OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Luglio - agosto 2026

Luglio e agosto 2026

I principali aggiornamenti in materia di TMT & Data Protection dei mesi di luglio e agosto.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Dai Garanti europei le linee guida su anonimizzazione, web scraping e blockchain; [Link]
- AI Act, Garante: sì allo schema di decreto legislativo, ma con maggiori garanzie; [Link]
- AI Act, Garante privacy: rafforzare le tutele per i dati biometrici. [Link]

EDPB

- L'EDPB fa luce sull'anonimizzazione e sullo scraping web per l'IA generativa e adotta la versione finale delle linee guida sulla blockchain. [Link]

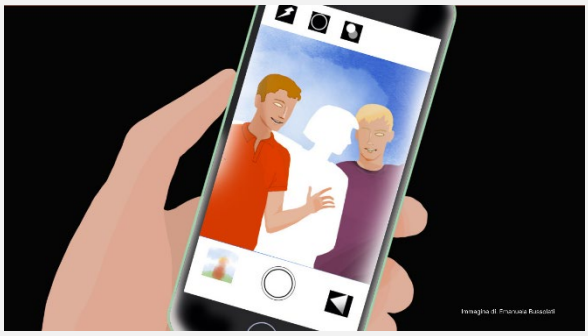
AGCOM

- Digital Services Act – Relazione annuale 2025; [Link]
- Atto integrativo delle linee guida per le campagne di comunicazione contro i disturbi da gioco d'azzardo. [Link]

ACN

- Pubblicate le FAQ ACN sulle attività di monitoraggio, vigilanza ed esecuzione nei confronti dei soggetti NIS; [Link]
- Aggiornate le FAQ ACN sulle misure di sicurezza per la supply chain dei soggetti NIS; [Link]
- Aggiornate le FAQ ACN sugli obblighi degli organi di amministrazione e direttivi dei soggetti NIS. [Link]

Minori online: il nuovo quadro regolatorio tra verifica dell'età e obblighi per le imprese



Circa il 97% dei minori nell'UE utilizza Internet quotidianamente e i *social media* sono la principale fonte di informazioni per il 65% di loro[1]. Per tale ragione, il legislatore europeo e quello italiano stanno ridefinendo le regole del rapporto tra minori e servizi digitali.

Per le imprese che operano *online*, si tratta di un cambiamento significativo: **nuovi obblighi di progettazione dei servizi**, meccanismi di **verifica dell'età** in fase di definizione e soglie di **consenso digitale** in evoluzione.

L'ambiente digitale è parte integrante della quotidianità dei più giovani. Se, da un lato, ciò offre opportunità in ambiti quali lo sviluppo dell'identità, l'apprendimento, la partecipazione civica, le relazioni e la creatività, dall'altro la fruizione dei servizi della società dell'informazione può comportare rischi rilevanti: esposizione a contenuti illegali o dannosi (violenti, terroristici o pornografici), rischi di contatto (come il cyberbullismo o dinamiche di adescamento), uso eccessivo o compulsivo del servizio ed esposizione a pratiche di sfruttamento come il gioco d'azzardo.

L'avvento dell'intelligenza artificiale generativa (in cui rientrano, ad esempio, sistemi come ChatGPT, Grok, Gemini) ha inoltre introdotto ulteriori minacce: la possibilità di **creare contenuti sintetici realistici** (*deepfake*) **senza il consenso dei soggetti ritratti**, l'impiego di sistemi conversazionali capaci di **condizionare comportamenti e decisioni**, e la personalizzazione algoritmica dei contenuti sulle vulnerabilità cognitive degli utenti più giovani.

Queste dinamiche hanno impresso un'accelerazione significativa alla risposta normativa a livello europeo e nazionale.

Il contesto normativo

Ad oggi non è presente una disciplina unitaria sulla protezione dei minori nel digitale. Ne consegue che le imprese devono orientarsi tra **una pluralità di fonti** che intervengono su aspetti diversi ma interconnessi e che richiedono una lettura sistematica.

Tra le normative principali, sul fronte della **protezione dei dati personali**, il GDPR e il Codice Privacy stabiliscono le condizioni per il trattamento lecito dei dati dei minori, incluse le regole sul consenso digitale.

In materia di **servizi digitali**, il Regolamento (UE) 2022/2065 (il "**Digital Services Act**" o "**DSA**") impone obblighi specifici ai fornitori di piattaforme *online*, dalla pubblicità mirata ai minori alla progettazione sicura dei servizi.

Il quadro è completato dalle Linee guida della Commissione europea sulla protezione dei minori (le "**Linee Guida**"), con cui la Commissione ha individuato le misure che le piattaforme accessibili ai minori dovrebbero adottare per garantire un elevato livello di tutela, sicurezza e privacy [2], e dalla Raccomandazione (UE)

[1] https://digital-strategy.ec.europa.eu/it/policies/protecting-young-people-online

[2] Per maggiori approfondimenti sulle Linee Guida rinviamo al nostro precedente contributo "*Proteggere i minori nel digitale: le linee guida della Commissione europea sul DSA*".

2026/1035 sulla verifica dell'età (la "**Raccomandazione**"), che indica agli Stati membri le azioni da intraprendere entro il 31 dicembre 2026 per assicurare a tutti i cittadini dell'UE l'accesso a una soluzione di verifica dell'età solida e rispettosa della vita privata.

Per le **piattaforme di condivisione video**, la Direttiva 2010/13/UE, come modificata dalla Direttiva (UE) 2018/1808 (la "**Direttiva SMAV**") e recepita in Italia con il d.lgs. n. 208/2021 (il "**TUSMA**"), impone ai fornitori l'adozione di misure adeguate a proteggere i minori dai contenuti che possano nuocere al loro sviluppo fisico, mentale o morale, tra cui meccanismi di segnalazione dei contenuti dannosi, sistemi di verifica dell'età, strumenti di controllo parentale e sistemi di classificazione (in Italia, in particolare, ai sensi dell'art. 42 del TUSMA).

Quanto all'**intelligenza artificiale**, l'AI Act (Reg. UE 1689/2024) vieta i sistemi di IA che sfruttano le vulnerabilità delle persone in ragione, tra l'altro, dell'età e introduce specifici obblighi di trasparenza sui *deepfake* e il divieto delle c.d. *nudify apps*. A livello nazionale, la Legge 132/2025 dedica disposizioni specifiche all'utilizzo dei sistemi di IA da parte dei minori.

