La duplice radice dell'Intelligenza Artificiale: fra le esigenze di innovazione e la tutela dei più fragili*

Manuela Luciana Borgese

Abstract

L'impatto delle nuove tecnologie diviene ogni giorno più significativo, semplificando ed agevolando sensibilmente persone, imprese e servizi pubblici. Tale progresso è incoraggiato e sostenuto non soltanto da una crescente digitalizzazione di servizi e processi, ma anche dall'innovativo apporto dei sistemi di intelligenza artificiale, ogni giorno sempre più presenti nei più diversi contesti della vita quotidiana. A causa dell'elevata capacità di apprendere e di elaborare attraverso l'esposizione ai dati personali raccolti, il ricorso a tali sistemi è causa di forti preoccupazioni, soprattutto per l'esposizione spesso incontrollata a categorie di soggetti fragili, quali i minori. L'obiettivo del paper è quindi quello di esaminare il contesto normativo, fra i vantaggi e i possibili strumenti di tutela.

The impact of new technologies becomes more significant every day, significantly simplifying and facilitating people, businesses and public services. This progress is encouraged and supported not only by a growing digitalisation of services and processes, but also by the innovative contribution of artificial intelligence systems, which are increasingly present every day in the most diverse contexts of daily life. Due to the high capacity to learn and process through exposure to the personal data collected, the use of such systems causes strong concerns, especially due to the often uncontrolled exposure to categories of fragile subjects, such as minors. The objective of the paper is therefore to examine the regulatory context, including the advantages and possible protection tools.

Sommario

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Keywords

intelligenza artificiale – diritti digitali – *data protection* – categorie vulnerabili – minori

1. Introduzione

Le nuove tecnologie assumono un ruolo sempre più presente ed essenziale nella nostra realtà, con un livello di diffusione in costante crescita. Il coinvolgimento di tali innovazioni non incontra più significative barriere, raggiungendo trasversalmente i più diversi contesti socio-economici. Infatti, moltissimi sono gli ambiti che ne vengono influenzati, fra i quali la ricerca scientifica, l'istruzione, le infrastrutture e i trasporti. I risvolti pratici non si limitano ad evidenze di natura economica ma anche qualitativa, a vantaggio di una categoria sempre più ampia di destinatari.

L'aumento del *range* di diffusione è legato all'incremento delle performance di utilizzo, reso possibile grazie all'avanzamento tecnologico che ne supporta il funzionamento.

Tale fruibilità si traduce in un'indubbia versatilità di uso e in output molto rapidi, anche con interessanti riduzioni di costi, a vantaggio comune per cittadini, imprese e pubblica amministrazione.

Il ricorso a tali sistemi può infatti tradursi in miglioramenti significativi della vita per l'accesso a servizi nuovi, veloci e performanti e in linea con i diritti delle persone.

In tale scenario, uno dei fattori di particolare interesse è connesso all'utilizzo dell'intelligenza artificiale (IA), sistema tecnologico certamente non nuovo che ha trovato nello sviluppo infrastrutturale di cui si è fatto cenno, il naturale habitat di crescita e di evoluzione, culminata con l'affermazione di questa tecnologia nell'AI Act[1], recentemente entrato in vigore e che si avrà modo di esaminare in prosieguo.

Il quadro ottimistico delineato, per quanto ricco di opportunità non deve lasciare intendere che tale situazione sia esente da rischi.

Una delle principali perplessità riguarda i ragionevoli dubbi in termini di chiarezza e liceità delle modalità di funzionamento dei sistemi algoritmici che ne sono alla base, per l'impossibilità di intervenire su tale discrezionalità e di potersi difendere in caso di ingiuste dinamiche. Perché mentre da un lato è d'impatto la percezione dell'estrema versatilità degli algoritmi, dall'altro si contrappone l'opacità di tali sistemi, soprattutto in termini di etica e correttezza, parametri strutturali in una società basata su diritti e valori. Ciò soprattutto a tutela di fasce più vulnerabili, quali i minori o le persone con alterata capacità psicologica, che devono appunto essere destinatarie di più intensi livelli di tutela.

Delineato il quadro di riferimento, occorrerà ora esaminare il concreto assetto di benefici e rischi, quindi la duplice natura di questa tecnologia, comparando le dinamiche e l'efficacia del rinnovato contesto normativo vigente, che si rivela certamente avanza-

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

to ma ancora in divenire rispetto agli scenari di rischio e alle sfide emergenti.

2. Benefici e rischi dell'IA: fra opportunità e nuove esigenze di tutela

Il quadro di opportunità connesse all'utilizzo dei sistemi di IA acquisisce quotidianamente nuovi ed inaspettati parametri. Tali sistemi divengono ogni giorno più potenti e capaci di offrire maggiori vantaggi ma, come si avrà modo di rilevare, questa straordinaria capacità non è esente da problematiche.

Per inquadrare correttamente il fenomeno è bene, anzitutto, partire dalla definizione di IA resa dal Regolamento, che identifica un sistema di IA[2] come «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».

Si tratta quindi di sistemi di indubbia utilità e di grande versatilità, capaci di eseguire dei task a supporto dell'attività umana, semplificandola e riducendo tempi e costi. Secondo le indagini elaborate dal Parlamento Europeo[3], gli impatti positivi sulle organizzazioni sono di assoluto interesse, contribuendo ad erogare servizi qualitativamente migliori e automazione di processi, ripetitivi e costosi, a vantaggio di tutte le categorie di beneficiari. In particolare, per i cittadini, potrebbe comportare servizi sanitari più sicuri e performanti, posti di lavoro più garantiti e innovativi delegando ai robot le funzioni più rischiose, servizi pubblici più vicini alle proprie aspettative e nel rispetto delle garanzie di legge. Per le imprese, l'IA può rappresentare un sistema efficace di automatizzazione di processi con impatti interessanti su costi e risorse, contribuendo, secondo l'analisi del PE, all'aumento stimato della produttività del lavoro grazie all'IA. Infine, notevole risulta essere anche l'impatto sulla qualità del servizio pubblico con vantaggi su istruzione, servizio sanitario e gestione dell'energia e della sostenibilità dei beni[4].

Altra straordinaria opportunità è rappresentata dalla nuova generazione di modelli di IA per finalità generali[5], contraddistinti dalla capacità di svolgere un'ampia gamma di compiti distinti. A tale categoria, appartengono i modelli di IA generativa[6], basati su tecnologia di tipo *large language model* (LLM) divenuti largamente utilizzati grazie al lancio di sistemi quali ChatGPT di OpenAI o Gemini di Google, che consentono una generazione flessibile ed immediata di contenuti, ad esempio sotto forma di testo,

[2] Art. 3, n. 1, AI Act.

[3] ? *European Parliamentary Research Service,* giugno 2020 e Opportunities of Artificial Intelligence, *Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies*, giugno 2020.

[4] Tale serie di opportunità si colloca con un altro asse strategico del piano europeo, il Green deal, spiegato nella comunicazione; in questo senso COM (2020) 65 final, par. 1, e COM(2019) 640 final.

[5] Considerando 97 e art. 3, par 63, AI Act.

[6] Considerando 99 AI Act.

audio, immagini o video. Tale tecnologia[7], presenta opportunità di innovazione uniche, grazie all'utilizzo intuitivo e alla grande immediatezza di risposta. Infatti, con una semplice domanda, in base alle istruzioni dell'utente (c.d. *prompt*)[8], il sistema è in grado di elaborare un documento o una ricerca attraverso l'analisi di enormi quantitativi di dati, estratti da varie fonti.

La grande versatilità di utilizzo cela, tuttavia, notevoli inside. In primo luogo, riguardo i possibili effetti dannosi sulle alterazioni della capacità di apprendimento degli esseri umani per effetto dell'uso di questi sistemi[9]. Inoltre, in un contesto educativo, l'assenza di uno specifico controllo metodologico, potrebbe comportare significativi pericoli, più gravi in caso di categorie vulnerabili o destinatarie di bisogni speciali di istruzione. La consapevolezza su questi possibili rischi è stata alla base delle linee programmatiche del legislatore, rappresentando uno dei capisaldi su cui si è andata strutturando la normativa in esame[10]. Non vi è dubbio che nella forte attenzione verso l'avanzamento tecnologico e la primazia economica europea, lo scenario di fondo sia rappresentato dai valori fondamentali su cui si basa l'Unione, fra cui i diritti: di libertà; alla dignità umana; alla non discriminazione basata su elementi quali sesso, origine etnica, religione o disabilità; alla protezione dei dati personali; alla tutela giudiziale e a un giudice imparziale alla tutela effettiva dei consumatori. L'asse di tali valori potrebbe inclinarsi in negativo, laddove le caratteristiche proprie delle strutture algoritmiche creino contrasti rispetto a dette tutele. Su un piano di attenta osservazione devono quindi essere posti elementi propri della strutturazione algoritmica quale l'insita opacità della progettazione, la mancanza di sorveglianza umana nell'esecuzione dell'elaborazione, la

[7] V. Brühl, *Generative Artificial Intelligence – Foundations, Use Cases and Economic Potential, ZBW – Leibniz Information Centre for Economics*, in *Intereconomics*, 1, 2024, 4-9.

