OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Marzo 2023

MONTHLY ROUNDUP

Marzo 2023

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Garante e altre autorità europee

- La difesa in giudizio non giustifica l'accesso alla posta elettronica del lavoratore [Link]
- GDPR: focus dei Garanti europei sul ruolo dei responsabili della protezione dei dati [Link]
- Telemarketing: il Garante privacy approva il Codice di condotta. Le regole entreranno in vigore una volta costituito l'Organismo di monitoraggio [Link]
- Deliberazione del 26 gennaio 2023 - Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio-giugno 2023 [Link]
- Autorità Garante austriaca (DSB): l'uso del pixel di tracciamento di Facebook viola direttamente il GDPR [Link]

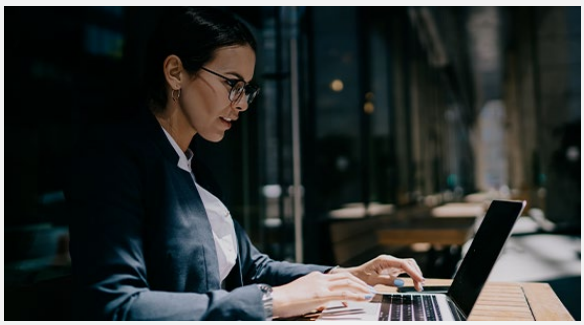
Provvedimenti EDPB

- EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain [Link]

PRINCIPALI AGGIORNAMENTI

- Whistleblowing: il decreto legislativo di recepimento della Direttiva
- Morri Rossetti 'Contributor' of Chambers' TMT Guide 2023
- Focus 2023 dei Garanti privacy europei sul ruolo dei DPO
- Intelligenza artificiale, dal Garante Privacy stop alla chatbot "Replika"

Whistleblowing: il decreto legislativo di recepimento della Direttiva europea



*Pubblicato in Gazzetta Ufficiale n. 63 del 15 marzo 2023, il Decreto Legislativo n. 24 del 10 marzo 2023, che entrerà in vigore il 30 marzo p.v. (il "***Decreto WB***"), ha recepito in via definitiva la Direttiva (UE) 2019/1937 in materia di whistleblowing ("****Direttiva WB****").*

L'implementazione obbligatoria di canali di segnalazione richiederà di valutare numerosi temi connessi di corporate governance, risk management, protezione dei dati personali e diritti dei lavoratori.

Whistleblowing: quadro normativo

La normativa prevede tutele specifiche per la protezione dei whistleblowers che segnalano violazioni di disposizioni normative nazionali ed europee, che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato.

In materia di *whistleblowing*, era già prevista nel nostro ordinamento la Legge n. 179/2017 che ha apportato rilevanti modifiche sia al D. Lgs. n. 165/2001, recante la disciplina in materia di protezione del segnalante nel settore pubblico, sia al D. Lgs. n. 231/2001 attraverso l'introduzione del comma 2 dell'art. 6, che regola la tutela per il segnalante nel settore privato.

Finalità del Decreto WB

Il nuovo testo del Decreto WB persegue la finalità di rafforzare i principi di trasparenza e responsabilità, senza alcuna distinzione tra organizzazione pubblica o privata, con riferimento ai settori indicati dalla Direttiva WB (tra questi: appalti pubblici, servizi finanziari, sicurezza dei prodotti e dei trasporti, ambiente, alimenti, salute pubblica, privacy, sicurezza della rete e dei sistemi informatici, concorrenza).

Soggetti obbligati

Ai sensi del Decreto WB, l'obbligo di istituzione di un canale di segnalazione è previsto:

- per tutti i soggetti del settore pubblico, compresi i soggetti di proprietà o sotto il controllo di tali soggetti, nonché per i Comuni con più di 10.000 abitanti;
- a decorrere dal 15 luglio 2023, per i soggetti del settore privato con più di 250 dipendenti, a prescindere dall'adozione o meno di un Modello Organizzativo ex D.lgs. 231/2001;
- a partire dal 17 dicembre 2023, per i soggetti del settore privato che abbiano impiegato nell'ultimo anno una media di lavoratori subordinati tra i 50 e i 249, a prescindere dall'adozione o meno di un Modello Organizzativo ex D.lgs. 231/2001.