A questo quadro si aggiunge, infine, il Disegno di Legge n. 1136 (il "**DDL 1136**"), attualmente all'esame del Parlamento, che propone nuove regole sull'accesso dei minori ai *social network* e sulla verifica dell'età.

Le sfide operative per le imprese

Al di là della complessità del quadro normativo, le imprese devono confrontarsi con **tre sfide operative** concrete:

1. Verificare l'età degli utenti

Qualsiasi soglia di età – per l'accesso ai servizi o per il consenso al trattamento dei dati – è efficace solo se supportata da meccanismi di verifica affidabili. I sistemi di autodichiarazione, ancora largamente diffusi, sono ampiamente riconosciuti come **insufficienti**.

La Raccomandazione ricorda che è fondamentale che l'applicazione dei metodi di verifica dell'età sia adeguata e proporzionata e comprenda solide garanzie di sicurezza e caratteristiche di tutela della vita privata per prevenire la raccolta non necessaria di dati, l'accesso non autorizzato o l'uso improprio di informazioni personali, sottolineando che, al fine di evitare la frammentazione del mercato interno, è necessario adottare una soluzione armonizzata.

La Commissione agevola lo sviluppo, negli Stati membri, di soluzioni dell'UE di verifica dell'età armonizzate, che tutelino la vita privata, siano cybersicure, conformi alle norme in materia di protezione dei dati e solide, attraverso un progetto che consiste in specifiche tecniche allineate a quelle dei portafogli europei di identità digitale (c.d. EU Digital Wallet) e un'implementazione o*pen source* di tali soluzioni come un'*app mobile* che può essere personalizzata in funzione dei contesti nazionali (la soluzione, sviluppata dalla Commissione europea in *open source*, è già in fase di sperimentazione in diversi Stati membri, inclusa l'Italia).

Per tutelare la vita privata, i metodi di verifica dell'età dovrebbero almeno prevedere la divulgazione selettiva di informazioni alla parte facente affidamento sulla certificazione e limitare le informazioni, per impostazione predefinita, a una risposta di tipo vero/falso per quanto riguarda le informazioni relative all'età richieste dalla parte facente affidamento sulla certificazione, senza fornire ulteriori informazioni sul cittadino.

Al fine di proteggere i cittadini dai rischi per la vita privata e per la protezione dei dati, tra cui il

tracciamento della loro attività online, tali metodi dovrebbero inoltre comprendere garanzie tecniche, tra cui l'uso di dimostrazioni a conoscenza zero (*zero-knowledge proof*).

In particolare, secondo questo sistema, la piattaforma riceve esclusivamente un'informazione binaria ("età superiore alla soglia richiesta: sì/no"), **senza accedere al nome**, **alla data di nascita** o ad altri **dati identificativi** dell'utente.

La Raccomandazione prevede che la responsabilità di fornire servizi di verifica dell'età dovrà essere affidata solo a fornitori affidabili e rigorosamente controllati, dei quali sarà stilato un elenco consultabile dai fornitori di piattaforme online e da tutte le parti interessate[3].

Sul piano interno, il DDL 1136 – se approvato nell'attuale formulazione – introdurrebbe, 'in capo ai fornitori di servizi della società dell'informazione operanti in Italia, uno specifico obbligo di verificare l'età degli utenti, secondo modalità tecniche e di processo che l'AGCOM, sentito il Garante Privacy, dovrà definire entro sessanta giorni dall'entrata in vigore della legge (art. 2).

2. Progettare servizi sicuri per i minori (*safety by design*)

Il *focus* regolatorio si sta spostando dal controllo dei singoli contenuti alla responsabilità per le scelte progettuali che possono risultare dannose per gli utenti più giovani.

Le Linee Guida qualificano espressamente come incompatibili con un elevato livello di protezione dei minori tecniche quali lo *scrolling* infinito, le notifiche calibrate per massimizzare l'attenzione, i sistemi di raccomandazione ottimizzati per il tempo di permanenza, l'*autoplay* e i meccanismi di ricompensa intermittente.

Le Linee Guida prevedono, tra l'altro, di rendere gli *account* dei minori più privati per impostazione predefinita e di impedire che *account* sconosciuti contattino i minori, di modificare i sistemi di raccomandazione per ridurre al minimo il rischio che i minori si imbattano in contenuti illegali o dannosi, di disabilitare per impostazione predefinita le caratteristiche che contribuiscono a un uso eccessivo, di mettere in atto misure di garanzia per i chatbot di IA integrati nelle piattaforme *online* e di migliorare gli strumenti di moderazione e segnalazione.

Per le imprese, questo si traduce nel dovere di ripensare la progettazione dei propri servizi secondo il principio del *safety by design*: integrare la **protezione dei minori nella fase di sviluppo del servizio**, adottando impostazioni predefinite protettive, configurando algoritmi che non sfruttino le vulnerabilità cognitive dei più giovani, ed **eliminando le funzionalità che incentivano un utilizzo compulsivo**.

L'intensità di questi obblighi varia in base alla dimensione dell'impresa. Le piattaforme *online* di dimensioni molto grandi (VLOP) e i motori di ricerca di dimensioni molto grandi (VLOSE) sono soggetti a **obblighi rafforzati** di valutazione e mitigazione dei rischi sistemici, che possono includere l'adeguamento degli algoritmi, l'introduzione di strumenti di verifica dell'età e misure specifiche di moderazione dei contenuti.

[3] Per essere registrati negli elenchi gestiti dalla Commissione, i fornitori di attestati comprovanti l'età e di soluzioni di verifica dell'età dovrebbero rispettare i requisiti stabiliti nel regime dell'UE di verifica dell'età, nel Regolamento (UE) n. 910/2014, nel Regolamento di esecuzione (UE) 2025/2160 e nella Direttiva (UE) 2022/2555. La Commissione verificherà che tali requisiti siano continuamente rispettati. Qualora i fornitori non rispettino tali standard elevati, la Commissione provvederà affinché siano rimossi dagli elenchi.

3. Le soglie di età per il consenso digitale

Le soglie di età per il consenso digitale dei minori restituiscono un quadro frammentario. Il DSA non preclude l'applicazione di altre normative nazionali e, come ribadito dalla Commissione nelle Linee Guida, gli Stati membri possono introdurre discipline nazionali che, in conformità al diritto 'dell'Unione, prescrivano un'età minima per accedere a determinati prodotti o servizi offerti su una piattaforma online.

L'art. 8 del GDPR prevede, con riferimento all'offerta diretta di servizi della società dell'informazione ai minori, che il trattamento dei loro dati personali sia lecito ove il minore abbia almeno **16 anni**, consentendo agli Stati membri di abbassare tale soglia fino a 13 anni. L'Italia ha esercitato tale facoltà fissando la soglia a **14 anni** (art. 2-*quinquies* del Codice Privacy).