[8] C. Novelli- F. Casolari - P.Hacker - G. Spedicato - L. Floridi, *Generative AI in EU Law*: L*iability, Privacy, Intellectual Property, and Cybersecurity*, in *Computer Law & Security Review*, 55, 2024, 1-16 che offre un'approfondita ricostruzione dell'attuale configurazione dei LLM e delle tecnologie generative basate su tale modello, prospettando i principali rischi e le eventuali lacune alla luce della nuova legislazione esistente.

[9] H. Bastani - O. Bastani - A. Sungu - H. Ge - O. Kabakcı - R. Mariman, *Generative AI Can Harm Learning*, in *The Wharton School Research Paper,* 1, 2024, 1-59, in cui vengono rappresentati i risultati sugli effetti di tali tecnologie sugli utilizzatori, basati su test pratici. Fra i diversi passaggi di rilievo dell'articolo, si riporta «Quando la tecnologia automatizza un'attività, gli esseri umani possono perdere una preziosa esperienza nell'esecuzione di tale attività. Di conseguenza, una tale tecnologia può indurre un compromesso in cui migliorano le prestazioni in media ma introducono nuovi casi di guasto a causa della riduzione delle capacità umane. Ad esempio, l'eccessiva dipendenza dal pilota automatico ha portato la Federal Aviation Administration a raccomandare ai piloti di ridurre al minimo l'uso di questa tecnologia. La loro guida precauzionale garantisce che i piloti abbiano le competenze necessarie per mantenere la sicurezza in situazioni in cui l'autopilota non funziona correttamente», giungendo alla conclusione «questi risultati suggeriscono che, sebbene l'accesso all'IA generativa possa migliorare le prestazioni, può inibire sostanzialmente l'apprendimento. I nostri risultati hanno implicazioni significative per gli strumenti basati sull'intelligenza artificiale generativa: sebbene tali strumenti abbiano il potenziale per migliorare le prestazioni umane, devono essere implementati con protezioni adeguate quando l'apprendimento è importante».

[10] Commissione Europea, Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia, COM(202) 65 final, Gruppo di esperti ad alto livello sull'intelligenza artificiale, Orientamenti etici per un'IA affidabile, Bruxelles, 8 aprile 2019.

possibile presenza di distorsioni o bias[11] (es: di tipo razziale o etnico[12]) e l'impossibilità di intervento umano. L'AI Act non interviene per ampliare l'elencazione dei diritti oggetto di protezione[13] ma si qualifica come strumento di tutela che si aggiunge a quelli già esaminati e a quelli previsti dalle ulteriori normative. Fra queste, è impossibile non dedicare una specifica menzione ad un asse strutturale dei diritti fondamentali quale quello alla riservatezza e al lecito e corretto trattamento dei dati personali, disciplinato dal GDPR[14] e dalla Direttiva e-privacy[15], relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, su cui si rendono necessarie alcune riflessioni.

Un primo punto viene offerto dal parere congiunto delle principali istituzioni privacy europee, il Comitato europeo per la protezione dei dati (EDPB) e il Garante Europeo per la protezione dei dati (EDPS)[16], laddove si indica, con riguardo ai rischi specificamente connessi ai diritti fondamentali, che «affidare alle macchine il compito di prendere decisioni sulla base di dati comporterà rischi per i diritti e le libertà delle persone che incideranno sulla loro vita privata e potrebbero nuocere a categorie sociali o persino a intere società». Il disallineamento prospettato riguarda veri e propri pilastri dei valori dell'UE, quali il menzionato diritto alla riservatezza, quelli alla vita privata e familiare, di cui alla Dichiarazione universale dei diritti dell'uomo[17], alla Convenzione europea dei diritti dell'uomo[18] e alla Carta dei diritti fondamentali dell'Unione europea[19], che li tutelano ponendo l'obbligo di impedire che le persone possano subire interferenze o lesioni illecite.

Un particolare aspetto, che rende sempre più complessa l'interazione fra IA e normativa privacy, è collegato al fatto che lo sviluppo, l'addestramento e l'apprendimento[20] di

[11] Parlamento Europeo, Artificial intelligence: How does it work, why does it matter, and what can we do about it?, *European Parliamentary Research Service,* giugno 2020.

[12] Con riguardo alla lotta contro la discriminazione basata su pregiudizi razziali o etnici, è molto interessante la ricostruzione resa nella ricerca del Parlamento Europeo, EU legislation and policies to address racial and ethnic discrimination, *European Parliamentary Research Service,* 20 marzo 2023, di rilievo fondamentale ma non diretto oggetto del presente contributo. Questa ricerca offre un quadro molto approfondito dell'estrema, quanto diffusa, gravità del fenomeno e delle azioni comunitarie mirate alla lotta contro questi fenomeni, anche sul fronte dei problemi nascenti da output algoritmici.

[13] F. Donati, *La protezione dei diritti fondamentali nel Regolamento sull'Intelligenza Artificiale*, in *Rivista Associazione Italiana Costituzionalisti*, 1, 2025, 1-20.

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

[15] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[16] Parere congiunto 5/2021 sulla proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale).

[17] Art. 12 Dichiarazione universale dei diritti dell'uomo.

[18] Art. 12 della Convenzione europea dei diritti dell'uomo.

[19] Artt.7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

[20] H. Ruschemeier, *Generative AI and Data Protection*, in *Cambridge Forum on AI: Law and Governance,* 1, 2025, 1–16.

tali modelli avviene attraverso la raccolta di grandi quantità di dati, anche personali[21] e particolari[22], testo, immagini e video. L'esigenza è che il tutto si svolga nel pieno rispetto delle prescrizioni normative, per evitare possibili violazioni dei diritti fondamentali normativamente previsti. Nel costellato quadro degli adempimenti privacy, si avrà modo di soffermarsi su due particolari aspetti previsti dal GDPR, fortemente coinvolti nell'utilizzo di tali tecnologie, relativi alla trasparenza e alle condizioni di liceità[23].

La trasparenza rappresenta un pilastro fondamentale a presidio dei diritti degli interessati che, in un siffatto contesto, acquisisce una specifica declinazione rispetto ai trattamenti effettuati per il tramite di sistemi di Intelligenza Artificiale. Le prescrizioni in materia sono previste dagli artt. 12-14 GDPR ed impongono che l'interessato, ovvero la persona fisica cui si riferiscono i dati trattati, ha diritto di ottenere informazioni trasparenti, dettagliate, comprensibili e facilmente disponibili sul trattamento dei propri dati. Con riguardo specificamente ai trattamenti effettuati attraverso sistemi di IA, è fondamentale richiamare la disposizione dell'art. 13, par. 2, lett. f) che impone al titolare del trattamento di indicare l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui ai parr. 1 e 4 dell'art. 22 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Tale disposizione deve poi essere letta nel combinato disposto dell'art. 22 GDPR, laddove stabilisce che «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». Questa disposizione non si applica laddove la decisione «a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato». Nei casi di cui alle lettere a) e b) il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione[24]. Tali previsioni, insieme all'ulteriore assetto di obblighi derivanti dalla

[21] Considerando 105 AI Act. Sulla definizione di dato personale si veda art. 4, n. 1, regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), "GDPR".

[22] Si tratta dei dati definiti dall'art. 9, par. 1, GDPR (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) e che possono essere trattati solo in presenza delle condizioni previste dalla normativa privacy.

[23] Art. 5 GDPR: I dati personali sono: a) trattati in modo *lecito*, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»). Con riguardo alle condizioni di liceità, si vedano le disposizioni dell'art. 6 GDPR.

[24] Si veda in tal senso anche quanto argomentato nelle Linee guida sulle decisioni individuali automatizzate e sulla profilazione ai fini del Regolamento 2016/679 (wp251rev.01), European Data Protection Board.

normativa privacy, devono essere attentamente esaminati e messi in pratica, congiuntamente a quelli previsti dall'IA ACT.

Il secondo principio oggetto di analisi è quello di liceità, che impone che il trattamento dei dati, nel cui concetto rientra anche la raccolta[25], avvenga lecitamente ovvero in presenza di una delle condizioni previste dal GDPR[26].

Trattasi di un aspetto di fondamentale importanza poiché, come si è già accennato, il funzionamento dei tali sistemi dipende dalla disponibilità di elevati volumi di dati, necessari all'addestramento degli algoritmi per l'elaborazione dei risultati richiesti dalla macchina.

Il reperimento di tali dati innesca delicate problematiche dal punto di vista privacy, soprattutto quando avviene attraverso la raccolta massiva di dati personali dal web, c.d. *web scraping*[27]. Si tratta di un aspetto sempre più al centro dell'attenzione delle Autorità di controllo privacy e dei principali stakeholders, anche a causa delle *querelle*[28] sorte su OpenAI, oggetto di successiva analisi, nonché in conseguenza della comunicazione della società Meta che informava gli utenti dell'avvio dell'utilizzo delle informazioni relative agli anni precedenti (post, immagini, messaggi ecc) per addestrare la propria IA, avvalendosi della base giuridica del legittimo interesse.

