Edizione provvisoria

CONCLUSIONI DELL'AVVOCATO GENERALE
GIOVANNI PITRUZZELLA
presentate il 27 aprile 2023(1)

Causa C-340/21

VB
contro
Natsionalna agentsia za prihodite

[domanda di pronuncia pregiudiziale proposta dal Varhoven administrativen sad (Corte suprema amministrativa, Bulgaria)]

«Rinvio pregiudiziale – Protezione dei dati personali – Regolamento (UE) 2016/679 – Responsabilità del titolare del trattamento – Sicurezza del trattamento – Violazione della sicurezza del trattamento dei dati personali – Danno morale subito a causa dell'inerzia del titolare del trattamento – Azione risarcitoria»

L'illecita diffusione di dati personali detenuti da un'agenzia pubblica, a causa di un attacco pirata, può dar luogo al risarcimento del danno morale a favore di un soggetto titolare dei dati per il solo fatto che quest'ultimo abbia il timore di un eventuale futuro uso improprio dei propri dati? Quali sono i criteri di imputabilità della responsabilità al titolare del trattamento? Come sono ripartiti gli oneri probatori all'interno del giudizio? Quale l'ampiezza dello scrutinio del giudice?

I. Contesto normativo

1. L'articolo 4, rubricato «Definizioni», del regolamento 2016/679 (2) (in prosieguo: il «Regolamento») dispone:

«Ai fini del presente regolamento si intende per

(...)

(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

(...)».

2. L'articolo 5, intitolato «Principi applicabili al trattamento di dati personali» recita:

«1. I dati personali sono:

(…)

(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")».

3. L'articolo 24 del medesimo regolamento, rubricato «Responsabilità del titolare del trattamento», stabilisce:

«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».

4. L'articolo 32, rubricato «Sicurezza del trattamento», prevede:

«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:

(…)

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.

(…)».

5. L'articolo 82 del medesimo regolamento, intitolato «Diritto al risarcimento e responsabilità» dispone:

«1. 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.

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».

II. Fatti, procedimento e questioni pregiudiziali

6. In data 15 luglio 2019 i media bulgari diffondevano la notizia che si fosse verificato un accesso non autorizzato al sistema informatico della Natsionalna agentsia za prihodite (Agenzia nazionale delle entrate, Bulgaria, in prosieguo: la «NAP» (3)) e che differenti informazioni fiscali e previdenziali di milioni di persone, sia cittadini che stranieri, fossero state pubblicate su internet.

7. Numerose persone, tra cui VB, ricorrente nel procedimento principale, convenivano quindi in giudizio la NAP per ottenere il risarcimento dei danni morali.

8. Nel caso di specie, la ricorrente di cui al procedimento principale adiva l'Administrativen sad Sofia-grad (Tribunale amministrativo della città di Sofia, Bulgaria; in prosieguo: l'«ASSG»), sostenendo che la NAP avesse violato le norme nazionali, nonché l'obbligo di trattare i dati personali in qualità di titolare del trattamento in modo da «garantire idonei standard di sicurezza» mediante l'adozione di adeguate misure tecniche ed organizzative, ai sensi degli articoli 24 e 32 del regolamento n. 679/2016. La ricorrente affermava poi di aver subito un danno morale, manifestatosi sotto forma di apprensioni e timori per un futuro uso improprio dei suoi dati personali.

9. La controparte sottolineava, invece, di non aver ricevuto alcuna richiesta dalla ricorrente nel procedimento principale con l'indicazione dei dati personali che esattamente fossero stati oggetto di accesso. Inoltre, a seguito della notizia dell'intrusione avrebbe convocato dei vertici con gli esperti a tutela dei diritti e degli interessi dei cittadini. Secondo la NAP mancava inoltre un nesso di causalità tra l'attacco informatico ed il danno asseritamente lamentato, avendo l'agenzia implementato tutti i sistemi di gestione delle procedure e quelli per la sicurezza delle informazioni, conformemente alle norme internazionali vigenti in materia.

10. Il giudice di primo grado, l'ASSG, rigettava la domanda, ritenendo che la diffusione dei dati non fosse imputabile all'agenzia, che l'onere della prova sull'adeguatezza delle misure adottate gravasse sulla ricorrente e, infine, che nessun danno morale fosse risarcibile.

11. La sentenza di primo grado veniva poi impugnata con ricorso dinanzi al Varhoven administrativen sad (Corte suprema amministrativa, Bulgaria). Tra i rilievi avanzati, la ricorrente nel procedimento principale sottolineava che il giudice di primo grado avesse errato nel ripartire l'onere della prova rispetto alla mancata adozione delle misure di sicurezza. Neppure, il danno morale dovrebbe costituire oggetto di onere della prova, dal momento che si tratta di un danno morale effettivo e non meramente potenziale.

12. La NAP dal canto suo ribadiva di aver adottato le misure tecniche ed organizzative necessarie in qualità di titolare del trattamento e contestava l'esistenza della prova di un danno morale effettivo. L'ansia ed i timori, infatti, sarebbero degli stati emotivi non risarcibili.

13. Il giudice del rinvio constatava diversi esiti con riguardo ai singoli procedimenti che i danneggiati avevano distintamente iniziato contro la NAP per il risarcimento dei danni morali.

14. In tale contesto, il giudice del rinvio sospendeva il procedimento e sottoponeva alla Corte le seguenti questioni pregiudiziali:

«1) Se 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)] 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 medesimo regolamento, 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 regolamento (UE) 2016/679.

3) In caso di risposta negativa alla prima questione, se il principio di responsabilità di cui agli articoli 5, paragrafo 2, e 24 del regolamento (UE) 2016/679, 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 dello stesso regolamento. 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 regolamento (UE) 2016/679 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 regolamento (UE) 2016/679, 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 morale, 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».

III. Analisi giuridica

A. Osservazioni preliminari

15. La presente causa ha ad oggetto delle interessanti e, in parte, inedite questioni riguardanti l'interpretazione di diverse disposizioni del Regolamento (4).

16. Le cinque domande pregiudiziali ruotano tutte attorno alla medesima questione: le condizioni di risarcibilità del danno morale ad un soggetto i cui dati personali, in possesso di un'Agenzia pubblica, sono stati oggetto di pubblicazione su internet a seguito di un attacco hacker.

17. Per comodità espositiva proporrò sintetiche risposte separate a tutte le domande pregiudiziali dell'ordinanza di rinvio, pur consapevole di qualche sovrapposizione concettuale, dal momento che le prime quattro sono tutte mirate a identificare i presupposti per l'imputabilità della violazione delle disposizioni del Regolamento al titolare del trattamento (5) e la quinta riguarda più precisamente la nozione di danno morale ai fini del risarcimento (6).

18. Segnalo che sull'articolo 82 del Regolamento sono attualmente pendenti diverse cause presso la Corte e in una di queste sono già state lette le conclusioni dell'avvocato generale di cui terrò conto nella presente analisi (7).

