FIVERS

Aggiornamento
Data protection, AI, IT and IP

n. 12 / 2024

DATA PROTECTION.

9 Ottobre 2024 – Comitato europeo per la protezione dei dati personali: adottate le Linee Guida sul trattamento dei dati personali basato sul legittimo interesse.

---

9 Ottobre 2024 – Comitato europeo per la protezione dei dati personali: adottato un parere sull'articolo 28 del GDPR e su taluni obblighi derivanti dalla designazione del Responsabile esterno del trattamento (e dei sub-responsabili).

---

9 Ottobre 2024 – Comitato europeo per la protezione dei dati personali: il diritto alla cancellazione ("diritto all'oblio") sarà il tema della quarta azione coordinata di esecuzione (CEF).

---

4 Ottobre 2024 – Corte di Giustizia UE: Un social network online come Facebook non può utilizzare l'insieme dei dati personali ottenuti a fini di pubblicità mirata, senza limitazione temporale e senza distinzione basata sulla natura di tali dati.

---

4 Ottobre 2024 – Corte di Giustizia UE: gli Stati membri possono prevedere la possibilità, per i concorrenti del presunto autore di una violazione della protezione dei dati personali, di contestarla in giudizio in quanto pratica commerciale sleale vietata.

---

4 Ottobre 2024 – Corte di Giustizia UE: i limiti del legittimo interesse quale base di legittimità del trattamento che persegue scopi marketing e di natura commerciale.

---

4 Ottobre 2024 – Corte di Giustizia UE: condizioni per esercitare il diritto di cancellare i dati personali dal Registro delle Imprese detenuto da uno Stato Membro e per richiedere il risarcimento del danno morale in caso di diniego.

4 Ottobre 2024 – Corte di Giustizia UE: il risarcimento dei danni non patrimoniali ai sensi del GDPR.

INTELLIGENZA ARTIFICIALE.

14 Ottobre 2024 – Consiglio UE: approvata in via definitiva la direttiva sui lavoratori delle piattaforme digitali.

11 Ottobre 2024 – G7 delle Autorità garanti per la protezione dei dati personali: ruolo delle DPA nella regolamentazione dell'Intelligenza Artificiale.

MERCATI DIGITALI

10 Ottobre 2024 – Consiglio UE: definitivamente approvato il *Cyber Resilience Act* (CRA) che prevede nuovi requisiti di sicurezza per i prodotti digitali.

10 Ottobre 2024 – Pubblicato nella Gazzetta Ufficiale il decreto legislativo 7 Ottobre 2024, n. 144 di armonizzazione della normativa nazionale con il Regolamento UE 2022/868 sulla governance europea dei dati (Data Governance Act – DGA).

9 Ottobre 2024 – European Banking Authority: Linee Guida per gli emittenti di token di riferimento di asset (ART) e di token di moneta elettronica (EMT) per garantire un riscatto ordinato e tempestivo dei token in caso di incapacità dell'emittente di adempiere ai propri obblighi.

INFORMATION TECHNOLOGY

8 Ottobre 2024 – Agenzia delle Entrate: provvedimento n. 379575/2024 sulle modalità di comunicazione, variazione e revoca dei dati relativi al domicilio digitale speciale e per confermare o revocare l'indirizzo PEC.

2 Ottobre 2024 – Il 16 ottobre entra in vigore il D.lgs. n. 138/2024, di recepimento della Direttiva (UE) 2022/2555 NIS 2 su un livello comune di cybersicurezza nella UE.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

10 Ottobre 2024 – Le misure IP nel Decreto Omnibus, convertito in legge 143/2024.

DATA PROTECTION

9 Ottobre 2024 – Comitato europeo per la protezione dei dati personali: adottate le Linee Guida sul trattamento dei dati personali basato sul legittimo interesse.

I titolari del trattamento dei dati hanno bisogno di una base giuridica per trattare i dati personali in modo lecito. L'interesse legittimo è una delle sei possibili basi giuridiche.

Le Linee guida analizzano i criteri di cui all'articolo 6, paragrafo 1, lettera f) del GDPR che i titolari del trattamento devono soddisfare per trattare lecitamente i dati personali sulla base di un interesse legittimo. Prende inoltre in considerazione la recente sentenza della Corte di giustizia in materia (C-621/22 del 4 ottobre 2024).

Per poter fare affidamento sul legittimo interesse, il titolare del trattamento deve soddisfare tre condizioni cumulative:

- il perseguimento di un legittimo interesse da parte del titolare del trattamento o di un terzo;
- la necessità di trattare i dati personali ai fini del perseguimento del legittimo interesse;
- gli interessi o le libertà e i diritti fondamentali delle persone fisiche non prevalgono sull'interesse legittimo del titolare del trattamento o di un terzo (ponderazione).

Innanzitutto, possono essere considerati legittimi solo gli interessi legittimi, articolati in modo chiaro e preciso, reali e presenti. Ad esempio, tali interessi legittimi potrebbero esistere in una situazione in cui l'individuo è un cliente o al servizio del titolare del trattamento.

In secondo luogo, se esistono alternative ragionevoli, altrettanto efficaci, ma meno invasive per raggiungere gli interessi perseguiti, il trattamento può non essere considerato necessario. Anche la necessità di un trattamento dovrebbe essere esaminata con il principio della minimizzazione dei dati.

In terzo luogo, il titolare del trattamento deve garantire che sul suo legittimo interesse non prevalgano gli interessi, i diritti o le libertà fondamentali dell'individuo. In questo esercizio di bilanciamento, il titolare del trattamento deve tenere conto degli interessi delle persone, dell'impatto del trattamento e delle loro ragionevoli aspettative, nonché dell'esistenza di garanzie aggiuntive che potrebbero limitare l'impatto sulla persona.

