HOTĂRÂREA CURȚII (Camera a treia)

14 decembrie 2023 *

„Trimitere preliminară – Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal – Regulamentul (UE) 2016/679 – Articolul 5 – Principii referitoare la această prelucrare – Articolul 24 – Răspunderea operatorului – Articolul 32 – Măsuri implementate pentru a asigura securitatea prelucrării – Aprecierea caracterului adecvat al unor astfel de măsuri – Întinderea controlului jurisdicțional – Administrarea probelor – Articolul 82 – Dreptul la despăgubiri și răspunderea – Eventuala exonerare de răspundere a operatorului în cazul unei încălcări săvârșite de părți terțe – Cerere de despăgubire pentru un prejudiciu moral întemeiată pe temerea față de o potențială utilizare abuzivă a datelor cu caracter personal”

În cauza C-340/21,

având ca obiect o cerere de decizie preliminară formulată în temeiul articolului 267 TFUE de Varhoven administrativen sad (Curtea Administrativă Supremă, Bulgaria), prin decizia din 14 mai 2021, primită de Curte la 2 iunie 2021, în procedura

VB

împotriva

Natsionalna agentsia za prihodite,

CURTEA (Camera a treia),

compusă din doamna K. Jürimäe, președintă de cameră, și domnii N. Piçarra, M. Safjan, N. Jääskinen (raportor) și M. Gavalec, judecători,

avocat general: domnul G. Pitruzzella,

grefier: domnul A. Calot Escobar,

având în vedere procedura scrisă,

luând în considerare observațiile prezentate:

– pentru Natsionalna agentsia za prihodite, de R. Spetsov;

– pentru guvernul bulgar, de M. Georgieva și L. Zaharieva, în calitate de agenți;

* Limba de procedură: bulgara.

– pentru guvernul ceh, de O. Serdula, M. Smolek și J. Vláčil, în calitate de agenți;

– pentru Irlanda, de M. Browne, Chief State Solicitor, A. Joyce, J. Quaney și M. Tierney, în calitate de agenți, asistați de D. Fennelly, BL;

– pentru guvernul italian, de G. Palmieri, în calitate de agent, asistată de E. De Bonis, avvocato dello Stato;

– pentru guvernul portughez, de P. Barros da Costa, A. Pimenta, J. Ramos și C. Vieira Guerra, în calitate de agenți;

– pentru Comisia Europeană, de A. Bouchagiar, H. Kranenborg și N. Nikolova, în calitate de agenți,

după ascultarea concluziilor avocatului general în ședința din 27 aprilie 2023,

pronunță prezenta

Hotărâre

1 Cererea de decizie preliminară privește interpretarea articolului 5 alineatul (2), a articolelor 24 și 32, precum și a articolului 82 alineatele (1)-(3) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1, denumit în continuare „RGPD”).

2 Această cerere a fost formulată în cadrul unui litigiu între VB, o persoană fizică, pe de o parte, și Natsionalna agentsia za prihodite (Agenția Națională a Veniturilor Publice, Bulgaria) (denumită în continuare „NAP”), pe de altă parte, în legătură cu despăgubirea pentru prejudiciul moral pe care persoana respectivă afirmă că l-a suferit ca urmare a unei pretinse neîndepliniri de către această autoritate publică a obligațiilor legale ce îi revin în calitatea sa de operator de date cu caracter personal.

Cadrul juridic

3 Considerentele (4), (10), (11), (74), (76), (83), (85) și (146) ale RGPD au următorul cuprins:

„(4) […] Prezentul regulament respectă toate drepturile fundamentale și libertățile și principiile recunoscute în [Carta drepturilor fundamentale a Uniunii Europene] astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, […] dreptul la o cale de atac eficientă și la un proces echitabil […]

[…]

(10) Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii [Europene], nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. Aplicarea consecventă și omogenă a normelor în materie de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ar trebui să fie asigurată în întreaga Uniune. […]

(11) Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și stabilirea în detaliu a drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, […]

[…]

(74) Ar trebui să se stabilească responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul ar trebui să fie obligat să implementeze măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să țină seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice.

[…]

(76) Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul ar trebui apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.

[…]

(83) În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective ar trebui să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, ar trebui să se acorde atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

[…]

(85) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea

neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul ar trebui să notifice această încălcare autorității de supraveghere, fără întârziere nejustificată […]

[…]

(146) Operatorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezentul regulament. Operatorul sau persoana împuternicită de operator ar trebui să fie exonerați de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. Conceptul de prejudiciu ar trebui interpretat în sens larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele prezentului regulament. Această dispoziție nu aduce atingere niciunei cereri de despăgubire care rezultă din încălcarea altor norme din dreptul Uniunii sau din dreptul intern. O prelucrare care încalcă prezentul regulament include și prelucrarea care încalcă actele delegate și de punere în aplicare adoptate în conformitate cu prezentul regulament și cu dreptul intern care specifică norme din prezentul regulament. Persoanele vizate ar trebui să primească despăgubiri integrale și eficace pentru prejudiciul pe care l-au suferit. […]”

4 Articolul 4 din acest regulament, intitulat „Definiții”, prevede:

„În sensul prezentului regulament:

1. «date cu caracter personal» înseamnă orice informații privind o persoană fizică identificată sau identificabilă («persoana vizată»); […]

2. «prelucrare» înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate […]

[…]

7. «operator» înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;

[…]

10. «parte terță» înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

[…]

12. «încălcarea securității datelor cu caracter personal» înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau la accesul neautorizat la acestea;

[…]”

5 Articolul 5 din regulamentul menționat, intitulat „Principii legate de prelucrarea datelor cu caracter personal”, prevede:

„(1) Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată («legalitate, echitate și transparență»);

[…]

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare («integritate și confidențialitate»);

(2) Operatorul este responsabil de respectarea alineatului (1) și poate demonstra această respectare («responsabilitate»).”

6 Potrivit articolului 24 din același regulament, intitulat „Responsabilitatea operatorului”:

„(1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alineatul (1) includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.

(3) Aderarea la coduri de conduită aprobate, menționate la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.”

7 Articolul 32 din RGPD, intitulat „Securitatea prelucrării”, prevede:

„(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

(a) pseudonimizarea și criptarea datelor cu caracter personal;

(b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;

(c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

(d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.

