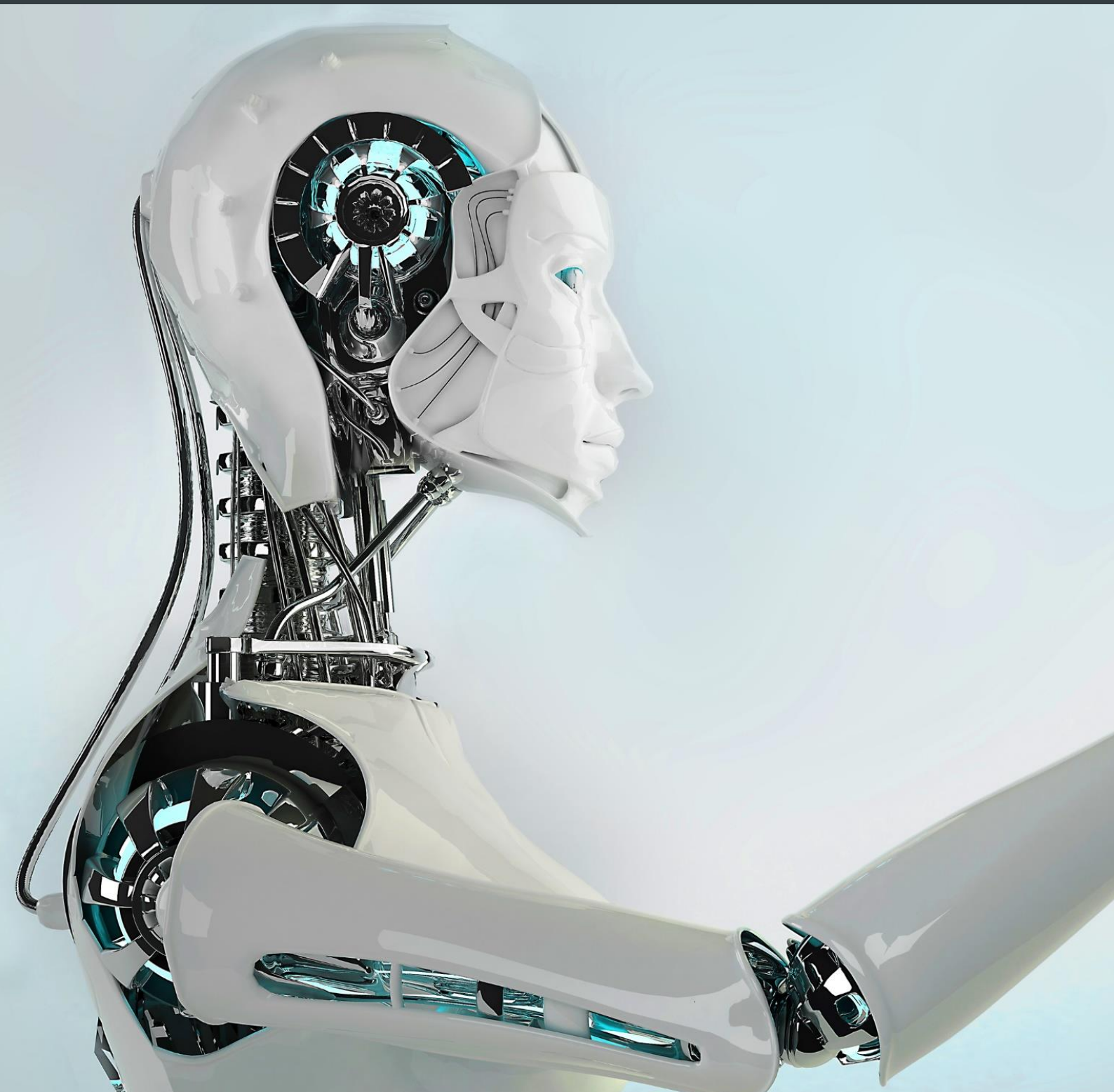
Bird & Bird

Intelligenza artificiale: il nostro osservatorio sulla legislazione in arrivo



Intelligenza artificiale: il nostro osservatorio sulla legislazione in arrivo

Al fine di istituire regole armonizzate a livello europeo per lo sviluppo, la commercializzazione e l'uso dei sistemi di intelligenza artificiale (d'ora in avanti, "**Sistema di IA**"), il 21 aprile 2021 la Commissione Europea ha pubblicato una Proposta di Regolamento[1] (d'ora in avanti, "**Proposta**").

