



Sicurezza e affidabilità i pilastri del nuovo Regolamento europeo sull'Intelligenza Artificiale

📅 30/04/2021

📖 DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, PROSPETTIVE

Roberto A. Jacchia
Marco Stillo

In data 21 aprile 2021, la Commissione ha presentato una proposta di Regolamento¹ che stabilisce un quadro giuridico uniforme per lo sviluppo, la commercializzazione e l'utilizzo delle intelligenze artificiali (IA), in grado di garantire la sicurezza e i diritti fondamentali delle persone e delle imprese, rafforzando la posizione di *leadership* dell'Unione a livello mondiale.

La proposta si pone a coronamento di una serie di iniziative che, nel corso degli ultimi anni, le istituzioni europee hanno intrapreso in materia di IA

riconoscendone il ruolo crescente nella società del terzo millennio nonché le capacità, attraverso la progressiva automatizzazione dei processi in un numero esponenziale di settori e di utilizzi, quali, ad esempio, la diminuzione degli incidenti stradali, l'ottimizzazione dell'impiego delle risorse scarse quali l'energia e l'acqua, la riduzione dell'uso dei pesticidi in agricoltura, il potenziamento della competitività del settore manifatturiero e la sempre maggiore affidabilità della chirurgia e della tele-chirurgia. Già nella sua strategia europea sull'IA del 2018², la Commissione aveva evidenziato l'intenzione di dare impulso alla capacità

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.*

² Com. Comm. COM(2018) 237 final del 25.04.2018, *L'intelligenza artificiale per l'Europa.*



tecnologica ed industriale dell'Unione e all'adozione dell'IA in tutti i settori, al tempo stesso assicurando un quadro etico e giuridico adeguato, basato sui valori della Carta dei diritti fondamentali. Alla strategia europea avevano fatto seguito nel 2020, da un lato, il Libro Bianco sull'IA³, che delineava l'impegno della Commissione a favorire i progressi scientifici, preservare la *leadership* tecnologica dell'Unione e garantire che le nuove tecnologie siano al servizio di tutti gli europei e ne migliorino la qualità della vita rispettandone i diritti e, dall'altro, la Relazione sulle Implicazioni dell'Intelligenza Artificiale, dell'Internet delle cose e della Robotica in materia di Sicurezza e di Responsabilità⁴, in base alla quale la società moderna, più esposta a maggiori rischi di sicurezza dovuti alla connettività e all'apertura dei sistemi, necessita di una regolamentazione più specifica non solo per quanto riguarda la raccolta neutrale di dati di qualità, e bensì anche sulla possibilità di ritenere tali sistemi "responsabili" dei danni eventualmente causati.

Dal canto suo, in data 20 ottobre 2020 il Parlamento aveva approvato tre Risoluzioni contenenti specifiche raccomandazioni alla Commissione in ordine alla futura disciplina delle IA in materia di proprietà intellettuale, principi etici e responsabilità civile.

Per quanto riguarda la proprietà intellettuale⁵, il Parlamento aveva posto l'accento sull'importanza fondamentale di un sistema di protezione equilibrata e pluridimensionale in grado di assicurare la certezza giuridica e di creare la fiducia necessaria ad incoraggiare gli investimenti e garantirne tanto la redditività a lungo termine quanto l'utilizzo prolungato da parte dei

consumatori. Più particolarmente, il Parlamento, da un lato, aveva invitato la Commissione a tenere conto delle diverse dimensioni dell'IA attraverso definizioni tecnologicamente neutre che garantiscano la flessibilità necessaria per adeguarsi alle future evoluzioni ed ai successivi utilizzi e, dall'altro, aveva stabilito alcuni requisiti minimi quali, tra gli altri, la brevettabilità dei metodi matematici solo quando soddisfano i requisiti caratteristici delle invenzioni, l'assenza di titolarità giuridica alla AI per quanto riguarda opere creative prodotte autonomamente, e la disciplina dell'utilizzo dei dati non personali anche tramite di accordi di licenza.

