SENTENZA DELLA CORTE (Terza Sezione)

14 dicembre 2023

«Rinvio pregiudiziale – Protezione delle persone fisiche con riguardo al trattamento dei dati personali – Regolamento (UE) 2016/679 – Articolo 5 – Principi relativi a tale trattamento – Articolo 24 – Responsabilità del titolare del trattamento – Articolo 32 – Misure adottate per garantire la sicurezza del trattamento – Valutazione dell'adeguatezza di tali misure – Portata del sindacato giurisdizionale – Assunzione delle prove – Articolo 82 – Diritto al risarcimento e responsabilità – Esonero eventuale dalla responsabilità del titolare del trattamento in caso di violazione commessa da terzi – Domanda di risarcimento di un danno immateriale fondata sul timore di un potenziale utilizzo abusivo di dati personali»

Nella causa C-340/21,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Varhoven administrativen sad (Corte suprema amministrativa, Bulgaria), con decisione del 14 maggio 2021, pervenuta in cancelleria il 2 giugno 2021, nel procedimento

VB

contro

Natsionalna agentsia za prihodite,

LA CORTE (Terza Sezione),

composta da K. Jürimäe, presidente di sezione, N. Piçarra, M. Safjan, N. Jääskinen (relatore) e M. Gavalec, giudici,

avvocato generale: G. Pitruzzella

cancelliere: A. Calot Escobar

vista la fase scritta del procedimento,

considerate le osservazioni presentate:

– per la Natsionalna agentsia za prihodite, da R. Spetsov;

– per il governo bulgaro, da M. Georgieva e L. Zaharieva, in qualità di agenti;

– per il governo ceco, da O. Serdula, M. Smolek e J. Vláčil, in qualità di agenti;

– per l'Irlanda, da M. Browne, Chief State Solicitor, A. Joyce, J. Quaney e M. Tierney, in qualità di agenti, assistiti da D. Fennelly, BL;

– per il governo italiano, da G. Palmieri, in qualità di agente, assistita da E. De Bonis, avvocato dello Stato;

– per il governo portoghese, da P. Barros da Costa, A. Pimenta, J. Ramos e C. Vieira Guerra, in qualità di agenti;

– per la Commissione europea, da A. Bouchagiar, H. Kranenborg e N. Nikolova, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 27 aprile 2023,

ha pronunciato la seguente

Sentenza

1 La domanda di pronuncia pregiudiziale verte 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 (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1; in prosieguo: il «RGPD»).

2 Tale domanda è stata presentata nell'ambito di una controversia tra VB, una persona fisica, e la Natsionalna agentsia za prihodite (Agenzia nazionale per le entrate pubbliche, Bulgaria) (in prosieguo: la «NAP») in merito al risarcimento del danno immateriale che tale persona sostiene di aver subito a causa di una presunta violazione da parte di tale autorità pubblica dei suoi obblighi legali in qualità di titolare del trattamento dei dati personali.

Contesto normativo

3 I considerando 4, 10, 11, 74, 76, 83, 85 e 146 del RGPD sono così formulati:

«4) (...) Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla [Carta dei diritti fondamentali dell'Unione europea], sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, (...) il diritto a un ricorso effettivo e a un giudice imparziale (...)

(...)

10 Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione [europea], il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. (...)

11 Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, (...)

(...)

74 È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

(...)

76 La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del

trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

(...)

83 Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

(...)

85 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. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo (...)

(...)

146 Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. 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. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito (...)».

4 L'articolo 4 di tale regolamento, intitolato «Definizioni», dispone quanto segue:

«Ai fini del presente regolamento si intende per:

1) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); (...)

2) "trattamento": qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati o insiemi di dati personali (...);

(...)

7) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; (...)

(...)

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;

(...)

12) "violazione dei dati personali" la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

(...)».

5 L'articolo 5 del medesimo regolamento, rubricato «Principi applicabili al trattamento di dati personali», prevede quanto segue:

«1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

(...)

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")».

6 L'articolo 24 del medesimo regolamento, rubricato «Responsabilità del titolare del trattamento», prevede quanto segue:

«1. 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.

2. 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.

3. 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».

7 L'articolo 32 del RGPD, rubricato «Sicurezza del trattamento», prevede quanto segue:

«1. 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.

2. 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.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

(...)».

8 L'articolo 79 di detto regolamento, intitolato «Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento», al paragrafo 1 così recita:

«Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento».

9 L'articolo 82 di detto regolamento, intitolato «Diritto al risarcimento e responsabilità», ai paragrafi da 1 a 3 così recita:

«1. Chiunque subisca un danno materiale o 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.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. (...)

3. 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».

