OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Marzo 2024

MONTHLY ROUNDUP

Marzo 2024

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

---

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- Data breach: il Garante sanziona UniCredit per 2,8 milioni di euro [Link]
- App per diabetici: il Garante Privacy multa una società di dispositivi medici [Link]
- Autovelox, Garante Privacy: parere favorevole al Mit [Link]
- Le Autorità privacy Ue avranno maggiore autonomia contro le imprese extra Ue [Link]

Provvedimenti AGCOM

- Linee guida attuative delle disposizioni dell'Agcom sulla qualità di accesso a Internet da postazione fissa ai sensi dell'art. 2, comma 7, dell'Allegato A alla delibera n. 156/23/CONS [Link]
- Linee guida volte alla verifica dell'esistenza di posizioni di significativo potere di mercato lesive del pluralismo, ai sensi dell'art. 51, comma 5, del D. Lgs. 8 novembre 2021, n. 208 [Link]

PRINCIPALI AGGIORNAMENTI

- Il Gigabit Infrastructure Act: sarà veramente una svolta per la connettività in Europa?
- Il risarcimento del danno immateriale da utilizzo abusivo di dati personali: il verdetto della Corte di Giustizia dell'Unione europea

Il Gigabit Infrastructure Act: sarà veramente una svolta per la connettività in Europa?

Nel panorama in cui l'infrastruttura digitale si afferma sempre più come pilastro fondamentale per l'economia globale, insieme ai servizi essenziali tradizionali come elettricità, gas, acqua e trasporti, emerge una questione cruciale: come può l'Europa colmare il deficit di investimenti (valutato a circa 65 miliardi di euro l'anno) [1] necessari per sviluppare reti digitali all'avanguardia? La connettività, essenziale per il progresso economico e sociale, richiede, infatti, un'accelerazione nell'adozione di servizi online avanzati e connessioni Internet ad alta velocità.

In risposta a questa sfida, la Commissione europea ha presentato una proposta di riforma della direttiva sulla riduzione dei costi della banda larga, nota come "*Broad Cost Reduction Directive*" ("*BCRD*")[2], con l'obiettivo di ridurre gli ostacoli che frenano lo sviluppo delle infrastrutture digitali. Questa iniziativa mira a superare le inefficienze procedurali, le difficoltà di coordinamento delle opere civili, le complessità amministrative e gli ostacoli nell'installazione di infrastrutture all'interno degli edifici.

Lo sforzo della Commissione si è tradotto nella proposta di regolamento "*Gigabit Infrastructure Act*" (in breve "**GIA**") presentata il 23 febbraio 2023. Il regolamento è volto ad introdurre misure finalizzate a ridurre i costi dell'installazione di reti di comunicazione elettronica ad altissima capacità, fisse e senza fili/mobili (VHCN, Very High Capacity Network o Gigabit), vale a dire i collegamenti di rete che permettono di trasferire dati a una velocità più elevata (1 Gigabit al secondo) in downstream, quindi, dalla rete Internet verso la LAN[3] o il sistema locale. Il GIA fa parte del cd. "**pacchetto connettività**"[4] e, nelle intenzioni delle Istituzioni europee, una volta approvato, dovrebbe rappresentare una pietra miliare nella regolamentazione del settore delle telecomunicazioni in Europa.

---

1 Comunicazione della Commissione europea del 2020 "Plasmare il futuro digitale dell'Europa".

2 Direttiva 2014/61/UE (cd. "*Broad Cost Reduction Directive*" o "**BCRD**"), la quale, adottata in risposta alla necessità di attuare politiche capaci di abbattere i costi di installazione della banda larga, contiene misure sulla condizione delle infrastrutture, sul coordinamento delle opere di genio civile e sulla riduzione degli oneri amministrativi.

3 Una rete LAN (*Local Area Network*) è una rete informatica estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti. Una rete LAN può essere piccola o grande, da una rete domestica con un utente a una rete aziendale con migliaia di utenti e dispositivi.