La tutela del *whistleblower*

Ai sensi dell'art. 3 del Decreto WB, l'ambito di applicazione soggettivo delle disposizioni del citato Decreto ricomprende dipendenti, collaboratori, lavoratori subordinati e autonomi, liberi professionisti ed appartenenti ad altre categorie come volontari, tirocinanti e azionisti. Inoltre, le misure di protezione si applicano anche ai cosiddetti "facilitatori", ossia colleghi, parenti o affetti stabili del soggetto che ha segnalato.
Le misure di protezione previste sono volte a garantire la riservatezza del segnalante e il divieto

di atti ritorsivi. La gestione dei canali di segnalazione deve essere affidata a una persona o a un ufficio interno oppure a un soggetto esterno, autonomo e con personale specificamente formato.

Le segnalazioni possono essere rese in forma scritta o orale ovvero, su richiesta specifica del segnalante, attraverso incontri diretti e posti in essere entro un termine ragionevole.

In ottemperanza a quanto previsto dal Decreto WB, può beneficiare delle tutele anche chi effettua la segnalazione mediante la divulgazione pubblica, a patto che sia stato preliminarmente utilizzato il canale interno o esterno, ma non vi sia stata una risposta appropriata o che non siano stati utilizzati i canali interni o esterni per rischio di ritorsione o per inefficacia di quei sistemi.

Segnalazione di condotte illecite e sanzioni

L'Autorità Nazionale Anticorruzione ("**ANAC**") viene individuata, in presenza delle condizioni elencate dall'art. 6 del Decreto WB, quale unica autorità competente a ricevere e gestire segnalazioni in materia di whistleblowing attraverso appositi canali di segnalazione esterni.

Inoltre, in caso di mancato adeguamento o violazione della disciplina, l'ANAC può irrogare le sanzioni amministrative pecuniarie **da 10.000 a 50.000 euro** nei casi in cui vengano commesse ritorsioni o quando viene accertato che una segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza, oppure **da 10.000 a 50.000 euro** nel caso accerti che non sono stati istituiti canali di segnalazione o che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni; inoltre sono previste sanzioni **da 500 a 2.500** euro, nel caso in cui venga accertata la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia.

Profili privacy connessi alle segnalazioni e relativi adempimenti ai sensi del GDPR

Con riferimento ai profili relativi al trattamento dei dati personali, l'art. 13 del nuovo Decreto WB stabilisce che ogni trattamento dovrà essere posto in essere nel rispetto del Regolamento (UE) 679/2016 ("GDPR").

L'art. 13 del Decreto WB chiarisce i dubbi interpretativi scaturiti dal Parere dell'Autorità Garante per la protezione dei dati personali ("**Garante Privacy**") in merito alla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza ("OdV") eventualmente designato ai sensi del D.lgs. 231/2001.

In quell'occasione, il Garante Privacy si concentrò unicamente sui profili privacy connessi ai trattamenti svolti dall'OdV nell'attività di vigilanza (qualificando i membri dell'OdV come "soggetti autorizzati" ai sensi dell'art. 29 del GDPR e dell'art. 2 *quaterdecies* del D.lgs. 196/2003 così come modificato dal D.lgs. 101/2018, "**Codice Privacy**"), senza occuparsi, invece, di quelli derivanti da eventuali segnalazioni.

Il predetto articolo interviene quindi sul punto, individuando in modo chiaro i *ruoli privacy* delle parti coinvolte nei trattamenti connessi alla gestione delle segnalazioni e definendone le relative responsabilità.

Nello specifico, i trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni saranno svolti dai soggetti individuati dal Decreto WB in qualità di autonomi titolari del trattamento, i quali quindi saranno responsabili del rispetto di tutti gli obblighi previsti dal GDPR.

Rispetto agli adempimenti previsti dal GDPR, i titolari del trattamento sono tenuti - oltre che al rispetto dei principi di cui all'art. 5 e 25 del GDPR (rispettivamente, i principi applicabili al

trattamento e il principio di privacy *by design* e *by default*) e all'adempimento di tutti gli ulteriori obblighi previsti dal GDPR (ad es., obblighi di trasparenza nei confronti degli interessati, etc.) - anche ad adottare e implementare una serie di misure sia tecniche che organizzative volte a tutelare la riservatezza del segnalante, nonché l'integrità e la confidenzialità dei dati personali oggetto di segnalazione.