Procedimento principale e questioni pregiudiziali

10 La NAP è un'autorità collegata al Ministro delle Finanze bulgaro. Nell'ambito dei suoi compiti, consistenti, tra l'altro, nell'identificazione, nella salvaguardia e nel recupero dei crediti pubblici, essa è titolare del trattamento di dati personali, ai sensi dell'articolo 4, punto 7, del RGPD.

11 Il 15 luglio 2019 i media hanno rivelato che aveva avuto luogo un accesso non autorizzato al sistema informatico della NAP e che, in seguito a tale attacco hacker, taluni dati personali contenuti in detto sistema erano stati pubblicati su internet.

12 Più di sei milioni di persone fisiche, di nazionalità bulgara o straniera, sono state interessate da tali eventi. Alcune centinaia di esse, tra cui la ricorrente nel procedimento principale, hanno proposto,

contro la NAP, azioni di risarcimento dei danni morali che sarebbero derivati dalla divulgazione dei loro dati personali.

13 È in tale contesto che la ricorrente nel procedimento principale ha proposto dinanzi all'Administrativen sad Sofia-grad (Tribunale amministrativo della città di Sofia, Bulgaria) un ricorso diretto ad ottenere che la NAP le versasse la somma di 1 000 leva bulgari (BGN) (circa EUR 510) a titolo di risarcimento danni, sulla base dell'articolo 82 del RGPD e di disposizioni del diritto bulgaro. A sostegno di tale domanda, essa ha sostenuto di aver subito un danno immateriale derivante da una violazione di dati personali, ai sensi dell'articolo 4, punto 12, del RGPD, più in particolare una violazione della sicurezza che sarebbe stata causata da una violazione della NAP degli obblighi ad essa incombenti in forza, in particolare, dell'articolo 5, paragrafo 1, lettera f), nonché degli articoli 24 e 32 di tale regolamento. Il suo danno immateriale 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.

14 A sua difesa, la NAP, anzitutto, ha fatto valere che la ricorrente nel procedimento principale non le aveva chiesto informazioni relative ai dati precisi che erano stati divulgati. La NAP ha poi prodotto documenti volti a dimostrare di aver adottato tutte le misure necessarie, a monte, per prevenire la violazione dei dati personali contenuti nel suo sistema informatico nonché, a valle, per limitare gli effetti di tale violazione e per rassicurare i cittadini. Inoltre, secondo la NAP, non esisteva alcun nesso di causalità tra il danno immateriale lamentato e detta violazione. Infine, essa ha sostenuto che, avendo a sua volta subito un danno doloso da parte di persone che non erano suoi dipendenti, non può essere considerata responsabile delle relative conseguenze dannose.

15 Con decisione del 27 novembre 2020, l'Administrativen sad Sofia-grad (Tribunale amministrativo della città di Sofia) ha respinto il ricorso della ricorrente nel procedimento principale. Tale giudice ha ritenuto, da un lato, che l'accesso non autorizzato alla banca dati della NAP derivasse da una pirateria informatica commessa da terzi e, dall'altro, che la ricorrente nel procedimento principale non avesse dimostrato l'inerzia della NAP quanto all'adozione di misure di sicurezza. Inoltre, essa ha ritenuto che tale ricorrente non avesse subito un danno immateriale tale da far sorgere il diritto al risarcimento.

16 La ricorrente nel procedimento principale ha proposto ricorso per cassazione avverso detta decisione dinanzi al Varhoven administrativen sad (Corte suprema amministrativa, Bulgaria), giudice del rinvio nella presente causa. A sostegno della sua impugnazione, essa sostiene che il giudice di primo grado ha commesso un errore di diritto nella ripartizione dell'onere della prova relativo alle misure di sicurezza adottate dalla NAP e che quest'ultima non ha dimostrato la sua assenza di inerzia al riguardo. Inoltre, la ricorrente nel procedimento principale sostiene che il timore di possibili utilizzi abusivi dei suoi dati personali nel futuro costituisce un danno immateriale reale, e non ipotetico. A sua difesa, la NAP contesta ciascuno di tali argomenti.

17 Il giudice del rinvio considera, anzitutto, la possibilità che la constatazione della sopravvenienza di una violazione di dati personali consenta, di per sé, di concludere che le misure attuate dal titolare del trattamento di tali dati non erano «adeguate», ai sensi degli articoli 24 e 32 del RGPD.

18 Tuttavia, nell'ipotesi in cui tale constatazione fosse insufficiente per giungere a una siffatta conclusione, esso si interroga, da un lato, sulla portata del controllo che i giudici nazionali devono effettuare per valutare l'adeguatezza delle misure di cui trattasi e, dall'altro, sulle norme relative all'assunzione delle prove che devono applicarsi in tale contesto, con riguardo sia all'onere della prova sia ai mezzi di prova, in particolare quando tali giudici sono aditi per un'azione di risarcimento fondata sull'articolo 82 di tale regolamento.

