CONCLUZIILE AVOCATULUI GENERAL
DOMNUL GIOVANNI PITRUZZELLA
prezentate la 27 aprilie 2023 [1]

Cauza C-340/21

VB
împotriva
Natsionalna agentsia za prihodite

[cerere de decizie preliminară formulată de Varhoven administrativen sad (Curtea Supremă Administrativă, Bulgaria)]

„Trimitere preliminară – Protecția datelor cu caracter personal – Regulamentul (UE) 2016/679 – Răspunderea operatorului – Securitatea prelucrării – Încălcarea securității prelucrării datelor cu caracter personal – Prejudiciu moral suferit ca urmare a inacțiunii operatorului – Acțiune în despăgubire”

Divulgarea nelegală a datelor cu caracter personal deținute de o agenție publică, ca urmare a unui atac de piraterie informatică, poate da naștere dreptului la repararea prejudiciului moral suferit de o persoană vizată, pentru simplul motiv că persoana vizată este preocupată de faptul că datele sale pot fi utilizate în mod abuziv în viitor? Care sunt criteriile de imputabilitate a răspunderii operatorului? Cum este repartizată sarcina probei în cadrul procedurii în instanță? Care este amploarea controlului efectuat de instanță?

I. Cadrul juridic

1. Articolul 4, intitulat „Definiții”, din Regulamentul 2016/679 [2] (denumit în continuare „regulamentul”) prevede:

„În sensul prezentului regulament:

[…]

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;

[1] Limba originală: italiana.

[2] 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).

[…]”

2. Articolul 5, intitulat „Principii legate de prelucrarea datelor cu caracter personal”, prevede:

„(1) Datele cu caracter personal sunt:

[…]

(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»).”

3. Articolul 24 din același regulament, intitulat „Responsabilitatea operatorului”, prevede:

„(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.”

4. Articolul 32, 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:

[…]

(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.

[…]”

5. Articolul 82 din același regulament, intitulat „Dreptul la despăgubiri și răspunderea”, prevede:

„(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.”

II. Situația de fapt, procedura și întrebările preliminare

6. La 15 iulie 2019, mass-media bulgară a relatat că a avut loc un acces neautorizat la sistemul informatic al Natsionalna agentsia za prihodite (Agenția Națională a Veniturilor Publice, Bulgaria, denumită în continuare „NAP”[3]) și că au fost publicate pe internet diferite informații fiscale și legate de asigurări sociale referitoare la milioane de persoane, atât cetățeni bulgari, cât și străini.

7. Mai multe persoane, printre care VB, recurenta din litigiul principal, au introdus o acțiune împotriva NAP pentru repararea prejudiciului moral.

8. În speță, recurenta din litigiul principal a introdus o acțiune la Administrativen sad Sofia-grad (Tribunalul Administrativ din Sofia, Bulgaria, denumit în continuare „ASSG”), susținând că NAP a încălcat normele naționale și obligația de a prelucra datele cu caracter personal în calitate de operator astfel încât să „garanteze un nivel de securitate corespunzător” prin adoptarea unor măsuri tehnice și organizatorice adecvate, în conformitate cu articolele 24 și 32 din Regulamentul 2016/679. În continuare, recurenta a arătat că a suferit un prejudiciu moral, manifestat sub forma unor preocupări și temeri că datele sale cu caracter personal ar putea fi utilizate în mod abuziv în viitor.

9. Partea adversă a subliniat, în schimb, că nu a primit nicio cerere din partea recurentei din litigiul principal în care să fie indicate cu exactitate datele cu caracter personal care au fost accesate. În plus, ca urmare a relatărilor privind intruziunea, ar fi convocat reuniuni la nivel înalt cu experți pentru a proteja drepturile și interesele cetățenilor. Potrivit NAP, nu ar fi existat nicio legătură de cauzalitate între atacul cibernetic și prejudiciul pretins invocat, întrucât agenția a introdus sisteme de management al proceselor și sisteme de management al securității informațiilor, în conformitate cu normele internaționale în vigoare în materie.

[3] NAP este operator în sensul articolului 4 punctul 7 din regulament. Potrivit dreptului național, aceasta este o autoritate specializată aflată în subordinea ministrului Finanțelor, competentă pentru stabilirea, conservarea și perceperea fondurilor, precum și a creanțelor publice ale statului și a creanțelor private ale statului stabilite prin lege. În exercitarea competențelor publice care îi sunt transferate, ea prelucrează date cu caracter personal.

10. Instanța de fond, ASSG, a respins cererea, considerând că divulgarea datelor nu era imputabilă agenției, că sarcina probei în legătură cu caracterul adecvat al măsurilor luate revenea recurentei și, în sfârșit, că nu exista niciun prejudiciu moral care să dea dreptul la despăgubiri.

11. Hotărârea pronunțată în primă instanță a fost ulterior atacată la Varhoven administrativen sad (Curtea Administrativă Supremă, Bulgaria). Printre motivele invocate, recurenta din litigiul principal a subliniat că instanța de fond a săvârșit o eroare în repartizarea sarcinii probei în ceea ce privește neadoptarea măsurilor de securitate. De asemenea, prejudiciul moral nu ar trebui să facă obiectul unei sarcini a probei, din moment ce este vorba despre un prejudiciu moral real, iar nu pur potențial.

12. La rândul său, NAP a reiterat că a luat măsurile tehnice și organizatorice necesare în calitatea sa de operator și a contestat existența dovezilor privind existența unui prejudiciu moral real. Anxietatea și temerile ar fi stări emoționale care nu pot face obiectul reparației.

13. Instanța de trimitere a constatat că există mai multe soluții în ceea ce privește diferitele proceduri pe care părțile prejudiciate le-au inițiat separat împotriva NAP în vederea reparării prejudiciului moral.

14. În acest context, instanța de trimitere a suspendat procedura și a adresat Curții următoarele întrebări preliminare:

„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 este suficient ca divulgarea neautorizată a datelor cu caracter personal, respectiv accesul neautorizat la acestea, în sensul articolului 4 punctul 12 din regulamentul menționat, să fi fost efectuate de persoane care nu fac parte din personalul administrației operatorului și care nu sunt supuse controlului acestuia pentru a se considera că măsurile tehnice și organizatorice implementate nu sunt 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 Regulamentul (UE) 2016/679?

3) În cazul unui răspuns negativ la prima întrebare, principiul responsabilității prevăzut la articolul 5 alineatul (2) și la articolul 24 din Regulamentul (UE) 2016/679 coroborate cu considerentul (74) al acestuia trebuie interpretat în sensul că, în cadrul acțiunii formulate în temeiul articolului 82 alineatul (1) din Regulamentul (UE) 2016/679, operatorului îi revine sarcina de a dovedi că măsurile tehnice și organizatorice implementate sunt adecvate în temeiul articolului 32 din acest regulament? Obținerea unui raport de expertiză poate fi considerată un mijloc de probă necesar și suficient pentru a se stabili dacă măsurile tehnice și organizatorice implementate de operator au fost adecvate într-un caz precum cel din speță, în care accesul neautorizat la datele cu caracter personal și divulgarea neautorizată a acestora sunt consecința unui «atac cibernetic»?

4) Articolul 82 alineatul (3) din Regulamentul (UE) 2016/679 trebuie interpretat în sensul că divulgarea neautorizată a datelor cu caracter personal sau accesul neautorizat la acestea, în sensul articolului 4 punctul 12 din Regulamentul (UE) 2016/679, astfel cum este cazul în speță, prin intermediul unui «atac cibernetic» efectuat de persoane care nu fac parte din personalul administrației operatorului și care nu sunt supuse controlului acestuia constituie o împrejurare pentru care operatorul nu este deloc răspunzător și care permite exonerarea de răspundere?