19. Prima di esaminare le questioni sollevate, ritengo opportuna qualche considerazione preliminare su principi e finalità del Regolamento che tornerà utile per la soluzione delle singole questioni pregiudiziali.

20. L'articolo 24 del Regolamento stabilisce in termini generali l'obbligo, per il titolare del trattamento, di mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali sia conforme al Regolamento stesso e di essere in grado di dimostrarlo, mentre l'articolo 32 stabilisce più specificamente lo stesso obbligo per quanto riguarda la sicurezza del trattamento. Gli articoli 24 e 32 declinano in modo più specifico quanto già previsto dall'articolo 5, paragrafo 2, che introduce, proprio tra i «principi applicabili al trattamento dei dati personali», il «principio di responsabilizzazione». Esso segue logicamente ed è complementare al «principio di integrità e riservatezza» previsto dall'articolo 5, paragrafo 1, lettera f), ed entrambi vanno letti alla luce dell'approccio basato sul rischio su cui si fonda il Regolamento.

21. Il principio di responsabilizzazione è uno dei pilastri del Regolamento e una delle sue innovazioni più significative. Esso attribuisce al titolare del trattamento la responsabilità di intraprendere azioni proattive per garantire la conformità al Regolamento e di essere pronto a dimostrarla (8).

22. In dottrina si è parlato di un vero e proprio cambiamento culturale come effetto della «portata globale dell'obbligo di responsabilità» (9). Non è tanto il formale rispetto dell'obbligo legale o della misura puntuale quanto l'insieme della strategia aziendale adottata a esonerare il titolare da responsabilità perché *compliant* della disciplina di protezione dati.

23. Le misure tecniche e organizzative richieste dal principio di responsabilizzazione devono essere «adeguate» in considerazione dei fattori specificati nell'articolo 24: la natura, l'ambito di applicazione, il contesto e le finalità del trattamento e la probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche.

24. L'articolo 24 impone, pertanto, l'adeguatezza delle misure al fine di poter dimostrare la conformità del trattamento ai principi e alle disposizioni del Regolamento.

25. L'articolo 32 proietta, invece, il principio di responsabilizzazione sulle misure concrete da adottare per garantire «un livello di sicurezza adeguato al rischio». E nel far questo, aggiunge ai fattori già previsti di cui tenere conto nella predisposizione delle misure tecniche e organizzative, lo stato dell'arte e i costi di attuazione.

26. La nozione di adeguatezza richiede che le soluzioni adottate a garanzia dei sistemi informatici raggiungano un livello di accettabilità, sia in termini tecnici (pertinenza delle misure), che qualitativi (efficacia della protezione). Per garantire il rispetto dei principi di necessità, pertinenza e proporzionalità, i trattamenti devono essere, non solo idonei ma anche soddisfacenti rispetto alle finalità che si intendono perseguire. E in questa logica gioca un ruolo decisivo il principio di minimizzazione, in virtù del quale tutte le fasi del trattamento dei dati devono costantemente tendere alla riduzione al minimo dei rischi di sicurezza (10).

27. Tutto il Regolamento è improntato alla prevenzione del rischio e alla responsabilizzazione del titolare del trattamento e, dunque, a un approccio teleologico che miri al risultato migliore possibile in termini di efficacia, ben lontano cioè da logiche formalistiche connesse al mero obbligo di adempiere a specifiche procedure per liberarsi dalla responsabilità (11).

28. L'articolo 24 non contiene un'elencazione esaustiva di misure «adeguate»: si dovrà procedere ad una valutazione caso per caso. Ciò in linea con la filosofia del Regolamento che disvela come si sia preferito che le procedure da adottare siano scelte sulla base di attenta valutazione della situazione specifica in modo tale da potere essere il più possibile efficaci (12).

B. Prima questione pregiudiziale

29. Con la sua prima questione, il giudice del rinvio chiede, in sostanza, se gli articoli 24 e 32 del Regolamento debbano essere interpretati nel senso che il verificarsi di una «violazione dei dati personali», come definita all'articolo 4, paragrafo 12, sia di per sé sufficiente per concludere che le misure tecniche e organizzative attuate dal titolare del trattamento non erano «adeguate» a garantire la protezione dei dati.

30. Dal testo degli articoli 24 e 32 del Regolamento si evince che il titolare del trattamento, quando sceglie le misure tecniche e organizzative che è tenuto a mettere in atto per garantire la conformità al Regolamento stesso, deve tenere conto di una serie di fattori di valutazione elencati in tali articoli e sopra ricordati.

31. Il titolare del trattamento dispone di un certo margine di manovra per quanto riguarda la determinazione delle misure più appropriate alla luce della sua situazione specifica ma tale scelta è comunque soggetta a un eventuale controllo giurisdizionale della conformità delle misure applicate a tutti gli obblighi e alle finalità del Regolamento stesso.

32. In particolare, per quanto riguarda le misure di sicurezza, l'articolo 32, paragrafo 1, impone al titolare del trattamento di tenere conto dello «stato dell'arte». Ciò implica una limitazione del livello tecnologico di misure da attuare a ciò che è ragionevolmente possibile nel momento in cui le misure sono adottate: l'idoneità della misura a prevenire il rischio va cioè commisurata alle soluzioni che lo stato di avanzamento della scienza, della tecnica, della tecnologia e della ricerca attuali offre, anche in considerazione, come si vedrà, dei costi di attuazione.

33. Delle misure possono essere «adeguate» in un determinato momento e, nonostante questo, essere aggirate da criminali informatici che utilizzano strumenti molto sofisticati idonei a violare anche misure di sicurezza conformi allo stato dell'arte.

34. D'altro canto appare illogico ritenere che l'intenzione del legislatore dell'Unione fosse quella di imporre al titolare del trattamento l'obbligo di prevenire qualsiasi violazione dei dati personali, indipendentemente dalla diligenza nella predisposizione delle misure di sicurezza (13).

35. Come sopra detto, il Regolamento si muove in un'ottica lontana da automatismi, richiedendo un'elevata responsabilizzazione del titolare del trattamento che non può però portare all'impossibilità per quest'ultimo di dimostrare di aver correttamente adempiuto agli obblighi a lui imposti.

36. Inoltre, l'articolo 32, paragrafo 1, prevede che si tenga conto, come detto, dei «costi di attuazione» delle misure tecniche e organizzative in esame. Ne consegue che la valutazione dell'adeguatezza di tali misure deve basarsi su un bilanciamento tra gli interessi dell'interessato, che generalmente tendono a un livello di protezione più elevato, e gli interessi economici e la capacità tecnologica del titolare del trattamento, che talvolta tendono a un livello di protezione inferiore. Tale bilanciamento deve rispettare i requisiti del principio generale di proporzionalità.

37. A ciò va poi aggiunto, in un'ottica di interpretazione sistematica, che il legislatore contempla la possibilità che delle violazioni dei sistemi si verifichino; l'articolo 32, comma 1, lettera c), 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. La previsione tra le misure di sicurezza che garantiscono un livello di sicurezza adeguato al rischio di tale capacità sarebbe inutile se si ritenesse che la sola violazione dei sistemi rappresenti di per sé la prova dell'inadeguatezza delle misure stesse.

