LE LINEE GUIDA DELLA COMMISSIONE SULLE PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE: ANALISI GENERALE E PROFILI DI PRIVACY

5 febbraio 2025

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Giovanni Lombardi
Associate

L'approvazione, da parte della Commissione Europea, della bozza delle Linee Guida sulle pratiche di intelligenza artificiale vietate, avvenuta con la Comunicazione del **4 febbraio 2025**, rappresenta un momento di particolare rilevanza per l'attuazione del **Regolamento UE 2024/1689 (AI Act)**, che costituisce il primo quadro normativo organico a livello europeo per la regolamentazione dell'intelligenza artificiale.

Queste linee guida, pur non vincolanti, assumono un ruolo determinante nel fornire **chiarezza interpretativa** sull'articolo 5 dell'AI Act, che elenca le pratiche vietate in quanto ritenute incompatibili con i principi fondamentali dell'Unione, tra cui **il rispetto della dignità umana, la tutela dei diritti fondamentali e la protezione della sicurezza pubblica**.

L'AI Act si caratterizza per un approccio basato sul rischio, classificando i sistemi di IA in quattro categorie, che vanno dai sistemi a **rischio minimo** (per i quali non sono previsti obblighi specifici) fino ai sistemi a **rischio inaccettabile**, il cui utilizzo è vietato. La normativa introduce così **un sistema di prevenzione e vigilanza**, volto a garantire che le applicazioni di intelligenza artificiale operino in modo conforme ai valori e ai diritti sanciti nell'ordinamento dell'Unione Europea.

L'analisi del documento in esame consente di evidenziare il quadro di riferimento nel quale si inseriscono i divieti previsti dall'AI Act, soffermandosi, in particolare, sugli aspetti più critici e sulle possibili implicazioni per la tutela della privacy e dei dati personali.

▼ ▼ ▼

IL CONTENUTO DELLE LINEE GUIDA

Le Linee Guida della Commissione si propongono di fornire una lettura uniforme e coerente delle disposizioni dell'articolo 5 dell'AI Act, chiarendo gli ambiti di applicazione, le deroghe ammesse, i soggetti coinvolti e il coordinamento con le altre normative dell'Unione.

L'articolo 5 del Regolamento sancisce, in particolare, il divieto assoluto di alcune pratiche di IA, individuate in quanto incompatibili con i principi fondamentali dell'UE, tra cui la protezione dei dati personali, la non discriminazione e il diritto alla sicurezza.

Le pratiche di IA vietate dall'articolo 5 dell'AI Act

Il documento della Commissione analizza nel dettaglio le otto categorie di pratiche vietate, chiarendone la portata applicativa e le eventuali eccezioni:

- **manipolazione e inganno** (art. 5(1)(a)): proibizione di sistemi che utilizzano **tecniche subliminali** o **strategie manipolative** per distorcere il comportamento degli individui in modo significativo, alterandone la capacità decisionale;
- **sfruttamento di vulnerabilità** (art. 5(1)(b)): divieto di impiegare IA per **approfittare di vulnerabilità legate all'età, a disabilità o a condizioni socio-economiche**, inducendo gli utenti a compiere scelte svantaggiose o dannose;
- ***social scoring*** (art. 5(1)(c)): proibizione dell'uso di IA per classificare gli individui in base a **comportamenti sociali, personali o professionali**, qualora ciò comporti trattamenti ingiustificati o discriminatori;
- **predizione del rischio criminale** (art. 5(1)(d)): divieto di sistemi di IA che valutano **il rischio di commissione di reati** basandosi esclusivamente su **profilazione automatizzata** o **caratteristiche personali**;
- ***scraping* massivo di immagini facciali** (art. 5(1)(e)): proibizione della raccolta **indiscriminata e senza consenso** di dati biometrici (ad esempio, attraverso il prelievo di immagini da Internet o CCTV) per la creazione di database di riconoscimento facciale;
- **riconoscimento delle emozioni** (art. 5(1)(f)): divieto di utilizzare IA per **inferire le emozioni** di individui in contesti lavorativi o scolastici, salvo specifiche deroghe per motivi di sicurezza o sanitari;
- **categorizzazione biometrica per dati sensibili** (art. 5(1)(g)): divieto di impiegare IA per **dedurre caratteristiche sensibili**, come **razza, religione, opinioni politiche, orientamento sessuale o appartenenza sindacale**;
- **identificazione biometrica remota in tempo reale** (art. 5(1)(h)): proibizione dell'uso di sistemi di riconoscimento biometrico remoto negli **spazi pubblici** per finalità di *law enforcement*, salvo eccezioni limitate e rigorosamente regolamentate.

