di generare testo coerente rispetto a qualsivoglia *prompt* dell'utente in ingresso, operando attraverso complessi modelli statistici influenzati sia dai *dataset* su cui sono addestrati, sia dall'*input* dell'utente, sia dalle informazioni rinvenute in Rete.[680] L'aspettativa di "esattezza" nell'*output* di un LLM si scontra quindi con la sua stessa natura di modello probabilistico; a differenza di un motore di ricerca tradizionale o di una banca dati, ChatGPT inferisce risposte basandosi su distribuzioni di probabilità apprese durante l'addestramento.[681] La veridicità fattuale delle sue risposte è senz'altro auspicabile, ma non costituisce la finalità del trattamento, né dovrebbe esserci un'aspettativa in tal senso in capo agli utenti, quando adeguatamente informati sul funzionamento del modello e a seguito dell'accettazione dei termini di servizio. Del resto, come evidenziato in dottrina, una lettura eccessivamente rigida del principio di esattezza condurrebbe a ritenere illecita ogni attività di profilazione, in quanto per sua natura basata su modelli statistici e di aggregazione per categorie.[682]

Significativamente, nel provvedimento n. 755 del 2024 il Garante si dice consapevole della complessità della questione dell'accuratezza degli LLM, evidenziando come il tema sia oggetto di intenso dibattito dottrinale e di valutazione a livello europeo, in particolare nell'ambito della *task-force* istituita dall'EDPB. Quest'ultimo sembra seguire un approccio più sfumato, distinguendo anzitutto tra dati in *input* (utilizzati per

---

[679] Regolamento (UE) 2016/679, art. 5, par. 1, lett. d).
[680] Riva, "IA e Internet," 340.
[681] Riva, 340.
[682] Riva, 340-341. Sul punto, l'autore evidenzia come la discussione in merito al principio di esattezza e agli LLM sia riconducibile al più ambito dibattito in merito alla compatibilità della normativa del GDPR e il fenomeno dei *big data*. In tal senso, l'autore rimanda a Alessandro Mantelero, "From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era," in *Group Privacy: New Challenges of Data Technologies*, a cura di Linnet Taylor, Luciano Floridi e Bart van der Sloot (Cham: Springer, 2017), 139–158.

l'addestramento del modello) e dati in *output* (le risposte del modello), e riconoscendo che la finalità del trattamento è piuttosto quella di addestrare il modello alla base di ChatGPT, e non di fornire risposte fattualmente accurate. Nonostante ciò, il *Board* europeo ritiene che la fornitura di informazioni da parte del titolare in merito alla natura probabilistica del sistema e alla possibile inesattezza delle risposte fornite dal *chatbot* non sia di per sé sufficiente ad assicurare il rispetto del principio di esattezza.[683]

Alla luce di questi rilievi, il Garante ritiene la questione giuridica "tutt'altro che risolta", e dal momento che dal punto di vista tecnico il rischio di "allucinazioni" da parte di ChatGPT non può dirsi ancora del tutto scongiurato, la violazione viene qualificata come "continuativa", e dunque ancora in essere alla data 15 febbraio 2024. Per tanto, trovando applicazione a partire da tale data il meccanismo dello sportello unico, il Garante non può far altro che rilevare difetto di competenza e trasmettere gli atti alla DPA irlandese, in qualità di Autorità di controllo capofila.[684] Le future determinazioni dell'Autorità irlandese rivestiranno indubbia importanza per la definizione della complessa questione interpretativa relativa al principio di esattezza e il funzionamento degli LLM; non meno rilevanti, per il quadro regolamentare futuro, si preannunciano eventuali chiarimenti provenienti dall'EDPB, anche in relazione alle possibili intersezioni tra GDPR e AI Act.

3. Il disegno di legge n. 1146: la regolazione dell'IA nel contesto nazionale

Mentre nelle sedi europee proseguiva l'*iter* di definizione dell'AI Act, l'Italia ha intrapreso, con il disegno di legge n. 1146 del 2024 (in seguito: "il DDL"),[685] il primo tentativo in ambito europeo di dotarsi di una normativa nazionale dedicata all'IA. Composto da 26 articoli, il DDL recante "disposizioni e delega al Governo in materia di intelligenza artificiale" si propone di *"*riequilibrare il rapporto tra le opportunità che offrono le nuove tecnologie e i rischi legati al loro uso improprio*"*, introducendo sia

[683] EDPB, *Report of the Work Undertaken by the ChatGPT Taskforce*, 7-8.
[684] Garante, *Provvedimento n.* 755, 2 novembre 2024.
[685] *Disposizioni e delega al Governo in materia di intelligenza artificiale*, Disegno di legge n. 1146 (Senato, 20 maggio 2024).

norme di principio sia disposizioni di settore per promuovere un utilizzo dell'IA antropocentrico e fornire soluzioni per la gestione del rischio.[686] Presentato dal Governo il 20 maggio 2024 e attualmente in corso di esame in commissione presso il Senato, il documento si articola in sei capi: (i) principi e finalità; (ii) disposizioni di settore; (iii) strategia nazionale, autorità nazionali e azioni promozione; (iv) disposizioni a tutela degli utenti e in materia di diritto d'autore; (v) disposizioni penali; (vi) disposizioni finanziarie.

Allo stato attuale, l'*iter* di approvazione del DDL risulta sensibilmente rallentato da un significativo numero di emendamenti e da alcune criticità strutturali. Tra tutte, emerge la questione dei finanziamenti: gli articoli 19, 20 e 21 del disegno di legge prevedono infatti diverse misure di promozione e sostegno finanziario all'IA. L'articolo 21, in particolare, prevede un investimento complessivo pari a un miliardo di euro da destinarsi non solo all'intelligenza artificiale, alla cybersicurezza e al calcolo quantistico (*quantum computing*), ma anche ai settori delle telecomunicazioni e delle tecnologie abilitanti correlate.[687] L'obiettivo è favorire lo sviluppo, la crescita e il consolidamento delle imprese in tale settore aventi sede legale e operativa in Italia.[688] L'erogazione di tali investimenti avverrà principalmente attraverso l'istituzione di uno o più fondi appositamente dedicati ai settori indicati, nonché mediante coinvestimenti di altri fondi gestiti da Cassa Depositi e Prestiti - Venture Capital Sgr.[689] Nonostante l'entità di tali previsioni di spesa, l'articolo 26 del DDL è chiaro nel prevedere che dall'attuazione della legge non dovranno derivare nuovi o maggiori oneri a carico della finanza pubblica.[690] La difficoltà di individuare fonti di finanziamento compatibili con il vincolo posto dall'articolo 26, stando a quanto riferito da fonti parlamentari e giornalistiche, sembra rappresentare al momento una delle principali cause di rallentamento dell'*iter* legislativo.[691]

---

[686] Consiglio dei Ministri, *Comunicato stampa n. 78*, 23 aprile 2024, https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-78/25501.
[687] Disegno di legge n. 1146, art. 21.
[688] Relazione al Disegno di legge n. 1146, 13.
[689] Disegno di legge n. 1146, art. 21, comma 2.
[690] Disegno di legge n. 1146, art. 26.
[691] Fabio Salamida, "Che fine ha fatto il DDL sull'intelligenza artificiale," *Wired*, 16 gennaio 2025, https://www.wired.it/article/ddl-intelligenza-artificiale-che-fine-ha-fatto-news/#:~:text=in%20Senato%2C%20dove%20lo%20avevamo,lontana%20dal%20vedere%20la%20luce.

A causa di tale rallentamento, l'AI Act dell'Unione Europea è entrato in vigore in data anteriore all'approvazione di una legge nazionale sull'intelligenza artificiale. Sebbene inizialmente concepito per anticipare il quadro regolatorio europeo, il DDL qualora approvato, ne sarà di fatto successivo. Ciò nondimeno, tale circostanza potrebbe tradursi in un vantaggio di natura regolatoria: consentire l'integrazione, nel testo di legge, delle previsioni dell'AI Act nella sua versione definitiva, garantendo una maggiore coerenza e sinergia tra i livelli normativi. In tale prospettiva, merita menzione il parere circostanziato reso dalla Commissione Europea nel novembre 2024 sul DDL italiano,[692] in cui si evidenzia il rischio non solo di una potenziale difformità tra la normativa nazionale e quella europea, ma anche di una inammissibile duplicazione di disposizioni europee nel diritto interno, in contrasto con la giurisprudenza consolidata della Corte di Giustizia dell'Unione Europea.[693]

Il disegno di legge sull'intelligenza artificiale resta, in ogni caso, meritevole di analisi, non fosse altro per mettere in luce le principali novità proposte dal Governo, la sua compatibilità con il quadro normativo europeo e l'architettura di *governance* nazionale ivi delineata. Tali profili rappresentano l'oggetto di questo paragrafo.

3.1. Principi, disposizioni di settore e compatibilità con il quadro normativo europeo

L'attenzione alla dimensione etica dell'IA è evidente sin dal Capo I del provvedimento, in cui vengono delineate una serie di norme di principio che "si innestano ... nelle diverse fasi del ciclo di vita dell'intelligenza artificiale, dalla ricerca fino

---

[692] Commissione Europea, *Parere*, C(2024) 7814. Le considerazioni relative al parere C(2024) 7814 della Commissione Europea si basano sull'analisi del resoconto sommario n. 214 della 4a Commissione permanente del Senato della Repubblica (seduta del 27 novembre 2024), in assenza di fonti ufficiali pubblicamente accessibili del testo integrale del parere. Senato della Repubblica, *4a Commissione permanente – Resoconto sommario n. 214*, 27 novembre 2024, https://www.senato.it/japp/bgt/showdoc/19/SommComm/0/1435866/index.html?part=doc_dc-allegato_a:1

[693] La Commissione fa riferimento alla giurisprudenza della Corte di giustizia secondo cui è vietato agli Stati membri duplicare le disposizioni di un regolamento europeo nel diritto nazionale e quindi nascondere la loro origine nel diritto dell'Unione. *Si veda* Corte di Giustizia dell'Unione Europea, causa 34/73, *Fratelli Variola S.p.A. contro Amministrazione italiana delle Finanze*, ECLI:EU:C:1973:101. Corte di Giustizia dell'Unione Europea, causa 50/76, *Amsterdam Bulb BV contro Produktschap voor Siergewassen*, ECLI:EU:C:1977:13.

all'adozione e al concreto utilizzo dei sistemi e dei modelli" di IA.[694] L'obiettivo dichiarato è quello di porre al centro di ogni attività legata all'IA l'autodeterminazione umana,[695] nonché accompagnare e integrare il quadro europeo senza sovrapporsi ad esso, intervenendo negli spazi riservati al diritto interno e preparando il terreno all'applicazione dell'AI Act.[696] A tal fine, l'art. 1, comma 2 prevede che le disposizioni del disegno di legge "si applicano conformemente al diritto dell'Unione Europea", in ossequio all'art. 117, comma 1 della Carta costituzionale.[697] All'art. 3 del DDL sono quindi declinati i "Principi generali" che costituiscono il fulcro concettuale dell'intera normativa. Si tratta, per lo più, di principi mutuati dalle elaborazioni dell'AI HLEG, e che nel testo di legge diventano strumento per il perseguimento di tre interessi: il trattamento algoritmico equo e corretto, la protezione dei dati e la sostenibilità digitale.[698]