C. Seconda questione pregiudiziale

38. Con la seconda questione, il giudice del rinvio chiede, in sostanza, quale debba essere l'oggetto e la portata del controllo giurisdizionale, nel verificare l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento dei dati personali ai sensi dell'articolo 32 del Regolamento.

39. Data la variabilità delle situazioni che possono presentarsi nella pratica, il Regolamento, come detto, non stabilisce disposizioni vincolanti per la determinazione delle misure tecniche e organizzative che il titolare del trattamento deve adottare per soddisfare i requisiti del Regolamento stesso. L'adeguatezza delle misure adottate andrà dunque valutata in concreto, verificando se le specifiche misure siano state idonee a prevenire ragionevolmente il rischio e a minimizzare gli effetti negativi della violazione.

40. Se è senz'altro vero che la scelta e l'attuazione di tali misure rientra nella valutazione soggettiva del titolare del trattamento, poiché le misure menzionate nel Regolamento sono solo esempi, lo

scrutinio del giudice non può limitarsi al controllo dell'osservanza da parte del titolare del trattamento degli obblighi derivanti dagli articoli 24 e 32, cioè dell'avere (formalmente) previsto determinate misure tecniche e organizzative. Esso deve procedere a un'analisi concreta del contenuto di tali misure, del modo in cui sono state applicate e dei loro effetti pratici, sulla base degli elementi di prova di cui dispone e delle circostanze del caso specifico. Come efficacemente osservato dal governo portoghese «il modo in cui ha adempiuto ai suoi obblighi appare inseparabile dal contenuto delle misure adottate, al fine di dimostrare che, tenendo conto del trattamento specifico dei dati (la sua natura, la portata, il contesto e le finalità), dello stato dell'arte delle tecnologie disponibili e dei loro costi, nonché dei rischi per i diritti e le libertà dei cittadini, il titolare del trattamento ha adottato tutte le misure necessarie e appropriate per garantire un livello di sicurezza adeguato al rischio sottostante» (14).

41. Il controllo giurisdizionale dovrà tenere conto, pertanto, di tutti i fattori contenuti negli articoli 24 e 32 che, come detto, elencano una serie di criteri per valutare l'adeguatezza e forniscono esempi di misure che possono essere considerate adeguate. Inoltre, come sottolineato dalla Commissione e da tutti gli Stati membri che hanno presentato osservazioni sulla seconda domanda, l'articolo 32, paragrafi da 1 a 3, sottolinea la necessità di «garantire un livello di sicurezza adeguato al rischio», indicando altri fattori pertinenti a tal fine, come l'eventuale adozione da parte del titolare del trattamento di un codice di condotta approvato o di un sistema di certificazione approvato, come previsto rispettivamente dagli articoli 40 e 42 del Regolamento.

42. L'adozione di codici di condotta o di sistemi di certificazione può offrire un utile elemento di valutazione, ai fini dell'assolvimento dell'onere probatorio e del connesso controllo giurisdizionale. Con la precisazione però che al titolare del trattamento non è sufficiente aderire ad un codice di condotta ma egli ha l'onere di provare di aver adottato concretamente le misure che esso prevede, in conformità con il principio di responsabilizzazione. La certificazione, invece, costituisce «di per sé prova della conformità al regolamento dei trattamenti effettuati pur se suscettibile di essere smentita sul piano pratico» (15).

43. Da ultimo va osservato che tali misure devono essere riesaminate e aggiornate se necessario, ex articolo 24, paragrafo 1. E anche questo sarà oggetto di valutazione del giudice nazionale. L'articolo 32, paragrafo 1 del Regolamento (16), impone, infatti, a carico del titolare del trattamento, un onere di controllo e monitoraggio costante, preventivo e successivo rispetto alle attività di trattamento, ma anche di manutenzione e possibile aggiornamento delle misure adottate, allo scopo sia di prevenire le violazioni sia, eventualmente, di limitarne gli effetti.

44. Tenderei, tuttavia, ad escludere l'opportunità che la prossima sentenza includa un elenco di elementi sostanziali, come quello suggerito dal governo portoghese (17). Ciò potrebbe offrire spazio a interpretazioni contrastanti non potendo ovviamente l'elenco essere mai esaustivo.

D. Terza questione pregiudiziale

45. Con la prima parte della sua terza questione, il giudice del rinvio chiede in sostanza alla Corte di stabilire se, tenuto conto del principio di responsabilizzazione di cui all'articolo 5, paragrafo 2, e all'articolo 24, in combinato disposto con il considerando 74 (18), del Regolamento, nell'ambito di un'azione di risarcimento danni ai sensi dell'articolo 82, l'onere della prova sull'adeguatezza delle misure tecniche e organizzative ai sensi dell'articolo 32 incomba sul titolare del trattamento dei dati personali.

46. Le considerazioni svolte in precedenza mi consentono di rispondere sinteticamente a questa domanda in senso affermativo.

47. La lettera della legge, il contesto e le finalità del Regolamento depongono, infatti, in senso univoco verso l'onere della prova a carico del titolare del trattamento.

48. Dalla formulazione di diverse disposizioni del Regolamento si evince che il titolare del trattamento deve essere «in grado» o «capace» di «dimostrare» il rispetto degli obblighi previsti dal Regolamento e, in particolare, di aver attuato misure adeguate a tal fine, come indicato nel considerando 74, nell'articolo 5, paragrafo 2, e nell'articolo 24, paragrafo 1. Come sottolinea il

governo portoghese, il suddetto considerando 74 specifica che l'onere della prova così posto a carico del titolare deve comprendere la prova dell'«efficacia delle misure» in questione.

49. Questa interpretazione letterale mi sembra supportata dalle seguenti considerazioni pratiche e teleologiche.

50. Per quanto riguarda la ripartizione dell'onere della prova, nell'ambito di un'azione di risarcimento danni basata sull'articolo 82, l'interessato che ha promosso l'azione contro il titolare del trattamento deve provare, in primo luogo, che si è verificata una violazione del Regolamento, in secondo luogo, che ha subito un danno e, in terzo luogo, che esiste un nesso causale tra i due elementi precedenti, come è stato rilevato in tutte le osservazioni scritte sulla quinta questione pregiudiziale. Si tratta di tre condizioni cumulative, come risulta anche dalla giurisprudenza consolidata della Corte e del Tribunale, nel contesto della responsabilità extracontrattuale dell'Unione (19).

51. Tuttavia, ritengo che l'obbligo del ricorrente di dimostrare l'esistenza di una violazione del Regolamento non possa spingersi fino a richiedere di dimostrare come le misure tecniche e organizzative attuate dal titolare del trattamento non siano adeguate, ai sensi degli articoli 24 e 32.

