Osservatorio sui
Conti Pubblici Italiani
https://osservatoriocpi.unicatt.it
osservatoriocpi@unicatt.it

Osservatorio sui Conti Pubblici Italiani

Osservatorio sui Conti Pubblici Italiani

@osservatoriocpi

Osservatorio CPI

Direttore: Giampaolo Galli

Il commento

OCPI

Il nuovo regolamento europeo sull'IA: cosa cerca di fare e cosa fa

di Alessio Capacci, Giampaolo Galli, Andrea Loreggia e Ilaria Maroccia

22 febbraio 2024

Non c'è dubbio che l'Intelligenza Artificiale (IA) necessiti di una qualche forma di regolazione. Non sappiamo bene quali siano i rischi, anche perché non sappiamo cosa sarà in grado di fare l'IA fra sei mesi o fra tre anni. Ma sappiamo che dei rischi esistono. A fronte di una tecnologia sfuggente e in rapidissima evoluzione, il legislatore ha prodotto un testo legislativo lungo, tortuoso, di difficilissima interpretazione, che assomiglia più a una legge delega che a un regolamento; un testo pieno di incertezze e ambiguità. Dunque, l'AI Act è modesto dal punto di vista della tecnica legislativa, ma forse, data la natura sfuggente dell'oggetto regalato, era difficile fare diversamente. I suoi effetti saranno valutabili solo dopo che saranno state emanate le decine di atti secondari (deleghe, regolamenti europei e norme nazionali) che sono previste. Molto dipenderà da come gli Stati membri recepiranno la normativa. Un rischio è quello che si istituiscano autorità europee e nazionali molto costose, in quanto dotate di personale specializzato in tante materie diverse, che legittimamente cercheranno di operare come previsto dalla norma e finiranno per oberare le imprese di oneri entrando in contrasto con le autorità di settore; un esito del genere sarebbe un serio ostacolo all'innovazione nell'Unione europea.[1]

* * *

L'intelligenza artificiale (IA) sta portando una serie di benefici economici,[2] ma comporta anche rischi e solleva questioni etiche e giuridiche. Per questo, la Commissione europea ha proposto un regolamento (l'AI Act), volto a regolarne lo sviluppo nell'Unione.

L'AI Act, proposto dalla Commissione nell'aprile 2021, dopo varie revisioni, ha ottenuto il voto unanime del Consiglio dei rappresentanti permanenti degli

[1] Gli autori ringraziano Ettore Russo di Anitec-Assinform per molti utili suggerimenti. Le opinioni espresse e gli eventuali errori o imprecisioni sono da attribuire interamente agli autori della nota.

[2] Si veda la nostra precedente nota "Verso il G7 sull'Intelligenza Artificiale".

Stati membri dell'Unione (Coreper) il 2 febbraio 2024.[3] Si attende ora il voto finale dell'Europarlamento, previsto per il 24 aprile.

Obiettivi generali e classi risk-based

L'obiettivo del legislatore è quello di promuovere l'uso dell'intelligenza artificiale nell'Unione, garantendo al contempo la tutela della salute, della sicurezza e dei diritti fondamentali degli individui. Per questo vengono regolati l'immissione sul mercato e l'utilizzo dei sistemi di IA, coprendo tutti gli operatori coinvolti nell'Unione (produttori, sviluppatori, importatori, distributori e utilizzatori).

In linea di principio e salvo eccezioni, l'AI Act classifica i sistemi di IA in base ai rischi legati non alla tecnologia, ma al loro utilizzo. I sistemi di IA sono classificati come: (i) a rischio minimo (per esempio quelli utilizzati nei videogiochi, nelle raccomandazione delle piattaforme di streaming e nell'e-commerce), per i quali non è previsto alcun obbligo; (ii) a rischio limitato, per i quali sono previsti obblighi di trasparenza, nel senso che gli utenti dovranno essere consapevoli di stare interagendo con un sistema IA; (iii) a rischio alto, che avranno bisogno di una specifica autorizzazione per poter essere immessi sul mercato; e (iv) a rischio inaccettabile, che sono vietati.