L'interesse al trattamento algoritmico equo e corretto si realizza mediante la previsione che tutte le attività legate all'IA siano svolte nel rispetto dei diritti fondamentali della persona, nonché in ossequio ai principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.[699] Come si evince dalla relazione di accompagnamento, il disegno di legge pone particolare enfasi sul principio di non discriminazione, vietando qualsiasi forma di discriminazione basata su sesso, età, origine etnica, credo religioso, orientamento sessuale, opinioni politiche, condizioni personali, sociali ed economiche.[700] Legato al tema della non discriminazione, vi è il principio del pieno accesso delle persone con disabilità ai sistemi di IA, *ex* art. 3, comma 6 del DDL in esame.[701] Ulteriore interesse perseguito, si è detto, è la protezione dei dati, assicurata attraverso la previsione del principio generale in base al quale lo sviluppo dei sistemi e modelli di IA deve avvenire nel rispetto del principio di proporzionalità, garantendo correttezza, attendibilità, sicurezza, qualità, appropriatezza e trasparenza del dato,[702] nonché assicurando la

---

[694] Relazione al Disegno di legge n. 1146, 4.
[695] Relazione al Disegno di legge n. 1146, 4.
[696] Consiglio dei Ministri, *Comunicato stampa n. 78*.
[697] Disegno di legge n. 1146, art. 1.
[698] Relazione al Disegno di legge n. 1146, 5-6.
[699] Disegno di legge n. 1146, art. 1, comma 1.
[700] Relazione al Disegno di legge n. 1146, 6.
[701] Disegno di legge n. 1146, art. 3, comma 6.
[702] Disegno di legge n. 1146, art. 3, comma 2.

cybersicurezza dei sistemi durante tutto il loro ciclo di vita.[703] Infine, l'interesse alla sostenibilità digitale è perseguito stabilendo che lo sviluppo e l'applicazione dell'IA debbano avvenire nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità e della spiegabilità.[704] In linea con quanto previsto all'art. 46 della Costituzione, l'utilizzo dell'IA non deve pregiudicare "lo svolgimento con metodo democratico della vita istituzionale e politica" del Paese.[705]

I successivi articoli 4 e 5 del disegno di legge specificano ulteriormente i principi di cui all'articolo 3. In materia di informazione, è previsto che l'impiego di sistemi di IA nel settore debba avvenire senza pregiudicare i principi di libertà e pluralismo, la libertà di espressione e il diritto all'obiettività, completezza, imparzialità e lealtà dell'informazione.[706] Quanto al trattamento dei dati personali, l'articolo 4 ribadisce che, in conformità con quanto previsto dal diritto dell'Unione Europea, l'uso di sistemi di IA dovrà garantire che il trattamento sia lecito, corretto, trasparente e compatibile con le finalità per le quali i dati sono stati raccolti; le informative sul trattamento indirizzate all'interessato, poi, dovranno adottare un linguaggio chiaro e semplice.[707] I soggetti di età superiore ai quattordici anni e inferiore ai diciotto possono esprimere il loro consenso al trattamento se adeguatamente informati, mentre per i minori di quattordici anni il requisito del consenso genitoriale sembrerebbe operare non solo per il trattamento dei dati, bensì in generale per "l'accesso alle tecnologie di intelligenza artificiale".[708] Sul punto, si vuole avanzare un rilievo critico: sebbene l'articolo 2 del DDL fornisca una definizione di "sistemi di intelligenza artificiale", non è definito il concetto, ben più generico e lato, di "tecnologie di IA", locuzione di per sé assai ambigua e indefinita, specialmente alla luce delle difficoltà definitorie intrinseche alla nozione stessa di IA, come discusso nel primo capitolo di questa trattazione.[709] Ne deriva una non trascurabile ambiguità circa l'effettiva portata applicativa della disposizione in esame.

---

[703] Disegno di legge n. 1146, art. 3, comma 5.
[704] Disegno di legge n. 1146, art. 3, comma 3.
[705] Disegno di legge n. 1146, art. 3, comma 4.
[706] Disegno di legge n. 1146, art. 4, comma 1.
[707] Disegno di legge n. 1146, art. 4, commi 2 e 3.
[708] Disegno di legge n. 1146, art. 4, comma 4.
[709] *Vedi* capitolo I, paragrafo 2.

Quanto all'articolo 5 del DDL, rubricato "Principi in materia di sviluppo economico", è attribuito allo Stato un ruolo attivo nella promozione dell'utilizzo dell'IA in tutti i settori produttivi, nel favorire la "creazione di un mercato dell'intelligenza artificiale innovativo, equo, aperto e concorrenziale", nel facilitare l'accesso a dati di alta qualità e nell'orientare le procedure di *e-procurement* della pubblica amministrazione verso soluzioni di intelligenza artificiale che assicurino la localizzazione dei "dati critici" sul territorio nazionale ed elevati *standard* di trasparenza.[710]

In linea con quanto previsto dall'AI Act all'art. 2, par. 3, sono escluse dall'ambito di applicazione del provvedimento le attività svolte per scopi di sicurezza nazionale, per la cybersicurezza nazionale nonché quelle svolte per scopi di difesa dalle forze armate e dalle forze di polizia.[711]

Nonostante la dichiarata intenzione del Governo italiano di integrare e accompagnare il quadro normativo europeo sull'IA, evitando sovrapposizioni, la Commissione Europea, avvalendosi degli strumenti di *moral suasion* previsti dalla direttiva (UE) 2015/1535, ha evidenziato attraverso il parere C(2024) 7814 una serie di criticità del disegno di legge italiano. Se è vero che i principi etici enunciati nel Capo I del DDL – *e.g.* trasparenza, non discriminazione, rispetto dei diritti fondamentali e controllo umano – sono per lo più convergenti con i pricipi dell'AI Act e con gli Orientamenti Etici dell'AI HLEG, e che l'enfasi italiana sull'approccio antropocentrico si allinea con il modello europeo di promozione di un'"IA affidabile", emerge tuttavia una serie di difformità. Manca, anzitutto, uno specifico riferimento all'AI Act all'articolo 1 del DDL.[712] In secondo luogo, le definizioni dei due testi non sembrano del tutto coincidenti: sebbene l'articolo 2 mutui la definizione di "sistemi di IA" direttamente dal regolamento europeo, analogo allineamento non si verifica per i "modelli di IA", definiti nel DDL come "modelli che identificano strutture ricorrenti attraverso l'uso di collezioni di dati, che hanno la capacità di svolgere un'ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni".[713] Pur presentando alcune affinità, la nozione non coincide con la più precisa e circoscritta definizione

[710] Disegno di legge n. 1146, art. 5.
[711] Disegno di legge n. 1146, art. 6.
[712] Senato, *Resoconto sommario n. 214*.
[713] Senato, *Resoconto sommario n. 214*. Disegno di legge n. 1146, art. 2, comma 1, lett. c).

europea di "modelli di IA per finalità generali".[714] Analogamente, appare poco chiara e foriera di dubbi l'espressione "dati critici" di cui all'articolo 5, concetto che andrebbe meglio definito e limitato ai casi relativi alla sicurezza nazionale.[715]

Si è detto di come il disegno di legge dedichi il Capo II alla previsione di diverse disposizioni di settore. Particolare attenzione è dedicata al settore sanitario. In ossequio al principio di non discriminazione, è fatto divieto di introdurre sistemi di IA che possano determinare discriminazioni nell'accesso alle prestazioni sanitarie.[716] È poi sancito il diritto del paziente a essere informato qualora "tecnologie di IA" siano impiegate nei processi diagnostici o terapeutici, nonché sui vantaggi apportati dall'utilizzo di tali tecnologie e sulla loro logica decisionale.[717] In ogni caso, il ruolo dell'intelligenza artificiale nel settore sanitario dovrà configurarsi in termini di supporto, e non dovrà mai pregiudicare la decisione del medico nei processi di prevenzione, diagnosi, cura e scelta terapeutica.[718] Di primo interesse anche quanto previsto all'art. 8 del DDL in merito ai trattamenti di dati, inclusi i dati personali e i c.d. dati sensibili, eseguiti da "soggetti pubblici e privati senza scopo di lucro per la ricerca e la sperimentazione scientifica" ai fini di realizzare sistemi di IA in ambito sanitario. Tali trattamenti sono espressamente dichiarati come "di rilevante interesse pubblico", e ne viene dunque *ex lege* autorizzato l'uso secondario per tali finalità; non sarà pertanto necessario replicare il consenso dell'interessato per il trattamento ulteriore.[719] La norma, tuttavia, subordina tale autorizzazione al rispetto di due obblighi: l'obbligo di fornire un'informativa agli interessati, che può essere adempiuto anche mediante la pubblicazione di un'informativa di carattere generale sul sito web del titolare del trattamento; l'obbligo di comunicazione del trattamento al Garante. Si prevede qui l'introduzione di un meccanismo di silenzio-

---

[714] Regolamento (UE) 2024/1689, art. 3, par. 1, n. 63: "un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato"

[715] Disegno di legge n. 1146, art. 5, comma 1, lett. d).

[716] Disegno di legge n. 1146, art. 7, comma 2.

[717] Disegno di legge n. 1146, art. 7, comma 3.

[718] Disegno di legge n. 1146, art. 7, comma 5.

[719] Disegno di legge n. 1146, art. 8, comma 1.

assenso: in assenza di un provvedimento inibitorio da parte del Garante nel termine dei trenta giorni successivi alla comunicazione, le attività di trattamento potranno essere legittimamente avviate.[720]

L'approccio antropocentrico è evidente anche nelle disposizioni dedicate all'utilizzo di sistemi di IA nel contesto lavorativo. In base all'art. 10 del DLL, l'intelligenza artificiale è impiegata al fine di migliorare le condizioni di lavoro, tutelare l'integrità psico-fisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività.[721] È imposto in capo al datore di lavoro o al committente l'obbligo di informare i lavoratori circa l'utilizzo dell'IA, secondo le modalità indicate all'art. 1-bis del d.lgs. 152/1997.[722] Qualora siano impiegati sistemi di IA per l'organizzazione o la gestione del rapporto di lavoro, ciò dovrà avvenire nel rispetto dei principi di equità e non discriminazione.[723] Di particolare rilievo, poi, quanto previsto all'articolo 12: il governo ritiene sia necessario preservare le professioni intellettuali da un impiego dell'IA che ne snaturi la funzione intrinseca, consistente nella messa a disposizione di competenze e risorse intellettuali personali all'interno di un rapporto fiduciario con il cliente.[724] Si stabilisce, pertanto, che nelle professioni intellettuali il "pensiero critico umano" debba sempre risultare prevalente rispetto all'uso di strumenti di IA,[725] consentiti unicamente per attività strumentali e di supporto all'attività professionale.[726] Al fine di garantire il rapporto fiduciario tra professionista e cliente, è sancito l'obbligo di comunicare al cliente, con linguaggio chiaro, semplice ed esaustivo, le informazioni relative ai sistemi di intelligenza artificiale eventualmente impiegati.[727]

---

[720] Disegno di legge n. 1146, art. 8, commi 2 e 3.
[721] Disegno di legge n. 1146, art. 10, comma 1.
[722] Disegno di legge n. 1146, art. 10, comma 2. D.lgs. n. 152/1997, *Attuazione della direttiva 91/533/CEE*, art. 1-bis: "1. Il datore di lavoro o il committente pubblico e privato è tenuto a informare il lavoratore dell'utilizzo di sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori".
[723] Disegno di legge n. 1146, art. 10, comma 3.
[724] Relazione al Disegno di legge n. 1146, 9.
[725] Relazione al Disegno di legge n. 1146, 9.
[726] Disegno di legge n. 1146, art. 12, comma 1.
[727] Disegno di legge n. 1146, art. 12, comma 2.