Il DDL 1136 interverrebbe su questo assetto lungo due direttrici: da un lato, sancirebbe la nullità dei contratti per l'accesso ai servizi della società dell'informazione conclusi da minori di 15 anni, salvo il caso in cui il contratto sia stato concluso, per conto del minore, da chi ne esercita la responsabilità genitoriale o dal tutore (art. 3); dall'altro, abrogherebbe la deroga italiana del Codice Privacy (art. 4), spostando così, sul piano pratico, in avanti la soglia rilevante per l'accesso autonomo dei minori ai servizi digitali.

La situazione si complica sul fronte dell'intelligenza artificiale: la Legge n. 132/2025 consente ai minori di utilizzare autonomamente i sistemi di IA a partire dai **14 anni**, purché venga prestato il consenso da chi esercita la responsabilità genitoriale[4].

Un'impresa che gestisce un servizio con componenti *social* e funzionalità basate sull'IA potrebbe dunque dover applicare soglie di età diverse alla medesima platea di utenti – una complessità operativa non trascurabile.

Obblighi concreti per le imprese

Gli obblighi applicabili variano in funzione del tipo di servizio fornito e delle dimensioni dell'impresa. In particolare:

- fornitori di piattaforme *online* (inclusi *social network*)

I fornitori di piattaforme *online* devono rispettare il divieto di pubblicità basata sulla profilazione dei minori e progettare i propri servizi garantendo una protezione effettiva.

In concreto, ciò richiede l'adozione di impostazioni predefinite protettive, la configurazione di sistemi di raccomandazione che non massimizzino l'attenzione e il coinvolgimento degli utenti, l'eliminazione delle funzionalità che inducono comportamenti compulsivi e la predisposizione di strumenti di controllo parentale.

Le VLOP e le VLOSE devono inoltre condurre valutazioni periodiche dei rischi sistemici che i propri servizi possono generare per i minori e adottare misure di attenuazione ragionevoli, proporzionate ed efficaci.

È opportuno precisare che la mera previsione, nei termini e condizioni d'uso, secondo cui il servizio è destinato esclusivamente a utenti maggiorenni **non è sufficiente a escludere l'applicazione di tali obblighi**.

Qualora non siano adottate misure concrete ed efficaci volte a impedire l'accesso ai minori, il

[4] La L. 132/2025 prevede altresì che il minore di 18 anni che abbia compiuto 14 anni possa esprimere autonomamente il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di IA, purché le informazioni e le comunicazioni relative al trattamento siano facilmente accessibili e comprensibili.

servizio deve considerarsi, a tutti gli effetti, accessibile anche a questi ultimi;

- piattaforme di condivisione video

Oltre agli obblighi comuni a tutte le piattaforme online, i fornitori di piattaforme di condivisione video soggetti alla giurisdizione italiana devono predisporre, ai sensi del TUSMA, sistemi di verifica dell'età per i contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori, nonché strumenti di controllo parentale;

- altri fornitori di servizi della società dell'informazione

Per le imprese che offrono servizi diversi dalle piattaforme *online* (ad esempio servizi di *e-commerce*) o che trattano dati di minori senza operare come piattaforma, non sussiste attualmente un obbligo espresso di verifica dell'età.

La normativa privacy richiede di adottare misure adeguate a garantire la validità del consenso del minore, senza prescrivere uno specifico meccanismo tecnico.

In questo contesto, rappresenta una buona prassi condurre un *risk assessment* per valutare se, in ragione della natura del servizio offerto, della tipologia di dati trattati e della plausibile presenza di minori tra gli utenti, sia opportuno adottare meccanismi di verifica dell'età conformi al *framework* europeo o a standard equivalenti.

Le novità attese dal DDL 1136

Se approvato nella sua attuale formulazione, il DDL 1136 introdurrebbe **due novità di portata** rilevante per i fornitori di servizi della società dell'informazione che operano in Italia, riguardanti, da un lato, la validità dei contratti conclusi con i minori e, dall'altro, l'obbligo di verifica dell'età degli utenti.

Sotto il primo profilo, l'art. 3 del DDL prevede la nullità dei contratti per l'accesso ai servizi della società dell'informazione conclusi da minori di 15 anni, salvo il caso in cui il contratto sia stato concluso, per conto del minore, da chi ne esercita la responsabilità genitoriale o dal tutore.

La norma precisa che tali contratti non possono nemmeno costituire base giuridica del trattamento dei dati personali. In parallelo, l'art. 4 abrogherebbe il comma 1 dell'art. 2-*quinquies* del Codice Privacy, che oggi fissa a 14 anni la soglia per il consenso digitale del minore: il combinato disposto delle due disposizioni innalzerebbe, sul piano pratico, a 15 anni la soglia rilevante per l'accesso autonomo dei minori ai servizi digitali.

L'onere di dimostrare la corretta conclusione dei contratti graverebbe sui fornitori, esposti alle sanzioni previste dal TUSMA e dal GDPR, ciascuno per quanto di rispettiva competenza.

Sotto il secondo profilo, l'art. 2 introdurrebbe uno specifico obbligo di verifica dell'età degli utenti in capo ai fornitori che offrono servizi in Italia, con modalità tecniche e di processo che dovranno essere definite dall'AGCOM, sentito il Garante, entro 60 giorni dall'entrata in vigore della legge.

L'obbligo si applicherebbe, per espressa previsione della norma, ai soli fornitori che registrino un numero di accessi unici mensili superiore alla soglia dimensionale che sarà anch'essa determinata dall'AGCOM, ferma restando l'esigenza di assicurare un livello di sicurezza adeguato al rischio e il rispetto del principio di minimizzazione dei dati.

Che misure possono adottare concretamente le imprese in questo contesto normativo in rapida evoluzione?

In uno scenario regolatorio in rapida evoluzione, le imprese possono impostare fin da subito un

percorso di adeguamento articolato in più passaggi.

In primo luogo, è opportuno mappare i servizi che coinvolgono o sono accessibili ai minori, individuando le normative applicabili in ragione della tipologia di servizio e delle dimensioni dell'impresa.

In parallelo, occorre riesaminare le scelte di *design* dei propri prodotti, verificando che le interfacce e le funzionalità algoritmiche non incentivino comportamenti compulsivi né sfruttino le vulnerabilità cognitive dei più giovani.