Seguiremo i futuri sviluppi di questa Proposta nel suo *iter* presso le istituzioni europee fino alla sua approvazione e successiva entrata in vigore.

Il Sistema di IA viene definito nella Proposta come "*un software sviluppato con una o più delle tecniche e degli approcci di cui all'Allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*".

Il suddetto Allegato I alla Proposta, nel dettaglio, fa riferimento ai seguenti approcci: i) di apprendimento automatico[2]; ii) basati sulla logica e sulla conoscenza[3]; iii) statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

Nel prosieguo è riportata una sintesi di alcuni dei principali punti disciplinati all'interno della Proposta.

1. Tipologie di Sistemi di IA: Sistemi di IA vietati e Sistemi di IA ad Alto Rischio

La Proposta opera innanzitutto una distinzione tra Sistemi di IA "vietati", cioè il cui utilizzo non è consentito *tour court* (d'ora in avanti, "**Sistemi di IA Vietati**") e Sistemi di IA "ad alto rischio", cioè che possono essere realizzati, commercializzati e utilizzati nel rispetto di una serie di obblighi e adempimenti previsti dalla Proposta stessa (d'ora in avanti, "**Sistemi di IA ad Alto Rischio**").

Con riferimento ai Sistemi di IA Vietati, si tratta di Sistemi di IA che comportano un rischio inaccettabile, in quanto contrari ai valori dell'Unione Europea (ad esempio, perché violano i diritti fondamentali).

A titolo esemplificativo, vi rientrano i Sistemi di IA che:

a utilizzano tecniche subliminali;

b sfruttano la vulnerabilità di uno specifico gruppo di persone;

[1] Il testo della Proposta è disponibile al seguente *link*: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52021PC0206.
[2] Sono compresi in questa categoria l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (*deep learning*).
[3] Sono compresi in questa categoria la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti.

c attuano tecniche di *credit scoring*;

d utilizzano i sistemi di identificazione biometrica remota "in tempo reale"[4] in spazi accessibili al pubblico ai fini di attività di contrasto[5] (salvo eccezioni previste dalla Proposta).

Costituisce, invece, un c.d. Sistema di IA ad Alto Rischio:

a il Sistema di IA destinato ad essere utilizzato come componente di sicurezza di un prodotto o è esso stesso un prodotto, qualora lo stesso sia disciplinato da una ampia serie di provvedimenti normativi dell'Unione Europea (indicati all'interno dell'Allegato alla Proposta); o

b il Sistema di AI che costituisce il prodotto, il cui componente di sicurezza è il Sistema di IA o il Sistema di IA stesso, in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa dell'Unione elencata nella Proposta; o

c una serie di Sistemi di IA specificamente indicati nella Proposta e destinati ad operare nelle seguenti aree:

i. identificazione e categorizzazione biometrica delle persone fisiche;
ii. gestione e funzionamento delle infrastrutture critiche;
iii. istruzione e formazione professionale;
iv. occupazione, gestione dei lavoratori e accesso al lavoro autonomo;
v. accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi;
vi. attività di contrasto di cui all'Allegato III, punto 6, alla Proposta;
vii. gestione della migrazione, dell'asilo e del controllo delle frontiere; amministrazione della giustizia e processi democratici.

In generale, inoltre, tutti i Sistemi di IA devono garantire un adeguato livello di accuratezza (si indica, sul punto, che le relative metriche devono essere indicate nelle istruzioni per l'uso), di robustezza (mediante soluzioni tecniche di ridondanza, che possono includere piani di *backup* o *fail-safe*) e di cybersicurezza (mediante soluzioni tecniche per prevenire, tra gli altri, fenomeni di manipolazione del *set* di dati di addestramento, quale il fenomeno del *data poisoning*).

2. Requisiti ed obblighi relativi ai Sistemi di IA ad Alto Rischio

Con specifico riferimento ai Sistemi di IA ad Alto Rischio vengono prescritti l'adozione e il mantenimento, con un aggiornamento costante e continuo, di un sistema di gestione dei rischi, dettagliatamente descritto nella Proposta.