4 Il "pacchetto connettività" è un pacchetto di misure presentato dalla Commissione europea che include anche:

- una consultazione esplorativa sul futuro del settore della connettività e delle relative infrastrutture (iniziata il 23 febbraio 2023 e conclusa il 19 maggio 2023), volta a raccogliere opinioni sul modo in cui l'aumento della domanda di connettività e i progressi tecnologici potrebbero incidere sulle esigenze e sugli sviluppi futuri. I risultati della consultazione sono stati pubblicati il 10 ottobre 2023 e forniscono le prospettive dei fornitori di telecomunicazioni, delle emittenti, dei fornitori e delle piattaforme di servizi cloud, delle associazioni di imprese, delle organizzazioni dei consumatori, dei cittadini, delle organizzazioni non governative, delle autorità pubbliche, dei sindacati e del mondo accademico. La consultazione è emersa la necessità di infrastrutture di connettività affidabili e resilienti; e
- un progetto di raccomandazione sulla connettività Gigabit, volta a fornire orientamenti alle autorità nazionali di regolamentazione sulla condizione di accesso alle reti di telecomunicazione degli operatori che detengono un significativo potere di mercato, per incentivare un più rapido abbandono delle tecnologie preesistenti e una diffusione accelerata delle reti Gigabit. La raccomandazione Gigabit è stata adottata nel febbraio 2023 e sostituisce la raccomandazione sull'accesso di nuova generazione del 2010 e la raccomandazione del 2013 sulla non discriminazione e sulla metodologia dei costi.

Dopo un acceso dibattito sulla eliminazione o il mantenimento della nozione di silenzio assenso all'interno del regolamento, il Consiglio dell'UE e l'Europarlamento hanno finalmente raggiunto una quadra.

Le finalità perseguite dal GIA sono:

- **superare la sfida della lenta e costosa implementazione delle infrastrutture fisiche** destinate ad ospitare elementi che sostengono le reti Gigabit avanzate senza diventare elementi attivi della rete stessa (ad es. tubature, piloni, cavidotti, pozzi di ispezione e pozzetti). Ciò potrebbe avvenire mediante la possibilità, per gli operatori, di richiedere agli enti pubblici che possiedono o controllano infrastrutture fisiche o agli altri operatori di rete, l'accesso a tali infrastrutture a condizioni eque e ragionevoli per poter installare gli elementi di reti ad altissima capacità o risorse correlate;
- **semplificare e rendere più rapida la procedura per il rilascio delle autorizzazioni** necessarie per l'implementazione delle reti Gigabit, mediante la previsione del principio del silenzio-assenso, vale a dire l'ottenimento dell'autorizzazione in assenza di una risposta da parte dell'autorità competente entro un determinato periodo di tempo a seguito dell'invio della richiesta da parte dell'operatore;
- **migliorare il coordinamento dei lavori tra gli operatori di rete** [5] per implementare le infrastrutture fisiche sottostanti, come condotti e tralicci, e garantire che i soggetti interessati ne ottengano l'accesso, mediante il diritto, in capo a ogni operatore di rete, di **negoziare accordi sul coordinamento delle opere di genio civile**[6] con gli altri operatori.

Dalla proposta della Commissione è possibile ricavare che l'obiettivo di assicurare una connettività a tutti i cittadini dell'UE **verrà perseguito attraverso varie misure**, tra le quali, principalmente:

- l'obbligo, per tutti gli edifici presso la sede dell'utente finale di nuova costruzione o sottoposti a opere di ristrutturazione importante, **di dotarsi di un'infrastruttura fisica interna all'edificio predisposta per la fibra**[7] ai punti terminali di rete, così come di un cablaggio in fibra interno all'edificio [8], consentendo a tutti gli utenti di avere una connessione più veloce e aumentando il valore degli edifici nuovi o ristrutturati;

- **l'obbligo**, per tutti i condomini di nuova costruzione o sottoposti ad una ristrutturazione importante, **di dotarsi di**

5 Per operatori di rete si intendono le imprese che forniscono o sono autorizzate a fornire una rete pubblica di comunicazione elettronica, o una risorsa correlata (cfr. art. 2(29) della Direttiva (UE) 2018/1972 che istituisce il Codice europeo delle Comunicazioni Elettroniche), le imprese che forniscono un'infrastruttura fisica destinata alla prestazione di un servizio di produzione, trasporto o distribuzione di gas, elettricità (compresa l'illuminazione pubblica, riscaldamento, acqua (comprese le fognature e gli impianti di trattamento delle acque reflue, e sistemi di drenaggio), le imprese che forniscono un'infrastruttura fisica destinata alla prestazione di servizi di trasporto, compresi ferrovie, strade, porti e aeroporti.

6 Le opere di genio civile sono il risultato di un insieme di lavori edilizi o di genio civile che di per sé esplicano una funzione economica o tecnica e comportano uno o più elementi di un'infrastruttura fisica (art. 2(3) della proposta di GIA).