[…]”

8 Articolul 79 din acest regulament, intitulat „Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator”, prevede la alineatul (1):

„Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere în temeiul articolului 77, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezentul regulament.”

9 Articolul 82 din regulamentul menționat, intitulat „Dreptul la despăgubiri și răspunderea”, prevede la alineatele (1)-(3):

„(1) Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

(2) Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prezentul regulament. […]

(3) Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere în temeiul alineatului (2) dacă dovedește că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.”

Litigiul principal și întrebările preliminare

10 NAP este o autoritate atașată ministrului finanțelor bulgar. În cadrul atribuțiilor sale, care constau printre altele în identificarea, securizarea și recuperarea creanțelor publice, aceasta este operator de date cu caracter personal, în sensul articolului 4 punctul 7 din RGPD.

11 La 15 iulie 2019, mass-media a arătat că sistemul informatic al NAP a fost accesat în mod neautorizat și că, în urma acestui atac cibernetic, datele cu caracter personal conținute în sistemul respectiv au fost publicate pe internet.

12 Peste șase milioane de persoane fizice, de cetățenie bulgară sau străină, au fost afectate de aceste evenimente. Câteva sute dintre acestea, printre care și reclamanta din litigiul principal, au introdus acțiuni împotriva NAP în despăgubirea prejudiciilor morale care ar fi rezultat din divulgarea datelor lor cu caracter personal.

13 În acest context, reclamanta din litigiul principal a formulat o acțiune la Administrativen sad Sofia-grad (Tribunalul Administrativ din Sofia, Bulgaria) prin care urmărea plata de către NAP a sumei de 1 000 de leva bulgărești (BGN) (aproximativ 510 euro) cu titlu de daune interese, în temeiul articolului 82 din RGPD și al dispozițiilor dreptului bulgar. În susținerea acestei cereri, ea a susținut că a suferit un prejudiciu moral rezultat dintr-o încălcare a securității datelor cu caracter personal, în sensul articolului 4 punctul 12 din RGPD, mai precis o încălcare a securității care ar fi fost cauzată de neîndeplinirea de către NAP a obligațiilor ce îi revin printre altele în temeiul articolului 5 alineatul (1) litera (f), precum și al articolelor 24 și 32 din respectivul regulament. Prejudiciul moral ar consta în temerea că datele sale cu caracter personal ce au fost publicate fără consimțământul său ar putea fi utilizate în mod abuziv în viitor sau că ea însăși ar putea fi șantajată agresată sau chiar răpită.

14 În apărare, NAP a arătat mai întâi că reclamanta din litigiul principal nu i-a solicitat informații referitoare la datele precise care fuseseră divulgate. În continuare, NAP a prezentat documente prin care urmărea să dovedească faptul că a luat toate măsurile necesare în amonte pentru a preveni încălcarea securității datelor cu caracter personal conținute în sistemul său informatic, precum și în aval, pentru a limita efectele acestei încălcări și pentru a liniști cetățenii. În plus, potrivit NAP, nu exista o legătură de cauzalitate între prejudiciul moral invocat și încălcarea amintită. În sfârșit, aceasta a susținut că, întrucât ea însăși a fost victima unui atac malițios din partea unor persoane care nu erau angajații săi, nu poate fi considerată răspunzătoare pentru consecințele prejudiciabile ale acestui atac.

15 Prin decizia din 27 noiembrie 2020, Administrativen sad Sofia-grad (Tribunalul Administrativ din Sofia) a respins acțiunea reclamantei din litigiul principal. Această instanță a considerat, pe de o parte, că accesul neautorizat la baza de date a NAP rezulta dintr-o piratare informatică săvârșită de părți terțe și, pe de altă parte, că reclamanta din litigiul principal nu a dovedit că NAP nu și-a îndeplinit obligațiile în ceea ce privește adoptarea unor măsuri de securitate. În plus, aceasta a apreciat că reclamanta menționată nu a suferit un prejudiciu moral care dă naștere unui drept la despăgubire.

16 Reclamanta din litigiul principal a formulat recurs împotriva deciziei respective la Varhoven administrativen sad (Curtea Administrativă Supremă, Bulgaria), care este instanța de trimitere în prezenta cauză. În susținerea recursului formulat, ea afirmă că instanța de prim grad de jurisdicție a săvârșit o eroare de drept în repartizarea sarcinii probei referitoare la măsurile de securitate adoptate de NAP și că aceasta din urmă nu a demonstrat lipsa unei neîndepliniri a obligațiilor în această privință. În plus, reclamanta din litigiul principal susține că temerea față de posibile utilizări abuzive ale datelor sale cu caracter personal în viitor constituie un prejudiciu moral real, iar nu ipotetic. În apărare, NAP contestă fiecare dintre aceste argumente.

17 Instanța de trimitere are în vedere, mai întâi, posibilitatea ca constatarea producerii unei încălcări a securității datelor cu caracter personal să permită, în sine, să se concluzioneze că măsurile implementate de operator nu erau „adecvate”, în sensul articolelor 24 și 32 din RGPD.

18 Cu toate acestea, în ipoteza în care această constatare ar fi insuficientă pentru a ajunge la o asemenea concluzie, ea ridică, pe de o parte, problema întinderii controlului pe care instanțele naționale trebuie să îl efectueze pentru a evalua caracterul adecvat al măsurilor în cauză și, pe de altă parte, problema normelor referitoare la administrarea probelor care trebuie aplicate în acest cadru, atât în ceea ce privește sarcina probei, cât și mijloacele de probă, în special atunci când aceste instanțe sunt sesizate cu o acțiune în despăgubire întemeiată pe articolul 82 din acest regulament.

19 În continuare, această instanță urmărește să afle dacă, în raport cu articolul 82 alineatul (3) din regulamentul respectiv, faptul că încălcarea securității datelor cu caracter personal rezultă dintr-un act săvârșit de părți terțe, în speță dintr-un atac cibernetic, constituie un factor ce exonerează în mod sistematic operatorul acestor date de răspundere pentru prejudiciul cauzat persoanei vizate.

