DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Violazione dei dati personali: criteri di responsabilità e risarcibilità del danno

8 Giugno 2023

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners
Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners
Gaia Leoncini, Ristuccia Tufarelli & Partners

DB non solo diritto bancario

Luca Tufarelli, Partner & Founder, Ristuccia Tufarelli & Partners

Maria Lilia La Porta, Senior Associate, Ristuccia Tufarelli & Partners

Gaia Leoncini, Ristuccia Tufarelli & Partners

Luca Tufarelli

L'avvocato Luca Tufarelli, Partner e socio fondatore dellotudio Ristuccia Tufarelli & Partners, ha conoscenze specifiche nei campi del diritto civile, commerciale, amministrativo e del diritto dell'informatica dove assiste sia soggetti privati che pubblici. Ha contribuito alla realizzazione di progetti speciali nei settori delle tecnologie innovative, delle telecomunicazioni, della informatizzazione della PA e del commercio elettronico occupandosi anche degli aspetti consumeristici e di compliance regolamentare (privacy, tutela del mercato e vigilanza delle comunicazioni).

Studio associato

Ristuccia Tufarelli & Partners

1. Premessa – Le Conclusioni presentate il 27 aprile 2023 dall'Avvocato Generale UE causa C-340/21

Il 27 aprile 2023 l'Avvocato Generale della Corte dell'Unione Europea, Giovanni Pitruzzella, ha presentato le proprie conclusioni in merito alla Causa C-340/21, riguardante la responsabilità del titolare del trattamento in caso di violazione dei dati personali per accesso illecito da parte di terzi.

La causa è scaturita da un attacco hacker avvenuto nel luglio 2019 a danno dell'Agenzia Nazionale delle Entrate bulgara (NAP). A causa dell'attacco sono state pubblicate su internet varie informazioni fiscali e previdenziali di milioni di contribuenti bulgari.

Molti dei contribuenti colpiti dall'attacco hanno convenuto in giudizio l'Agenzia delle Entrate bulgara, lamentando il mancato rispetto dei principi del trattamento dei dati personali enunciati dal Regolamento UE n. 679/2016 ("GDPR" o solo "Regolamento") ed in particolare la mancata adozione di adeguate misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Uno dei soggetti lesi, in particolare, ha sostenuto di aver subito un danno morale, consistente nel timore di subire future ulteriori violazioni dei propri dati personali, chiedendone il risarcimento. Ne è conseguita, dunque, una causa avente ad oggetto (i) l'accertamento della responsabilità del titolare del trattamento per la suddetta violazione, nonché (ii) il profilo della risarcibilità del danno morale consistente in apprensioni e timori di un futuro uso improprio dei propri dati.

In primo grado, il giudice ha rigettato la domanda del ricorrente, affermando che (i) l'accesso ai dati dell'interessato da parte di un terzo non fosse imputabile alla NAP (ii) che gravasse sul ricorrente l'onere di provare l'inadeguatezza delle misure adottate dall'Agenzia e (iii) negando la risarcibilità del danno morale.

La sentenza di primo grado è stata appellata dal ricorrente e in tale sede, la Corte Suprema amministrativa bulgara ha deciso di sottoporre alla Corte di Giustizia Europea alcune questioni pregiudiziali riguardanti (i) la verifica delle violazioni al trattamento dei dati, (ii) le responsabilità del titolare del trattamento e, infine, (iii) la risarcibilità del danno morale consistente nel timore dei possibili futuri e potenziali utilizzi illeciti dei dati personali esfiltrati.

vedi l'articolo online

Alla luce dell'analisi delle predette questioni, l'Avvocato Generale della Corte UE ha presentato le seguenti conclusioni:

1. il verificarsi di una «violazione dei dati personali» non è di per sé sufficiente per concludere che le misure tecniche e organizzative attuate dal responsabile del trattamento non erano «adeguate» a garantire la protezione dei dati;

2. nel verificare l'adeguatezza delle misure attuate dal titolare, il giudice nazionale deve procedere ad un'analisi concreta di tali misure sulla base dei principi sanciti dall'art. 24 del Regolamento;

3. spetta al titolare del trattamento dimostrare di aver predisposto delle misure adeguate alla tutela della protezione dei dati personali;

4. una violazione di dati personali causata da un soggetto terzo non esonera di per sé il titolare del trattamento dalla responsabilità, salvo che lo stesso dimostri, con un livello di prova molto elevato, che l'evento dannoso non gli è in alcun modo imputabile;

5. il pregiudizio consistente nel timore di un potenziale futuro uso improprio di dati personali può costituire danno morale e quindi essere oggetto di risarcimento a condizione che l'interessato dimostri che si tratti di un rischio reale e concreto e non di un semplice disagio o fastidio dell'interessato i cui dati sono stati esfiltrati.