Sistemi di IA vietati

L'AI Act contiene un elenco (non esaustivo delle fattispecie regolate dal diritto penale) di sistemi di IA vietati.[4] Fra questi vi sono: i sistemi che usano tecniche subliminali o manipolative, o che sfruttano la vulnerabilità degli individui in base a età, disabilità o status socio-economico; sistemi che categorizzano gli individui in base a razza, opinioni politiche, orientamento sessuale, comportamento sociale o tratti della personalità, con trattamento discriminatorio o comunque ingiusto; sistemi che usano strumenti di identificazione biometrica da remoto in tempo reale negli spazi pubblici; sistemi che usano strumenti di valutazione del rischio per prevedere il comportamento criminale basandosi esclusivamente su profili o tratti della personalità; sistemi che creano o ampliano database di riconoscimento facciale attraverso lo scraping (raccolta massiva) non mirato di immagini.

Sistemi di IA ad alto rischio

[3] Il testo dell'accordo del 2 febbraio è disponibile al seguente link. Tutti gli articoli citati nella nota si riferiscono a questa versione del regolamento.
[4] Si veda l'articolo 5 dell'AI Act.

Sono considerati ad alto rischio,[5] per esempio, i sistemi usati per fini biometrici, come nell'identificazione da remoto, nel riconoscimento delle emozioni manifestate dall'utente o nella categorizzazione dell'individuo sulla base di attributi personali; per operare infrastrutture critiche, come nel controllo del traffico su strada, la gestione delle acque, del gas, del riscaldamento o dell'elettricità; in ambito educativo, per esempio per determinare l'idoneità di uno studente a un certo programma scolastico; per filtrare curriculum di candidati, o per monitorare i dipendenti; per determinare il diritto all'accesso dei servizi sanitari, pubblici o privati, o per valutare le prove raccolte durante un'indagine da parte delle autorità giudiziarie.

Prima di immettere un prodotto sul mercato, il produttore dovrà stilare una documentazione tecnica che dovrà indicare, tra le altre cose: lo scopo del sistema; il modo con cui il sistema interagisce con hardware e software o con sistemi IA esterni; tutti gli elementi e le componenti che costituiscono il sistema e il processo che ha portato al suo sviluppo; gli algoritmi e le ipotesi necessarie per il suo funzionamento e tutti gli elementi forniti da terzi, specificando se sono stati modificati dal produttore.

Si tratta di una documentazione molto complessa. Per esempio, non è chiaro come si possano prevedere le modalità con cui il sistema interagisce con qualsiasi potenziale sistema di IA esterno, in considerazione anche della velocità con cui cresce la tecnologia.

Dovranno essere istituiti anche un sistema di risk management e uno di quality management, che dovranno essere attivi per tutto il periodo di utilizzo del sistema ed essere aggiornati periodicamente.[6]

Monitoraggio e attività post-vendita

Una volta che il prodotto viene immesso sul mercato, i produttori dei sistemi di IA ad alto rischio dovranno elaborare un programma di monitoraggio post-vendita proporzionato ai rischi del sistema immesso. Sarà necessaria quindi un'analisi dei dati sulle prestazioni della IA per la durata di utilizzo del prodotto, in modo da verificarne la continua conformità con il regolamento.[7]

Nei 10 anni dopo l'immissione del prodotto i produttori dovranno conservare la documentazione tecnica, la documentazione relativa al sistema di quality management e quella riguardante eventuali cambiamenti approvati dalle autorità competenti. Dovranno inoltre conservare i 'logs' (i.e., gli eventi)

[5] Si veda articolo 6 e l'Allegato III.
[6] Si veda l'articolo 9.
[7] Si veda l'articolo 61.

generati dai sistemi per 6 mesi, salvo se diversamente disposto dall'Unione o dallo Stato membro.[8]

Infine, i produttori dovranno riportare qualsiasi incidente grave alle autorità di sorveglianza dei rispettivi Stati membri.[9] Qualora il produttore concludesse in base a nuovi sviluppi che il sistema possa rappresentare un rischio alla sicurezza degli utenti dovrà informare immediatamente le autorità competenti.[10]

La governance

Il Titolo VI dell'AI Act definisce un'architettura di governance assai complessa e potenzialmente pesante da istituire su scala nazionale ed europea. A livello europeo dovranno essere istituiti:

