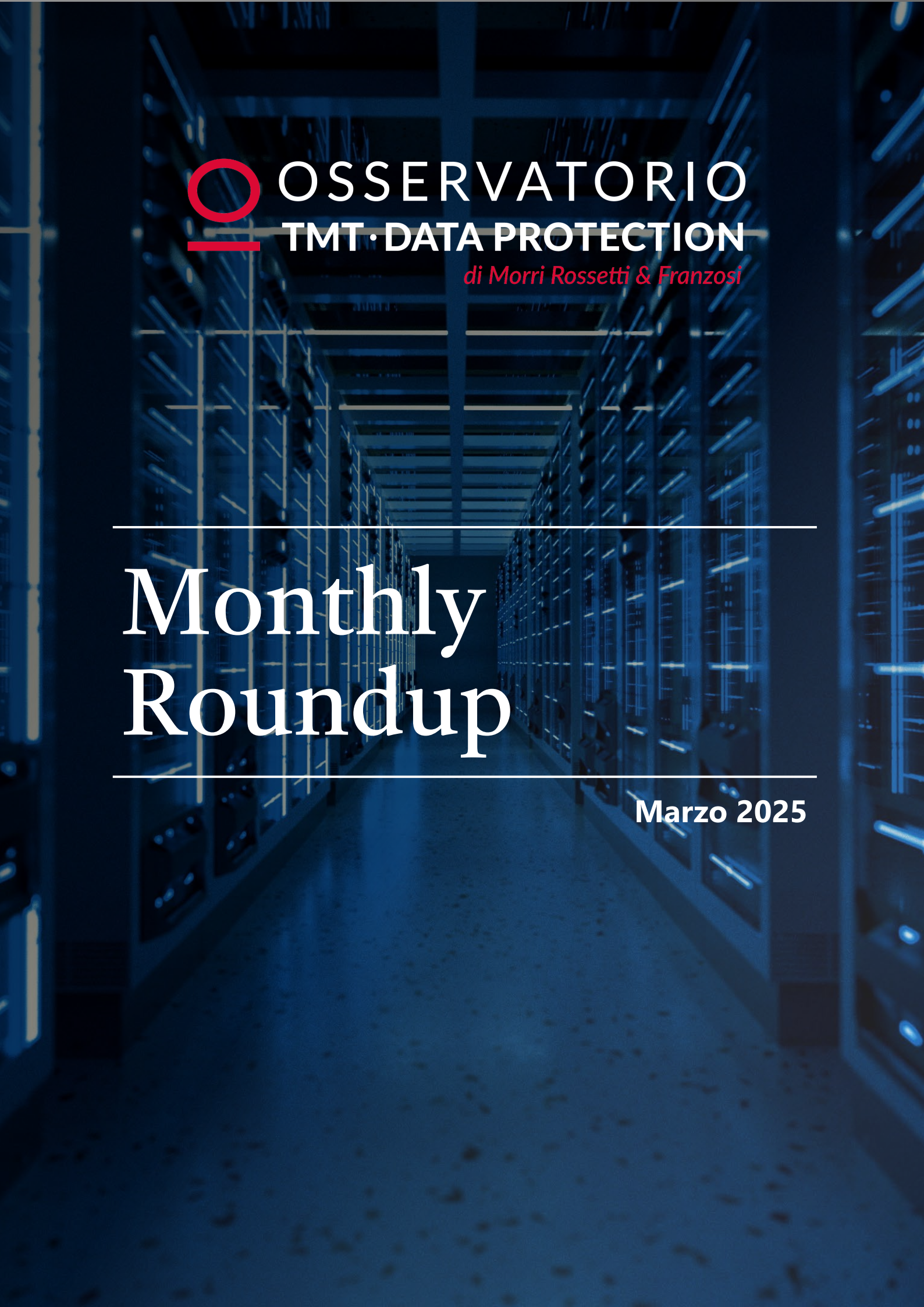

OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Marzo 2025

Marzo 2025

I principali aggiornamenti in materia di TMT & Data Protection del mese.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- Telemarketing: Garante privacy, stop ai consensi "omnibus"; [Link]
- Lavoro: Garante privacy, no al controllo a distanza; [Link]
- Garante: ok al nuovo sistema di fatturazione elettronica per gli operatori sanitari; [Link]
- Propaganda elettorale: Garante, no all'uso dei dati dei pazienti. [Link]