IMPLICAZIONI OPERATIVE E PROFILI CRITICI DI COMPLIANCE

Nell'ambito dell'articolato sistema di disposizioni delineato dalle Linee Guida, emerge con particolare evidenza la necessità, per le imprese che sviluppano o implementano sistemi di intelligenza artificiale, di procedere ad una attenta valutazione preliminare circa la sussistenza di eventuali profili di incompatibilità con i divieti sanciti dall'articolo 5 dell'AI Act.

In tale contesto, particolare rilevanza assume l'adozione di **adeguate misure organizzative e tecniche** volte a garantire, sin dalla fase di progettazione, la conformità dei sistemi di IA ai requisiti normativi. Ciò implica, anzitutto, la necessità di implementare **procedure di valutazione d'impatto preliminare** che tengano conto non solo dei profili di *data protection* - già oggetto di specifica disciplina nell'ambito del GDPR - ma altresì delle ulteriori dimensioni di rischio individuate dall'AI Act. La correlazione tra l'AI Act e la disciplina in materia di protezione dei dati personali assume carattere di preminente rilevanza, atteso che numerose delle pratiche oggetto di divieto attengono al trattamento di dati personali e biometrici, ambiti già oggetto di specifica regolamentazione nell'ambito del Regolamento Generale sulla Protezione dei Dati (GDPR) e della Direttiva 2016/680 sul trattamento dei dati per finalità di law enforcement.

Di particolare rilievo risulta, inoltre, la previsione di meccanismi di controllo e **monitoraggio continuativo** della conformità dei sistemi di IA ai divieti normativi, atteso che, come chiarito dalle Linee Guida, la valutazione circa la sussistenza di pratiche vietate deve essere condotta non solo in fase di prima implementazione, bensì durante l'intero ciclo di vita del sistema.

Scraping di dati biometrici e riconoscimento facciale

Uno dei divieti più rilevanti riguarda la creazione di database biometrici attraverso lo scraping massivo di immagini da fonti pubbliche. Tale pratica è già oggetto di particolare attenzione da parte delle autorità garanti della protezione dei dati personali, in quanto contraria ai principi di minimizzazione e finalità del trattamento sanciti dal GDPR. Tuttavia, le Linee Guida non chiariscono completamente i limiti di legittimità dell'utilizzo di immagini biometriche per addestrare modelli di IA, lasciando spazio a possibili conflitti normativi.

Social scoring e predizione del rischio criminale

Le tecniche di profilazione algoritmica finalizzate a valutazioni di affidabilità sociale o a previsioni di rischio criminale pongono problemi particolarmente complessi in materia di protezione dei dati, nonché rispetto ai principi di proporzionalità e non

discriminazione. Tali sistemi possono infatti condurre a pregiudizi automatizzati, con un impatto significativo sulla presunzione di innocenza e sul diritto alla non discriminazione.

Identificazione biometrica remota e privacy negli spazi pubblici

Il divieto di utilizzo di sistemi di riconoscimento facciale in tempo reale negli spazi pubblici costituisce una delle disposizioni maggiormente restrittive dell'AI Act e si pone in linea di continuità con il quadro di tutele delineato dal GDPR in materia di trattamento dei dati biometrici.

Nondimeno, la previsione di deroghe per finalità di prevenzione di gravi minacce alla sicurezza pubblica solleva interrogativi di non agevole soluzione circa il corretto bilanciamento tra le esigenze di sicurezza pubblica e la tutela del diritto alla riservatezza, con particolare riferimento alla necessità di individuare criteri oggettivi per la valutazione della proporzionalità delle misure adottate.

In tale contesto, assume particolare rilevanza la previsione di specifici obblighi di documentazione e registrazione delle attività di trattamento, nonché la necessità di effettuare preventive valutazioni d'impatto sui diritti fondamentali, secondo quanto previsto dall'art. 35 GDPR e dalle disposizioni dell'AI Act in materia di sistemi ad alto rischio.