Inoltre, i presenti orientamenti spiegano in che modo tale valutazione dovrebbe essere effettuata nella pratica, anche in una serie di contesti specifici quali la prevenzione delle frodi, il marketing diretto e la sicurezza delle informazioni. Il documento spiega anche il rapporto tra questa base giuridica e una serie di diritti degli interessati ai sensi del GDPR.

Gli orientamenti saranno oggetto di consultazione pubblica fino al 20 novembre 2024.

---

9 Ottobre 2024 – Comitato europeo per la protezione dei dati personali: adottato un parere sull'articolo 28 del GDPR e su taluni obblighi derivanti dalla designazione del Responsabile esterno del trattamento (e dei sub-responsabili).

L'articolo 64, paragrafo 2, del GDPR prevede che qualsiasi autorità di protezione dei dati possa chiedere al Comitato di emettere un parere su questioni di applicazione generale o che producono effetti in più di uno Stato membro. A seguito di una richiesta ai sensi dell'articolo 64, paragrafo 2, del GDPR al Comitato europeo per la protezione dei dati personali da parte dell'Autorità danese per la protezione dei dati (DPA), il Comitato (EDPB) ha rilasciato un parere che riguarda le situazioni in cui i titolari del trattamento si affidano a uno o più responsabili del trattamento e sub-responsabili del trattamento.

In particolare, il parere affronta otto questioni relative all'interpretazione di taluni obblighi dei titolari del trattamento che si avvalgono di responsabili del trattamento e sub-responsabili del trattamento, nonché fornisce chiarimenti in merito alla formulazione dei contratti tra titolare del trattamento e responsabile del trattamento, ai sensi dall'articolo 28 del RGPD.

Il parere spiega che i titolari del trattamento dovrebbero avere a disposizione in qualsiasi momento le informazioni sull'identità (ad esempio nome, indirizzo, persona di contatto) di tutti i responsabili del trattamento, sub-responsabili ecc., in modo che possano adempiere al meglio ai loro obblighi ai sensi dell'articolo 28 del GDPR. Inoltre, l'obbligo del titolare del trattamento di verificare se i (sub)responsabili del trattamento presentino «garanzie sufficienti» dovrebbe applicarsi indipendentemente dal rischio per i diritti e le libertà degli interessati, sebbene la portata di tale verifica possa variare, in particolare sulla base dei rischi associati al trattamento.

Il parere afferma inoltre che, sebbene il responsabile del trattamento iniziale debba assicurarsi di proporre sub-responsabili del trattamento con sufficienti garanzie, la decisione finale e la responsabilità di incaricare uno specifico sub-responsabile del trattamento spettano al titolare del trattamento.

L'EDPB ritiene che, ai sensi del GDPR, il titolare del trattamento non abbia l'obbligo di richiedere sistematicamente i contratti di sub-trattamento per verificare se gli obblighi di protezione dei dati sono stati trasmessi lungo la catena di trattamento. Il titolare del trattamento dovrebbe valutare se la richiesta di una copia di tali contratti o la loro revisione sia necessaria per poter dimostrare la conformità al regolamento generale sulla protezione dei dati.

Inoltre, qualora i trasferimenti di dati personali al di fuori dello Spazio economico europeo avvengano tra due (sub)responsabili del trattamento, il responsabile del trattamento in qualità di esportatore dei dati dovrebbe preparare la documentazione pertinente, ad esempio relativa al motivo del trasferimento utilizzato, alla valutazione d'impatto del trasferimento e alle eventuali misure supplementari. Tuttavia, poiché il titolare del trattamento è ancora soggetto agli obblighi derivanti dall'articolo 28, paragrafo 1, del GDPR sulle "garanzie sufficienti", oltre a quelli di cui all'articolo 44 per assicurare che il livello di protezione non sia compromesso dai trasferimenti di dati personali, dovrebbe valutare tale documentazione ed essere in grado di mostrarla all'Autorità per la protezione dei dati personali competente.

---

9 Ottobre 2024 – Comitato europeo per la protezione dei dati personali: il diritto alla cancellazione ("diritto all'oblio") sarà il tema della quarta azione coordinata di esecuzione (CEF).

Il Comitato europeo per la protezione dei dati (EDPB) ha selezionato l'argomento per la sua quarta azione coordinata di esecuzione (CEF), che riguarderà l'attuazione del diritto alla cancellazione ("diritto all'oblio") da parte dei titolari del trattamento. L'azione sarà avviata nel corso del primo semestre del 2025.

Il diritto alla cancellazione (art. 17 GDPR) è uno dei diritti di protezione dei dati più frequentemente esercitati e uno dei diritti in merito ai quali le autorità di protezione dei dati ricevono frequentemente reclami. L'obiettivo di questa azione coordinata sarà, tra l'altro, quello di valutare l'attuazione pratica di tale diritto. Ad esempio, ciò avverrà analizzando e confrontando i processi messi in atto dai diversi titolari del trattamento per identificare le questioni più importanti per il rispetto di questo diritto, ma anche per ottenere una panoramica delle migliori pratiche.

Nell'ambito di un'azione coordinata di contrasto, l'EDPB dà priorità a un tema specifico su cui le autorità di protezione dei dati devono lavorare a livello nazionale. Negli ultimi tre anni, le autorità di protezione dei dati hanno già coordinato le loro azioni nazionali su diversi temi, vale a dire: l'uso del cloud nel settore pubblico, la designazione e la posizione dei responsabili della protezione dei dati e l'attuazione del diritto di accesso da parte dei titolari del trattamento.