5) Articolul 82 alineatele (1) și (2) din Regulamentul (UE) 2016/679 coroborat cu considerentele (85) și (146) ale acestuia trebuie să fie interpretat în sensul că, într-un caz precum cel din speță, de atingere adusă protecției datelor cu caracter personal constând în accesul neautorizat la date cu caracter personal și în divulgarea acestora prin intermediul unui «atac cibernetic», sub incidența noțiunii de prejudiciu moral interpretate în sens larg intră, singure, îngrijorările, temerile și stările de anxietate suferite de persoana vizată cu privire la o posibilă utilizare abuzivă în viitor a datelor cu caracter personal și dau acestea dreptul la despăgubiri, atunci când o asemenea utilizare abuzivă nu a fost constatată și/sau persoana vizată nu a suferit niciun alt prejudiciu?”

III. Analiză juridică

A. Observații preliminare

15. Prezenta cauză are ca obiect chestiuni interesante și, în parte, inedite privind interpretarea mai multor dispoziții ale regulamentului [4].

16. Toate cele cinci întrebări preliminare se axează pe aceeași problemă: condițiile de reparare a prejudiciului moral suferit de o persoană ale cărei date cu caracter personal, deținute de o agenție publică, au fost publicate pe internet în urma unui atac cibernetic.

17. Pentru ușurința expunerii, vom propune răspunsuri sintetice separate la toate întrebările preliminare enunțate în ordonanța de trimitere, deși suntem conștienți că există o anumită suprapunere conceptuală, întrucât primele patru vizează toate identificarea condițiilor de stabilire a răspunderii operatorului pentru încălcarea dispozițiilor regulamentului [5], iar cea de a cincea se referă mai precis la noțiunea de prejudiciu moral în scopul despăgubirii [6].

[4] Articolul 5 alineatul (2) (referitor la principiul responsabilității oricărui operator de date cu caracter personal), articolul 24 (referitor la măsurile care trebuie luate de operatorul respectiv pentru a se asigura că prelucrarea este conformă cu acest regulament), articolul 32 (referitor la această obligație, în special în ceea ce privește securitatea prelucrării) și articolul 82 alineatele (1)-(3) (referitor la despăgubirile pentru prejudiciile rezultate în urma unei încălcări a acestui regulament și la posibilitatea ca operatorul să ia măsuri pentru a asigura respectarea regulamentului), pe lângă considerentele (74), (85) și (146) care au legătură cu articolele menționate.

[5] a) prima urmărește stabilirea aspectului dacă din simpla încălcare a sistemelor poate fi dedus caracterul inadecvat al măsurilor instituite; b) a doua se referă la întinderea controlului jurisdicțional asupra caracterului adecvat al acestor măsuri; c) a treia se referă la sarcina probei în ceea ce privește caracterul adecvat în sine și la anumite modalități tehnice pentru obținerea probelor; d) a patra se referă la relevanța, în scopul exonerării de răspundere, a faptului că atacul asupra sistemului provine din exterior.

[6] În ceea ce privește dispozițiile regulamentului invocate, primele trei întrebări se referă la aspectele legate de responsabilitatea operatorului în ceea ce privește caracterul adecvat al măsurilor care trebuie adoptate (articolele 5, 24 și 32), iar a patra și a cincea, la condițiile care trebuie îndeplinite pentru exonerarea de răspundere și la noțiunea de prejudiciu moral pentru care pot fi acordate despăgubiri (articolul 82).

18. Subliniem că sunt în prezent pendinte la Curte mai multe cauze referitoare la articolul 82 din regulament, iar în una dintre ele au fost deja prezentate concluziile avocatului general, de care vom ține seama în cadrul acestei analize [7].

19. Înainte de a examina întrebările adresate, considerăm oportun să formulăm câteva observații introductive cu privire la principiile și la finalitatea regulamentului, care se vor dovedi utile pentru răspunsul la fiecare dintre întrebările preliminare.

20. Articolul 24 din regulament stabilește, în termeni generali, obligația operatorului de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a se asigura că prelucrarea datelor cu caracter personal este în conformitate cu regulamentul și pentru a fi în măsură să demonstreze acest lucru, în timp ce articolul 32 stabilește în mod mai specific aceeași obligație în ceea ce privește securitatea prelucrării. Articolele 24 și 32 prevăd în mod mai detaliat ceea ce se enunță deja la articolul 5 alineatul (2), care introduce, printre „principiile legate de prelucrarea datelor cu caracter personal", „principiul responsabilității". Acesta urmează în mod logic și este complementar „principiului integrității și confidențialității" prevăzut la articolul 5 alineatul (1) litera (f) și trebuie interpretat în lumina abordării bazate pe riscuri pe care regulamentul este fondat.

21. Principiul responsabilității este unul dintre pilonii regulamentului și una dintre cele mai importante inovații ale acestuia. El încredințează operatorului responsabilitatea de a lua măsuri proactive pentru a asigura respectarea regulamentului și pentru a fi pregătit să dovedească acest lucru [8].

22. În doctrină s-a vorbit despre o veritabilă schimbare culturală ca efect al „întinderii globale a obligației de responsabilitate" [9]. Nu atât respectarea formală a obligației legale sau a măsurii specifice, cât întreaga strategie corporativă exonerează operatorul de răspundere întrucât respectă normele privind protecția datelor.

23. Măsurile tehnice și organizatorice impuse de principiul responsabilității trebuie să fie „adecvate", având în vedere factorii menționați la articolul 24: natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și probabilitatea și gravitatea riscurilor la adresa drepturilor și libertăților persoanelor fizice.

24. Prin urmare, articolul 24 prevede caracterul adecvat al măsurilor pentru a se putea demonstra că prelucrarea respectă principiile și dispozițiile regulamentului.

25. În schimb, articolul 32 stabilește principiul responsabilității cu privire la măsurile concrete care trebuie luate pentru a asigura „[un] nivel de securitate corespunzător [riscului]". În acest sens, adaugă stadiul actual al dezvoltării și costurile implementării la factorii deja prevăzuți a fi luați în considerare la instituirea măsurilor tehnice și organizatorice.

[7] A se vedea Concluziile avocatului general Campos Sánchez-Bordona prezentate în cauza Österreichische Post (Prejudiciu moral legat de prelucrarea datelor cu caracter personal) (C-300/21, EU:C:2022:756).

[8] C. Docksey, Article 24. „Responsibility of the controller", în C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 561. Principiile și obligațiile prevăzute de reglementările privind protecția datelor ar trebui să pătrundă în structura culturală a organizațiilor, la toate nivelurile, iar nu să fie privite drept un set de cerințe legale care trebuie bifate de departamentul juridic.

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

26. Noțiunea de caracter adecvat presupune ca soluțiile adoptate pentru protejarea sistemelor informatice să atingă un nivel de acceptabilitate, atât din punct de vedere tehnic (relevanța măsurilor), cât și calitativ (eficacitatea protecției). Pentru a asigura respectarea principiilor necesității, relevanței și proporționalității, operațiunile de prelucrare trebuie să fie nu numai adecvate, ci și satisfăcătoare în raport cu obiectivele urmărite. În această logică, principiul minimizării, conform căruia toate etapele prelucrării datelor trebuie să vizeze întotdeauna reducerea la minimum a riscurilor de securitate, are un rol decisiv [10].