Anche laddove non sussista un obbligo espresso di verifica dell'età, rappresenta buona prassi condurre un *risk assessment* dedicato alla presenza di minori tra gli utenti, così da valutare se sia opportuno adottare, in via anticipata, meccanismi di *age assurance* conformi al *framework* europeo, destinato a costituire progressivamente lo standard di riferimento. Un monitoraggio costante dell'iter del DDL 1136 e degli sviluppi applicativi delle Linee Guida e della

Raccomandazione consentirà, infine, di intercettare tempestivamente i nuovi obblighi e di calibrare gli interventi organizzativi, tecnici e contrattuali necessari.

Il quadro normativo complessivo – in atto e in divenire – restituisce un messaggio chiaro: la tutela dei minori nell'ambiente digitale non è più un adempimento formale né un tema affidato alle sole clausole d'uso, ma un vincolo di progettazione che attraversa l'intero ciclo di vita del servizio.

La sfida operativa per le imprese consiste nel ricondurre gli obblighi eterogenei che stanno prendendo forma a un presidio interno unitario – di *governance*, *risk management* e *product design* – coerente con il livello di rischio effettivamente generato dai propri prodotti per gli utenti più giovani.

* * *

Intelligenza artificiale generativa e protezione dei dati personali: il Garante Privacy sanziona Character.AI

Con provvedimento n. 487 del 3 luglio 2026, il Garante ha accertato l'illiceità di una serie di trattamenti effettuati da Character Technologies, Inc. ("**Character**"), società statunitense che offre Character.AI, un servizio di intelligenza artificiale generativa disponibile in Italia tramite app e piattaforma *web*.

Il servizio consente agli utenti di creare e interagire, via *chat*, con personaggi virtuali già esistenti o creati *ad hoc*. All'esito dell'istruttoria, l'Autorità ha irrogato alla società una sanzione amministrativa pecuniaria di 158.000 euro e le ha ingiunto di adottare una serie di misure correttive per rendere i trattamenti conformi al GDPR.

Il provvedimento è di particolare interesse in quanto affronta in modo organico diversi profili critici propri dei servizi di *generative AI*: dalla trasparenza delle informative privacy, alla base giuridica e all'utilizzo di dati personali per il pre-addestramento dei *large language models* ("**LLM**"), fino alla tutela dei minori e alla corretta impostazione della DPIA.

La trasparenza delle informative privacy nei servizi di IA

Una parte rilevante del provvedimento è dedicata all'esame dell'informativa privacy adottata dalla società e dei suoi successivi aggiornamenti.

Il Garante ha accertato numerose criticità relative alla trasparenza delle informazioni rese agli utenti, evidenziando, tra l'altro, l'assenza di una versione in lingua italiana per il periodo in cui il servizio era già offerto in Italia, l'indicazione poco chiara della facoltà degli interessati di esercitare il diritto di opposizione, la mancata indicazione del rappresentante nell'Unione europea, la presenza di imprecisioni linguistiche che rendono l'informativa non intellegibile, l'impiego di espressioni vaghe e probabilistiche nella descrizione dei periodi di conservazione e dei trasferimenti extra-UE, nonché l'indicazione di più basi giuridiche alternative per le medesime attività di trattamento, tale da risultare potenzialmente fuorviante per gli interessati.

Di particolare interesse è la valutazione dell'Autorità sull'approccio "multi base giuridica". Il Garante ha ribadito che la base giuridica deve essere unica per ciascun trattamento e chiaramente comunicata agli interessati, in quanto essa incide sui diritti loro riconosciuti dal GDPR: ad esempio, un trattamento per finalità di pubblicità personalizzata non può fondarsi contemporaneamente sul consenso e sul legittimo interesse, così come un trattamento per finalità di autenticazione non può essere alternativamente ricondotto alla base giuridica del contratto o al legittimo interesse.

L'esigenza di contemperare gli obblighi informativi di ordinamenti diversi non giustifica una simile pluralità, specie all'interno dell'informativa dedicata all'area SEE, ove trova applicazione un quadro normativo unico e armonizzato.

Il Garante ha inoltre valorizzato la necessità di correlare puntualmente ciascuna categoria di dati trattati alla specifica finalità, alla base giuridica e al periodo di conservazione.

L'ancoraggio dei tempi di conservazione a categorie generiche di finalità non è stato ritenuto conforme al dettato normativo, che impone l'indicazione precisa dei periodi di conservazione o, in mancanza, dei criteri utilizzati per determinarli.

Il trattamento dei dati per il pre-addestramento dei modelli

Il provvedimento affronta uno dei temi più discussi in materia di IA generativa, ossia gli obblighi di trasparenza riguardo ai dati personali utilizzati nella fase di sviluppo degli LLM.

Il Garante ha accertato la violazione dell'art. 14 del GDPR per non aver Character fornito un'adeguata informativa agli interessati italiani in relazione alle operazioni di trattamento finalizzate al pre-addestramento dei propri LLM proprietari.

L'Autorità ha inoltre respinto la tesi difensiva secondo cui la privacy policy pubblicata sul sito e gli aggiornamenti resi disponibili sul proprio *blog* e *forum* di terze parti (quali Reddit e Discord) potessero soddisfare l'obbligo informativo.

In particolare, il Garante ha rilevato che la privacy policy si rivolgeva unicamente agli utenti del servizio e riguardava esclusivamente la fase di post-addestramento, mentre gli aggiornamenti diffusi su piattaforme di terzi non consentono di dimostrare, nemmeno in ottica di *accountability*, l'effettiva conoscibilità delle informazioni da parte degli interessati.

Parimenti, il Garante ha respinto l'argomento secondo cui il pre-addestramento potrebbe aver

comportato un trattamento di dati personali incidentale e non intenzionale, essendo basato su *dataset* pubblicamente disponibili raccolti da terze parti: la verifica in ordine alla presenza di dati personali nei *dataset* di addestramento costituisce onere precipuo del titolare in virtù del principio di *accountability*, e la mera possibilità che tali dati fossero incidentalmente inclusi non esclude, ma anzi presuppone, l'obbligo di adottare le misure appropriate di trasparenza.

Il Garante ha invece ritenuto non integrata la contestata violazione relativa alla predisposizione di meccanismi *ad hoc* di *opt-out* preventivo: l'obbligo specifico di offrire agli interessati la possibilità di opporsi incondizionatamente al trattamento prima che questo abbia luogo, secondo l'Autorità, discende dal parere EDPB n. 28/2024[5] (adottato il 17 settembre 2024) e non può trovare applicazione retroattiva rispetto ad attività di pre-addestramento cessate anteriormente alla sua adozione.