I risultati di queste azioni nazionali vengono quindi aggregati e analizzati insieme per ottenere una visione più approfondita dell'argomento e consentire un follow-up mirato sia a livello nazionale che a livello dell'UE.

Nel 2023 l'EDPB ha pubblicato la relazione sulla sua prima azione coordinata sull'uso dei servizi basati su cloud da parte del settore pubblico. All'inizio di quest'anno, l'EDPB ha anche pubblicato la relazione sui risultati della seconda azione coordinata sulla designazione e la posizione dei responsabili della protezione dei dati.

La relazione sui risultati dell'azione coordinata 2024 sul diritto di accesso sarà adottata all'inizio del 2025. Le azioni coordinate fanno seguito alla decisione dell'EDPB di istituire un quadro coordinato per l'applicazione delle norme (MCE) nell'ottobre 2020. L'MCE è un'azione chiave dell'EDPB nell'ambito della sua strategia 2024-2027, insieme al pool di esperti di sostegno. Le due iniziative mirano a semplificare l'applicazione e la cooperazione tra le autorità di protezione dei dati.

---

4 Ottobre 2024 – Corte di Giustizia UE: Un social network online come Facebook non può utilizzare l'insieme dei dati personali ottenuti a fini di pubblicità mirata, senza limitazione temporale e senza distinzione basata sulla natura di tali dati.

Maximilian Schrems – noto per le sue battaglie e cause avanti ai tribunali UE e alla Corte di Giustizia – ha contestato dinanzi ai giudici austriaci il trattamento, a suo avviso illecito, dei suoi dati personali da parte della Meta Platforms Ireland nell'ambito del social network online Facebook. Si è trattato, tra l'altro, di dati relativi al suo orientamento sessuale.

La Meta Platforms raccoglie dati personali degli utenti di Facebook, tra i quali Maximilian Schrems, relativi alle attività di questi utenti tanto su tale social network che al di fuori di esso. Si tratta, in particolare, di dati relativi alla consultazione della piattaforma online nonché di pagine internet e di applicazioni di terzi. A tal fine, la Meta Platforms utilizza "cookie", "social plugin" e "pixel" inseriti sulle pagine Internet interessate. Visti i dati a sua disposizione, la Meta Platforms può anche individuare l'interesse che Maximilian Schrems manifesta relativamente a temi sensibili, come l'orientamento sessuale, e ciò le consente di rivolgergli della pubblicità mirata al riguardo. Si pone pertanto la questione se Maximilian Schrems abbia manifestamente reso pubblici dati personali sensibili che lo riguardano, avendo comunicato in occasione di una tavola rotonda pubblica il fatto di essere omosessuale, e ne abbia quindi autorizzato il trattamento, in forza del regolamento generale sulla protezione dei dati (RGPD).

In tale contesto, la Corte suprema austriaca ha chiesto alla Corte di giustizia di interpretare il GDPR.

In primo luogo, la Corte risponde che il principio della «minimizzazione dei dati», stabilito dal GDPR, osta a che l'insieme dei dati personali che un Titolare del trattamento, come il gestore di una piattaforma di social network online, abbia ottenuto dall'interessato o da terzi e che siano stati raccolti sia su tale piattaforma che al di fuori di essa, siano aggregati, analizzati ed elaborati ai fini di pubblicità mirata, senza limitazione temporale e senza distinzione basata sulla natura di tali dati.

In secondo luogo, secondo la Corte, non è escluso che, con la sua dichiarazione in occasione della tavola rotonda in questione, Maximilian Schrems abbia manifestamente reso pubblico il suo orientamento sessuale. Spetta alla Corte suprema austriaca verificarlo. Il fatto che una persona abbia reso manifestamente pubblico un dato riguardante il suo orientamento sessuale comporta che tale dato possa essere oggetto di trattamento, nel rispetto delle disposizioni del GDPR. Tuttavia, tale circostanza non autorizza, di per sé, il trattamento di altri dati personali relativi all'orientamento sessuale di tale persona.

Pertanto, la circostanza che una persona si sia espressa sul suo orientamento sessuale in occasione di una tavola rotonda pubblica non autorizza il gestore di una piattaforma di social network online a trattare altri dati relativi all'orientamento sessuale di tale persona ottenuti, se del caso, al di fuori di tale piattaforma a partire da applicazioni e siti Internet di partner terzi, ai fini di aggregarli e analizzarli per proporre a tale persona della pubblicità personalizzata.

---

4 Ottobre 2024 – Corte di Giustizia UE: gli Stati membri possono prevedere la possibilità, per i concorrenti del presunto autore di una violazione della protezione dei dati personali, di contestarla in giudizio in quanto pratica commerciale sleale vietata.

La Corte federale di giustizia tedesca è chiamata a risolvere una controversia tra due farmacisti tedeschi. Il farmacista titolare della farmacia «Lindenapotheke» commercializza su Amazon, dal 2017, medicinali la cui vendita è riservata alle farmacie. I clienti devono inserire diverse informazioni all'atto dell'ordine online di tali medicinali.

Basandosi sulla normativa tedesca in materia di pratiche commerciali sleali, un farmacista concorrente ha chiesto alla giustizia tedesca di ordinare al titolare della Lindenapotheke di cessare tale attività finché non sia garantito che i clienti possano dare il loro consenso preventivo al trattamento di dati relativi alla salute.

