Judikatūras krājums

ĢENERĀLADVOKĀTA DŽOVANNI PITRUCELLAS
[*GIOVANNI PITRUZZELLA*]
SECINĀJUMI,
sniegti 2023. gada 27. aprīlī [1]

Lieta C-340/21

VB
pret
Natsionalna agentsia za prihodite

(*Varhoven administrativen sad* (Augstākā administratīvā tiesa, Bulgārija) lūgums sniegt prejudiciālu nolēmumu)

Lūgums sniegt prejudiciālu nolēmumu – Personas datu aizsardzība – Regula (ES) 2016/679 – Pārziņa atbildība – Apstrādes drošība – Personas datu apstrādes drošības pārkāpums – Nemateriāls kaitējums, kas nodarīts pārziņa bezdarbības dēļ – Prasība par kaitējuma atlīdzību

Vai kādas publiskas iestādes rīcībā esošu personas datu nelikumīga izpaušana "hakeru uzbrukuma" dēļ var būt pamats nemateriālā kaitējuma atlīdzināšanai datu subjektam tikai tāpēc vien, ka viņam ir uztraukums un bažas par viņa personas datu iespējamu turpmāku ļaunprātīgu izmantošanu? Kādi ir kritēriji, lai pie atbildības sauktu datu pārzini? Kā ir sadalīts pierādīšanas pienākums tiesvedībā? Kāds ir tiesas izvērtējuma apjoms?

I. Atbilstošās tiesību normas

1. Regulas 2016/679 [2] (turpmāk tekstā – "Regula") 4. pantā "Definīcijas" ir noteikts:

"Šajā regulā:

[..]

(12) "personas datu aizsardzības pārkāpums" ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem

[..]."

[1] Oriģinālvaloda – itāļu.

[2] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula).

2. Regulas 5. pantā "Personas datu apstrādes principi" ir noteikts:

"1. Personas dati:

[..]

(f) tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus ("integritāte un konfidencialitāte").

2. Pārzinis ir atbildīgs par atbilstību 1. punktam un var to uzskatāmi parādīt ("pārskatatbildība")."

3. Tās pašas regulas 24. pantā "Pārziņa atbildība" ir noteikts:

"1. Ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis īsteno atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu un spētu uzskatāmi parādīt, ka apstrāde notiek saskaņā ar šo regulu. Ja nepieciešams, minētos pasākumus pārskata un atjaunina.

2. Ja tas ir samērīgi attiecībā uz apstrādes darbībām, 1. punktā minētajos pasākumos ietver to, ka pārzinis īsteno atbilstīgu politiku attiecībā uz datu aizsardzību.

3. Atbilstību apstiprinātam rīcības kodeksam, kā minēts 40. pantā, vai apstiprinātam sertifikācijas mehānismam, kā minēts 42. pantā, var izmantot kā elementu, ar ko apliecina pārziņa pienākumu izpildi."

4. Tās 32. pantā "Apstrādes drošība" ir noteikts:

"1. Ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam, tostarp attiecīgā gadījumā cita starpā:

[..]

2. Novērtējot atbilstīgo drošības līmeni, ņem vērā jo īpaši riskus, ko rada apstrāde, jo īpaši nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

3. Atbilstību apstiprinātam rīcības kodeksam, kā minēts 40. pantā, vai apstiprinātam sertifikācijas mehānismam, kā minēts 42. pantā, var izmantot kā elementu, ar ko apliecina šā panta 1. punktā izklāstīto prasību izpildi.

[..]."

5. Tās pašas regulas 82. pantā "Tiesības uz kompensāciju un atbildība" ir noteikts:

"1. Jebkurai personai, kurai šīs regulas pārkāpuma rezultātā ir nodarīts materiāls vai nemateriāls kaitējums, ir tiesības no pārziņa vai apstrādātāja saņemt kompensāciju par tai nodarīto kaitējumu.

2. Jebkurš apstrādē iesaistītais pārzinis ir atbildīgs par kaitējumu, kas nodarīts ar apstrādi, kura pārkāpj šo regulu. [..].

3. Pārzini vai apstrādātāju atbrīvo no atbildības saskaņā ar 2. punktu, ja tas pierāda, ka nekādā veidā nav atbildīgs par notikumu, ar ko nodarīts attiecīgais kaitējums."