Nonostante il maturarsi di primi orientamenti da parte delle Autorità privacy europee[29], si rendeva necessario un più definito inquadramento della questione, tanto da spingere l'autorità privacy irlandese a chiedere un parere al Comitato Europeo per la protezione dei dati (EPDB), con riguardo, fra l'altro, all'adeguatezza dell'interesse legittimo come base giuridica per il trattamento dei dati personali nel contesto delle fasi di sviluppo e distribuzione di modelli di intelligenza artificiale.

---

[25] Art. 4, n. 2, GDPR.

[26] Art. 6, par. 1, GDPR: 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. Tale disposizione disciplina il trattamento dei dati comuni, per i dati particolari vigono le disposizioni dell'art.9 GDPR e per i dati relativi a condanne penali e giudiziarie valgono invece le indicazioni dell'art.10 GDPR Con riguardo all'ordinamento italiano, valgono poi le disposizioni integrative previste dal d. Lgs 196/2003 s.m.i..

[27] In tal senso anche U. Pagallo - J. Ciani Sciolla, A*natomy of web data scraping: ethics, standards, and the troubles of the law*, in *European Journal of Privacy Law & Technologies*, 1, 2023, 1 ss.

[28] L'associazione NOYB, al centro della cronaca per le sue azioni rispetto a temi fondamentali legati al trattamento dei dati personali, come quelle legate ai ricorsi a inerenti le condizioni di liceità per il trasferimento dei dati verso gli Stati Uniti (come nelle sentenze della CGUE n.ri C-362/14 e C-311/18, conosciute rispettivamente come c.d. Schrems I e Schrems II), ha recentemente comunicato di aver sollecitato 11 Autorità garanti privacy europee di fermare immediatamente l'abuso dei dati personali da parte di Meta per l'IA.

[29] A titolo esemplificativo, si vedano in tal senso il provvedimento del Garante Privacy italiano del 20 maggio 2024, (doc web n. 10020334), le linee guida della CNIL, Autorità privacy francese, del 2 luglio 2024.

Con il parere n. 28/2024[30], il Comitato ha richiamato gli importanti rischi derivanti dall'uso di tali tecnologie, evidenziando che «in relazione ai diritti e alle libertà fondamentali degli interessati, lo sviluppo e l'implementazione di modelli di IA possono comportare gravi rischi per i diritti tutelati dalla Carta dei diritti fondamentali dell'UE tra cui, a titolo esemplificativo ma non esaustivo, il diritto alla vita privata e familiare (articolo 7 Carta dell'UE) e il diritto alla protezione dei dati personali (articolo 8 Carta dell'UE)». Tali rischi possono verificarsi in qualsiasi fase del ciclo di sviluppo di tali modelli come durante la fase di sviluppo (come nel caso di raccolta dei dati personali contro la volontà degli interessati o senza che questi ne siano consapevoli) o di distribuzione (come ad esempio quando i dati personali vengono elaborati in violazione dei diritti degli interessati, o quando è possibile dedurre, accidentalmente o tramite attacchi, quali dati personali sono contenuti nel database di apprendimento) comportando conseguenze quali un rischio reputazionale, furto o frode di identità o un rischio per la sicurezza[31]. A tale categoria di interessi compromessi, se ne accompagna un'altra, menzionata nel punto successivo del parere[32] laddove si evidenzia che «la raccolta di dati su larga scala e indiscriminata da parte di modelli di IA nella fase di sviluppo potrebbe creare un senso di sorveglianza per gli interessati, soprattutto considerando le difficoltà nell'impedire che i dati pubblici vengano raccolti. Ciò potrebbe indurre gli individui ad autocensurarsi e presentare rischi di indebolimento della loro libertà di espressione (articolo 11 della Carta UE)», compromettendo l'autodeterminazione e il mantenimento del controllo sui propri dati personali, soprattutto quelli raccolti ed elaborati dal modello di IA. «Nel contesto dell'implementazione di un modello di IA, gli interessi delle persone possono includere, ma non sono limitati a, interessi nel mantenimento del controllo sui propri dati personali (ad esempio i dati elaborati una volta implementato il modello), interessi finanziari (ad esempio quando un modello di IA viene utilizzato dall'interessato per generare entrate o viene utilizzato da un individuo nel contesto della propria attività professionale), benefici personali (ad esempio quando un modello di IA viene utilizzato per migliorare l'accessibilità a determinati servizi) o interessi socioeconomici (ad esempio quando un modello di IA consente l'accesso a un'assistenza sanitaria migliore o facilita l'esercizio di un diritto fondamentale come l'accesso all'istruzione) ciò consentirà di comprendere chiaramente la realtà dei benefici e dei rischi da prendere in considerazione nel test di bilanciamento[33]. L'art. 6, par. 1, lett. f), del GDPR prevede che, nel valutare le diverse componenti nel contesto del test di bilanciamento, il titolare del trattamento debba tenere conto degli interessi, dei diritti fondamentali e delle libertà degli interessati. Gli interessi degli interessati sono quelli che possono essere interessati dal trattamento in questione. Interessi, diritti e libertà fondamentali degli interessati Inoltre, un modello di IA che raccomanda contenuti inappropriati a individui vulnerabili può presentare rischi per la loro salute mentale

[30] European Data Protection Board, Opinion of the board (art. 64) n. 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, del 17 dicembre 2024.

[31] Cfr. punto 79 del Parere.

[32] Cfr. punto 80 del Parere.

[33] Per i contenuti del c.d. test di bilanciamento, si vedano le indicazioni esplicative prescritte al punto 3.3.2 della citata Opinion 28/2024 dell'EDPB.

(art. 3(1) della Carta UE). In altri casi, l'impiego di modelli di IA può anche portare a conseguenze negative sul diritto dell'individuo a trovare un lavoro (art. 15 della Carta UE), ad esempio quando le domande di lavoro vengono preselezionate utilizzando un modello di IA»[34]. Allo stesso modo, un modello di IA potrebbe presentare rischi per il diritto alla non discriminazione (art. 21 della Carta UE), ad esempio in base a determinate caratteristiche personali (come la nazionalità o il genere), presentare rischi per la sicurezza degli individui o sulla loro integrità fisica o mentale[35].

Nel richiamare i principali adempimenti legati alla normativa privacy, fra cui quello di accountability, di liceità correttezza e trasparenza, di limitazione della finalità ed il principio di minimizzazione, fra i punti di maggiore interesse del parere vi è quello dell'individuazione della corretta base giuridica per il trattamento dei dati oggetto di addestramento. A tal proposito, il Comitato ricorda che non esiste una gerarchia tra le basi giuridiche previste dal GDPR e che spetta ai titolari il compito di individuare quella corretta. Pertanto, non è precluso scegliere tale base giuridica, certamente più favorita rispetto ad altre come ad esempio il consenso, ma tale scelta dev'essere preceduta da particolari cautele a tutela dei diritti degli interessati[36].

Nell'individuazione della base giuridica corretta, devono essere tenute in debita considerazione le prescrizioni in materia, anche derivanti dalle linee guida delle autorità privacy[37], valutando caso per caso le circostanze normative incidenti sul trattamento, l'estensione del margine di tutela riconosciuto all'interessato il bilanciamento dei diritti in esame.

Un caso molto recente che introduce sulla complessità di tale operazione è quello del Tribunale di Amburgo[38] che si è pronunciato sull'utilizzo delle opere dell'ingegno pubblicate su internet (nel caso di specie, una fotografia) per la creazione di set di dati utilizzati per l'addestramento dei sistemi di IA (c.d. *text and data mining* ovvero l'estrazione di testi e dati). La decisione, di significativo impatto sul piano europeo, ha disposto l'applicazione dell'esenzione del diritto di autore[39], in relazione alle fasi di pre-training

[34] A tale riguardo, altro possibile rischio derivante dal ricorso ai sistemi algoritmici è l'erroneità dei risultati offerti, con conseguenze particolarmente gravi quali l'adozione di decisioni errate a danno degli interessati nel contesto lavorativo. A tal proposito, può farsi menzione della sanzione comminata dal Garante per la protezione dei dati con riguardo alla sofferta discriminazione subita dai lavoratori di una società di consegne a domicilio, per effetto dell'ingiusto uso di un algoritmo, in assenza di qualsivoglia adempimento normativo.
Garante privacy - Provvedimento del 2 novembre 2024 (doc. web n. 10085455).

[35] Si richiama in tal senso anche il contenuto delle Linee guida EDPB 1/2024 sul trattamento dei dati personali in base all'articolo 6(1)(f) GDPR del 20 novembre 2024.