19 Detto giudice intende poi sapere se, alla luce dell'articolo 82, paragrafo 3, di detto regolamento, il fatto che la violazione di dati personali risulti da un atto commesso da terzi, nel caso di specie da un attacco informatico, costituisca un fattore che esonera sistematicamente il titolare del trattamento di tali dati dalla sua responsabilità per il danno causato all'interessato.

20 Infine, detto giudice si chiede se il timore provato da una persona che i suoi dati personali possano essere oggetto di un utilizzo abusivo in futuro, nel caso di specie a seguito di un accesso non autorizzato agli stessi e della loro divulgazione da parte di criminali informatici, possa, di per sé, costituire un «danno immateriale», ai sensi dell'articolo 82, paragrafo 1, del RGPD. In caso affermativo, tale persona sarebbe dispensata dal dimostrare che terzi hanno compiuto, anteriormente alla sua domanda di risarcimento, un uso illecito di tali dati, quale un'usurpazione della sua identità.

21 Alla luce di tali circostanze, il Varhoven administrativen sad (Corte suprema amministrativa) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se gli articoli 24 e 32 del [RGPD] debbano essere interpretati nel senso che è sufficiente che abbia avuto luogo una divulgazione o un accesso non autorizzati ai dati personali, ai sensi dell'articolo 4, punto 12, del [RGPD], da parte di persone che non sono dipendenti dell'amministrazione del titolare del trattamento e non sono soggette al suo controllo, per ritenere che le misure tecniche e organizzative adottate non siano adeguate.

2) In caso di risposta negativa alla prima questione, quale debba essere l'oggetto e la portata del controllo giurisdizionale di legittimità nell'esame dell'adeguatezza delle misure tecniche e organizzative adottate dal titolare del trattamento ai sensi dell'articolo 32 del [RGPD].

3) In caso di risposta negativa alla prima questione, se il principio di responsabilità di cui agli articoli 5, paragrafo 2, e 24 [del RGPD], in combinato disposto con il considerando 74 di tale regolamento, debba essere interpretato nel senso che, in un procedimento giudiziario conformemente all'articolo 82, paragrafo 1, del citato regolamento, incombe sul titolare del trattamento l'onere di provare che le misure tecniche e organizzative sono adeguate ai sensi dell'articolo 32 del [RGPD].

Se una perizia possa essere considerata un mezzo di prova necessario e sufficiente per determinare se le misure tecniche e organizzative adottate dal titolare del trattamento, in un caso come quello di specie, fossero adeguate, qualora l'accesso e la divulgazione non autorizzati di dati personali siano conseguenza di un "attacco hacker".

4) Se l'articolo 82, paragrafo 3, del [RGPD] debba essere interpretato nel senso che la divulgazione o l'accesso non autorizzati a dati personali ai sensi dell'articolo 4, paragrafo 12, di tale regolamento che, come nel caso di specie, ha avuto luogo mediante un "attacco hacker" da parte di persone che non sono dipendenti dell'amministrazione del titolare del trattamento e che non sono soggette al suo controllo configura un evento che non è in alcun modo imputabile a quest'ultimo e che gli consente di essere esonerato dalla responsabilità.

5) Se l'articolo 82, paragrafi 1 e 2, del [RGPD], in combinato disposto con i considerando 85 e 146 di tale regolamento, debba essere interpretato nel senso che, in un caso come quello di specie, in cui ha avuto luogo una compromissione della protezione dei dati personali, verificatasi sotto forma dell'accesso non autorizzato e nella diffusione di dati personali mediante un "attacco hacker", le sole inquietudini e ansie e i soli timori provati dalla persona interessata in merito ad un eventuale futuro uso improprio dei dati personali rientrino nella nozione di danno immateriale, che deve essere interpretata estensivamente, e facciano sorgere il diritto al risarcimento, qualora tale uso improprio non sia stato accertato e/o la persona interessata non abbia subito alcun ulteriore danno».

Sulle questioni pregiudiziali

Sulla prima questione

22 Con la sua prima questione, il giudice del rinvio si chiede, in sostanza, se gli articoli 24 e 32 del RGPD 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, 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.

23 In limine, si deve ricordare che, per giurisprudenza costante, i termini di una disposizione del diritto dell'Unione, che, al pari degli articoli 24 e 32 del RGPD, non contenga alcun rinvio espresso al diritto degli Stati membri al fine di determinare il suo significato e la sua portata, devono di norma dar luogo, in tutta l'Unione, ad un'interpretazione autonoma e uniforme, da effettuarsi tenendo conto, segnatamente, dei termini di tale disposizione, degli obiettivi che essa persegue e del contesto in cui si inserisce [v., in tal senso, sentenze del 18 gennaio 1984, Ekro, 327/82, EU:C:1984:11, punto 11; del 1º ottobre 2019, Planet49, C-673/17, EU:C:2019:801, punti 47 e 48, nonché del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punto 29].

