L’intelligenza artificiale tra regolamentazione e innovazione. Sfide, compromessi e criticità della corsa alla *governance* europea

21/07/2023 PRIVACY E CYBERSECURITY, DIRITTO EUROPEO E DELLA CONCORRENZA, PROSPETTIVE

Roberto A. Jacchia
Federico Aluigi

Che cosa si intende per Intelligenza Artificiale?

L’intelligenza artificiale è l’abilità di una macchina di mostrare capacità umane quali il ragionamento, l’apprendimento, la pianificazione e la creatività. Tali abilità si manifestano tramite tecnologie che consentono di simulare i processi dell’intelligenza umana attraverso la creazione e l'applicazione di algoritmi integrati in un ambiente di calcolo dinamico.

Come viene regolata l’Intelligenza Artificiale nell’Unione Europea?

In seguito ad una serie di iniziative di *soft law* intraprese negli ultimi anni, in data 21 aprile 2021 la Commissione Europea ha presentato una proposta di Regolamento (c.d. “*AI Act*”) con l’obbiettivo di plasmare la legislazione europea sull’intelligenza artificiale (“IA”), armonizzando la normativa applicabile e promuovendo l’innovazione, la sicurezza e la tutela dei diritti individuali[1]. Il razionale del Regolamento consiste nel garantire che tutti i sistemi di IA utilizzati siano sicuri, trasparenti, etici, imparziali e sotto il controllo umano, rafforzando così la

[1] Com. Comm. COM (2021) 26 final del 21.04.2021, Proposal for a Regulation of the European Parliament and of The Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.
Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.

fiducia dei cittadini nel loro utilizzo[2]. Il Regolamento si applicherà sia agli operatori europei, sia agli utilizzatori e fornitori di sistemi IA stabiliti fuori dall'Unione, qualora l'*output* dei sistemi sviluppati o utilizzati venga impiegato al suo interno. Non si applicherà, invece, alle autorità pubbliche in Paesi terzi e alle organizzazioni internazionali, ma solo se utilizzano sistemi di IA nell'ambito di programmi di cooperazione giudiziaria o investigativa (con l'Unione o con uno Stato Membro).

Cos'è il c.d. "*risk-based approach*" e come si articola?

La proposta della Commissione prevede una classificazione in base al rischio su quattro livelli, basati sulle ripercussioni che potrebbe avere l'IA sulla sicurezza delle persone e dei diritti fondamentali: maggiore l'invasività, maggiori i presidi.

Al primo livello si collocano i sistemi di IA a rischio inaccettabile[3], la cui commercializzazione e i cui possibili utilizzi sono banditi in modo pressoché assoluto dal Regolamento, quali, tra gli altri: i) quelli che utilizzano tecniche subliminali per influenzare indebitamente in maniera sostanziale il comportamento di una persona, così causandole, o potendole causare, danni fisici o psichici, oppure causarne ad altri; ii) quelli che sfruttano la vulnerabilità legata all'età o ad una disabilità di uno specifico gruppo di persone al fine di influenzare indebitamente il comportamento di una persona appartenente a tale gruppo; iii) l'uso di sistemi di valutazione e classificazione dell'affidabilità delle persone fisiche sulla base del comportamento sociale o delle caratteristiche personali, con relativi punteggi (c.d. *social scoring*) attribuiti dalle autorità pubbliche o da chi agisce per loro conto; iv) l'uso in tempo reale di sistemi di identificazione biometrica da remoto in luoghi accessibili al pubblico.

Al secondo livello si collocano i sistemi di IA a rischio alto[4], a loro volta suddivisi in due categorie. Più particolarmente, mentre nella prima essi sono meri componenti di sicurezza di prodotti soggetti ad una valutazione di conformità *ex ante* da parte di terzi, la seconda è costituita dai sistemi indipendenti di cui all'Allegato III, identificati sulla base di criteri quali, tra gli altri, il livello di utilizzo dell'applicazione di IA, la sua finalità prevista, il numero di persone potenzialmente interessate, la dipendenza dai risultati e l'irreversibilità dei danni. Ai fini dell'immissione sul mercato, tali prodotti devono aderire a una serie di stringenti obblighi di trasparenza e di sorveglianza.