Per quanto riguarda gli aspetti etici⁶, il Parlamento aveva sottolineato come qualsiasi quadro normativo che preveda obblighi giuridici e principi etici per lo sviluppo, la diffusione e l'utilizzo dell'IA, della robotica e delle tecnologie correlate debba rimanere incentrato sull'individuo, rispettandone la dignità, l'autonomia e l'autodeterminazione. Oltre a ritenere fondamentali per la nuova disciplina principi quali, tra gli altri, la sicurezza, la trasparenza, la responsabilità, la non discriminazione, il diritto al risarcimento, la tutela della *privacy* e la sostenibilità ambientale, il Parlamento aveva anche evidenziato la centralità del coordinamento a livello europeo assicurato dalla Commissione e dalle istituzioni, dagli organi e dagli organismi specifici eventualmente da designarsi al fine di evitare la frammentazione delle competenze con un approccio armonizzato che favorisca lo sviluppo dell'innovazione e sensibilizzi i cittadini riguardo alle opportunità e ai rischi inerenti a tali tecnologie.

³ Com. Comm. COM(2020) 65 final del 19.02.2020, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*.

⁴ Com. Comm. COM(2020) 64 final del 19.02.2020, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*.

⁵ Risoluzione del Parlamento europeo, del 20 ottobre 2020, sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale.

⁶ Risoluzione del Parlamento europeo, del 20 ottobre 2020, recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate.

Per quanto riguarda la responsabilità civile⁷, infine, la risoluzione del Parlamento si era incentrata sui sistemi di IA c.d. “ad alto rischio”, prevedendo una gradazione dei regimi di responsabilità. Più particolarmente, mentre l’operatore di un sistema di IA “ad alto rischio” era ritenuto oggettivamente responsabile di qualsiasi danno o pregiudizio causato da un’attività, dispositivo o processo fisico o virtuale da esso guidato, a meno che lo stesso non fosse da ascrivere a cause di forza maggiore, l’operatore di un sistema di IA non ad alto rischio era soggetto ad un regime di responsabilità per colpa, con facoltà di dimostrare che l’evento dannoso non era a lui imputabile in quanto, alternativamente, il sistema di IA si era attivato senza che egli ne fosse a conoscenza (pur essendo state adottate tutte le misure ragionevoli e necessarie per evitare tale attivazione) oppure che era stata adoperata la dovuta diligenza.

Il nuovo quadro giuridico, che si applicherà ai soggetti pubblici e privati a condizione che il sistema sia immesso sul mercato dell’Unione o che il suo utilizzo abbia effetti sulle persone ivi situate (potendo perciò riguardare sia i fornitori che gli utenti) si fonda, appunto, su una classificazione dei sistemi di IA basata sul rischio.

In primo luogo, i sistemi di IA che comportano un rischio minimo per i diritti o la sicurezza dei cittadini, categoria in cui rientra la grande maggioranza di quelli attualmente utilizzati nell’Unione, possono essere liberamente sviluppati ed utilizzati nel rispetto delle norme vigenti, con possibilità, per i relativi fornitori, di aderire a codici di condotta volontari redatti sulla base degli stessi criteri previsti per i sistemi ad alto rischio⁸.

In secondo luogo, i sistemi a rischio limitato, come i c.d. “*chatbot*”⁹, sono sottoposti ad obblighi di trasparenza qualora interagiscano con le persone. Più particolarmente, tali sistemi devono essere sviluppati in modo tale da rendere gli individui consapevoli di interagire con una macchina, di modo da consentire loro di scegliere liberamente se proseguire o meno nel loro utilizzo¹⁰.