7 Per infrastruttura fisica interna all'edificio predisposta per la fibra si intende l'infrastruttura fisica presente all'interno dell'edificio e destinata a ospitare elementi in fibra ottica (art. 2(8) della proposta di GIA).

8 Per cablaggio in fibra interno all'edificio si intendono i cavi di fibre ottiche presenti nella sede dell'utente finale, compresi gli elementi oggetto di comproprietà, destinati a fornire servizi di comunicazione elettronica, che collegano il punto di accesso dell'edificio con il punto terminale di rete (art. 2(7) della proposta di GIA).

un punto di accesso[9], riducendo per gli operatori di rete i costi individuali per l'accesso all'infrastruttura, nonché garantendo una maggiore scelta, da parte degli utenti finali, tra più operatori che offrono servizi in fibra;

- in assenza di un'infrastruttura interna all'edificio predisposta per la fibra, il diritto, per i fornitori di reti pubbliche di comunicazione elettronica, **di far terminare la propria rete nella sede dell'abbonato**, a condizione di aver ottenuto l'accordo dell'abbonato e purché l'impatto sulla proprietà privata di terzi venga ridotta al minimo. In questo modo, gli utenti che si trovano in aree non coperte da infrastrutture in fibra ottica potranno comunque ottenere una connessione veloce.

Considerando i rapidi progressi compiuti nel contesto delle tecnologie digitali e dalla crescente necessità di diffusione di connettività derivante dallo sviluppo e dall'uso di tecnologie sempre più innovative, le previsioni del GIA predisposte sotto forma di **regolamento e non più di direttiva** e, in particolare, la previsione del principio del silenzio-assenso e **la digitalizzazione degli sportelli unici** per consentire il rispetto di tutti gli obblighi previsti dalla normativa, potrebbero ridurre i **tempi e i costi richiesti** per l'implementazione da parte degli operatori di telecomunicazioni di reti ad alta e altissima capacità, in parte causati dalle procedure di rilascio delle autorizzazioni prima dell'installazione delle reti.

Con gli sportelli unici, messi a disposizione per consentire l'esercizio online di tutti i diritti, gli operatori di rete saranno in grado di **implementare rapidamente** le reti attraverso procedure semplificate, digitalizzate e meno costose. La normativa potrebbe anche essere in grado di **facilitare l'ingresso di nuovi operatori** nel mercato delle telecomunicazioni, favorendo la concorrenza e l'innovazione.

Le misure potrebbero essere rilevanti nel mercato italiano, anche in considerazione delle risultanze emerse dal *Digital Economy and Society Index*, l'indice di digitalizzazione dell'economia e della società, pubblicato nel 2022 dalla Commissione europea. Secondo tale indice, infatti, seppur l'Italia si collochi al 7° posto tra gli Stati membri dell'UE in termini di connettività, **la percentuale di famiglie italiane che hanno accesso alla rete fissa ad altissima capacità è pari al 44%.** Tale percentuale risulta molto bassa se si considera la media dell'UE è pari al 70%.

Il divario, peraltro, sembra aumentare nelle zone rurali. Come riportato nell'indice DESI di tutti gli Stati membri dell'UE, infatti, la copertura Internet ad alta velocità totale delle famiglie raggiunge quasi il 50%, mentre meno del 20% delle famiglie ubicate nelle zone rurali ha accesso alla rete fissa ad altissima capacità. In attesa del testo definitivo e della sua approvazione, sorge spontaneo chiedersi se tale regolamento potrà effettivamente aumentare la connettività in Europa. Resta da vedere se, a seguito di tali misure, la connettività in Italia e negli altri Stati membri dell'UE aumenterà effettivamente o se verranno riscontrati dei problemi applicativi.

* * *

[9] Il punto di accesso è un punto fisico situato all'interno o all'esterno dell'edificio e accessibile a una o più imprese che forniscono o sono autorizzate a fornire reti pubbliche di comunicazione elettronica, che consente la connessione con l'infrastruttura fisica interna all'edificio predisposta per la fibra (art. 2(11) della proposta di GIA).

Il risarcimento del danno immateriale da utilizzo abusivo di dati personali: il verdetto della Corte di Giustizia dell'Unione europea

La Corte di Giustizia dell'Unione europea (la "**CGUE**" o la "**Corte**"), con la sentenza resa nella causa C-340/21, VB v. Natsionalna agentsia za prihodite (la "**Sentenza**"), il 14 dicembre scorso, si è pronunciata sulle condizioni per il risarcimento dei danni immateriali derivanti dalla pubblicazione di dati personali su Internet a seguito di un attacco hacker, costituente una violazione di dati personali ai sensi del Regolamento (UE) 2016/679 (il "**GDPR**" o il "**Regolamento**").