Al terzo livello si collocano i sistemi a rischio limitato[5], che devono rispondere a precisi obblighi minimi di trasparenza, quanto ai quali il *focus* è posto sulla consapevolezza dell'utente di interagire con una macchina e sul relativo consenso al suo utilizzo.

Al quarto livello si collocano infine i sistemi a rischio minimo[6], che fermo il rispetto della legislazione vigente e la possibilità di una "auto-regolazione" aderendo a codici di condotta volontari, non sono soggetti ad obblighi particolari ai sensi della proposta di Regolamento.

Quale livello di rischio presenta maggiori oneri in termini di *compliance*?

I sistemi di IA ad alto rischio comportano molteplici obblighi a cui i fornitori devono attenersi prima dell'immissione sul mercato europeo e durante il loro ciclo di vita.

In primo luogo, si introduce una procedura di valutazione della conformità *ex ante* rispetto ai requisiti del Regolamento e l'obbligo di registrazione presso una Banca dati dell'Unione istituita appositamente per i sistemi di IA

[2] Si veda il Considerando 5 del Regolamento.
[3] Si veda l'articolo 5 del Regolamento.
[4] Si veda l'articolo 6 del Regolamento.
[5] Si veda l'articolo 69 del Regolamento.
[6] Si veda l'articolo 52 del Regolamento.

ad alto rischio[7]. Questa sarà gestita dalla Commissione al fine di aumentare la trasparenza nei confronti del pubblico e la sorveglianza, nonché per rafforzare il controllo *ex post* da parte delle autorità competenti.

In secondo luogo, i fornitori dovranno dotarsi di un adeguato sistema di gestione dei rischi[8], inteso come processo interattivo e continuo di verifica che preveda, valuti e analizzi i rischi prevedibili, sulla base dell'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato. Sempre nella logica di un controllo dell'intero ciclo, i risultati elaborati dai sistemi ad alto rischio dovranno essere poi verificati e tracciati lungo la vita del sistema.

La documentazione tecnica, da sottoporsi ad aggiornamento continuo, deve essere disponibile già prima della immissione sul mercato[9]. Ancora, è prevista la registrazione automatica degli eventi (i c.d. *file di log*) che indicano il periodo di ogni utilizzo del sistema (data e ora di inizio e data e ora di fine) ed identificano le persone fisiche coinvolte nella verifica dei risultati. Le registrazioni vengono conservate ai fini del monitoraggio del funzionamento del sistema di IA ad alto rischio, garantendone un livello di tracciabilità adeguato alla finalità prevista dal sistema[10].

Si prevede un'onnipresente garanzia di supervisione umana, attuata per mezzo di strumenti d'interfaccia tra uomo e macchina, tramite cui il primo possa sempre controllare (e così ignorare, interrompere, annullare) l'attività della seconda[11]

Infine, su richiesta di un'autorità nazionale competente, i fornitori avranno l'obbligo di dimostrare la conformità del sistema di IA[12], nonché notificare alla stessa ogni serio incidente o malfunzionamento del sistema che possa costituire una violazione degli obblighi previsti dall'ordinamento dell'Unione a tutela dei diritti fondamentali[13]

Quali sanzioni sono previste in caso di inosservanza delle prescrizioni del Regolamento?

Gli Stati Membri debbono prevedere sanzioni "effettive" e "dissuasive"[14] in caso di violazioni delle disposizioni del Regolamento. L'apparato sanzionatorio è concepito su tre soglie: i) fino a 30 milioni di euro o al 6% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni relative a pratiche vietate o per l'inosservanza di requisiti in materia di dati personali ; ii) fino a 20 milioni di euro o al 4% del fatturato mondiale totale annuo dell'esercizio precedente come categoria residuale per l'inosservanza di qualsiasi altro requisito o obbligo del Regolamento; iii) fino a 10 milioni di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente per la fornitura di informazioni inesatte, fuorvianti o incomplete agli organismi notificati ed alle autorità nazionali competenti in risposta a una richiesta.