Quanto alla pubblica amministrazione, il DDL promuove l'utilizzo dell'IA, considerato la "leva" per rendere effettivi i principi di imparzialità, buon andamento ed efficienza di cui all'art. 97 della Costituzione.[728] Tale promozione si accompagna però all'affermazione della centralità dei principi di autodeterminazione e responsabilità umana. L'utilizzo dell'IA, dunque, è contemplato in funzione strumentale e di supporto all'attività provvedimentale, ma la persona resta l'unica responsabile dei procedimenti e dei provvedimenti.[729] Ancora più restrittivi, invece, appaiono i limiti previsti per l'impiego di sistemi di IA nell'amministrazione della giustizia: questo è consentito esclusivamente per l'organizzazione e la semplificazione del lavoro giudiziario, nonché per la ricerca giurisprudenziale e dottrinale.[730] È espressamente previsto che ogni potere decisionale – le decisioni sull'interpretazione della legge, la valutazione dei fatti e delle prove, l'adozione di ogni provvedimento – rimanga integralmente riservato al magistrato.[731]

In seguito a questa breve rassegna sulle principali disposizioni settoriali proposte dal disegno di legge, è possibile avanzare alcuni rilievi in merito alla loro compatibilità con quanto previsto dal quadro normativo europeo, anche in considerazione dell'entrata in vigore all'AI Act.

Partendo dalla fine, non può far a meno di notarsi come alcune disposizioni appaiano eccessivamente restrittive rispetto a quanto previsto dall'AI Act. Si consideri l'art. 14 del DDL. La Commissione Europea ha invitato ad allinearlo al Regolamento europeo,[732] il quale prevede non siano considerati "ad alto rischio" i sistemi di IA che non presentano, in concreto, un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, "anche nel senso di non influenzare materialmente il risultato del processo decisionale".[733] Adottando una visione d'insieme, però, si vuole qui avanzare un'ulteriore considerazione: il DDL italiano sembra escludere qualsiasi utilizzo di sistemi di IA nell'attività giudiziaria che vada oltre le attività di organizzazione e semplificazione del lavoro, ricerca giurisprudenziale e dottrinale. È

[728] Relazione al Disegno di legge n. 1146, 9.
[729] Disegno di legge n. 1146, art. 13, comma 2.
[730] Disegno di legge n. 1146, art. 14, comma 1.
[731] Disegno di legge n. 1146, art. 14, comma 2.
[732] Senato, *Resoconto sommario n. 214*.
[733] Regolamento (UE) 2024/1689, art. 6, par. 3.

senz'altro vero che l'AI Act include, nell'elenco dei sistemi ad alto rischio di cui all'Allegato III, i sistemi di IA destinati a "essere usati da un'autorità giudiziaria ... nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge ...",[734] ma ciò non significa che tali sistemi siano proibiti. Il Regolamento non osta affatto a un loro utilizzo più ampio – inclusa l'assistenza nell'interpretazione di fatti e norme –, purché nel rispetto degli obblighi prescritti per i sistemi ad alto rischio.

Un orientamento eccessivamente restrittivo, da parte del Governo italiano, si riscontra anche in relazione a quanto previsto all'art. 12 del DDL, concernente l'impiego dell'IA nelle professioni intellettuali. La Commissione Europea, infatti, ha invitato il legislatore a eliminare dal testo qualsiasi restrizione nell'uso di sistemi di IA non ad alto rischio.[735] Si permetta, anche in questo caso, di evidenziare un'ulteriore criticità, e cioè l'ambiguità insita nella formulazione letterale dell'art. 12, laddove richiede che il lavoro intellettuale sia "prevalente".[736] La disposizione rischia di essere foriera di incertezze interpretative e appare difficile, se non impossibile, accertare in concreto la prevalenza del lavoro intellettuale rispetto all'uso di sistemi di IA, considerando che questi ultimi operano comunque sulla base delle direttive e degli *input* del professionista. In alternativa, per garantire maggiore coerenza con l'AI Act, potrebbe essere preferibile introdurre anche in questo contesto un obbligo di sorveglianza umana e riaffermare il principio di autonomia decisionale.

Quanto al settore sanitario, la Commissione ha espresso perplessità in merito all'ampiezza degli obblighi informativi verso i pazienti previsti dal DDL a carico degli operatori di sistemi di IA, suggerendo di circoscriverli al solo impiego dell'IA, senza estenderli anche "ai vantaggi diagnostici e terapeutici" o alla "logica decisionale utilizzata" dal sistema.[737] A tal proposito, è meritevole di menzione anche il parere reso dal Garante sul disegno di legge.[738] Pur esprimendo parere favorevole al DDL, l'Autorità

---

[734] Regolamento (UE) 2024/1689, Allegato III, punto 8, lett. a).

[735] Senato, *Resoconto sommario n. 214*.

[736] Disegno di legge n. 1146, art. 12, comma 1: "L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è consentito esclusivamente per esercitare attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera".

[737] Senato, *Resoconto sommario n. 214*.

[738] Garante per la protezione dei dati personali, *Provvedimento n. 477*, 2 agosto 2024, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10043532

ha infatti proposto diversi correttivi, volti ad assicurare la piena conformità del provvedimento al GDPR e ai requisiti dell'AI Act. Tra i rilievi principali si segnala: la richiesta di inserire, nel Capo I del DDL, una clausola generale di conformità al GDPR; la necessità di rimodulare gli articoli 7-9 allineandoli ai requisiti previsti dall'art. 10 dell'AI Act, in materia di dati e *data governance* per i sistemi di IA ad alto rischio; la richiesta di adeguare la disciplina prevista per il settore sanitario ai principi di determinatezza di cui agli articoli 6 e 9 del GDPR e alle garanzie previste dall'articolo 89 del medesimo regolamento. Con riguardo all'uso secondario dei dati, il Garante ha richiesto la soppressione della previsione relativa all'informativa generica pubblicata sul sito *web* del titolare del trattamento (art. 8 del DDL), ritenendola incompatibile con i principi del GDPR. Infine, in merito al meccanismo di silenzio-assenso di cui all'art. 8, il Garante ha chiarito che il decorso del termine non impedisce l'esercizio futuro dei poteri di controllo dell'Autorità.[739]

Nel concludere questo paragrafo, vuole farsi un breve cenno a un ulteriore rilievo mosso dalla Commissione Europea nel suo parere circostanziato. Il Capo IV del DDL introduce, nell'ambito del "Testo unico per la fornitura di servizi di media audiovisivi",[740] una serie di misure volte a favorire l'identificazione e il riconoscimento dei sistemi di intelligenza artificiale nella creazione di contenuti testuali, fotografici, audiovisivi e radiofonici da parte dei fornitori dei relativi servizi. L'art. 23, comma 1, lett. b) del DDL prevede infatti un obbligo di etichettatura per i contenuti generati dai sistemi di IA, da adempiere mediante apposizione del segno grafico "IA" o con un annuncio audio. Obbligo, secondo la Commissione, più stringente rispetto a quanto prescritto dall'AI Act, il quale, salvo il caso specifico dei *deepfake*, si limita a prevedere la marcatura dei contenuti in un formato "leggibile meccanicamente".[741] Similmente, sembra sovrapporsi agli obblighi di cui all'art. 50 dell'AI Act anche quanto previsto dall'art. 23, comma 1, lett. c) del DDL.[742]

---

[739] I rilievi di cui si è fatta menzione sono contenuti in Garante, *Provvedimento n. 477*.

[740] D.lgs. n. 208/2021, *Testo unico per la fornitura di servizi di media audiovisivi*.

[741] Regolamento (UE) 2024/1689, art. 50, par. 2.

[742] In riferimento all'articolo 23, comma 1, lettera c), del disegno di legge, che impone ai fornitori di piattaforme di *video sharing* soggetti alla giurisdizione italiana di attuare misure a tutela del ″grande pubblico da contenuti informativi che siano stati, attraverso l'utilizzo di sistemi di intelligenza artificiale, completamente generati ovvero, anche parzialmente, modificati o alterati in modo da presentare come reali

3.2. Le autorità nazionali per l'intelligenza artificiale

Il modello di *governance* delineato dal DDL contempla anzitutto un ruolo centrale della Presidenza del Consiglio nella definizione della "Strategia nazionale per l'intelligenza artificiale". Questa è "predisposta e aggiornata dalla struttura della Presidenza del Consiglio dei ministri competente in materia di innovazione tecnologica e transizione digitale, d'intesa con le Autorità nazionali per l'intelligenza artificiale di cui all'art. 18, sentito il Ministro delle imprese e del *made in Italy* per i profili di politica industriale e di incentivazione e il Ministro della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale, ed è approvata con cadenza almeno biennale dal Comitato interministeriale per la transizione digitale".[743] Una simile previsione sembra comunicare la volontà del Governo di trattare l'IA come un tema trasversale, coordinando l'azione e le conoscenze dei diversi dicasteri.

Si è detto di come l'art. 70 dell'AI Act preveda l'obbligo, per gli Stati membri, d'istituire almeno un'autorità di notifica e almeno un'autorità di vigilanza sul mercato.[744] In risposta a tale previsione, il DDL delinea un sistema di *governance* "a trazione duale",[745] individuando nell'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN) le "Autorità nazionali per l'intelligenza artificiale".[746] Più precisamente, ferme restando le funzioni già attribuite, AgID è l'autorità che provvede a "definire le procedure e ad esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale",[747] mentre ACN è l'autorità "responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi

---

dati, fatti e informazioni che non lo sono", la Commissione europea non ritiene chiaro in che modo tale disposizione non si sovrapponga all'articolo 50, comma 1, 2 e 4, dell'AI Act. Così Senato, *Resoconto sommario n. 214*.

[743] Disegno di legge n. 1146, art. 17, comma 1.

[744] *Vedi* capitolo IV, paragrafo 1.

[745] Marco Cappai, "Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?," *Federalismi*, n. 30 (dicembre 2024): 199. L'autore rinvia a Alessandro Pajno, "La governance dell'intelligenza artificiale tra regolamento europeo e disciplina nazionale," *Astrid Rassegna*, n. 13 (settembre 2024).

[746] Disegno di legge n. 1146, art. 18, comma 1.

[747] Disegno di legge n. 1146, art. 18, comma 1, lett. a).

di intelligenza artificiale".[748] Presso la Presidenza del Consiglio è poi istituito un Comitato di coordinamento, composto dai direttori generali delle due Agenzie e dal Capo del Dipartimento per la trasformazione digitale della stessa Presidenza, ai fini di promuovere il raccordo tra le autorità nell'esercizio delle loro funzioni.[749]

Come è evidente, le "autorità designate" nel DDL non sono autorità indipendenti, bensì agenzie governative. La legittimità di tale scelta è stata – ed è tutt'oggi – oggetto di intenso dibattito dottrinale: l'AI Act prevede infatti che l'attività delle autorità di notifica e vigilanza sia non solo imparziale (in linea, per altro, con quanto previsto per l'operato della pubblica amministrazione *ex*. art. 97 della Costituzione italiana) ma anche indipendente.[750] Indipendenza che non riguarda solo la nomina dei componenti, ma che si estende alla dimensione finanziaria, strumentale, infrastrutturale e, soprattutto, funzionale, delle autorità.[751] Non sorprende, dunque, che la Commissione Europea abbia ritenuto necessario ribadire che tali autorità "devono possedere lo stesso livello di indipendenza previsto dalla direttiva (UE) 2016/680 per le autorità preposte alla protezione dei dati nelle attività delle forze dell'ordine, nella gestione delle migrazioni e controllo delle frontiere, nell'amministrazione della giustizia e nei processi democratici".[752]

Parte della letteratura, di converso, ritiene che la scelta del Governo italiano sia coerente con l'impostazione seguita dal legislatore europeo. Del resto si è visto come, ai fini del coordinamento a livello unionale, l'AI Act non abbia optato per l'istituzione di un'agenzia europea, quanto piuttosto di un Ufficio interno alla Commissione.[753] L'architettura di *governance* nazionale, dunque, si farebbe specchio di quella europea: il controllo esercitato dall'Ufficio per l'IA (a livello europeo) e dalle autorità (a livello nazionale) è senz'altro tecnico, ma le scelte della Commissione (a livello europeo) e della Presidenza del consiglio (attraverso la "Strategia nazionale" per l'IA, di cui al Capo III

[748] Disegno di legge n. 1146, art. 18, comma 1, lett. b).
[749] Disegno di legge n. 1146, art. 18, comma 2.
[750] Maddalena Rabitti e Fabio Bassan, "L'applicazione dell'AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti," *Federalismi*, n. 30 (dicembre 2024): 253.
[751] Regolamento (UE) 2024/1689, art. 70, par. 3.
[752] Senato, *Resoconto sommario n. 214*.
[753] Regolamento (UE) 2024/1689, art. 64.

del DDL) sono e restano di natura politica.[754] Adottando una prospettiva di diritto comparato, poi, l'attribuzione delle funzioni di notifica e vigilanza ad agenzie governative non sembra costituire un'anomalia nel panorama europeo.[755]

Il punto critico della questione, dunque, sembra essere piuttosto un altro. Se si condivide la prospettiva secondo cui la *governance* dell'IA, intesa in senso lato – ossia con riferimento al fenomeno nel suo complesso, e non limitatamente al perimetro del DDL –, coinvolge molteplici attori,[756] diviene allora dirimente indagare i meccanismi di raccordo e coordinamento tra le autorità designate dal DDL e le autorità indipendenti di settore già esistenti.