52. Come sottolinea la Commissione, la presentazione di tali prove sarebbe spesso quasi impossibile nella pratica, poiché gli interessati non hanno generalmente né conoscenze sufficienti per poter analizzare tali misure, né accesso a tutte le informazioni in possesso del titolare del trattamento contestato, in particolare per quanto riguarda i metodi applicati per garantire la sicurezza di tale trattamento. Inoltre, il titolare del trattamento potrebbe talvolta sostenere che il suo rifiuto di rivelare questi fatti agli interessati si basa sul motivo legittimo di non rendere pubblici i propri affari interni, o anche elementi coperti da segreto professionale, tra l'altro proprio per motivi di sicurezza.

53. Pertanto, se si ritenesse che l'onere della prova spetti alla persona interessata, il risultato pratico sarebbe che il diritto di ricorso previsto dall'articolo 82, paragrafo 1, perderebbe gran parte della sua portata. A mio avviso, ciò non sarebbe in linea con le intenzioni del legislatore dell'UE, che, adottando questo Regolamento, ha cercato di rafforzare i diritti degli interessati e gli obblighi dei responsabili del trattamento, rispetto alla direttiva 95/46 che ha sostituito. È quindi più logico, e giuridicamente sostenibile, che il titolare del trattamento sia tenuto a dimostrare, nell'ambito della sua difesa da un'azione di risarcimento danni, di aver rispettato gli obblighi derivanti dagli articoli 24 e 32 di tale Regolamento adottando misure effettivamente adeguate.

54. Con la seconda parte della sua terza domanda, il giudice del rinvio chiede alla Corte, in sostanza, se una perizia giudiziaria possa essere considerata una prova necessaria e sufficiente per valutare l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento dei dati personali in una situazione in cui l'accesso e la divulgazione non autorizzati dei dati personali sono il risultato di un'attività di *hacking*.

55. Ritengo, come è stato sottolineato (nella sostanza) anche dai governi bulgaro e italiano, l'Irlanda e la Commissione, che la risposta a queste domande debba basarsi sulla nostra giurisprudenza consolidata secondo la quale, in base al principio dell'autonomia procedurale, in assenza di norme dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro disciplinare le modalità procedurali dei procedimenti giudiziari volti a tutelare i diritti delle persone, a condizione, tuttavia, che tali norme non siano, nelle situazioni disciplinate dal diritto dell'Unione, meno favorevoli di quelle che disciplinano situazioni analoghe soggette al diritto nazionale (principio di equivalenza) e non rendano impossibile nella pratica o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività).

56. Nel caso di specie, osservo che il Regolamento non contiene alcuna disposizione volta a determinare i metodi di prova ammissibili e il loro valore probatorio, in particolare per quanto riguarda gli atti istruttori (come una perizia) che i tribunali nazionali possono o devono ordinare per valutare se un titolare del trattamento dei dati personali abbia adottato misure adeguate ai sensi di tale Regolamento. Ritengo pertanto che, in assenza di norme armonizzate in materia, spetti all'ordinamento giuridico interno di ciascuno Stato membro determinare tali modalità procedurali, fermo restando il rispetto dei principi di equivalenza e di effettività.

57. Il suddetto «principio di effettività», che implica che un giudice indipendente deve effettuare una valutazione imparziale, potrebbe essere compromesso, se l'aggettivo «sufficiente» dovesse essere inteso nel senso che mi pare attribuirgli il giudice del rinvio e cioè di poter dedurre automaticamente da una perizia che le misure adottate dal titolare del trattamento sono adeguate (20).

E. Quarta questione pregiudiziale

58. Con la quarta questione, il giudice del rinvio chiede, in sostanza, se l'articolo 82, paragrafo 3, del Regolamento debba essere interpretato nel senso che, in caso di violazione di tale Regolamento (consistente, come nel caso di specie, nella «divulgazione non autorizzata» o nell'«accesso non autorizzato» a dati personali ai sensi dell'articolo 4, paragrafo 12) da parte di persone che non sono dipendenti del titolare del trattamento di tali dati e non sono sotto il controllo di quest'ultimo, ciò costituisce un evento che non è in alcun modo imputabile al titolare del trattamento, e quindi un motivo di esonero dalla sua responsabilità, ai sensi dell'articolo 82, paragrafo 3.

59. La risposta alla domanda discende linearmente da quanto sopra esposto sulla filosofia generale del Regolamento: non sono previsti automatismi e dunque il solo fatto che la divulgazione o l'accesso non autorizzati a dati personali ha avuto luogo a causa di soggetti fuori dalla sfera di controllo del titolare del trattamento non esonera da responsabilità quest'ultimo.

60. In primo luogo, in termini letterali, va notato che né l'articolo 82, paragrafo 3, né il considerando 146 stabiliscono particolari condizioni che possono essere soddisfatte affinché il titolare del trattamento sia esonerato dalla responsabilità, salvo dimostrare che «l'evento dannoso non gli è in alcun modo imputabile». Da questa formulazione si evince, da un lato, che il titolare del trattamento può essere esonerato dalla responsabilità solo se dimostra che l'evento che ha causato il danno in questione non gli è imputabile e, dall'altro, che il livello di prova richiesto da questa disposizione è elevato, dato l'uso del termine «in alcun modo», come ha sottolineato la Commissione (21).

61. Il regime di responsabilità previsto dall'articolo 82 e, più in generale dall'intero Regolamento, è stato oggetto di ampio dibattito nella dottrina dei diversi Stati membri. Esso, infatti, contiene elementi tradizionali propri della responsabilità extracontrattuale ma anche elementi che, nella struttura delle disposizioni, lo avvicinano alla responsabilità contrattuale o addirittura a una forma di responsabilità oggettiva, in ragione della intrinseca pericolosità dell'attività di trattamento dei dati. Non è questa la sede per dar conto dell'articolato dibattito ma, a mio parere, l'articolo 82 non sembra individuare un regime di responsabilità oggettiva (22).

62. Il danno da violazione dei dati personali può configurarsi quale conseguenza colposa della mancata adozione delle misure tecniche e organizzative ragionevoli e comunque adeguate a scongiurarlo, tenuto conto dei rischi per i diritti e le libertà delle persone connessi all'attività di trattamento. Tali rischi rendono l'obbligo di prevenire ed evitare il danno più rigoroso, ampliando il dovere di diligenza incombente sul titolare del trattamento. Pertanto, dalla lettura coordinata degli obblighi di condotta in capo ai titolari del trattamento e della previsione sulla prova liberatoria posta a carico del danneggiante, è possibile trarre argomento in favore del riconoscimento della natura di responsabilità aggravata per colpa presunta alla fattispecie di responsabilità da illecito trattamento di dati personali disegnata dall'articolo 82 del Regolamento (23).