Il principio è comunque destinato ad assumere rilievo per le attività di sviluppo dei modelli attualmente in corso o avviate in futuro. L'EDPB distingue, a questo riguardo, tra la fase di sviluppo del modello, che comprende le attività precedenti alla sua diffusione, incluse la raccolta e l'elaborazione dei dati di addestramento, e la successiva fase di diffusione.

Con riferimento alla fase di sviluppo, l'EDPB sottolinea l'opportunità di mettere a disposizione degli interessati, fin dall'inizio, strumenti che consentano loro di opporsi al trattamento. Tale indicazione riflette l'esigenza di adattare l'applicazione dei principi in materia di protezione dei dati alle specificità tecnologiche e operative dei sistemi di IA generativa.

La tutela dei minori: verifica dell'età e impostazioni predefinite

Uno dei profili di maggiore rilievo del provvedimento riguarda l'adeguatezza delle misure adottate dalla società per impedire l'accesso al servizio ai minori di sedici anni residenti nell'area SEE.

Nel corso dell'istruttoria, il Garante ha accertato che un utente italiano che aveva dichiarato di avere quindici anni era riuscito a completare la registrazione al servizio e che il relativo profilo risultava pubblico per impostazione predefinita.

Pur riconoscendo che il GDPR non impone specifiche misure di *age verification* e che, allo stato, manca uno *standard* europeo armonizzato in materia, l'Autorità ha ribadito che il titolare è comunque tenuto a adottare – e a dimostrare l'adeguatezza di – misure tecniche e organizzative proporzionate ai rischi.

La circostanza che il servizio, pur non espressamente rivolto a minorenni, presenti caratteristiche tali da renderlo attrattivo per soggetti particolarmente vulnerabili impone un elevato standard di diligenza, che nel caso di specie è mancato quantomeno nel periodo compreso tra l'8 aprile 2024 e l'8 aprile 2025.

L'Autorità ha valorizzato, altresì, il principio della *privacy by default* con riferimento all'impostazione dei profili degli utenti minorenni. Richiamando le linee guida EDPB in materia[6], il Garante ha ritenuto che l'impostazione predefinita del profilo di un minore come pubblico sia in radicale contrasto con l'obbligo di riservare a tali soggetti una tutela rafforzata, ordinando alla società di adottare, tra le misure

[5] Per maggiori approfondimenti sul tema, rinviamo al nostro precedente contributo "*Protezione dei dati personali nell'IA: il Parere dell'EDPB su anonimizzazione, interesse legittimo e conseguenze di un trattamento illecito*".

[6] EDPB, Linee Guida n. 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita.

correttive, la predisposizione dei profili dei minorenni in modalità privata *by default*.

La DPIA

Il Garante ha inoltre contestato la tardiva predisposizione della DPIA, rilevando come tale valutazione sia stata effettuata soltanto dopo l'avvio del servizio e a seguito dell'intervento dell'Autorità, anziché in via preventiva rispetto ai trattamenti effettuati.

L'Autorità ha ricordato [7] che la DPIA è obbligatoria per i trattamenti effettuati mediante tecnologie innovative – tra cui espressamente i sistemi di intelligenza artificiale – quando ricorra almeno un altro dei nove criteri individuati dal WP Art. 29 nelle proprie linee guida sulla DPIA (es., monitoraggio sistematico degli interessati, trattamenti di dati su larga scala, etc.)[8] .

Nel caso di specie il rischio elevato doveva ritenersi presunto in ragione della compresenza di più fattori: l'impiego di una tecnologia particolarmente innovativa come l'IA generativa, il trattamento di dati su larga scala per lo sviluppo degli LLM proprietari e il coinvolgimento di soggetti vulnerabili quali i minorenni.

Non è stato ritenuto sufficiente il richiamo generico a valutazioni interne, asseritamente condotte sin dal lancio del servizio: il principio di *accountability* impone la formalizzazione delle analisi svolte attraverso la predisposizione di una DPIA e non mediante non meglio precisate e documentate valutazioni interne aziendali.

La nomina del rappresentante nell'Unione europea

Il Garante ha inoltre contestato la tardiva designazione del rappresentante nell'Unione europea, rilevando come tale nomina sia intervenuta soltanto dopo che il servizio era già stato reso disponibile agli utenti dell'area SEE, e specificamente a quelli italiani.

L'Autorità ha respinto la tesi difensiva secondo cui l'attività di trattamento avrebbe avuto natura occasionale, rilevando come tale eccezione non possa applicarsi ai trattamenti connessi a un servizio stabilmente offerto in lingua italiana e destinati anche al pre-addestramento di LLM su larga scala.

Cosa dovrebbero fare le imprese che sviluppano o offrono sistemi di IA generativa

Il provvedimento del Garante offre indicazioni operative di rilievo per tutte le imprese che sviluppano o rendono disponibili al pubblico europeo sistemi di IA generativa, indipendentemente dalla loro dimensione.

In primo luogo, esso conferma la necessità di considerare gli obblighi in materia di protezione dei dati personali sin dalla fase di progettazione del servizio: la DPIA e le misure di *privacy by design* e *by default* non costituiscono adempimenti da posticipare al lancio

[7] Provvedimento n. 467 dell'11 ottobre 2018, doc. web. 9058979.

[8] In particolare, le linee guida individuano i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato": 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3) monitoraggio sistematico degli interessati; 4) dati sensibili o dati aventi carattere altamente personale; 5) trattamento di dati su larga scala; 6) creazione di corrispondenze o combinazione di insiemi di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9) quando il trattamento in sé impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

commerciale, ma condizioni imprescindibili per l'avvio stesso del trattamento.

In secondo luogo, il provvedimento evidenzia come la trasparenza nei confronti degli interessati richieda un elevato grado di precisione.

Le informative privacy dovrebbero associare puntualmente ogni categoria di dati alla specifica finalità, alla base giuridica e al periodo di conservazione, evitando formulazioni astratte, verbi probabilistici e l'indicazione plurima di basi giuridiche alternative per il medesimo trattamento.

Analoga attenzione va riservata alla traduzione dei testi nelle lingue dei mercati serviti, evitando terminologia impropria o suscettibile di generare fraintendimenti.

Con particolare riferimento al ciclo di vita dei modelli, le imprese dovrebbero distinguere chiaramente, nelle informative, tra fase di sviluppo e fase di diffusione, illustrando in modo specifico le operazioni di pre-addestramento e post-addestramento, le categorie di dati coinvolti e le modalità con cui gli interessati (utenti e non utenti) possono esercitare i propri diritti, compreso il diritto di opposizione nei modi indicati dall'EDPB nel parere n. 28/2024.