20 În sfârșit, instanța menționată ridică problema dacă temerea resimțită de o persoană că datele sale cu caracter personal pot face obiectul unei utilizări abuzive în viitor, în speță ca urmare a unui acces neautorizat la acestea și a divulgării lor de către infractorii cibernetici, poate constitui, în sine, un „prejudiciu moral”, în sensul articolului 82 alineatul (1) din RGPD. În cazul unui răspuns afirmativ, această persoană ar fi scutită de obligația de a dovedi că, anterior cererii sale de despăgubire, părți terțe au utilizat în mod nelegal aceste date, precum în cazul unei fraude a identității.

21 În aceste condiții, Varhoven administrativen sad (Curtea Administrativă Supremă) a hotărât să suspende judecarea cauzei și să adreseze Curții următoarele întrebări preliminare:

„1) Dispozițiile articolelor 24 și 32 din [RGPD] pot fi interpretate în sensul că divulgarea sau accesul neautorizat la date cu caracter personal, în sensul articolului 4 punctul 12 din [RGPD], de către persoane care nu fac parte din personalul administrației operatorului de date cu caracter personal și care nu sunt supuse controlului acestuia sunt suficiente pentru a se considera că măsurile tehnice și organizatorice implementate nu erau adecvate?

2) În cazul unui răspuns negativ la prima întrebare, care trebuie să fie obiectul și întinderea controlului jurisdicțional al legalității în examinarea aspectului dacă măsurile tehnice și organizatorice implementate de operator sunt adecvate în temeiul articolului 32 din [RGPD]?

3) În cazul unui răspuns negativ la prima întrebare, principiul răspunderii în sensul articolului 5 alineatul (2) [din RGPD] și al articolului 24 [din acest regulament] coroborate cu considerentul (74) [al acestuia] pot fi interpretate în sensul că, în cadrul unei acțiuni întemeiate pe articolul 82 alineatul (1) [din regulamentul menționat], operatorului îi revine sarcina de a dovedi că măsurile tehnice și organizatorice implementate sunt adecvate în temeiul articolului 32 din [același] regulament?

În cazul în care instanța dispune efectuarea unei expertize judiciare, aceasta poate fi considerată un mijloc de probă necesar și suficient pentru a stabili dacă măsurile tehnice și organizatorice implementate de operator au fost adecvate într-un caz precum cel din speță, în care accesul și divulgarea neautorizate sunt consecința unui «atac cibernetic»?

4) Articolul 82 alineatul (3) din [RGPD] poate fi interpretat în sensul că divulgarea sau accesul neautorizat la date cu caracter personal, în sensul articolului 4 punctul 12 din [RGPD], în speță prin intermediul unui «atac cibernetic» efectuat de persoane care nu fac parte din personalul administrației operatorului de date cu caracter personal și care nu sunt supuse controlului acestuia, constituie un fapt care nu este nicidecum imputabil operatorului de date cu caracter personal și reprezintă un motiv de exonerare de răspundere?

5) Dispozițiile articolului 82 alineatele (1) și (2) [din RGPD] coroborate cu considerentele (85) și (146) [ale acestui regulament] pot fi interpretate în sensul că, într-un caz precum cel din speță, de încălcare a securității datelor cu caracter personal, care se traduce printr-un acces și o difuzare neautorizată de date cu caracter personal, în cadrul unui «atac cibernetic», îngrijorările, temerile și frica persoanei vizate, în sine, de o posibilă utilizare abuzivă în viitor a datelor cu caracter personal, fără ca o astfel de utilizare abuzivă să fie constatată și/sau fără ca persoana vizată să fi suferit alte prejudicii, se încadrează în sensul larg al noțiunii de prejudiciu moral și justifică o despăgubire?"

Cu privire la întrebările preliminare

Cu privire la prima întrebare

22 Prin intermediul primei întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolele 24 și 32 din RGPD trebuie interpretate în sensul că o divulgare neautorizată a datelor cu caracter personal sau un acces neautorizat la asemenea date de către „o parte terță", în sensul articolului 4 punctul 10 din acest regulament, sunt suficiente în sine pentru a considera că măsurile tehnice și organizatorice implementate de operatorul în cauză nu erau „adecvate", în sensul acestor articole 24 și 32.

23 Cu titlu introductiv, trebuie amintit că, potrivit unei jurisprudențe constante, termenii unei dispoziții de drept al Uniunii care, precum articolele 24 și 32 din RGPD, nu conține nicio trimitere expresă la dreptul statelor membre pentru a stabili sensul și domeniul său de aplicare trebuie, în mod normal, să primească în întreaga Uniune o interpretare autonomă și uniformă, care trebuie stabilită în special ținând seama de formularea dispoziției în cauză, de obiectivele urmărite de aceasta din urmă și de contextul în care se înscrie [a se vedea în acest sens Hotărârea din 18 ianuarie 1984, Ekro, 327/82, EU:C:1984:11, punctul 11, Hotărârea din 1 octombrie 2019, Planet49, C-673/17, EU:C:2019:801, punctele 47 și 48, precum și Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctul 29].

24 În primul rând, în ceea ce privește formularea dispozițiilor relevante, trebuie arătat că articolul 24 din RGPD prevede o obligație generală, ce revine operatorului de date cu caracter personal, de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și pentru a putea demonstra că prelucrarea se efectuează în conformitate cu acest regulament.

25 În acest scop, articolul 24 menționat enumeră, la alineatul (1), o serie de criterii ce trebuie luate în considerare pentru evaluarea caracterului adecvat al unor asemenea măsuri, și anume natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice. Această dispoziție adaugă că măsurile amintite se revizuiesc și se actualizează dacă este necesar.

26 Din această perspectivă, articolul 32 din RGPD precizează obligațiile operatorului și ale unei eventuale persoane împuternicite de acesta în ceea ce privește securitatea prelucrării. Astfel, alineatul (1) al acestui articol prevede că aceștia din urmă trebuie să implementeze măsurile tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscurilor menționate la punctul anterior din prezenta hotărâre, ținând seama de stadiul actual al dezvoltării, de costurile implementării, precum și de natura, domeniul de aplicare, contextul și scopurile prelucrării în cauză.

27 De asemenea, alineatul (2) al articolului respectiv prevede că la evaluarea nivelului adecvat de securitate trebuie să se țină seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal.

28 În plus, atât articolul 24 alineatul (3) din acest regulament, cât și articolul 32 alineatul (3) din acesta indică faptul că operatorul sau persoana împuternicită de operator poate demonstra că a îndeplinit cerințele prevăzute la alineatele (1) ale acestor articole, întemeindu-se pe faptul că aderă la un cod de conduită aprobat sau la un mecanism de certificare aprobat, menționate la articolele 40 și 42 din regulamentul amintit.