I tribunali di primo e secondo grado hanno ritenuto che tale commercializzazione costituisse effettivamente una pratica sleale e illecita, in quanto contraria al regolamento sulla protezione dei dati personali (RGPD). Infatti, in assenza di un consenso esplicito da parte dei clienti che acquistano medicinali, la vendita comporterebbe il trattamento di dati relativi alla salute, vietato ai sensi di tale regolamento.

La Corte federale di giustizia tedesca si chiede

(a) se la normativa nazionale, che consente a un concorrente di agire in giudizio contro il presunto autore delle violazioni del RGPD sulla base del divieto delle pratiche commerciali sleali, sia conforme a tale regolamento. Infatti, secondo il RGPD, in linea di principio spetta alle autorità nazionali di controllo sorvegliare e far applicare tale regolamento e agli interessati (in questo caso, i clienti) difendere i loro diritti;

(b) se le informazioni inserite in occasione degli acquisti online di medicinali la cui vendita è riservata alle farmacie costituiscano dati relativi alla salute ai sensi del RGPD, anche nel caso in cui tali medicinali non siano soggetti a prescrizione medica. Si è quindi rivolta alla Corte di giustizia.

La Corte risponde, in primo luogo, che il RGPD non osta a una normativa nazionale che, al di là dei diritti e dei poteri conferiti dal RGPD alle autorità nazionali di controllo, agli interessati e alle associazioni che rappresentano tali persone, consenta ai concorrenti del presunto autore di una violazione della protezione dei dati personali di agire in giudizio nei suoi confronti, per violazioni di tale regolamento, sulla base del divieto delle pratiche commerciali sleali. Al contrario, ciò contribuisce indubbiamente a rafforzare i diritti degli interessati e a garantire loro un elevato livello di protezione. Inoltre, ciò può rivelarsi particolarmente efficace, in quanto si potrebbero, in tal modo, prevenire un gran numero di violazioni del RGPD.

In secondo luogo, per la Corte costituiscono dati relativi alla salute ai sensi del RGPD le informazioni inserite dai clienti (quali il loro nome, l'indirizzo di consegna e gli elementi necessari all'individuazione dei medicinali) al momento dell'ordine online dei medicinali riservati alle farmacie, anche qualora la vendita di questi ultimi non sia soggetta a prescrizione medica. Infatti, tali dati sono idonei a rivelare, mediante un'operazione intellettuale di raffronto o di deduzione, informazioni sullo stato di salute di una persona fisica identificata o identificabile, perché viene stabilito un nesso tra quest'ultima e un medicinale, le sue indicazioni terapeutiche o i suoi usi, indipendentemente dal fatto che tali informazioni riguardino il cliente o qualsiasi altra persona per la quale quest'ultimo effettui l'ordine. Pertanto, è indifferente che, in mancanza di prescrizione medica, sia solo con una certa probabilità, e non con certezza assoluta, che tali medicinali siano destinati ai clienti che li hanno ordinati. Distinguere in base al tipo di medicinali e al fatto che la loro vendita sia o meno soggetta a prescrizione medica sarebbe contrario all'obiettivo di protezione elevata previsto dal RGPD. Di conseguenza, il venditore deve informare tali clienti in modo accurato, completo e facilmente comprensibile in merito alle caratteristiche e alle finalità specifiche del trattamento di tali dati e chiedere il loro consenso esplicito a tale trattamento.

---

4 Ottobre 2024 – Corte di Giustizia UE: i limiti del legittimo interesse quale base di legittimità del trattamento che persegue scopi marketing e di natura commerciale.

Un’associazione di club di tennis olandese ha comunicato i dati dei propri tesserati, senza il loro consenso, a terze parti esterne (taluni sponsor), tra cui una società che commercializza prodotti sportivi, nonché alla "*Nederlandse Loterij Organisatie BV*", la più grande società di giochi d’azzardo e di *casinò games* nei Paesi Bassi. Quest’ultima, ha versato all’associazione un corrispettivo per la messa a disposizione dei dati personali dei tesserati (nomi, indirizzi, date di nascita, recapiti telefonici di telefono fisso e cellulare, e-mail). Questi dati sono poi stati utilizzati per una campagna di chiamate promozionali da parte dei call center di cui si è avvalsa la società di giochi d’azzardo.

A seguito della sanzione comminata dal Garante olandese all’associazione sportiva, quest’ultima ha impugnato il provvedimento, sostenendo la liceità del trattamento sulla base del legittimo interesse ai sensi dell’articolo 6, comma 1, lettera (f) del GDPR.

I giudici si sono dunque rivolti alla Corte di Giustizia chiedendo in che modo l'espressione "legittimo interesse" di cui all'articolo 6, paragrafo 1, primo comma, lettera f), del GDPR debba essere interpretata, e in particolare se per "interesse legittimo" debba intendersi esclusivamente un interesse sancito e determinato da una legge, considerato meritevole di tutela dal legislatore dell'Unione o dal legislatore nazionale, oppure se il legittimo interesse non deve necessariamente derivare da un diritto fondamentale o da un principio giuridico, ma qualsiasi interesse può costituire un legittimo interesse, salvo che esso sia contrario alla legge, e che tale interesse deve essere quindi valutato secondo un «criterio negativo».

I giudici olandesi chiedono in particolare se un interesse strettamente commerciale e l'interesse come quello in oggetto, ossia la fornitura di dati personali dietro pagamento senza consenso dell'interessato, in talune circostanze possa essere considerato *legittimo interesse.* In caso affermativo, quali circostanze determinano se un interesse strettamente commerciale sia un legittimo interesse.