Quali figure istituzionali sono introdotte dalla Proposta di Regolamento?

A livello europeo si prevede l'istituzione di un Comitato europeo per l'intelligenza artificiale (*Artificial Intelligence Board*) con funzione principalmente consultiva sulle questioni relative all'attuazione del Regolamento e sulle specifiche criticità

[7] Si veda l'articolo 60 del Regolamento. Per ulteriori approfondimenti circa la struttura e le funzioni della Banca dati, si consulti la Relazione sulla proposta di Regolamento, par. 5.1.
[8] Si veda l'articolo 9 del Regolamento.
[9] Si veda l'articolo 11 del Regolamento.
[10] Si veda l'articolo 12 del Regolamento.
[11] Si veda l'articolo 14 del Regolamento.
[12] Si veda l'articolo 23 del Regolamento.
[13] Si veda l'articolo 62 del Regolamento.
[14] Si veda l'articolo 71 del Regolamento.

relative all'IA, e sussidiariamente di cooperazione con le autorità nazionali e la Commissione.

A livello nazionale è contemplata l'istituzione, da parte di ciascun Stato Membro, di una o più autorità nazionali di controllo, che rappresenteranno anche il singolo Paese nell'ambito del "*Artificial Intelligence Board*". Ad esse fa capo il ruolo primario di supervisione dell'attuazione e del rispetto del Regolamento e di responsabilità della vigilanza del mercato[15].

Quali emendamenti introduce alla Proposta di Regolamento la posizione del Parlamento Europeo del 14 giugno 2023?

La recente posizione negoziale approvata dal Parlamento Europeo non interviene sull'impianto del Regolamento, ma apporta alcune importanti modifiche alla proposta della Commissione[16]:

i. viene coniata, in linea con gli orientamenti dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE)[17], una definizione più restrittiva di "Intelligenza Artificiale" che valorizza la capacità di apprendimento automatico, escludendone i tradizionali processi computazionali e di *software*[18];

ii. si introducono dei principi generali da applicarsi a tutti i sistemi di IA che, al fine di realizzare il c.d. approccio "umano-centrico", debbono rispettare i principi di sorveglianza umana, robustezza tecnica e sicurezza, benessere sociale e ambientale, trasparenza ed equità[19];

iii. viene previsto l'obbligo, in capo a fornitori e operatori dei sistemi di IA, di adottare misure per garantire che il personale addetto possieda una adeguata alfabetizzazione in materia[20];

iv. viene ampliata la categoria IA classificata come rischio inaccettabile[21], ricomprendendovi i) i sistemi di categorizzazione biometrica basati su caratteristiche sensibili, ii) i sistemi di polizia predittiva basati su profilazione del soggetto, sua ubicazione o precedenti penali, iii) i sistemi di riconoscimento delle emozioni utilizzati da o per conto delle autorità pubbliche competenti, o da agenzie, uffici o organismi dell'Unione nella gestione delle frontiere, nel luogo di lavoro e negli istituti d'istruzione, e iv) l'estrazione non mirata di dati biometrici da internet o da filmati di telecamere a circuito chiuso per creare database di riconoscimento facciale;

v. viene ridefinita anche la categoria di rischio alto[22], con l'inclusione dei potenziali danni alla salute, alla sicurezza, ai diritti fondamentali o all'ambiente. Si aggiungono espressamente i sistemi di intelligenza artificiale per influenzare gli elettori nelle campagne politiche e nei sistemi di raccomandazione utilizzati dalle piattaforme di *social media*;

vi. vengono ulteriormente specificati gli obblighi di trasparenza previsti per i sistemi di IA che interagiscono con persone fisiche, di talchè, i fornitori dovranno garantirne la progettazione e lo sviluppo in modo tale che il sistema stesso, il fornitore o l'utilizzatore informino in modo tempestivo, chiaro e comprensibile la persona fisica esposta del fatto di interagire con un sistema di IA, a