29 Trimiterea ce figurează la articolul 32 alineatele (1) și (2) din RGPD la „[un] nivel de securitate corespunzător acestui risc” și la un „[nivel] adecvat de securitate” dovedește că acest regulament instituie un regim de gestionare a riscurilor și că nu urmărește nicidecum eliminarea riscurilor de încălcare a securității datelor cu caracter personal.

30 Astfel, din modul de redactare a articolelor 24 și 32 din RGPD reiese că aceste dispoziții se limitează să impună operatorului să adopte măsuri tehnice și organizatorice destinate să evite, în măsura posibilului, orice atingere adusă datelor cu caracter personal. Caracterul adecvat al unor asemenea măsuri trebuie evaluat în mod concret, examinând dacă aceste măsuri au fost implementate de acest operator ținând seama de diferitele criterii prevăzute la articolele menționate și de nevoile de protecție a datelor inerente în mod specific prelucrării în cauză, precum și riscurilor pe care le presupune aceasta din urmă.

31 Prin urmare, articolele 24 și 32 din RGPD nu pot fi interpretate în sensul că o divulgare neautorizată a datelor cu caracter personal sau un acces neautorizat la astfel de date de către o parte terță sunt suficiente pentru a concluziona că măsurile adoptate de operatorul în cauză nu erau adecvate, în sensul acestor dispoziții, fără ca măcar să i se permită acestuia din urmă să facă proba contrară.

32 O atare interpretare se impune cu atât mai mult cu cât articolul 24 din RGPD prevede în mod expres că operatorul trebuie să fie în măsură să demonstreze conformitatea cu acest regulament a măsurilor pe care le-a pus în aplicare, posibilitate de care ar fi privat dacă s-ar admite o prezumție irefragabilă.

33 În al doilea rând, elemente de ordin contextual și teleologic coroborează această interpretare a articolelor 24 și 32 din RGPD.

34 În ceea ce privește, pe de o parte, contextul în care se înscriu aceste două articole, este necesar să se arate că din articolul 5 alineatul (2) din RGPD reiese că operatorul trebuie poată demonstra că a respectat principiile referitoare la prelucrarea datelor cu caracter personal prevăzute la alineatul (1) al articolului menționat. Această obligație este reluată și precizată la articolul 24

alineatele (1) și (3), precum și la articolul 32 alineatul (3) din acest regulament, în ceea ce privește obligația de a implementa măsuri tehnice și organizatorice pentru protejarea unor asemenea date cu ocazia prelucrării efectuate de acest operator. Or, o asemenea obligație de a demonstra caracterul adecvat al acestor măsuri nu ar avea sens dacă operatorul ar fi obligat să împiedice orice atingere adusă datelor respective.

35 În plus, considerentul (74) al RGPD subliniază că este important ca operatorul să fie obligat să pună în aplicare măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu acest regulament, inclusiv eficacitatea măsurilor, care ar trebui să țină seama de criteriile referitoare la caracteristicile prelucrării în cauză și la riscul prezentat de aceasta, prevăzute la articolele 24 și 32.

36 De asemenea, potrivit considerentului (76) al acestui regulament, probabilitatea și gravitatea riscului depind de particularitățile tratamentului în cauză, iar acest risc ar trebui apreciat pe baza unei evaluări obiective.

37 Pe de altă parte, din articolul 82 alineatele (2) și (3) din RGPD rezultă că, deși un operator este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă acest regulament, el este totuși exonerat de răspundere dacă dovedește că nu este răspunzător în niciun fel pentru evenimentul care a cauzat prejudiciul.

38 Pe de altă parte, interpretarea efectuată la punctul 31 din prezenta hotărâre este de asemenea susținută de considerentul (83) al RGPD, care enunță, în prima sa teză, că, „[î]n vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri”. Procedând astfel, legiuitorul Uniunii și-a manifestat intenția de a „atenua” riscurile de încălcare a securității datelor cu caracter personal, fără a pretinde că ar fi posibil să le elimine.

39 Având în vedere motivele care precedă, este necesar să se răspundă la prima întrebare că articolele 24 și 32 din RGPD trebuie interpretate în sensul că o divulgare neautorizată de date cu caracter personal sau un acces neautorizat la asemenea date de către „părți terțe”, în sensul articolului 4 punctul 10 din acest regulament, nu sunt în sine suficiente pentru a considera că măsurile tehnice și organizatorice implementate de operatorul în cauză nu erau „adecvate”, în sensul acestor articole 24 și 32.

Cu privire la a doua întrebare

40 Prin intermediul celei de a doua întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 32 din RGPD trebuie să fie interpretat în sensul că caracterul adecvat al măsurilor tehnice și organizatorice implementate de operator în temeiul acestui articol trebuie să fie apreciat de instanțele naționale în mod concret, ținând seama în special de riscurile legate de prelucrarea respectivă.

41 În această privință, trebuie amintit că, după cum s-a subliniat în cadrul răspunsului la prima întrebare, articolul 32 din RGPD impune operatorului și persoanei împuternicite de acesta, după caz, să implementeze măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, ținând seama de criteriile de apreciere prevăzute la

alineatul (1) al acestuia. În plus, alineatul (2) al articolului respectiv enumeră, în mod neexhaustiv, o serie de factori pertinenți pentru evaluarea nivelului adecvat de siguranță în raport cu riscurile pe care le prezintă prelucrarea în cauză.

42 Reiese din articolul 32 alineatele (1) și (2) că caracterul adecvat al unor astfel de măsuri tehnice și organizatorice trebuie apreciat în două etape. Pe de o parte, trebuie identificate riscurile de încălcare a securității datelor cu caracter personal care rezultă din prelucrarea în cauză și eventualele consecințe ale acestora pentru drepturile și libertățile persoanelor fizice. Această apreciere trebuie efectuată în mod concret, luând în considerare gradul de probabilitate a riscurilor identificate și gradul lor de gravitate. Pe de altă parte, este necesar să se verifice dacă măsurile implementate de operator sunt adaptate la aceste riscuri, ținând seama de stadiul actual al dezvoltării, de costurile implementării, precum și de natura, domeniul de aplicare, contextul și scopurile acestei prelucrări.