Inoltre, i Sistemi di IA ad Alto Rischio che usano dati per l'addestramento di modelli devono essere sviluppati sulla base di *set* di dati di addestramento, convalida e prova che sono soggetti ad adeguate pratiche di *governance* e gestione dei dati in linea con le modalità specificamente indicate nella Proposta.

In aggiunta a quanto sopra, per i Sistemi di IA ad Alto Rischio la Proposta stabilisce i requisiti relativi alla documentazione tecnica, alla trasparenza, alla fornitura di informazioni agli utenti e alla conservazione delle registrazioni (per i Sistemi di IA che consentono la registrazione automatica degli eventi "*log*" durante il loro funzionamento).

---

[4] Per "sistema di identificazione biometrica remota" si intende, ai sensi della Proposta, un sistema in cui il confronto e l'identificazione avvengono senza ritardi significativi. Tra questi, vi sono le identificazioni istantanee e quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione della normativa.
[5] Per "attività di contrasto" si intende, ai sensi della Proposta, le attività svolte dalle autorità di contrasto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse.

Di fondamentale importanza è il requisito della **sorveglianza umana**. I Sistemi di IA ad Alto Rischio infatti devono essere progettati per poter essere supervisionati in modo efficace da persone fisiche durante il periodo in cui il Sistema di IA viene utilizzato. Per questo motivo devono essere adottati anche strumenti di interfaccia uomo-macchina adeguati.

La Proposta fornisce una serie di prescrizioni relative alla modalità con cui deve essere garantita la sorveglianza umana.

La richiesta dell'intervento dell'uomo è chiaramente volta a prevenire o ridurre i rischi per la salute, la sicurezza o i diritti fondamentali che potrebbero emergere dall'uso di un Sistema di IA ad Alto Rischio, anche laddove tale uso sia conforme alla finalità prevista.

Per maggiore chiarezza, la Proposta individua gli obblighi sia per i fornitori di sistemi di IA ad Alto Rischio sia per gli utenti e altri soggetti coinvolti, quali importatori, distributori e rappresentanti autorizzati.

Tra gli obblighi per i fornitori vi è quello di istituire un sistema di gestione della qualità che garantisce la conformità alla Proposta, di redigere la documentazione tecnica, di valutare la conformità del Sistema di IA prima della sua immissione sul mercato/messa in servizio e di conservare i *log* generati automaticamente dal Sistema laddove tali *log* siano sotto il loro controllo ai sensi di un contratto con l'utente o in forza di legge.

Per quanto riguarda la registrazione del Sistema di IA ad Alto Rischio, tale procedura deve essere fatta dal fornitore o, ove applicabile, dal rappresentante autorizzato prima che il Sistema venga immesso sul mercato o messo in servizio. Il suddetto Sistema viene così registrato nella banca dati dell'UE dedicata ai Sistemi di IA ad Alto Rischio.

Da notare che il fabbricante del prodotto si assume la responsabilità della conformità del Sistema di IA ad Alto Rischio alla Proposta e ha gli stessi obblighi previsti in capo al fornitore ai sensi della Proposta medesima. Tale assunzione di responsabilità opera quando il Sistema di IA ad Alto Rischio sia collegato a un prodotto a cui si applica una delle normative di cui all'Allegato II alla Proposta, quali per esempio il regolamento sui dispositivi medici o la direttiva sulla sicurezza dei giocattoli o il regolamento sugli apparecchi che bruciano carburanti gassosi.

3. Le autorità di notifica e gli organismi notificati

La Proposta dedica un intero capo al quadro normativo relativo alle c.d. autorità di notifica e agli organismi notificati che saranno coinvolti come terze parti indipendenti nelle procedure di valutazione della conformità del Sistema di IA. A tal proposito, la Proposta differenzia le suddette procedure sulla base del tipo di Sistema di IA ad Alto Rischio.

In ogni caso, ogni volta che sia attuata una modifica sostanziale, i Sistemi di IA ad Alto Rischio devono essere sottoposti a una nuova procedura di valutazione della conformità.

Vengono forniti anche dettagli su cosa si intenda per "modifica sostanziale": ad esempio, non sono considerate modifiche sostanziali le modifiche apportate al Sistema di IA ad Alto Rischio che prosegue il suo apprendimento dopo essere stato immesso sul mercato/messo in servizio e che, da un lato, sono state predeterminate dal fornitore in occasione della valutazione iniziale della conformità e, dall'altro, rientrano nella documentazione tecnica.