1. un AI Office, che farà parte della Commissione con la responsabilità di fornire linee guida per facilitare l'applicazione dell'AI Act e la creazione dei sandbox normativi nell'Unione;[11]

2. uno European Artificial Intelligence Board, composto da un rappresentante per Stato membro. Il Board assisterà Commissione e Stati membri nell'applicazione dell'AI Act e contribuirà all'armonizzazione delle pratiche tra autorità nazionali responsabili dell'applicazione del regolamento;

3. un Advisory Forum composto da stakeholders, figure legate al mondo dell'IA e provenienti dal privato e dal mondo accademico. Il Forum fornirà consulenza tecnica al Board e alla Commissione;

4. un Comitato scientifico, formato da esperti indipendenti scelti dalla Commissione, il cui scopo sarà di supportare l'AI Office nell'implementazione del regolamento, qualora richiesto.[12]

A livello nazionale, ciascuno Stato membro dovrà istituire almeno:

5. un'autorità "di notifica" responsabile di istituire e attuare le procedure necessarie per la valutazione e notifica degli organismi di valutazione della conformità dei sistemi ad alto rischio e per il loro monitoraggio;

6. un'autorità di sorveglianza del mercato, con poteri investigativi e correttivi, compreso quello di accedere ai dati personali in fase di elaborazione e alle informazioni necessarie per eseguire i loro compiti.

[8] Si vedano gli articoli 12 e 20.
[9] Si veda l'articolo 62.
[10] Si veda l'articolo 21.
[11] Sull'AI Office, si veda il seguente link.
[12] Si veda l'articolo 58b.

"AI regulatory sandboxes"

Gli stati membri dovranno istituire una o più 'AI Regulatory Sandbox', al fine di fornire un sistema controllato che favorisca l'innovazione e agevoli lo sviluppo di tecnologie IA all'interno dell'Unione. L'istituzione di questi sandbox normativi mira soprattutto ad agevolare l'accesso dei sistemi di IA al mercato europeo, in particolare per le piccole-medie imprese e le start-ups.

"General-Purpose AI Models"

Una buona parte delle applicazioni che fanno uso di IA sono progettate per eseguire compiti specifici e circoscritti. Esistono tuttavia dei sistemi di IA che possono essere impiegati per svolgere un'ampia gamma di compiti. Il termine "General-Purpose AI Systems" (GPAI), è stato definito per identificare questi modelli. Questi sistemi possono portare a nuove opportunità di sviluppo e innovazione, ma, secondo il legislatore, la grande quantità di dati richiesta per il loro sviluppo può rappresentare anche un rischio in termini di privacy e di cybersecurity.

Va detto che questo ragionamento si allontana dall'approccio basato sul rischio dell'utilizzo, che è invece alla base del resto dell'AI Act; un Large Language Model può avere dimensioni molto grandi, ma essere del tutto innocuo perché per esempio nel suo utilizzo è previsto che si limiti a dare suggerimenti con linguaggio naturale. Inoltre, porre limiti quantitativi a un sistema può significare limitare o comunque rallentare lo sviluppo della tecnologia.

L'AI Act delinea i principi per regolamentare i modelli GPAI a livello europeo.[13] In particolare, il regolamento definisce un modello come "GPAI a rischio sistemico" se, per essere sviluppato, è stata superata una certa quantità cumulata di potenza di calcolo.

La supervisione a livello europeo sui sistemi GPAI verrà affidata all'AI Office. Avendo i poteri di sorveglianza del mercato, l'ufficio dovrà essere in grado di compiere tutte le azioni necessarie per monitorare l'effettiva attuazione di quanto previsto dal regolamento. In particolare, l'ufficio dovrà essere in grado di verificare le possibili violazioni delle norme da parte dei produttori dei modelli GPAI sia su propria iniziativa, in base alle proprie attività di monitoraggio, sia su richiesta delle altre autorità competenti.

[13] Come specificato dall'articolo 3(44d), un rischio sistemico a livello europeo si riferisce al rischio specifico rappresentato dal possibile impatto che un modello GPAI può avere sul mercato interno e sui potenziali effetti negativi che un suo utilizzo può avere sulla salute pubblica, la sicurezza e i diritti fondamentali degli individui.