[36] Il parere richiama il c.d. test in tre fasi (1-identificazione dell'interesse legittimo perseguito dal titolare del trattamento o da una terza parte; 2. analisi della necessità del trattamento ai fini dell'interesse legittimo perseguito (anche denominato "test di necessità"); e 3. valutazione che l'interesse legittimo non sia superato dagli interessi o dai diritti e dalle libertà fondamentali degli interessati (anche denominato "test di bilanciamento").

[37] Ci si riferisce, ad esempio, alle linee guida dell'EDPB: n. 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati dell'8 ottobre 2019; Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 del 4 maggio 2020.

[38] Tribunale di Amburgo, Rif.: 310 O 227/23 (Kneschke/LAION).

[39] Art. 3 della direttiva (UE) 2019/790 sul diritto d'autore e sui diritti connessi nel mercato unico

algoritmico per gli scopi di ricerca scientifica. La conseguenza diretta è l'affievolimento della posizione degli interessati, pur titolari del diritto di proprietà, con la limitazione, di fatto, della possibilità di potersi opporre. Questo esempio esprime pienamente la complessità dell'iter decisione dei presupposti di liceità di trattamento e della necessaria attività di compliance.

A questo punto, appare interessante rilevare lo stato dell'arte nazionale attraverso i provvedimenti del Garante privacy italiano inerenti tali tematiche. Fra i casi più interessanti vi è quello inerente alla società statunitense Clearview[40], destinataria di una sanzione di 20 milioni di euro, per aver messo in atto un vero e proprio monitoraggio biometrico mediante un sistema di ricerca avanzato, basato su sistemi di ricerca IA. Secondo quanto contestato, i dati a supporto di tale servizio erano immagini di volti di persone di tutto il mondo, estratte tramite *web scarping* e incrociate con altre informazioni correlate, in assenza di adeguate misure di trasparenza e di una idonea base giuridica[41], nei termini già rappresentati. Fra gli altri e più recenti provvedimenti, certamente merita una specifica analisi quello a carico di OpenAI, per il notorio ChatGPT, di recentissima adozione e di sostanziale portata[42]. Tra i diversi punti alla base della contestazione, rientrano temi cruciali fra i quali: i requisiti di trasparenza in relazione alla raccolta e al trattamento dei dati utilizzati per l'addestramento degli algoritmi, sia degli utenti del servizio che degli interessati terzi nonché l'adeguata messa a disposizione dell'informativa privacy; la variazione della corretta base giuridica per il trattamento di tali dati, diversa da quella contrattuale che era stata individuata dalla società; messa a disposizione di adeguati strumenti per il diritto di opposizione dei dati acquisiti in sede di utilizzo degli algoritmi. Una menzione a parte merita un punto decisivo del provvedimento, relativo al mancato accertamento dell'età degli utenti per la potenziale esposizione di minori ai rischiosi trattamenti effettuati dagli algoritmi, per la cui delicatezza

digitale e che modifica le direttive 96/9/CE e 2001/29/CE: «Gli Stati membri dispongono un'eccezione ai diritti di cui all'articolo 5, lettera a), e all'articolo 7, paragrafo 1, della direttiva 96/9/CE, all'articolo 2 della direttiva 2001/29/CE, e all'articolo 15, paragrafo 1, della presente direttiva per le riproduzioni e le estrazioni effettuate da organismi di ricerca e istituti di tutela del patrimonio culturale ai fini dell'estrazione, per scopi di ricerca scientifica, di testo e di dati da opere o altri materiali cui essi hanno legalmente accesso».

[40] Garante privacy - Ordinanza ingiunzione nei confronti di Clearview AI del 10 febbraio 2022 (doc. web 9751362).

[41] Nella nota informativa del 20 maggio 2024, doc. web n. 10020334, Web scraping ed intelligenza artificiale generativa: nota informativa e possibili azioni di contrasto, il Garante privacy italiano esamina la complessa fattispecie del *webscraping* prescrivendo una serie di accorgimenti ai titolari di siti internet e piattaforme che utilizzano bot o sistemi di tale tipologia, indicando che «I gestori di siti web e di piattaforme online che rivestano al tempo stesso il ruolo di titolari del trattamento, fermi restando gli obblighi di pubblicità, accesso, riuso e di adozione delle misure di sicurezza previste dal GPD, dovrebbero valutare, caso per caso, quando risulti necessario, in conformità alla vigente disciplina, sottrarre i dati personali che trattano ai bot di terze parti mediante l'adozione di azioni di contrasto come quelle indicate che, sebbene non esaustive né per metodo, né per risultato, possono contenere gli effetti dello *scraping* finalizzato all'addestramento degli algoritmi di intelligenza artificiale generativa. In tal senso, si è anche esplicitamente espressa la Corte di Cassazione, I sez. civile, ordinanza 2021/14381, che ha statuito che nel caso di attività di elaborazioni algoritmiche (nel caso di specie, finalizzato all'elaborazione di profili reputazionali di persone fisiche o giuridiche, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivi dell'algoritmo e gli elementi di cui si compone, restino ignoti e non conoscibili da parte dell'interessato» e «la validità del trattamento è costituita dal consenso».

[42] Garante privacy, provvedimento del 27 novembre 2024 (doc. web 10077129).

nel prossimo paragrafo viene riservato un separato approfondimento.

3. IA e minori

Il coinvolgimento dei minori nel contesto tecnologico-digitale diviene ogni giorno più consistente, divenendo ormai una categoria fortemente utilizzatrice dei servizi della società dell'informazione[43]. I più recenti dati [44] dimostrano la forte attitudine di questa categoria all'utilizzo di internet, degli strumenti di identità digitale e degli acquisti online. Si tratta di una nuova categoria di utenti, nativamente inclini all'utilizzo di sistemi digitali ma ancora inesperti rispetto ai molteplici rischi nascosti nel contesto virtuale, sono destinatari di un livello più elevato di tutela[45], prevista dalla normativa internazionale e interna. Particolarmente significativi sono l'art. 24 della Carta dei diritti fondamentali[46], il considerando 38 del GDPR[47]. In generale l'approccio regolamentativo[48] verso questa specifica categoria di utenti è tutt'altro che semplice ma nel contesto dei servizi della società dell'informazione diventa ancora più impegnativo. L'art. 8 del GDPR chiarisce che nel contesto di tali servizi, «per i trattamenti basati sul consenso, 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». Per lo spazio normativo consentito al legislatore nazionale, in Italia l'età si riduce a 14 anni[49]. Per rendere effettiva questo adempimento, il secondo paragrafo dell'art.8 impone l'impegno «in ogni modo ragionevole» di verificare «che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione

[43] La definizione di servizi della società dell'informazione è prevista dall' 1, par. 1, lett. b), della direttiva (UE) 2015/1535.

[44] Report ISTAT 2023 Competenze digitali e caratteristiche socio-culturali della popolazione. Si veda inoltre il contenuto della relazione del Senato del 18 giugno 2024 al progetto di legge "in materia di minori e Internet, con riferimento particolare all'accesso alle piattaforme e all'uso dell'immagine dei minori" che l 73% dei minori (tra i 6 e i 17 anni) ha dichiarato di connettersi a Internet quotidianamente.

[45] G.Wang - J.Zhao - M. Van Kleek - N.Shadbolt, *Informing Age-Appropriate AI: Examining Principles and Practices of AI for Children,* in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22), Association for Computing Machinery,* 536, 2022, 1 ss.

[46] «I minori hanno diritto alla protezione e alle cure necessarie per il loro benessere. Essi possono esprimere liberamente la propria opinione» e che impone l'interesse preminente del minore. Si ricorda inoltre l'art. 24 dalla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, ulteriormente sviluppati nell'osservazione generale n. 25 della Convenzione delle Nazioni Unite dell'infanzia e dell'adolescenza per quanto riguarda l'ambiente digitale, che prevedono la necessità di tenere conto delle loro vulnerabilità e di fornire la protezione e l'assistenza necessarie al loro benessere.

[47] «I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali». In tal senso, I. A. Caggiano, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 1, 2018, 3 ss. e D. Marcello, *Il trattamento dei dati digitali del minore*, in *Actualidad Jurídica Iberoamericana,* 17 bis, 1305 ss.

[48] In prospettiva comparatistica, cfr. M.L. Chiarella, *Paradigmi della minore età. Opzioni e modelli di regolazione giuridica tra autonomia, tutela e responsabilità. Profili di diritto comparato*, Soveria Mannelli, 2008, *passim*.

