Verso l'*Artificial Intelligence Act*: le novità da Bruxelles

06/11/2023

DIRITTO EUROPEO E DELLA CONCORRENZA, PRIVACY E CYBERSECURITY, PROSPETTIVE.

Jacopo Piemonte
Federico Aluigi

L'intelligenza artificiale (conosciuta anche come "AI" dall'abbreviazione dell'espressione inglese *artificial intelligence*) è il vero argomento di discussione di questo periodo nell'agenda globale.

Mentre scriviamo quest'articolo si sta svolgendo ad esempio in Inghilterra l'*AI Summit* in cui i principali *leader* mondiali si stanno interrogando - anche in un'ottica di salvaguardia dei diritti umani - su rischi e opportunità che possono offrire queste nuove tecnologie. Inoltre, è già noto che il prossimo semestre del G7 (che sarà guidato dall'Italia) avrà come tema proprio l'impatto dei sistemi di AI sul mercato del lavoro.

Tali iniziative evidenziano in maniera chiara come sia fortemente sentita - a livello globale - la necessità che l'intelligenza artificiale venga regolata. In questo scenario, l'Unione Europea sta cercando di ergersi come protagonista dell'ambizioso progetto volto a costruire il primo Regolamento al mondo inteso ad introdurre confini - giuridici, etici e politici - nell'utilizzo dei sistemi di AI.

La Commissione Europea ha presentato la proposta di Regolamento per l'intelligenza artificiale già in data 21 aprile 2021 (nota anche come "AI *Act*" e a cui in questo articolo ci si riferirà anche come "Regolamento"). Successivamente si è svolto il canonico *iter* legislativo che si sta ora concludendo con i triloghi tra Consiglio, Commissione e Parlamento. Negli ambienti di lavoro di Bruxelles si respira ottimismo e ci si attende presto una "fumata bianca" sul testo definitivo. Vediamo dunque a che punto siamo.

1) Le colonne portanti dell'AI *Act*

Vale la pena, in primo luogo, soffermarsi sulla struttura di base dell'AI *Act* che a questo punto non dovrebbe cambiare. Rimandando al nostro precedente

articolo sul tema per i dettagli[1], ricordiamo di seguito i capi saldi di questo rivoluzionario strumento legislativo.

A) Sistema di rischio

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

Al primo livello si collocano i sistemi di AI a rischio inaccettabile, la cui commercializzazione e i cui possibili utilizzi sono banditi in modo pressoché assoluto dal Regolamento[2].

Al secondo livello si collocano i sistemi di AI a rischio alto, 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 AI, 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, 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, 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.

B) Le figure istituzionali introdotte dalla Proposta

Oltre al sistema *risk-based approach* dettagliato sopra, "marchio di fabbrica" dell'*AI Act* dovrebbe essere un sistema di *Governance* "nuovo di zecca".

A livello europeo si prevede infatti 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 relative all'AI, e sussidiariamente di cooperazione con le autorità nazionali e la Commissione.

A livello nazionale è invece 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. In tal senso, nell'attesa di risultati dalle sedi europee, in Italia il nodo sulla figura istituzionale nazionale che avrà competenza in materia di AI resta irrisolto, in uno scenario dove, se da una parte il Garante

[1] Per un quadro sulla regolamentazione dell'AI e relative problematiche, si veda il nostro precedente contributo al seguente LINK.

[2] Ci si riferisce in particolare a: *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.

per la Protezione dei Dati Personale (GPDP) appare in *pole position*[3], dall'altra parte spicca la figura dell'Agenzia per l'Italia Digitale (AgID) come altra possibile candidata[4].

C) Quali sanzioni sono previste in caso di inosservanza delle prescrizioni regolamentari?

Infine, non da ultimo, sulla scia di quanto proposto dal GDPR, nella proposta di AI *Act* è previsto un sistema di sanzioni che mirano ad avere un forte effetto deterrente. Gli Stati Membri sono chiamati infatti a prevedere sanzioni "effettive" e "dissuasive" in caso di violazioni delle disposizioni del Regolamento[5].

2) I punti in sospeso

Veniamo ora ad una serie di questioni che sono invece ancora oggetto di aperto dibattito. I negoziati interistituzionali stanno infatti cercando di dirimere una serie di punti irrisolti. In particolare, nell'incontro tenutosi in data 24 ottobre 2023 si è discusso di quanto segue.