Ulteriore profilo di attenzione è rappresentato dalla tutela dei minori. Le imprese dovrebbero valutare, sulla base di un approccio fondato sul rischio, le misure di *age assurance* più adeguate al contesto del proprio servizio, verificarne periodicamente il corretto funzionamento e assicurare che le impostazioni predefinite del prodotto siano configurate in modo da minimizzare l'esposizione dei minori, in particolare con riferimento alla visibilità dei profili e dei contenuti generati.

Da ultimo, il provvedimento ribadisce la centralità degli adempimenti "strutturali" imposti dal GDPR ai titolari extra-UE, quali la tempestiva nomina del rappresentante e la predisposizione di canali di contatto pienamente funzionanti.

Si tratta di elementi che, benché talvolta percepiti come formali, rappresentano il presupposto operativo per l'effettivo esercizio dei diritti degli interessati e per l'interlocuzione con le autorità di controllo.

Nel complesso, il provvedimento conferma che le specificità tecnologiche dei servizi di IA generativa e l'evoluzione del relativo quadro giuridico non escludono l'applicazione dei principi fondamentali in materia di protezione dei dati personali.

Per le imprese, la sfida consiste nell'integrare tali principi fin dall'origine nelle scelte di prodotto, nei processi di *governance* e nelle attività di sviluppo tecnologico, evitando che gli adempimenti privacy siano affrontati soltanto dopo il lancio del servizio o l'intervento dell'autorità di controllo.

* * *

Piattaforme digitali e responsabilità: la decisione della CGUE sul caso Google/YouTube

La recente sentenza della Corte di giustizia dell'Unione europea ("**CGUE**" o la "**Corte**") nel caso Google/YouTube sposta in modo significativo il baricentro del dibattito sulla responsabilità dei prestatori di servizi digitali.

La questione riguarda la possibilità del gestore di una piattaforma *online* di essere qualificato come *hosting provider* "passivo", beneficiando dell'esenzione di responsabilità prevista dall'art. 14 della Direttiva 2000/31/CE ("**Direttiva e-Commerce**"), oppure come "attivo", con conseguente perdita di questo beneficio.

La Corte ha da sempre qualificato i provider come attivi o passivi guardando alla tecnologia impiegata dalla piattaforma: attività di indicizzazione, filtro, catalogazione, raccomandazione algoritmica (per un maggior approfondimento circa la differenza tra le due figure di *hosting provider*, rinviamo a un nostro precedente contributo, disponibile qui).

Oggi la Corte, applicando quei medesimi principi, chiarisce che, laddove tra la piattaforma e il *content creator* sia in essere un accordo commerciale, la qualifica potrebbe cambiare: ciò che sembrerebbe assumere rilievo non è più solo la modalità con cui la piattaforma processa i contenuti, ma anche la struttura del rapporto contrattuale con chi quei contenuti li carica.

Il caso

La vicenda trae origine da un provvedimento con cui, nel luglio 2022, l'AGCOM aveva irrogato a Google una sanzione amministrativa di 750.000 euro. L'Autorità aveva contestato la promozione, tramite alcuni canali della piattaforma YouTube, di numerosi siti di gioco d'azzardo *online*, in violazione del divieto di pubblicità sancito dall'art. 9 del D.L. 87/2018 (c.d. Decreto Dignità).

I canali sanzionati erano riconducibili a un unico *content creator*, che aveva aderito allo *YouTube Partner Program*, ossia al programma di *partnership* commerciale che consente ai *creator* di monetizzare i contenuti attraverso la condivisione dei ricavi pubblicitari.

In primo grado, il TAR Lazio aveva annullato la sanzione ritenendo che Google svolgesse il ruolo di mero prestatore di servizi di *hosting* e potesse beneficiare dell'esenzione della Direttiva e-Commerce.

In appello, il Consiglio di Stato ha sospeso il giudizio e sottoposto alla Corte di giustizia due questioni pregiudiziali: la prima sull'applicabilità della Direttiva e-Commerce all'attività di *hosting* di pubblicità di giochi d'azzardo; la seconda sulla possibilità di invocare l'esenzione con riferimento ai contenuti diffusi dai *creator* dei canali YouTube legato a Google da un accordo di *partnership* commerciale.

La decisione della Corte

Sul primo quesito, la Corte ha chiarito che l'attività di *hosting online* conserva la propria autonomia rispetto ai contenuti veicolati.

Ciò che il diritto dell'Unione esclude dal proprio ambito di applicazione, in forza dell'art. 1, par. 5, della Direttiva e-Commerce, è il gioco d'azzardo *online* in quanto tale (e la relativa pubblicità), ma non l'attività di chi si limita a

memorizzare e rendere accessibili contenuti che casualmente vertano su quel settore: l'attività di *hosting online* non è intrinsecamente connessa a tali giochi d'azzardo.

Al contrario, è un'attività in linea di principio neutra, che non presenta un nesso diretto con i giochi d'azzardo né è volta a promuoverli. Ne consegue che l'*hosting* di video contenenti pubblicità di giochi d'azzardo rientra pienamente nell'ambito di applicazione della Direttiva e-Commerce.

Sul secondo quesito, la risposta è di segno opposto: nel caso di specie l'esenzione non può essere invocata. La Corte ha valorizzato le peculiarità del rapporto tra Google e il *creator*, e in particolare le attività svolte da Google nell'ambito dello *YouTube Partner Program*.

Per ammettere un canale al programma, la piattaforma effettua una verifica preventiva – che può includere anche una revisione umana – del canale medesimo, esaminandone i temi trattati, i video più visti, i metadati e le sezioni informative.

Una volta ammesso, il canale genera ricavi pubblicitari che Google condivide con il *creator*, e consente agli utenti di sottoscrivere abbonamenti il cui corrispettivo è riscosso direttamente da Google.

Queste attività, ha affermato la Corte, non sono riconducibili a un intervento meramente tecnico e automatico: denotano un coinvolgimento della piattaforma nella gestione del rapporto commerciale con il *creator* e le conferiscono un livello di conoscenza e di controllo sui contenuti veicolati incompatibile con il requisito di neutralità.

Perché conta più il rapporto contrattuale che la tecnologia

Il precipitato più interessante della sentenza sta nel modo in cui la Corte utilizza i tradizionali "indici di interferenza" elaborati dalla giurisprudenza (filtro, indicizzazione, catalogazione, promozione dei contenuti) per individuare la figura dell'*hosting provider* attivo.