43 Desigur, operatorul dispune de o anumită marjă de apreciere pentru a stabili măsurile tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscului, după cum impune articolul 32 alineatul (1) din RGPD. Nu este mai puțin adevărat că o instanță națională trebuie să poată evalua aprecierea complexă efectuată de operator și, astfel, să se asigure că măsurile reținute de acesta sunt apte să garanteze un atare nivel de securitate.

44 O asemenea interpretare este de altfel de natură să asigure, pe de o parte, efectivitatea protecției datelor cu caracter personal pe care o evidențiază considerentele (11) și (74) ale acestui regulament și, pe de altă parte, dreptul la o cale de atac judiciară eficientă împotriva unui operator, astfel cum este protejat de articolul 79 alineatul (1) din regulamentul amintit coroborat cu considerentul (4) al aceluiași regulament.

45 Prin urmare, pentru a controla caracterul adecvat al măsurilor tehnice și organizatorice implementate în temeiul articolului 32 din RGPD, o instanță națională nu trebuie să se limiteze să constate în ce mod operatorul în cauză a înțeles să îndeplinească obligațiile ce îi revin în temeiul acestui articol, ci trebuie să examineze pe fond aceste măsuri, în raport cu toate criteriile menționate la articolul respectiv, precum și cu împrejurările proprii speței și cu elementele de probă de care dispune instanța în această privință.

46 O asemenea examinare necesită efectuarea unei analize concrete atât a naturii, cât și a conținutului măsurilor care au fost implementate de operator, a modului în care au fost aplicate aceste măsuri și a efectelor lor practice asupra nivelului de securitate pe care acesta era obligat să îl garanteze, având în vedere riscurile inerente acestei prelucrări.

47 În consecință, este necesar să se răspundă la a doua întrebare că articolul 32 din RGPD trebuie interpretat în sensul că caracterul adecvat al măsurilor tehnice și organizatorice implementate de operator în temeiul acestui articol trebuie să fie apreciat de instanțele naționale în mod concret, ținând seama de riscurile legate de prelucrare și apreciind dacă natura, conținutul și implementarea acestor măsuri sunt adaptate acestor riscuri.

Cu privire la a treia întrebare

Cu privire la prima parte a celei de a treia întrebări

48 Prin intermediul primei părți a celei de a treia întrebări, instanța de trimitere solicită în esență să se stabilească dacă principiul răspunderii operatorului, enunțat la articolul 5 alineatul (2) din RGPD și concretizat la articolul 24 din acesta, trebuie interpretat în sensul că, în cadrul unei acțiuni în despăgubire întemeiate pe articolul 82 din acest regulament, operatorului în cauză îi revine sarcina de a dovedi caracterul adecvat al măsurilor de securitate pe care le-a implementat în temeiul articolului 32 din regulamentul respectiv.

49 În această privință, trebuie amintit, în primul rând, că articolul 5 alineatul (2) din RGPD stabilește un principiu al responsabilității în temeiul căruia operatorul este responsabil de respectarea principiilor referitoare la prelucrarea datelor cu caracter personal prevăzute la alineatul (1) al acestui articol și prevede că operatorul menționat trebuie să fie în măsură să demonstreze că aceste principii sunt respectate.

50 În special, operatorul trebuie, în conformitate cu principiul integrității și confidențialității datelor cu caracter personal prevăzut la articolul 5 alineatul (1) litera (f) din acest regulament, să se asigure că asemenea date sunt prelucrate într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri tehnice sau organizatorice corespunzătoare, și trebuie să fie în măsură să demonstreze că acest principiu este respectat.

51 Este de asemenea necesar să se arate că atât articolul 24 alineatul (1) din RGPD coroborat cu considerentul (74) al acestuia, cât și articolul 32 alineatul (1) din acest regulament impun operatorului, în ceea ce privește orice prelucrare a datelor cu caracter personal efectuată de el însuși sau în numele său, să implementeze măsuri tehnice și organizatorice adecvate pentru a se asigura și a fi în măsură să demonstreze că prelucrarea este efectuată în conformitate cu regulamentul menționat.

52 Reiese fără ambiguitate din modul de redactare a articolului 5 alineatul (2), a articolului 24 alineatul (1) și a articolului 32 alineatul (1) din RGPD că sarcina de a dovedi că datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a acestora din urmă, în sensul articolului 5 alineatul (1) litera (f) și al articolului 32 din acest regulament, revine operatorului în cauză [a se vedea prin analogie Hotărârea din 4 mai 2023, Bundesrepublik Deutschland (Căsuță electronică judiciară), C-60/22, EU:C:2023:373, punctele 52 și 53, precum și Hotărârea din 4 iulie 2023, Meta Platforms și alții (Condiții generale de utilizare a unei rețele sociale), C-252/21, EU:C:2023:537, punctul 95].

53 Aceste trei articole prevăd astfel o normă de aplicare generală, care, în lipsa unei indicații contrare în RGPD, trebuie să se aplice și în cadrul unei acțiuni în despăgubire întemeiate pe articolul 82 din acest regulament.

54 În al doilea rând, este necesar să se constate că interpretarea literală care precedă este susținută de luarea în considerare a obiectivelor urmărite de RGPD.

55 Pe de o parte, din moment ce nivelul protecției vizate de RGPD depinde de măsurile de securitate adoptate de operatorii de date cu caracter personal, aceștia trebuie să fie încurajați, prin intermediul faptului că suportă sarcina de a demonstra caracterul adecvat al acestor măsuri, să facă tot posibilul pentru a preveni apariția unor operațiuni de prelucrare neconforme cu acest regulament.

56 Pe de altă parte, dacă ar trebui să se considere că sarcina probei privind caracterul adecvat al măsurilor menționate revine persoanelor vizate, așa cum sunt definite la articolul 4 punctul 1 din RGPD, ar rezulta că dreptul la despăgubiri prevăzut la articolul 82 alineatul (1) din acesta ar fi privat de o parte semnificativă a efectului său util, în condițiile în care legiuitorul Uniunii a intenționat să consolideze atât drepturile acestor persoane, cât și obligațiile operatorilor, în raport cu dispozițiile anterioare acestui regulament, după cum se arată în considerentul (11) al acestuia.