[15] Si vedano gli articoli 56-58 del Regolamento.
[16] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.
[17] OCSE, *Recommendation of the Council on Artificial Intelligence,* OCSE/LEGAL/0449.
[18] Si veda il nuovo articolo 3 del Regolamento.
[19] Si veda il nuovo articolo 4-*bis* del Regolamento.
[20] Si veda il nuovo articolo 4-*ter* del Regolamento.
[21] Si veda il nuovo articolo 5 del Regolamento.
[22] Si veda il nuovo articolo 6 del Regolamento.

meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo[23];

vii. vengono inasprite le sanzioni: l'utilizzo dei sistemi di IA vietati *ex* art. 5 del Regolamento può comportare una sanzione pecuniaria fino a 40 milioni di euro o fino al 7% del fatturato globale annuo in caso di società. Se non sono rispettate le norme relative alla *data governance* e alla trasparenza e fornitura di informative agli utenti, la sanzione va fino a 20 milioni di euro o al 4% del fatturato globale annuo[24];

viii. infine, viene data nuova enfasi ai c.d. spazi di sperimentazione normativa[25], per realizzare uno sviluppo fondato su studi in un quadro esperienziale reale ed ottimizzarne l'infrastruttura giuridica. In particolare, questi permetteranno di testare i sistemi di IA nella quotidianità, senza controlli ed in presenza di condizioni di sicurezza nella fase di sperimentazione. Ogni Stato Membro, da solo o congiuntamente ad altri Stati Membri, dovrà istituire almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sarà operativo al più tardi il giorno dell'entrata in vigore del Regolamento, di modo che, da una parte, le autorità forniscano orientamenti ai potenziali fornitori di sistemi per una maggiore conformità alla normativa europea applicabile e, dall'altra, i potenziali fornitori consentano e agevolino la sperimentazione e lo sviluppo di soluzioni innovative relative ai sistemi di IA sperimentati.

Quando entrerà in vigore il Regolamento?

In seguito alla posizione negoziale assunta il 14 giugno 2023 dal Parlamento Europeo, hanno avuto inizio i c.d. triloghi[26]. A condizione che si possa raggiungere un accordo in tale sede entro la fine del corrente anno, il Regolamento potrebbe entrare in vigore intorno a metà del 2024. Viene tuttavia previsto un periodo transitorio di 24 mesi[27] al fine di preparare tutti gli attori coinvolti all'impatto che *l'AI Act* comporterà in termini di *compliance.*

Come può configurarsi una responsabilità in capo ad un sistema di IA nel caso in cui questo causi dei danni?

I sistemi di IA, in quanto intrinsecamente connotati da complessità, autonomia e "opacità" (c.d. *black box effect*), nonché caratterizzati da una catena di approvvigionamento che annovera molteplici attori, rendono l'imputazione della responsabilità extracontrattuale controversa. La Commissione era intervenuta in punto già il 28 settembre 2022 con una proposta di Direttiva[28]. Quest'ultima, volta a adeguare le norme

[23] Si veda il nuovo articolo 52 del Regolamento.
[24] Si veda il nuovo articolo 71 del Regolamento.
[25] Si veda il nuovo articolo 53 del Regolamento.
L'articolo 3, punto 44-*octies*, definisce lo spazio di sperimentazione normativa "un ambiente controllato stabilito da un'autorità pubblica che facilita lo sviluppo, le prove e la convalida in condizioni di sicurezza di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico soggetto a vigilanza regolamentare".
Per approfondimenti sugli obiettivi degli spazi di sperimentazione normativa, si veda il nuovo Considerando 72 del Regolamento.
[26] Per "triloghi" si intendono i negoziati informali cui prendono parte alcuni rappresentanti di Parlamento, Consiglio e Commissione. Nel corso di tali negoziati le tre istituzioni concordano orientamenti politici e bozze di emendamento riguardo alle proposte legislative avanzate dalla Commissione.
[27] Si veda il nuovo articolo 85 del Regolamento.
[28] Com. Comm. COM (2022) 496 final del 28.09.2022, Proposal for a Directive of the European Parliament and of the Council on liability for defective products.
Si consideri che il processo legislativo per l'adozione della Direttiva è appena iniziato, e verosimilmente dovrà coordinarsi con l'adozione del Regolamento sull'intelligenza artificiale.

in materia di responsabilità civile extracontrattuale ai contesti della IA, detta disposizioni *ad hoc* sulla prova del danno causato da un sistema di IA ed offre nuovi strumenti di tutela in sede processuale per il danneggiato[29].