In terzo luogo, i sistemi di IA che comportano un rischio inaccettabile saranno vietati in quanto considerati una minaccia per la sicurezza, i mezzi di sussistenza e i diritti fondamentali delle persone. Nello specifico, non saranno ammessi quei sistemi che, tra le altre cose, manipolano il comportamento umano attraverso tecniche subliminali per aggirare il libero arbitrio degli utenti, sfruttano le vulnerabilità di specifici gruppi di individui a causa della loro età o di loro particolari caratteristiche, oppure consentono ai governi di attribuire un punteggio sociale agli individui. Anche l’uso dell’identificazione biometrica remota in tempo reale in spazi accessibili al pubblico con finalità di contrasto è in linea di principio vietata, salvi gli usi per la ricerca mirata di potenziali vittime specifiche di reato, per la risposta ad una minaccia imminente di attacco terroristico o per l’individuazione degli autori di reati gravi¹¹.

Infine, un numero limitato di sistemi di IA sono considerati ad alto rischio a causa delle loro ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali. Più particolarmente, la proposta individua due categorie di sistemi IA ad alto rischio¹², quelli destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti ad una valutazione di conformità *ex ante* da parte di terzi, e quelli indipendenti (ossia non integrati in

⁷ Risoluzione del Parlamento europeo, del 20 ottobre 2020, recante raccomandazioni alla Commissione su un regime di responsabilità civile per l’intelligenza artificiale.

⁸ Si veda l’articolo 69 della proposta.

⁹ Un *chatbot* è un software progettato per simulare una conversazione con un essere umano.

¹⁰ Si veda l’articolo 52 della proposta.

¹¹ Si veda l’articolo 5 della proposta.

¹² Si veda l’articolo 6 della proposta.

prodotti) di cui all'Allegato III¹³, 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. Onde poter essere immessi sul mercato, tali sistemi dovranno rispettare gli obblighi specifici previsti dalla proposta, relativi i) ad un sistema di valutazione e attenuazione dei rischi, consistente in un processo continuo eseguito durante l'intero ciclo di vita del sistema, di modo da rendere i rischi residui accettabili¹⁴, ii) all'utilizzo di insiemi di dati di elevata qualità che riducano al minimo i rischi di risultati discriminatori¹⁵, iii) alla conservazione e all'aggiornamento dei documenti necessari per dimostrare che il sistema è conforme ai requisiti della proposta¹⁶, iv) alla predisposizione di strumenti che consentano la registrazione automatica degli eventi durante l'utilizzo del sistema¹⁷, v) alla trasparenza e alla fornitura di informazioni che ne consentano un utilizzo appropriato da parte degli utenti¹⁸, vi) alla sorveglianza umana, di modo da prevenire o ridurre al minimo i rischi per la sicurezza e la salute degli individui¹⁹, e vii) ad un livello di robustezza, accuratezza e cybersicurezza appropriato²⁰.

La proposta prevede anche diversi obblighi per i fornitori dei sistemi di IA ad alto rischio, che dovranno essere soddisfatti prima della loro immissione sul mercato europeo. Più particolarmente, oltre ad attuare sistemi di gestione della qualità per garantire la

conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e le persone interessate²¹, a conservare tutta la necessaria documentazione nonché a collaborare con le autorità nazionali competenti²², i fornitori dovranno sottoporre il sistema ad una valutazione di conformità, di modo da dimostrare che lo stesso rispetta i requisiti previsti. Tale valutazione, che in caso di modifica sostanziale del sistema o della sua finalità dovrà essere ripetuta, può basarsi, alternativamente, sul controllo interno di cui all'Allegato VI oppure sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica, con il coinvolgimento di un organismo notificato conformemente a quanto disposto nell'Allegato VII²³.

