# Dati personali. La Corte di Giustizia si pronuncia sull'esonero eventuale dalla responsabilità del titolare del trattamento in caso di violazione commessa da terzi

18/12/2023

DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, CONTENZIOSO

Marco Stillo

In data 14 dicembre 2023, la Corte di Giustizia dell'Unione Europea si è pronunciata nella Causa C-340/21, *VB contro Natsionalna agentsia za prihodite*, sull'interpretazione dell'articolo 5, paragrafo 2, degli articoli 24 e 32, nonché dell'articolo 82, paragrafi da 1 a 3, del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (*General Data Protection Regulation*, GDPR)[1].

Tale domanda era stata presentata nell'ambito di una controversia tra VB e la *Natsionalna agentsia za prihodite* (Agenzia nazionale bulgara per le entrate pubbliche, NAP) in merito al risarcimento del danno immateriale che tale persona sosteneva di aver subito a causa di una presunta violazione, da parte di quest'ultima, dei suoi obblighi legali in qualità di titolare del trattamento dei dati personali.

Questi i fatti.

In data 15 luglio 2019, i media avevano rivelato che, in seguito ad un attacco *hacker*, i dati personali di oltre 6 milioni di persone contenuti nel sistema

[1] GUUE L 119 del 04.05.2016.

informatico della NAP erano stati pubblicati su *internet*. Di conseguenza, VB aveva proposto dinanzi all'*Administrativen sad Sofia-grad* (Tribunale amministrativo della città di Sofia) un ricorso diretto ad ottenere che la NAP le versasse la somma pari a circa 510 euro a titolo di risarcimento del danno immateriale derivante da una violazione di dati personali. Poiché, tuttavia, tale ricorso era stato respinto, VB aveva adito il *Varhoven administrativen sad* (Corte suprema amministrativa; il "giudice del rinvio") che, alla luce della necessità di interpretare la normativa europea rilevante in materia, aveva deciso di sospendere il procedimento e di sottoporre alla Corte di Giustizia cinque questioni pregiudiziali.

Con la prima questione, il giudice del rinvio si chiedeva se gli articoli 24[2] e 32[3] del GDPR debbano essere interpretati nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di "terzi", ai sensi dell'articolo 4, punto 10[4], di tale regolamento, siano sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento di cui trattasi non fossero "adeguate" ai sensi di tali articoli 24 e 32.

La Corte ha preliminarmente ricordato che gli articoli 24 e 32 del GDPR si limitano ad imporre al titolare del trattamento di adottare misure tecniche e organizzative destinate ad evitare, per quanto possibile, qualsiasi violazione di dati personali, la cui adeguatezza deve essere valutata in concreto esaminando se esse siano state attuate tenendo conto dei diversi criteri ivi previsti, delle esigenze di protezione dei dati specificamente inerenti al trattamento in questione nonché ai rischi indotti da quest'ultimo. Di conseguenza, tali articoli non possono essere intesi nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di un terzo siano

[2] L'articolo 24 GDPR, intitolato "Responsabilità del titolare del trattamento", dispone: "*... Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*
*Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento...*".

[3] L'articolo 32 GDPR, intitolato "Sicurezza del trattamento", ai paragrafi 1-2 dispone: "*... 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, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali;*
*b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
*c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
*d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*
*Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati...*".

[4] L'articolo 4 GDPR, intitolato "Definizioni", al punto 10 dispone: "*... Ai fini del presente regolamento s'intende per:*
*(...)*
*10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile...*".

sufficienti per concludere che le misure adottate dal titolare del trattamento in questione non erano appropriate, senza neppure consentire a quest'ultimo di fornire la prova contraria. L'articolo 24 del GDPR, infatti, prevede espressamente che il titolare del trattamento deve essere in grado di dimostrare la conformità a tale regolamento delle misure da esso attuate, possibilità di cui sarebbe privato se fosse ammessa una presunzione assoluta.

Con la seconda questione, il giudice del rinvio chiedeva se l'articolo 32 del GDPR debba essere interpretato nel senso che l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento, ai sensi di tale articolo, debba essere valutata dai giudici nazionali in concreto, in particolare tenendo conto dei rischi connessi al trattamento di cui trattasi.

La Corte ha preliminarmente ricordato che l'adeguatezza delle misure tecniche e organizzative che il titolare o il responsabile del trattamento devono attuare deve essere valutata in due tempi. Da un lato, occorre individuare i rischi di violazione dei dati personali indotti dal trattamento in questione e le loro eventuali conseguenze per i diritti e le libertà delle persone fisiche, prendendo in considerazione il grado di probabilità dei rischi individuati e il loro grado di gravità. Dall'altro lato, occorre verificare se le misure siano adeguate a tali rischi, tenuto conto dello stato dell'arte, dei costi di attuazione nonché della natura, della portata, del contesto e delle finalità di tale trattamento. Di conseguenza, sebbene il titolare del trattamento disponga di un certo margine di discrezionalità per determinare le misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza adeguato al rischio, come richiesto dall'articolo 32, paragrafo 1, del GDPR, un giudice nazionale deve poter valutare la complessa ponderazione effettuata da quest'ultimo e, in tal modo, assicurarsi che le misure adottate siano idonee a garantire un tale livello di sicurezza, tenendo conto delle circostanze proprie del caso concreto nonché degli elementi di prova di cui egli dispone.