In particolare, rileva l'articolo 3 della Direttiva che, seppur limitato ai sistemi ad alto rischio, prevede il potere del giudice di ordinare la divulgazione o conservazione di elementi di prova sul sistema IA che si sospetta abbia causato dei danni, qualora il fornitore non vi provveda. Nel caso in cui il convenuto non si conformi all'ordine del giudice, opera una presunzione di non conformità del sistema rispetto all'obbligo di diligenza che gli elementi di prova richiesti miravano a dimostrare.

A seguire, l'articolo 4 della Direttiva introduce una presunzione relativa del nesso di causalità in caso di colpa, per il quale l'organo giurisdizionale nazionale presume l'esistenza del nesso causale tra la colpa del convenuto e l'*output* prodotto da un sistema di IA o la mancata produzione di un *output* da parte di tale sistema se sono soddisfatte tutte le condizioni seguenti: i) l'attore ha dimostrato o il giudice ha presunto la colpa del convenuto, consistente nella non conformità a un obbligo di diligenza previsto dal diritto dell'Unione o nazionale e direttamente inteso ad evitare il danno verificatosi; ii) si può ritenere ragionevolmente probabile che, sulla base delle circostanze del caso, la condotta colposa abbia influito sull'output prodotto/omesso dal sistema; iii) l'attore ha dimostrato che il danno è stato causato dall'output prodotto/omesso dal sistema di intelligenza artificiale.

Il potere di divulgazione o conservazione della prova del giudice nazionale incontra delle limitazioni?

L'articolo 3 della Direttiva impone ai giudici nazionali di tenere in considerazione gli interessi legittimi di tutte le parti nel determinare se un ordine di divulgazione o di conservazione delle prove sia proporzionato: con specifico riferimento alla Direttiva (UE) 2016/943[30] (c.d. *trade secrets*) e alla normativa nazionale recepente, la norma lascia al giudice del merito il compito di individuare la prevalenza tra l'interesse del titolare alla tutela del segreto e quello degli altri r *stakeholder* alla divulgazione e conservazione.

Peraltro, anche qualora avvenga la divulgazione di un segreto commerciale, i giudici nazionali hanno il potere, su richiesta motivata di una parte o d'ufficio, di adottare misure specifiche necessarie a preservarne la segretezza. Ciò può avvenire, a mente della Direttiva *trade secrets*, attraverso la limitazione dell'accesso alla documentazione riservata ad un ristretto novero di persone, limiti di accesso alle udienze, registrazioni e trascrizioni, ed oscuramento delle parti sensibili delle decisioni[31].

Il danno da prodotto difettoso consistente in una IA configura una fattispecie specifica?

Congiuntamente alla proposta di Direttiva relativa alla responsabilità extracontrattuale, è intervenuta nella medesima data un'ulteriore proposta[32] allo scopo di modificare taluni aspetti della disciplina in vigore in materia di responsabilità per danno da prodotti difettosi[33], adeguando la stessa alle

[29] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.
[30] Con la Direttiva (UE) 2016/943 dell'8 giugno 2016 del Parlamento europeo e del Consiglio, è stato fornito agli Stati membri un quadro comune sulla protezione del *know-how* e delle informazioni commerciali riservate (segreti commerciali).
[31] Si veda l'articolo 9 della Direttiva (UE) 2016/943.
[32] Com. Comm. COM(2022) 495 final del 28.09.2022, Proposta di Direttiva del Parlamento e del Consiglio sulla responsabilità per danno da prodotti difettosi.
[33] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, GUUE L 210 del 07.08.1985.

evoluzioni della *digital economy* e così individuando uno spazio normativo destinato ai prodotti basati su IA[34].