27. Întregul regulament se bazează pe prevenirea riscurilor și pe responsabilitatea operatorului și, prin urmare, pe o abordare teleologică care vizează obținerea celui mai bun rezultat posibil în ceea ce privește eficacitatea, cu alte cuvinte, o abordare foarte îndepărtată de logica formalistă legată de simpla obligație de a respecta proceduri specifice pentru a fi exonerat de răspundere [11].

28. Articolul 24 nu conține o listă exhaustivă de măsuri „adecvate”: va trebui efectuată o evaluare de la caz la caz. Acest lucru este în conformitate cu filosofia regulamentului, care explică că este de preferat ca procedurile care trebuie adoptate să fie selectate pe baza unei evaluări atente a situației specifice, astfel încât ele să fie cât mai eficiente posibil [12].

B. Prima întrebare preliminară

29. Prin intermediul primei întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolele 24 și 32 din regulament trebuie interpretate în sensul că producerea unei „încălcări a securității datelor cu caracter personal”, astfel cum este definită la articolul 4 punctul 12, este suficientă în sine pentru a concluziona că măsurile tehnice și organizatorice implementate de operator nu erau „adecvate” pentru a asigura protecția datelor.

30. Din modul de redactare a articolelor 24 și 32 din regulament rezultă că operatorul, atunci când alege măsurile tehnice și organizatorice pe care trebuie să le implementeze pentru a asigura respectarea regulamentului, trebuie să ia în considerare o serie de factori de evaluare enumerați la articolele respective și amintiți mai sus.

31. Operatorul dispune de o anumită marjă de manevră în stabilirea celor mai adecvate măsuri, având în vedere situația sa specifică, dar această alegere face totuși obiectul unui eventual control jurisdicțional al conformității măsurilor aplicate cu toate obligațiile și obiectivele stabilite în regulamentul propriu-zis.

32. În special, în ceea ce privește măsurile de securitate, articolul 32 alineatul (1) impune operatorului să ia în considerare „stadiul actual al dezvoltării”. Acest lucru implică limitarea nivelului tehnologic al măsurilor care trebuie implementate la ceea ce este posibil în mod

[10] E. Belisario, G. Riccio, G. Scorza, *GDPR, op. cit.*, p. 380.

[11] Acesta este motivul pentru care, după cum vom vedea, răspunsul la prima și la a patra întrebare preliminară nu poate fi decât negativ. Din dispozițiile regulamentului nu se poate deduce niciun automatism: de asemenea, simplul fapt că datele cu caracter personal au fost divulgate nu este suficient pentru a concluziona că măsurile tehnice și organizatorice adoptate nu sunt adecvate, dar nici faptul că divulgarea însăși a avut loc ca urmare a implicării unor persoane din afara organizației operatorului și din afara sferei de control a acestuia nu este suficient pentru a exonera operatorul de răspundere.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, p. 201. Legiuitorul european merge așadar dincolo de conceptul de securitate a prelucrării bazat pe prezența unor măsuri de securitate prestabilite, adoptând o metodologie specifică standardelor internaționale privind gestionarea sistemelor de informații bazată pe riscuri: aceasta prevede identificarea măsurilor de atenuare a riscurilor fără liste de verificare preconfigurate și de aplicare generală. Prin urmare, ar trebui utilizate orientări și standarde internaționale. Rezultatul acestei evaluări a riscurilor devine așadar obligatoriu atunci când organizația ia decizii pentru a reduce riscurile identificate, asumându-și astfel responsabilitatea.

rezonabil în momentul în care sunt luate măsurile: prin urmare, caracterul adecvat al măsurii de prevenire a riscurilor trebuie să fie proporțional cu soluțiile pe care le oferă stadiul actual al științei, tehnicii, tehnologiei și cercetării, ținând seama, de asemenea, după cum se va vedea, de costurile implementării.

33. Măsurile pot fi „adecvate” la un moment dat și, în pofida acestui fapt, pot fi eludate de infractorii cibernetici, prin utilizarea de instrumente foarte sofisticate care pot încălca inclusiv măsurile de securitate de ultimă generație.

34. În schimb, pare ilogic să se considere că intenția legiuitorului Uniunii a fost de a impune operatorului obligația de a preveni orice încălcare a securității datelor cu caracter personal, indiferent de diligența de care a dat dovadă în instituirea măsurilor de securitate [13].

35. Astfel cum s-a menționat mai sus, regulamentul se îndepărtează de automatisme, impunând un grad ridicat de responsabilitate din partea operatorului, ceea ce nu poate conduce însă la imposibilitatea acestuia de a dovedi că a respectat în mod corect obligațiile care îi revin.

36. În plus, articolul 32 alineatul (1) prevede că trebuie să se țină seama, după cum s-a menționat, de „costurile implementării” măsurilor tehnice și organizatorice în cauză. Rezultă că aprecierea caracterului adecvat al unor astfel de măsuri trebuie să se bazeze pe o evaluare comparativă între interesele persoanei vizate, care tind, în general, să se situeze la un nivel mai ridicat de protecție, și interesele economice și capacitatea tehnologică a operatorului, care uneori tind să se situeze la un nivel de protecție mai scăzut. Această evaluare comparativă trebuie să respecte cerințele principiului general al proporționalității.

37. Ar trebui adăugat, de asemenea, în vederea unei interpretări sistematice, că legiuitorul are în vedere posibilitatea producerii unor încălcări ale sistemelor; articolul 32 alineatul (1) litera (c) include printre măsurile propuse 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. Includerea unei astfel de capacități printre măsurile de securitate care garantează un nivel de securitate adaptat la risc ar fi inutilă dacă s-ar considera că simpla încălcare a sistemelor reprezintă, în sine, o dovadă a caracterului inadecvat al acestor măsuri.

C. A doua întrebare preliminară

38. Prin intermediul celei de a doua întrebări, instanța de trimitere solicită în esență să se stabilească care este obiectul și întinderea controlului jurisdicțional atunci când se verifică caracterul adecvat al măsurilor tehnice și organizatorice implementate de operatorul de date cu caracter personal în temeiul articolului 32 din regulament.

39. Având în vedere variabilitatea situațiilor care pot apărea în practică, regulamentul nu prevede, astfel cum s-a menționat mai sus, dispoziții obligatorii pentru stabilirea măsurilor tehnice și organizatorice care trebuie luate de operator pentru a se conforma cerințelor regulamentului. Prin urmare, caracterul adecvat al măsurilor luate va trebui evaluat *in concreto*, verificând dacă măsurile specifice au fost adecvate pentru a preveni în mod rezonabil riscul și pentru a reduce la minimum efectele negative ale încălcării.

[13] Noțiunea de caracter adecvat demonstrează fără echivoc intenția de a nu atribui relevanță tuturor măsurilor tehnice și organizatorice care sunt teoretic posibile. A se vedea în acest sens M. Gambini, „Responsabilità e risarcimento nel trattamento dei dati personali”, în V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 1059.

40. Deși este adevărat că alegerea și implementarea unor astfel de măsuri intră în sfera evaluării subiective a operatorului, întrucât măsurile menționate în regulament constituie simple exemple, controlul jurisdicțional nu poate fi limitat la controlul respectării de către operator a obligațiilor care decurg din articolele 24 și 32, și anume de a fi prevăzut (în mod formal) anumite măsuri tehnice și organizatorice. Prin intermediul acestui control trebuie să se efectueze o analiză concretă a conținutului măsurilor respective, a modului în care au fost aplicate și a efectelor practice ale acestora, pe baza elementelor disponibile și a împrejurărilor speței. După cum a observat în mod util guvernul portughez, „modul în care și-a îndeplinit obligațiile pare indisociabil de conținutul măsurilor adoptate, pentru a demonstra că, ținând seama de prelucrarea specifică a datelor (natura, domeniul de aplicare, contextul și scopurile acesteia), de stadiul actual al tehnologiei disponibile și de costurile sale, precum și de riscurile pentru drepturile și libertățile cetățenilor, operatorul a luat toate măsurile necesare și adecvate pentru a asigura un nivel de securitate adecvat riscului subiacent” [14].