A tale fine, nell'ambito dell'implementazione del proprio modello di ricevimento e gestione delle segnalazioni interne, gli enti pubblici e privati destinatari delle nuove norme dovranno svolgere una valutazione di impatto (cd. "*Data Protection Impact Assesment*") ex art. 35 del GDPR al fine di individuare le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati.

Con riferimento alla **conservazione della documentazione inerente alle segnalazioni**, l'art. 14 del Decreto WB stabilisce che la stessa debba essere conservata per il **tempo strettamente necessario al trattamento della segnalazione** e comunque non oltre cinque anni a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza e del principio di limitazione della conservazione di cui all'art. 5 del GDPR.

Questo periodo massimo di conservazione è, secondo il Parere del Garante Privacy espressosi a gennaio 2023 sullo schema di Decreto, compatibile con la durata media del termine prescrizionale dei principali illeciti suscettibili di verificarsi.

Infine, con riferimento alla **riservatezza delle segnalazioni e all'identità del segnalante**, l'art. 12 del Decreto WB sancisce il principio generale secondo cui le segnalazioni non possano essere utilizzate se non per darvi seguito, con **espresso divieto di rivelazione dell'identità del segnalante a persone diverse da quelle specificamente autorizzate** anche ai sensi degli articoli 29 e 32(4) del GDPR e 2-*quaterdecies* del Codice Privacy, ad eccezione del caso in cui il segnalante abbia manifestato il proprio consenso espresso.

Invece, nell'ambito del procedimento penale, l'identità del segnalante è di per sé coperta da segreto ai sensi dell'articolo 329 c.p.p., mentre nel procedimento dinanzi alla magistratura contabile essa non può essere rivelata sino alla chiusura della fase istruttoria.

Nell'ambito del procedimento disciplinare, infine, l'identità del segnalante non può essere rivelata ove la contestazione dell'illecito disciplinare si fondi su accertamenti distinti e ulteriori rispetto alla segnalazione.

Profili giuslavoristici

Da un punto di vista giuslavoristico, è necessario porre l'accento sulla tema della tutela offerta al *whistleblower* e agli altri soggetti ad esso equiparati.

Gli aspetti principali da segnalare sono quelli riguardanti la **tutela della riservatezza dell'identità del segnalante e il divieto, da parte del datore di lavoro, di porre in essere condotte ritorsive nei confronti dello stesso** (i.e. licenziamento, mutamento di mansioni, così come ogni altra misura che possa essere ritenuta tale), con conseguenze anche dal punto di vista processuale in quanto viene alleggerito l'onere probatorio in capo al segnalante. Grava sul datore di lavoro, infatti, dimostrare che le misure adottate nei confronti del dipendete sono fondate su ragioni estranee alla segnalazione.

L'articolo 17 del Decreto WB, poi, sancisce espressamente il divieto di ritorsione nei confronti del segnalante e fornisce, in linea con

quanto indicato anche nell'art. 19 della Direttiva WB, un elenco non esaustivo di possibili fattispecie ritorsive, quali il licenziamento, il mutamento di funzioni, il cambiamento del luogo di lavoro o la modifica dell'orario di lavoro, la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa, le note di merito negative o le referenze negative, l'adozione di misure disciplinari.

La garanzia di riservatezza nei confronti del segnalante viene garantita anche nell'ambito del procedimento disciplinare avviato nei confronti del soggetto segnalato in quanto non possono essere rivelate, a persone diverse da quelle espressamente autorizzate, senza il consenso espresso del segnalante, l'identità di quest'ultimo e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, la stessa.

Con la modifica dell'articolo 4 della legge n. 604 del 1966, viene prevista la **nullità del licenziamento conseguente all'esercizio di un diritto ovvero alla segnalazione**, **alla denuncia all'autorità giudiziaria o contabile o alla divulgazione pubblica effettuate in base alle norme sul *whistleblowing*.**

Infine, quale ulteriore tutela nei confronti del whistleblower, l'articolo 22 del Decreto WB stabilisce che le rinunce e le transazioni, integrali o parziali, che hanno per oggetto i diritti e le tutele previsti dal decreto medesimo non sono valide, salvo che siano effettuate nelle forme e nei modi di cui all'art. 2113(4) del c.c.

Conclusioni: come adeguarsi alle nuove previsioni?