[49] Art. 2 *quinquies,* d.lgs. 30 giugno 2003, n. 196.

delle tecnologie disponibili», che va inquadrato in combinazione con gli artt. 24[50] e 25[51] inerenti l'accountability del Titolare e i principi di privacy by design e by default.
Il recente provvedimento del Garante privacy su ChatGPT, di cui al paragrafo precedente, tocca il tema nodale dell'age verification (o age gate) per l'accesso ai servizi della società dell'informazione, che coinvolgono a pieno titolo anche quelli legati a sistemi o a modelli di intelligenza artificiale. La questione pendente in tale parere era quella di verificare se la società avesse provveduto ad implementare siffatti sistemi, sia rispetto ai nuovi utenti sia rispetto a quelli già registrati fino a quel momento, per impedire l'utilizzo del servizio a minori di 13 anni e per consentirlo ai minori di 18 anni solo previo valido consenso del titolare della responsabilità genitoriale.
Altro provvedimento del Garante privacy inerente il chatbot Replika[52] ci conduce ad un'ulteriore problematica fondamentale inerente i rischi della pervasività algoritmica a danno di categorie vulnerabili e, nello specifico, dei minori.
Il sistema conversazionale Replika si presentava come uno strumento di benessere, dotato di interfaccia scritta e vocale basata sull'intelligenza artificiale, capace di incidere positivamente sull'umore e sul benessere emotivo. Attraverso la comprensione dei pensieri e dei sentimenti dell'utente, Replika teneva traccia delle variazioni dell'umore e della capacità di controllo dello stress e dell'ansia, proponendosi quale supporto per razionalizzare gli obiettivi, socializzare nonché sul piano sentimentale.
Il sistema poteva essere configurato da semplice "amico virtuale" fino a partner romantico e mentore. Tuttavia, l'utilizzo pratico dimostrava l'insidiosa natura dell'algoritmo, strutturata in assenza di filtri per l'adattamento dei contenuti[53] in relazione all'età o alla tipologia dell'utente. Da alcuni test effettuati e poi diramati, nemmeno la dichiarazione esplicita della minore età attuava modifiche sostanziali ai contenuti delle conversazioni da parte del bot. Il cosiddetto "amico virtuale", a prescindere da un accertamento o

[50] Art.24 GDPR: «1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento».

[51] Art. 25 GDPR: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

[52] Garante Privacy, provvedimento del 2 febbraio 2023 (doc. web 9852214).

[53] Scorza: "Perché abbiamo bloccato Replika, minori a rischio" - Intervento di Guido Scorza, 4 febbraio 2023, in *garanteprivacy.it* (doc. web 9854194).

dai contenuti delle dichiarazioni, spingeva la conversazione verso contenuti sessuali sempre più espliciti, sollecitando l'invio di materiale pornografico e giungendo poi a proporre una versione del programma ancora più spinta, ma con l'obbligo di pagare un abbonamento mensile. Inoltre, in alcuni casi, il sistema giungeva a suggerire azioni e comportamenti inaccettabili e non consentiti, sul piano sia morale sia legale. In alcuni passaggi, la chat stimolava il suo interlocutore a compiere azioni fuori da ogni parametro, quali ad esempio il suicidio o l'uccisione del proprio genitore, argomentando e sostenendo tale indicazione nel caso in cui l'interlocutore umano esprimesse perplessità al riguardo. Il tutto con impatti devastanti su soggetti vulnerabili, come quelli affetti da particolari malattie anche psichiatriche e i minori.

Per il suo ruolo cruciale, il tema dell'*age verification* sta instancabilmente interessando i tavoli di lavoro delle principali autorità istituzionali coinvolte sul piano europeo[54] e nazionale[55].

Inoltre, anche le organizzazioni comunitarie[56] e internazionali stanno intensamente lavorando su questo tema, evidenziando la necessità e l'urgenza di un intervento risolutivo. L'Unicef[57] e World Economic Forum hanno presentato un documento di lavoro, aperto ai contributi degli stakeholders, che individua zone di vulnerabilità quali la privacy e la sicurezza, la possibile esposizione a contenuti dannosi, i rischi per la salute e l'identità, le implicazioni cognitive e psicologiche, i diritti di uguaglianza e di inclusione. Le mire europee, il cui assetto normativo globale verrà esaminato nel paragrafo successivo, consapevoli di tali esigenze, si esplicano su politiche e comunicazioni che insistono sulla creazione di un ambiente sicuro[58] in cui tali tipologie di utenti possano

---

[54] Vedasi in tal senso, a titolo esemplificativo: l'attività dell'Autorità garante spagnola AEPD Decálogo de
principios *Verificación de edad y protección de personas menores de edad ante contenidos inadecuados*, dicembre 2023 e l'annuncio dell'istituzione di una task force in Spagna per progettare un sistema di age verification, 12 marzo 2024; le indagini dell'autorità garante francese CNIL *Online age verification: balancing privacy and the protection of minors*; la strategia per i minori e il di condotta per i minori dell'Autorità garante inglese ICO; il piano di coordinamento fra Autorità garante privacy italiana e AGCOM.

[55] Si segnala la recente comunicazione del 7 ottobre 2024 in cui l'AGCOM ha approvato lo schema di regolamento che disciplina le modalità tecniche e di processo per l'accertamento della maggiore età degli utenti (*age assurance*, ovvero "garanzia dell'età", talvolta indicato come "*age verification*"), in attuazione della legge 13 novembre 2023, n. 159 ("Decreto Caivano"). A seguito di tale approvazione, dovrà essere istituito un tavolo tecnico di monitoraggio e analisi delle evoluzioni tecniche, normative e regolamentari in materia di sistemi di age assurance.

[56] La tematica coincide con un'altra normativa fondamentale nel piano strategico UE, il Regolamento (UE) 2022/2065 del Parlamento Europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali), DSA, che mira a creare un ambiente digitale inclusivo e sicuro per tutti gli utenti, specialmente per i minori. In tale contesto, la Commissione ha istituito una specifica task force on Age Verification, cui partecipa, per l'Italia, l'Autorità Garante per le Garanzie nelle Comunicazioni. L'Autorità è impegnata su tale tema in forza delle disposizioni di cui al c. 3 dell'art. 13-bis del decreto-legge n. 123/2023 che ha appunto demandato ad AGCOM il compito di individuare le modalità tecniche e di processo che i soggetti individuati dalla norma sono tenuti ad adottare per l'accertamento della maggiore età degli utenti.

[57] Unicef e World Economic Forum,in unicef.org Children and AI Where are the opportunities and risks?.

[58] Comunicazione Un decennio digitale per bambini e giovani: la nuova strategia europea per un internet migliore per i ragazzi (BIK+); Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (cap.V).

interagire in sicurezza.

4. IA e scenario normativo europeo e nazionale di riferimento

La regolamentazione dell'IA rientra fra le priorità della Commissione Europea [59], dalla portata rivoluzionaria ed innovativa. A seguito della proposta della Commissione del 2021[60] e di un iter normativo tutt'altro che in discesa, il legislatore europeo ha conseguito il primato mondiale nella regolamentazione dei principi strutturali di una materia estremamente complessa e soprattutto in continuo divenire. L'AI Act si inserisce nel percorso individuato dal legislatore comunitario per dare attuazione alla strategia industriale europea[61], pilastro strutturale dell'azione della Commissione, per puntare[62] ad accrescere la leadership, l'indipendenza in campo tecnologico e il rafforzamento del mercato unico[63].

Con questa normativa, l'Europa punta a completare tale quadro strategico per beneficiare dell'enorme potenziale economico e commerciale derivante dallo sviluppo e dall'utilizzo di queste tecnologie[64]. Tale piano è reso ancora più efficace dal crescente volume di dati[65], linfa vitale dello sviluppo economico, nel contesto pubblico e privato, per la creazione di nuovi prodotti e servizi, l'incremento della produttività, risorsa ne-

[59] Le priorità della Commissione Europea 2019-2024, .

[60] Proposta di Regolamento del Parlamento 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.

[61] L'analisi elaborata alla base della (COM(2020) 66 final) evidenzia come la Commissione miri alla supremazia economica unionale anche puntando all'eliminazione delle dipendenze strategiche relativi a beni, prodotti o servizi dal forte impatto economico con basso potenziale di diversificazione e e sostituzione nella produzione UE, come quello del settore tecnologico anche in ambito infrastrutturale.

[62] Tale priorità rientra nel piano 2019-2024 della Commissione Europea e ha portato all'adozione di altri regolamenti di elevatissima portata fra cui il Regolamento sui chip (Regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio del 13 settembre 2023 che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il Regolamento (UE) 2021/694 (Regolamento sui chip) e Regolamento (UE) 2024/1252 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro atto a garantire un approvvigionamento sicuro e sostenibile di materie prime critiche e che modifica i regolamenti (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1724 e (UE) 2019/1020.

[63] Commissione europea, Direzione generale della Comunicazione, Mercato unico, Ufficio delle pubblicazioni, 2020

[64] In tal senso è fondamentale evidenziare come l'impostazione adottata sia conseguenza delle attente analisi realizzate nella fase preparatoria della normativa, come ad esempio il *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia* della Commissione Europea, legato alla creazione di due principali elementi costitutivi: ecosistema di eccellenza, nell'intera catena di valore dalla progettazione dei sistemi fino all'adozione dei medesimi da parte degli utilizzatori. ecosistema di fiducia, basato appunto sul rispetto delle normative vigenti, per incentivare l'utilizzo di tali sistemi da parte di cittadini e imprese.