41. Prin urmare, controlul jurisdicțional va trebui să ia în considerare toți factorii cuprinși la articolele 24 și 32, care, după cum s-a menționat mai sus, enumeră o serie de criterii pentru evaluarea caracterului adecvat și oferă exemple de măsuri care pot fi considerate adecvate. În plus, astfel cum au subliniat Comisia și toate statele membre care au prezentat observații cu privire la a doua întrebare, articolul 32 alineatele (1)-(3) subliniază necesitatea de a „asigura un nivel de securitate corespunzător riscului”, indicând alți factori relevanți în acest scop, cum ar fi posibila adoptare de către operator a unui cod de conduită aprobat sau a unui sistem de certificare aprobat, astfel cum se prevede la articolul 40 și, respectiv, la articolul 42 din regulament.

42. Adoptarea unor coduri de conduită sau a unor sisteme de certificare poate oferi un element util de evaluare în scopul îndeplinirii sarcinii probei și al controlului jurisdicțional aferent. Trebuie precizat însă că nu este suficient ca operatorul să adere la un cod de conduită, ci că îi revine sarcina de a dovedi că a luat efectiv măsurile pe care acesta le prevede, în conformitate cu principiul responsabilității. În schimb, certificarea constituie „în sine dovada conformității prelucrărilor efectuate cu regulamentul, chiar dacă aceasta este susceptibilă de a fi infirmată în practică” [15].

43. În sfârșit, trebuie remarcat că aceste măsuri trebuie revizuite și actualizate, dacă este necesar, în conformitate cu articolul 24 alineatul (1). Acest aspect va face de asemenea obiectul unei aprecieri din partea instanței naționale. Articolul 32 alineatul (1) din regulament [16] impune astfel operatorului o sarcină de control și de monitorizare constantă, atât anterior, cât și ulterior activităților de prelucrare, dar și de menținere și, eventual, de actualizare a măsurilor adoptate, atât pentru a preveni încălcările, cât și, după caz, pentru a limita efectele acestora.

[14] Observațiile scrise, punctul 31.

[15] M. Gambini, *Responsabilità*, *op. cit.*, p. 1067. Deținerea unei certificări se traduce, așadar, printr-o răsturnare a sarcinii probei în favoarea operatorului, căruia îi este înlesnită dovedirea faptului că a acționat cu respectarea obligațiilor prevăzute de regulament.

[16] Fiind prevăzut în mod expres, la litera (d), că aprecierea caracterului adecvat se extinde la eficacitatea măsurilor luate, care trebuie să fie testată, evaluată și apreciată cu regularitate, fie în faza inițială, fie periodic, pentru a garanta securitatea efectivă a tuturor tipurilor de prelucrare, indiferent de nivelul lor de risc; în plus, fiind prevăzut în mod explicit, la litera (c), faptul că măsurile tehnice și organizatorice implementate trebuie să prezinte 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. A se vedea M. Gambini, *Responsabilità*, *op. cit.*, p. 1064-1065.

44. Totuși, am fi înclinați să considerăm că nu este oportun ca următoarea hotărâre să includă o listă de elemente de fond, precum cea sugerată de guvernul portughez [17]. Acest lucru ar putea permite interpretări contradictorii, deoarece lista nu poate fi, bineînțeles, niciodată exhaustivă.

D. A treia întrebare preliminară

45. Prin intermediul primei părți a celei de a treia întrebări, instanța de trimitere solicită în esență Curții să stabilească dacă, având în vedere principiul responsabilității prevăzut la articolul 5 alineatul (2) și la articolul 24 coroborate cu considerentul (74) al regulamentului [18], în contextul unei acțiuni în despăgubire în temeiul articolului 82, sarcina probei privind caracterul adecvat al măsurilor tehnice și organizatorice în sensul articolului 32 revine operatorului de date cu caracter personal.

46. Considerațiile care precedă ne permit să răspundem pe scurt la această întrebare în sens afirmativ.

47. Modul de redactare, contextul și obiectivele regulamentului indică fără echivoc faptul că sarcina probei revine operatorului.

48. Din modul de redactare a diferitelor dispoziții ale regulamentului rezultă că operatorul trebuie să fie „în măsură” sau „să poată” „să demonstreze” respectarea obligațiilor prevăzute în regulament și, în special, să fi pus în aplicare măsuri adecvate în acest scop, astfel cum se arată în considerentul (74), la articolul 5 alineatul (2) și la articolul 24 alineatul (1). Așa cum subliniază guvernul portughez, la considerentul (74) menționat anterior se precizează că sarcina probei care revine astfel persoanei împuternicite de operator trebuie să includă dovada „eficacității măsurilor” în cauză.

49. Considerăm că această interpretare literală este susținută de considerațiile practice și teleologice menționate în continuare.

50. În ceea ce privește repartizarea sarcinii probei, în cadrul unei acțiuni în despăgubire întemeiate pe articolul 82, persoana vizată care a introdus acțiunea împotriva operatorului trebuie să dovedească, în primul rând, că a existat o încălcare a regulamentului, în al doilea rând, că a suferit un prejudiciu și, în al treilea rând, că există o legătură de cauzalitate între cele două elemente menționate anterior, astfel cum se menționează în toate observațiile scrise cu privire la

[17] Punctul 30 din observațiile scrise: „operatorul va trebui să demonstreze modul în care a evaluat toți factorii și circumstanțele referitoare la prelucrarea în cauză și, în special, rezultatul analizei de risc efectuate, riscurile identificate, măsurile concrete identificate pentru atenuarea acestor riscuri, justificarea opțiunilor alese în lumina soluțiilor tehnologice disponibile pe piață, eficacitatea măsurilor, corelația dintre măsurile tehnice și organizatorice, formarea personalului care prelucrează datele, existența externalizării operațiunilor de prelucrare a datelor, inclusiv dezvoltarea și menținerea de tehnologii informatice, precum și existența unui control din partea operatorului și a unor instrucțiuni precise date persoanelor împuternicite de către operator, în conformitate cu articolul 28 din RGPD, cu privire la prelucrarea datelor cu caracter personal de către acestea din urmă; modul în care a fost evaluată infrastructura de sprijin pentru sistemele informatice și de comunicații și modul în care a fost calificat nivelul de risc la adresa drepturilor și libertăților persoanelor vizate”.

[18] Potrivit considerentului (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.”

a cincea întrebare preliminară. Este vorba despre trei condiții cumulative, după cum reiese și din jurisprudența constantă a Curții și a Tribunalului, în contextul răspunderii extracontractuale a Uniunii [19].

51. Totuși, considerăm că obligația recurentei de a demonstra existența unei încălcări a regulamentului nu poate merge până la a-i solicita să demonstreze în ce mod măsurile tehnice și organizatorice implementate de operator nu sunt adecvate, în sensul articolelor 24 și 32.

52. Așa cum subliniază Comisia, prezentarea unor astfel de elemente de probă ar fi adesea aproape imposibilă în practică, întrucât persoanele vizate nu dispun, în general, de cunoștințe suficiente pentru a putea analiza aceste măsuri, nici de acces la toate informațiile aflate în posesia operatorului în cauză, în special în ceea ce privește metodele aplicate pentru a asigura securitatea unei asemenea prelucrări. În plus, operatorul ar putea uneori să susțină că refuzul său de a divulga aceste elemente persoanelor vizate se bazează pe motivul legitim de a nu face publice activitățile sale interne sau chiar pe aspecte care intră sub incidența secretului profesional, printre altele tocmai din motive de securitate.