II. Fakti, tiesvedība un prejudiciālie jautājumi

6. 2019. gada 15. jūlijā Bulgārijas plašsaziņas līdzekļi izplatīja ziņu, ka esot konstatēta neatļauta piekļuve *Natsionalna agentsia za prihodite* (Valsts ieņēmumu dienests, Bulgārija; turpmāk tekstā – "*NAP*" [3]) informācijas sistēmai un ka internetā esot tikusi publiskota dažāda informācija par miljoniem personu – gan Bulgārijas pilsoņu, gan ārvalstnieku – nodokļiem un sociālo apdrošināšanu.

7. Daudzas personas, tostarp VB, kas ir kasācijas sūdzības iesniedzēja pamatlietā, cēla tiesā prasību pret *NAP*, lai tas viņām atlīdzinātu nemateriālo kaitējumu.

8. Šajā lietā kasācijas sūdzības iesniedzēja pamatlietā cēla prasību *Administrativen sad Sofia-grad* (Sofijas pilsētas Administratīvā tiesa, Bulgārija; turpmāk tekstā – "*ASSG*"), apgalvojot, ka *NAP* esot pārkāpis valsts tiesību normas, kā arī neesot izpildījis savu pārziņa pienākumu apstrādāt personas datus tādā veidā, "lai tiktu nodrošināta atbilstoša [..] drošība", īstenojot atbilstīgus tehniskos un organizatoriskos pasākumus saskaņā ar Regulas 679/2016 24. un 32. pantu. Kasācijas sūdzības iesniedzēja vēl apgalvoja, ka tai esot nodarīts nemateriāls kaitējums, kas esot izpaudies kā bažas un bailes par viņas personas datu turpmāku ļaunprātīgu izmantošanu.

9. Savukārt pretējā puse uzsvēra, ka neesot no kasācijas sūdzības iesniedzējas pamatlietā saņēmusi nevienu pieteikumu ar norādītiem personas datiem, kuriem konkrēti būtu notikusi piekļuve. Turklāt pēc ziņas par šo uzbrukumu *NAP* esot sasaucis augstākā līmeņa vadības sapulci ar ekspertiem pilsoņu tiesību un interešu aizsardzībai. *NAP* ieskatā, trūkstot arī cēloņsakarības starp kiberuzbrukumu un apgalvoto kaitējumu, jo dienests bija ieviesis visas procesu vadības sistēmas un informācijas drošības vadības sistēmas atbilstoši šajā jomā spēkā esošajiem starptautiskajiem standartiem.

10. Lietu pirmajā instancē izskatījusī *ASSG* noraidīja prasību, uzskatot, ka par datu izpaušanu dienests neesot atbildīgs, ka pierādīšanas pienākums jautājumā par veikto pasākumu atbilstību esot kasācijas sūdzības iesniedzējai un, visbeidzot, ka nekāds nemateriālais kaitējums neesot atlīdzināms.

[3] *NAP* ir pārzinis Regulas 4. panta 7. punkta izpratnē. Saskaņā ar valsts tiesību normām šis dienests ir Finanšu ministrijas padotībā esoša specializēta administratīva iestāde, kuras kompetencē ir veikt valsts finanšu līdzekļu uzskaiti, glabāšanu un iekasēšanu, kā arī likumā noteikto publisko un privāto valsts prasījumu uzskaiti, glabāšanu un iekasēšanu. *NAP* deleģēto publiskās varas funkciju izpildē tas apstrādā personas datus.

11. Pirmās instances tiesas spriedums tika pārsūdzēts, iesniedzot kasācijas sūdzību *Varhoven administrativen sad* (Augstākā administratīvā tiesa, Bulgārija). Izvirzītajos pamatos kasācijas sūdzības iesniedzēja pamatlietā norādīja, ka pirmās instances tiesa esot kļūdaini attiecinājusi pierādīšanas pienākumu jautājumā par drošības pasākumu neveikšanu. Arī nemateriālais kaitējums neesot jāpierāda, jo runa esot par faktisku, nevis tikai iespējamu nemateriālu kaitējumu.