24 In primo luogo, per quanto riguarda la formulazione delle disposizioni pertinenti, occorre rilevare che l'articolo 24 del RGPD prevede un obbligo generale, gravante sul titolare del trattamento di dati personali, di attuare misure tecniche e organizzative adeguate per garantire che detto trattamento sia effettuato conformemente a tale regolamento, e di poterlo dimostrare.

25 A tal fine, detto articolo 24 elenca, al suo paragrafo 1, un certo numero di criteri da prendere in considerazione per valutare l'adeguatezza di siffatte misure, vale a dire la natura, l'ambito di applicazione, il contesto e le finalità del trattamento nonché i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Tale disposizione aggiunge che dette misure sono riesaminate e aggiornate qualora necessario.

26 In tale prospettiva, l'articolo 32 del RGPD precisa gli obblighi del titolare del trattamento e di un eventuale responsabile del trattamento in merito alla sicurezza di tale trattamento. In tal senso, il paragrafo 1 di tale articolo dispone che questi ultimi devono attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato ai rischi menzionati al punto precedente della presente sentenza, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del contesto e delle finalità del trattamento di cui trattasi.

27 Parimenti, il paragrafo 2 di detto articolo enuncia che, nel valutare l'adeguato livello di sicurezza, si deve tener 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 non autorizzato, in modo accidentale o illegale, a dati personali.

28 Inoltre, sia l'articolo 24, paragrafo 3, di detto regolamento, sia l'articolo 32, paragrafo 3, di esso indicano che il titolare del trattamento o il responsabile del trattamento possono dimostrare di aver rispettato i requisiti dei rispettivi paragrafi 1 di tali articoli basandosi sul fatto che applicano un codice di condotta approvato o un meccanismo di certificazione approvato, come previsto agli articoli 40 e 42 di detto regolamento.

29 Il riferimento, contenuto nell'articolo 32, paragrafi 1 e 2, del RGPD, a «un livello di sicurezza adeguato al rischio» e a un «adeguato livello di sicurezza» dimostra che tale regolamento istituisce un regime di gestione dei rischi e che esso non pretende affatto di eliminare i rischi di violazione dei dati personali.

30 Pertanto, dal tenore letterale degli articoli 24 e 32 del RGPD risulta che tali disposizioni 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. L'adeguatezza di siffatte misure deve essere valutata in concreto, esaminando se tali misure siano state attuate da detto responsabile tenendo conto dei diversi criteri previsti dai menzionati articoli e delle esigenze di protezione dei dati specificamente inerenti al trattamento di cui trattasi nonché ai rischi indotti da quest'ultimo.

31 Pertanto, gli articoli 24 e 32 del RGPD 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 sufficienti per concludere che le misure adottate dal titolare del trattamento di cui trattasi non erano appropriate, ai sensi di tali disposizioni, senza neppure consentire a quest'ultimo di fornire la prova contraria.

32 Una siffatta interpretazione si impone a maggior ragione in quanto l'articolo 24 del RGPD 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.

33 In secondo luogo, elementi di ordine contestuale e teleologico corroborano tale interpretazione degli articoli 24 e 32 del RGPD.

34 Per quanto riguarda, da una parte, il contesto in cui si inseriscono questi due articoli, occorre rilevare che dall'articolo 5, paragrafo 2, del RGPD risulta che il titolare del trattamento deve essere in grado di dimostrare di aver rispettato i principi relativi al trattamento dei dati personali enunciati al paragrafo 1 di detto articolo. Tale obbligo è ripreso e precisato all'articolo 24, paragrafi 1 e 3, nonché all'articolo 32, paragrafo 3, di tale regolamento, con riguardo all'obbligo di attuare misure tecniche e organizzative per proteggere tali dati in occasione del trattamento effettuato da tale titolare. Orbene, un siffatto obbligo di dimostrare l'adeguatezza di tali misure non avrebbe senso se il titolare del trattamento fosse obbligato ad impedire qualsiasi danno di detti dati.

35 Inoltre, il considerando 74 del RGPD sottolinea che è importante che il titolare del trattamento sia tenuto ad attuare misure adeguate ed efficaci e sia in grado di dimostrare la conformità delle attività di trattamento con tale regolamento, compresa l'efficacia delle misure, le quali dovrebbero tener conto dei criteri, connessi alle caratteristiche del trattamento in questione e al rischio presentato da quest'ultimo, che sono altresì enunciati ai suoi articoli 24 e 32.