57 Prin urmare, este necesar să se răspundă la prima parte a celei de a treia întrebări că principiul răspunderii operatorului, enunțat la articolul 5 alineatul (2) din RGPD și concretizat la articolul 24 din acesta, trebuie interpretat în sensul că, în cadrul unei acțiuni în despăgubire întemeiate pe articolul 82 din acest regulament, operatorului în cauză îi revine sarcina de a dovedi caracterul adecvat al măsurilor de securitate pe care le-a implementat în temeiul articolului 32 din regulamentul amintit.

Cu privire la a doua parte a celei de a treia întrebări

58 Prin intermediul celei de a doua părți a celei de a treia întrebări, instanța de trimitere urmărește să afle în esență dacă articolul 32 din RGPD și principiul efectivității dreptului Uniunii trebuie interpretate în sensul că, pentru a aprecia caracterul adecvat al măsurilor de securitate pe care operatorul le-a implementat în temeiul acestui articol, o expertiză judiciară constituie un mijloc de probă necesar și suficient.

59 În această privință, trebuie amintit că, potrivit unei jurisprudențe constante, în lipsa unor norme ale Uniunii în materie, revine ordinii juridice interne a fiecărui stat membru atribuția de a stabili, în temeiul principiului autonomiei procedurale, modalitățile procedurale ale acțiunilor în justiție destinate să asigure apărarea drepturilor justițiabililor, cu condiția însă ca acestea să nu fie, în situațiile care intră sub incidența dreptului Uniunii, mai puțin favorabile decât cele aplicabile unor situații similare supuse dreptului intern (principiul echivalenței) și să nu facă imposibilă în practică sau excesiv de dificilă exercitarea drepturilor conferite de dreptul Uniunii (principiul efectivității) [Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctul 53 și jurisprudența citată].

60 În speță, este necesar să se arate că RGPD nu prevede norme referitoare la admiterea și la valoarea probantă a unui mijloc de probă precum o expertiză judiciară, care trebuie să fie aplicate de instanțele naționale sesizate cu o acțiune în despăgubire întemeiată pe articolul 82 din acest regulament și însărcinate să aprecieze, în raport cu articolul 32 din acesta, caracterul adecvat al măsurilor de securitate pe care operatorul în cauză le-a implementat. Prin urmare, în conformitate cu cele amintite la punctul precedent din prezenta hotărâre și în lipsa unor norme de drept al Uniunii în materie, revine ordinii juridice interne a fiecărui stat membru atribuția de a stabili modalitățile acțiunilor destinate să asigure protecția drepturilor conferite justițiabililor de acest articol 82 și în special normele aferente mijloacelor de probă ce permit evaluarea caracterului adecvat al unor astfel de măsuri în acest context, sub rezerva respectării principiilor

echivalenței și efectivității menționate [a se vedea prin analogie Hotărârea din 21 iunie 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, punctul 297, precum și Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctul 54].

61 În prezenta procedură, Curtea nu dispune de niciun element de natură să dea naștere unor îndoieli cu privire la respectarea principiului echivalenței. Situația este diferită în ceea ce privește conformitatea cu principiul efectivității, întrucât însuși modul de redactare a celei de a doua părți a celei de a treia întrebări prezintă recurgerea la o expertiză judiciară ca un „mijloc de probă necesar și suficient”.

62 În special, o normă de procedură națională în temeiul căreia ar fi „necesar” în mod sistematic ca instanțele naționale să dispună efectuarea unei expertize judiciare este susceptibilă să încalce principiul efectivității. Astfel, recurgerea sistematică la o asemenea expertiză se poate dovedi superfluă având în vedere celelalte probe deținute de instanța sesizată, în special, după cum a arătat guvernul bulgar în observațiile sale scrise, având în vedere rezultatele unui control al respectării măsurilor de protecție a datelor cu caracter personal care a fost efectuat de o autoritate independentă și instituită de lege, cu condiția ca acest control să fie recent, întrucât măsurile menționate trebuie, conform articolului 24 alineatul (1) din RGPD, să fie revizuite și actualizate dacă este necesar.

63 În plus, după cum a arătat Comisia Europeană în observațiile sale scrise, principiul efectivității ar putea fi încălcat în ipoteza în care termenul „suficient” ar trebui înțeles ca însemnând că o instanță națională trebuie să deducă exclusiv sau automat dintr-un raport de expertiză judiciară că măsurile de securitate implementate de operatorul în cauză sunt „adecvate”, în sensul articolului 32 din RGPD. Or, protecția drepturilor conferite de acest regulament, pe care o urmărește principiul efectivității amintit, și în special dreptul la o cale de atac judiciară efectivă împotriva operatorului, care este garantat de articolul 79 alineatul (1) din acesta, impun ca o instanță imparțială să efectueze o apreciere obiectivă a caracterului adecvat al măsurilor în cauză, în loc să se limiteze la o astfel de deducție (a se vedea în acest sens Hotărârea din 12 ianuarie 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, punctul 50).

64 Având în vedere motivele care precedă, este necesar să se răspundă la a doua parte a celei de a treia întrebări că articolul 32 din RGPD și principiul efectivității dreptului Uniunii trebuie interpretate în sensul că, pentru a aprecia caracterul adecvat al măsurilor de securitate pe care operatorul le-a implementat în temeiul acestui articol, o expertiză judiciară nu poate constitui un mijloc de probă în mod sistematic necesar și suficient.

Cu privire la a patra întrebare

65 Prin intermediul celei de a patra întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 82 alineatul (3) din RGPD trebuie interpretat în sensul că operatorul este exonerat de obligația de a repara prejudiciul suferit de o persoană, în temeiul articolului 82 alineatele (1) și (2) din acest regulament, pentru simplul fapt că prejudiciul respectiv rezultă dintr-o divulgare neautorizată de date cu caracter personal sau dintr-un acces neautorizat la asemenea date de către „părți terțe”, în sensul articolului 4 punctul 10 din regulamentul menționat.

66 Cu titlu introductiv, trebuie precizat că din articolul 4 punctul 10 din RGPD rezultă că au calitatea de „parte terță”, printre altele, alte persoane decât cele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal. Această definiție include persoane care nu sunt angajați ai operatorului și nu se află sub controlul acestuia, precum cele menționate în întrebarea adresată.