Indipendentemente dal rischio sistemico, i produttori di sistemi GPAI dovranno redigere una documentazione tecnica del modello. La documentazione dovrà comprendere: una descrizione del sistema (per esempio, i compiti che deve svolgere, il numero di parametri utilizzati, la data di rilascio del prodotto e la sua modalità di distribuzione, ecc.); un riassunto dello sviluppo del modello; le specifiche di tutte le tecniche e le risorse utilizzate a questo fine.[14] I produttori di modelli di GPAI che presentano un potenziale rischio sistemico dovranno eseguire tutti questi compiti, e in più dovranno porre un'attenzione particolare alle potenziali esternalità negative che potrebbero ricadere sul mercato unico; sarà richiesto inoltre un maggior livello di cybersecurity del sistema.[15]

Un commento

In un'audizione alla Camera dei Deputati del 14 febbraio scorso l'amministratore delegato di Leonardo, Roberto Cingolani, ha detto che il rischio dell'AI Act è quello di "fare il codice della strada prima di avere le automobili e la strada".[16] Il problema è che in Europa ci sono pochissime aziende che fanno IA e mancano, o sono insufficienti, alcune delle infrastrutture o delle componenti critiche (cloud computing, cybersecurity, produzione di microchips). Inoltre, non è chiarissimo come si possa normare un fenomeno che cambia con una velocità enorme, quali siano i confini dell'Intelligenza Artificiale (che in varie forme esiste da decine di anni) e, soprattutto, come si possano governare fenomeni enormemente diversi fra di loro con un unico atto normativo e con autorità dedicate ad hoc. Un'auto a guida autonoma è cosa del tutto diversa da un Large Language Model, o da un sistema che suggerisce diagnosi mediche, oppure la bozza di una sentenza o un metodo di apprendimento per gli studenti. Ognuno di questi utilizzi dell'IA pone problemi etici e giuridici diversi e soprattutto richiede specializzazioni diverse: ingegneri elettronici, giuristi, medici, pedagoghi, filosofi ecc.

Al netto del caso delle banche, che hanno un trattamento particolare,[17] l'AI Act sembra avere l'ambizione di governare tutte le autorizzazioni di prodotti che hanno un qualche contenuto di IA, ma ovviamente non riesce a spingersi fino a questo punto perché travalicherebbe le competenze di autorità consolidate. Di qui deriva una certa difficoltà a comprendere gli effetti reali del Regolamento. Si consideri l'esempio di un'automobile con un'elevata

[14] Per maggiori informazioni sulla documentazione tecnica richiesta per i produttori di modelli di GPAI si veda l'articolo 52 e l'Allegato IXa. Per i produttori di sistemi IA che fanno utilizzo di modelli di GPAI nel loro prodotto si veda l'allegato IXb.
[15] Per maggiori informazioni sugli obblighi dei produttori di modelli GPAI con rischi sistemici si veda l'articolo 52d.
[16] Si veda l'audizione sull'Indagine conoscitiva sull'Intelligenza artificiale, disponibile al seguente link.
[17] Si veda a questo link il parere reso dalla BCE su una precedente bozza del regolamento.

componente di automazione intelligente. Quale sarà l'autorità competente per le verifiche prima e dopo l'immissione sul mercato? Quale autorità avrà i poteri ispettivi necessari per verificare la compliance dopo l'immissione sul mercato? Immaginiamo che, come avviene attualmente, i controlli ex-post (ossia su strada) spetteranno alle forze di polizia. Che rapporto ci sarà fra queste e le autorità preposte ai controlli sull'IA?

Forse per i motivi detti sopra, o forse per l'esigenza di trovare compromessi fra tante spinte diverse, l'AI Act è un documento assai lungo, complesso e a tratti tortuoso. Inoltre, moltissime delle disposizioni che contano saranno definite in atti legislativi (deleghe) e regolamentari successivi. Ciò rende anche difficile dare un giudizio; molto dipende da come la Commissione e gli Stati membri applicheranno le disposizioni del Regolamento.

Si consideri infatti quanto segue.