La Corte ha accolto l'interpretazione secondo cui anche il mero timore dell'interessato di un potenziale futuro utilizzo abusivo dei propri dati personali da parte di terzi può di per sé costituire un "danno immateriale" risarcibile ai sensi dell'art. 82 del GDPR. Il titolare del trattamento, infatti, non può essere esonerato dal suo obbligo di risarcire il danno subito dall'interessato per il solo fatto che tale danno derivi da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di "terzi" quali criminali informatici.

La Sentenza, inoltre, riconoscendo un risarcimento pari ad un importo di circa 500,00 euro, conferma che – contrariamente al prevalente orientamento della giurisprudenza italiana[10] – il danno è risarcibile anche se non raggiunge una soglia minima. Secondo la Corte, infatti, quest'ultima contrasterebbe sia con il principio di effettività del danno (che richiede che venga risarcito nella sua integrità, non essendoci nel Regolamento alcuna norma che imponga al soggetto interessato l'obbligo di sopportare il danno alla privacy), che con il principio di uniformità (poiché, altrimenti, la soglia minima sarebbe interpretata diversamente da parte di ciascuno Stato membro).

Il regime di responsabilità introdotto dall'art. 82 del GDPR

Prima di analizzare il caso da cui trae origine la sentenza della CGUE e le conclusioni cui è approdata, si richiama, nelle parti che qui interessano, il disposto dell'art. 82 del GDPR.

Nello specifico, la norma, al suo primo comma, riconosce il diritto ad ottenere il risarcimento dal titolare del trattamento o dal responsabile del trattamento a chiunque abbia subito un danno materiale o immateriale a causa di una violazione del Regolamento. Vi sono, dunque, tre condizioni che devono sussistere affinché possa essere riconosciuto un diritto al risarcimento del danno ai sensi dell'art. 82 del Regolamento:

1. un danno subito;
2. la violazione del Regolamento;
3. il nesso causale tra danno subito dall'interessato e violazione.

L'art. 82(3) del GDPR esclude la responsabilità in caso di non imputabilità, al titolare o al responsabile, dell'evento dannoso[11].

10 Sez. Un. n. 26972/2008, Cass. Sez. III n. 7726/2016, Cass. Sez. VI, ord. n. 17383/2020. In tale ultima ordinanza, la Corte di cassazione ritiene che, ai fini della risarcibilità dei danni ai dati personali, sia necessario che la lesione venga valutata tenendo conto del principio di solidarietà (art. 2 Cost.), per cui vi sarà la tolleranza dei danni lievi e il giudice di merito dovrà condannare al risarcimento solo in caso di danni gravi o serietà della lesione, ossia quando vi sia una perdita di natura personale effettivamente patita dall'interessato. Anche in presenza di una violazione delle prescrizioni di legge, il risarcimento sarà dovuto solo se la violazione della norma offende in modo sensibile la sua portata effettiva.

11 L'avvocato generale della CGUE (Sanchez), relativamente alla problematica del criterio di imputazione della

Nell'ordinamento italiano, un'analoga previsione si rinviene anche nell'art. 2050 c.c.[12]., in forza del quale, il trattamento dei dati personali è considerato, per sua natura o, meglio, per la natura dei mezzi adoperati, quale attività pericolosa. Nel trattamento di dati vi è dunque un rischio intrinseco che titolare e responsabile del trattamento devono tenere presente e, conseguentemente, sono tenuti ad adottare le più opportune precauzioni per limitare quanto più possibile il rischio.

L'art. 82 del Regolamento deve infine essere letto in combinato disposto con gli artt. 5, 24 e 32 del GDPR, che pongono in capo al titolare del trattamento l'obbligo di accountability, ossia di adottare – tenuto conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto, delle finalità del trattamento e del rischio di probabilità e gravità per i diritti e le libertà delle persone fisiche – misure tecniche ed organizzative adeguate ed efficaci per garantire e dimostrare la conformità del trattamento al GDPR.