12. *NAP* savukārt apgalvoja, ka pārziņa statusā esot veicis nepieciešamos tehniskos un organizatoriskos pasākumus, un apstrīdēja, ka faktisks nemateriālais kaitējums būtu pierādīts. Proti, bažas un bailes esot emocionālie stāvokļi, par kuriem neesot tiesību uz atlīdzinājumu.

13. Iesniedzējtiesa konstatēja atšķirīgus rezultātus tiesvedībās, kurās personas, kam nodarīts kaitējums, pret *NAP* bija cēlušas prasību par nemateriālā kaitējuma atlīdzināšanu.

14. Minētajos apstākļos iesniedzējtiesa apturēja tiesvedību un uzdeva Tiesai šādus prejudiciālos jautājumus:

"1) Vai [Eiropas Parlamenta un Padomes] Regulas (ES) 2016/679 [(2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)] 24. un 32. pants ir jāinterpretē tādējādi, ka ar konstatējumu par to, ka personas datu neatļautu izpaušanu vai piekļuvi tiem Regulas (ES) 2016/679 4. panta 12. punkta izpratnē ir izdarījušas personas, kuras nav pārziņa iestādes darbinieki un nav pakļautas tās kontrolei, ir pietiekami, lai varētu atzīt, ka pārziņa veiktie tehniskie un organizatoriskie pasākumi nav atbilstīgi?

2) Ja atbilde uz pirmo jautājumu būtu noliedzoša, kas un kādā apjomā ir jāizvērtē, veicot likumības pārbaudi tiesā saistībā ar vērtējumu par to, vai Regulas (ES) 2016/679 32. pantā minētie tehniskie un organizatoriskie pasākumi, kurus veicis pārzinis, ir atbilstīgi?

3) Ja atbilde uz pirmo jautājumu būtu noliedzoša, vai pārskatatbildības princips Regulas (ES) 2016/679 5. panta 2. punkta un 24. panta – kopsakarā ar tās 74. apsvērumu – izpratnē ir jāinterpretē tādējādi, ka tiesvedībā atbilstoši Regulas (ES) 2016/679 82. panta 1. punktam pārzinim ir pienākums pierādīt, ka tehniskie un organizatoriskie pasākumi, kas veikti saskaņā ar 32. pantu, ir atbilstīgi? Vai eksperta atzinuma saņemšana ir uzskatāma par nepieciešamu un pietiekamu pierādījumu tam, lai konstatētu, vai pārziņa veiktie tehniskie un organizatoriskie pasākumi tādā situācijā kā šeit aplūkojamā bija atbilstīgi, ja neatļautā piekļuve personas datiem un to neatļautā izpaušana ir "hakeru uzbrukuma" sekas?

4) Vai Regulas (ES) 2016/679 82. panta 3. punkts ir jāinterpretē tādējādi, ka personas datu neatļautā izpaušana vai piekļuve tiem Regulas (ES) 2016/679 4. panta 12. punkta izpratnē, ko, izmantojot "hakeru uzbrukumu", ir veikušas personas, kuras nav pārziņa iestādes darbinieki un kuras nav pakļautas tās kontrolei, kā tas noticis izskatāmajā lietā, ir uzskatāma par notikumu, par ko pārzinis nekādā veidā nav atbildīgs un kas attaisno tā atbrīvošanu no atbildības?

5) Vai Regulas (ES) 2016/679 82. panta 1. un 2. punkts - kopsakarā ar tās 85. un 146. apsvērumu - ir jāinterpretē tādējādi, ka tādā situācijā kā šeit aplūkojamā, kad noticis personas datu aizsardzības pārkāpums, kas izpaužas kā neatļauta piekļuve personas datiem un to neatļauta izpaušana "hakeru uzbrukuma" rezultātā, ja šāda ļaunprātīga izmantošana nav konstatēta un/vai ja datu subjektam nav nodarīts citāds kaitējums, plaši interpretējamajā nemateriālā

kaitējuma jēdzienā ietilpst – un dod tiesības saņemt attiecīgu kompensāciju – jau datu subjekta rūpes, bažas un bailes par personas datu iespējamu ļaunprātīgu izmantošanu nākotnē?"