IL REGIME SANZIONATORIO

L'AI Act adotta un approccio particolarmente rigoroso sul piano sanzionatorio per quanto attiene alle violazioni dei divieti di cui all'articolo 5, prevedendo l'applicazione delle sanzioni più elevate tra quelle contemplate dal Regolamento. In particolare, le violazioni delle pratiche vietate possono comportare l'irrogazione di sanzioni amministrative pecuniarie fino a 35 milioni di euro ovvero, per le imprese, fino al 7% del fatturato mondiale totale dell'esercizio precedente, se superiore.

Tale impianto sanzionatorio, che denota la particolare gravità attribuita dal legislatore europeo alle violazioni in questione, si applica indistintamente sia ai fornitori che agli utilizzatori dei sistemi di IA, ciascuno per quanto di propria competenza. Per gli enti pubblici, gli Stati membri mantengono un margine di discrezionalità circa l'applicabilità delle sanzioni amministrative pecuniarie, ferma restando la necessità di prevedere misure effettive, proporzionate e dissuasive.

Di particolare rilievo risulta, inoltre, la previsione secondo cui, in caso di violazioni reiterate, l'importo massimo della sanzione può essere aumentato fino al 2%, con un evidente effetto deterrente rispetto a pratiche sistematiche di violazione dei divieti.

CRITICITÀ INTERPRETATIVE E PROSPETTIVE DI *ENFORCEMENT*

Le Linee Guida, pur fornendo rilevanti elementi di chiarificazione circa l'ambito applicativo dei divieti, lasciano tuttavia aperti alcuni significativi interrogativi interpretativi, con particolare riferimento:

- alle concrete modalità di coordinamento tra le autorità di controllo competenti in materia di IA e le autorità garanti della protezione dei dati personali;
- ai criteri di valutazione della "significatività" del pregiudizio richiesto ai fini della configurabilità di talune pratiche vietate;
- all'individuazione dei confini tra pratiche vietate e pratiche consentite nell'ambito delle deroghe previste dal Regolamento.

Le imprese si trovano, dunque, dinanzi alla necessità di confrontarsi con un quadro normativo particolarmente complesso e articolato, che richiede l'adozione di un approccio proattivo alla compliance in materia di IA. Tale sfida, tuttavia, può rappresentare altresì un'opportunità per ripensare i processi di sviluppo e implementazione dei sistemi di IA in chiave maggiormente responsabile e sostenibile.

In tale prospettiva, risulta fondamentale:

- l'adozione di framework di governance dell'IA che integrino, sin dalla fase di design, i requisiti normativi previsti dall'AI Act;
- l'implementazione di procedure di risk assessment continuativo;
- l'investimento nella formazione del personale coinvolto nello sviluppo e nell'utilizzo dei sistemi di IA;
- la previsione di meccanismi di documentazione e tracciabilità delle valutazioni di conformità effettuate.

Le Linee Guida della Commissione, pertanto, pur non risolvendo tutte le questioni interpretative poste dall'AI Act, costituiscono un importante punto di riferimento per le imprese nel percorso di adeguamento alla nuova disciplina, fornendo indicazioni operative che dovranno necessariamente essere integrate alla luce dell'esperienza applicativa e dei chiarimenti che emergeranno dalla prassi delle autorità di controllo.

La sfida dei prossimi mesi sarà, dunque, quella di tradurre i principi e i divieti delineati dal legislatore europeo in concrete prassi operative, bilanciando l'esigenza di innovazione tecnologica con la necessità di garantire il pieno rispetto dei diritti fondamentali dei soggetti coinvolti nell'utilizzo dei sistemi di IA.

TIMELINE IMPLEMENTAZIONE AI ACT

2 FEBBRAIO 2025

- entrata in vigore delle disposizioni sui divieti (art. 5)
- obbligo di conformità per tutti i sistemi di IA, anche se già in uso

2 AGOSTO 2025

- designazione delle autorità di vigilanza nazionali
- entrata in vigore del sistema sanzionatorio
- avvio dei poteri di *enforcement* delle autorità

2 AGOSTO 2026

- applicazione generale dell'AI Act
- gli Stati membri devono rendere operativi i *sandbox* regolamentari per l'IA
- inizio degli obblighi di conformità per i sistemi di IA ad alto rischio

2 AGOSTO 2027

- applicazione dell'articolo 6(1) sui sistemi di IA ad alto rischio
- termine per la conformità dei modelli di IA *general-purpose* immessi sul mercato prima del 2 agosto 2025.

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Giovanni Lombardi

Associate