EDPB

- EDPB Letter on the procedural rules regulation; [Link]
- Statement 2/2025 on the implementation of the PNR Directive in light of CJUE Judgment C-817/19; [Link]
- EDPB Document Setting Forth a Co-Operation procedure for the approval of Binding Corporate Rules for controllers and processors. [Link]

AGCOM

- Delibera 58/25/CONS – Modifiche e integrazioni al Regolamento concernente l'organizzazione e il funzionamento dell'Autorità per le garanzie nelle comunicazioni. [Link]

AI Act e GDPR: equilibrio tra innovazione e protezione dei dati nella lotta alla discriminazione algoritmica

Con l'entrata in vigore del Regolamento (UE) 1689/2024 ("**AI Act**") nell'agosto 2024, si impone una riflessione sulla sua interazione con il Regolamento (UE) 679/2016 ("**GDPR**"), specialmente in rapporto al tema della **discriminazione algoritmica**.

Il **Servizio di Ricerca del Parlamento Europeo** (*European Parliamentary Research Service* – "**EPRS**") ha evidenziato una rilevante criticità giuridica: l'**AI Act** consente, entro precisi limiti, il trattamento di **categorie particolari di dati personali** per individuare ed eliminare distorsioni (c.d. *bias*) nei sistemi di AI ad alto rischio, mentre il **GDPR** appare più restrittivo, subordinando tale trattamento a condizioni più stringenti.

Da questa divergenza normativa deriva un'incertezza interpretativa che potrebbe rendere necessaria una riforma legislativa o, quantomeno, linee guida chiarificatrici.

I principali scenari di discriminazione algoritmica

L'uso dell'intelligenza artificiale ("**AI**") può determinare discriminazioni e ledere i diritti fondamentali degli individui. Alcuni scenari emblematici includono:

- **sistemi di AI generativa:** *chatbot* o modelli di generazione testuale che, pur non essendo classificati come ad alto rischio, potrebbero produrre contenuti discriminatori o incitare all'odio;
- **veicoli autonomi**: auto a guida autonoma in grado di riconoscere con maggior precisione i pedoni con la pelle chiara rispetto a quelli con pelle scura, con conseguenti implicazioni etiche e giuridiche;
- **algoritmi di selezione del personale**: sistemi di *recruiting* che favoriscono determinate categorie di candidati in base a *bias* impliciti legati al genere o alla salute;
- **sistemi di *credit scoring***: modelli di valutazione del merito creditizio che, pur senza una discriminazione esplicita, penalizzano soggetti appartenenti a specifiche aree geografiche o gruppi etnici.

Le principali criticità normative

Uno degli obiettivi principali dell'AI Act è mitigare i*bias* nello sviluppo, nell'implementazione e nell'uso dei sistemi di AI ad alto rischio.

A tal fine, l'art. 10, par. 5, dell'AI Act[1] consente il **trattamento di categorie particolari di dati**

[1] In particolare, l'articolo 10 dell'AI Act – che si occupa dello sviluppo e della *governance* dei sistemi di AI ad alto rischio – sottolinea l'importanza di basare tali sistemi su *set* di dati di addestramento, validazione e prova che soddisfino specifici criteri di qualità, così da garantire l'affidabilità e l'eticità del sistema. Le pratiche di *governance* e gestione dei dati riguardano: (i) scelte processuali pertinenti; (ii) processi di raccolta dei dati, la loro origine e la finalità originaria di raccolta dei dati personali; (iii) operazioni di trattamento pertinenti ai fini della preparazione dei dati (annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione); (iv) formulazione di ipotesi; (v) valutazione della disponibilità, quantità e adeguatezza dei *dataset* necessari; (vi) esame di potenziali *bias* che potrebbero incidere sulla salute, sicurezza e diritti fondamentali o generare discriminazioni; (vii) misure adeguate per individuare, prevenire e attenuare simili

personali, purché siano adottate misure adeguate per garantire la tutela della protezione dei dati, al fine di individuare e prevenire eventuali discriminazioni nell'uso di tali tecnologie.