63. Da ciò discende la possibilità per il titolare del trattamento di offrire una prova liberatoria (non consentita nella responsabilità oggettiva). Con riguardo all'articolazione dell'onere probatorio, l'articolo 82, paragrafo 3, del Regolamento detta un regime favorevole al danneggiato, disponendo una forma di inversione dell'onere della prova della colpa del danneggiante (24), in piena simmetria con la predetta inversione dell'onere della prova per quanto attiene all'adeguatezza delle misure adottate. Il legislatore mostra così di essere consapevole dei pericoli insiti nell'accoglimento di una diversa distribuzione dell'onere probatorio; che, ove ponesse a carico della persona fisica-danneggiata la prova della colpa del danneggiante, finirebbe col gravarne eccessivamente la posizione e dunque col compromettere, nei fatti, l'operatività della tutela risarcitoria, in un ambito di norme legate all'utilizzo delle nuove tecnologie. Potrebbe, infatti, risultare particolarmente oneroso per l'interessato ricostruire ed avere accesso alle modalità di produzione del danno e, conseguentemente, provare la colpa del

titolare. Al contrario, il titolare del trattamento si trova nella migliore posizione per offrire la prova liberatoria per dimostrare che l'evento dannoso non gli è in alcun modo imputabile (25).

64. Il titolare del trattamento dovrà anche dimostrare, in linea con il principio di responsabilizzazione sopra descritto, di aver fatto tutto il possibile per ripristinare tempestivamente la disponibilità e l'accesso dei dati personali.

65. Tornando alla domanda del giudice del rinvio, sulla base di quanto fin qui esposto sulla natura della responsabilità del titolare del trattamento, se, come detto, il titolare del trattamento può andare esente da responsabilità dimostrando che la violazione è dovuta a causa a lui in alcun modo imputabile, non può ritenersi tale il solo fatto che l'evento è stato causato da un soggetto fuori dalla sua sfera di controllo.

66. Quando un titolare del trattamento è vittima di un attacco da parte di criminali informatici l'evento che ha dato origine al danno potrebbe essere considerato non attribuibile al titolare del trattamento ma non è escluso che la negligenza del titolare del trattamento dei dati sia stata all'origine dell'attacco in questione, agevolandolo a causa dell'assenza o dell'inadeguatezza delle misure di sicurezza dei dati personali che quest'ultimo è tenuto ad attuare. Si tratta di valutazioni fattuali, specifiche per ogni caso, che sono lasciate al giudice nazionale adito, alla luce delle prove prodotte davanti a lui.

67. È poi esperienza comune che gli attacchi esterni ai sistemi di soggetti pubblici o privati titolari di una gran mole di dati personali sia di gran lunga più frequente degli attacchi interni. Il titolare del trattamento deve, pertanto, predisporre misure adeguate a fronteggiare in particolare gli attacchi esterni.

68. In ultimo luogo, da un punto di vista teleologico, va notato che il Regolamento persegue l'obiettivo di un elevato livello di protezione. A questo proposito, la Corte ha già sottolineato che dall'articolo 1, paragrafo 2, del Regolamento, letto in combinato disposto con i suoi considerando 10, 11 e 13, risulta che tale regolamento impone alle istituzioni agli organi, uffici e agenzie dell'Unione e alle autorità competenti degli Stati membri il compito di assicurare un livello elevato di tutela dei diritti relativi alla protezione dei dati personali garantiti dall'articolo 16 del TFUE e dall'articolo 8 della Carta (26).

69. Se la Corte dovesse optare per l'interpretazione secondo cui, quando la violazione del Regolamento è stata commessa da un terzo, il titolare del trattamento dovrebbe essere automaticamente esonerato dalla responsabilità ai sensi dell'articolo 82, paragrafo 3, una tale interpretazione avrebbe un effetto incompatibile con l'obiettivo di protezione perseguito da tale strumento, poiché indebolirebbe i diritti degli interessati, in quanto limiterebbe tale responsabilità ai casi in cui la violazione è dovuta a persone che sono sotto l'autorità e/o il controllo di tale titolare del trattamento.

F. Quinta questione pregiudiziale

70. Con la quinta questione, il giudice nazionale chiede alla Corte, in sostanza, di interpretare la nozione di «danno morale» (nel linguaggio del regolamento «immateriale») ai sensi dell'articolo 82 del Regolamento. In particolare, chiede di sapere se le disposizioni dell'articolo 82, paragrafi 1 e 2, del Regolamento, in combinato disposto con i considerando 85 e 146 dello stesso (27), debbano essere interpretate nel senso che, in una situazione in cui la violazione di tale regolamento consisteva nell'accesso non autorizzato a dati personali e nella divulgazione non autorizzata di tali dati da parte di criminali informatici, il fatto che l'interessato tema un potenziale uso improprio dei suoi dati personali in futuro possa costituire di per sé un danno (morale) che dà diritto a un risarcimento.

71. Né l'articolo 82 né i considerando relativi al risarcimento del danno forniscono una chiara risposta alla domanda ma da essi si possono trarre alcuni elementi utili per l'analisi: il danno immateriale (o morale) può essere oggetto di risarcimento in aggiunta a quello materiale (o patrimoniale); alla violazione del regolamento non consegue automaticamente il danno che da essa è «causato» o, più precisamente, la violazione dei dati personali «può provocare» danni fisici, materiali o immateriali alle persone fisiche; la nozione di danno dovrebbe essere interpretata «in senso lato» alla

luce della giurisprudenza della Corte, in modo tale da rispecchiare pienamente gli obiettivi del Regolamento; il risarcimento per il danno «subito» dovrebbe essere «pieno ed effettivo».

72. Il tenore letterale delle disposizioni del Regolamento già sgombra il campo da ogni possibile suggestione di danni *in re ipsa*: l'obiettivo principale della responsabilità civile prevista dal Regolamento è quello di dare soddisfazione all'interessato, proprio tramite un «pieno ed effettivo» risarcimento del danno subito e, dunque, ripristinare l'equilibrio della situazione giuridica modificata negativamente dalla violazione del diritto (28).

73. D'altro canto, anche sotto il profilo sistematico, come nel diritto antitrust, il Regolamento prevede due pilastri di tutela: uno di natura pubblicistica, con la previsione di sanzioni nel caso di violazioni delle disposizioni del Regolamento, uno di natura privatistica, prevedendo appunto una responsabilità civile di natura extracontrattuale, qualificabile come aggravata per colpa presunta con le caratteristiche, anche con riferimento alla prova liberatoria, sopra accennate (29).

74. Pertanto, un'interpretazione ampia(30) della nozione di danno (morale) non può spingersi a far ritenere che il legislatore abbia rinunciato alla necessità che un vero e proprio «danno» sia configurabile.

75. Il vero problema sostanziale è se, una volta accertata l'esistenza della violazione e del nesso causale, possa sorgere il diritto al risarcimento a causa di mere inquietudini, ansie e timori provati dalla persona interessata in merito ad un eventuale futuro uso improprio dei dati personali, qualora tale uso improprio non sia stato accertato e/o la persona interessata non abbia subito alcun ulteriore danno.

76. Secondo una giurisprudenza costante della Corte, alle nozioni di una disposizione di diritto dell'Unione, che non rinvia espressamente al diritto degli Stati membri per determinarne il senso e la portata, deve essere data, di norma, un'interpretazione autonoma e uniforme in tutta l'Unione, che deve essere ricercata tenendo conto del tenore letterale della disposizione in questione, del contesto in cui essa si colloca, degli obiettivi perseguiti dall'atto di cui fa parte e della genesi di tale disposizione (31).

