LA PROPOSTA DI REGOLAMENTO EUROPEO IN MATERIA DI INTELLIGENZA ARTIFICIALE (IA)

Commissione Europea - Comunicazione del 21 aprile 2021

Di fronte al rapido sviluppo tecnologico dell'IA e a un contesto politico globale in cui sempre più paesi stanno investendo massicciamente nell'IA, l'Unione Europea intende agire per sfruttare le numerose opportunità e affrontare le relative sfide. Per promuovere lo sviluppo e affrontare i rischi potenziali elevati che comporta per la sicurezza e per i diritti fondamentali, la Commissione Europea ha presentato sia una proposta per un quadro normativo sia un piano coordinato rivisto sull'IA.

di Elena BASSOLI, avvocato di diritto e nuove tecnologie; è docente di "Diritto della comunicazione elettronica" presso l'Università di Genova, nonché del Master Universitario di II Livello in Cyber Security and Data Protection, presso il DIBRIS Unige, autore di oltre 250 pubblicazioni in materia dal 1995 ad oggi; è Formatore per il Ministero di Giustizia e già per il Ministero dell'Interno. È inoltre Presidente nazionale ANGIF (Associazione nazionale giuristi informatici e forensi) e CSIG-Genova (Centro studi informatica giuridica).

1. Premessa

Gli ultimi 3 anni sono stati densi di novità a livello europeo sui temi dell'intelligenza artificiale. Il tessuto normativo sul quale si innesta il nuovo Regolamento IA, in via di emanazione, pubblicato sotto forma di proposta il 21 aprile 2021 dalla Commissione, dunque, non è il primo a tentare la regolamentazione della delicata materia dell'algoritmizzazione dei diritti umani. È tuttavia il primo atto normativo con forza di Regolamento, e di ciò occorre tenere conto in relazione alla sua cogenza ed applicabilità diretta in tutti e 27 i Paesi membri dell'Unione.

L'applicabilità diretta del Regolamento, ai sensi dell'articolo 288 del TFUE, dovrebbe ridurre, nelle intenzioni del legislatore, la frammentazione giuridica e facilitare lo sviluppo di un mercato unico per sistemi di IA.

Per approcciarsi correttamente alla materia occorre quindi tenere presenti anche la proposta di Regolamento sulle macchine [COM (2021) 202 final], che stabilisce i requisiti di sicurezza dei prodotti, sostituendo l'attuale "Direttiva Macchine" n. 2006/42/CE; la consultazione pubblica sul Libro Bianco sull'Intelligenza Artificiale (COM 2020) 65 final del 19 febbraio 2020); le Linee guida etiche finali per un'intelligenza artificiale affidabile, del Gruppo ad alto livello sull'intelligenza artificiale, pubblicate l'8 aprile 2019; il Rapporto sulla responsabilità per l'Intelligenza Artificiale e altre tecnologie emergenti, del Gruppo di esperti sulla responsabilità e le nuove tecnologie, pubblicato il 21 novembre 2019 ed, infine, la Dichiarazione di cooperazione sull'intelligenza artificiale, firmata da 25 paesi europei il 10 aprile 2018, che si basa sui risultati e sugli investimenti della comunità europea della ricerca e delle imprese nell'IA e stabilisce le basi per il Piano coordinato sull'IA.

Traspare dalla bozza di Regolamento come la Commissione europea abbia individuato specifiche finalità della regolamentazione, conscia che l'uso dell'intelligenza artificiale può supportare risultati vantaggiosi dal punto di vista sociale e ambientale e fornire vantaggi competitivi fondamentali alle imprese e all'economia europea, in particolare nei settori ad alto impatto, tra cui il cambiamento climatico, l'ambiente, il settore pubblico, le finanze, la mobilità, gli affari interni e l'agricoltura.

Tuttavia, gli stessi elementi e tecniche che alimentano i benefici socioeconomici dell'IA possono comportare nuovi rischi o conseguenze negative per gli individui o la società. Il Regolamento si propone di disciplinare la materia in modo che i cittadini possano confidare che le tecnologie di IA siano utilizzate in modo sicuro e conforme alla legge, con particolare attenzione al rispetto dei diritti fondamentali.

2. Gli obiettivi del Regolamento IA

Il quadro normativo proposto dalla Commissione si pone i seguenti obiettivi specifici:

- garantire che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino il diritto esistente in materia di diritti fondamentali e valori dell'Unione;
- garantire la certezza del diritto per facilitare gli investimenti e l'innovazione nell'IA;
- migliorare la *governance* e l'effettiva applicazione della legge esistente sui diritti fondamentali e sui requisiti di sicurezza applicabili ai sistemi di IA;
- facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili ed evitare la frammentazione del mercato.