Nel caso di specie la CGUE non si limita a valutare la presenza o l'assenza di uno di questi elementi tecnici. Guarda al contratto. E rileva che è il rapporto di *partnership* – con la valutazione preventiva del canale, la condivisione dei ricavi, la riscossione degli abbonamenti – a rendere la piattaforma qualcosa di più di un mero fornitore di un'infrastruttura tecnica.

In altri termini, esaminando i canali YouTube, Google non poteva ragionevolmente ignorare che gli stessi avevano come tema principale i giochi d'azzardo e la loro pubblicità, in violazione dell'art. 9 del Decreto Dignità.

La pronuncia alla luce del DSA

La sentenza è stata resa con riferimento alla Direttiva e-Commerce, ma la sua rilevanza pratica va misurata sull'assetto del Regolamento (UE) 2022/2065 (*Digital Services Act* – "**DSA**"), che ne ha ereditato l'impianto del *safe harbour*.

L'art. 6 del DSA riproduce sostanzialmente l'art. 14 della Direttiva e-Commerce; il Considerando 18 codifica espressamente il test dell'"attivo/passivo" che la Corte ha applicato nella sentenza, prevedendo che l'esenzione non si applichi quando il prestatore, invece di limitarsi a fornire i servizi in modo neutrale mediante un trattamento meramente tecnico e automatico delle informazioni, svolga un ruolo attivo di natura tale da conferirgli conoscenza o controllo sulle informazioni medesime.

Merita una menzione anche l'art. 7 del DSA, che codifica la c.d. clausola del "buon samaritano": le attività volontarie di rilevazione e rimozione di contenuti illeciti, svolte in buona fede e in modo diligente, non fanno perdere il beneficio dell'esenzione di responsabilità.

Nel caso di specie, la Corte non fonda l'esclusione sull'esercizio di attività di moderazione (che non sarebbe, di per sé, un elemento in grado di produrre quell'effetto), bensì sul rapporto contrattuale tra le parti.

Ne consegue che la pronuncia non entra in tensione con l'art. 7 del DSA e che, anzi, ne conferma indirettamente la portata: le piattaforme possono e devono investire in strumenti di *content moderation* senza che questo, in sé, comporti la perdita del *safe harbour*.

Va infine ricordato che Google e YouTube sono state designate dalla Commissione europea quale *Very Large Online Platform* e sono pertanto soggette agli obblighi rafforzati in materia di gestione dei rischi sistemici, *audit* indipendenti e trasparenza previsti dal DSA.

Considerazioni conclusive

Ridotta all'essenziale, la sentenza della CGUE opera una distinzione concettuale che merita di essere colta nella sua portata più ampia. La responsabilità del prestatore di servizi digitali non viene fatta discendere, di per sé, dalle scelte tecnologiche o di prodotto della piattaforma, ossia dal fatto che essa indicizzi, ordini, suggerisca, filtri o moderi i contenuti che ospita.

Discenderebbe piuttosto dalla decisione economica di trasformare lo spazio di *hosting* in un'infrastruttura di *business* condiviso con i produttori dei contenuti stessi. Il *creator* legato alla piattaforma da un accordo commerciale non è un utente qualunque, e la piattaforma che lo remunera non è più un intermediario qualunque.

Sul piano pratico, si delineano due fasce di rapporti destinati a convivere nella stessa piattaforma con regole di responsabilità differenti: da un lato l'insieme degli utenti che caricano contenuti nell'anonimato dei termini di servizio *standard*; dall'altro, la fascia più ristretta ma economicamente decisiva dei *creator* con cui la piattaforma stringe accordi di *partnership* commerciale.

Sarebbe un errore, tuttavia, leggere la pronuncia come una condanna del modello di monetizzazione condivisa. La Corte non ha vietato la *partnership* tra piattaforma e *content creator*, né ha imposto un obbligo generale di sorveglianza sui contenuti, che l'art. 8 del DSA continua espressamente a escludere.

Ha affermato, più semplicemente, che quando la piattaforma sceglie di trasformare un utente in un *partner* commerciale, rischia poi di non potersi presentare come un intermediario neutro rispetto ai contenuti oggetto di quel rapporto.

* * *

Trasparenza retributiva e protezione dei dati personali: gli impatti *privacy* del D.Lgs. 96/2026

Lo scorso 7 giugno 2026 è entrato in vigore il D.Lgs. 96/2026 (il "**Decreto**"), che ha dato attuazione nel nostro ordinamento alla Direttiva (UE) 2023/970 sulla trasparenza retributiva e sul rafforzamento del principio della parità di retribuzione tra uomini e donne per uno stesso lavoro o per un lavoro di pari valore.

La nuova disciplina introduce una serie di obblighi destinati a incidere sia sulla fase di selezione del personale sia sul rapporto di lavoro già in essere.

Da un lato, riconosce ai candidati il diritto di ricevere informazioni sulla retribuzione iniziale o sulla relativa fascia retributiva prima dell'assunzione e vieta ai datori di lavoro di acquisire informazioni sulla storia retributiva dei candidati.

Dall'altro, attribuisce ai lavoratori il diritto di ottenere, entro due mesi dalla richiesta, informazioni sui livelli retributivi medi, distinti per sesso, dei lavoratori che svolgono lo stesso lavoro o un lavoro di pari valore, nonché sui criteri utilizzati per determinare la progressione economica[9].

Il Decreto non soltanto rileva da un punto di vista giuslavoristico, ma anche sotto il profilo della protezione dei dati personali. La nuova disciplina, infatti, comporta un significativo ampliamento delle occasioni in cui le informazioni retributive devono essere raccolte, elaborate e comunicate, rendendo necessario verificare che tali trattamenti siano conformi ai principi del GDPR.

Le informazioni retributive come dati personali

Le informazioni relative alla retribuzione, ai livelli retributivi e ai criteri di progressione economica costituiscono dati personali quando consentono di identificare, direttamente o indirettamente, a un lavoratore.

Sotto questo profilo, il Decreto ribadisce che le informazioni sui livelli retributivi e quelle relative al divario retributivo di genere, ove comportino il trattamento di dati personali, devono essere trattate nel rispetto del GDPR e non possono essere utilizzate per finalità diverse da quelle connesse all'attuazione del principio della parità di retribuzione.

La vera novità, tuttavia, non riguarda la natura del dato retributivo – già qualificabile come dato personale prima dell'entrata in vigore del Decreto – quanto piuttosto la crescente circolazione di tali informazioni all'interno dell'organizzazione aziendale.