Insieme ad un'estensione della definizione di "prodotto" ricomprendente i sistemi di IA[35], vengono ritenuti suscettibili di "difettosità" anche le funzioni di interconnessione e apprendimento automatico dei sistemi di IA, che si aggiungono così all'elenco di fattori di cui gli organi giurisdizionali devono tenere conto nel valutare l'esistenza di difetti[36]. L'onere della prova resta a carico del danneggiato, ma si introducono presunzioni circa il carattere difettoso dei prodotti, il nesso di causalità tra difetto e danno od entrambi gli elementi[37]. Infine, viene promossa la parità di trattamento tra i fabbricanti dell'Unione e quelli dei Paesi terzi, ed i consumatori che subiscono danni causati da prodotti non sicuri importati potranno esigere un risarcimento dall'importatore o dal rappresentante del fabbricante nell'Unione[38].

Quali sono i profili di intersezione tra proprietà intellettuale e IA?

Lo sviluppo delle IA introduce profili inesplorati rispetto ai tradizionali modelli di tutela delle opere dell'ingegno e delle invenzioni, aprendo così una serie di potenziali criticità ad oggi prive di risposte univoche[39]:

- Soggettività: L'IA può creare opere originali, come opere d'arte, musica o testi, che sollevano interrogativi sulla proprietà intellettuale. Ci si domanda se un'opera generata da un algoritmo sia da considerare come proprietà di chi ha sviluppato l'algoritmo, dell'operatore dell'IA o dell'IA stessa;

- Originalità: L'IA può sviluppare nuove invenzioni, ma è incerto se l'IA possa essere riconosciuta come inventore. I sistemi di IA possono combinare e rielaborare elementi, ma fino ad ora non si riconosce loro la capacità di concepire idee originali come un essere umano; in taluni Paesi, sia dell'Unione Europea, che Paesi terzi, gli uffici nazionali della proprietà intellettuale si sono allo stato pronunciati nel senso che quale inventore, della IA o dell'invenzione generata da questa, debba essere indicata una persona fisica

- Protezione dei dati: L'IA richiede massive quantità di dati per apprendere e migliorare le sue capacità e funzionalità. Questi dati possono contenere informazioni proprietarie o riservate che potrebbero venire utilizzate dalla IA senza autorizzazione o in violazione dei diritti di proprietà intellettuale dei terzi;

- Licenze: Lo sviluppo e l'utilizzo dell'IA può richiedere l'accesso a più brevetti, diritti d'autore o altre forme di proprietà intellettuale, indispensabili per realizzare il risultato, e l'assenza di standardizzazioni liberamente disponibili o di licenze concesse a condizioni ragionevoli per il loro utilizzo può ostacolare il progresso tecnico o comportare costi eccessivi per gli sviluppatori; non è inverosimile che, anche nel campo delle IA, si giunga a soluzioni di licenza secondo termini equi e ragionevoli (c.d. condizioni FRAND) comparabili a quelle che sono state sviluppate, ad esempio nell'industria delle telecomunicazioni e dell'audiovisuale, per i c.d. *standard essential patents* (SEP);

- Responsabilità: L'IA può sollevare questioni inedite di responsabilità in relazione alle violazioni della proprietà intellettuale dei terzi. Ad esempio, se

[34] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.
[35] Si veda l'articolo 4 della Direttiva.
[36] Si veda l'articolo 6 della Direttiva.
[37] Si veda l'articolo 9 della Direttiva.
[38] Si veda l'articolo 7 della Direttiva.
[39] Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.

(come è destinato a verificarsi sempre più di frequente, con il potenziamento esponenziale delle capacità di auto-apprendimento di un sistema, inevitabilmente al di fuori del controllo giuridico dell'operatore) un sistema di IA viola un brevetto o utilizza indebitamente un'opera protetta da *copyright*, rimane da determinare chi ne sarà responsabile: il creatore dell'algoritmo, il proprietario del sistema di IA o l'operatore?.

In che modo l'*AI Act* interviene sulle questioni sollevate dalla proprietà intellettuale?

La posizione del Parlamento Europeo del 14 giugno 2023 relativamente all'*AI Act* si rivolge in primo luogo ed esplicitamente all'IA generativa (sul solco del clamore suscitato da piattaforme come *ChatGTP*), introducendo l'obbligo per il fornitore di documentare e rendere disponibile al pubblico un riassunto sufficientemente dettagliato dell'utilizzo dei dati protetti da *copyright*, prima che il modello venga immesso sul mercato o messo in servizio nell'UE[40].