I fatti oggetto di causa

La vicenda trae origine da un accesso abusivo al sistema informatico dell'Agenzia nazionale per le entrate pubbliche bulgara (la "**NAP**"), a seguito del quale sono stati diffusi online i dati personali di oltre sei milioni di interessati. Fra questi, una ricorrente ha adito il Tribunale amministrativo della città di Sofia, chiedendo il risarcimento di una somma pari a 510,00 euro in considerazione del danno immateriale subito.

Secondo la ricorrente il danno consisterebbe "*nel timore che i suoi dati personali che sono stati pubblicati senza il suo consenso siano oggetto di un utilizzo abusivo, in futuro, o che essa subisca un ricatto, un'aggressione, o addirittura un rapimento*"[13].

Tuttavia, il giudice di primo grado respingeva il ricorso: secondo il tribunale, infatti, la ricorrente non aveva dimostrato la mancata adozione di misure di sicurezza adeguate da parte della NAP. La ricorrente si rivolgeva, dunque, alla Corte suprema amministrativa bulgara, la quale investiva la CGUE di diverse questioni pregiudiziali, tra le quali:

1. se la divulgazione non autorizzata dei dati personali possa far automaticamente considerare inadeguate le misure di sicurezza adottate dal titolare del trattamento;
2. la competenza a valutare l'adeguatezza delle misure di sicurezza adottate dal titolare;
3. la parte su cui grava l'onere della prova;
4. se la circostanza che la divulgazione non autorizzata sia stata causata da terze parti possa o meno esonerare il titolare del trattamento dall'onere di risarcire il danno;
5. se il timore di un utilizzo improprio dei dati personali, a causa di una violazione del GDPR, possa di per sé essere considerata un "danno immateriale", risarcibile ai sensi dell'art. 82(1) del GDPR.

responsabilità dell'art. 82 del GDPR e se l'assenza di colpa o la colpa lieve incida sulla quantificazione del danno alla privacy, rileva come tale norma, prevedendo come esimente che il titolare e/o il responsabile provino che il danno non è loro in alcun modo imputabile, non importa la necessità degli stessi di provare l'esistenza di colpa lieve o l'inesistenza della colpa, poiché l'art. 82 non si basa su una colpa con inversione dell'onere probatorio. Cfr. CGUE, 4 gennaio 2024, C-667/2021.

12 La norma, proprio come il GDPR, prevede un obbligo risarcitorio a meno che non si provi "*di aver adottato tutte le misure idonee ad evitare il danno*".

13 Cfr. punto 13 della Sentenza.

La responsabilità del titolare in caso di *data breach*

La CGUE ha sottolineato che, in caso di divulgazione non autorizzata o accesso non autorizzato ai dati personali, è fondamentale esaminare l'adeguatezza delle misure di sicurezza adottate dal titolare del trattamento.

Di per sé, dunque, **il solo fatto che vi sia stato un data breach, non può far considerare tali misure come inadeguate, né tantomeno assurgere a presunzione assoluta di responsabilità del titolare.** Nel GDPR, infatti, sebbene venga richiesta l'adozione di un sistema di sicurezza adeguato ai rischi, non vi è alcuna pretesa verso una loro completa eliminazione.

Con specifico riferimento alla responsabilità del titolare, la Corte ha altresì ribadito[5] che una simile violazione non può essere imputata al titolare del trattamento a meno che quest'ultimo non la abbia resa possibile violando un obbligo previsto dal GDPR.

La valutazione dell'adeguatezza delle misure di sicurezza e l'onere della prova

La Corte ha peraltro precisato che l'adeguatezza delle misure di sicurezza dev'essere valutata in concreto.

Sebbene, infatti, il titolare disponga di un certo margine di discrezionalità per determinare le misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza proporzionato al rischio (come richiesto dall'art. 32(1) GDPR), **la valutazione della loro adeguatezza spetta ai tribunali nazionali**. È compito dei Tribunali, infatti, esaminare se tali misure sono state attuate secondo criteri di adeguatezza, efficacia e proporzionalità, tenendo conto delle esigenze di protezione dei dati specificamente inerenti al trattamento di cui trattasi nonché dei rischi indotti da quest'ultimo. Tale verifica di adeguatezza può essere fatta mediante gli strumenti processuali ritenuti più adeguati e conformi all'ordinamento dello Stato membro, anche eventualmente mediante perizie giurate (come richiesto dai giudici bulgari), ma tale strumento non può costituire mezzo di prova necessario e sufficiente.

L'onere di provare che tali misure siano adeguate, grava invece, coerentemente con il principio di *accountability* enunciato all'art. 5 e concretizzato all'art. 24 del GDPR, sul titolare.