Le autorità di vigilanza e regolazione dei mercati, del resto, hanno maturato competenze specialistiche nei mercati di riferimento e si confrontano già da tempo con questioni concernenti l'utilizzo di sistemi di IA.[757] La materia dell'intelligenza artificiale costituisce infatti un tema regolatorio trasversale. In ragione di ciò, il modello di *governance* delineato dal DDL, similmente a quanto accaduto per la tutela della concorrenza e la protezione dei dati personali, è di tipo "orizzontale", dal momento che l'IA è suscettibile di applicazione in diversi mercati "verticali".[758]

Ciascuna autorità indipendente conserva senz'altro una vocazione elettiva a intervenire sul mercato di propria competenza, data la pregressa conoscenza delle dinamiche settoriali e degli operatori; è però soltanto l'ACN l'autorità responsabile di vigilare "orizzontalmente" su tutti i sistemi di IA, fungendo da punto di raccordo. In tale prospettiva, è imprescindibile che questa assicuri il coordinamento e la collaborazione con le altre pubbliche amministrazioni e autorità indipendenti.[759] Nonostante ciò, fatta eccezione per quanto previsto all'art. 18, comma 2, mancano nel DDL disposizioni in merito ai termini e alle modalità con cui verrebbe a realizzarsi una simile collaborazione.

---

[754] Rabitti e Bassan, "L'applicazione dell'AI Act in Italia," 253.
[755] Cappai, "Intelligenza artificiale e protezione dei dati personali," 201-203.
[756] Cappai, 200. L'autore parla a tal proposito di una *governance* "a geometria variabile".
[757] Per alcuni esempi di come le autorità indipendenti di settore stiano già sviluppando importanti competenze in merito all'intelligenza artificiale, il rinvio è sempre a Rabitti e Bassan, "L'applicazione dell'AI Act in Italia," 259-262.
[758] Rabitti e Bassan, 256.
[759] Disegno di legge n. 1146, art. 18, comma 2.

Un rilievo conclusivo appare necessario proprio in merito a quanto previsto dall'art. 18, comma 2. Come acutamente osservato in dottrina, nell'incardinare il Comitato di coordinamento presso la Presidenza del Consiglio, la disposizione in esame sembra essere il risultato di una trasposizione decontestualizzata dell'art. 65 dell'AI Act, che istituisce il Consiglio europeo per l'intelligenza artificiale.[760] Quest'ultimo, si è detto, si compone di rappresentanti degli Stati membri, solitamente di nomina ministeriale. Sul piano del diritto interno, tuttavia, il coordinamento "politico" appare già sufficientemente garantito dal procedimento di approvazione della Strategia nazionale, e non si ravvisa la necessità di prevedere un ulteriore controllo governativo, per lo più in sede di coordinamento tra autorità designate e autorità indipendenti di settore.[761]

Se già in dottrina sussistono fondati dubbi in ordine alla sussistenza dei requisiti di indipendenza di AgID e ACN – entrambe, peraltro, non certo annoverabili tra le autorità indipendenti –, l'introduzione di un ulteriore livello di controllo governativo, lungi dal dissipare tali perplessità, non può che acuire tali riserve, sollevando importanti interrogativi sulla compatibilità del modello di *governance* del DDL con il quadro normativo europeo.

[760] Cappai, "Intelligenza artificiale e protezione dei dati personali," 205.
[761] Cappai, 205.

CONCLUSIONI

Nel corso di questo lavoro si è tentato di indagare le principali sfide che si trova ad affrontare chi si pone l'obiettivo di regolare l'intelligenza artificiale, evidenziando alcune criticità dei modelli seguiti sin ora dal legislatore nazionale ed europeo.

Pur rappresentando un primo, coraggioso tentativo di regolare la materia, il Regolamento europeo sull'intelligenza artificiale presenta ancora zone d'ombra e importanti margini di incertezza applicativa. La definizione di "sistema di IA" fornita dal regolamento, si è detto, è volutamente ampia e flessibile, ma potrebbe essere foriera di dubbi nel suo momento applicativo. Permangono, invero, significative incertezze interpretative in ordine alle pratiche di IA vietate, aspetto di indubbia rilevanza, dal momento che il divieto di immissione sul mercato, messa in servizio e uso di sistemi di IA che incorporano pratiche vietate non conosce deroghe. Sebbene sia prevista una valutazione annuale da parte della Commissione, con la facoltà di adottare atti delegati volti a modificare l'elenco di pratiche di cui all'art. 5 dell'AI Act,[762] tale meccanismo potrebbe rivelarsi insufficiente a garantire una veloce evoluzione della disciplina.

Si è discusso, poi, di come il Regolamento lasci agli Stati membri un ampio margine di discrezionalità nell'implementazione di aspetti di cruciale importanza, non solo con riferimento alle pratiche di IA vietate ma anche, e soprattutto, nella definizione dell'architettura nazionale di *governance*. Diversi approcci nazionali potrebbero tradursi in livelli di tutela disomogenei nel territorio dell'Unione; dal momento che la materia incide direttamente sui diritti fondamentali, una simile scelta appare problematica.

Per ultimo, permangono dubbi sull'interazione tra l'AI Act e la disciplina del GDPR. Nonostante la clausola di salvaguardia *ex*. art. 2, par. 7 del Regolamento, che dichiara salvo l'*acquis* comunitario in materia di protezione dei dati, il potenziale conflitto tra le disciplina di *data governance* per i sistemi di IA ad alto rischio e i principi del GDPR sembra non essere del tutto risolto.

Più in generale, come si evince anche dai provvedimenti del Garante italiano su ChatGPT, permangoo rilevanti incertezze riguardo l'individuazione di una base giuridica che possa legittimare il trattamento di dati personali necessario all'addestramenti dei

[762] Regolamento (UE) 2024/1689, art. 112.

sistemi AI. Sebbene l'argomento esuli dall'ambito di questa trattazione, inizia a porsi in dottrina il dubbio che, in ultima analisi, a necessitare di una revisione normativa non sia proprio il GDPR, la cui previsioni appaiono sempre più difficilmente conciliabili con la logica dei *Big Data*. Si è visto, del resto, come il caso ChatGPT abbia palesato che un'interpretazione eccessivamente formalistica del principio di esattezza del dato sancito dal GDPR rischia di collidere con la natura probabilistica dei sistemi di IA generativa.

L'analisi dei provvedimenti adottati dal Garante italiano nei casi ChatGPT e DeepSeek ben evidenzia il complesso equilibrio tra la protezione dei dati personali e la promozione dell'innovazione tecnologica. Il raffronto con l'intervento dell'Autorità nei confronti di DeepSeek solleva però alcuni dubbi sulla coerenza complessiva delle scelte del Garante, nonché sulla discrezionalità di cui gode l'Autorità nell'adozione delle misure correttive previste dal GDPR. Il caso ChatGPT ha senz'altro posto il Garante italiano al centro del dibattito europeo, stimolando interventi coordinati in materia. La mancanza di un'azione coordinata con le altre DPA europee e la successiva istituzione di una *task-force* dell'EDPB su ChatGPT, tuttavia, tradiscono un sistema di *governance* ancora frammentato e per lo più reattivo. Al di là delle questioni inerenti la proporzionalità e la legittimità dei provvedimenti, emerge una più ampia criticità di sistema: l'efficacia di una regolazione perseguita, per lo più, attraverso interventi *ex post*, appare senz'altro dubbia se confrontata con la rapidità con cui nuovi attori e servizi si affacciano sul mercato dell'intelligenza artificiale.

Restando sul piano nazionale, si è visto come il disegno di legge n. 1146 abbia rappresentato il primo tentativo di uno Stato membro di dotarsi di una disciplina nazionale dell'IA. Se da un lato la dichiarata volontà di integrare e accompagnare il Regolamento europeo appare condivisibile, dall'altro, il rischio di difformità tra la normativa nazionale e quella europea, nonché di una inammissibile duplicazione di disposizioni europee nel diritto interno, rischia di minare la coerenza del quadro regolatorio complessivo. Analogamente, si è detto come la struttura di *governance* delineata nel DDL, designando quali autorità competenti ai fini dell'AI Act agenzie governative in luogo di autorità indipendenti, ha portato la dottrina ha sollevare numerose riserve in merito alla conformità del provvedimento con quanto previsto dal quadro normativo europeo.

Una considerazione conclusiva si rende doverosa con riguardo ai rischi di *over-regulation* e alle possibili ricadute negative sullo sviluppo del settore dell'intelligenza

artificiale. L'Unione Europea ha messo in campo, in pochi anni, un'imponente produzione normativa sul digitale. Questa strategia regolatoria è motivata anche dalla presa d'atto del ritardo competitivo accumulato dall'economia europea nello sviluppo di nuove tecnologie e dall'obiettivo politico di garantire una sovranità digitale europea. Un eccesso di regolazione, tuttavia, potrebbe soffocare l'innovazione e frenare la crescita di un'industria dell'IA europea ancora nascente.

Il bilanciamento tra tutela dei diritti fondamentali ed esigenze del mercato si conferma delicatissimo: un quadro regolatorio inefficiente rischia di tradursi non solo in un freno allo sviluppo economico, ma anche di non garantire l'effettiva tutela dei diritti della persona, non raggiungendo né l'uno, né l'altro obiettivo regolatorio. Evitare gli eccessi opposti appare dunque la principale sfida della regolazione dell'IA. Da un lato, non appare percorribile (né auspicabile) la strada di una *deregulation* totale – o di una mera autoregolazione– che rimetta interamente ai privati la tutela di valori fondamentali come la dignità umana, la non discriminazione, la tutela dei dati personali. Le derive di un approccio *laissez-faire* sono state scongiurate anche dal vivace dibattito etico degli ultimi anni: al crescere della consapevolezza sui rischi dell'IA, si è affermata l'aspettativa sociale di un intervento regolatorio a garanzia di un'IA "affidabile" e antropocentrica. Allo stesso tempo, occorre guardarsi dalla tendenza opposta: le esperienze pregresse insegnano che il proliferare di dichiarazioni di principio e linee guida dal linguaggio vago finisce per compromettere l'effettività della regolazione.

Si profilano dunque alcune direttrici per il futuro: norme chiare nelle definizioni e negli obiettivi, flessibili nell'adeguarsi al progresso tecnologico; un quadro di *governance* che assicuri un coordinamento sovranazionale forte ma che garantisca uniformità applicativa; il coinvolgimento informato degli *stakeholder* (industria, accademia, società civile) nella definizione di *standard* tecnici e *best practice*; meccanismi di regolazione agile (*adaptive regulation*), capaci di essere aggiornati man mano che la tecnologia evolve.