Le disposizioni del Decreto WB hanno effetto a decorrere dal 15 luglio 2023.

Per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, fino a duecentoquarantanove, l'obbligo di istituzione del canale di segnalazione interna ha effetto a decorrere dal 17 dicembre 2023.

In considerazione di quanto sopra, i soggetti interessati dalla nuova normativa dovranno quindi prevedere all'interno del proprio contesto aziendale tutti quei processi necessari per dare attuazione al Decreto WB e, in particolare, tali soggetti dovranno:

- predisporre o implementare appositi canali di segnalazione interni per consentire di inviare segnalazioni sia per iscritto (attraverso una piattaforma online, un indirizzo e-mail o per posta) sia a voce (tramite una hotline telefonica o un sistema di segreteria telefonica).

Se i canali di segnalazione interni non dovessero essere implementati, i segnalanti potranno rivolgersi solo alleautorità pubbliche o ai media, con evidenti conseguenze finanziarie e reputazionali per le aziende;

- tutelare la riservatezza del segnalante e del contenuto della segnalazione, anche tramite l'implementazione di misure tecniche ed organizzative ai sensi del GDPR (ad esempio, strumenti di crittografia);
- adeguare i canali di segnalazione già adottati, se si tratta di enti e società già dotati di Modelli di Organizzazione e Gestione;
- regolamentare la gestione dei canali di segnalazione mediante la predisposizione di una specifica procedura, che disciplini le modalità e i destinatari della segnalazione, i relativi adempimenti e le funzioni coinvolte;

- informare e sensibilizzare dipendenti e terzi interessati in merito alle finalità, alle modalità di utilizzo dei canali di segnalazione e alle procedure adottate.

* * *

Morri Rossetti 'Contributor' of Chambers' TMT Guide 2023

The TMT 2023 guide features 29 jurisdiction and provides the latest legal information on the metaverse, the digital economy, cloud computing, AI and big data, the internet of things (IoT), audio-visual media service regulation, telecommunications rules, technology agreements, and trust services and digital signatures.

You can find here the Italian Chapter of the Guide.

* * *

Focus 2023 dei Garanti privacy europei sul ruolo dei DPO

In data 15 marzo 2023, il Comitato europeo per la protezione dei dati personali ("**EDPB**") ha reso nota la sua **seconda iniziativa** nell'ambito del *Coordinated Enforcement Framework* ("CEF"): il focus dell'indagine sarà il **ruolo dei Data Protection Officer** ("**DPO**").

Il CEF mira ad armonizzare l'attuazione delle norme previste dal Regolamento UE 2016/679 ("**GDPR**") e la cooperazione tra le autorità di controllo nazionali. Già nel 2022, il CEF aveva avviato la sua prima indagine in merito all'uso dei servizi cloud nel settore pubblico.

Nel corso del 2023, infatti, le 26 autorità di controllo dello Spazio Economico Europeo, compreso il Garante europeo della protezione dei dati (EDPS), parteciperanno all'indagine avviata dal CEF focalizzandosi sul **controllo del rispetto dei requisiti di cui agli articoli 37-39 del GDPR** per la designazione e la posizione dei DPO.

Come sottolineato dall'EDPB nel suo comunicato stampa, il tema oggetto dell'indagine assume rilevanza in quanto la posizione ricoperta dai DPO – che funge da intermediario tra le Autorità di protezione dei dati personali, gli interessati e i titolari del trattamento – è essenziale ai fini dell'attuazione delle norme dal GDPR e, in particolare, al fine di garantire una tutela efficace dei diritti degli interessati.

L'indagine sarà pertanto volta a verificare che la posizione ricoperta dai DPO all'interno delle

organizzazioni rispetti le previsioni del GDPR e sarà focalizzata, in particolare, a verificare l'effettivo svolgimento delle attività demandate al DPO, la sussistenza delle risorse necessarie per lo svolgimento di tali compiti (ex art. 38, co. 2 del GDPR) così come la sussistenza di eventuali conflitti di interessi (ex art. 38, co. 6 del GDPR).