53. Astfel, în cazul în care sarcina probei ar reveni persoanei interesate, rezultatul practic ar fi acela că dreptul la o cale de atac prevăzut la articolul 82 alineatul (1) ar fi în mare măsură golit de substanță. În opinia noastră, acest lucru nu ar fi în conformitate cu intențiile legiuitorului Uniunii, care, prin adoptarea acestui regulament, a urmărit să consolideze drepturile persoanelor vizate și obligațiile operatorilor în raport cu Directiva 95/46 pe care a înlocuit-o. Prin urmare, este mai logic și mai viabil din punct de vedere juridic ca operatorul să fie obligat să dovedească, în cadrul apărării sale în contextul unei acțiuni în despăgubire, că a respectat obligațiile care decurg din articolele 24 și 32 din regulamentul menționat prin adoptarea unor măsuri care sunt în mod efectiv adecvate.

54. Prin intermediul celei de a doua părți a celei de a treia întrebări, instanța de trimitere solicită Curții în esență să stabilească dacă un raport de expertiză judiciară poate fi considerat un element de probă necesar și suficient pentru a aprecia caracterul adecvat al măsurilor tehnice și organizatorice implementate de operatorul de date cu caracter personal într-o situație în care accesul neautorizat la date cu caracter personal și divulgarea neautorizată a acestora rezultă dintr-o activitate de piraterie informatică.

55. Considerăm, astfel cum au subliniat (în esență) și guvernele bulgar și italian, Irlanda și Comisia, că răspunsul la aceste întrebări trebuie să se întemeieze pe jurisprudența constantă a Curții potrivit căreia, în temeiul principiului autonomiei procedurale, în lipsa unei reglementări a Uniunii în materie, revine ordinii juridice interne a fiecărui stat membru atribuția de a reglementa modalitățile procedurale aplicabile procedurilor jurisdicționale de protecție a drepturilor particularilor, cu condiția totuși ca aceste modalități să nu fie, în situațiile reglementate de dreptul Uniunii, mai puțin favorabile decât cele aplicabile unor situații similare reglementate de dreptul național (principiul echivalenței) și să nu facă imposibilă în practică sau excesiv de dificilă exercitarea drepturilor conferite de ordinea juridică a Uniunii (principiul efectivității).

[19] A se vedea în special Hotărârea Curții din 5 septembrie 2019, Uniunea Europeană/Guardian Europe și Guardian Europe/Uniunea Europeană (C-447/17 P și C-479/17 P, EU:C:2019:672, punctul 147), Hotărârea Curții din 28 octombrie 2021, Vialto Consulting/Comisia (C-650/19 P, EU:C:2021:879, punctul 138), Hotărârea Tribunalului din 13 ianuarie 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, punctul 116), și Hotărârea Tribunalului din 29 septembrie 2021, Kočner/Europol (T-528/20, nepublicată, EU:T:2021:631, punctul 61), în care se amintește că trebuie îndeplinite trei condiții, și anume „nelegalitatea comportamentului imputat instituției Uniunii, caracterul real al prejudiciului și existența unei legături de cauzalitate între comportamentul acestei instituții și prejudiciul invocat”.

56. În speță, observăm că regulamentul nu conține nicio dispoziție care să stabilească metodele de probă admisibile și valoarea probatorie a acestora, în special în ceea ce privește măsurile de cercetare judecătorească (cum ar fi un raport de expertiză) pe care instanțele naționale pot sau trebuie să le dispună pentru a aprecia dacă un operator de date cu caracter personal a luat măsuri adecvate în temeiul acestui regulament. Prin urmare, considerăm că, în lipsa unor norme armonizate în materie, revine ordinii juridice interne a fiecărui stat membru sarcina de a stabili aceste modalități procedurale, sub rezerva respectării principiilor echivalenței și efectivității.

57. Acest „principiu al efectivității", care implică faptul că o instanță independentă trebuie să efectueze o apreciere imparțială, ar putea fi subminat dacă adjectivul „suficient" ar trebui înțeles în sensul care pare să îi fi fost atribuit de instanța de trimitere, cu alte cuvinte, să se poată deduce în mod automat, pe baza unei expertize, caracterul adecvat al măsurilor luate de operator [20].

E. A patra întrebare preliminară

58. Prin intermediul celei de a patra întrebări, instanța de trimitere solicită în esență să se stabilească dacă articolul 82 alineatul (3) din regulament trebuie interpretat în sensul că, în cazul unei încălcări a acestui regulament (care, precum în speță, constă în „divulgarea neautorizată" a datelor cu caracter personal sau în „accesul neautorizat" la acestea în sensul articolului 4 punctul 12) care a fost săvârșită de persoane care nu fac parte din personalul operatorului acestor date și care nu se află sub controlul său, acest fapt constituie un eveniment care nu este nicidecum imputabil operatorului și, prin urmare, un motiv de exonerare de răspundere în sensul articolului 82 alineatul (3).

59. Răspunsul la întrebare rezultă în mod direct din cele expuse mai sus cu privire la filosofia generală a regulamentului: nu este prevăzut niciun automatism și, prin urmare, simplul fapt că divulgarea neautorizată a datelor cu caracter personal sau accesul neautorizat la acestea a avut loc din cauza unor persoane aflate în afara controlului operatorului nu exonerează operatorul de răspundere.

60. În primul rând, din punct de vedere literal, trebuie arătat că nici articolul 82 alineatul (3), nici considerentul (146) nu prevăd condiții speciale care să poată fi îndeplinite pentru ca operatorul să fie exonerat de răspundere, cu excepția cazului în care se poate demonstra că „nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul". Din această formulare rezultă, pe de o parte, că operatorul nu poate fi exonerat de răspundere decât dacă dovedește că nu este răspunzător pentru evenimentul care a cauzat prejudiciul în cauză și, pe de altă parte, că nivelul probatoriu impus de această dispoziție este ridicat, având în vedere utilizarea sintagmei „în niciun fel", astfel cum a arătat Comisia [21].

61. Regimul răspunderii prevăzut la articolul 82 și, mai general, în întregul regulament a făcut obiectul unor ample dezbateri în doctrina diferitelor state membre. Acesta conține, de fapt, elemente tradiționale specifice răspunderii extracontractuale, dar și elemente care, din punctul de vedere al structurii dispozițiilor, o apropie de răspunderea contractuală sau chiar de o formă

[20] Observațiile scrise, punctul 39.

[21] Conform jurisprudenței constante a Curții potrivit căreia excepțiile de la o normă generală trebuie interpretate în mod restrictiv, eventuala exonerare de răspundere prevăzută la articolul 82 alineatul (3) trebuie interpretată în mod restrictiv. A se vedea prin analogie Hotărârea din 15 octombrie 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, punctul 53), și Hotărârea din 5 aprilie 2022, Commissioner of An Garda Síochána și alții (C-140/20, EU:C:2022:258, punctul 40).

de răspundere obiectivă, ca urmare a periculozității inerente activității de prelucrare a datelor. Nu este acesta contextul adecvat pentru a realiza o dezbatere complexă, dar, în opinia noastră, articolul 82 nu pare să instituie un regim de răspundere obiectivă [22].