Governare l'Intelligenza Artificiale senza soffocarne lo sviluppo: l'obiettivo dovrà essere quello di incanalare l'innovazione tecnologica affinché sia al servizio dell'uomo, garantendo nel contempo che l'IA si sviluppi in modo sicuro, etico e conforme ai valori costituzionali ed europei.

Bibliografia

Fonti normative, rapporti di enti e documenti delle Istituzioni

Commissione Europea. *eEurope 2002: Impatto e priorità.* COM(2001) 140 def. 13 marzo 2001.

Commissione Europea. *eEurope 2005: una società dell'informazione per tutti*. COM(2002) 263 def. 28 maggio 2002.

Commissione Europea. *Un'agenda digitale europea*. COM(2010) 245 def. 19 maggio 2010.

Commissione Europea. *Strategia per il mercato unico digitale in Europa.* COM(2015) 192 final. 6 maggio 2015.

Commissione Europea. *L'intelligenza artificiale per l'Europa*. COM(2018) 237 final. 25 aprile 2018.

Commissione Europea. *Piano coordinato sull'intelligenza artificiale*. COM(2018) 795 final. 7 dicembre 2018.

Commissione Europea. *Creare fiducia nell'intelligenza artificiale antropocentrica*. COM(2019) 168 final. 8 aprile 2019.

Commissione Europea. *Libro Bianco sull'intelligenza artificiale: Un approccio europeo all'eccellenza e alla fiducia.* COM(2020) 65 final. 19 febbraio 2020.

Commissione Europea. *Una strategia europea per i dati.* COM(2020) 66 final. 19 febbraio 2020.

Commissione Europea. *Plasmare il futuro digitale dell'Europa*. COM(2020) 67 final. 19 febbraio 2020.

Commissione Europea. *Bussola per il digitale 2030: il modello europeo per il decennio digitale*. COM(2021) 118 final. 9 marzo 2021.

Commissione Europea. *Proposta di 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*. COM(2021) 206 final. 21 aprile 2021.

Commissione Europea. *Better Regulation Toolbox*. 2023.

Commissione Europea. *Decisione del 24 gennaio 2024, che istituisce l'Ufficio Europeo per l'Intelligenza Artificiale*. C(2024) 390 final. 24 gennaio 2024.

Commissione Europea. *Parere* C(2024) 7814. 5 novembre 2024.

Consiglio dei Ministri. *Comunicato stampa n. 78*. 23 aprile 2024. https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-78/25501.

Consiglio di Stato, sezione VI, sentenza 13 dicembre 2019, n. 8472.

Corte di Giustizia dell'Unione Europea. Sentenza 15 luglio 1964, causa 6/64, *Flaminio Costa contro ENEL*. ECLI:EU:C:1964:66.

Corte di Giustizia dell'Unione Europea. Sentenza 10 ottobre 1973, causa 34/73, *Fratelli Variola S.p.A. contro Amministrazione italiana delle Finanze*. ECLI:EU:C:1973:101.

Corte di Giustizia dell'Unione Europea. Sentenza 2 febbraio 1977, causa 50/76, *Amsterdam Bulb BV contro Produktschap voor Siergewassen*. ECLI:EU:C:1977:13.

Corte di Giustizia dell'Unione Europea. Sentenza 29 gennaio 2008, causa C-275/06, *Productores de Música de España (Promusicae) contro Telefónica de España SAU*. ECLI:EU:C:2008:54.

European Data Protection Supervisor. *Opinion 7/2015: Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability*. 19 novembre 2015. https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf

European Data Protection Board. *Report of the Work Undertaken by the ChatGPT Taskforce*. 23 maggio 2024. https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf.

European Data Protection Board. *Statement 3/2024 on Data Protection Authorities' Role in the Artificial Intelligence Act Framework*. 16 luglio 2024. https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf.

Garante per la protezione dei dati personali. *Provvedimento n. 39*. 2 febbraio 2023. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9852214.

Garante per la protezione dei dati personali. *Provvedimento n. 112*. 30 marzo 2023. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870832.

Garante per la protezione dei dati personali. *Provvedimento n. 114*. 11 aprile 2023. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702.

Garante per la protezione dei dati personali. *Provvedimento n. 477*. 2 agosto 2024. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10043532.

Garante per la protezione dei dati personali. *Provvedimento n. 755*. 2 novembre 2024. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085455.

Garante per la protezione dei dati personali. *Comunicato stampa*. 30 gennaio 2025. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10097450.

Garante per la protezione dei dati personali. *Provvedimento n. 33*. 30 gennaio 2025. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10098477.

High Level Expert Group on Artificial Intelligence. *A Definition of AI: Main Capabilities and Scientific Disciplines*. 18 dicembre 2018. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.

High Level Expert Group on Artificial Intelligence. *Ethics Guidelines for Trustworthy AI*. 8 aprile 2019. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Italia. Decreto Legislativo 26 maggio 1997, n. 152. *Attuazione della direttiva 91/533/CEE concernente l'obbligo del datore di lavoro di informare il lavoratore delle condizioni applicabili al contratto o al rapporto di lavoro*.

Italia. Decreto legislativo 30 giugno 2003, n. 196. *Codice in materia di protezione dei dati personali*.

Italia. Decreto legislativo 7 marzo 2005, n. 82, *Codice dell'Amministrazione Digitale*.

Italia. Disegno di legge n. 1146. *Disposizioni e delega al Governo in materia di intelligenza artificiale*. 20 maggio 2024.

OCSE. *Raccomandazione del Consiglio sui principi sull'intelligenza artificiale.* 22 maggio 2019. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

Senato della Repubblica. *4ª Commissione permanente – Resoconto sommario n. 214*, 27 novembre 2024. https://www.senato.it/japp/bgt/showdoc/19/SommComm/0/1435866/index.html?part=doc_dc-allegato_a:1

Stati Uniti. *Telecommunications Act of 1996*. Public Law No. 104-104, 110 Stat. 56 (1996).

Unione Europea. *Carta dei Diritti Fondamentali dell'Unione Europea*. GUUE C 326, 26 ottobre 2012.

Unione Europea. *Trattato sul Funzionamento dell'Unione Europea*. GUUE C 326, 26 ottobre 2012.

Unione Europea. 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*). GUUE L 178, 17 luglio 2000.

Unione Europea. 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 e alla libera circolazione di tali dati (*Regolamento generale sulla protezione dei dati*). GUUE L 119, 4 maggio 2016.

Unione Europea. Regolamento (UE) 2017/745 del Parlamento Europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio. GUUE L 117, 5 maggio 2017.

Unione Europea. Regolamento (UE) 2017/1128 del Parlamento Europeo e del Consiglio, del 14 giugno 2017, relativo alla portabilità transfrontaliera di servizi di contenuti online nel mercato interno. GUUE L 168, 30 giugno 2017.

Unione Europea. Regolamento (UE) 2018/302 del Parlamento Europeo e del Consiglio, del 28 febbraio 2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno e che modifica i regolamenti (CE) n. 2006/2004 e (UE) 2017/2394 e la direttiva 2009/22/CE. GUUE L 60 I, 2 marzo 2018.

Unione Europea. Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea. GUUE L 303, 28 novembre 2018.

Unione Europea. Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione Europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (*Regolamento sulla cibersicurezza*). GUUE L 151, 7 giugno 2019.

Unione Europea. Direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico. GUUE L 172, 26 giugno 2019.

Unione Europea. 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*). GUUE L 152, 3 giugno 2022.

Unione Europea. 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*). GUUE L 265, 12 ottobre 2022.

Unione Europea. 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*). GUUE L 277, 27 ottobre 2022.

Unione Europea. Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore

finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011. GUUE L 333, 27 dicembre 2022.

Unione Europea. Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (*Direttiva NIS 2*). GUUE L 333, 27 dicembre 2022.

Unione Europea. 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*). GUUE L, 22 Dicembiore 2023.

Unione Europea. Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (*Regolamento sull'intelligenza artificiale*). GUUE L, 12 luglio 2024.

Letteratura scientifica e articoli di riviste on-line

Albus, James S. “Outline for a Theory of Intelligence.” *IEEE Transactions on Systems, Man, and Cybernetics* 21, n. 3 (maggio 1991): 473-509.

Alemanno, Alberto. “The Past, Present and Future of Risk Regulation.” *European Journal of Risk Regulation* 8, n. 1 (marzo 2017): 1–3. doi:10.1017/err.2017.4.

Aleo, Salvatore, a cura di. *Evoluzione scientifica e profili di responsabilità: neuroscienze, intelligenza artificiale, tutela della persona e modelli di responsabilità.* Pisa: Pacini Giuridica, 2022.

Almada, Marco. “Regulation by Design and the Governance of Technological Futures.” *European Journal of Risk Regulation* 14, n. 4 (maggio 2023): 697–709. doi:10.1017/err.2023.37.

Almada, Marco. “Two Dogmas of Technology-Neutral Regulation.” *SSRN* (settembre 2024). doi:10.2139/ssrn.4953377.

Alpa, Guido, a cura di. *Diritto e intelligenza artificiale.* Pisa: Pacini Giuridica, 2020.

Amato Mangiameli, Agata C. “Algoritmi e big data. Dalla carta sulla robotica.” *Rivista di filosofia del diritto* 1 (giugno 2019): 107-124. doi:10.4477/93369.

Andreessen, Marc. “The Techno-Optimist Manifesto.” *Andreessen Horowitz*. 16 ottobre 2023. https://a16z.com/the-techno-optimist-manifesto/.

Angelini, Roberta. “Intelligenza artificiale e governance. Alcune riflessioni di sistema.” In *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti, 293-318. Torino: Giappichelli, 2018.

Arthur, Charles. “Tech Giants May Be Huge, but Nothing Matches Big Data.” *The Guardian*, 23 agosto 2013. https://www.theguardian.com/technology/2013/aug/23/tech-giants-data.

Babbage, Charles. *Passages from the Life of a Philosopher.* Londra: Longman and Co., 1864.

Balkin, Jack M. “The Three Laws of Robotics in the Age of Big Data.” *Ohio State Law Journal* 78, n. 5 (2017): 1219-1241.

Bara, Bruno G. *Il metodo della scienza cognitiva. Un approccio evolutivo allo studio della mente.* Torino: Bollati Boringhieri, 2000.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Electronic Frontier Foundation* (febbraio 1996). https://www.eff.org/cyberspace-independence.

Bathaee, Yavar. “The Artificial Intelligence Black Box and the Failure of Intent and Causation.” *Harvard Journal of Law & Technology* 31, n. 2 (marzo 2018): 889-938

Beecher, Karl. *Computational Thinking: A Beginner’s Guide to Problem-Solving and Programming.* Swindon: BCS, The Chartered Institute for IT, 2017.

Bertola, Vittorio, e Stefano Quintarelli. *Internet fatta a pezzi: Sovranità digitale, nazionalismi e big tech.* Torino: Bollati Boringhieri, 2023.

Bertolini, Andrea. *Intelligenza artificiale e responsabilità civile: Problema, sistema, funzioni*. Bologna: Il Mulino, 2025.

Biever, Celeste. "The Easy Intelligence Tests That AI Chatbots Fail." *Nature* 619 (luglio 2023): 686-689. doi:10.1038/d41586-023-02361-7.

Black, Julia. "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World." *Current Legal Problems* 54, n. 1 (dicembre 2001): 103–146. doi:10.1093/clp/54.1.103.

Black, Julia, e Andrew Murray. "Regulating AI and Machine Learning: Setting the Regulatory Agenda." *European Journal of Law and Technology* 10, n. 3 (dicembre 2019): 1-21. https://www.ejlt.org/index.php/ejlt/article/view/722/980.