Nonostante spetti agli Stati Membri il compito di stabilire sanzioni effettive, proporzionate e dissuasive (nonché di comunicarle alla Commissione) per i casi di immissione sul mercato o messa in servizio di sistemi di IA in violazione delle disposizioni del Regolamento, quest'ultimo stabilisce delle soglie di sanzione che dovranno essere tenute in considerazione²⁴. Più particolarmente, mentre le violazioni relative alle pratiche vietate o all'inosservanza dei requisiti in materia di dati dovrebbero essere soggette ad un'ammenda fino a 30 milioni di euro o, nel caso in cui il responsabile sia un'impresa, fino al 6% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore), quelle relative a tutte le altre disposizioni del Regolamento dovrebbero essere

¹³ Nello specifico, si tratta di quei sistemi in cui l'IA è utilizzata, tra gli altri, in infrastrutture critiche, nell'istruzione o formazione professionale, nell'ambito dell'occupazione, della gestione dei lavoratori e dell'accesso al lavoro autonomo, in servizi pubblici e privati essenziali, nella gestione della migrazione, dell'asilo e del controllo delle frontiere e nell'amministrazione della giustizia e nei processi democratici.

¹⁴ Si veda l'articolo 9 della proposta.

¹⁵ Si veda l'articolo 10 della proposta.

¹⁶ Si veda l'articolo 11 della proposta.

¹⁷ Si veda l'articolo 12 della proposta.

¹⁸ Si veda l'articolo 13 della proposta.

¹⁹ Si veda l'articolo 14 della proposta.

²⁰ Si veda l'articolo 15 della proposta.

²¹ Si veda l'articolo 17 della proposta.

²² Si veda l'articolo 23 della proposta.

²³ Si veda l'articolo 43 della proposta.

²⁴ Si veda l'articolo 71 della proposta.

sanzionate con un'ammenda fino a 20 milioni di euro o, nel caso in cui il responsabile sia un'impresa, al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore). Infine, la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati e alle autorità nazionali competenti in risposta ad una richiesta dovrebbe essere punita con un'ammenda fino a 10 milioni di euro o, nel caso in cui il responsabile sia un'impresa, al 2% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore).

Per quanto riguarda la *governance*, infine, la proposta prevede un sistema a doppio livello. Mentre a livello nazionale ciascuno Stato Membro dovrà designare una o più autorità competenti nonché un'autorità di controllo incaricate di supervisionare l'applicazione e l'attuazione del Regolamento²⁵, a livello unionale verrà istituito il Comitato Europeo per l'Intelligenza Artificiale (*European Artificial Intelligence Board*), composto dai rappresentanti di alto livello

delle autorità nazionali di controllo, del Garante europeo della protezione dei dati (*European Data Protection Supervisor*, EDPS) e della Commissione, allo scopo di formulare raccomandazioni e pareri in merito ai sistemi di IA ad alto rischio e ad altri aspetti pertinenti per l'attuazione efficace e uniforme del Regolamento²⁶.

La proposta della Commissione delinea un piano d'azione unitario che si propone di garantire il buon funzionamento del mercato interno sfruttando appieno, da un lato, tutte le opportunità offerte dalle IA e tenendo adeguatamente conto, dall'altro, sia dei loro benefici che dei loro rischi. Il Regolamento dovrà ora essere adottato dal Parlamento e dal Consiglio nell'ambito della procedura legislativa ordinaria, divenendo in seguito direttamente applicabile in tutta l'Unione.

²⁵ Si veda l'articolo 59 della proposta.


²⁶ Si vedano gli articoli 56-58 della proposta.



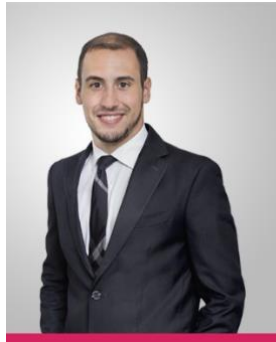
Roberto A. Jacchia

PARTNER

 r.jacchia@dejalex.com

 +39 02 72554.1


 Via San Paolo 7
20121 - Milano




Marco Stillo

ASSOCIATE

 m.stillo@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 Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com