A) L'approccio basato sul rischio ed il livello di rischio alto: troppi oneri per troppe imprese?

Come abbiamo visto sopra, sul solco del c.d. *risk-based approach*, la proposta di Regolamento introduce una classificazione in base al rischio su quattro livelli, fondati sulle ripercussioni che potrebbe avere l'AI sulla sicurezza delle persone e dei diritti fondamentali. A questo riguardo, Il livello di rischio alto si presenta come quello più oneroso in termini di *compliance*, comportando molteplici obblighi a cui i fornitori devono attenersi prima dell'immissione del sistema sul mercato europeo e durante il ciclo di vita[6]. In tale categoria sono inclusi anche i sistemi in grado di arrecare danni alla salute, alla sicurezza, ai diritti fondamentali o all'ambiente[7].

Questo contenitore è dunque ampio e comporterebbe un gravoso carico di adempimenti in capo a numerose imprese (rischiando di bloccare l'apparato produttivo europeo *in primis*). Per tale motivo, si sta tentando di introdurre condizioni di "filtro", soddisfacendo le quali i fornitori di intelligenza artificiale potrebbero considerare il loro sistema esentato dalla categoria ad alto rischio (e dunque non dovrebbero sottostare alle rigide regole altrimenti previste)[8].

---

[3] In argomento, si veda il Comunicato Stampa del Garante della Privacy al seguente LINK.
[4] Per ulteriori informazioni sull'AgID si veda il seguente LINK.
[5] 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.
[6] Si pensi, ad esempio, alla procedura di valutazione della conformità *ex ante* rispetto ai requisiti del Regolamento (articolo 60 della proposta); al sistema di gestione dei rischi, 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 (articolo 9 della proposta); alla garanzia "onnipresente" di supervisione umana (articolo 14 della proposta).
[7] Si veda il nuovo articolo 6 della proposta di Regolamento che, dopo gli emendamenti apportati dalla posizione negoziale del Parlamento Europeo in data 14 giugno 2023, al paragrafo 2 statuisce che "… *Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio i sistemi di IA che rientrano in uno o più settori critici e casi d'uso di cui all'allegato III, se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali delle persone fisiche. Qualora un sistema di IA rientri nell'allegato III, punto 2, è considerato ad alto rischio se presenta un rischio significativo di danno per l'ambiente* …".
[8] Le condizioni esimenti sarebbero giustificate dal carattere accessorio di alcuni sistemi di AI, destinati a svolgere un ruolo prettamente procedurale, o semplicemente a confermare o migliorare

B) Più regolamentazione per l'AI generativa

In secondo luogo, persistono criticità circa la regolamentazione dei c.d. *foundation models*[9], vale a dire dei sistemi sostanzialmente della specie di ChatGPT.

Come noto, al momento della presentazione della proposta di regolamento sull'intelligenza artificiale nell' aprile 2021, questa questione non era ancora sul "tavolo". ChatGTP è stato infatti ufficialmente lanciato nel 2022. Il legislatore Europeo ha dunque dovuto rapidamente adeguarsi a tale nuovo fenomeno e alla proliferazione di questo tipo di sistemi[10].

Sul punto, il nuovo approccio ora proposto prevederebbe ulteriori obblighi di trasparenza orizzontale per tutti i modelli, in particolare nella documentazione riportante il processo di formazione degli stessi, nonché nella valutazione dei parametri di riferimento stabiliti prima del lancio sul mercato. Si sta ora valutando se abbia senso impostare un'ulteriore distinzione nei sistemi di AI generativa con imposizione di ulteriori oneri a seconda del loro grado di "impatto"[11].

C) La proposta di una gestione centralizzata dell'enforcement dei sistemi di intelligenza artificiale più rischiosi

Infine, certe componenti politiche stanno spingendo affinché il controllo di sistemi di intelligenza artificiale che potrebbero porre rischi sistemici sia centralizzato anche per quanto riguarda l'*enforcement* dell'AI *Act*. A tale fine verrebbe istituito un altro organo a livello europeo (denominato "Ufficio IA") che dovrebbe operare in seno alla Commissione Europea, seppur dotato di indipendenza funzionale. Non sono ancora del tutto chiari i rapporti che l'Ufficio IA avrebbe con gli altri organi di *Governance* (vedi sopra punto 2b).