[65] Come emerge dalle stime della Commissione Europea, il volume dei dati è in costante crescita: da 33 zettabyte nel 2018 a 175 zettabyte previsti per il 2025 con un corrispondente aumento del 530% e con un valore stimato di 829 miliardi di euro.

cessaria per il *training* e il funzionamento dei sistemi di intelligenza artificiale[66].
Grazie a questo Regolamento, vengono finalmente consolidate le classificazioni dei sistemi di IA, classificando la vasta categoria di soggetti coinvolti (fornitori; deployer; rappresentante autorizzato; importatore; distributore; operatore[67]) ed improntando un approccio basato sul rischio cui vengono collegati specifici obblighi di trasparenza.
La scelta adottata è di elevatissimo pregio, prevedendo il divieto per sistemi c.d. a rischio inaccettabile [68], strutturando delle cautele e degli adempimenti proporzionali per quelli cui invece corrispondono livelli di rischio alto[69], limitato e minimo o nullo.
Lo scopo fondamentale dell'AI Act[70] è di contribuire al miglioramento del mercato interno attraverso un quadro giuridico uniforme per disciplinare lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'IA antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, la tutela dei valori democratici e di protezione dei dati personali[71], al riparto dagli effetti

[66] Su tale strategia vedasi come nella citata European Data Strategy, la Commissione Europea abbia strutturato una serie di interventi normativi mirati alla supremazia europea in materia di dati, personali e non.

[67] Cfr. definizioni art. 3, parr.3-8), AI Act.

[68] Art. 5 AI Act, che prevede l'esclusione per sistemi la cui attività possa configurare: «sfruttamento delle vulnerabilità delle persone, manipolazione e utilizzo di tecniche subliminali; punteggio sociale per finalità pubbliche e private; attività di polizia predittiva individuale basate unicamente sulla profilazione delle persone;
scraping non mirato di immagini facciali da internet o telecamere a circuito chiuso per la creazione o l'ampliamento di banche dati; riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota);
categorizzazione biometrica delle persone fisiche sulla base di dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche o orientamento sessuale. Sarà ancora possibile etichettare o filtrare set di dati e categorizzare i dati nell'ambito delle attività di contrasto; identificazione biometrica remota in tempo reale in spazi accessibili al pubblico da parte delle autorità di contrasto, fatte salve limitate eccezioni». Schema riepilogativo del PE.

[69] Art. 6 AI Act.

[70] Considerando 1 AI Act. Vedasi anche le stesse indicazioni nel considerando 2, che testualmente indica «Il presente regolamento dovrebbe essere applicato conformemente ai valori dell'Unione sanciti dalla Carta agevolando la protezione delle persone fisiche, delle imprese, della democrazia e dello Stato di diritto e la protezione dell'ambiente, promuovendo nel contempo l'innovazione e l'occupazione e rendendo l'Unione un leader nell'adozione di un'IA affidabile» e nell'art.1.

[71] C. Novelli - G. Sandri, *Digital Democracy in the Age of Artificial Intelligence*, in *SSRN Electronic Journal,* 1, 2024, 1 ss., in cui viene offerto un focus, non rientrante nel presente contributo, inerente i possibili rischi in un particolare contesto cruciale con riguardo agli aspetti democratici quale è quello elettorale. In questo senso è molto interessante l'inciso in cui viene indicato (spec. 19) che «Se da un lato l'intelligenza artificiale può migliorare l'efficienza e la personalizzazione delle campagne, dall'altro comporta rischi significativi. La disinformazione generata dall'intelligenza artificiale e i dilemmi etici sono problemi prevalenti, di cui i deepfake sono un esempio notevole. Questi video realistici ma falsi possono manipolare la percezione del pubblico e diffondere informazioni false. Possono quindi essere utilizzati per promuovere una competizione non etica, se non illegale, tra i candidati». Altro passaggio particolarmente significativo è quello del ruolo dell'IA nelle piattaforme, laddove chiarisce (spec. 21) «Le piattaforme digitali hanno rimodellato la partecipazione politica, offrendo nuove strade per

nocivi dei sistemi di IA nell'Unione.

Il Regolamento non assume solo il primato nel disciplinare una materia obiettivamente complessa, ma anche di farlo in maniera etica[72] e responsabile, affrontando fin da subito un tema estremamente fondamentale quale è quello della tutela dei diritti fondamentali delle persone. Il perché di questo primo obiettivo è chiaramente spiegato nel considerando 7, laddove viene chiarito che «L'IA (...) può nel contempo, a seconda delle circostanze relative alla sua applicazione, al suo utilizzo e al suo livello di sviluppo tecnologico specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale, compreso il pregiudizio fisico, psicologico, sociale o economico».

Ciò si verifica quando tale tecnologia venga utilizzata impropriamente trasformandosi, ad esempio, in un potente strumento legato a pratiche di manipolazione, sfruttamento e controllo sociale[73], al fine di indurre le persone a comportamenti indesiderati o ad alterarne il processo decisionale e la libera scelta. Si tratta di pratiche particolarmente pervasive, contrarie ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e ai diritti dei minori, fra cui quelli consacrati nel Trattato sull'Unione Europea (TUE).

A completare il quadro europeo è intervenuta recentemente la Convenzione quadro sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto, adottata il 17 maggio 2024 dal Consiglio d'Europa[74]. Il testo definitivo è giunto a seguito di un lungo lavoro di elaborazione e aperto alla firma a partire dal 5 settembre 2024, che ha coinvolto sia gli stati membri del Consiglio d'Europa che stati non membri, rendendo

l'impegno civico e la difesa. L'intelligenza artificiale migliora questi processi attraverso la comunicazione personalizzata, il monitoraggio in tempo reale e l'analisi dei dati, ma pone anche rischi di manipolazione e disinformazione. L'intelligenza artificiale migliora l'efficienza e l'integrità dei moderni processi elettorali attraverso la registrazione degli elettori, il voto elettronico e la tabulazione dei risultati. Tuttavia, solleva anche problemi di privacy, sicurezza e fiducia. Le capacità predittive dell'IA nel comportamento elettorale introducono nuove dinamiche nella competizione politica, sollevando preoccupazioni etiche sulla manipolazione e sulla legittimità democratica».

[72] Riguardo la questione sull'etica e sulla responsabilità dell'IA, fondamentale è stato il contributo della *soft law* sviluppatasi nel corso dei lavori preparatori dell'AI Act. In particolare, è doveroso menzionare l'elaborazione dei principi etici di cui al già menzionato contributo "Orientamenti etici per un'IA affidabile", accolto poi anche dalla Commissione nella comunicazione dell'8 aprile 2019 COM(2019) 168 final, precisamente riguardo i quattro principi etici (rispetto autonomia umana, prevenzione dei danni, equità, esplicabilità) e dei sette requisiti fondamentali (intervento e sorveglianza umana, robustezza tecnica e sicurezza, riservatezza e governance dei dati, trasparenza, diversità e non discriminazione, benessere sociale e ambientale, accountability).

[73] Considerando 28 AI Act.

[74] Testo ufficiale della Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto. Vedasi il comunicato stampa del Consiglio d'Europa del 17 maggio 2024 e in particolare quanto ha dichiarato la Segretaria generale del Consiglio d'Europa, Marija Pejčinović: «La Convezione quadro sull'intelligenza artificiale è un trattato globale unico nel suo genere, che assicurerà che l'intelligenza artificiale rispetti i diritti delle persone. È una risposta alla necessità di disporre di una norma di diritto internazionale sostenuta da Stati di diversi continenti uniti da valori comuni, che consenta di trarre vantaggio dall'intelligenza artificiale, riducendo al contempo i rischi che questa presenta. Con questo nuovo trattato, intendiamo assicurare un utilizzo responsabile dell'IA che rispetti i diritti umani, la democrazia e lo Stato di diritto».

il trattato un elemento unificante sulla protezione mondiale dei diritti umani nei sistemi di IA.

Senza interferire con le disposizioni del Regolamento, dal contenuto più legato ad aspetti economici e tecnici, la Convenzione incentiva in tutto il ciclo di vita dei sistemi di IA l'applicazione dei principi in materia di diritti umani quali: la tutela della dignità umana e dell'autonomia individuale; la trasparenza e il controllo, fondamentali nel contrasto all'opacità e all'autonomia propria dei sistemi algoritmici; il principio di responsabilità dei soggetti che detengono il controllo delle varie fasi del ciclo di vita dei sistemi di IA; l'eguaglianza e la non discriminazione, contro i c.d. "*bias* cognitivi"; la garanzia dell'efficacia degli strumenti di tutela; l'affidabilità dei sistemi; le garanzie per un sistema sicuro per lo sviluppo, la sperimentazione e i test di sistemi di intelligenza artificiale.

A completamento di questo quadro, la Convenzione prevede poi una strutturata serie di rimedi per gli interessati danneggiati da tali sistemi e un obbligo di alfabetizzazione digitale per promuovere un utilizzo consapevole degli strumenti digitali e di IA.