Affinché le disposizioni dell'AI Act sulla rilevazione dei *bias* siano compatibili con il GDPR, occorre che:

- il trattamento di dati "sensibili" avvenga nel **rispetto dei principi del GDPR**, come la minimizzazione dei dati, la limitazione della finalità e della conservazione, l'integrità e la riservatezza, la *privacy by design* e *by default*;
- siano adottate **misure di sicurezza tecniche e organizzative robuste**, al fine di prevenire violazioni dei dati personali;
- il trattamento sia "**strettamente necessario**" per proteggere altri diritti fondamentali, come il diritto alla non discriminazione;
- sussista una **base giuridica idonea** ai sensi dell'art. 9 GDPR, eventualmente riconducibile ai motivi di **interesse pubblico rilevante** (art. 9, par. 2, lett. g) del GDPR) [2] , dove l'AI Act rappresenterebbe il fondamento normativo dell'Unione e la lotta alla discriminazione costituirebbe l'interesse pubblico rilevante.

Ulteriormente, la discriminazione potrebbe derivare anche dal trattamento di dati non rientranti nelle "categorie particolari" dell'art. 9 del GDPR, come ad esempio dalla disabilità, dall'età o dal genere.

In questi casi, la base giuridica applicabile andrebbe individuata nell'**art. 6 del GDPR**, che offre criteri più ampi rispetto all'art. 9, come, ad esempio, l'**interesse legittimo**, rendendo più agevole giustificare il trattamento dei dati per ridurre i *bias*.

Prospettive future e raccomandazioni

Vi è un'incertezza diffusa su come interpretare la disposizione dell'AI Act relativa al trattamento di categorie particolari di dati per evitare la discriminazione.

Il GDPR, imponendo limiti stringenti al trattamento di tali dati, potrebbe rivelarsi un ostacolo nell'attuale contesto economico, dove l'AI viene impiegata in molti settori e implica il trattamento massivo di dati personali e non personali.

Per affrontare queste problematiche, l'EPRS suggerisce due possibili interventi:

- una **riforma del GDPR**, che chiarisca la sua interazione con l'AI Act;
- **linee guida specifiche** per fornire maggiore certezza giuridica ai soggetti coinvolti nel trattamento di dati per finalità di *bias detection* e loro relativa correzione.

* * *

distorsioni; (viii) individuazione di lacune o carenze nei dati tali da pregiudicare il rispetto dell'AI Act e le modalità per colmarle.

[2] L'articolo 9, par. 2, lett. g) del GDPR consente il trattamento di categorie particolari di dati personali quando ciò sia necessario per motivi di interesse pubblico rilevante sulla base del diritto europeo o nazionale, sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure adeguate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati.

Il DDL sull'Intelligenza Artificiale: approvazione dal Senato

L'IA non rappresenta esclusivamente una tecnologia, bensì una sfida di natura etica e giuridica.

A conferma di ciò, nella seduta del 20 marzo 2025, il Senato ha approvato il disegno di legge sull'IA (il "**DDL IA**"), volto a disciplinare lo sviluppo e l'applicazione nel contesto nazionale, integrando le disposizioni già previste dall'AI Act.

Il disegno era rimasto bloccato in Senato a causa di oltre 400 emendamenti e le criticità sollevate dalla Commissione europea [3] in relazione ad alcune incongruenze con l'AI Act, le quali sono state solo parzialmente risolte.

Anche il Garante Privacy italiano aveva espresso il proprio parere con il provvedimento n. 477 del 2 agosto 2024, ai sensi dell'art. 36, par. 4 del GDPR, evidenziando la necessità di un coordinamento sistematico tra le disposizioni in materia di IA e la normativa sulla protezione dei dati personali[4].

La Camera dei deputati è ora chiamata a esaminare il testo. L'implementazione delle norme, tuttavia, è subordinata all'adozione di decreti legislativi da parte del Governo, un passaggio che avverrà successivamente all'approvazione parlamentare.