Il presente contributo è volto ad analizzare, alla luce delle principali disposizioni del Regolamento UE n. 679/2016, i due temi principali emersi dalla causa citata: (i) la responsabilità del titolare del trattamento e (ii) il risarcimento del danno morale in caso di violazione dei dati personali. L'obbiettivo è anche fornire alcune considerazioni e spunti di riflessione.

2. La responsabilità del titolare del trattamento

L'aspetto centrale della disciplina in materia di protezione dei dati personali è rappresentato dal c.d. principio di responsabilizzazione ("*accountability*") - disciplinato dall'art. 5, comma 2, del Regolamento - ossia il principio che attribuisce in capo al titolare del trattamento la responsabilità nell'adozione di comportamenti proattivi volti a garantire il rispetto dei principi fondamentali in materia di trattamento di dati personali e a evitare rischi per i diritti e le libertà degli interessati.

Il principio di responsabilizzazione è sicuramente una delle principali novità introdotte dal GDPR, che ha rafforzato i doveri che gravano sui titolari del trattamento in termini di analisi preventiva dei rischi e dell'impatto dei trattamenti sui diritti e le libertà degli interessati in termini di probabilità e gravità. L'art. 24 del Regolamento dispone infatti che, tenendo conto di una serie di fattori[1], "il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate *per "garantire* << nelle operazioni di trattamento di dati personali>> *un livello di sicurezza adeguato al rischio*", così come affermato anche nell'art. 32 dello stesso GDPR[2].

Il GDPR, quindi, assegna al titolare del trattamento la responsabilità di trattare i dati in modo tale da garantire che dal trattamento non possano derivare rischi per i diritti e le libertà degli interessati e il potere di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce dei criteri indicati nel Regolamento stesso. Spetta, dunque, al titolare del trattamento il compito di valutare quali sono le misure tecniche e organizzative da adottare e verificare continuamente se siano proporzionate e adeguate ai rischi.

Alla luce di ciò, una prima questione pregiudiziale da analizzare riguarda la corretta interpretazione da dare agli artt. 24 e 32 del GDPR nel caso in cui si verifichi una violazione dei dati personali, ai sensi dell'articolo 4, punto 12, del medesimo Regolamento, da parte di persone che non sono dipendenti dell'amministrazione del titolare del trattamento e non sono soggette al suo controllo. Occorre capire se tale evento sia sufficiente per ritenere che le misure tecniche e organizzative adottate dal titolare del trattamento non siano adeguate.

Sul punto, l'Avvocato Generale della Corte UE evidenzia innanzitutto che nella scelta delle misure ade-

1 Cfr. prima parte dell'art. 24 GDPR, il quale dispone che "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche…*".

2 Cfr. art. 32, GDPR: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (…)*".

guate il titolare deve tener conto di una serie di fattori, elencati nelle suindicate disposizioni, tra cui in particolare:

- lo stato dell'arte, inteso come lo stato di avanzamento della scienza, della tecnica, della tecnologia e della ricerca esistente nel momento di adozione delle misure. É chiaro che il titolare sarà limitato nella scelta da ciò che è ragionevolmente possibile in quel momento e ciò può implicare che una misura sia adeguata in un determinato momento ma comunque venga aggirata da criminali informatici che utilizzano strumenti molto sofisticati idonei a violare anche misure di sicurezza conformi allo stato dell'arte;

- i costi di attuazione, ossia le risorse in generale, compresi il tempo e le risorse umane. Il fattore costo implica che il titolare deve operare un bilanciamento tra gli interessi dell'interessato e gli interessi economici del titolare del trattamento, sulla base del principio di proporzionalità, non impiegando una quantità sproporzionata di risorse nel caso in cui esistano misure alternative, meno dispendiose, ma efficaci[3].

Per di più è il legislatore stesso, nella formulazione delle predette disposizioni, ad aver contemplato che le violazioni si possano verificare comunque, nella parte in cui include tra le misure suggerite la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico[4].