III. Juridiskā analīze

A. Ievada apsvērumi

15. Šī lieta attiecas uz interesantiem un daļēji arī vēl nebijušiem jautājumiem par vairāku Regulas noteikumu [4] interpretāciju.

16. Visi pieci prejudiciālie jautājumi ir par vienu un to pašu, proti, par nosacījumiem tāda nemateriālā kaitējuma atlīdzināmībai, kas nodarīts datu subjektam, kura personas dati, kas atrodas kādas publiskas iestādes rīcībā, hakeru uzbrukuma rezultātā ir publiskoti internetā.

17. Ērtības labad ierosināšanu īsas atsevišķas atbildes uz katru lūgumā sniegt prejudiciālu nolēmumu ietverto prejudiciālo jautājumu, lai arī apzinos, ka konceptuāli notiks zināma pārklāšanās, jo četri pirmie jautājumi ir par to, kā identificēt priekšnosacījumus pārziņa saucamībai pie atbildības par Regulas noteikumu pārkāpumu [5], un piektais konkrētāk attiecas uz nemateriālā kaitējuma jēdzienu tā atlīdzināmības nolūkos [6].

18. Jāteic, ka par Regulas 82. pantu pašlaik Tiesā jau tiek skatītas vairākas lietas, vienā no kurām jau ir sniegti ģenerāladvokāta secinājumi, ko šajā analīzē ņemšu vērā [7].

19. Pirms uzdoto jautājumu iztirzāšanas uzskatu par lietderīgu izklāstīt dažus ievada apsvērumus par Regulas principiem un mērķiem; tie palīdzēs atbildēt uz katru prejudiciālo jautājumu atsevišķi.

20. Regulas 24. pantā ir vispārīgi noteikts pārziņa pienākums īstenot atbilstīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu, ka personas datu apstrāde atbilst Regulai, un spētu to pierādīt, savukārt 32. pantā konkrētāk ir noteikts tas pats pienākums attiecībā uz apstrādes drošību. Regulas 24. un 32. pantā ir konkrētāk izklāstīti noteikumi, kas jau paredzēti 5. panta 2. punktā un "personas datu apstrādes principu" skaitu papildina ar "pārskatatbildības principu". Tas loģiski seko 5. panta 1. punkta f) apakšpunktā noteiktajam "integritātes un konfidencialitātes principam" un papildina to; abi ir lasāmi Regulas pamatā esošās uz risku balstītās pieejas gaismā.

[4] Regulas 5. panta 2. punkts (par jebkura personas datu apstrādes pārziņa pārskatatbildības principu), 24. pants (par pasākumiem, kas minētajam datu pārzinim jāveic, lai nodrošinātu veiktās apstrādes atbilstību minētajai regulai), 32. pants (par šādu pienākumu konkrēti attiecībā uz apstrādes drošību) un 82. panta 1.–3. punkts (par kaitējuma, ko izraisa minētās regulas pārkāpums, atlīdzināšanu un par iespēju datu pārzinim veikt pasākumus, lai nodrošinātu atbilstību minētajai regulai), kā arī ar minētajiem pantiem saistītais 74., 85. un 146. apsvērums.

[5] a) pirmais jautājums ir par to, vai noteikto pasākumu neatbilstība ir izsecināma no tā vien, ka ir noticis uzbrukums sistēmām; b) otrais jautājums – par to, cik lielā mērā minēto pasākumu atbilstība ir pārbaudāma tiesā; c) trešais jautājums – par pašu pierādīšanas pienākumu un par vairākiem tehniskiem pierādījumu meklēšanas risinājumiem; d) ceturtais jautājums – par to, kāda nozīme saistībā ar atbrīvojamību no atbildības ir apstāklim, ka uzbrukums sistēmai noticis no ārpuses.

[6] Par piesauktajām Regulas jāteic, ka pirmie trīs jautājumi attiecas uz datu apstrādes pārziņa atbildības aspektiem saistībā ar veicamo pasākumu atbilstību (5., 24. un 32. pants), savukārt ceturtais un piektais – uz nosacījumiem atbrīvošanai no atbildības un atlīdzināma nemateriālā kaitējuma jēdzienu (82. pants).

[7] Skat. ģenerāladvokāta M. Kamposa Sančesa-Bordonas [*M. Campos Sánchez-Bordona*] secinājumus lietā *Österreichische Post* (Nemateriālais kaitējums saistībā ar personas datu apstrādi) (C-300/21, EU:C:2022:756).