36 Del pari, secondo il considerando 76 di tale regolamento, la probabilità e la gravità del rischio dipendono dalle specificità del trattamento in questione e tale rischio dovrebbe essere oggetto di una valutazione obiettiva.

37 Inoltre, dall'articolo 82, paragrafi 2 e 3, del RGPD risulta che, se è pur vero che il titolare del trattamento è responsabile del danno causato dal trattamento che costituisce una violazione di tale regolamento, esso è tuttavia esonerato dalla sua responsabilità se prova che il fatto che ha provocato il danno non gli è in alcun modo imputabile.

38 D'altra parte, l'interpretazione sviluppata al punto 31 della presente sentenza è supportata anche dal considerando 83 del RGPD, il quale afferma, nella sua prima frase, che «[per] mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi». Così facendo, il legislatore dell'Unione ha manifestato la sua intenzione di «limitare» i rischi di violazione dei dati personali, senza affermare che sarebbe possibile eliminarli.

39 Alla luce dei motivi che precedono, occorre rispondere alla prima questione dichiarando che gli articoli 24 e 32 del RGPD 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.

Sulla seconda questione

40 Con la sua seconda questione, il giudice del rinvio chiede, in sostanza, se l'articolo 32 del RGPD 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.

41 A tale proposito, occorre ricordare che, come sottolineato nel contesto della risposta alla prima questione, l'articolo 32 del RGPD impone al titolare del trattamento e al responsabile del trattamento, a seconda dei casi, di attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dei criteri di valutazione di cui al paragrafo 1 dello stesso. Inoltre, il paragrafo 2 di tale articolo elenca, in modo non esaustivo, una serie di fattori rilevanti per valutare il livello di sicurezza adeguato ai rischi presentati dal trattamento in questione.

42 Da detto articolo 32, paragrafi 1 e 2, risulta che l'adeguatezza di siffatte misure tecniche e organizzative deve essere valutata in due tempi. Da un lato, occorre individuare i rischi di violazione dei dati personali indotti dal trattamento di cui trattasi e le loro eventuali conseguenze per i diritti e le libertà delle persone fisiche. Tale valutazione deve essere effettuata in concreto, prendendo in considerazione il grado di probabilità dei rischi individuati e il loro grado di gravità. Dall'altro lato, occorre verificare se le misure attuate dal titolare del trattamento 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.

43 È vero che il titolare del trattamento dispone 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 RGPD. Ciò non toglie che un giudice nazionale deve poter valutare la complessa ponderazione effettuata dal titolare del trattamento e, in tal modo, assicurarsi che le misure adottate da quest'ultimo siano idonee a garantire un siffatto livello di sicurezza.

44 Una siffatta interpretazione è peraltro idonea a garantire, da un lato, l'effettività della protezione dei dati personali evidenziata dai considerando 11 e 74 di tale regolamento e, dall'altro, il diritto a un ricorso giurisdizionale effettivo nei confronti di un titolare del trattamento, quale tutelato dall'articolo 79, paragrafo 1, di detto regolamento, in combinato disposto con il considerando 4 del medesimo regolamento.

45 Pertanto, per controllare l'adeguatezza di misure tecniche e organizzative attuate ai sensi dell'articolo 32 del RGPD, un giudice nazionale deve non limitarsi a constatare in che modo il titolare del trattamento interessato abbia inteso adempiere gli obblighi ad esso incombenti in forza di tale articolo, bensì effettuare un esame di tali misure nel merito, alla luce di tutti i criteri menzionati in detto articolo nonché delle circostanze proprie del caso di specie e degli elementi di prova di cui tale giudice dispone al riguardo.

46 Un siffatto esame richiede di procedere a un'analisi concreta sia della natura e del contenuto delle misure che sono state attuate dal titolare del trattamento, del modo in cui tali misure sono state applicate e dei loro effetti pratici sul livello di sicurezza che quest'ultimo era tenuto a garantire, tenuto conto dei rischi inerenti a tale trattamento.

47 Di conseguenza, occorre rispondere alla seconda questione dichiarando che l'articolo 32 del RGPD deve 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.

Sulla terza questione

Sulla prima parte della terza questione

48 Con la prima parte della sua terza questione, il giudice del rinvio chiede, in sostanza, se il principio di responsabilità del titolare del trattamento, enunciato all'articolo 5, paragrafo 2, del RGPD 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 di tale 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 di detto regolamento.

49 A tal riguardo, occorre, in primo luogo, ricordare che l'articolo 5, paragrafo 2, del RGPD sancisce un principio di responsabilità, in forza del quale il titolare del trattamento è responsabile del rispetto dei principi relativi al trattamento dei dati personali enunciati al paragrafo 1 di tale articolo, e prevede che detto titolare deve essere in grado di dimostrare che tali principi sono rispettati.