La proposta stabilisce una metodologia di rischio per l'individuazione e la definizione di sistemi di IA "ad alto rischio" che pongono rischi significativi per la salute e la sicurezza o i diritti fondamentali delle persone.
I sistemi "ad alto rischio" dovranno rispettare una serie di requisiti obbligatori e seguire procedure di valutazione della conformità, prima di poter essere immessi sul mercato dell'Unione. Obblighi prevedibili, proporzionati e chiari sono imposti anche ai fornitori e agli utenti di tali sistemi per garantire la sicurezza e il rispetto della legislazione posti a tutela dei diritti fondamentali durante l'intero ciclo di vita dei sistemi di IA.

Per alcuni sistemi di IA specifici vengono proposti obblighi minimi di trasparenza, in particolare quando vengono utilizzati chatbot o *deep fake*.
Le norme del Regolamento saranno applicate attraverso un sistema di governance a livello di Stati membri, sulla base di istituti già esistenti, e un meccanismo di cooperazione a livello dell'Unione con l'istituzione di un comitato europeo per l'intelligenza artificiale.

3. La disciplina europea dell'IA

Il Regolamento si apre con il campo di applicazione delle nuove norme che riguardano l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA, e fornisce le definizioni utilizzate all'interno dell'atto. La nuova disciplina prevede un elenco di sistemi IA vietati, seguendo un approccio basato sul rischio, differenziando tra gli usi dell'IA che creano:

- un rischio inaccettabile;
- un rischio elevato;
- un rischio basso o minimo.

L'elenco delle pratiche vietate di cui al titolo II comprende tutti i sistemi di IA il cui uso è considerato inaccettabile in quanto in contrasto con i valori dell'Unione, ad esempio perché viola i diritti fondamentali o perché possiede un potenziale significativo di manipolazione delle persone attraverso tecniche subliminali o perché sfrutta vulnerabilità di specifici gruppi come bambini o persone con disabilità al fine di distorcere materialmente il loro comportamento in modo tale da causare loro o a un'altra persona danni psicologici o fisici.

Per quanto riguarda persone fisiche adulte il Regolamento demanda alla legislazione vigente in materia di protezione dei dati, di protezione dei consumatori e di servizi digitali la protezione contro pratiche manipolatorie che potrebbero essere implementate nei sistemi di IA, anche tramite adeguate informative, ove venga esplicitata la libera scelta di non essere soggette a profilazione o ad altre pratiche che potrebbero influire sul loro comportamento.
La proposta vieta inoltre il punteggio sociale basato sull'IA svolto dalle autorità pubbliche e l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico ai fini dell'applicazione della legge, a meno che non si applichino alcune eccezioni limitate.

4. I rischi dell'IA

Nell'ambito della Strategia europea per l'Intelligenza Artificiale, la Commissione europea ha quindi pubblicato il 21 aprile, la proposta di Regolamento sull'approccio europeo all'Intelligenza Artificiale [COM (2021) 206 final], che propone il primo quadro giuridico europeo sull'IA.
La proposta valuta i rischi dell'Intelligenza Artificiale, con la finalità di salvaguardare i valori e i diritti fondamentali dell'UE e la sicurezza degli utenti e si prevede, a tal fine, anche un nuovo piano coordinato sull'Intelligenza Artificiale 2021 [COM (2021) 205 final] avente il compito di incrementare l'adozione dell'IA, gli investimenti e l'innovazione nel settore di tutta l'Unione.
In generale, nella proposta di Regolamento si prevedono regole di trasparenza armonizzate applicabili a tutti i sistemi di IA, mentre sono previste specifiche disposizioni per i sistemi di IA classificati "ad alto rischio", per i quali viene introdotta una definizione *ad hoc*, affinché rispettino determinati requisiti obbligatori relativi alla loro affidabilità.

In linea con un approccio basato sul rischio, tali sistemi di IA "ad alto rischio" sono consentiti nel rispetto di determinati requisiti obbligatori e di una valutazione ex ante della conformità.
La classificazione di un sistema di IA, come ad alto rischio, si basa sullo scopo previsto del sistema di IA in linea con la legislazione vigente in materia di sicurezza dei prodotti. Pertanto, la classificazione come "ad alto rischio" non dipende solo dalla funzione svolta dal sistema di IA, ma anche dalle specifiche modalità e finalità per le quali tale sistema viene utilizzato.