Bobev, Tervel. "Defining AI in the AI Act: Pin the Tail on the System." *KU Leuven CiTiP Blog*. 2 aprile 2024. https://www.law.kuleuven.be/citip/blog/defining-ai-in-the-ai-act-pin-the-tail-on-the-system/.

Boden, Margaret. *L'intelligenza artificiale.* Bologna: Il Mulino, 2019.

Bogoviz, Aleksei V., a cura di. *Big Data in Information Society and Digital Economy.* Cham: Springer, 2023.

Booch, Grady, Francesco Fabiano, Lior Horesh, Kiran Kate, Jonathan Lenchner, Nick Linck, Andreas Loreggia, Keerthiram Murgesan, Nicholas Mattei, Francesca Rossi, e Biplav Srivastava. "Thinking Fast and Slow in AI." *Proceedings of the AAAI Conference on Artificial Intelligence* 35, n. 17 (2021): 15042-46. doi:10.1609/aaai.v35i17.17765.

Borges, Georg, e Christoph Sorge, a cura di. *Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech.* Cham: Springer, 2022.

Borgobello, Massimo. "DeepSeek, privacy zero: comincia in Italia lo scontro di diritti." *Agenda Digitale*. 30 gennaio 2025. https://www.agendadigitale.eu/sicurezza/privacy/deepseek-privacy-zero-in-italia-e-scontro-di-diritti/.

Boschetti, Barbara. "La transizione della pubblica amministrazione verso il modello *Government as a platform*." In *L'amministrazione pubblica nell'era digitale*, a cura di Angelo Lalli, 1-37. Torino: Giappichelli, 2022.

Bradford, Anu. *The Brussels Effect: How the European Union Rules the World.* Oxford: Oxford University Press, 2020.

Bradford, Anu. *Digital Empires: The Global Battle to Regulate Technology.* Oxford: Oxford University Press, 2023.

Braun, Martin, Anne Vallery e Itsiq Benizri. "What Are High-Risk Artificial Intelligence Systems Within the Meaning of the European Union's Artificial Intelligence Act

and What Requirements Apply to Them?" *The Global Regulatory Developments Journal* 1, n. 6 (novembre 2024): 429–436.

Brownsword, Roger, e Karen Yeung, a cura di. *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*. Oxford: Hart Publishing, 2008.

Busuioc, Madalina, Deirdre Curtin e Marco Almada. "Reclaiming Transparency: Contesting the Logics of Secrecy Within the AI Act." *European Law Open* 2 (2023): 79–105. doi:10.1017/elo.2022.47.

Cappai, Marco. "Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?" *Federalismi* n. 30 (dicembre 2024): 186–206.

Carotti, Bruno. "L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice." *Giornale di diritto amministrativo* 23, n. 1 (gennaio 2017): 7-18.

Carotti, Bruno. "La politica europea sul digitale: ancora molto rumore." *Rivista trimestrale di diritto pubblico* 72, n. 4 (2022): 997-1013.

Casaburo, Donatella, e Lorenzo Gugliotta. "The EU AI Act Proposal(s): Manipulative and Exploitative AI Practices." *KU Leuven CiTiP Blog*. 22 settembre 2023. https://www.law.kuleuven.be/citip/blog/the-eu-ai-act-proposals-manipulative-and-exploitative-ai-practices/.

Caselli, Antonio. "Dagli artifici dell'intelligenza all'Intelligenza Artificiale." In *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti, 191-205. Torino: Giappichelli, 2018.

Casini, Lorenzo. "Il futuro dello Stato (digitale)." *Rivista trimestrale di diritto pubblico* 2 (aprile 2024): 433-469.

Cefaliello, Aude, e Miriam Kullmann. "Offering False Security: How the Draft Artificial Intelligence Act Undermines Fundamental Workers' Rights." *European Labour Law Journal* 13, n. 4 (2022): 567–588. doi:10.1177/20319525221114474.

Ćemalović, Uroš. "Prohibited Artificial Intelligence Practices According to Article 5 of the European Union's Regulation on AI—Between the 'Too Late' and the 'Not Enough.'" *International Journal of Law and Information Technology* 32, n. 1 (dicembre 2024). doi:10.1093/ijlit/eaae023.

Center for Research on Foundation Models. "On the Opportunities and Risks of Foundation Models." *arXiv*, n. arXiv:2108.07258 (agosto 2021). https://arxiv.org/abs/2108.07258.

Chiti, Edoardo, Barbara Marchetti, e Nicoletta Rangone. "L'impiego di sistemi di intelligenza artificiale nelle pubbliche amministrazioni italiane: prove generali." *BioLaw Journal - Rivista di BioDiritto*, n. 2 (luglio 2022): 489-507. doi:10.15168/2284-4503-2351.

Chiti, Edoardo. "Doppio volto: il diritto amministrativo alla prova dell'amministrazione digitale e algoritmica." In *La regolazione pubblica delle tecnologie digitali e*

dell'intelligenza artificiale, a cura di Angelo Lalli, 79-98. Torino: Giappichelli, 2024.

Chowdhary, K.R. *Fundamentals of Artificial Intelligence.* Heidelberg: Springer, 2020.

Christakis, Theodore, e Theodoros Karathanasis. "Tools for Navigating the EU AI Act: (2) Visualisation Pyramid." *HAL Open Science*, n. hal-04845277f (marzo 2024). https://hal.univ-grenoble-alpes.fr/hal-04845277v1.

Clarich, Marcello. *Autorità indipendenti: Bilancio e prospettive di un modello*. Bologna: Il Mulino, 2009.

Contissa, Giuseppe. *Information Technology for the Law.* Torino: Giappichelli, 2017.

Costanzo, Pasquale. "Lo 'Stato digitale': considerazioni introduttive." Relazione presentata al *Convegno annuale dell'Associazione "Gruppo di Pisa"*, Genova, 18 giugno 2021. https://gruppodipisa.it/images/convegni/2021_Convegno_Genova/Pasquale_Costanzo_-_Relazione_introduttiva.pdf

Cristianini, Nello. *La scorciatoia: Come le macchine sono diventate intelligenti senza pensare in modo umano.* Bologna: Il Mulino, 2023.

D'Acquisto, Giuseppe. "Qualità dei dati e Intelligenza Artificiale: intelligenza dai dati e intelligenza dei dati." In *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti, 265-292. Torino: Giappichelli, 2018.

De Anna, Gabriele. "Automi, responsabilità e diritto." *Rivista di filosofia del diritto, Journal of Legal Philosophy* 1 (giugno 2019): 125-142. doi:10.4477/93370.

De Franceschi, Alberto. "Il 'pagamento' mediante dati personali." In *I dati personali nel diritto europeo*, a cura di Vincenzo Cuffaro, Roberto D'Orazio e Vincenzo Ricciuto, 1381-1413. Torino: Giappichelli, 2019.

De Gregorio, Giovanni, e Raffaele Torino. "Privacy, protezione dei dati personali e big data." In *Privacy digitale: Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di Emilio Tosi, 447-484. Milano: Giuffrè, 2019.

De Mauro, Andrea, Marco Greco, e Michele Grimaldi. "A Formal Definition of Big Data Based on Its Essential Features." *Library Review* 65, n. 3 (marzo 2016): 122-135. doi:10.1108/LR-06-2015-0061.

Donati, Filippo. "Quale disciplina per l'intelligenza artificiale?" In *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce, 45-52. Torino: Giappichelli, 2023.

Dreyfus, Hubert. *What Computers Still Can't Do.* New York: MIT Press, 1979.

Faraone, Nicola M.F. "Chi prima arriva [forse non] primo alloggia: questioni aperte in tema di concorrenza e regolamentazione ex-ante nei mercati digitali." In *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce, 107-148. Torino: Giappichelli, 2023.

Finocchiaro, Giusella. *Intelligenza artificiale. Quali regole?* Bologna: Il Mulino, 2024.

Floridi, Luciano. *La rivoluzione dell'informazione.* Torino: Codice edizioni, 2012.

Floridi, Luciano. "Soft Ethics, the Governance of the Digital and the General Data Protection Regulation." *Philosophical Transactions of the Royal Society A* 376, n. 2133 (novembre 2018). doi:10.1098/rsta.2018.0081.

Floridi, Luciano. "Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical." *Philosophy and Technology* 32, n. 2 (maggio 2019): 185–193. doi:10.1007/s13347-019-00354-x.

Floridi, Luciano. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33 (agosto 2020): 369–378. doi:10.1007/s13347-020-00423-6.

Floridi, Luciano. *Etica dell'intelligenza artificiale: Sviluppi, opportunità, sfide.* Milano: Raffaello Cortina, 2022.

Franco, Elio. "ChatGPT è il buco nero della privacy, il Garante ha fatto bene: ecco perché." *Cybersecurity360*. 3 aprile 2023. https://www.cybersecurity360.it/legal/privacy-dati-personali/chatgpt-e-il-buco-nero-della-privacy-il-garante-ha-fatto-bene-ecco-perche/.

Franklin, Matija, Philip Moreira Tomei e Rebecca Gorman. "Vague Concepts in the EU AI Act Will Not Protect Citizens from AI Manipulation." *OECD.AI Policy Observatory*. 7 settembre 2023. https://oecd.ai/en/wonk/eu-ai-act-manipulation-definitions.

Frosini, Tommaso Edoardo. "L'Ordine giuridico del digitale." In *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce, 17-43. Torino: Giappichelli, 2023.

Fumagalli, Andrea. "Web Scraping: Cos'è, perché si usa e come difendersi da 'intrusioni' indesiderate." *Agenda Digitale*. 23 aprile 2021. https://www.agendadigitale.eu/sicurezza/web-scraping-cose-perche-si-usa-e-come-difendersi-da-intrusioni-indesiderate/.

Gabbrielli, Maurizio. "Dalla logica al *deep learning*: una breve riflessione sull'intelligenza artificiale." In *XXVI lezioni di diritto dell'intelligenza artificiale*, a cura di Ugo Ruffolo, 21-30. Torino: Giappichelli, 2021.

Galland, Jean-Pierre. "The Difficulties of Regulating Markets and Risks in Europe through Notified Bodies." *European Journal of Risk Regulation* 4, n. 3 (2013): 365–373.

Gambino, Alberto M. "Piattaforme, IA e data sharing: premessa." In *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce, 77-83. Torino: Giappichelli, 2023.

Gömann, Merlin. "The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement." *Common Market Law Review* 54, n. 2 (aprile 2017): 567–590. doi:10.54648/COLA2017035.

Gonçalves, Bernardo. “The Turing Test is a Thought Experiment.” *Minds & Machines* 33 (marzo 2023): 1-31. doi:10.1007/s11023-022-09616-8.

Grady, Patrick. “The AI Act Should Be Technology-Neutral.” *Center for Data Innovation* (febbraio 2023). https://www2.datainnovation.org/2023-ai-act-technology-neutral.pdf.

Greenberg, Brad A. “Rethinking Technology Neutrality.” *Minnesota Law Review* 100 (marzo 2016): 1495–1562.

Grozdanovski, Ljupcho, e Jérôme De Cooman. “Forget the Facts, Aim for the Rights! On the Obsolescence of Empirical Knowledge in Defining the Risk/Rights-Based Approach to AI Regulation in the European Union.” *Rutgers Computer and Technology Law Journal* 49, n. 2 (settembre 2023): 207–330.

Hacker, Philipp, Andreas Engel e Marco Mauer. “Regulating ChatGPT and Other Large Generative AI Models.” In *FAccT '23: The 2023 ACM Conference on Fairness, Accountability, and Transparency*, 1112–1123. New York: Association for Computing Machinery, 2023.