50 In particolare, il titolare del trattamento deve, conformemente al principio di integrità e di riservatezza dei dati personali enunciato all'articolo 5, paragrafo 1, lettera f), di tale regolamento, provvedere affinché tali dati siano trattati in modo da garantirne un'adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante misure tecniche o organizzative adeguate e deve essere in grado di dimostrare che tale principio è rispettato.

51 Occorre altresì rilevare che sia l'articolo 24, paragrafo 1, del RGPD, letto alla luce del considerando 74 di quest'ultimo, sia l'articolo 32, paragrafo 1, di tale regolamento impongono al titolare del trattamento, con riguardo a qualsiasi trattamento di dati personali effettuato da lui stesso o per suo conto, di mettere in atto misure tecniche e organizzative adeguate per assicurarsi ed essere in grado di dimostrare che il trattamento è effettuato conformemente a detto regolamento.

52 Dal disposto dell'articolo 5, paragrafo 2, dell'articolo 24, paragrafo 1, e dell'articolo 32, paragrafo 1, del RGPD risulta senza ambiguità che l'onere di provare che i dati personali sono trattati in modo tale da garantire una loro adeguata sicurezza ai sensi dell'articolo 5, paragrafo 1, lettera f), e dell'articolo 32 di detto regolamento incombe al titolare del trattamento in parola [v., per analogia, sentenze del 4 maggio 2023, Bundesrepublik Deutschland (Casella di posta elettronica degli uffici giudiziari), C-60/22, EU:C:2023:373, punti 52 e 53, nonché del 4 luglio 2023, Meta Platforms e a. (Condizioni generali di utilizzo di un social network), C-252/21, EU:C:2023:537, punto 95].

53 Questi tre articoli enunciano quindi una regola, di applicazione generale, che occorre, in mancanza di indicazione contraria nel RGPD, applicare anche nell'ambito di un'azione di risarcimento fondata sull'articolo 82 di tale regolamento.

54 In secondo luogo, va notato che la suddetta interpretazione letterale è supportata dalla considerazione degli obiettivi perseguiti dal RGPD.

55 Da un lato, poiché il livello di protezione di cui al RGPD dipende dalle misure di sicurezza adottate dai titolari del trattamento di dati personali, questi ultimi devono essere indotti, sopportando l'onere di dimostrare l'adeguatezza di tali misure, a fare tutto il possibile per prevenire operazioni di trattamento non conformi a tale regolamento.

56 Dall'altro lato, se si dovesse ritenere che l'onere della prova riguardo all'adeguatezza di dette misure gravi sugli interessati, come definiti all'articolo 4, punto 1, del RGPD, ne conseguirebbe che

il diritto al risarcimento previsto all'articolo 82, paragrafo 1, di quest'ultimo sarebbe privato di gran parte del suo effetto utile, mentre il legislatore dell'Unione ha inteso rafforzare sia i diritti di tali persone sia gli obblighi dei titolari del trattamento, rispetto alle disposizioni anteriori a tale regolamento, come indicato dal considerando 11 di quest'ultimo.

57 Occorre quindi rispondere alla prima parte della terza questione dichiarando che il principio di responsabilità del titolare del trattamento, enunciato all'articolo 5, paragrafo 2, del RGPD 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.

Sulla seconda parte della terza questione

58 Con la seconda parte della sua terza questione, il giudice del rinvio chiede, in sostanza, se l'articolo 32 del RGPD 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.

59 A tal riguardo, occorre ricordare che, conformemente a una giurisprudenza costante, in mancanza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro stabilire le modalità procedurali dei ricorsi giurisdizionali destinati a garantire la salvaguardia dei diritti dei singoli, in forza del principio di autonomia processuale, a condizione tuttavia che tali modalità non siano meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano in pratica impossibile o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività) [sentenza del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punto 53].

60 Nel caso di specie, occorre rilevare che il RGPD 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 interessato. Pertanto, conformemente con quanto ricordato al punto precedente, della presente sentenza 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 in siffatto contesto, fatto salvo il rispetto dei suddetti principi di equivalenza e di effettività [v., per analogia, sentenze del 21 giugno 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, punto 297, nonché del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punto 54].

61 Nel presente procedimento, la Corte non dispone di alcun elemento tale da suscitare dubbi sul rispetto del principio di equivalenza. Diverso è il caso della conformità al principio di effettività, nei limiti in cui la formulazione stessa della seconda parte della terza questione presenta il ricorso a una perizia giudiziaria come un «mezzo di prova necessario e sufficiente».