L'esercizio dei nuovi diritti riconosciuti ai lavoratori e gli obblighi di rendicontazione imposti alle imprese comportano infatti un aumento dei trattamenti di dati retributivi, rendendo necessario definire procedure idonee a garantire l'esattezza delle informazioni comunicate e a limitare il rischio di accessi o divulgazioni non autorizzate.

[9] I datori di lavoro che impiegano meno di 50 dipendenti non sono tenuti a rendere disponibili i criteri per la progressione economica.

Il rischio di identificazione del lavoratore

Uno dei profili più delicati riguarda il rischio che le informazioni comunicate consentano di risalire, anche indirettamente, alla retribuzione di uno specifico lavoratore.

Per tale ragione, il Decreto prevede che, quando la divulgazione delle informazioni retributive possa rendere identificabile un singolo dipendente, l'accesso sia riservato esclusivamente ai rappresentanti dei lavoratori, all'Ispettorato nazionale del lavoro e agli organismi di parità territorialmente competenti.

Tali soggetti possono assistere i lavoratori nell'esercizio dei diritti riconosciuti dal Decreto, senza tuttavia divulgare i livelli retributivi individuali.

Si tratta di una previsione che richiede un'attenta valutazione caso per caso. Il rischio di identificazione, infatti, non dipende esclusivamente dal dato comunicato, ma anche dal contesto organizzativo dell'impresa. In aziende di piccole dimensioni, oppure in reparti caratterizzati dalla presenza di poche figure altamente specializzate, anche informazioni aggregate potrebbero consentire di individuare con relativa facilità il trattamento economico di uno specifico dipendente.

Per questo motivo, le imprese dovrebbero definire procedure interne che disciplinino la gestione di simili richieste da parte dei lavoratori, individuando i soggetti autorizzati a fornire le informazioni e prevedendo verifiche preventive volte a escludere il rischio di identificazione indiretta dei lavoratori.

I processi di selezione del personale

Le novità introdotte dal Decreto riguardano anche la fase di *recruiting*. I candidati dovranno ricevere informazioni sulla retribuzione iniziale o sulla relativa fascia retributiva e sulle disposizioni del CCNL applicabile già nell'annuncio di lavoro o, comunque, prima dello svolgimento del colloquio.

Parallelamente, il datore di lavoro non potrà richiedere informazioni sulle retribuzioni percepite in precedenza, né acquisirle indirettamente tramite soggetti terzi.

Dal punto di vista della protezione dei dati personali, tali obblighi impongono di riesaminare l'intero processo di selezione.

Non sarà sufficiente eliminare eventuali domande dai moduli di candidatura: occorrerà verificare anche le prassi adottate durante i colloqui e le istruzioni fornite alle società di *recruiting*, affinché non vengano raccolte informazioni che la normativa non consente più di acquisire.

Le imprese che si avvalgono di *recruiter* esterni dovrebbero inoltre verificare che gli accordi contrattuali e le istruzioni impartite ai responsabili del trattamento siano coerenti con le nuove prescrizioni.

Gli obblighi di rendicontazione sul *gender pay gap*

Il Decreto introduce inoltre specifici obblighi di comunicazione relativi al divario retributivo di genere[10], destinati ad applicarsi gradualmente in funzione delle dimensioni dell'impresa.

[10] In particolare, i datori di lavoro dovranno comunicare all'organismo di monitoraggio (istituito presso il MLPS) le seguenti tipologia di dati: il divario retributivo di genere; il divario retributivo di genere nelle componenti complementari o variabili; il divario retributivo mediano di genere; il divario retributivo mediano di genere nelle componenti complementari o variabili; la percentuale di lavoratori di sesso femminile e di quelli di sesso maschile che ricevono componenti complementari o variabili; la percentuale di lavoratori di sesso femminile e di quelli di sesso maschile in ogni quartile retributivo; il divario

Per le imprese con almeno 250 dipendenti, i dati dovranno essere raccolti entro il 7 giugno 2027 e successivamente con cadenza annuale.

Le imprese che occupano tra 150 e 249 dipendenti dovranno effettuare la prima comunicazione entro la stessa data e, successivamente, ogni tre anni. Per le imprese con un numero di dipendenti compreso tra 100 e 149 lavoratori, il primo adempimento decorrerà invece dal 7 giugno 2031, con cadenza triennale.

Le imprese con meno di 100 dipendenti potranno effettuare la comunicazione su base volontaria, salvo che la normativa nazionale disponga diversamente.
Sotto il profilo operativo, la predisposizione di tali informazioni non rappresenta un mero adempimento formale.

La qualità e l'affidabilità dei dati presuppongono infatti la definizione di criteri coerenti per individuare i lavoratori che svolgono lo stesso lavoro o un lavoro di pari valore, nonché un efficace coordinamento tra le funzioni HR, legale, privacy e, ove necessario, i responsabili dei sistemi informativi.

Cosa dovrebbero fare le imprese

L'adeguamento al Decreto richiede una revisione dei processi attraverso i quali vengono gestite le informazioni retributive. In particolare, le imprese dovrebbero verificare che il registro dei trattamenti, le informative privacy rivolte a dipendenti e candidati e le istruzioni ai soggetti autorizzati riflettano i nuovi flussi di dati previsti dalla disciplina.

Analoga attenzione dovrebbe essere riservata ai rapporti con eventuali fornitori che trattano dati retributivi in qualità di responsabili del trattamento, verificando che gli accordi in essere siano adeguati alle nuove modalità di trattamento.

Sarà inoltre opportuno predisporre procedure interne per la gestione delle richieste presentate dai lavoratori, individuando le funzioni competenti, definendo modalità uniformi di risposta e introducendo controlli idonei a evitare comunicazioni che possano determinare l'identificazione indiretta dei dipendenti.

Nel complesso, il Decreto rappresenta un'occasione per ripensare la *governance* delle informazioni retributive. Se fino ad oggi tali dati erano prevalentemente confinati nell'ambito amministrativo e *payroll*, la nuova disciplina li pone al centro di un sistema di trasparenza che coinvolge HR, uffici legali, funzioni privacy e *management*.

Proprio per questo, la conformità al GDPR non costituisce un adempimento accessorio rispetto alla disciplina sulla trasparenza retributiva, ma una condizione essenziale per la sua corretta attuazione.

retributivo di genere tra lavoratori per categorie di lavoratori ripartito in base al salario o allo stipendio normale di base e alle componenti complementari o variabili.

Per maggiori informazioni e approfondimenti

Carlo Impalà

Partner e Responsabile Osservatorio TMT&DP

Carlo.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