62. Prejudiciul care rezultă dintr-o încălcare a securității datelor cu caracter personal poate fi o consecință culpabilă a neadoptării unor măsuri tehnice și organizatorice rezonabile și, în orice caz, adecvate pentru a preveni încălcarea, ținând seama de riscurile la adresa drepturilor și libertăților persoanelor fizice legate de activitatea de prelucrare. Aceste riscuri fac ca obligația de prevenire și de evitare a prejudiciului să fie mai strictă, fiind extinsă obligația de diligență care revine operatorului și persoanei împuternicite de acesta. Prin urmare, din interpretarea coroborată a obligațiilor de conduită ce revin operatorilor și persoanelor împuternicite de operator, precum și a dispoziției privind prezentarea de probe în scopul exonerării de răspundere, pusă în sarcina părții care a cauzat prejudiciul, pot fi aduse argumente în favoarea recunoașterii agravării răspunderii pentru culpa prezumată în ceea ce privește responsabilitatea pentru prelucrarea ilegală a datelor cu caracter personal în sensul articolului 82 din regulament [23].

63. Acest lucru are drept rezultat posibilitatea ca operatorul să prezinte probe în vederea exonerării (care nu sunt permise în cazul răspunderii obiective). În ceea ce privește sarcina probei, articolul 82 alineatul (3) din regulament stabilește norme favorabile persoanei prejudiciate, prevăzând o formă de răsturnare a sarcinii probei în ceea ce privește culpa persoanei care a cauzat prejudiciul [24], în deplină simetrie cu răsturnarea sarcinii probei menționată mai sus în ceea ce privește caracterul adecvat al măsurilor adoptate. Astfel, legiuitorul arată că este conștient de pericolele inerente acceptării unei repartizări diferite a sarcinii probei, respectiv că, în cazul în care ar stabili că revine persoanei fizice prejudiciate sarcina probei cu privire la culpa persoanei care a cauzat prejudiciul, aceasta ar reprezenta o sarcină excesivă și, prin urmare, ar periclita, în practică, eficacitatea protecției conferite prin acordarea de despăgubiri, în contextul unor norme legate de utilizarea noilor tehnologii. Ar putea fi deosebit de împovărător pentru persoana vizată să reconstituie și să aibă acces la modul în care a fost cauzat prejudiciul și, în consecință, să dovedească culpa autorului. Dimpotrivă, operatorul este în cea mai bună poziție pentru a oferi probe exoneratoare cu scopul de a dovedi că nu este în niciun fel răspunzător de evenimentul care a cauzat prejudiciul [25].

64. De asemenea, operatorul va trebui să demonstreze, în conformitate cu principiul responsabilității descris mai sus, că a făcut tot posibilul pentru a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util.

[22] Răspunderea civilă tinde să fie calificată drept obiectivă ori de câte ori persoana care acționează este obligată să ia toate măsurile teoretic posibile pentru a evita prejudiciul, independent de cunoștințele efective pe care le-a avut despre acestea sau de viabilitatea lor economică. În schimb, în cazul în care persoana care acționează este obligată să ia măsuri care sunt respectate în mod normal de un operator din sectorul economic relevant pentru a menține siguranța și pentru a preveni prejudiciile care pot rezulta din activitatea desfășurată, imputarea acestui prejudiciu tinde să se îndrepte către un regim de răspundere pentru o culpă specifică. M. Gambini, *Responsabilità*, *op. cit.*, p. 1055.

[23] M. Gambini, *Responsabilità*, *op. cit.*, p. 1059. În aceeași ordine de idei, pentru opinia potrivit căreia dovada adoptării măsurilor corespunzătoare nu constă în simpla invocare a diligenței maxime impuse, ci în demonstrarea unui al treilea fapt generator al prejudiciului, care prezintă caracteristicile de imprevizibilitate și de inevitabilitate proprii cazului fortuit și forței majore, S. Sica, „Sub art. 82”, în R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „dacă *dovedește* că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul” [articolul 82 alineatul (3)].

[25] M. Gambini, *Responsabilità*, *op. cit.*, p. 1060.

65. Revenind la întrebarea instanței de trimitere, pe baza celor arătate mai sus cu privire la natura răspunderii operatorului, în cazul în care, astfel cum am arătat, operatorul poate fi exonerat de răspundere demonstrând că încălcarea are o cauză de care nu este răspunzător în niciun fel, simplul fapt că evenimentul a fost cauzat de o persoană aflată în afara controlului său nu poate fi considerat a îndeplini această cerință.

66. În cazul în care un operator este victima unui atac din partea infractorilor cibernetici, evenimentul care a cauzat prejudiciul ar putea fi considerat ca nefiind imputabil operatorului, dar nu este exclus ca neglijența operatorului să se fi aflat la originea atacului în cauză, facilitând producerea acestuia ca urmare a lipsei sau insuficienței măsurilor de securitate a datelor cu caracter personal pe care operatorul este obligat să le implementeze. Este vorba despre aprecieri de fapt, specifice fiecărei cauze, care sunt lăsate la latitudinea instanței naționale sesizate, având în vedere elementele de probă care îi sunt prezentate.

67. De asemenea, reprezintă o experiență comună faptul că atacurile externe asupra sistemelor entităților publice sau private care dețin o cantitate mare de date cu caracter personal sunt mult mai frecvente decât atacurile interne. Prin urmare, operatorul trebuie să instituie măsuri adecvate pentru a face față în special atacurilor externe.

68. În sfârșit, din punct de vedere teleologic, trebuie remarcat faptul că regulamentul urmărește obiectivul unui nivel ridicat de protecție. În această privință, Curtea a subliniat deja că rezultă din articolul 1 alineatul (2) din regulament coroborat cu considerentele (10), (11) și (13) ale acestuia că regulamentul menționat impune instituțiilor organelor, oficiilor și agențiilor Uniunii, precum și autorităților competente ale statelor membre sarcina de a asigura un nivel ridicat de protecție a drepturilor referitoare la protecția datelor cu caracter personal garantate la articolul 16 TFUE și la articolul 8 din cartă [26].

69. În situația în care Curtea ar trebui să opteze pentru interpretarea potrivit căreia, în cazul în care încălcarea regulamentului ar fi săvârșită de un terț, operatorul ar trebui să fie exonerat în mod automat de răspundere în temeiul articolului 82 alineatul (3), o astfel de interpretare ar avea un efect incompatibil cu obiectivul de protecție urmărit de acest instrument, deoarece ar slăbi drepturile persoanelor vizate, în măsura în care ar limita această răspundere la cazurile în care încălcarea se datorează unor persoane care se află sub autoritatea și/sau controlul operatorului respectiv.

F. A cincea întrebare preliminară

70. Prin intermediul celei de a cincea întrebări, instanța de trimitere solicită Curții în esență să interpreteze noțiunea de „prejudiciu moral” în sensul articolului 82 din regulament. În special, aceasta solicită să se stabilească dacă dispozițiile articolului 82 alineatele (1) și (2) din regulament coroborate cu considerentele (85) și (146) ale acestuia [27] trebuie interpretate în sensul că, într-o

[26] A se vedea în acest sens Hotărârea din 15 iunie 2021, Facebook Ireland și alții (C-645/19, EU:C:2021:483, punctele 44 și 45).

[27] Potrivit considerentului (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 […]”. Potrivit considerentului (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. […]. Persoanele vizate ar trebui să primească despăgubiri integrale și eficace pentru prejudiciul pe care le-au suferit […]”

situație în care încălcarea acestui regulament a constat în accesul neautorizat la date cu caracter personal și în divulgarea neautorizată a acestor date de către infractorii cibernetici, împrejurarea că persoana vizată are temeri legate de o eventuală utilizare abuzivă a datelor sale cu caracter personal în viitor poate constitui în sine un prejudiciu (moral) care dă naștere unui drept la despăgubire.