77. La Corte, come ricordato dall'avvocato generale Campos Sánchez-Bordona (32), non ha elaborato una definizione generale di «danno» applicabile indistintamente in qualsiasi ambito (33). Per quanto attiene ai danni morali, dalla sua giurisprudenza può dedursi che: quando uno degli obiettivi della disposizione da interpretare è la protezione dell'individuo, o di una determinata categoria di individui (34), il concetto di danno deve essere ampio; coerentemente con tale criterio, il risarcimento si estende al danno immateriale, anche qualora esso non sia menzionato nella disposizione interpretata (35).

78. Sebbene la giurisprudenza della Corte autorizzi a sostenere che, nei termini sopra esposti, esiste nel diritto dell'Unione un principio di risarcimento del danno immateriale, sono d'accordo con l'avvocato generale Campos che non se ne possa dedurre una regola in base alla quale *ogni* danno immateriale, a prescindere dalla sua gravità, è risarcibile (36).

79. In tale contesto, è rilevante la distinzione tra danno immateriale risarcibile e altri *svantaggi derivanti dall'inosservanza della legalità* che, data la loro scarsa entità, non darebbero necessariamente diritto a un risarcimento (37).

80. La Corte riconosce tale differenza laddove fa riferimento ai disagi e fastidi in quanto categoria autonoma rispetto a quella del danno, in ambiti nei quali ritiene che essi debbano essere risarciti (38).

81. Empiricamente può osservarsi che qualsiasi violazione di una norma in materia di protezione dei dati personali determina una reazione negativa dell'interessato. Un risarcimento dovuto per la mera sensazione di malessere di fronte all'altrui inosservanza della legge si confonderebbe facilmente con un risarcimento senza danno che, come abbiamo detto, non pare configurabile nella fattispecie di cui all'articolo 82 del Regolamento.

82. Il fatto che, in circostanze come quelle del procedimento principale, l'uso improprio dei dati personali sia solo potenziale, e non già effettivo, è sufficiente per ritenere che l'interessato possa aver subito un danno morale causato dalla violazione del Regolamento, a condizione che l'interessato

dimostri che il timore di tale uso improprio gli abbia concretamente e specificamente causato un danno emotivo reale e certo (39).

83. Il confine tra la mera irritazione (non risarcibile) e il vero e proprio danno immateriale (risarcibile) è senz'altro sottile, ma i giudici nazionali, cui spetta il compito di delimitare caso per caso tale confine, dovrebbero effettuare un'attenta valutazione di tutti gli elementi forniti dall'interessato che richiede il risarcimento, cui spetterà l'onere di allegare con precisione, e non in modo generico, elementi concreti che possano condurre alla configurabilità di un «danno morale effettivamente subito» a causa della violazione dei dati personali, pur senza che esso raggiunga una soglia di particolare gravità predeterminata: ciò che conta è che non si tratti di una mera percezione soggettiva, mutevole e dipendente anche da elementi caratteriali e personali, ma la oggettivizzazione di un disagio, seppur lieve ma comprovabile, alla propria sfera fisica o psichica o alla propria vita di relazione; la natura dei dati personali coinvolti e la rilevanza che essi ricoprono nella vita dell'interessato e forse anche la percezione che, in quel momento, abbia la società di quello specifico disagio connesso alla violazione dei dati (40).

IV. Conclusione

84. Sulla base di tutte le suesposte considerazioni, suggerisco alla Corte di rispondere alle questioni pregiudiziali proposte nel seguente modo:

«Gli articoli 5, 24, 32 e 82 del Regolamento 2016/679 devono essere interpretati nel senso che:

la mera esistenza di una "violazione dei dati personali", come definita all'articolo 4, paragrafo 12, non sia di per sé sufficiente per concludere che le misure tecniche e organizzative attuate dal titolare del trattamento non erano "adeguate" a garantire la protezione dei dati in questione;

nel verificare l'adeguatezza delle misure tecniche e organizzative attuate dal titolare del trattamento dei dati personali, il giudice nazionale adito deve effettuare un controllo che si estende a un'analisi concreta sia del contenuto di tali misure sia del modo in cui sono state applicate e dei loro effetti pratici;

nell'ambito di un'azione di risarcimento danni ai sensi dell'articolo 82 del GDPR, il titolare del trattamento dei dati personali ha l'onere di dimostrare l'adeguatezza delle misure che ha attuato ai sensi dell'articolo 32 di tale regolamento;

in conformità al principio dell'autonomia procedurale, spetta all'ordinamento giuridico interno di ciascuno Stato membro determinare i metodi di prova ammissibili e il loro valore probatorio, compresi i mezzi istruttori che i tribunali nazionali possono o devono ordinare, al fine di valutare se un titolare del trattamento dei dati personali abbia attuato misure adeguate ai sensi di tale regolamento, nel rispetto dei principi di equivalenza e di efficacia definiti dal diritto dell'Unione;

il fatto che la violazione di tale regolamento che ha causato il danno in questione sia stata commessa da un terzo non costituisce di per sé un motivo per esonerare il titolare del trattamento dalla responsabilità e, per beneficiare dell'esenzione prevista da tale disposizione, il titolare del trattamento deve dimostrare che la violazione non gli è in alcun modo imputabile;

il pregiudizio consistente nel timore di un potenziale futuro uso improprio dei suoi dati personali, di cui l'interessato abbia dimostrato la sussistenza, può costituire un danno morale che dà diritto a un risarcimento, a condizione che l'interessato dimostri di aver subito individualmente un danno emotivo reale e certo, circostanza che spetta al giudice nazionale adito verificare in ogni singolo caso».

---

1 Lingua originale: l'italiano.

---

2 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).

.

3 La NAP è titolare del trattamento ai sensi dell'articolo 4, punto 7, del Regolamento. In forza del diritto nazionale, essa è un organismo amministrativo dotato di competenza specifica, sottoposta al Ministro delle Finanze, e incaricata dell'accertamento, della salvaguardia e del recupero delle Finanze, nonché incaricata dell'accertamento, della salvaguardia e del recupero di crediti dello Stato, pubblici e privati determinati *ex lege*. Essa, nell'esercizio dei poteri pubblici che le sono devoluti, tratta dati personali.

4 L'articolo 5, paragrafo 2 (relativo al principio di responsabilità di qualsiasi titolare del trattamento dei dati personali), l'articolo 24 (relativo alle misure che tale titolare del trattamento è tenuto a mettere in atto per garantire che il suo trattamento sia conforme a tale regolamento), l'articolo 32 (relativo a tale obbligo specificamente per quanto riguarda la sicurezza del trattamento) e l'articolo 82, paragrafi da 1 a 3 (relativo al risarcimento dei danni derivanti da una violazione di tale regolamento e alla possibilità per il titolare del trattamento di adottare misure per garantire il rispetto di tale regolamento), oltre i considerando 74, 85 e 146 che sono collegati agli articoli suddetti.