Le indagini relative al controllo del rispetto dei requisiti di cui agli articoli 37-39 del GDPR potranno essere svolte dalle autorità di controllo competenti in vari modi, tra i quali:

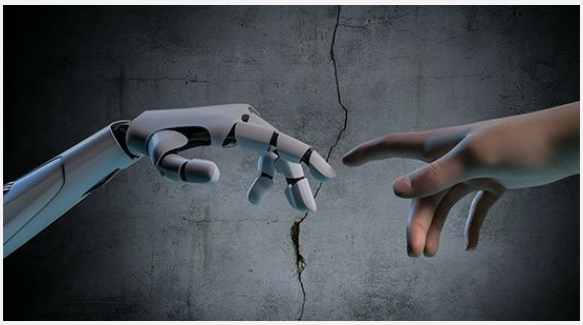
a) attraverso l'invio ai DPO di questionari finalizzati a raccogliere elementi istruttori ovvero per individuare la necessità di accertamenti formali;
b) attraverso l'avvio di accertamenti formali;
c) follow-up di accertamenti formali in corso.

I risultati dell'iniziativa congiunta saranno analizzati in modo coordinato e le autorità di controllo nazionali avranno la facoltà di decidere in merito a possibili ulteriori azioni nazionali di vigilanza e applicazione. Inoltre, i risultati saranno aggregati, generando una visione più approfondita dell'argomento e consentendo un follow-up mirato a livello dell'UE.

L'EDPB, come già effettuato nel 2022, pubblicherà una relazione sull'esito di questa analisi una volta che le azioni saranno concluse.

* * *

Intelligenza artificiale, dal Garante Privacy stop alla chatbot "Replika"



"Replika" è una chatbot dotata di una interfaccia scritta e vocale che - basandosi sull'intelligenza artificiale - genera un "amico virtuale" che l'utente può decidere di configurare come amico, partner romantico o mentore ("**Replika**" o l'"**Applicazione**").

Più dettagliatamente, sembrerebbe che Replika sia in grado di migliorare il benessere emotivo dell'utente, aiutandolo a comprendere i suoi pensieri e i suoi sentimenti, a tenere traccia del suo umore, ad apprendere capacità di *coping* (ossia, di controllo dello stress) a calmare l'ansia e a lavorare verso obiettivi come il pensiero positivo, la gestione dello stress, la socializzazione e la ricerca dell'amore.

Tali caratteristiche, riconducibili principalmente ad interventi sull'umore della persona, sono state ritenute potenzialmente idonee ad accrescere i rischi per i minori d'età e, più in generale, per le persone in stato di fragilità emotiva, anche in considerazione della proposizione agli stessi di risposte assolutamente inidonee al loro grado di sviluppo (ad esempio, diverse recensioni pubblicate nei principali "App store" contengono commenti di utenti che lamentano contenuti sessualmente inopportuni forniti dalla stessa Applicazione).

Per tale ragione, l'Autorità Garante per la protezione dei dati personali ("**Garante Privacy**" o l'"**Autorità**") – con il provvedimento dello scorso 2 febbraio 2023 – ha disposto con effetto

immediato, nei confronti della società statunitense Luka Inc. che sviluppa e gestisce Replika, la limitazione provvisoria del trattamento dei dati personali degli utenti italiani.

Alla base della decisione del Garante Privacy sono poste problematiche connesse al trattamento dei dati personali dei minori.

Infatti, come rilevato dall'Autorità, Replika – sebbene nella propria privacy policy dichiari di non raccogliere consapevolmente dati personali di minori di età inferiore ai 13 anni e incoraggi i genitori e i tutori legali a (i) monitorare l'utilizzo di Internet da parte dei propri figli, (ii) rispettare la privacy policy istruendo i minori a non fornire dati personali nell'ambito dell'utilizzo dell'applicazione senza la loro autorizzazione e (iii) a contattare la piattaforma nell'ipotesi in cui abbiano motivo di ritenere che un minore abbia fornito dati personali affinché questi possano essere eliminati dai database – tuttavia durante la fase di creazione di un account, l'Applicazione non prevede alcuna procedura di verifica e controllo dell'età dell'utente (di cui il sistema chiede unicamente nome, e-mail e genere), né tantomeno meccanismi di interdizione o blocco dell'utente stesso a fronte di dichiarazioni che esplicitino la sua minore età.