1. Dimensioni. L'AI Act è composto da 88.610 parole. Per confronto, il regolamento generale sulla sicurezza dei prodotti non alimentari e non farmaceutici (che regola la quasi totalità dei prodotti immessi sul mercato, anche on line)18 è composto da 29.409 parole, poco più di un terzo dell'AI ACT. Una dimensione maggiore (118.006 parole) la si trova, per esempio, nel testo unico bancario del 1993 (con le decine di aggiornamenti ad oggi, come riferiti nel testo pubblicato dalla Banca d'Italia).19 Si noti che il Testo unico bancario, al pari dell'AI Act, regola anche le governance, ossia l'architettura, i poteri e il funzionamento delle autorità di vigilanza.

2. Atti normativi successivi. Gli atti successivi a carico della Commissione sono moltissimi. L'espressione "delegated act" (decreti delegati che richiedono l'approvazione del Parlamento) compare ben 34 volte. L'espressione "implemeting act" (regolamenti che non richiedono la successiva approvazione del Parlamento") compare 39 volte. A questi bisogna aggiungere le norme con cui i 27 stati membri recepiranno il Regolamento, per esempio per quanto riguarda l'individuazione delle authority e delle loro risorse umane e materiali. Il rinvio ad atti successivi può essere vista come una intelligente scelta di flessibilità a fronte di una tecnologia che evolve molto rapidamente, ma rivela anche una certa difficoltà a incapsulare una materia tanto complessa in un unico atto normativo.

3. L'espressione "fundamental rights" compare ben 170 volte. In 117 casi è accompagnato dalla parola "safety" (sicurezza") e in 74 casi dalla parola "health" (salute), il che testimonia della complessità e forse della tortuosità

[18] Si veda il seguente link.
[19] Si veda il seguente link.

del documento. L'impressione che se ne ricava è che persino su concetti di fondo come quelli dei diritti fondamentali, della salute e sicurezza si nutrano tanti dubbi applicativi. E si senta la necessità di prevedere singoli casi, eccezioni, rafforzativi, deleghe a futura memoria. Ad esempio, l'articolo 6(2) prevede che tutti i sistemi minuziosamente elencati nell'Allegato III (che definisce i sistemi ad alto rischio) siano considerati ad alto rischio. Tuttavia il successivo comma 2a, stabilisce che: "In deroga al paragrafo 2, i sistemi di IA non sono considerati ad alto rischio se non presentano un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali delle persone fisiche, inclusi quelli che non influenzano materialmente l'esito del processo decisionale" (evidenziazione nostra). Dunque, in buona sostanza, sono ad alto rischio tutte le attività elencate nell'allegato III, salvo quello che non lo sono. Se non bastasse nel successivo comma 2d, una delega chiede alla Commissione di fare esattamente il contrario e cioè di allungare l'elenco dei rischi, ma solo quando "vi siano prove concrete e attendibili che ciò sia necessario al fine di mantenere il livello di protezione della salute, della sicurezza e dei diritti fondamentali nell'Unione". E ancora, a scanso di equivoci, alla riga successiva si dice che "qualsiasi modifica dei criteri […] non riduce il livello generale di protezione della salute, della sicurezza e dei diritti fondamentali nell'Unione". Forse repetita iuvant. Ma qui le ripetizioni danno l'impressione di grande incertezza su cosa possa comportare dei rischi per i diritti, la salute e la sicurezza.

4. GPAI. L'espressione GPAI (General Purpose AI) compare ben 362 volte. Il fatto è che l'impostazione originaria dell'AI Act (regolare gli utilizzi rischiosi, non la tecnologia di per sé) è stata messa in crisi quando OpenAI ha reso pubblico ChatGPT. Questo LLM può avere tanti utilizzi diversi ed è dunque difficile classificarne la rischiosità in base agli utilizzi. Questo ha reso necessario aggiungere un intero Titolo (VIIIA) e vari articoli (dal 52a al 52e) dedicati al tema. Inoltre, in tutti gli articoli che riguardano le procedure per i sistemi ad alto rischio è stato necessario aggiungere anche i GPAI.