Halevy, Alon, Peter Norvig, e Fernando Pereira. “The Unreasonable Effectiveness of Data.” *IEEE Intelligent Systems* 24, n. 2 (marzo 2009): 8-12. doi:10.1109/MIS.2009.36.

Haugeland, John. *Artificial Intelligence: The Very Idea.* Cambridge, MA: MIT Press, 1985.

Heaven, Douglas, a cura di. *Macchine che pensano. La nuova era dell'intelligenza artificiale.* Tradotto da Valeria Lucia Gili. Bari: Edizioni Dedalo, 2018.

Hilbert, Martin. “Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective.” *Dialogues in Clinical Neuroscience* 22, n. 2 (giugno 2020): 189-194. doi:10.31887/DCNS.2020.22.2/mhilbert.

Hinton, Geoffrey, Oriol Vinyals e Jeff Dean. “Distilling the Knowledge in a Neural Network.” *arXiv*, n. arXiv:1503.02531 (marzo 2015). https://arxiv.org/abs/1503.02531.

Hoffmann-Riem, Wolfgang. “Artificial Intelligence as a Challenge for Law and Regulation.” In *Regulating Artificial Intelligence*, a cura di Thomas Wischmeyer e Timo Rademacher, 1–29. Cham: Springer, 2020.

Iannuzzi, Antonio. *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione.* Napoli: Editoriale Scientifica, 2018.

Iannuzzi, Antonio. “I regolamenti intersettoriali per l’istituzione dei ‘data spaces’: Data Governance Act e Data Act.” In *La regolazione europea della società digitale*, a cura di Franco Pizzetti, 107-133. Torino: Giappichelli, 2024.

Iannuzzi, Antonio. “Le fonti del diritto dell’Unione europea per la disciplina della società digitale.” In *La regolazione europea della società digitale*, a cura di Franco Pizzetti, 9–52. Torino: Giappichelli, 2024.

Iaselli, Michele. “Privacy e nuove tecnologie.” In *Diritto e nuove tecnologie. Prontuario giuridico ed informatico*, a cura di Michele Iaselli, 121-194. Milano: Altalex, 2016.

Iaselli, Michele. “Le origini dell’IA, evoluzione e rapporti con il diritto.” In *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli, 13-43. Rimini: Maggioli, 2024.

Italiano, Giuseppe Francesco. “Le sfide interdisciplinari dell'intelligenza artificiale.” *Analisi Giuridica dell'Economia* 1 (giugno 2019): 9-20. doi:10.1433/94541.

Johnson, David R., e David G. Post. “Law and Borders - the Rise of Law in Cyberspace.” *Stanford Law Review* 48 (1996): 1367-1402.

Jordan, Michael I. “Artificial Intelligence—The Revolution Hasn’t Happened Yet.” *Harvard Data Science Review* 1, n. 1 (luglio 2019). doi:10.1162/99608f92.f06c6e61.

Jung, Alexander. *Machine Learning: The Basics.* Singapore: Springer, 2022.

Kahneman, Daniel. *Pensieri lenti e veloci.* Tradotto da Laura Serra. Milano: Mondadori, 2020.

Kamara, Irene. “Co-regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation ‘Mandate.’” *European Journal of Law and Technology* 8, n. 1 (marzo 2017): 1–24. https://ejlt.org/index.php/ejlt/article/view/545/725.

Knappertsbusch, Inka, e Kai Gondlach, a cura di. *Work and AI 2030: Challenges and Strategies for Tomorrow's Work.* Wiesbaden: Springer, 2023.

Koniakou, Vasiliki. “From the ‘Rush to Ethics’ to the ‘Race for Governance’ in Artificial Intelligence.” *Information Systems Frontiers* 25, n. 1 (febbraio 2023): 71–102. doi:10.1007/s10796-022-10300-6.

Kosseff, Jeff. *The Twenty-Six Words That Created the Internet.* Ithaca: Cornell University Press, 2019.

Kumar, Sachin, Prayag Tiwari, e Mikhail Zymbler. “Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review.” *Journal of Big Data* 6, n. 111 (dicembre 2019). doi:10.1186/s40537-019-0268-2.

La Spina, Antonio, e Giandomenico Majone. *Lo Stato regolatore.* Bologna: Il Mulino, 2000.

Laidlaw, Emily B. *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility.* Cambridge: Cambridge University Press, 2015.

Lalli, Angelo, a cura di. *L’amministrazione pubblica nell’era digitale.* Torino: Giappichelli, 2022.

Laney, Doug. *3D Data Management: Controlling Data Volume, Velocity, and Variety.* Stamford, CT: META Group, 2001.

Larsen, Benjamin Cedric. “The Geopolitics of AI and the Rise of Digital Sovereignty.” *Brookings*. 8 dicembre 2022. https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.

LeCun, Yann, Yoshua Bengio, e Geoffrey Hinton. “Deep Learning.” *Nature* 521, n. 7553 (maggio 2015): 436-444. doi:10.1038/nature14539.

Lessig, Lawrence. “The Law of the Horse: What Cyberlaw Might Teach.” *Harvard Law Review* 113, n. 2 (dicembre 1999): 501–549.

Lessig, Lawrence. *Code and Other Laws of Cyberspace.* New York: Basic Books, 1999.

Liang, Paul Pu, Amir Zadeh, e Louis-Philippe Morency. “Foundations and Trends in Multimodal Machine Learning: Principles, Challenges, and Open Questions.” *arXiv*, n. arXiv:2209.03430 (settembre 2022). https://arxiv.org/abs/2209.03430.

Lisinska, Justyna, e Daniel Castro. “Why AI-Generated Content Labeling Mandates Fall Short.” *Center for Data Innovation* (dicembre 2024). https://www2.datainnovation.org/2024-ai-watermarking.pdf.

Longo, Alessandro. “Privacy, faro su Deepseek: a rischio i dati di milioni di italiani.” *Il Sole 24 Ore*. 28 gennaio 2025. https://www.ilsole24ore.com/art/il-garante-la-privacy-accende-faro-deepseek-e-apre-indagine-AGWUATbC.

Longo, Erik. “La disciplina del rischio digitale.” In *La regolazione europea della società digitale*, a cura di Franco Pizzetti, 53–82. Torino: Giappichelli, 2024.

Maceratini, Arianna. “Dall’Internet of Things alle Smart Roads. Riflessioni informatico-giuridiche su strade intelligenti, veicoli automatici e connessi.” *Rivista elettronica di diritto economia e management*, n. 3 (gennaio 2019): 71-91.

Maggino, Filomena, e Gabriele Cicerchia. “Algoritmi, etica e diritto.” *Il diritto dell'informazione e dell'informatica* 35, n. 6 (2019): 1161-1167.

Mahari, Robert, e Alex Pentland. “Regulation by Design: A New Paradigm for Regulating AI Systems.” In *Digital Single Market and Artificial Intelligence: AI Act and Intellectual Property in the Digital Transition*, a cura di Mario Franzosi, Oreste Pollicino e Gianluca Campus, 431-441. Roma: Aracne, 2024.

Majone, Giandomenico. “From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance.” *Journal of Public Policy* 17, n. 2 (maggio 1997): 139–167.

Majone, Giandomenico. “The Regulatory State and Its Legitimacy Problems.” *West European Politics* 22, n. 1 (1999): 1–24. doi:10.1080/01402389908425284.

Mandarà, Elena. “Il Regolamento UE sull'intelligenza artificiale.” In *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli, 45-108. Rimini: Maggioli, 2024.

Mantelero, Alessandro. “From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era.” In *Group Privacy:*

New Challenges of Data Technologies, a cura di Linnet Taylor, Luciano Floridi e Bart van der Sloot, 139–158. Cham: Springer, 2017.

Mantelero, Alessandro. *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI*. The Hague: T.M.C. Asser Press, 2022.

Marchetti Spaccamela, Alberto, e Fabrizio Silvestri. "Trasparenza e interpretabilità delle decisioni dei sistemi di Intelligenza Artificiale." In *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, a cura di Angelo Lalli, 159-178. Torino: Giappichelli, 2024.

Marchetti, Barbara. "L'amministrazione digitale." In *Enciclopedia del diritto. Vol. III - Le funzioni amministrative*, a cura di Bernardo Giorgio Mattarella e Margherita Ramajoli, 75-109. Milano: Giuffrè, 2022.

Mărcuţ, Mirela. *Crystalizing the EU Digital Policy: An Exploration into the Digital Single Market.* Cham: Springer, 2017.

Masuda, Yoneji. *The Information Society as Post-Industrial Society.* Tokyo: World Future Society, 1980.

McCulloch, Warren S., e Walter H. Pitts. "A Logical Calculus of the Ideas Immanent in Nervous Activity." *The Bulletin of Mathematical Biophysics* 5 (1943): 115-133.

Minaee, Shervin, Tomas Mikolov, Narjes Nikzad, Meysam Chenaghlu, Richard Socher, Xavier Amatriain, e Jianfeng Gao. "Large Language Models: A Survey." *arXiv*, n. arXiv:2402.06196 (febbraio 2024). https://arxiv.org/abs/2402.06196.

Mobilio, Giuseppe. "L'intelligenza artificiale e i rischi di una 'disruption' della regolamentazione giuridica." *BioLaw Journal - Rivista di BioDiritto*, n. 2 (luglio 2020): 401-424. doi:10.15168/2284-4503-669.

Moses, Lyria Bennett. "How to Think about Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target." Law, Innovation and Technology 5, n. 1 (2013): 1–20. doi:10.5235/17579961.5.1.1.

Neuwirth, Rostam J. "Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)." *Computer Law & Security Review* 48 (aprile 2023). doi:10.1016/j.clsr.2023.105798.

Newell, Allen, e Herbert A. Simon. "Computer Science as Empirical Inquiry: Symbols and Search." *Communications of the ACM* 19, n. 3 (marzo 1976): 113–126. doi:10.1145/360018.360022.

Nichols, James A., Hsien W. Herbert Chan, e Matthew A. B. Baker. "Machine Learning: Applications of Artificial Intelligence to Imaging and Diagnosis." *Biophysical Reviews* 11, n. 1 (febbraio 2019): 111-118. doi:10.1007/s12551-018-0449-9.

Nicita, Antonio. "Il dato profilato nella prospettiva economica tra privacy, propertization, secrecy." In *I dati personali nel diritto europeo*, a cura di Vincenzo Cuffaro, Roberto D'Orazio e Vincenzo Ricciuto, 1163-1180. Torino: Giappichelli, 2019.

Niger, Sergio. *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali.* Padova: Cedam, 2006.

Nikolinakos, Nikos Th. *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act*. Cham: Springer, 2023.

Novelli, Claudio, Philipp Hacker, Jessica Morley, Jarle Trondal e Luciano Floridi. "A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities." *European Journal of Risk Regulation* (2024): 1–25. doi:10.1017/err.2024.57.

OpenAI. "GPT-4 Technical Report." *arXiv*, n. arXiv:2303.08774v6 (marzo 2024). https://arxiv.org/abs/2303.08774.

Ottolia, Andrea. *Big Data e innovazione computazionale.* Torino: Giappichelli, 2017.

Pajno, Alessandro, Marco Bassini, Giovanni De Gregorio, Marco Macchia, Francesco Paolo Patti, Oreste Pollicino, Serena Quattrocolo, Dario Simeoli, e Pietro Sirena. "AI: Profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista." *BioLaw Journal - Rivista di BioDiritto*, n. 3 (novembre 2019): 205-235. doi:10.15168/2284-4503-449.

Pajno, Alessandro. "Forum: Law and Artificial Intelligence." *BioLaw Journal – Rivista di BioDiritto* 1 (marzo 2020): 471–502. doi:10.15168/2284-4503-538.