71. Nici articolul 82, nici considerentele referitoare la repararea prejudiciului nu oferă un răspuns clar la această întrebare, dar din acestea pot fi extrase câteva elemente utile pentru analiză: prejudiciul moral, în plus față de prejudiciul material (sau patrimonial), poate da naștere dreptului la despăgubire; încălcarea regulamentului nu are în mod automat drept rezultat prejudiciul „cauzat” de aceasta sau, mai precis, încălcarea securității datelor cu caracter personal „poate conduce la” prejudicii fizice, materiale sau morale persoanelor fizice; noțiunea de prejudiciu ar trebui interpretată „în sens larg” în lumina jurisprudenței Curții, astfel încât să reflecte pe deplin obiectivele regulamentului; despăgubirea pentru prejudiciul „suferit” ar trebui să fie „integrală și eficace”.

72. Formularea literală a dispozițiilor regulamentului elimină deja orice eventuală sugestie că prejudiciul rezultă *in re ipsa*: obiectivul principal al răspunderii civile prevăzute de regulament este de a oferi satisfacție persoanei vizate, tocmai prin intermediul reparării „integrale și eficace” a prejudiciului suferit și, prin urmare, de a restabili echilibrul situației juridice afectate de încălcarea legii [28].

73. În plus, tot din punct de vedere sistematic, precum în dreptul concurenței, regulamentul prevede doi piloni de protecție: unul este de natură publică, prevăzând sancțiuni în cazul încălcării dispozițiilor regulamentului, celălalt de natură privată, prevăzând tocmai o răspundere civilă de natură extracontractuală, care poate fi calificată drept agravată pentru culpa prezumată, cu caracteristicile, inclusiv în ceea ce privește probele exoneratoare, evocate mai sus [29].

74. Prin urmare, o interpretare largă [30] a noțiunii de prejudiciu (moral) nu poate conduce la concluzia că legiuitorul a renunțat la necesitatea existenței unui „prejudiciu” real.

75. Adevărata problemă de fond este dacă, odată stabilită existența încălcării și legătura de cauzalitate, se poate naște un drept la despăgubiri pe baza unor simple îngrijorări, stări de anxietate și temeri resimțite de persoana vizată cu privire la o posibilă utilizare abuzivă viitoare a datelor cu caracter personal, în cazul în care o astfel de utilizare abuzivă nu a fost constatată și/sau persoana vizată nu a suferit niciun alt prejudiciu.

76. Potrivit unei jurisprudențe constante a Curții, noțiunile cuprinse într-o dispoziție de drept al Uniunii, care 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

[28] A se vedea Concluziile avocatului general Campos Sánchez-Bordona, citate mai sus, punctul 29 și nota de subsol 11. În aceleași concluzii, avocatul general își încheie în mod întemeiat analiza sub aspect literal, istoric, contextual și teleologic, excluzând caracterul „punitiv” al daunelor interese care trebuie acordate persoanelor vizate în temeiul articolului 82 (punctele 27-55), arătând, pe de o parte, că statele membre „nu trebuie (și nici nu pot) să aleagă între mecanismele prevăzute în capitolul VIII pentru a garanta protecția datelor. În cazul unei încălcări care nu dă naștere unor prejudicii, persoana vizată are în continuare (cel puțin) dreptul de a depune o plângere la o autoritate de supraveghere” și, pe de altă parte, că „perspectiva de a obține despăgubiri în afara oricărui prejudiciu ar stimula probabil litigiile civile și acțiuni care nu sunt, probabil, întotdeauna justificate și, în această măsură, ar putea descuraja activitatea de prelucrare a datelor” (punctele 54 și 55).

[29] Refuzul unui drept la despăgubiri pentru sentimente sau emoții slabe și trecătoare legate de o încălcare a normelor privind prelucrarea datelor nu ar lăsa, așadar, persoana vizată complet neprotejată (a se vedea în acest sens Concluziile avocatului general Campos Sánchez-Bordona, citate mai sus, punctul 115).

[30] Sau „în sens larg” potrivit formulării considerentului (146).

autonomă și uniformă, care trebuie stabilită ținând seama nu numai de formularea acesteia, ci și de contextul său, de obiectivele urmărite de reglementarea din care face parte această dispoziție și de geneza acesteia [31].

77. Astfel cum a subliniat domnul avocat general Campos Sánchez-Bordona [32], Curtea nu a elaborat o definiție generală a noțiunii de „prejudicii” care să poată fi aplicată în mod nediscriminatoriu în orice domeniu [33]. În ceea ce privește prejudiciul moral, din jurisprudența Curții se poate deduce că: atunci când unul dintre obiectivele dispoziției interpretate este protecția individului sau a unei anumite categorii de indivizi [34], noțiunea de prejudiciu trebuie să fie largă; în conformitate cu această abordare, despăgubirea se extinde la prejudiciile morale, chiar dacă acestea nu sunt menționate în dispoziția care face obiectul interpretării [35].

78. Deși jurisprudența Curții permite să se susțină că, în termenii enunțați, în dreptul Uniunii există un principiu de reparare a prejudiciului moral, suntem de acord cu domnul avocat general Campos că din aceasta nu se poate deduce o regulă potrivit căreia orice prejudiciu moral, oricât de grav ar fi, poate fi reparat [36].

79. În acest context, este relevantă distincția între prejudiciul moral care trebuie reparat și alte *inconveniente care rezultă din nerespectarea legii* și care, ca urmare a gravității lor minore, nu ar da naștere în mod obligatoriu dreptului la despăgubiri [37].

80. Curtea recunoaște diferența respectivă atunci când se referă la dificultăți și la neplăceri ca la o categorie distinctă de cea a prejudiciilor, în domeniile în care consideră că acestea trebuie să fie reparate [38].

31 A se vedea Hotărârea din 15 aprilie 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, punctul 48), și Hotărârea din 10 iunie 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, punctul 25).

32 A se vedea Concluziile avocatului general Campos Sánchez-Bordona, citate mai sus, punctul 104.

33 Curtea nu a identificat nici o metodă de interpretare – autonomă sau prin trimitere la legislația națională – care ar fi preferabilă: aceasta depinde de problema supusă examinării. A se vedea Hotărârea din 10 mai 2001, Veedfald (C-203/99, EU:C:2001:258, punctul 27), cu privire la produsele defecte, Hotărârea din 6 mai 2010, Walz (C-63/09, EU:C:2010:251, punctul 21), cu privire la răspunderea operatorilor de transport aerian și Hotărârea din 10 iunie 2021, Van Ameyde España (C-923/19, EU:C:2021:475, punctul 37 și următoarele), cu privire la răspunderea civilă aplicabilă accidentelor rezultate din circulația autovehiculelor.

34 De exemplu consumatorii de produse sau victimele accidentelor rutiere.

35 În domeniul pachetelor de servicii de călătorie, a se vedea Hotărârea din 12 martie 2002, Leitner (C-168/00, EU:C:2002:163); în domeniul răspunderii civile pentru pagubele produse de autovehicule, a se vedea Hotărârea din 24 octombrie 2013, Haasová (C-22/12, EU:C:2013:692, punctele 47-50), Hotărârea din 24 octombrie 2013, Drozdovs (C-277/12, EU:C:2013:685, punctul 40), și Hotărârea din 23 ianuarie 2014, Petillo (C-371/12, EU:C:2014:26, punctul 35).