La Corte UE ha chiarito che un trattamento di dati personali consistente nella comunicazione a titolo oneroso di dati personali dei membri di una federazione sportiva, al fine di soddisfare un interesse commerciale del titolare del trattamento (cioè l'associazione che trasmette i dati), può essere considerato necessario ai fini del legittimo interesse perseguito da tale titolare solo a condizione che tale trattamento sia strettamente necessario alla realizzazione del legittimo interesse in questione e che, alla luce di tutte le circostanze pertinenti, non prevalgano su tale legittimo interesse gli interessi o le libertà e i diritti fondamentali dei suddetti membri. Sebbene detta disposizione non esiga che un interesse siffatto sia determinato dalla legge, essa richiede che il legittimo interesse invocato sia lecito. E inoltre, se è possibile chiedere agli interessati il consenso al trattamento e alla comunicazione dei loro dati a scopi marketing, ecco che l'interesse legittimo non è una base di legittimità del trattamento correttamente richiamabile e utilizzabile in casi del genere.

Infine, la sentenza sottolinea che il legittimo interesse non può fondare il trattamento dei dati degli interessati se vi è la comunicazione a una società di giochi d'azzardo, stante il rischio di esporre quelle persone (poi destinatarie di chiamate commerciali) al pericolo di sviluppare ludopatie.

---

4 Ottobre 2024 – Corte di Giustizia UE: condizioni per esercitare il diritto di cancellare i dati personali dal Registro delle Imprese detenuto da uno Stato Membro e per richiedere il risarcimento del danno morale in caso di diniego.

La Corte di giustizia dell'Unione europea (CGUE) ha pubblicato la sentenza nella causa C-200/23, relativa al rifiuto *dell'Agentsia po vpisvaniyata* (Il Registro delle Imprese bulgaro) di cancellare alcuni dati personali relativi a una persona fisica contenuti in un contratto di partenariato pubblicato nel registro delle imprese ai sensi del Regolamento generale sulla protezione dei dati (GDPR).

Il caso: la persona fisica era socio di una società a responsabilità limitata di diritto bulgaro. L'8 luglio 2021, l'interessato ha chiesto all'Agenzia di cancellare i dati personali che lo riguardano contenuti nel suddetto accordo di partenariato, specificando che intendeva revocare il proprio consenso. In assenza di risposta da parte dell'Agenzia, l'interessato ha adito il Tribunale amministrativo di Dobrich, che ha annullato il rifiuto implicito dell'Agenzia di cancellare i dati e ha rinviato il caso all'Agenzia per una nuova decisione. Con una lettera, l'Agenzia ha fornito una copia autenticata dell'accordo di partenariato in questione, che nascondeva i dati personali dell'individuo, salvo quanto previsto dalla legge. La persona ha fatto nuovamente ricorso al Tribunale amministrativo chiedendo che la lettera fosse annullata e che l'Agenzia fosse condannata a risarcirle il danno non patrimoniale della lettera, che violava i suoi diritti ai sensi del GDPR. Il Tribunale amministrativo ha annullato la lettera e ha ordinato all'Agenzia di risarcire la persona per il danno non patrimoniale, ai sensi dell'articolo 82 del GDPR. L'Agenzia ha presentato ricorso alla Corte amministrativa suprema, che ha successivamente rinviato il caso alla CGUE.

La CGUE ha ritenuto, tra l'altro, che la direttiva 2017/1132 debba essere interpretata nel senso che non impone a uno Stato membro l'obbligo di autorizzare la pubblicazione, nel registro delle imprese, di un contratto aziendale soggetto all'obbligo di pubblicazione della direttiva e contenente dati personali diversi da quelli minimi richiesti, la cui pubblicazione non è prescritta dalla legislazione di tale Stato membro.

Inoltre, la CGUE ha ritenuto che l'articolo 4, paragrafi 7 e 9, del GDPR debba essere interpretato nel senso che l'autorità che tiene il registro delle imprese di uno Stato membro e che pubblica in tale registro i dati personali contenuti in un contratto di società soggetto all'obbligo di pubblicazione previsto dalla direttiva,

che le sono stati trasmessi nel contesto di una domanda di registrazione da parte della società, è allo stesso tempo il destinatario dei dati e, in particolare nella misura in cui li mette a disposizione del pubblico, il responsabile del trattamento di tali dati, anche se tale contratto contiene dati personali non richiesti dalla direttiva o dalla legge di tale Stato membro.

Inoltre, la CGUE ha affermato che l'articolo 82, paragrafo 1, del GDPR deve essere interpretato nel senso che la perdita di controllo per un periodo limitato da parte dell'interessato sui propri dati personali, dovuta alla messa a disposizione del pubblico di tali dati online nel registro delle imprese di uno Stato membro, può essere sufficiente a causare un "danno morale", a condizione che l'interessato dimostri di aver effettivamente subito tale danno, per quanto minimo, senza che la nozione di "danno morale" richieda la dimostrazione dell'esistenza di ulteriori conseguenze negative tangibili.

---

4 Ottobre 2024 – Corte di Giustizia UE: il risarcimento dei danni non patrimoniali ai sensi del GDPR.

La Corte di giustizia dell'Unione europea (CGUE) ha pubblicato la sentenza relativa alla causa C-507/23 sul risarcimento dei danni non patrimoniali ai sensi del Regolamento generale sulla protezione dei dati (GDPR).