In ragione di quanto sopra esposto, dunque, le circostanze in cui il titolare del trattamento può pretendere di essere esonerato dalla responsabilità civile in cui incorre ai sensi dell'art. 82 del GDPR, devono essere strettamente limitate a quelle in cui è in grado di dimostrare la **mancanza di imputabilità del danno**, ossia:

- perché le misure di sicurezza predisposte erano adeguate, e
- perché si è tempestivamente attivato per mitigare le conseguenze dannose.

Il concetto di "danno immateriale" ai sensi dell'art. 82(1) del GDPR

La CGUE ha stabilito che l'art. 82(1) del Regolamento dev'essere interpretato nel senso che **le preoccupazioni, le ansie e i timori di un potenziale utilizzo abusivo dei dati personali di un interessato da parte di terzi a seguito di una violazione del GDPR possono, di per sé, costituire un "danno immateriale" a tutti gli effetti risarcibile**.

L'orientamento della Corte si basa sul Considerando 146 del GDPR, secondo il quale "*il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente*

regolamento". La Corte, dunque, rimarca[14] una **nozione ampia di danno**, che comprende sia un danno già prodotto attraverso l'utilizzo illecito dei dati personali, sia la sola paura percepita dall'interessato che un siffatto utilizzo possa in futuro prodursi.

Tuttavia, occorre precisare che l'interessato deve dimostrare di aver realmente sofferto di simili ansie, preoccupazioni e timori e che, di conseguenza, sarà compito del giudice nazionale adito verificare che tali paure possano essere considerate fondate, nelle circostanze specifiche di cui trattasi e nei confronti dell'interessato.

Ciò posto, la Corte, richiamata la precedente sentenza del 4 maggio 2023 resa nella causa C-300/21 (*Österreichische Post*), ha altresì ribadito che la violazione di specifici obblighi discendenti dal GDPR non comporta necessariamente un danno (e, dunque, il sorgere di responsabilità in capo al titolare): per fondare un diritto al risarcimento deve infatti sussistere un nesso di causalità tra la violazione di un obbligo del GDPR e il danno subito e, inoltre, non è necessario che quest'ultimo **superi una determinata soglia di gravità**.

La decisione della CGUE rappresenta un'ulteriore pietra miliare nella giurisprudenza in materia di protezione dei dati personali. I principi che ne derivano possono essere sintetizzati come segue:

la divulgazione non autorizzata dei dati personali non implica automaticamente che le misure di sicurezza adottate dal responsabile siano inadeguate;
la valutazione dell'adeguatezza di tali misure spetta ai tribunali nazionali, che possono utilizzare qualsiasi mezzo processuale ritenuto adeguato dall'ordinamento interno;
è dovere del titolare del trattamento provare che le misure di sicurezza adottate erano adeguate;
se la divulgazione non autorizzata è causata da terze parti (i c.d. hackers), il titolare del trattamento potrebbe essere tenuto a risarcire i soggetti colpiti, a meno che dimostri di non essere in alcun modo responsabile del danno;
il timore di un utilizzo improprio dei propri dati personali, a causa di una violazione del GDPR, è di per sé considerata un "danno immateriale".
Con la Sentenza, la Corte arretra la soglia di risarcibilità del danno: ad essere risarcibile non è solo il fatto vero e proprio dell'utilizzo illecito dei dati sottratti, ma anche la mera esposizione al rischio di un loro utilizzo abusivo da parte di chi li ha sottratti illecitamente. Infatti, ansie, preoccupazioni e paure rappresentano solitamente il primo danno subito da un interessato.

Pertanto, sarà interessante osservare come questa nuova concezione di danno, risarcibile anche se lieve, si ripercuoterà nelle aule dei tribunali italiani ove, la Suprema Corte di cassazione, con un orientamento ormai consolidato, ritiene che il danno, per essere risarcibile, debba rispondere ai requisiti di "gravità della lesione" e "serietà del danno".

La Corte, inoltre, ha evidenziato la necessità di un'analisi approfondita sull'adeguatezza delle misure di sicurezza adottate dai titolari del trattamento. Sarà dunque fondamentale per le aziende investire tempo e risorse nelle attività di prevenzione di data breach e sicurezza del trattamento dei dati personali.

[14] CGUE 4 maggio 2023, Österreichische Post, C-300/21.

* * *

Per maggiori informazioni, potete contattare:

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

LinkedIn

Morri Rossetti

Osservatorio TMT&DP

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it