L'obiettivo del legislatore è quello di rafforzare ulteriormente il livello di tutela legata all'impiego dell'IA, con particolare attenzione a determinati ambiti e settori.

Il contenuto del DDL IA

Il DDL IA è strutturato in quattro sezioni principali:

1. i principi guida e la strategia nazionale per l'utilizzo dell'IA;
2. la regolamentazione di settore in specifici ambiti (sanità, lavoro, giustizia, pubblica amministrazione, sicurezza nazionale, tutela degli utenti e diritto d'autore);
3. la governance e le autorità nazionali competenti in materia (l'Agenzia per l'Italia digitale e l'Agenzia per la cybersicurezza nazionale);
4. gli aspetti penali con la previsione di aggravanti in caso di reati commessi con l'IA e una nuova fattispecie di reato in caso di diffusione di deep fake.

Vengono dettati alcuni principi fondamentali per l'utilizzo dell'IA, tra cui:

- la necessità di garantire che tali sistemi siano sottoposti a supervisione umana tramite la possibilità di intervento e controllo, nel rispetto dell'autonomia decisionale degli individui;
- la trasparenza e la comprensibilità delle informazioni relative al funzionamento di tali sistemi e al trattamento dei dati, mediante una comunicazione chiara e accessibile, con particolare riguardo ai

[3] Il 5 novembre 2024, la Commissione europea ha trasmesso all'Italia un parere circostanziato (C(2024) 7814), in cui sottolineando i punti critici del DDL IA: (i) richiedeva un allineamento all'AI Act (ad esempio con riguardo alle definizioni); (ii) poneva un sostanziale divieto di creare nuove e ulteriori restrizioni all'applicazione dei sistemi di IA; e (iii) richiedeva di rispettare il principio di indipendenza delle Autorità di controllo del settore.

[4] Si rimanda a un nostro precedente contributo, disponibile qui: Il parere del Garante Privacy sul DDL IA: modifiche essenziali per la conformità con il GDPR e l'AI Act.

minori, per i quali è previsto il consenso genitoriale per l'uso di tecnologie di IA sotto i 14 anni;

- la sicurezza e la sovranità digitale dei sistemi di IA destinati all'uso pubblico attraverso l'obbligo di installazione su server situati in Italia, al fine di garantire la protezione dei dati personali e la sicurezza nazionale, salvo specifiche eccezioni;
- la tutela del diritto d'autore e, in particolare, la tutela giuridica delle opere generate con l'IA, laddove il contributo umano sia stato determinante nella creazione dell'opera stessa.

Il DDL AI ha subito variazioni lievi rispetto al testo del 23 aprile 2024, tra di esse vi è stato un allineamento alle definizioni dell'AI Act, nonché una delega al Governo per definire una disciplina organica per l'uso di dati, algoritmi e metodi matematici nel training dei sistemi di AI.

Tali modifiche derivano anche dal parere circostanziato C(2024)7814 della Commissione europea, la quale aveva espresso riserve, evidenziando sia la difformità delle definizioni rispetto all'AI Act, sia la mancanza di indipendenza delle autorità di governance.

In ogni caso, il disegno, seppur con piccole variazioni, rimane pressoché invariato. Il DDL IA comprende 28 articoli e stabilisce criteri normativi volti a bilanciare le opportunità offerte dalle nuove tecnologie con i rischi associati al loro uso improprio, non uso o all'utilizzo dannoso.

Con un approccio antropocentrico, analogo a quello adottato dal legislatore europeo, il DDL IA stabilisce che l'intero ciclo di vita dei sistemi e dei modelli di IA debba rispettare i diritti e le libertà fondamentali dell'individuo.

A titolo esemplificativo, il principio che circonda l'utilizzo dell'IA nel contesto lavorativo risulta rappresentato da una prospettiva incentrata sull'uomo.