3) Le tempistiche di approvazione dell'AI *Act*

Il prossimo trilogo avverrà in data 6 dicembre 2023.

---

elementi accessori di una valutazione umana, o a svolgere compiti preparatori. A riguardo, detti criteri sono stati parzialmente rivisti nel successivo trilogo, tuttavia mantenendosi il caposaldo per cui qualsiasi sistema di intelligenza artificiale che effettui la profilazione delle persone sarà considerato ad alto rischio, a nulla valendo i detti criteri. Inoltre, la Commissione avrebbe il compito di sviluppare un elenco completo di esempi pratici volti a chiarire cosa sia "alto" o "non alto" rischio; e avrebbe la facoltà di aggiungere nuovi filtri ma solo laddove vi siano prove concrete e affidabili che i sistemi di IA non rientrino nella categoria ad alto rischio pur senza comportare un rischio significativo per le persone.

[9] I modelli di fondazione sono una tipologia di intelligenza artificiale generativa (AI generativa). Generano *output* da uno o più *input* (*prompt*) sotto forma di istruzioni in linguaggio umano. In altre parole, tali modelli sono in grado di utilizzare schemi e relazioni appresi per prevedere l'elemento successivo in una sequenza.
Nei documenti di preparazione ai trilogi predisposti dalla Presidenza spagnola del Consiglio dell'Unione, tale modello viene definito come "… *AI model that is capable to competently perform a wide range of distinctive tasks …*".

[10] La proposta di Regolamento emendata al 14 giugno 2023 già aveva introdotto il nuovo articolo 28 ter, che statuisce una serie di obblighi per i fornitori dei modelli di fondazione.

[11] Verrebbe stabilito un sistema di classificazione su più livelli tale per cui si introdurrebbe una nuova categoria di modelli "molto capaci" (o "ad alto impatto") soggetti ad obblighi aggiuntivi e qualificati sulla base di parametri (ampiamente oggetto di discussione) come la potenza di calcolo utilizzata per la formazione, i dati consumati per l'addestramento, il potenziale impatto sugli utenti. Ancora, tali modelli dovrebbero essere sottoposti a regolari verifiche da parte di enti esterni e a controlli di conformità da parte di revisori indipendenti, oltre a stabilire un sistema di mitigazione dei rischi prima dell'accesso al mercato. Si auspicherebbe peraltro un terzo livello comprendente i sistemi di intelligenza artificiale di uso generale costruiti su modelli di fondazione e utilizzati su larga scala. Qui, gli obblighi includerebbero un controllo esterno e la creazione di un sistema di mitigazione del rischio. Infine, tutti i fornitori di AI per scopi generici dovrebbero dichiarare se il loro sistema può essere utilizzato per usi ad alto rischio e agire di conseguenza con gli opportuni presidi.

Come abbiamo visto, vi sono ancora dei punti abbastanza importanti da “definire”.

Ciononostante, si auspica da più parti che questo possa essere l’ultimo negoziato interistituzionale e che possa portare direttamente alla definizione finale del testo. Sono dunque previste febbrili negoziazioni in quest’ultimo mese.

A condizione che si raggiunga un accordo in sede europarlamentare entro la fine del corrente anno, il Regolamento potrebbe poi entrare in vigore intorno alla metà del 2024[12].

Tale sviluppo sarebbe effettivamente un atto di portata rivoluzionaria dato che darebbe all’Europa la “palma” di primo attore a regolamentare tale materia.

L’AI *Act* potrebbe diventare dunque in futuro uno tra i principali *standard* globali a cui fare riferimento per la regolamentazione dell’intelligenza artificiale. Quanto meno sul lato legislativo, dunque, l’Europa potrebbe dunque guadagnare importante terreno in questo campo rispetto agli altri *player* globali.

[12] Occorre considerare che l’AI Act prevede un periodo transitorio di 24 mesi dalla sua entrata in vigore al fine di preparare tutti gli attori coinvolti all'impatto che l'AI Act comporterà in termini di compliance (Si veda l’articolo 85 della proposta di Regolamento).

Jacopo Piemonte

ASSOCIATE

j.piemonte@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 – Milano
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles

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
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com