Con riguardo allo scenario nazionale, il quadro dei valori è individuabile nel dettato della Costituzione italiana, soprattutto in alcune specifiche definizioni dalla grande portata nel contesto in esame[75]. Nel novero degli interessi in gioco e dei rischi delle parti, meritano una speciale menzione gli artt. 15 e 21 Cost., inerenti, rispettivamente, i diritti alla riservatezza e alla libertà di espressione, l'art.3 sul diritto di uguaglianza[76], l'art. 32 sul diritto alla salute e l'art. 4 sul diritto al lavoro[77], parziali tasselli del composito quadro di diritti fondamentali possibilmente coinvolti dai rischi concreti emergenti dall'utilizzo dei sistemi di IA. Separata menzione certamente merita l'art. 2, che recita «La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale» rappresentando un fattivo impegno statale[78].

Evidentemente, proprio in forza di tale responsabilizzazione, l'Italia è stata il primo stato ad accompagnare sul piano interno le previsioni dell'AI Act, ancora prima dell'approvazione dell'AI Act, procedendo all'emanazione di uno schema di disegno di legge

[75] Per un'articolata disamina su tutti i diritti coinvolti, R. Razzante, *AI e tutela dei diritti fondamentali*, in *Dirittifondamentali.it,* 1, 2024, 133 ss.

[76] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal - Rivista di BioDiritto* ,1, 2019, 63 ss.

[77] Sui possibili impatti rispetto al contesto lavorativo, L. Rinaldi, *Intelligenza artificiale, diritti e doveri nella Costituzione italiana*, in *DPCE online,* 2022, 1, 201 ss., laddove rappresenta il duplice rischio inerente la perdita da chance lavorative per effetto della modernizzazione tecnologica dei contesti lavorativi e le possibili discriminazioni derivanti da un'ingiustizia algoritmica.

[78] La nostra Costituzione, attraverso il più articolato complesso di diritti riconosciuti e garantiti, riesce, a parere di chi scrive, ad abbracciare le nuove esigenze derivanti dal rinnovato contesto tecnologico rappresentato nel presente contributo. Tuttavia sono molto accese in dottrina discussioni inerenti l'effettiva efficacia dell'insieme di tutele offerte dalla Costituzione e l'eventuale necessità di un nuovo intervento integrativo. In questo senso, si veda, fra gli altri, A. Adinolfi, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE* ,15, 2023, 321 ss. e O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet,* in questa *Rivista*, 2018, 1, 48 ss.

recante disposizioni e deleghe in materia di intelligenza artificiale (DDL)[79]. Il DDL si propone l'obiettivo di individuare un bilanciamento tra opportunità e rischi attraverso una previsione che promuova «l'utilizzo di tali tecnologie per il miglioramento delle condizioni di vita dei cittadini e della coesione sociale e, dall'altro, fornisca soluzioni per la gestione del rischio fondate sulla visione antropocentrica»[80].

Senza sovrapporsi all'AI Act, l'obiettivo del DDL è di dettare[81] una normativa nazionale che predisponga un sistema di principi, governance e misure specifiche adatte al contesto italiano per cogliere tutte le opportunità dell'intelligenza artificiale. Gli obiettivi generali[82] sono «il rafforzamento della competitività italiana e garantire ai cittadini italiani l'uso affidabile e responsabile dell'IA, assicurando la supervisione umana in ogni fase di sviluppo e di utilizzo dei sistemi IA e la tutela dei diritti fondamentali».

In particolare, lo scopo è di assicurare che l'utilizzo dell'IA non comporti una lesione dei diritti fondamentali dell'individuo, ai sensi dell'art. 2 Cost.[83]. Il DDL si apre con un ambito di definizioni, individuando i principi applicabili all'IA, procedendo poi con norme specifiche sull'utilizzo dell'IA nel settore sanitario, nel diritto del lavoro, nelle professioni intellettuali, nella PA e nell'attività giudiziaria. Altro aspetto fondamentale è l'individuazione dell'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN), quali autorità di controllo ed espletare le funzioni richieste dall'AI Act, anche finalizzate a dare sostegno e impulso alla realizzazione di sistemi di IA sul piano interno, nei termini e nelle competenze individuati nell'art. 18 DDL[84].

---

[79] Disegno di legge presentato dal Presidente del Consiglio dei Ministri (Meloni) e dal Ministro della giustizia (Nordio) comunicato alla Presidenza il 20 maggio 2024 Disposizioni e delega al Governo in materia di intelligenza artificiale, testo DDL.

[80] Relazione del DDL, 3.

[81] Analisi del quadro normativo in materia di Intelligenza artificiale (D.D.L. IA e regolamento (UE) su IA) Focus IA.

[82] Premessa Relazione del DDL, cit.

[83] Punto 4) Analisi d'impatto della regolamentazione, relativa al DDL, ivi, 16.

[84] Art. 18 DDL: «a) l'AgID è responsabile di promuovere l'innovazione e lo sviluppo dell'intelligenza artificiale, fatto salvo quanto previsto dalla lettera b). L'AgID provvede, altresì, a definire le procedure e a 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, secondo quanto previsto dalla normativa nazionale e dell'Unione europea.
b) l'ACN, anche ai fini di assicurare la tutela della cybersicurezza, come definita dall'articolo 1, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale, secondo quanto previsto dalla normativa nazionale e dell'Unione europea. L'ACN è, altresì, responsabile per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza. c) l'AgID e l'ACN, ciascuna per quanto di rispettiva competenza, assicurano l'istituzione e la gestione congiunta di spazi di sperimentazione finalizzati alla realizzazione di sistemi di intelligenza artificiale conformi alla normativa nazionale e dell'Unione europea, sentito il Ministero della difesa per gli aspetti relativi ai sistemi di intelligenza artificiale impiegabili in chiave duale.
2. Le Autorità nazionali per l'intelligenza artificiale di cui al comma 1 assicurano il coordinamento e la collaborazione con le altre pubbliche amministrazioni e le autorità indipendenti, nonché ogni opportuno raccordo tra loro per l'esercizio delle funzioni di cui al presente articolo. A quest'ultimo fine, presso la Presidenza del Consiglio dei ministri è istituito un Comitato di coordinamento, composto dai direttori generali delle due citate Agenzie e dal capo del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri medesima».

Tale articolo, indica espressamente[85] che restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali, per l'assoluta indipendenza e verticalità della materia sul trattamento dei dati personali.

A tal proposito, è interessante richiamare il parere[86] reso dal Garante privacy sull'emanazione del DDL, con particolare riguardo agli impatti privacy derivanti dal medesimo. Il contenuto del parere è positivo ma rimane condizionato alla richiesta di più intense garanzie a tutela dei dati personali, evidenziando quindi la necessità di una maggiore attenzione su tale aspetto. Alcuni punti di tale parere meritano una separata menzione, anche ai fini del presente contributo, per evidenziare come il percorso verso l'equilibrio delle parti in gioco non possa ancora definirsi raggiunto.

Il primo aspetto che merita una particolare evidenza, anche alla luce della problematica emersa nel paragrafo precedente, riguarda la sicurezza dei minori rispetto all'utilizzo di tali tecnologie che giustifica la richiesta di riferimenti a sistemi di *age verification* per garantire limitazioni o divieti all'uso dei sistemi di IA per tale categoria. Poiché ai sensi del DDL IA[87], per il trattamento dei dati personali connessi all'utilizzo di sistemi di IA è richiesto il consenso del minore ultraquattordicenne, soglia allineata alle disposizioni dell'art. 2 *quinquies* del D.Lgs 193/2003 s.m.i., il Garante raccomanda di integrare tale previsione con un opportuno riferimento a misure idonee a garantire adeguati sistemi di verifica dell'età, per evitare che la soglia indicata possa essere in qualche modo elusa. A tal proposito, sono state richiamate le misure adottate ai sensi dell'art. 13-bis, c. 3, d.l. 123 del 2023, che prevede l'adozione di modalità tecniche da parte dell'Autorità per le garanzie delle comunicazioni (AGCOM) previo parere del Garante privacy, per l'accertamento della maggiore età degli utenti e il rispetto della minimizzazione dei dati[88], di cui si è già fatto cenno nel paragrafo precedente.

Ulteriore argomento particolarmente interessante del parere reso al Garante in relazione al DDL, riguarda la delicatissima categoria dei dati sanitari, sui quali l'autorità invoca maggiori cautele, un collegamento più sistematico fra l'art. 7 del DDL e le garanzie previste dall'art. 9 GDPR, nonché la predisposizione al futuro allineamento con lo Spazio Europeo dei dati sanitari[89]. Al di là delle ulteriori argomentazioni indicate in tale parere, anche in questo caso, come per gli altri ambiti di trattamento ivi menzionati, sembra che la questione necessiti di ulteriore consapevolezza e maggiore coordinamento per la migliore tutela degli interessati.