67 În continuare, trebuie amintit, în primul rând, că articolul 82 alineatul (2) din RGPD prevede că „orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă [acest] regulament” și că alineatul (3) al acestui articol prevede că un operator sau o persoană împuternicită de operator, după caz, este exonerată de o astfel de răspundere „dacă dovedește că nu este răspunzător în niciun fel pentru evenimentul care a cauzat prejudiciul”.

68 În plus, considerentul (146) al RGPD, care se referă în mod specific la articolul 82 din acesta, enunță, în prima și în a doua teză, că „[o]peratorul sau persoana împuternicită de operator ar trebui să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă [acest] regulament” și că „ar trebui să fie exonerați de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu”.

69 Din aceste dispoziții rezultă, pe de o parte, că operatorul în cauză trebuie, în principiu, să repare un prejudiciu cauzat de o încălcare a regulamentului legată de prelucrare și, pe de altă parte, că nu poate fi exonerat de răspundere decât dacă dovedește că nu este în niciun fel răspunzător pentru fapta care a provocat acest prejudiciu.

70 Astfel, după cum arată adăugarea expresă a locuțiunii adverbiale „în niciun fel” în cursul procedurii legislative, împrejurările în care operatorul poate pretinde să fie exonerat de răspunderea civilă ce îi revine în temeiul articolului 82 din RGPD trebuie să fie strict limitate la cele în care acest operator este în măsură să demonstreze că prejudiciul nu îi este imputabil.

71 Atunci când, precum în speță, o încălcare a securității datelor cu caracter personal, în sensul articolului 4 punctul 12 din RGPD, a fost săvârșită de infractori cibernetici și, prin urmare, de „părți terțe”, în sensul articolului 4 punctul 10 din acest regulament, această încălcare nu poate fi imputată operatorului, cu excepția cazului în care acesta a făcut posibilă încălcarea menționată prin nerespectarea unei obligații prevăzute de RGPD și în special a obligației de protecție a datelor de care este ținut în temeiul articolului 5 alineatul (1) litera (f) și al articolelor 24 și 32 din același regulament.

72 Așadar, în cazul unei încălcări a securității datelor cu caracter personal săvârșite de o parte terță, operatorul se poate exonera de răspunderea sa, în temeiul articolului 82 alineatul (3) din RGPD, prin dovedirea faptului că nu există nicio legătură de cauzalitate între eventuala sa încălcare a obligației de protecție a datelor și prejudiciul suferit de persoana fizică.

73 În al doilea rând, interpretarea care precedă a acestui articol 82 alineatul (3) este de asemenea conformă cu obiectivul RGPD ce constă în asigurarea unui nivel ridicat de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal, enunțat în considerentele (10) și (11) ale acestui regulament.

74 Având în vedere ansamblul acestor considerații, este necesar să se răspundă la a patra întrebare că articolul 82 alineatul (3) din RGPD trebuie interpretat în sensul că operatorul nu poate fi exonerat de obligația de a repara prejudiciul suferit de o persoană, în temeiul articolului 82 alineatele (1)

și (2) din acest regulament, pentru simplul fapt că prejudiciul respectiv rezultă dintr-o divulgare neautorizată de date cu caracter personal sau dintr-un acces neautorizat la asemenea date de către „părți terțe”, în sensul articolului 4 punctul 10 din regulamentul menționat, operatorul amintit trebuind să dovedească că faptul care a provocat acest prejudiciu nu îi este în niciun fel imputabil.

Cu privire la a cincea întrebare

75 Prin intermediul celei de a cincea întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 82 alineatul (1) din RGPD trebuie interpretat în sensul că temerea față de o potențială utilizare abuzivă a datelor sale cu caracter personal de către părți terțe pe care o resimte o persoană vizată în urma unei încălcări a acestui regulament poate constitui, în sine, un „prejudiciu moral”, în sensul dispoziției amintite.

76 În ceea ce privește, în primul rând, modul de redactare a articolului 82 alineatul (1) din RGPD, este necesar să se observe că acesta prevede că „[o]rice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentului regulament are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit”.

77 În această privință, Curtea a arătat că reiese cu claritate din modul de redactare a articolului 82 alineatul (1) din RGPD că existența unui „prejudiciu” sau a unei „daune” care a fost „suferit(ă)” constituie una dintre condițiile dreptului la despăgubiri prevăzut de dispoziția menționată, la fel ca existența unei încălcări a acestui regulament și a unei legături de cauzalitate între acest prejudiciu și această încălcare, cele trei condiții fiind cumulative [Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctul 32].

78 Pe de altă parte, întemeindu-se pe considerații deopotrivă de ordin literal, sistemic și teleologic, Curtea a interpretat articolul 82 alineatul (1) din RGPD în sensul că se opune unei norme sau unei practici naționale care subordonează obținerea de despăgubiri pentru un „prejudiciu moral”, în sensul acestei dispoziții, condiției ca prejudiciul suferit de persoana vizată să fi atins un anumit nivel de gravitate [Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctul 51].

79 Acestea fiind amintite, trebuie subliniat în speță că articolul 82 alineatul (1) din RGPD nu face distincție între situații în care, în urma unei încălcări dovedite a dispozițiilor acestui regulament, „prejudiciul moral” invocat de persoana vizată, pe de o parte, este legat de o utilizare abuzivă de către părți terțe a datelor sale cu caracter personal care s-a produs deja la data cererii sale de despăgubire sau, pe de altă parte, este legat de temerea resimțită de această persoană că o asemenea utilizare s-ar putea produce în viitor.

80 În consecință, modul de redactare a articolului 82 alineatul (1) din RGPD nu exclude ca noțiunea de „prejudiciu moral” ce figurează în această dispoziție să includă o situație precum cea vizată de instanța de trimitere, în care persoana în cauză invocă, în vederea obținerii unei despăgubiri în temeiul dispoziției respective, temerea sa ca datele sale cu caracter personal să facă obiectul unei utilizări abuzive în viitor de către părți terțe, ca urmare a încălcării ce a avut loc a acestui regulament.