Occorre precisare che nonostante il titolare abbia una certa autonomia ed un certo margine di manovra nella scelta e adozione delle misure, questo non esclude che possa esercitarsi un controllo giurisdizionale, che valuterà l'adeguatezza delle misure da un punto di vista concreto ed applicativo, estendendo l'analisi sia al contenuto sia al modo in cui sono state implementate e ai loro effetti pratici. Il controllo giurisdizionale dovrà tener conto, pertanto, di tutti i fattori disciplinati nel regolamento, tra cui, per esempio, la presenza di codici di condotta o sistemi di certificazione, i quali possono offrire utili elementi di valutazione ai fini dell'assolvimento dell'onere probatorio che grava sul titolare.

3 Sulla definizione di costi di attuazione cfr. anche le "Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita", pubblicate il 20 ottobre 2020, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf

4 Cfr. rt. 32, comma 2, lett. c)

Per i motivi già menzionati, in merito alla questione della ripartizione dell'onere della prova in caso di violazione dei dati personali, l'Avvocato Generale della Corte UE afferma che spetta al titolare l'onere di provare l'adeguatezza delle misure adottate. Ciò è in linea con quanto previsto dal Regolamento, il quale assegna al titolare non solo il compito di adottare politiche e attuare misure adeguate per garantire che il trattamento dei dati personali effettuato sia conforme alla normativa, ma anche l'onere di comprovarne la conformità. Pertanto, dovrà dimostrare di aver dato effettivamente attuazione alle previsioni normative e in che modo, anche documentando il processo decisionale e i criteri su cui ha basato le valutazioni effettuate, in virtù del principio dell'accountability.

Inoltre, l'Avvocato Pitruzzella specifica che sarebbe eccessivamente difficile far incombere questo onere sull'interessato, il quale non possiede né le conoscenze né i mezzi sufficienti per effettuare questo tipo di dimostrazione.

Dunque, la valutazione dell'adeguatezza svolta dal titolare del trattamento, strettamente correlata al requisito dell'efficacia, dovrà essere fatta caso per caso e il titolare del trattamento assumerà le proprie determinazioni sulla base della situazione concreta tenendo conto altresì, come già detto, dei concetti di probabilità e gravita dei trattamenti rispetto ai diritti e le libertà degli interessati.

Alla luce della rilevanza che assume la figura del titolare del trattamento, in qualità di centro di responsabilità a cui imputare le operazioni del trattamento compiute, nel caso in cui si verifichi una violazione dei dati personali, egli non può considerarsi mai esonerato *a priori* dalla responsabilità, neppure quando la divulgazione dei dati sia stata causata da soggetti terzi, esterni alla sfera di controllo del titolare.

Questo perché il concetto di titolare del trattamento serve a determinare chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Solo nel caso in cui dimostri che, ai sensi dell'art. 82, comma 3, "l'evento dannoso non gli è in alcun modo imputabile" il titolare può considerarsi esonerato dalla responsabilità.

vedi l'articolo online

3. Il risarcimento del danno morale in caso di violazione dei dati personali

Altra questione rilevante emergente dalla controversia oggetto d'esame è quella riguardante la risarcibilità a favore di un soggetto titolare dei dati del danno morale consistente nel timore di un eventuale futuro uso improprio dei propri dati.

In via preliminare, occorre precisare che alcune disposizioni del GDPR riconoscono espressamente, accanto al danno materiale, il danno immateriale come una delle possibili conseguenze di una violazione dei dati personali che potrebbe provocare l'insorgere del diritto al risarcimento[5].

Da questo primo rilievo, possiamo rilevare come la normativa sulla protezione dei dati personali non sia soggetta ad alcun automatismo e ciò emerge sotto un duplice profilo:

(i) In primo luogo, non ogni violazione di dati personali provoca automaticamente un danno, come è stato confermato anche da una recente pronuncia della Cassazione (Cass. n. 16402/2021), laddove si è ritenuto che una violazione delle prescrizioni in materia di dati personali non determini necessariamente una lesione ingiustificabile del diritto. La Cassazione ha chiarito che il danno non patrimoniale derivante da una violazione della normativa in materia di protezione dei dati personali, pur determinando una lesione di un diritto fondamentale, è considerato risarcibile soltanto qualora si accerti la "gravità della lesione" e la "serietà del danno". Anche per tale diritto opera, infatti, la regola di tolleranza della lesione minima (corollario del principio di solidarietà ex art. 2 Costituzione). Difatti, qualsiasi violazione di una norma in materia di protezione dei dati personali può generare una reazione negativa dell'interessato. Tuttavia, tale violazione assume rilevanza ai fini del risarcimento del danno solo quando offende in maniera sensibile la portata del diritto violato. Pertanto, non è sufficiente la mera lesione di un interesse tutelato per la configurazione del danno da violazione dei dati personali, ma è necessario che essa determini delle conseguenze pregiudizievoli nella sfera personale del danneggiato.