62 In particolare, 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. Infatti, il ricorso sistematico a una siffatta perizia può rivelarsi superfluo alla luce delle altre prove detenute dal giudice adito, in particolare, come indicato dal governo bulgaro

nelle sue osservazioni scritte, alla luce dei risultati di un controllo del rispetto delle misure di protezione dei dati personali effettuato da un'autorità indipendente e stabilita per legge, purché tale controllo sia recente, poiché dette misure, conformemente all'articolo 24, paragrafo 1, del RGPD, devono essere riesaminate e aggiornate se necessario.

63 Inoltre, come rilevato dalla Commissione europea nelle sue osservazioni scritte, il principio di effettività potrebbe essere violato nell'ipotesi in cui il termine «sufficiente» dovesse essere inteso nel senso che un giudice nazionale deve dedurre esclusivamente o automaticamente da una perizia giudiziaria che le misure di sicurezza attuate dal titolare del trattamento in questione sono «adeguate», ai sensi dell'articolo 32 del RGPD. Orbene, la salvaguardia dei diritti conferiti da tale regolamento, cui è diretto il principio di effettività, e, in particolare, il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento, garantito dall'articolo 79, paragrafo 1, dello stesso, richiedono che un giudice imparziale effettui una valutazione obiettiva dell'adeguatezza delle misure in questione, anziché limitarsi a tale deduzione (v., in tal senso, sentenza del 12 gennaio 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, punto 50).

64 Alla luce dei motivi che precedono, occorre rispondere alla seconda parte della terza questione dichiarando che l'articolo 32 del RGPD 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.

Sulla quarta questione

65 Con la sua quarta questione, il giudice del rinvio chiede, in sostanza, se l'articolo 82, paragrafo 3, del RGPD 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.

66 In via preliminare, occorre precisare che dall'articolo 4, punto 10, del RGPD risulta che hanno la qualità di «terzi», in particolare, le persone diverse da quelle che, poste sotto l'autorità diretta del titolare del trattamento o del responsabile del trattamento, sono autorizzate a trattare i dati personali. Tale definizione comprende persone che non sono dipendenti del titolare del trattamento e non sono sotto il controllo di quest'ultimo, come quelle di cui alla questione sollevata.

67 Occorre poi ricordare, in primo luogo, che l'articolo 82, paragrafo 2, del RGPD dispone che «[u]n titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi [tale] regolamento» e che il paragrafo 3 di tale articolo prevede che il titolare del trattamento, o il responsabile del trattamento, a seconda dei casi, è esonerato da tale responsabilità «se dimostra che l'evento dannoso non gli è in alcun modo imputabile».

68 Inoltre, il considerando 146 del RGPD, che si riferisce specificamente all'articolo 82 di quest'ultimo, enuncia, alla prima frase, che «[i] l titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni che una persona può subire a causa di un trattamento non conforme [a tale] regolamento» e «dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile».

69 Da tali disposizioni risulta, da un lato, che il responsabile del trattamento di cui trattasi deve in linea di principio risarcire un danno causato da una violazione di tale regolamento connessa a tale trattamento e, dall'altro, che 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.

70 Pertanto, come rivela l'aggiunta espressa dell'espressione «in alcun modo» nel corso del procedimento legislativo, 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 RGPD devono essere strettamente limitate a quelle in cui tale titolare è in grado di dimostrare, da parte sua, la mancanza di imputabilità del danno.

71 Qualora, come nel caso di specie, una violazione di dati personali, ai sensi dell'articolo 4, punto 12, del RGPD, sia stata commessa da criminali informatici, e quindi da «terzi», ai sensi dell'articolo 4, punto 10, di tale regolamento, tale violazione non può essere imputata al titolare del trattamento, a meno che quest'ultimo non abbia reso possibile detta violazione violando un obbligo previsto dal RGPD, e in particolare l'obbligo di protezione dei dati cui è tenuto in forza dell'articolo 5, paragrafo 1, lettera f), e degli articoli 24 e 32 del medesimo regolamento.

72 Pertanto, in caso di violazione di dati personali commessa da un terzo, il titolare del trattamento può esimersi dalla propria responsabilità, sulla base dell'articolo 82, paragrafo 3, del RGPD, dimostrando che non sussiste alcun nesso di causalità tra la sua eventuale violazione dell'obbligo di protezione dei dati e il danno subito dalla persona fisica.

73 In secondo luogo, l'interpretazione che precede di tale articolo 82, paragrafo 3, è altresì conforme all'obiettivo del RGPD consistente nel garantire un livello elevato di protezione delle persone fisiche con riguardo al trattamento dei loro dati personali, enunciato ai considerando 10 e 11 di tale regolamento.

74 Alla luce di tutte le suesposte considerazioni, occorre rispondere alla quarta questione dichiarando che l'articolo 82, paragrafo 3, del RGPD 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.

Sulla quinta questione

75 Con la sua quinta questione, il giudice del rinvio chiede, in sostanza, se l'articolo 82, paragrafo 1, del RGPD 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.