Il caso: il ricorrente è un giornalista esperto nel settore automotive ed ha chiesto al Centro per la tutela dei diritti dei consumatori della Lettonia (PTAC) di rimuovere una campagna video in cui compariva un personaggio che lo imitava senza il suo consenso. Ha anche chiesto il risarcimento del danno alla reputazione. Il Tribunale amministrativo distrettuale della Lettonia ha ordinato alla PTAC di interrompere la campagna video e di pagare un risarcimento. In appello al Tribunale amministrativo regionale della Lettonia, le azioni della PTAC sono state dichiarate illegittime, ma la richiesta di risarcimento danni è stata respinta in quanto si è ritenuto che l'intento della campagna video fosse quello di svolgere un compito di interesse pubblico, non di danneggiare la reputazione del ricorrente.

La Corte Suprema della Lettonia ha chiesto alla CGUE di emettere una sentenza pregiudiziale per chiarire se:

- l'articolo 82, paragrafo 1, del GDPR debba essere interpretato nel senso che un trattamento illecito può di per sé costituire un'interferenza ingiustificata con il diritto alla protezione dei dati e causare un danno alla persona;

- l'articolo 82, paragrafo 1, del GDPR consente di ordinare le scuse come unico rimedio per i danni non pecuniari; e

- l'articolo 82, paragrafo 1, del GDPR consente che le circostanze che rivelano l'intenzione e la motivazione del Titolare del trattamento giustifichino un risarcimento inferiore del danno.

La CGUE ha ritenuto che:

- una violazione del GDPR non è di per sé sufficiente a costituire un "danno" ai sensi dell'articolo 82, paragrafo 1, del GDPR, letto alla luce dell'articolo 8, paragrafo 1, della Carta dei diritti fondamentali;

- la presentazione di scuse può costituire un risarcimento adeguato per un danno non patrimoniale, in particolare, quando è impossibile ripristinare la situazione allo stato precedente al verificarsi di tale danno, a condizione che la forma di risarcimento sia in grado di compensare pienamente il danno subito; e

- l'articolo 82, paragrafo 1, del GDPR esclude che si tenga conto dell'atteggiamento e della motivazione del Titolare del trattamento nel concedere all'interessato un risarcimento inferiore.

INTELLIGENZA ARTIFICIALE.

14 Ottobre 2024 – Consiglio UE: approvata in via definitiva la direttiva sui lavoratori delle piattaforme digitali.

Si conclude l'iter di approvazione delle nuove norme volte a migliorare le condizioni di lavoro di tutti coloro che lavorano nelle piattaforme digitali in UE: il Consiglio UE ha infatti adottato la direttiva sul lavoro tramite piattaforma, che verrà ora pubblicata nella Gazzetta Ufficiale UE.

La nuova direttiva punta a promuovere una maggiore trasparenza nell'utilizzo degli algoritmi che gestiscono le risorse umane, assicurando il monitoraggio dei sistemi automatizzati da parte di personale qualificato e che le decisioni così adottate possano essere contestate dai lavoratori.

La nuova direttiva inoltre ha l'obiettivo di determinare correttamente lo stato occupazionale delle persone che lavorano presso le piattaforme digitali, consentendo loro di accedere ai diritti di cui devono godere tutti i lavoratori. In tal senso, gli Stati membri stabiliranno una presunzione legale di occupazione che verrà attivata allorché si riscontrino determinati fatti sintomatici di controllo e direzione.

Dal momento della pubblicazione in Gazzetta Ufficiale dell'UE, gli Stati membri avranno due anni a disposizione per recepire le disposizioni nella normativa interna.

---

11 Ottobre 2024 - G7 delle Autorità garanti per la protezione dei dati personali: ruolo delle DPA nella regolamentazione dell'Intelligenza Artificiale.

Nel corso del quarto appuntamento del G7 delle Autorità di protezione dati, coordinato quest'anno dal Garante italiano, le Autorità hanno convenuto sull'importanza del ruolo delle Autorità nella regolamentazione dell'IA, determinate proprio al fine di garantirne l'affidabilità. È stato, infatti, sottolineato come esse dispongano di competenze, oltre che dell'indipendenza necessarie ad assicurare garanzie indispensabili per governare un fenomeno così complesso. Si è, pertanto, concordato sull'opportunità di esprimere ai Governi l'auspicio del riconoscimento di un ruolo adeguato alle Autorità di protezione dei dati nel sistema complessivo di governance dell'IA.

I Garanti, inoltre, hanno deciso di svolgere un monitoraggio sugli sviluppi legislativi dell'IA e il ruolo delle Autorità privacy all'interno delle giurisdizioni coinvolte.

Questo, come altri obiettivi, sono contenuti nell'Action Plan, il documento che guarda al futuro del G7 stabilendone i propositi e le aree tematiche che saranno oggetto dei lavori del prossimo anno. Molto utile si è rivelato anche il confronto tra gli ordinamenti dei diversi Paesi sul tema della libera circolazione dei dati, che rappresenta un importante elemento di sviluppo e progresso anche economico e sociale.

MERCATI DIGITALI

10 Ottobre 2024 – Pubblicato nella Gazzetta Ufficiale il decreto legislativo 7 Ottobre 2024, n. 144 di armonizzazione della normativa nazionale con il Regolamento UE 2022/868 sulla governance europea dei dati (Data Governance Act – DGA).