5 a) la prima mira a rispondere al quesito se dalla mera violazione dei sistemi si può dedurre l'inadeguatezza delle misure predisposte; b) la seconda riguarda l'estensione del sindacato giurisdizionale sull'adeguatezza delle predette misure; c) la terza si riferisce all'onere probatorio dell'adeguatezza stessa e ad alcune modalità tecniche per la ricerca della prova; d) la quarta attiene alla rilevanza ai fini dell'esonero della responsabilità della circostanza che l'attacco al sistema provenga dall'esterno.

6 Quanto alle disposizioni del Regolamento richiamate, le prime tre domande riguardano i profili della responsabilità del titolare del trattamento in relazione all'adeguatezza delle misure da adottare (articoli 5, 24 e 32); la quarta e la quinta, le condizioni per l'esonero della responsabilità e la nozione di danno morale risarcibile (articolo 82).

7 V. conclusioni dell'avvocato generale Campos Sánchez-Bordona nella causa Österreichische Post (Danno morale legato al trattamento dei dati personali) (C-300/21, EU:C:2022:756).

8 C. Docksey, *Article 24. Responsibility of the controller*, in C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, pag. 561. I principi e gli obblighi delle regolamentazioni sulla protezione dei dati dovrebbero permeare il tessuto culturale delle organizzazioni, a tutti i livelli, piuttosto che essere considerati come una serie di requisiti legali da spuntare da parte dell'ufficio legale.

9 E. Belisario, G. Riccio, G. Scorza, *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, pag. 301.

10 E. Belisario, G. Riccio, G. Scorza, *GDPR* cit., pag. 380.

11 Per questo, come vedremo, la prima e la quarta questione pregiudiziale non possono che ricevere una risposta negativa. Nessun automatismo è deducibile dalle disposizioni del Regolamento: né il solo fatto che vi sia stata una divulgazione dei dati personali è sufficiente per ritenere che le misure tecniche e organizzative adottate non siano adeguate ma neppure la circostanza che la divulgazione stessa sia avvenuta per l'intervento di soggetti estranei all'organizzazione del titolare del trattamento e fuori dalla sfera di controllo dello stesso è sufficiente per esentarlo da responsabilità.

12 L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, pag. 201. Il legislatore europeo supera dunque la concezione della sicurezza del trattamento basata sulla presenza di misure di sicurezza predeterminate e adotta una metodologia propria degli standard internazionali sulla gestione dei sistemi di informazione *risk* based: essa prevede l'individuazione di misure di mitigazione dei rischi che prescindono da *checklist* preconfigurate e genericamente applicabili. Occorre pertanto ricorrere a linee guida e standard internazionali. Il frutto di tale valutazione dei rischi diventa quindi vincolante nel momento in cui l'organizzazione operi delle decisioni al fine di mitigare i rischi individuati, rendendosi *accountable*.

---

13 Il concetto di adeguatezza mostra inequivocabilmente l'intenzione di non attribuire rilevanza a tutte le misure tecniche e organizzative astrattamente possibili. V., in questo senso, M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo, Giappichelli*, 2019, pag. 1059.

---

14 Osservazioni scritte, punto 31.

---

15 M. Gambini, *Responsabilità* cit., pag. 1067. Il possesso di una certificazione si traduce pertanto in un'inversione dell'onere della prova in favore del titolare che è agevolato nel dimostrare di aver agito rispettando gli obblighi di cui al Regolamento.

---

16 Nel disporre espressamente, alla lettera d) che il giudizio di adeguatezza si estende all'efficacia delle misure adottate, che deve essere regolarmente testata, verificata e valutata, sia in fase iniziale, sia in fase periodica, al fine di assicurare la sicurezza effettiva di tutti i tipi di trattamento, quale che sia il loro livello di rischio; e, ancora, nel prevedere esplicitamente, alla lettera c), che le misure tecniche e organizzative messe in atto devono presentare la capacita di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico. Vedi M. Gambini, *Responsabilità* cit., pagg. 1064 e 1065.

---

17 Punto 30 delle osservazioni scritte: «spetterà al titolare del trattamento dimostrare come ha valutato tutti i fattori e le circostanze relative al trattamento in questione, e in particolare il risultato dell'analisi dei rischi effettuata, i rischi identificati, le misure concrete trovate per mitigare tali rischi, la giustificazione delle opzioni scelte alla luce delle soluzioni tecnologiche disponibili sul mercato, l'efficacia delle misure, la correlazione tra le misure tecniche e organizzative, la formazione del personale che tratta i dati, l'esistenza di un'esternalizzazione delle operazioni di trattamento dei dati, compreso lo sviluppo e la manutenzione delle tecnologie informatiche, e l'esistenza di un controllo da parte del titolare del trattamento e di istruzioni precise impartite agli incaricati del trattamento, ai sensi dell'articolo 28 del GDPR, sul trattamento dei dati personali da parte di questi ultimi; come è stata valutata l'infrastruttura di supporto dei sistemi di comunicazione e informazione e come è stato classificato il livello di rischio per i diritti e le libertà degli interessati».

---

18 Ai sensi del considerando 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».

---

19 Si vedano, in particolare, le sentenze della Corte del 5 settembre 2019, Unione europea/Guardian Europe e Guardian Europe/Unione europea (C-447/17 P e C-479/17 P, EU:C:2019:672, punto 147), e del 28 ottobre 2021, Vialto Consulting/Commissione (C-650/19 P, EU:C:2021:879, punto 138), nonché le sentenze del Tribunale del 13 gennaio 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, punto 116), e del 29 settembre 2021, Kočner/Europol (T-528/20, non pubblicata, EU:T:2021:631, punto 61), in cui si ricorda che devono

essere soddisfatte tre condizioni, ossia "l'illiceità del comportamento di cui è accusata l'istituzione dell'Unione, la realtà del danno e l'esistenza di un nesso di causalità tra il comportamento di tale istituzione e il danno invocato".

---

20 Osservazioni scritte, punto 39.

---

21 Conformemente alla costante giurisprudenza della Corte secondo cui le eccezioni a una norma generale devono essere interpretate in modo restrittivo, l'eventuale esenzione di responsabilità prevista dall'articolo 82, paragrafo 3, deve essere interpretata in modo restrittivo. Si vedano, per analogia, le sentenze del 15 ottobre 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, punto 53), e del 5 aprile 2022, Commissioner of An Garda Síochána e a. (C-140/20, EU:C:2022:258, punto 40).

---

22 La responsabilità civile tende ad essere qualificata come oggettiva ogni qual volta il soggetto agente sia tenuto ad adottare tutte le misure astrattamente possibili per evitare il danno, a prescindere dell'effettiva conoscenza che ne abbia avuto o dalla loro sostenibilità economica. Viceversa, qualora al soggetto agente sia imposta l'adozione di misure normalmente osservabili da un operatore del settore economico di riferimento per mantenere la sicurezza e prevenire i pregiudizi che possano derivare dall'attività svolta, l'imputazione del danno stesso tende a spostarsi verso un regime di responsabilità per colpa specifica. M. Gambini, *Responsabilità* cit., pag. 1055.