36 A se vedea Concluziile avocatului general Campos Sánchez-Bordona, citate mai sus, punctul 105. Curtea a recunoscut compatibilitatea cu normele europene a reglementării naționale care, în scopul calculării despăgubirii, face distincție între prejudiciile morale legate de vătămările corporale rezultate din accidente în funcție de originea lor; a se vedea Hotărârea din 23 ianuarie 2014, Petillo (C-371/12, EU:C:2014:26), dispozitiv: dreptul Uniunii nu se opune „unei legislații naționale […] care prevede un regim special de despăgubire pentru prejudiciile morale rezultate din vătămări corporale ușoare cauzate de accidentele de circulație rutieră care limitează despăgubirea acestor prejudicii în raport cu ceea ce se admite în materie de reparare a prejudiciilor identice care rezultă din alte cauze decât aceste accidente”.

37 Această distincție este percepută în sistemele juridice naționale ca un corolar inevitabil al vieții în societate. Recent, în domeniul protecției datelor, în Italia, Tribunale de Palermo, sez. I civile, hotărârea 5/10/2017 nr. 5261, precum și Cass. Civ., Ord. sez. VI, nr. 17383/2020. În Germania printre altele AG Diez, 7.11.2018 - 8 C 130/18, LG Karlsruhe, 2.08.2019 - 8 O 26/19, și AG Frankfurt pe Main, 10.07.2020 - 385 C 155/19 (70). În Austria, OGH 6 Ob 56/21k.

38 A se vedea Hotărârea din 23 octombrie 2012, Nelson și alții (C-581/10 și C-629/10, EU:C:2012:657, punctul 51), cu privire la distincția dintre „prejudicii”, în sensul articolului 19 din Convenția pentru unificarea anumitor norme referitoare la transportul aerian internațional, încheiată la Montreal la 28 mai 1999, și „neplăceri”, în sensul Regulamentului nr. 261/2004, pentru care se acordă despăgubiri în conformitate cu articolul 7 din acesta din urmă, în conformitate cu Hotărârea din 19 noiembrie 2009, Sturgeon și alții (C-402/07 și C-432/07, EU:C:2009:716). În acest sector, ca și în cel al transportului de persoane pe mare și pe căi navigabile interioare reglementat de Regulamentul nr. 1177/2010, legiuitorul a putut recunoaște o categorie abstractă, deoarece factorul care a condus la dificultăți și esența sa sunt identice pentru toate părțile vizate. În opinia noastră, această deducție nu este posibilă în materia protecției datelor.

81. Din punct de vedere empiric, se poate observa că orice încălcare a unei norme privind protecția datelor personale va genera o anumită reacție negativă din partea persoanei vizate. Despăgubirea rezultată dintr-un simplu sentiment de nemulțumire față de nerespectarea legii ar fi ușor de confundat cu despăgubirea care nu implică existența unui prejudiciu, ceea ce, astfel cum am arătat, nu pare să fie cazul articolului 82 din regulament.

82. Faptul că, în împrejurări precum cele din litigiul principal, utilizarea abuzivă a datelor cu caracter personal este doar potențială, iar nu efectivă, este suficient pentru a se considera că persoana vizată a putut suferi un prejudiciu moral cauzat de încălcarea regulamentului, cu condiția ca persoana vizată să demonstreze că temerea față de o astfel de utilizare abuzivă i-a cauzat în mod concret și specific un prejudiciu emoțional real și cert [39].

83. Granița dintre simplele nemulțumiri (pentru care nu se acordă prejudicii) și prejudiciile morale efective (care trebuie reparate) este una fină, însă instanțele naționale, care au sarcina de a o delimita de la caz la caz, ar trebui să efectueze o evaluare atentă a tuturor elementelor furnizate de persoana vizată care solicită despăgubiri, căreia îi va reveni sarcina de a invoca cu precizie, iar nu în mod general, elemente concrete ce pot determina existența unui „prejudiciu moral efectiv suferit” ca urmare a încălcării securității datelor cu caracter personal, chiar dacă acesta nu atinge un prag prestabilit de gravitate deosebită: ceea ce contează este că nu este vorba despre o simplă percepție subiectivă, schimbătoare și care depinde, de asemenea, de elemente de caracter și de elemente personale, ci de obiectivarea unei neplăceri, fie ea de mică intensitate, dar demonstrabilă, pentru sfera fizică sau psihică sau pentru viața relațională a unei persoane; natura datelor cu caracter personal în cauză și importanța acestora în viața persoanei vizate și, poate, de asemenea, percepția societății, la momentul respectiv, cu privire la acel inconvenient specific legat de încălcarea datelor [40].

IV. Concluzie

84. Având în vedere ansamblul considerațiilor care precedă, propunem Curții să răspundă la întrebările preliminare adresate după cum urmează:

„Articolele 5, 24, 32 și 82 din Regulamentul 2016/679 trebuie interpretate în sensul că:

simpla existență a unei «încălcări a securității datelor cu caracter personal», astfel cum este definită la articolul 4 punctul 12, nu este suficientă în sine pentru a concluziona că măsurile tehnice și organizatorice implementate de operator nu au fost «adecvate» pentru a asigura protecția datelor în cauză;

atunci când evaluează caracterul adecvat al măsurilor tehnice și organizatorice implementate de operatorul de date cu caracter personal, instanța națională sesizată trebuie să efectueze un control care să cuprindă o analiză concretă atât a conținutului acestor măsuri, cât și a modului în care au fost implementate și a efectelor practice ale acestora;

[39] Potrivit Irlandei, aceste considerente sunt deosebit de importante în practică, în contextul criminalității cibernetice, deoarece, dacă orice persoană afectată – chiar și într-o mică măsură – de o încălcare ar avea dreptul la repararea prejudiciului moral, acest lucru ar avea un impact puternic, în special asupra operatorilor de date din sectorul public, care sunt finanțați din fonduri publice limitate și ar trebui mai degrabă să servească intereselor colective, inclusiv îmbunătățirii securității datelor cu caracter personal (observațiile scrise, punctul 72).

[40] A se vedea Concluziile avocatului general Campos Sánchez-Bordona, citate mai sus, punctul 116.

în contextul unei acțiuni în despăgubire în temeiul articolului 82 din RGPD, operatorul de date cu caracter personal are sarcina de a demonstra caracterul adecvat al măsurilor pe care le-a implementat în temeiul articolului 32 din acest regulament;

în conformitate cu principiul autonomiei procedurale, revine ordinii juridice interne a fiecărui stat membru sarcina de a stabili mijloacele de probă admisibile și forța lor probantă, inclusiv măsurile de cercetare judecătorească pe care instanțele naționale pot sau trebuie să le dispună pentru a aprecia dacă un operator de date cu caracter personal a implementat măsuri adecvate în sensul regulamentului menționat, cu respectarea principiilor echivalenței și efectivității definite de dreptul Uniunii;

faptul că încălcarea regulamentului menționat, care a condus la prejudiciul în cauză, a fost săvârșită de un terț nu constituie în sine un motiv de exonerare de răspundere a operatorului și, pentru a beneficia de exonerarea prevăzută la această dispoziție, operatorul trebuie să dovedească că nu este în niciun fel răspunzător pentru această încălcare;

prejudiciul care constă în temerea față de o eventuală utilizare abuzivă viitoare a datelor sale cu caracter personal, a cărui existență a fost dovedită de persoana vizată, poate constitui un prejudiciu moral care dă naștere unui drept la despăgubire, cu condiția ca persoana vizată să demonstreze că a suferit în mod individual un prejudiciu emoțional real și cert, aspect a cărui verificare, în fiecare caz în parte, revine instanței naționale sesizate.”