Il provvedimento italiano individua quale Autorità nazionale l'AgiD – Agenzia per l'Italia Digitale che avrà responsabilità e funzioni regolatorie e sanzionatorie. AgiD sarà infatti l'organismo competente per assistere gli enti pubblici cui si richiedono i dati, fungerà da sportello unico per smistare le richieste di dati agli enti pubblici (primo pilastro del DGA), rivestirà il ruolo di autorità competente per i servizi di intermediazione dei dati (data sharing, secondo pilastro del DGA) e si occuperà della registrazione delle organizzazioni per l'*altruismo dei dati* (terzo pilastro del DGA). Potrà irrogare sanzioni che vanno da 10 a 100 mila euro o fino al 6% del fatturato mondiale globale dell'anno precedente nel caso di violazione delle norme del DGA.

Il decreto legislativo è di fondamentale importanza perché rende finalmente operativo un quadro normativo (comunque applicabile dal 24 Settembre 2023) che libera le potenzialità e le opportunità di *business* della cosiddetta Strategia europea dei dati, aprendo per le imprese – ad esempio - opportunità di ulteriore sviluppo di beni e servizi attraverso l'accesso e la condivisione del rilevante patrimonio informativo in possesso delle Pubbliche amministrazioni (primo pilastro del DGA: riutilizzo dei dati detenuti dai soggetti pubblici) oppure attraverso lo sviluppo dei nuovi servizi di *intermediazione dei dati* (secondo pilastro del DGA) in cui l'impresa mette in contatto per la stipula di una licenza commerciale di utilizzo dei dati (personali e non personali) chi ha diritto di accesso ai dati (il cosiddetto "*titolare dei dati*") e chi quei dati vuole utilizzare (il cosiddetto "*utente dei dati*").

10 Ottobre 2024 – Consiglio UE: definitivamente approvato il *Cyber Resilience Act* (CRA) che prevede nuovi requisiti di sicurezza per i prodotti digitali.

Il Consiglio UE ha definitivamente approvato il Cyber Resilience Act, la nuova legge che introduce requisiti di sicurezza informatica per i prodotti con elementi digitali, al fine di garantire che, ad esempio, telecamere domestiche connesse, frigoriferi, TV e giocattoli siano sicuri prima di essere immessi sul mercato. Lo scopo generale è colmare le lacune, chiarire i collegamenti e rendere più coerente il quadro legislativo sulla sicurezza informatica esistente, garantendo che i prodotti con componenti digitali siano sicuri lungo la catena di fornitura e durante il loro ciclo di vita.

Il regolamento si applicherà a tutti i prodotti che sono collegati direttamente o indirettamente a un altro dispositivo o a una rete. Vi sono alcune eccezioni per i prodotti per i quali i requisiti di sicurezza informatica sono già stabiliti nelle norme comunitarie esistenti, ad esempio dispositivi medici, prodotti aeronautici e automobili.

Nello specifico, il testo prevede l'introduzione di requisiti di sicurezza informatica a livello comunitario per la progettazione, lo sviluppo, la produzione e la messa a disposizione sul mercato di prodotti hardware e software, per evitare sovrapposizioni di requisiti derivanti da diverse normative degli stati membri. Ad esempio, i prodotti software e hardware recheranno la marcatura CE per indicare che sono conformi ai requisiti del regolamento.

Inoltre, si consentirà ai consumatori di tenere conto della sicurezza informatica quando selezionano e utilizzano prodotti che contengono elementi digitali, rendendo più facile per loro identificare i prodotti hardware e software dotati delle adeguate funzionalità di sicurezza informatica.

L'atto sarà ora firmato dai presidenti del Consiglio e del Parlamento europeo e poi pubblicato nella Gazzetta ufficiale dell'UE.

---

9 Ottobre 2024 – European Banking Authority: Linee Guida per gli emittenti di token di riferimento di asset (ART) e di token di moneta elettronica (EMT) per garantire un riscatto ordinato e tempestivo dei token in caso di incapacità dell'emittente di adempiere ai propri obblighi.

Il Final Report dell'EBA sui piani di riscatto, ai sensi degli articoli 47 e 55 del Regolamento (UE) 2023/1114, stabilisce linee guida per gli emittenti di token di riferimento di asset (ART) e di token di moneta elettronica (EMT) per garantire un riscatto ordinato e tempestivo dei token in caso di incapacità dell'emittente di adempiere ai propri obblighi.

Le linee guida includono strategie di liquidazione degli asset di riserva, la profilatura dei titolari di token, le procedure antiriciclaggio e la gestione dei rischi di liquidità. Il piano di riscatto deve garantire il trattamento equo di tutti i titolari di token, con l'obiettivo di minimizzare i danni economici e garantire la stabilità del mercato.

INFORMATION TECHNOLOGY

8 Ottobre 2024 – Agenzia delle Entrate: provvedimento n. 379575/2024 sulle modalità di comunicazione, variazione e revoca dei dati relativi al domicilio digitale speciale e per confermare o revocare l'indirizzo PEC.

Con il provvedimento n. 379575 del 7 ottobre 2024, l'Agenzia delle Entrate ha fornito chiarimenti in merito alle modalità di elezione del domicilio digitale speciale e di conferma o revoca degli indirizzi digitali già comunicati, ai sensi dell'art. 60-ter, c. 5, del d.P.R. n. 600/1973.

La procedura non riguarda le imprese e i professionisti i cui indirizzi PEC devono essere iscritti nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC). Possono eleggere il domicilio digitale speciale esclusivamente le persone fisiche, i professionisti e gli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese. Tali soggetti possono eleggere un unico domicilio digitale speciale.

Il domicilio digitale speciale è eletto mediante la specifica funzionalità disponibile nell'area riservata del sito internet dell'Agenzia delle Entrate. La data della messa a disposizione del servizio per comunicare tale domicilio sarà reso noto con apposita comunicazione pubblicata sul sito web dell'Amministrazione finanziaria.