Inoltre, il Garante Privacy ha ritenuto che la privacy policy dell'Applicazione non può ritenersi conforme ai principi e agli obblighi in tema di trasparenza previsti dal Regolamento UE 679/2016 ("**GDPR**"), in quanto non vengono identificati gli elementi essenziali del trattamento con particolare riguardo all'utilizzo dei dati personali dei minori, ponendosi quindi in contrasto con l'art. 13 del GDPR. Ne consegue quindi anche l'impossibilità di individuare la base giuridica delle varie operazioni di trattamento effettuate da Replika, dovendosi in ogni caso escludere che, con riguardo in particolare ai minori, questa possa – anche solo implicitamente – essere rinvenuta nella disciplina contrattuale, attesa la riconosciuta incapacità dei minori nell'ordinamento italiano di concludere contratti per la fruizione di servizi quale quello in esame.

Dall'analisi condotta dall'Autorità, deriva una chiara violazione degli artt. artt. 5 (**Principi applicabili al trattamento di dati personali**), 6 (**Liceità del trattamento**), 8 (**Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione**), 9 (**Trattamento di categorie particolari di dati personali**) e 25 (**Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**) del GDPR.

Alla luce delle violazioni sopra individuate, l'Autorità ha disposto nei confronti della società sviluppatrice dell'Applicazione, in via d'urgenza, la misura della limitazione provvisoria del trattamento di tutti i dati personali degli utenti stabiliti nel territorio italiano, invitando la predetta società a comunicare, entro 20 giorni, le misure intraprese in attuazione di quanto richiesto dal Garante Privacy, pena una sanzione fino a 20 milioni di euro o fino al 4% del fatturato globale annuo.

Conclusioni

L'intelligenza artificiale ("**AI**") non è fantascienza, fa già parte delle nostre vite: che si tratti di utilizzare un assistente personale virtuale per organizzare la nostra giornata lavorativa, viaggiare in un veicolo a guida autonoma o avere un telefono che ci suggerisce le canzoni o i ristoranti che potrebbero piacerci, l'IA è una realtà che, in modo sempre più pervasivo, influenza la quotidianità di numerosi individui.

Lo sviluppo tecnologico, le interazioni con tecnologie facenti uso di *software* di AI, la raccolta massiva di big data e la rielaborazione degli stessi attraverso tecniche e strumenti di machine learning, hanno rappresentato per il legislatore europeo un importante campanello di allarme per

cominciare a strutturare un quadro normativo in grado di permettere lo sviluppo tecnologico senza mettere a repentaglio i diritti fondamentali dell'individuo e i valori europei.

A tal fine, le istituzioni europee – già a partire dal 2018 – avevano manifestato la loro intenzione di ritagliarsi un ruolo proattivo in materia di intelligenza artificiale, stanziando investimenti consistenti sul relativo mercato, nonché implementando un quadro normativo solido volto a supportare lo sviluppo dell'AI attraverso la creazione di un ambiente improntato sulla fiducia e sulla responsabilità sia delle imprese che delle persone.

In considerazione di questi intenti, la Commissione europea ha presentato, nell'aprile del 2021, l'*Artificial Intelligence* Act ("AI ACT"), una proposta di regolamento europeo che rappresenta il primo tentativo al mondo di regolamentazione di questo settore, volto a stabilire regole armonizzate sull'AI.

Nello specifico, l'AI ACT classifica le applicazioni di AI in tre categorie di rischio di impatto negativo su diritti fondamentali quali la dignità umana, la libertà, l'uguaglianza, la democrazia, il diritto alla non discriminazione, la protezione dei dati, nonché la salute e la sicurezza. Infatti, tanto più le applicazioni sono in grado di minacciare questi diritti, quanto più severe saranno le misure adottate per eliminare o mitigare l'impatto negativo sui diritti fondamentali, fino al divieto assoluto di utilizzo di quei prodotti che sono completamente incompatibili con questi diritti.

A dicembre 2022, il Consiglio dell'Unione Europea ha raggiunto una posizione comune sulla proposta di regolamento e si attende che anche il Parlamento europeo adottati la propria posizione prima del trilogo finale tra le tre principali istituzioni comunitarie che dovrà conciliare i testi che dovranno poi essere ratificati perché la proposta diventi legge.
Si prospetta la chiusura di questo iter, e quindi l'adozione dell'AI ACT entro la fine dell'anno.

* * *

Per maggiori informazioni, potete contattare:

Carlo Impalà
Partner e Responsabile Dip. TMT e Data Protection
(Carlo.Impala@MorriRossetti.it)

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it