---

23 M. Gambini, *Responsabilità* cit. pag. 1059. In senso analogo, per l'opinione secondo cui la prova di aver adottato le misure idonee consista non nella mera allegazione della massima diligenza esigibile, ma nella dimostrazione di un fatto terzo generatore del danno, munito dei caratteri di imprevedibilità ed inevitabilità propri del caso fortuito e della forza maggiore, S. Sica, *Sub art. 82*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

---

24 «se *dimostra* che l'evento dannoso non gli è in alcun modo imputabile» (articolo 82, paragrafo 3).

---

25 M. Gambini, *Responsabilità* cit., pag. 1060.

---

26 Si veda, in tal senso, la sentenza del 15 giugno 2021, Facebook Ireland e a. (C-645/19, EU:C:2021:483, punti 43 e 44).

---

27 Ai sensi del considerando 85: «Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche […]». Ai sensi del considerando 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. […]. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito […]».

---

28 V. conclusioni dell'avvocato generale Campos Sánchez-Bordona cit., paragrafo 29 e nota 11. Nelle stesse conclusioni, l'avvocato generale correttamente conclude la sua analisi sotto i profili letterale, storico, contestuale e teleologico, escludendo la natura «punitiva» dei danni risarcibili agli interessati ai sensi dell'articolo 82 (paragrafi da 27 a 55), rilevando, da un lato, che gli Stati membri «non devono (e in realtà non possono) scegliere tra i meccanismi del capo VIII per assicurare la protezione dei dati. Di fronte ad una violazione che non provoca un danno, all'interessato è comunque garantito (come minimo) il diritto di presentare un reclamo ad un'autorità di controllo» e, dall'altro, che «la prospettiva di ottenere un

risarcimento indipendentemente da qualsiasi danno stimolerebbe probabilmente le controversie civili, con azioni magari non sempre giustificate, e potrebbe quindi disincentivare l'attività di trattamento dei dati» (paragrafi 54 e 55).

---

29 Il diniego del diritto al risarcimento per sentimenti o emozioni lievi e transitori connessi alla violazione delle norme sul trattamento non lascerebbe pertanto l'interessato completamente privo di tutela (v., in questo senso, le conclusioni dell'avvocato generale Campos Sánchez-Bordona cit., paragrafo 115).

---

30 O «in senso lato» nelle parole del considerando 146.

---

31 V. le sentenze del 15 aprile 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, punto 48), e del 10 giugno 2021, KRONE - Verlag (C-65/20, EU:C:2021:471, punto 25).

---

32 V. le conclusioni dell'avvocato generale Campos Sánchez-Bordona cit., paragrafo 104.

---

33 Né ha indicato un metodo di interpretazione – autonoma o per rinvio agli ordinamenti nazionali – preferibile: dipende dalla materia oggetto di esame. Cfr. sentenze del 10 maggio 2001, Veedfald (C-203/99, EU:C:2001:258, punto 27), in materia di prodotti difettosi, del 6 maggio 2010, Walz (C-63/09, EU:C:2010:251, punto 21), sulla responsabilità dei vettori aerei, e del 10 giugno 2021, Van Ameyde España (C-923/19, EU:C:2021:475, punti 37 e segg.), relativamente alla responsabilità civile per i sinistri derivanti dalla circolazione degli autoveicoli.

---

34 Ad esempio, i consumatori di prodotti o le vittime di sinistri stradali.

---

35 In materia di viaggi «tutto compreso», v. sentenza del 12 marzo 2002, Leitner (C-168/00, EU:C:2002:163); nell'ambito della responsabilità civile risultante dalla circolazione degli autoveicoli, sentenze del 24 ottobre 2013, Haasová (C-22/12, EU:C:2013:692, punti da 47 a 50), del 24 ottobre 2013, Drozdovs (C-277/12, EU:C:2013:685, punto 40), e del 23 gennaio 2014, Petillo (C-371/12, EU:C:2014:26, punto 35).

---

36 V. conclusioni dell'avvocato generale Campos Sánchez-Bordona cit., paragrafo 105. La Corte, ad esempio, ha riconosciuto la compatibilità con le norme europee di una legge nazionale che, ai fini del calcolo del risarcimento, distingue i danni immateriali connessi a lesioni corporali causate da un sinistro in funzione dell'origine di quest'ultimo; v. sentenza del 23 gennaio 2014, Petillo (C-371/12, EU:C:2014:26), dispositivo: il diritto dell'Unione non osta «ad una legislazione nazionale (…) la quale prevede un particolare sistema di risarcimento dei danni morali derivanti da lesioni corporali di lieve entità causate da sinistri stradali, che limita il risarcimento di tali danni rispetto a quanto ammesso in materia di risarcimento di danni identici risultanti da cause diverse da detti sinistri».

---

37 Questa distinzione è riscontrabile in alcuni ordinamenti giuridici nazionali, in quanto inevitabile corollario della vita in società. Recentemente, in materia di protezione dei dati, in Italia, Tribunale di Palermo, sez. I civile, sentenza 05/10/2017 n. 5261, nonché Cass. Civ., Ord. sez. VI, n. 17383/2020. In Germania, inter alia, AG Diez, 07.11.2018 – 8 C 130/18; LG Karlsruhe, 02.08.2019 – 8 O 26/19, e AG Frankfurt am Main, 10.07.2020 – 385 C 155/19 (70). In Austria, OGH 6 Ob 56/21k.

---

38 V. sentenza del 23 ottobre 2012, Nelson e a. (C-581/10 e C-629/10, EU:C:2012:657, punto 51), sulla distinzione tra «danni» ai sensi dell'articolo 19 della Convenzione per l'unificazione di alcune norme relative al trasporto aereo internazionale, conclusa a Montreal il 28 maggio 1999, e «fastidi» ai sensi del regolamento n. 261/2004, che sono risarcibili in forza dell'articolo 7 di quest'ultimo, ai sensi della sentenza del 19

novembre 2009, Sturgeon e a. (C-402/07 e C-432/07, EU:C:2009:716). In tale settore, così come in quello del trasporto di passeggeri via mare e per vie navigabili interne cui si riferisce il regolamento n. 1177/2010, il legislatore ha potuto riconoscere una categoria astratta in quanto l'elemento che determina il disagio, e l'essenza di quest'ultimo, sono identici per tutti gli interessati. Non credo che tale deduzione sia possibile in materia di protezione dei dati.

---

39 Secondo l'Irlanda, queste considerazioni sono particolarmente importanti nella pratica, nel contesto della criminalità informatica perché se ogni persona colpita – anche solo in minima parte – da una violazione avesse diritto a un risarcimento per danni non materiali, ciò avrebbe un forte impatto, in particolare sui titolari del trattamento dei dati del settore pubblico, che sono finanziati con fondi pubblici limitati e dovrebbero piuttosto servire interessi collettivi, compreso il miglioramento della sicurezza dei dati personali (osservazioni scritte, punto 72).

---

40 V. conclusioni dell'avvocato generale Campos Sánchez-Bordona cit., punto 116.