Più in generale, vale allo stato quanto si rinviene nei Considerando 58a e 60h della proposta di Regolamento, secondo cui gli implementatori di IA dovrebbero mitigare i rischi di violazione della proprietà intellettuale dei terzi nell'ambito dei requisiti generali di *governance*[41].

In che modo il GDPR interagisce con l'IA?

Il rapporto tra Regolamento sulla protezione dei dati personali (*General Data Protection Regulation,* GDPR) e la disciplina dell'IA presenta caratteristiche talora simbiotiche, e talora conflittuali. Come è noto, il GDPR si rivolge al trattamento dei dati personali, mentre la Proposta di Regolamento sull'IA riguarda (tra le altre cose) le tecnologie per effettuare tali trattamenti[42]. I due atti normativi sono fisiologicamente complementari, tuttavia con rischi di iper-regolazione in conseguenza delle sovrapposizioni. Infatti, la definizione estremamente ampia di IA, includente persino gli algoritmi e i modelli statistici, e l'onnipresente utilizzo dei dati personali nei sistemi di IA ad alto rischio[43], dovranno necessariamente condurre ad un coordinamento.

Ad oggi, il GDPR è uno dei testi normativi più utilizzati quando si guarda all'impatto dell'IA sui diritti fondamentali. Esso si pone l'obiettivo del rispetto dei "principi applicabili al trattamento dei dati personali"[44] presso i tribunali degli Stati Membri e dell'Unione Europea; prevede autorità di controllo nazionali (Garante per la Protezione dei Dati Personali - GDPD, l'autorità italiana), nonché di un Garante Europeo per la Protezione dei Dati (GEPD) e di un Comitato Europeo per la Protezione dei Dati (EDPB). Queste autorità hanno realizzato nel corso degli anni una vasta produzione di decisioni, pareri, linee guida e relazioni, in cui hanno informato, istruito, ma anche sentenziato, sulla liceità degli usi controversi degli strumenti di IA.

Tra i due sistemi normativi vi è, dunque, una continua interazione.

Le autorità di protezione dei dati personali sono legittimate ad intervenire in materia di IA?

[40] Si veda il nuovo articolo 28 del Regolamento.
[41] Il Considerando 58a collega la governance alla "mitigazione dei rischi per i diritti fondamentali" e tali diritti includono i "diritti di proprietà intellettuale" (Considerando 28a). Ancora, il Considerando 60h osserva che i sistemi di IA generativi sollevano questioni significative relative alla generazione di contenuti in violazione del diritto dell'Unione, delle norme sul diritto d'autore e del potenziale abuso, e richiede un monitoraggio periodico da parte della Commissione e dell'Ufficio IA.
[42] Si consideri che molte applicazioni di IA basano i loro risultati sul trattamento dei dati personali. Dalla polizia predittiva allo screening dei CV, molte applicazioni vengono addestrate, testate e utilizzate sulla base del trattamento di grandi quantità di dati personali.
[43] Si pensi all'identificazione biometrica, all'istruzione, alla sanità, alle prestazioni assistenziali, all'immigrazione, ecc.
[44] Si veda l'articolo 5 del GDPR.

Le autorità istituite dal sistema del GDPR hanno il potere di intervenire laddove l'IA tratti dati personali; ne risulta che la maggior parte dei sistemi di IA, poiché utilizzano algoritmi che si basano su grandi masse di dati personali (c.d. *machine learning*), sono potenzialmente soggetti a dette autorità[45]. Tuttavia, le autorità di protezione dei dati personali non sono state concepite dal GDPR per esercitare attribuzioni in materia di tecnologie di IA basate su dati personali contestati; di conseguenza, potrebbero determinarsi degli oneri aggiuntivi e non fisiologici per tali autorità, che già ora sono sottofinanziate rispetto ai loro ruoli istituzionali e verosimilmente attrezzate per affrontare nuovi compiti impegnativi. Allo stato, nonostante sia auspicabile un intervento legislativo di coordinamento, non si potrà prescindere né dai principi del GDPR (considerato che la stessa IA si nutre di dati e, in particolare, di quelli di natura personale), né da un ruolo centrale delle autorità garanti per la protezione dei dati a livello nazionale, nelle decisioni strategiche e di sistema e nelle regolamentazioni settoriali.