Con la prima parte della terza questione, il giudice del rinvio chiedeva se il principio di responsabilità del titolare del trattamento, enunciato all'articolo 5, paragrafo 2[5], del GDPR e concretizzato all'articolo 24 di quest'ultimo, debba essere interpretato nel senso che, nell'ambito di un'azione di risarcimento fondata sull'articolo 82[6] di tale

[5] L'articolo 5 GDPR, intitolato "Principi applicabili al trattamento di dati personali", al paragrafo 2 dispone: "*... Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)...*".

[6] L'articolo 82 GDPR, intitolato "Diritto al risarcimento e responsabilità", dispone: "*... 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.*
*Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*
*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.*
*Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.*
*Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del*

regolamento, al titolare del trattamento in questione incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'articolo 32.

Secondo la Corte, dal disposto dell'articolo 5, paragrafo 2, dell'articolo 24, paragrafo 1, e dell'articolo 32, paragrafo 1, del GDPR risulta che l'onere di provare che i dati personali sono trattati in modo tale da garantire una loro adeguata sicurezza incombe al titolare del trattamento in questione[7]. Questi tre articoli, pertanto, enunciano una regola di applicazione generale, che occorre, in mancanza di indicazione contraria nel GDPR, applicare anche nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento.

Con la seconda parte della terza questione, invece, il giudice del rinvio chiedeva se l'articolo 32 del GDPR e il principio di effettività del diritto dell'Unione debbano essere interpretati nel senso che, al fine di valutare l'adeguatezza delle misure di sicurezza che il titolare del trattamento ha attuato ai sensi di tale articolo, una perizia giudiziaria costituisce un mezzo di prova necessario e sufficiente.

La Corte ha preliminarmente ricordato che il GDPR non stabilisce norme relative all'ammissione e al valore probatorio di un mezzo di prova, quale una perizia giudiziaria, che devono essere applicate dai giudici nazionali investiti di un'azione di risarcimento danni basata sull'articolo 82 di tale regolamento e incaricati di valutare, alla luce dell'articolo 32 dello stesso, l'adeguatezza delle misure di sicurezza attuate dal responsabile del trattamento in questione. Di conseguenza, e in mancanza di norme del diritto dell'Unione in materia, spetta all'ordinamento giuridico di ciascuno Stato Membro stabilire le modalità delle azioni intese a garantire la tutela dei diritti spettanti ai singoli in forza di detto articolo 82 e, in particolare, le norme inerenti ai mezzi di prova che consentono di valutare l'adeguatezza di tali misure, fatto salvo il rispetto dei principi di equivalenza e di effettività[8].

Tutto ciò premesso, una norma procedurale nazionale in forza della quale sarebbe sistematicamente necessario che i giudici nazionali disponessero una perizia giudiziaria potrebbe contrastare con il principio di effettività. Il ricorso sistematico ad una tale perizia, infatti, può rivelarsi superfluo alla luce delle altre prove detenute dal giudice adito, in particolare dei risultati di un controllo del rispetto delle misure di protezione dei dati personali effettuato da un'autorità indipendente e stabilita per legge, poiché tali misure, conformemente all'articolo 24, paragrafo 1, del GDPR, devono essere riesaminate e aggiornate se necessario.

Con la quarta questione, il giudice del rinvio chiedeva se l'articolo 82, paragrafo 3, del GDPR debba essere interpretato nel senso che il titolare del trattamento è esonerato dal suo obbligo di risarcire il danno subito da una persona, ai sensi dell'articolo 82, paragrafi 1 e 2, di tale regolamento, per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di "terzi", ai sensi dell'articolo 4, punto 10, di detto regolamento.

---

*trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.*
*Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2...*".

[7] CGUE 04.07.2023, Causa C-252/21, *Meta Platforms e a. (Condizioni generali di utilizzo di un social network)*, punto 95; CGUE 04.05.2023, Causa C-60/22, *Bundesrepublik Deutschland (Casella di posta elettronica degli uffici giudiziari)*, punti 52-53.

[8] CGUE 04.05.2023, Causa C-300/21, *Österreichische Post (Danno inerente al trattamento di dati personali)*, punto 54; CGUE 21.06.2022, Causa C-817/19, *Ligue des droits humains*, punto 297.