4. Obblighi per Sistemi di IA che interagiscono con persone fisiche

Con riferimento a tutti i Sistemi di IA che interagiscono con le persone fisiche, i fornitori devono garantire che tali Sistemi siano progettati in modo tale che le persone fisiche siano informate del fatto che stanno interagendo con un Sistema di IA, a meno che ciò non sia evidente per le circostanze e il contesto di utilizzo. Un'eccezione è rappresentata ovviamente dai Sistemi di IA ad Alto Rischio usati per finalità legittime, quali le attività di contrasto di cui all'Allegato III, punto 6, alla Proposta.

Tali obblighi di trasparenza si applicano altresì ai Sistemi di IA che sono usati per rilevare emozioni o per stabilire un'associazione con categorie sociali sulla base dei dati biometrici oppure a quelli che generano o manipolano contenuti ("*deep fake*"), fermo restando le finalità legittime quali le attività di contrasto e la tutela delle libertà di espressione.

5. Obblighi in caso di incidenti o malfunzionamenti dei Sistemi di IA

In caso di incidenti gravi o malfunzionamenti del Sistemi di IA che costituiscano una violazione degli obblighi previsti dal diritto dell'UE, il fornitore deve segnalarli:

a dopo che il fornitore stesso ha stabilito con certezza o con ragionevole probabilità un nesso causale tra il Sistema di IA e l'incidente/malfunzionamento; e

b in ogni caso non oltre 15 giorni dopo che è venuto a conoscenza dell'incidente grave o del malfunzionamento.

Anche successivamente all'immissione sul mercato del Sistema di IA ad Alto Rischio, il fornitore deve istituire un sistema di monitoraggio che sia proporzionato alla natura e alle tecnologie dei Sistemi di IA.

6. Banca dati UE e Comitato Europeo per l'Intelligenza Artificiale

Tra le novità della Proposta vi è l'istituzione di una banca dati dell'UE, accessibile al pubblico, con le informazioni sui Sistemi di IA ad Alto Rischio registrati nonché l'introduzione di un c.d. comitato europeo per l'intelligenza artificiale, al quale è attribuita competenza per (i) facilitare la cooperazione tra autorità nazionali di controllo e Commissione UE in tema di intelligenza artificiale, (ii) supportare le autorità nazionale di controllo, la Commissione UE e altre autorità competenti sulle questioni emerse in tema di intelligenza artificiale, e (iii) assistere le autorità nazionali di controllo e la Commissione UE per l'applicazione del regolamento.

7. Profili sanzionatori

Il mancato rispetto dei termini e delle condizioni del Regolamento può comportare l'applicazione di sanzioni amministrative pecuniarie. All'interno della Proposta, in particolare, sono individuate sanzioni pecuniarie che, nel massimo edittale, possono raggiungere l'importo di Euro 30.000.000,00 o il 6% del fatturato totale mondiale annuo dell'esercizio precedente, se superiore.

*** *** ***

La Proposta ha aperto un *iter* legislativo complesso, che potrebbe culminare nella pubblicazione di un regolamento definitivo in non meno di 12-18 mesi. Nel corso di detto *iter*, è possibile che siano apportate numerose modifiche e integrazioni rispetto alla Proposta, anche sostanziali.

Il nostro *team* monitorerà lo *status* del procedimento legislativo e fornirà ulteriori aggiornamenti sulle novità che seguiranno nei prossimi mesi.

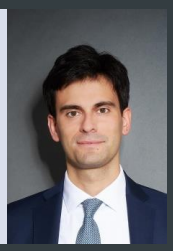
Contatti

Gian Marco Rinaldi
Counsel

Tel: +390230356000
gianmarco.rinaldi@twobirds.com

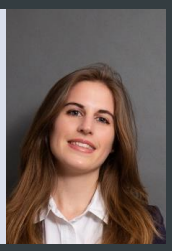
Niccolò Anselmi
Associate

Tel: +390230356000
niccolo.anselmi@twobirds.com



Marta Breschi
Associate

Tel: +390230356000
marta.breschi@twobirds.com



twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw & Satellite Office: Casablanca