L'implementazione di tali tecnologie dovrà, pertanto, essere volto a migliorare le condizioni di lavoro, tutelare l'integrità psicofisica dei lavoratori, accrescere la qualità delle prestazioni lavorative e la produttività delle persone, e dovrà essere effettuato in conformità al diritto dell'UE (per maggiori approfondimenti alla bozza del DDL IA del 23 aprile, si rimanda a un nostro precedente contributo, disponibile qui: Italy's new draft law on artificial intelligence).

Ad ogni modo, nonostante la risoluzione del primo rilievo, le restanti obiezioni della Commissione europea sembrano essere tutt'ora aperte. Si attende ora di capire se la Camera dei deputati modificherà il testo, tenendo conto delle osservazioni della Commissione, o se procederà all'approvazione senza ulteriori cambiamenti.

* * *

Divieto di riconoscimento delle emozioni sul lavoro e sue implicazioni alla luce dell'AI Act

L'entrata in vigore dell'Articolo 5 del Regolamento (UE) 1689/2024 ("**AI Act**") segna un passaggio fondamentale nella regolamentazione dell'intelligenza artificiale ("**AI**") nell'Unione europea.

Tale disposizione, rubricata "***Pratiche di AI vietate***", impone un divieto tassativo su specifici sistemi di AI che possano arrecare danni significati agli individui o pregiudicare i loro diritti fondamentali.

Il legislatore ha individuato sette pratiche particolarmente critiche, il cui utilizzo è ormai interdetto:

- la manipolazione del comportamento tramite inganno o sfruttando le vulnerabilità degli individui;
- i sistemi di *social scoring*;
- la valutazione del rischio di commissione di un reato da parte di un individuo;
- lo *scraping* non mirato di materiale da Internet o da CCTV per la creazione o l'espansione di *database* di riconoscimento facciale;
- il riconoscimento delle emozioni in ambito lavorativo e scolastico;
- la categorizzazione biometrica finalizzata alla deduzione di caratteristiche "sensibili" (quali orientamenti politici o convinzioni religiose);
- l'identificazione biometrica in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto.

Il mancato rispetto di tali divieti comporta l'applicazione delle più severe sanzioni previste dall'AI Act, con multe che possono raggiungere i **35 milioni di euro** o il **7% del fatturato annuo globale**, a seconda di quale importo sia maggiore.

Consapevole della necessità di garantire un'interpretazione uniforme e coerente del divieto, la Commissione europea, in attuazione dell'art. 96 dell'AI Act, ha adottato apposite **linee guida sull'applicazione delle regole relative alle pratiche di AI vietate** (le "**Linee Guida**").

Sebbene si tratti di un documento non vincolante, destinato a essere formalmente adottato solo in una fase successiva, esso rappresenta un punto di riferimento per le **autorità competenti**, nonché per i **fornitori** e i ***deployer*** di sistemi di AI, al fine di agevolare la comprensione e il rispetto delle prescrizioni normative.

Rimettendo ad una lettura delle Linee Guida per l'esame completo del loro contenuto, in questo contributo ci si soffermerà, in particolare, sull'ambito applicativo del **divieto di riconoscimento delle emozioni nei luoghi di lavoro**, evidenziandone il fondamento giuridico, le implicazioni pratiche e le possibili eccezioni.

Il divieto di riconoscimento delle emozioni in ambito lavorativo

L'AI Act sancisce il divieto di utilizzo di sistemi di AI per il riconoscimento delle emozioni nei luoghi di lavoro e negli istituti scolastici, salvo che per finalità mediche o di sicurezza.

Al di fuori di tale divieto, i sistemi di AI destinati al riconoscimento delle emozioni sono qualificati come ad alto rischio[5] e devono conformarsi agli obblighi normativi previsti per questa categoria di sistemi.

L'***affect technology***, ossia la tecnologia di riconoscimento delle emozioni, si sviluppa attraverso un insieme complesso di tecniche di raccolta, analisi e interpretazione di dati per inferire lo stato emotivo di un soggetto.

Le sue applicazioni spaziano dal neuromarketing all'industria dell'intrattenimento, dall'educazione alla selezione del personale, fino alla sanità.