5. Governance. Come si è visto sopra, l'architettura delle autorità di controllo è assai elaborata. Si creano quattro nuove strutture al centro (AI Office presso la Commissione, l'AI Board composto da rappresentanti degli Stati membri, l'Advisory Forum composto dagli stakeholders e il Comitato Scientifico formato da esperti scelti dalla Commissione) e due in ogni stato membro: una notifiying authority e una autorità di controllo. Quest'ultima dovrà essere dotata di una notevole compagine di personale per soddisfare i requisiti dell'articolo 59(4) che detta: "L'autorità nazionale competente dispone di un numero sufficiente di personale permanentemente

disponibile le cui competenze includono una conoscenza approfondita delle tecnologie dell'intelligenza artificiale, dei dati e dell'informatica, della protezione dei dati personali, della sicurezza informatica, dei diritti fondamentali, dei rischi per la salute e la sicurezza e conoscenza delle norme esistenti e dei requisiti legali". In considerazione dei tanti utilizzi che si possano già oggi fare dell'IA è facile prevedere che ci vorranno centinaia di esperti per soddisfare questi requisiti. Ed è facile prevedere conflitti con le autorità di settore. Per esempio, non è chiaro quale autorità sia preposta alla tutela della privacy: all'apparenza, gran parte del AI Act è costruito per tutelare la privacy, in quanto diritto fondamentale della persona, ma sul tema già vigilano le autorità garanti per la protezione dei dati personali.

In sintesi

Non c'è dubbio che l'IA necessiti di una qualche forma di regolazione. Non sappiamo bene quali siano i rischi, anche perché non sappiamo cosa sarà in grado di fare l'IA fra sei mesi o fra tre anni. Ma sappiamo che dei rischi esistono. L'IA scava in ogni anfratto di Internet, può trovare una conversazione su un social network che non sia stata schermata e rilanciarne i contenuti a milioni di persone. Può mettere in bocca a una figura pubblica parole che non ha mai detto e con questo rovinarne la reputazione. Vi sono poi tanti rischi nel momento in cui si affida alla macchina la decisione finale, come avviene nel caso delle automobili a guida autonoma.

Idealmente la regolazione dovrebbe limitarsi a rendere operativi i sette principi che sono enunciati nel preambolo dell'AI Act (punto 14a): "azione umana e supervisione; robustezza tecnica e sicurezza; privacy e governance dei dati; trasparenza; diversità, non discriminazione ed equità; benessere; responsabilità sociale e ambientale".

Il fatto è che per dare attuazione a questi principi, a fronte di una tecnologia sfuggente e in rapida evoluzione, il legislatore ha fatto ricorso ad un testo legislativo lungo, tortuoso, di difficilissima interpretazione, che assomiglia più a una legge delega che a un regolamento. In sostanza, si tratta di un testo pieno di incertezze e ambiguità.

Dal punto di vista dei big tech che producono le fondamentali innovazione in materia di IA, queste caratteristiche del testo non sono particolarmente problematiche, perché essi hanno le risorse umane a materiali necessarie per adeguare i sistemi a una regolazione complessa.

Diverso può essere l'effetto sulle PMI e sulle startup, a meno che i paesi membri non riescano a mettere in azione delle "sandbox" efficienti, ossia degli ambienti protetti che aiutino effettivamente le PMI a testare i loro sistemi e adeguarsi alla normativa.

In conclusione, l'AI Act è molto modesto dal punto di vista della tecnica legislativa, ma forse, data la natura sfuggente dell'oggetto regalato, era difficile fare diversamente. I suoi effetti saranno valutabili solo dopo che saranno state emanate le decine di atti secondari (deleghe, regolamenti europei e norme nazionali) che sono previste nell'AI Act. Molto dipenderà da come gli stati membri recepiranno la normativa; come sempre, possono complicare ulteriormente la normativa con il cosiddetto "gold plating", oppure possono recepire la norma europea creando al tempo stesso un ambiente favorevole all'innovazione. Anche in questo caso l'ambiguità delle norme dell'AI Act può aiutare, nel senso che non ci sembra che esso contenga norme cogenti che impediscono a uno stato membro di sviluppare un ecosistema favorevole all'innovazione. Un rischio è quello che si istituiscano autorità europee e nazionali molto costose, in quanto dotate di personale specializzato in tante materie diverse, che legittimamente cercheranno di operare come previsto dalla norma e finiranno per oberare le imprese di oneri entrando in contrasto con le autorità di settore; un esito del genere sarebbe un serio ostacolo all'innovazione nell'Unione europea.