L'Agenzia invia un messaggio contenente un codice di validazione al domicilio digitale speciale indicato per verificarne l'esistenza e l'effettiva disponibilità per il richiedente. L'inserimento del codice di validazione all'interno dell'area riservata dell'utente conclude positivamente la verifica e produce effetto, ai fini delle notificazioni e delle comunicazioni.

Allo stesso modo sono comunicate le variazioni del domicilio digitale speciale registrato; la revoca è comunicata mediante apposita funzionalità.

---

2 Ottobre 2024 - Il 16 ottobre entra in vigore il D.lgs. n. 138/2024, di recepimento della Direttiva (UE) 2022/2555 NIS 2 su un livello comune di cybersicurezza nella UE.

È stato pubblicato in Gazzetta Ufficiale n. 230/2024 il Decreto Legislativo n. 138 del 4 settembre 2024 recante «*Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*».

Il D.lgs. n. 138/2024 che entrerà in vigore il 16 ottobre 2024, stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'UE in modo da migliorare il funzionamento del mercato interno.

Il Decreto composto da 44 articoli, prevede nello specifico:

a) la Strategia nazionale di cybersicurezza, recante previsioni volte a garantire un livello elevato di sicurezza informatica;

b) l'integrazione del quadro di gestione delle crisi informatiche, nel contesto dell'organizzazione nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza;

c) la conferma dell'Agenzia per la cybersicurezza nazionale quale:

1) Autorità nazionale competente NIS, disciplinandone i poteri inerenti all'implementazione e all'attuazione del Decreto;

2) Punto di contatto unico NIS, assicurando il raccordo nazionale e transfrontaliero;

3) Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia);

d) la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della Direttiva (UE) 2022/2555, e del Ministero della difesa, ciascuno per gli ambiti di competenza indicati all'art. 2, c. 1, lettera g), quali Autorità nazionali di gestione delle crisi informatiche su vasta scala, assicurando la coerenza con il quadro nazionale esistente in materia di gestione generale delle crisi informatiche, fermi restando i compiti del Nucleo per la cybersicurezza di cui all'art. 9 del D.L. n. 82/2021;

e) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale, supportandone le funzioni svolte quale Autorità nazionale competente NIS e Punto di contatto unico NIS;

f) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;

g) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del decreto, in particolare, attraverso la partecipazione nazionale a livello dell'Unione europea:

1) al Gruppo di cooperazione NIS tra autorità competenti NIS e tra punti di contatto unici degli Stati membri dell'Ue, nell'ottica di incrementare la fiducia e la collaborazione a livello unionale;

2) alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi cibernetiche su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione europea;

3) alla Rete di CSIRT nazionali nell'ottica di assicurare una cooperazione, sul piano tecnico, rapida ed efficace.

PROPRIETA' INTELLETTUALE E INDUSTRIALE

10 Ottobre 2024 – Le misure IP nel Decreto Omnibus, convertito in legge 143/2024.

L'articolo 6-bis del D.L. n. 113/2024, ha modificato la Legge n. 93 del 2023 (la cosiddetta legge anti pezzotto). Con le modifiche – e premesso che ai sensi dell'articolo 2 l'Autorità per le Garanzie nelle comunicazioni (AGCM), con proprio provvedimento, può ordinare ai prestatori di servizi, compresi i prestatori di accesso alla rete, di disabilitare l'accesso a contenuti diffusi abusivamente mediante il blocco della risoluzione del Data Source Name (DNS) dei nomi di dominio e il blocco dell'instradamento del traffico di rete verso gli indirizzi IP univocamente destinati ad attività illecite – ora i prestatori di servizi di assegnazione di numeri IP, provvedono periodicamente a riabilitare la risoluzione dei nomi di dominio e l'instradamento del traffico di rete verso gli indirizzi IP bloccati, decorsi almeno sei mesi dal blocco, qualora non risultino utilizzati per finalità illecite. Inoltre, AGCOM, al fine di garantire l'esecuzione efficace degli ordini di inibizione, fissa limitatamente al primo anno, limiti quantitativi massimi di IP che possono essere oggetto di blocco contemporaneamente.

Il *Decreto Omnibus* ha anche introdotto a scopi antipirateria un nuovo articolo 174-*bis* alla Legge sul Diritto d'autore 633/1941. La nuova disposizione impone specifici obblighi di segnalazione e di comunicazione – la cui violazione è sanzionata con la pena della reclusione fino a un anno e con le sanzioni pecuniarie per delitti informatici e trattamento illecito di dati di cui all'articolo 24- *bis* del Decreto Legislativo 8 giugno 2001, n. 231 sui reati d'impresa - per i prestatori di servizi di accesso alla rete, i soggetti gestori di motori di ricerca e i fornitori di servizi della società dell'informazione, ivi inclusi i fornitori e gli intermediari di VPN o comunque di soluzioni tecniche che ostacolano l'identificazione dell'indirizzo IP di origine, gli operatori di *content delivery network*, i fornitori di servizi di sicurezza internet e di DNS distribuiti, che si pongono tra i visitatori di un sito, e gli hosting provider che agiscono come reverse proxy server per siti web.

Tali soggetti devono inoltre designare e notificare all'AGCOM un punto di contatto che consenta loro di comunicare direttamente, via elettronica, con l'Autorità stessa. Inoltre, quelli che non sono stabiliti nell'UE ma che offrono servizi in Italia devono designare per iscritto una persona fisica o giuridica che funga da loro rappresentante legale in Italia che consenta loro di comunicare direttamente, via elettronica, con l'Autorità medesima.