Con riguardo alla compatibilità e non contrasto della normativa in esame è intervenuta la Commissione Europea, che ha inviato un parere circostanziato (C(2024) 7814) al

---

85 Cfr. art. 18, c. 3, DDL, ivi, 16.

86 Garante privacy, *Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale*, 2 agosto 2024 (doc. web 10043532).

87 Cfr. art. 4, c. 4, DDL, ivi, 16.

88 In tal senso, viene richiamato il fondamentale principio di minimizzazione dei dati espresso dall'art. 5, par. 1, lett. c), GDPR per il quale i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati».

89 Nel caso poi di utilizzo di sistemi di IA in ambito sanitario ad alto rischio, il Garante ha chiesto di indicare particolari limitazioni per l'utilizzo dei dati (conservazione, divieto di trasmissione, trasferimento o comunicazione) e la preferenza per l'uso di dati sintetici o anonimi. Con riguardo allo Spazio Europeo sui dati sanitari, si veda la specifica sezione informativa della Commissione Europea.

Governo italiano[90], contenente l'invito a rimuovere alcune discrepanze rispetto all'AI Act. In particolare, la Commissione, ha messo in evidenza delle sostanziali divergenze sia di tipo terminologico[91], che di tipo sostanziale[92], soffermandosi inoltre sul punto inerente la designazione delle autorità nazionali competenti, ai sensi degli artt. 18 e 22 del DDL e previste dall'art.70 dell'IA ACT, questione al centro del dibattito nazionale per il quadro di "diffusa" governance[93] impostato dal DDL in esame. Su tale aspetto, la Commissione ha evidenziato che per la designazione è richiesto lo «stesso livello di indipendenza previsto dalla direttiva (UE) 2016/680[94] per le autorità preposte alla

[90] Il testo del menzionato parere non è reperibile tramite le fonti pubbliche, l'analisi è stata svolta in base alla sintesi diramata dal Senato, 4ª Commissione permanente - Resoconto sommario n. 214 del 27/11/2024.

[91] Cfr. sintesi del Senato: «- suggerisce di inserire all'articolo 1 un riferimento specifico al regolamento europeo sull'intelligenza artificiale (IA); - in riferimento alle definizioni di cui all'articolo 2, segnala che quella di "modelli di IA" differisce da quella del regolamento europeo sull'IA e che, comunque, la norma nazionale dovrebbe limitarsi a fare riferimento alle definizioni già contenute nel regolamento senza replicarle; - in riferimento all'articolo 5, comma 1, lettera d), del disegno di legge, la Commissione europea invita a chiarire il concetto di dati "critici", limitandolo ai casi in cui sono in gioco interessi di sicurezza nazionale».

[92] Cfr. sintesi del Senato: «- in riferimento all'articolo 7, comma 3, che stabilisce obblighi informativi per gli operatori di sistemi di IA in ambito sanitario e di visibilità nei confronti dei pazienti, la Commissione europea ritiene opportuno che gli obblighi informativi dell'operatore a beneficio del paziente debbano limitarsi esclusivamente all'impiego dell'IA, senza estenderli ai "vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo delle nuove tecnologie" e alle "informazioni sulla logica decisionale utilizzata", per non andare oltre quanto previsto dal regolamento europeo sull'IA;
- in riferimento all'articolo 12, sull'uso dei sistemi di IA nell'ambito delle professioni intellettuali, la Commissione europea invita a eliminare qualsiasi restrizione nell'uso di sistemi di IA non "ad alto rischio", per non porsi in contrasto con il regolamento;
- in riferimento all'articolo 14, che consente l'utilizzo dei sistemi di IA nell'attività giudiziaria solo per l'organizzazione e semplificazione del lavoro giudiziario e per la ricerca giurisprudenziale e dottrinale, la Commissione europea invita ad allineare tale norma, all'articolo 6, paragrafo 3, del regolamento sull'IA, che non esclude la possibilità di utilizzare sistemi di IA pur classificati come "ad alto rischio" ma che "non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, o non influenzano materialmente il risultato del processo decisionale";- in riferimento alla delega di cui al comma 3 dell'articolo 22, volta all'organica definizione della disciplina nei casi di uso di sistemi di intelligenza artificiale per finalità illecite, la Commissione europea ricorda che l'articolo 99 del regolamento sull'IA prevede specifiche disposizioni in materia di sanzioni per violazioni del regolamento da parte degli operatori;- in riferimento all'articolo 23, comma 1, lettera b), del disegno di legge, secondo cui i contenuti prodotti dai sistemi di intelligenza artificiale devono essere resi chiaramente riconoscibili mediante un segno visibile con l'acronimo "IA" o mediante un annuncio audio, la Commissione europea ritiene che tale obbligo si sovrapponga e vada oltre gli obblighi di cui all'articolo 50, paragrafi 2 e 4, del regolamento sull'IA;- in riferimento all'articolo 23, comma 1, lettera c), del disegno di legge, che impone ai fornitori di piattaforme per la condivisione di video 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 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, del regolamento sull'IA».

[93] M. Cappai, *Intelligenza artificiale e protezione dei dati personali nel d.d.l. n. 1146: quale governance nazionale?*, in *Federalismi.it*, 30, 2024, 186 ss., che differenzia la governance imposta regolamento IA, affidata alle autorità puntualmente individuate nel DDL (AgID, ACN e Garante privacy) e la governance del fenomeno IA nel suo complesso, definendola a "geometria variabile". Il fattore collusivo è rappresentato dalle indicazioni del Garante, contenute nel citato parere del 2 agosto 2024, che in più punti ha richiamato la necessità di integrare maggiori competenze in tale ambito.

[94] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa 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». I contenuti del parere, del tutto condivisibili, riflettono l'inevitabile immaturità del testo rispetto ai contenuti dell'AI Act e la necessità di maggiore integrazione, soprattutto con riguardo alla competenza delle autorità di controllo e a questioni di natura sostanziale relative alla giustizia e ai dati sanitari, sui quali il DDL deve puntare ad un maggiore coordinamento con il quadro europeo.

5. Conclusioni

L'analisi passata in rassegna rappresenta un quadro certamente innovativo e foriero di grandi opportunità. Il contesto tecnologico europeo ha abbracciato questa rivoluzione che vedrà lo sviluppo dell'IA, con benefici, come si è visto, in ogni contesto socio-economico. L'AI Act è stato predisposto appositamente per creare queste condizioni e per consentire all'Europa di cogliere questa sfida, attraverso la predisposizione di una regolamentazione coerente e articolata, che ne consenta l'efficace e rispettosa crescita. Gli aspetti etici e il rispetto dei diritti fondamentali sono fra i pilastri strutturali di tale normativa, ma gli estremi rischi che sono stati illustrati nel contributo dimostrano che l'adozione dell'AI Act non rappresenti la conclusione quanto l'avvio di un nuovo percorso. Prova ne sono l'elaborazione della Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo stato di diritto, intervenuta per disciplinare verticalmente a tali aspetti, nonché gli altri interventi da parte degli stati, come l'Italia, in cui si è voluto intervenire in maniera più incisiva per armonizzare le peculiarità nazionali. Tante questioni sono ancora aperte e le soluzioni adottate ancora aperte all'interpretazione.

Nel rapporto rischio-beneficio, probabilmente l'asticella è ancora disposta verso il primo. Per superare tale sbilanciamento, la prima soluzione da adottare in via prioritaria potrebbe essere di seguire il percorso indicato dallo stesso AI Act, che individua quale strumento risolutivo l'alfabetizzazione digitale[95]. Il considerando 20 infatti indica che «al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA». Si tratta quindi di uno strumento[96], attuato anche attraverso linee guida e

protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, attuata nell'ordinamento italiano con il decreto legislativo del 18 maggio 2018, n. 51.

[95] Art. 3, n. 56, AI Act: «le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare». L'alfabetizzazione è imposta quale obbligo a fornitori e *deployer* all'art. 4 AI Act.

[96] Art. 65 AI Act e considerando 20: «è affidato al Consiglio per l'IA il compito specifico di promuovere azioni e strumenti per l'alfabetizzazione, sensibilizzazione in materia di IA e la comprensione dei

codici di condotta[97] adottati di concerto con le istituzioni europee, che possa giungere nella forma più pratica e comprensibile ai rispettivi destinatari riguardo alle caratteristiche delle applicazioni di IA, alle misure da adottare, alle modalità per comprendere e selezionare gli output e comprendere l'incidenza della decisione di un sistema di IA. Secondo quello che viene indicato nel Regolamento, la piena attuazione delle misure di alfabetizzazione di IA potrebbe favorevolmente contribuire a migliorare le condizioni di lavoro e sostenere il percorso dell'UE verso un IA affidabile e sicura.
Si tratta di un percorso affascinante e ambizioso, ben tracciato ma certamente ancora in salita. Che vale certamente la pena di percorrere e di incoraggiare attraverso consapevolezza e coinvolgimento da parte di tutti i soggetti coinvolti.

benefici, dei rischi, delle garanzie, dei diritti e degli obblighi in relazione all'uso dei sistemi di IA».

[97] G7: inizia la fase Pilota per il monitoraggio del Codice di Condotta sull'Intelligenza Artificiale, Dipartimento della trasformazione digitale, 24 luglio 2024.