Tuttavia, l'utilizzo di tali strumenti in contesti lavorativi pone **rilevanti problematiche**, in quanto può determinare una lesione dei diritti

[5] Ciò ai sensi dell'Allegato III, punto 1(c), dell'AI Act.

fondamentali, *in primis* la **privacy**, la **dignità umana** e la **libertà di autodeterminazione**.

In particolare, il riconoscimento delle emozioni nel contesto lavorativo si inserisce in un ambiente caratterizzato da **un significativo squilibrio di potere** tra datore di lavoro e lavoratore, con il rischio di generare **forme di controllo pervasivo** e di condizionare il comportamento individuale.

Si pensi, ad esempio, a sistemi di AI in grado di monitorare il livello di attenzione o il grado di stress dei dipendenti, oppure di valutare il loro stato d'animo sulla base delle espressioni facciali o del tono di voce.

Si tratta di strumenti che, se utilizzati senza adeguate garanzie, possono risultare altamente invasivi e discriminatori.

L'ambito di applicazione del divieto

Le Linee Guida precisano che il divieto di riconoscimento delle emozioni si riferisce a quei sistemi di AI impiegati per **inferire** o **identificare**[6] le **emozioni** attraverso i **dati biometrici** di una persona[7]. Si distingue, in particolare, tra:

- **identificazione delle emozioni**, ossia l'associazione diretta tra una determinata espressione e uno stato emotivo predefinito nel sistema di AI (ad es., rilevazione della rabbia sulla base di un'espressione facciale);
- **inferenza delle emozioni**, che avviene attraverso analisi complesse di dati biometrici e di altro genere, permettendo di dedurre stati emotivi in modo indiretto (ad es., determinare il livello di stress di un dipendente analizzando la velocità di battitura sulla tastiera).

Quanto, invece, alla nozione di "emozioni", le Linee Guida specificano che dalla stessa sono esclusi gli stati fisici (ad es., dolore o affaticamento), la mera rilevazione di espressioni, gesti o movimenti chiaramente visibili, a meno che non siano utilizzati per identificare o dedurre emozioni[8].

Ad esempio, non costituisce "riconoscimento delle emozioni", l'osservazione che una persona stia sorridendo; al contrario, concludere che una persona è felice è riconoscimento delle emozioni (si pensi, ad esempio, ad un sistema di AI che deduce che un dipendente sia infelice o arrabbiato con i clienti da gesti del corpo, un cipiglio o la mancanza di un sorriso).

Nel contesto lavorati[9], il divieto si applica **indipendentemente dalla natura del rapporto di lavoro** (dipendente, collaboratore, tirocinante, etc.) e si estende anche alla **fase di selezione del personale**.

[6] Il Considerando 44 dell'AI Act chiarisce infatti che il divieto di cui all'art. 5, par. 1, lett. f) dell'AI Act riguarda i sistemi di AI destinati a identificare o inferire emozioni.

[7] Ciò per ragioni coerenza, in quanto questo divieto deve essere interpretato in modo analogo alle norme applicabili ad altri sistemi di riconoscimento delle emozioni (Allegato III, punto 1(c) e art. 50 dell'AI Act). La definizione di "dati biometrici" nell'AI Act è ampia e include qualsiasi dato biometrico utilizzato per il riconoscimento delle emozioni, la categorizzazione biometrica o altri scopi (*cfr*. art. 3, n. 34, dell'AI Act).

[8] Sulla nozione di "emozione, si veda, in particolare, il Considerando 18 dell'AI Act.

[9] Le Linee Guida chiariscono che il concetto di "luogo di lavoro" si riferisce a qualsiasi spazio fisico o virtuale specifico in cui le persone svolgono compiti e responsabilità assegnati dal loro datore di lavoro o dall'organizzazione a cui sono affiliate. Include qualsiasi contesto in cui viene svolto il lavoro e può variare notevolmente in base alla natura dello stesso.

Pertanto, devono essere considerati vietati, ad esempio, i sistemi nel *recruiting* per analizzare lo stato emotivo dei candidati, le tecnologie di monitoraggio delle emozioni durante riunioni virtuali o videochiamate di lavoro, oppure l'utilizzo di telecamere integrate con l'AI in grado di rilevare le emozioni dei dipendenti.