81 Această interpretare literală este confirmată, în al doilea rând, de considerentul (146) al RGPD, care privește în mod specific dreptul la despăgubiri prevăzut la articolul 82 alineatul (1) din RGPD și care menționează, în a treia teză, că „conceptul de prejudiciu ar trebui interpretat în sens

larg, din perspectiva jurisprudenței Curții de Justiție, într-un mod care să reflecte pe deplin obiectivele" acestui regulament. Or, o interpretare a noțiunii de „prejudiciu moral", în sensul acestui articol 82 alineatul (1), care nu ar include situațiile în care persoana vizată de o încălcare a regulamentului respectiv se prevalează de temerea că propriile date cu caracter personal ar putea face obiectul unei utilizări abuzive în viitor nu ar corespunde unei concepții largi a acestei noțiuni, așa cum a fost urmărită de legiuitorul Uniunii [a se vedea prin analogie Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctele 37 și 46].

82 Pe de altă parte, considerentul (85) prima teză al RGPD arată că, „[d]acă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, […] sau orice alt dezavantaj semnificativ de natură economică sau socială". Din această listă exemplificativă a „prejudiciilor" ce pot fi suferite de persoanele vizate reiese că legiuitorul Uniunii a intenționat să includă în aceste noțiuni în special simpla „[pierdere a] controlului" asupra propriilor date, în urma unei încălcări a acestui regulament, chiar dacă o utilizare abuzivă a datelor în cauză nu s-ar fi produs în mod concret în detrimentul persoanelor menționate.

83 În al treilea și ultimul rând, interpretarea ce figurează la punctul 80 din prezenta hotărâre este susținută de obiectivele RGPD, de care trebuie să se țină seama pe deplin pentru a defini noțiunea de „prejudiciu", după cum arată considerentul (146) a treia teză al acestui regulament. Or, o interpretare a articolului 82 alineatul (1) din RGPD potrivit căreia noțiunea de „prejudiciu moral", în sensul acestei dispoziții, nu ar include situațiile în care o persoană vizată se prevalează numai de temerea că datele sale ar putea să facă, în viitor, obiectul unei utilizări abuzive de către părți terțe nu ar fi conformă cu garantarea unui nivel ridicat de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal în cadrul Uniunii, urmărită de acest instrument.

84 Cu toate acestea, trebuie subliniat că o persoană vizată de o încălcare a RGPD care a avut consecințe negative împotriva sa este obligată să demonstreze că aceste consecințe constituie un prejudiciu moral, în sensul articolului 82 din acest regulament [a se vedea în acest sens Hotărârea din 4 mai 2023, Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal), C-300/21, EU:C:2023:370, punctul 50].

85 În special, atunci când o persoană care solicită despăgubiri în acest temei invocă temerea că o utilizare abuzivă a datelor sale cu caracter personal va surveni în viitor ca urmare a existenței unei astfel de încălcări, instanța națională sesizată trebuie să verifice dacă această temere poate fi considerată fondată, în împrejurările specifice în cauză și în raport cu persoana vizată.

86 Având în vedere motivele care precedă, este necesar să se răspundă la a cincea întrebare că articolul 82 alineatul (1) din RGPD trebuie interpretat în sensul că temerea față de o potențială utilizare abuzivă a datelor sale cu caracter personal de către părți terțe pe care o resimte o persoană vizată în urma unei încălcări a acestui regulament poate constitui, în sine, un „prejudiciu moral", în sensul dispoziției menționate.

Cu privire la cheltuielile de judecată

87 Întrucât, în privința părților din litigiul principal, procedura are caracterul unui incident survenit la instanța de trimitere, este de competența acesteia să se pronunțe cu privire la cheltuielile de judecată. Cheltuielile efectuate pentru a prezenta observații Curții, altele decât cele ale părților menționate, nu pot face obiectul unei rambursări.

Pentru aceste motive, Curtea (Camera a treia) declară:

1) **Articolele 24 și 32 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)**

   trebuie interpretate în sensul că

   o divulgare neautorizată de date cu caracter personal sau un acces neautorizat la asemenea date de către „părți terțe”, în sensul articolului 4 punctul 10 din acest regulament, nu sunt în sine suficiente pentru a considera că măsurile tehnice și organizatorice implementate de operatorul în cauză nu erau „adecvate”, în sensul acestor articole 24 și 32.

2) **Articolul 32 din Regulamentul 2016/679**

   trebuie interpretat în sensul că

   caracterul adecvat al măsurilor tehnice și organizatorice implementate de operator în temeiul acestui articol trebuie să fie apreciat de instanțele naționale în mod concret, ținând seama de riscurile legate de prelucrare și apreciind dacă natura, conținutul și implementarea acestor măsuri sunt adaptate acestor riscuri.

3) **Principiul răspunderii operatorului, enunțat la articolul 5 alineatul (2) din Regulamentul 2016/679 și concretizat la articolul 24 din acesta,**

   trebuie interpretat în sensul că

   în cadrul unei acțiuni în despăgubire întemeiate pe articolul 82 din acest regulament, operatorului în cauză îi revine sarcina de a dovedi caracterul adecvat al măsurilor de securitate pe care le-a implementat în temeiul articolului 32 din regulamentul amintit.

4) **Articolul 32 din Regulamentul 2016/679 și principiul efectivității dreptului Uniunii**

   trebuie interpretate în sensul că

   pentru a aprecia caracterul adecvat al măsurilor de securitate pe care operatorul le-a implementat în temeiul acestui articol, o expertiză judiciară nu poate constitui un mijloc de probă în mod sistematic necesar și suficient.

5) **Articolul 82 alineatul (3) din Regulamentul 2016/679**

trebuie interpretat în sensul că

operatorul nu poate fi exonerat de obligația de a repara prejudiciul suferit de o persoană, în temeiul articolului 82 alineatele (1) și (2) din acest regulament, pentru simplul fapt că prejudiciul respectiv rezultă dintr-o divulgare neautorizată de date cu caracter personal sau dintr-un acces neautorizat la asemenea date de către „părți terțe”, în sensul articolului 4 punctul 10 din regulamentul menționat, operatorul amintit trebuind să dovedească că faptul care a provocat acest prejudiciu nu îi este în niciun fel imputabil.

6) **Articolul 82 alineatul (1) din Regulamentul 2016/679**

trebuie interpretat în sensul că

temerea față de o potențială utilizare abuzivă a datelor sale cu caracter personal de către părți terțe pe care o resimte o persoană vizată în urma unei încălcări a acestui regulament poate constitui, în sine, un „prejudiciu moral”, în sensul dispoziției menționate.

Semnături