76 Per quanto riguarda, in primo luogo, la formulazione dell'articolo 82, paragrafo 1, del RGPD, occorre osservare che quest'ultimo prevede che «[c]hiunque 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».

77 A questo proposito, la Corte ha affermato che dalla formulazione dell'articolo 82, paragrafo 1, del RGPD emerge chiaramente che l'esistenza di un «danno» «subito» costituisce una delle condizioni del diritto al risarcimento previsto da tale disposizione, al pari dell'esistenza di una violazione di tale regolamento e di un nesso di causalità tra tale danno e tale violazione, essendo queste tre condizioni cumulative [sentenza del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punto 32].

78 Inoltre, basandosi su considerazioni di ordine al contempo letterale, sistematico e teleologico, la Corte ha interpretato l'articolo 82, paragrafo 1, del RGPD nel senso che esso osta a una norma o a una prassi nazionale che subordina il risarcimento di un «danno immateriale», ai sensi di tale

disposizione, alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità [sentenza del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punto 51].

79 Ciò premesso, occorre sottolineare, nel caso di specie, che l'articolo 82, paragrafo 1, del RGPD 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, da un lato, è collegato a 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, è collegato alla paura percepita da tale persona che un siffatto utilizzo possa prodursi, in futuro.

80 Pertanto, la formulazione dell'articolo 82, paragrafo 1, del RGPD non esclude che la nozione di «danno immateriale» contenuta in tale disposizione comprenda una situazione, come quella considerata dal giudice del rinvio, 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.

81 Tale interpretazione letterale è corroborata, in secondo luogo, dal considerando 146 del RGPD, che verte specificamente sul diritto al risarcimento previsto all'articolo 82, paragrafo 1, di quest'ultimo e che menziona, alla sua seconda frase, che «[i]l concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo da rispecchiare pienamente gli obiettivi» di tale regolamento. Orbene, un'interpretazione della nozione di «danno immateriale», ai sensi di detto articolo 82, paragrafo 1, che non includa le situazioni in cui l'interessato da una violazione di detto regolamento fa valere il timore che i suoi dati personali siano oggetto di utilizzo abusivo in futuro non risponderebbe a una concezione ampia di tale nozione, quale intesa dal legislatore dell'Unione [v., per analogia, sentenza del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punti 37 e 46].

82 Inoltre, il considerando 85, prima frase, del RGPD indica che «[u]na 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, (...) o qualsiasi altro danno economico o sociale significativo» Da tale elenco esemplificativo dei «danni» che possono essere subiti dagli interessati risulta che il legislatore dell'Unione ha inteso includere in tali nozioni, in particolare, la semplice «perdita di controllo» sui loro dati, a seguito di una violazione di tale regolamento, quand'anche un utilizzo abusivo dei dati di cui trattasi non si sia verificato concretamente a danno di dette persone.

83 In terzo e ultimo luogo, l'interpretazione esposta al punto 80 della presente sentenza è supportata dagli obiettivi del RGPD, che devono essere presi pienamente in considerazione nel definire la nozione di «danno», come indicato nella seconda frase del considerando 146 di tale regolamento. Orbene, un'interpretazione dell'articolo 82, paragrafo 1, del RGPD secondo la quale la nozione di «danno immateriale», ai sensi di tale disposizione, non includerebbe le situazioni in cui un interessato si avvale unicamente del suo timore che i suoi dati siano oggetto di un utilizzo abusivo da parte di terzi, in futuro, non sarebbe conforme alla garanzia di un livello elevato di protezione delle persone fisiche con riguardo al trattamento dei dati personali all'interno dell'Unione, cui si riferisce tale strumento.

84 Tuttavia, occorre sottolineare che una persona interessata da una violazione del RGPD, che abbia subito conseguenze negative, è tenuta a dimostrare che tali conseguenze costituiscono un danno immateriale, ai sensi dell'articolo 82 di tale regolamento [v., in tal senso, sentenza del 4 maggio 2023, Österreichische Post (Danno inerente al trattamento di dati personali), C-300/21, EU:C:2023:370, punto 50].

85 In particolare, qualora una persona che chiede un risarcimento su tale base invochi il timore che in futuro si verifichi un utilizzo abusivo dei suoi dati personali a causa dell'esistenza di una siffatta violazione, il giudice nazionale adito deve verificare che tale timore possa essere considerato fondato, nelle circostanze specifiche di cui trattasi e nei confronti dell'interessato.

86 Alla luce dei motivi che precedono, occorre rispondere alla quinta questione dichiarando che l'articolo 82, paragrafo 1, del RGPD 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.

Sulle spese

87 Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Terza Sezione) dichiara:

1) 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.

2) 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.

3) 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.

4) 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.

5) 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.

6) 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.

Firme