Il Regolamento stabilisce le regole di classificazione e identifica due categorie principali di sistemi di IA "ad alto rischio":

- Sistemi di IA destinati ad essere utilizzati come componenti di sicurezza dei prodotti soggetti a valutazione di conformità ex ante;
- altri sistemi di IA autonomi con implicazioni principalmente in materia di diritti fondamentali che sono esplicitamente elencati nell'allegato III, il quale contiene un numero limitato di sistemi di IA i cui rischi si sono già materializzati o probabilmente si materializzeranno nel prossimo futuro.

Il Regolamento definisce i requisiti legali per i sistemi di IA ad alto rischio in relazione alla governance dei dati, alla documentazione e alla conservazione delle registrazioni, alla trasparenza e alla fornitura di informazioni agli utenti, alla supervisione umana, alla robustezza, all'accuratezza e alla sicurezza.
I sistemi di IA destinati ad essere utilizzati come componenti di sicurezza dei prodotti disciplinati dalla nuova legislazione quadro legislativa (ad esempio macchinari, giocattoli,

dispositivi medici, ecc.) saranno soggetti agli stessi meccanismi di conformità e applicazione ex ante ed ex post dei prodotti di cui sono componenti. La differenza fondamentale è che i meccanismi *ex-ante* ed *ex post* garantiranno il rispetto non solo dei requisiti stabiliti dalla legislazione settoriale, come la già vigente responsabilità del produttore, ma anche dei requisiti stabiliti dal Regolamento.
Il Regolamento impone determinati obblighi di trasparenza per i sistemi che:

- interagiscono con gli esseri umani,
- sono utilizzati per rilevare le emozioni o determinare l'appartenenza a categorie sociali basate sui dati biometrici,
- generano o manipolano contenuti ("*deep fake*").

Quando le persone interagiscono con un sistema di IA o le loro emozioni o caratteristiche sono riconosciute con mezzi automatizzati, le persone devono essere informate di tale circostanza.
Se un sistema di intelligenza artificiale viene utilizzato per generare o manipolare contenuti di immagini, audio o video che assomigliano in maniera sensibile a contenuti autentici, dovrebbe esserci l'obbligo di rivelare che il contenuto è generato con mezzi automatizzati.

5. I sistemi di IA vietati

La proposta di Regolamento prevede le seguenti pratiche vietate di Intelligenza Artificiale, in quanto contrarie ai principi dell'Unione ed ai suoi diritti fondamentali:

a) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che utilizzino tecniche subliminali al di là della consapevolezza di una persona al fine di falsare in misura rilevante il comportamento di una persona in modo tale da provocare o da poter causare a tale persona o ad un'altra persona un danno fisico o psicologico;
b) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA che sfruttino qualsiasi vulnerabilità di un gruppo specifico di persone, per la loro età o disabilità fisica o mentale, al fine di falsarne in misura rilevante il comportamento in un modo che provochi o possa provocare danni fisici o psicologici agli stessi o ad altri;
c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte di pubbliche autorità o per loro conto, che valuti o classifichi l'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o caratteristiche o della personalità, note o previste, mediante un punteggio sociale che determini uno o entrambi i seguenti elementi:
   - un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non hanno alcun rapporto con i contesti con cui i dati sono stati originariamente generati o raccolti;
   - un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche che sia sproporzionato rispetto alla gravità del loro comportamento sociale;
d) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico ai fini dell'applicazione della legge.

6. Le eccezioni al divieto di identificazione biometrica remota in tempo reale

Il divieto di cui al punto d), sopra visto, sull'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico ai fini dell'applicazione della legge, risulta mitigato dalla previsione di eccezioni strettamente necessarie per motivi di salvaguardia della vita umana. In particolare, potranno essere utilizzati sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico, aventi specifici requisiti, solo per:

- la ricerca mirata di potenziali vittime di crimini, inclusi i bambini scomparsi;
- la prevenzione di specifiche e imminenti minacce alla vita di persone o di attacchi terroristici;
- l'accertamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore del reato o sospettato di un reato punibile con una pena o una misura massima di almeno tre anni.

In ogni caso, a livello nazionale, gli Stati membri dovranno designare una o più autorità nazionali competenti e, tra queste, l'autorità nazionale di controllo, al fine di controllare l'applicazione e l'attuazione del Regolamento.
Il Garante europeo della protezione dei dati fungerà da autorità competente per il controllo delle istituzioni, delle agenzie e degli organi dell'Unione quando rientrano nel campo di applicazione del Regolamento. ©