Pajno, Alessandro. "La governance dell'intelligenza artificiale tra regolamento europeo e disciplina nazionale." *Astrid Rassegna* n. 13 (settembre 2024).

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information.* Cambridge, MA: Harvard University Press, 2015.

Pellecchia, Enza. "Privacy, decisioni automatizzate e algoritmi." In *Privacy digitale: Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, a cura di Emilio Tosi, 417-446. Milano: Giuffrè, 2019.

Peluso, Maria Grazia. *Intelligenza artificiale e tutela dei dati: Prospettive critiche e possibili benefici per una governance efficace.* Milano: Giuffrè, 2023.

Perritt, Henry H., Jr. "Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism." *Berkeley Technology Law Journal* 12, n. 2 (settembre 1997): 413-438. doi:10.15779/Z38N08W.

Perrucci, Antonio. "Dai Big Data all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche." *Analisi Giuridica dell'Economia* 1 (giugno 2019): 61-88. doi:10.1433/94545.

Pizzetti, Franco. "La protezione dei dati personali e la sfida dell'Intelligenza Artificiale." In *Intelligenza artificiale, protezione dei dati personali e regolazione*, a cura di Franco Pizzetti, 5-187. Torino: Giappichelli, 2018.

Pizzetti, Franco. "AI, in Europa troppe regole? Pizzetti: 'Ecco i nodi da chiarire'." *Agenda Digitale*. 23 settembre 2024. https://www.agendadigitale.eu/sicurezza/privacy/ai-in-europa-troppe-regole-pizzetti-ecco-i-nodi-da-chiarire/.

Pizzetti, Franco. “Introduzione alla regolazione europea della società digitale.” In *La regolazione europea della società digitale*, a cura di Franco Pizzetti, 1–8. Torino: Giappichelli, 2024.

Pliauskaite, Laura, e Isabelle Roccia. “Governance: EU and National Stakeholders.” *Top 10 Operational Impacts of the EU AI Act*, *IAPP* (settembre 2024): 56–60. https://iapp.org/media/pdf/resource_center/top_10_impacts_eu_ai_act.pdf.

Police, Aristide. “Scelta discrezionale e decisione algoritmica.” In *Il diritto nell’era digitale: persona, mercato, amministrazione, giustizia*, a cura di Rosaria Giordano, Andrea Panzarola, Aristide Police, Stefano Preziosi e Massimo Proto, 493–504. Milano: Giuffrè, 2022.

Pop, Florina, Michaela Sullivan-Paul ed Elpida Longinidou. “Are Data Protection Authorities the New AI Market Surveillance Authorities?” *European Institute of Public Administration Blog*. 23 settembre 2024. https://www.eipa.eu/blog/are-data-protection-authorities-the-new-ai-market-surveillance-authorities/.

Pope, Richard. *Playbook: Government as a Platform.* Cambridge, MA: Ash Center for Democratic Governance and Innovation, Harvard Kennedy School, 2019. https://ash.harvard.edu/wp-content/uploads/2024/02/293091_hvd_ash_gvmnt_as_platform_v2.pdf.

Prifti, Kostina, Jessica Morley, Claudio Novelli e Luciano Floridi. “Regulation by Design: Features, Practices, Limitations, and Governance Implications.” *Minds & Machines* 34, n. 2 (maggio 2024): 1-21. doi:10.1007/s11023-024-09675-z.

Quintarelli, Stefano. *Intelligenza artificiale: Cos’è davvero, come funziona, che effetti avrà.* Torino: Bollati Boringhieri, 2020.

Rabitti, Maddalena, e Fabio Bassan. “L’applicazione dell’AI Act in Italia e la tutela del consumatore. Il ruolo delle autorità indipendenti.” *Federalismi* n. 30 (dicembre 2024): 250–265.

Reed, Chris, e Andrew Murray. *Rethinking the Jurisprudence of Cyberspace.* Cheltenham: Edward Elgar, 2020.

Renda, Andrea, e Alex Engler. “What’s in a Name? Getting the Definition of Artificial Intelligence Right in the EU’s AI Act.” *CEPS Explainer* (febbraio 2023). https://www.ceps.eu/ceps-publications/whats-in-a-name/.

Riva, Gianluigi Maria. “IA e Internet.” In *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli, 297–343. Rimini: Maggioli, 2024.

Romano, Giovanni. “Diritto, robotica e teoria dei giochi: riflessioni su una sinergia.” In *Diritto e Intelligenza Artificiale*, a cura di Guido Alpa, 103-123. Pisa: Pacini, 2020.

Ross, Philip, e Kasia Maynard. “Towards a 4th Industrial Revolution.” *Intelligent Buildings International* 13, n. 3 (marzo 2021): 159-161. doi:10.1080/17508975.2021.1873625.

Ruffolo, Ugo, Andrea Amidei, ed Enrico Al Mureden. “La responsabilità.” In *XXVI lezioni di diritto dell'intelligenza artificiale*, a cura di Ugo Ruffolo, 131-184. Torino: Giappichelli, 2021.

Ruschemeier, Hannah. “AI as a Challenge for Legal Regulation – The Scope of Application of the Artificial Intelligence Act Proposal.” *ERA Forum* 23 (gennaio 2023): 361-376.

Russell, Stuart J., e Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4ª ed. Londra: Pearson, 2020.

Sadin, Éric. *Critica della ragione artificiale. Una difesa dell’umanità.* Roma: LUISS University Press, 2019.

Salamida, Fabio. “Che fine ha fatto il DDL sull’intelligenza artificiale.” *Wired*. 16 gennaio 2025. https://www.wired.it/article/ddl-intelligenza-artificiale-che-fine-ha-fatto-news/#:~:text=in%20Senato%2C%20dove%20lo%20avevamo,lontana%20dal%20vedere%20la%20luce.

Salazar, Carmela. “Umano, troppo umano. O no? Robot, androidi e cyborg nel ‘mondo del diritto’ (prime notazioni).” *BioLaw Journal - Rivista di BioDiritto*, n. 1 (maggio 2014): 255-276. doi:10.15168/2284-4503-21.

Santosuosso, Amedeo. “Forum: Law and Artificial Intelligence. Questioni definitorie.” *BioLaw Journal – Rivista di BioDiritto* 1 (marzo 2020): 469-472. doi:10.15168/2284-4503-538.

Sapuppo, Valentina Grazia. “Etica ed IA.” In *AI Act: Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, a cura di Michele Iaselli, 109-141. Rimini: Maggioli, 2024.

Sarker, Iqbal H. "Machine Learning: Algorithms, Real-World Applications and Research Directions." *SN Computer Science* 2, n. 160 (marzo 2021). doi:10.1007/s42979-021-00592-x.

Schepisi, Cristina. “Brevi note sulla ‘dimensione europea’ della regolamentazione dell’intelligenza artificiale: principi, obiettivi e requisiti.” In *Strategia dei dati e intelligenza artificiale: Verso un nuovo ordine giuridico del mercato*, a cura di Valeria Falce, 53-74. Torino: Giappichelli, 2023.

Schuett, Jonas. “Risk Management in the Artificial Intelligence Act.” *European Journal of Risk Regulation* 15 (2024): 367–385. doi:10.1017/err.2023.1.

Schuilenburg, Marc, e Rik Peeters, a cura di. *The Algorithmic Society: Technology, Power, and Knowledge.* Londra: Routledge, 2020.

Schultz, Thomas. “Private Legal Systems: What Cyberspace Might Teach Legal Theorists.” *Yale Journal of Law & Technology* 10, n. 151 (gennaio 2007): 151-193.

Searle, John R. “Minds, Brains, and Programs.” *Behavioral and Brain Sciences* 3, n. 3 (1980): 417-424. doi:10.1017/S0140525X00005756.

Selznick, Philip. “Focusing Organisational Research on Regulation.” In *Regulatory Policy and the Social Sciences*, a cura di Roger G. Noll, 363–364. Berkeley: University of California Press, 1985.

Simoncini, Andrea. “Sovranità e potere nell'era digitale.” In *Diritti e libertà in Internet*, a cura di Tommaso Edoardo Frosini, Oreste Pollicino, Ernesto Apa e Marco Bassini. Milano: Mondadori Education, 2017.

Simoncini, Andrea. “Verso la regolamentazione della intelligenza artificiale. Dimensioni e governo.” *BioLaw Journal - Rivista di BioDiritto*, n. 2 (giugno 2021): 411–417.

Ślusarczyk, Beata. “Industry 4.0—Are We Ready?” *Polish Journal of Management Studies* 17, n. 1 (giugno 2018): 232-248. doi:10.17512/pjms.2018.17.1.19.

Smuha, Nathalie Alisa. “From a ‘Race to AI’ to a ‘Race to AI Regulation’ - Regulatory Competition for Artificial Intelligence.” *Law, Innovation and Technology* 13, n. 1 (2021): 1-26. doi:10.2139/ssrn.3501410.

Smuha, Nathalie A. “Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective.” In *European Sovereignty: The Legal Dimension*, a cura di Gavin Barrett, Peter-Christian Müller-Graff, Jean-Philippe Rageade e Viktor Vadász, 127–150. Cham: Springer, 2024.

Söderlund, Kasia, e Stefan Larsson. “Enforcement Design Patterns in EU Law: An Analysis of the AI Act.” *Digital Society* 3, (luglio 2024): 1–21. doi:10.1007/s44206-024-00129-8.

STOA - Panel for the Future of Science and Technology. *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence.* Bruxelles: European Parliamentary Research Service, giugno 2020.

Stonier, Tom. *Beyond Information: The Natural History of Intelligence.* Londra: Springer, 1992.

Taeihagh, Araz, M. Ramesh e Michael Howlett. “Assessing the Regulatory Challenges of Emerging Disruptive Technologies.” *Regulation and Governance* 15, n. 4 (marzo 2021): 1009–1019. doi:10.1111/rego.12392.

Torchia, Luisa. *Lo Stato digitale.* Bologna: Il Mulino, 2023.

Tremolada, Luca. “AI Act, tutto quello che sappiamo finora e qualche considerazione.” *Il Sole 24 Ore*. 16 dicembre 2023. https://www.infodata.ilsole24ore.com/2023/12/16/ai-act-tutto-quello-che-sappiamo-finora-e-qualche-considerazione/.

Turing, Alan M. “Computing Machinery and Intelligence.” *Mind* 59, n. 236 (ottobre 1950): 433-460. doi:10.1093/mind/LIX.236.433.

Tyson, Laura D., e John Zysman. “Automation, AI & Work.” *Daedalus* 151, n. 2 (maggio 2022): 256-271.

Uuk, Risto, Carlos Ignacio Gutierrez, Sandra Day, Daniel Guppy, Lode Lauwaert, Atoosa Kasirzadeh, Lucia Velasco, Peter Slattery e Carina Prunk. “A Taxonomy of

Systemic Risks from General-Purpose AI." *SSRN* (novembre 2024). doi:10.2139/ssrn.5030173.

Von der Leyen, Ursula. *Orientamenti politici per la prossima Commissione europea 2019-2024*. Lussemburgo: Ufficio delle pubblicazioni dell'Unione Europea, 2020. doi:10.2775/688283.

Warwick, Kevin. *Intelligenza artificiale. Le basi.* Tradotto da Chiara Barattieri di San Pietro e Giuseppe Maugeri. Palermo: Dario Flaccovio, 2015.

Yeung, Karen. *Securing Compliance: A Principled Approach.* Oxford: Hart Publishing, 2004.

Yeung, Karen. "Design for the Value of Regulation." In *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*, a cura di Jeroen van den Hoven, Pieter E. Vermaas e Ibo van de Poel, 447–472. Dordrecht: Springer, 2015.

"Exceptions to the One-Stop-Shop Rule of the GDPR." *GRUR International* 71, n. 1 (gennaio 2022): 64–81. doi:10.1093/grurint/ikab139.