La Corte ha preliminarmente ricordato che, da un lato, il responsabile del trattamento in questione deve in linea di principio risarcire un danno causato da una violazione del GDPR connessa a tale trattamento e che, dall'altro, egli può essere esonerato dalla sua responsabilità solo se fornisce la prova che il fatto che ha provocato tale danno non gli è in alcun modo imputabile. Le circostanze in cui il titolare del trattamento può pretendere di essere esonerato dalla responsabilità civile in cui incorre ai sensi dell'articolo 82 del GDPR, pertanto, devono essere strettamente limitate a quelle in cui egli è in grado di dimostrare, da parte sua, la mancanza di imputabilità del danno, di talché qualora, come nel caso concreto, una violazione di dati personali sia stata commessa da criminali informatici, e quindi da "terzi" ai sensi dell'articolo 4, punto 10, del regolamento, tale violazione non può essere imputata al titolare del trattamento, a meno che quest'ultimo non l'abbia resa possibile violando un obbligo previsto dal regolamento stesso, ed in particolare quello di protezione dei dati cui è tenuto in forza degli articoli 24 e 32.

Con la quinta questione, infine, il giudice del rinvio chiedeva se l'articolo 82, paragrafo 1, del GDPR debba essere interpretato nel senso che il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento possa, di per sé, costituire un "danno immateriale", ai sensi di tale disposizione.

La Corte ha preliminarmente ricordato che l'esistenza di un danno subito costituisce una delle condizioni del diritto al risarcimento previsto dall'articolo 82, paragrafo 1, del GDPR, al pari dell'esistenza di una violazione di quest'ultimo e di un nesso di causalità tra tale danno e tale violazione, essendo queste tre condizioni cumulative[9]. L'articolo 82, paragrafo 1, del GDPR, inoltre, osta ad una norma o a una prassi nazionale che subordina il risarcimento di un danno immateriale alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità[10].

Tutto ciò premesso, l'articolo 82, paragrafo 1, del GDPR non opera una distinzione tra fattispecie in cui, a seguito di una violazione accertata di disposizioni di tale regolamento, il danno immateriale lamentato dall'interessato è collegato, da un lato, ad un utilizzo abusivo da parte di terzi dei suoi dati personali che si è già prodotto, alla data della sua domanda di risarcimento, o, dall'altro, alla paura percepita da tale persona che un siffatto utilizzo possa prodursi in futuro. La formulazione di tale articolo, pertanto, non esclude che la nozione di "danno immateriale" ivi contenuta comprenda una situazione, come quella del caso concreto, in cui l'interessato invoca, al fine di ottenere un risarcimento sulla base di tale disposizione, il suo timore che i suoi dati personali siano oggetto di un futuro utilizzo abusivo da parte di terzi, a causa della violazione di tale regolamento che si è verificata.

Di conseguenza, la Corte ha statuito che:

"*Gli articoli 24 e 32 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) devono essere interpretati nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di «terzi», ai sensi dell'articolo 4, punto 10, di tale regolamento, non sono sufficienti, di per sé, per ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento in questione non fossero «adeguate», ai sensi di tali articoli 24 e 32.*

[9] CGUE 04.05.2023, Causa C-300/21, *Österreichische Post (Danno inerente al trattamento di dati personali)*, punto 32.
[10] *Ibidem*, punto 51.

*L'articolo 32 del regolamento 2016/679 dev'essere interpretato nel senso che l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento ai sensi di tale articolo deve essere valutata dai giudici nazionali in concreto, tenendo conto dei rischi connessi al trattamento di cui trattasi e valutando se la natura, il contenuto e l'attuazione di tali misure siano adeguati a tali rischi.*

*Il principio di responsabilità del titolare del trattamento, enunciato all'articolo 5, paragrafo 2, del regolamento 2016/679 e concretizzato all'articolo 24 di quest'ultimo, deve essere interpretato nel senso che nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento, al titolare del trattamento di cui trattasi incombe l'onere di dimostrare l'adeguatezza delle misure di sicurezza da esso attuate ai sensi dell'articolo 32 di detto regolamento.*

*L'articolo 32 del regolamento 2016/679 e il principio di effettività del diritto dell'Unione devono essere interpretati nel senso che al fine di valutare l'adeguatezza delle misure di sicurezza che il titolare del trattamento ha attuato ai sensi di tale articolo, una perizia giudiziaria non può costituire un mezzo di prova sistematicamente necessario e sufficiente.*

*L'articolo 82, paragrafo 3, del regolamento 2016/679 deve essere interpretato nel senso che il titolare del trattamento non può essere esonerato dal suo obbligo di risarcire il danno subito da una persona, ai sensi dell'articolo 82, paragrafi 1 e 2, di tale regolamento, per il solo fatto che tale danno deriva da una divulgazione non autorizzata di dati personali o da un accesso non autorizzato a tali dati da parte di «terzi», ai sensi dell'articolo 4, punto 10, di detto regolamento, dato che tale responsabile deve allora dimostrare che il fatto che ha provocato il danno in questione non gli è in alcun modo imputabile.*

*L'articolo 82, paragrafo 1, del regolamento 2016/679 deve essere interpretato nel senso che il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione di tale regolamento può, di per sé, costituire un «danno immateriale», ai sensi di tale disposizione*".


Marco Stillo

**ASSOCIATE**

m.stillo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles



MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com