Cosa ci si può attendere in pendenza dell'entrata in vigore dell'*AI Act*?

In attesa dell'*AI Act*, vi sono preoccupazioni a motivo del rapido sviluppo dell'IA, che richiede degli strumenti di controllo tempestivi e mal si concilia con i tempi tecnici previsti per la sua entrata in vigore. Se da un lato, si registra la presenza attiva delle autorità istituite dal GDPR nell'attuale fase di prima convivenza diffusa con il fenomeno, dall'altro lato, numerose di iniziative di *governance* dell'IA si moltiplicano a livello internazionale.

Sin dall'inizio del 2022, il Consiglio d'Europa ha istituito un Comitato sull'Intelligenza Artificiale[46], incaricato di redigere la futura Convenzione sull'Intelligenza Artificiale, i Diritti Umani, la Democrazia e lo Stato di Diritto.

In secondo luogo, è recente l'annuncio da parte di Unione Europea e Stati Uniti d'America della pubblicazione di un codice di condotta ad adesione volontaria per l'IA generativa, mirante ad un allineamento internazionale per un approccio comune alla sua *governance* , alla protezione del diritto d'autore, alla trasparenza, alla lotta alla disinformazione e alla promozione dell'uso responsabile di queste tecnologie.

Inoltre, mentre gli Stati Uniti avevano inizialmente adottato un approccio "leggero" nei confronti dell'IA, di recente si sono moltiplicate le richieste di regolamentazione. Anche la *Cyberspace Administration* cinese sta discutendo una proposta di regolamentazione dell'IA, mentre il Regno Unito sta lavorando a una serie di principi normativi a favore dell'innovazione che si rivolgono parimenti alla IA.

A livello internazionale, si annoverano, infine, l'Organizzazione per la Cooperazione e lo Sviluppo Economico (*Organisation for Economic Cooperation and Development*, - OECD), che ha adottato una raccomandazione (non vincolante) sull'IA nel 2019, e l'UNESCO, che ha adottato delle raccomandazioni sull'etica dell'IA nel 2021.

Quale lettura è possibile desumere da questo scenario, e quali sfide attendono i legislatori?

Lo scenario europeo in tema di IA si presenta come una "corsa alla *governance*" che costituisce un *unicum* nel lungo cammino dell'Unione Europea. Il tentativo di disciplinare un settore in così rapida evoluzione mette i legislatori e gli *stakeholder* davanti a molteplici difficoltà: dalle interferenze con le altre aree regolamentate, alla co-regolazione ad opera anche di altre autorità settoriali per esercitare delle attribuzioni effettive, l'IA si conferma un terreno inesplorato, dove persino le definizioni rischiano di diventare categorie obsolete, che faticano a tenere il passo della continua evoluzione tecnologica. L'*AI Act*, come primo Regolamento al mondo inteso ad

[45] Per ulteriori informazioni si consulti il seguente LINK.
[46] Per ulteriori informazioni si consulti il seguente LINK.

introdurre dei confini – giuridici, etici e politici - nell'utilizzo dell'IA si propone l'obiettivo ambizioso di resistere al tempo e fungere da modello per altri Paesi. L'auspicio è che l'*AI Act* possa costituire un punto mediano tra sovra-regolazione e *laissez faire*, in un ecosistema intangibile, dove troppe regole impedirebbero il progresso, ma l'assenza di regole comprometterebbe le garanzie dei diritti fondamentali e della società civile.

Roberto A. Jacchia

PARTNER

r.jacchia@dejalex.com

+39 02 72554.1

Via San Paolo 7
20121 - Milano

Federico Aluigi

ASSOCIATE

f.aluigi@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Sadovaya-Chernogryazskaya 8, build. 8 · 107078, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com