(ii) In secondo luogo, il danno da violazione del diritto alla protezione dei dati personali non è risarcibile *in re ipsa*. Difatti, l'Avvocato Generale della Corte UE pone l'accento sulla differenza tra un danno immateriale risarcibile e altri generali svantaggi e disagi che l'inosservanza di una norma di legge possono provocare in un soggetto titolare di diritti. Si tratta di una differenza molto sottile, che si deve comprendere non sotto il profilo della gravità - in quanto un danno morale risarcibile non deve essere necessariamente particolarmente grave - né dell'effettività, in quanto anche un danno meramente potenziale, come in questo caso l'uso improprio dei propri dati personali, è risarcibile seppur non effettivo. Ciò che rileva è piuttosto l'elemento della oggettività insita nel danno morale provocato dalla violazione dei dati, in quanto sono gli elementi concreti che rendono il danno, seppur consistente in un mero timore, comprovabile, non essendo sufficienti le mere percezioni soggettive e personali di un individuo. Spetterà poi all'interessato raccogliere elementi concreti che possano condurre alla configurabilità di un danno morale effettivamente subito.

Pertanto, la soluzione giuridica proposta dall'Avvocato alla Corte dell'Unione è stata quella di riconoscere la possibilità del risarcimento del danno morale - inteso come timore di un potenziale e futuro uso improprio dei propri dati personali - in linea con quanto affermato nell'art. 82, comma 1 del GDPR, purché l'interessato sia in grado di dimostrare l'effettiva sussistenza di un danno emotivo, reale e certo. Il diritto al risarcimento non si configura infatti laddove si tratti di mere inquietudini, ansie e timori di scarsa entità, derivate da percezioni soggettive, mutevoli e dipendenti anche da elementi caratteriali e personali. Una volta provata la serietà della lesione patita dal trattamento illecito, l'interessato dovrà anche dimostrare il nesso di causalità tra il danno e la violazione subita, in quanto il risarcimento verrà riconosciuto solo laddove la persona fisica abbia subito un danno come conseguenza della violazione stessa. L'accertamento di fatto è comunque rimesso al giudice di merito e resta ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale.

5 Art. 82, comma 1, Reg. Ue n. 679/2016: "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*". Cfr. inoltre considerando 85, primo periodo, in cui si afferma che: "*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata*".

4. Conclusioni

In conclusione, è evidente l'importanza nel sistema della protezione dei dati personali dell'attività del titolare del trattamento rivolta a tutelare i dati personali degli interessati dai rischi connessi al trattamento degli stessi. Il titolare dovrà, quindi, fare un'attenta valutazione di ogni elemento utile ai fini della predisposizione delle misure tecniche ed organizzative idonee a prevenire i rischi connessi al trattamento, tenendo conto che dovrà essere in grado di provare tale adeguatezza nel caso in cui si verifichino comunque violazioni di dati personali.

È importante ribadire che la valutazione dell'adeguatezza delle misure, sia da parte del titolare del trattamento, sia da parte del giudice nazionale, dovrà essere sempre svolta da un punto di vista concreto, sulla base degli elementi indicati negli artt. 24 e 32 del Regolamento 679/2016.

Pertanto, in caso di violazione dei dati personali da parte di un soggetto terzo esterno alla sfera di controllo del titolare, il quale abbia avuto accesso e/o divulgato dati personali, l'onere della prova sarà così ripartito: (i) al titolare del trattamento spetterà provare l'adeguatezza delle misure tecniche e organizzative adottate nonché la non imputabilità dell'evento dannoso; (ii) mentre l'interessato, dopo aver provato che si è verificata una violazione e che si è verificato un danno, materiale o immateriale che sia, sempre sulla base di elementi certi e reali, dovrà dimostrare il nesso di causalità tra la violazione ed il danno.

Inoltre, nel caso in cui il danno subito dall'interessato abbia natura di danno immateriale, consistente in meri timori e preoccupazioni di lesioni future ai propri dati personali, è possibile per lo stesso richiedere e ottenere il risarcimento, sempre che sia in grado di dimostrare che questo danno, anche se meramente emotivo, sia oggettivamente reale e certo.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it