L'eccezione al divieto: le finalità mediche o di sicurezza

L'AI Act contempla un'eccezione esplicita al divieto, limitata all'impiego di sistemi di riconoscimento delle emozioni utilizzati nell'ambito del luogo di lavoro e degli istituti educativi per finalità mediche o di sicurezza. Le Linee Guida precisano che tale deroga deve essere **interpretata in modo restrittivo**:

- gli **usi terapeutici** dovrebbero essere intesi come riferiti a dispositivi medici con marchio CE, escludendo quindi applicazioni di monitoraggio generico del benessere (ad es., un sistema di AI per rilevare *burnout* o depressione sul luogo di lavoro);
- il concetto di **motivi di sicurezza** deve essere inteso solo in relazione alla protezione della vita e della salute.

Profili giuslavoristici e protezione dei dati

Nel caso in cui un sistema di AI soddisfi le condizioni dell'eccezione per finalità mediche o di sicurezza, lo stesso dovrà in ogni caso rispettare i vincoli imposti dal Regolamento (UE) 679/2016 ("**GDPR**") e, in Italia, dall'articolo 4 della L. 300/1970, come modificato dal D.Lgs. 151/2015 ("**Statuto dei Lavoratori**"), relativo aicontrolli datoriali eseguiti tramite strumenti di monitoraggio a distanza della prestazione dei lavoratori.

Si pensi, ad esempio, ad un datore di lavoro che utilizzi un sistema di telecamere per monitorare le emozioni dei propri dipendenti unicamente per scopi di formazione personale, oppure ad un supermercato o una banca che utilizzino un simile sistema per rilevare clienti sospetti, ad esempio per capire se qualcuno stia per commettere una rapina.

Questi sistemi, possono essere utilizzati lecitamente, purché tuttavia **non influenzino la relazione lavorativa**, **non vengano monitorati i dipendenti** e siano **adottate adeguate misure di sicurezza**.

Pertanto, anche qualora un sistema rientrasse nelle eccezioni previste dall'AI Act, il datore di lavoro sarebbe tenuto a:

- garantire la trasparenza sia mediante **informativa privacy**, sia attraverso apposita **policy aziendale** – di solito, attraverso quella relativa all'utilizzo degli strumenti informatici – da pubblicizzare con le modalità più opportune;
- dimostrare la **necessità** e **proporzionalità** dell'utilizzo, valutando che non esistano mezzi alternativi meno invasivi in grado di raggiungere lo stesso obiettivo;
- effettuare, se del caso, una **valutazione d'impatto sulla protezione dei dati** ("**DPIA**") ai sensi dell'art. 35 GDPR;
- rispettare le **garanzie** e le **condizioni** di cui all'**art. 4 dello Statuto dei Lavoratori**, riguardanti la sussistenza di esigenze tassative (i.e. organizzative e produttive, di sicurezza del lavoro, di tela del patrimonio aziendale) e previo accordo collettivo o autorizzazione amministrativa, oltre al rispetto degli obblighi di trasparenza sopra citati.

Riflessioni finali: cosa devono fare in concreto le organizzazioni?

Alla luce delle disposizioni dell'AI Act e delle Linee Guida e onde evitare gravose sanzioni, le organizzazioni devono prioritariamente mappare e classificare i sistemi di AI che forniscono e/o utilizzano, al fine di individuare eventuali pratiche vietate, come il riconoscimento delle emozioni nei luoghi di lavoro.

Oltre a questa verifica preliminare, è essenziale valutare i rischi connessi e accertare se il sistema rientri nelle eccezioni previste dalla normativa, come quelle per finalità mediche o di sicurezza.

In ogni caso, anche laddove un sistema di AI rientri nell'eccezione sopra descritta, le aziende dovranno garantire il rispetto delle ulteriori normative applicabili, tra cui il GDPR e lo Statuto dei Lavoratori, adottando misure adeguate a tutelare la protezione dei dati personali e i diritti fondamentali dei lavoratori.

Per maggiori informazioni e approfondimenti

Carlo Impalà
Partner e Responsabile Osservatorio TMT&DP

Carloo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio TMT&DP**

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it