21. Pārskatatbildības princips ir viens no Regulas pīlāriem un viens no tās nozīmīgākajiem jaunievedumiem. Tas uzliek pārzinim pienākumu veikt proaktīvas aizsardzības darbības, lai nodrošinātu Regulas ievērošanu, un būt gatavam pierādīt šo atbilstību [8].

22. Juridiskajā literatūrā tiek runāts par reālām kultūras pārmaiņām, kas izriet no "pārskatatbildības pienākuma visaptverošā rakstura" [9]. Runa ir ne tik daudz par juridiskā pienākuma vai konkrētā pasākuma formālu ievērošanu, cik paar uzņēmuma stratēģijas kopumu, kas pieņemts, lai atbrīvotu pārzini no atbildības, jo tas pilda personas datu regulējuma prasības.

23. Pārskatatbildības principa prasītajiem tehniskajiem un organizatoriskajiem pasākumiem ir jābūt "atbilstīgiem", ievērojot 24. pantā precizētos faktorus: apstrādes raksturs, piemērošanas joma, konteksts un mērķi, un risku, kas apdraud fizisko personu tiesības un brīvības, iespējamība un smagums.

24. Tādējādi pasākumu atbilstīguma prasību 24. pants noteic tālab, lai būtu iespējams pierādīt, ka apstrādē ir ievēroti Regulas principi un noteikumi.

25. Savukārt 32. pantā pārskatatbildības princips tiek attiecināts uz konkrētiem pasākumiem, kas jāveic, lai nodrošinātu "tādu drošības līmeni, kas atbilst riskam". Šajā procesā papildus jau paredzētajiem faktoriem, kas jāpatur prātā tehnisko un organizatorisko pasākumu plānošanā, ir jāņem vērā arī tehnikas attīstības līmenis un īstenošanas izmaksas.

26. Atbilstīguma jēdziens prasa, lai informātikas sistēmu nodrošināšanai rastie risinājumi atbilstu gan tehniskajā (pasākumu svarīgums), gan kvalitātes (aizsardzības efektivitāte) ziņā pieņemamajam līmenim. Lai nodrošinātu nepieciešamības, svarīguma un samērīguma principu ievērošanu, apstrādei ir jābūt ne tikai piemērotai iecerētajiem mērķiem, bet arī tiem atbilstošai. Šajā loģikā izšķirīga loma ir minimizēšanas principam, saskaņā ar kuru visos datu apstrādes posmos pastāvīgi jātiecas līdz minimumam samazināt drošības riskus [10].

27. Regula kopumā ir vērsta uz riska novēršanu un pārziņa padarīšanu par pārskatatbildīgu, un tāpēc tajā tiek izmantota teleoloģiska pieeja, tiecoties sasniegt efektivitātes ziņā labāko iespējamo rezultātu, kuram nav nekā kopīga ar formālo pieeju, kas paredz tikai pienākumu izpildīt noteiktas procedūras, lai atbrīvotos no atbildības [11].

[8] Docksey, C., "Article 24. Responsibility of the controller", no: C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR)*: *A Commentary*, Oxford University Press, 2020, 561. lpp. Datu aizsardzību reglamentējošajās tiesību normās noteiktajiem principiem un pienākumiem būtu jācaurvijas organizāciju kultūrai visos tās slāņos, nevis tie būtu jāuzskata par juridisku prasību virkni, par kuru ievērošanu jāparūpējas juridiskajam dienestam.

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

[10] E. Belisario, G. Riccio, G. Scorza, "GDPR", minēts iepriekš, 380. lpp.

[11] Tāpēc, kā redzēsim, uz pirmo un ceturto prejudiciālo jautājumu var atbildēt vienīgi noliedzoši. No Regulas normām nav izsecināms nekāds automātiskums: ne tikai personas datu izpaušanas fakts nav pietiekams, lai uzskatītu, ka veiktie tehniskie un organizatoriskie pasākumi nav bijuši atbilstīgi, bet arī apstāklis, ka pati izpaušana ir notikusi, iejaucoties ar pārziņa organizāciju nesaistītiem un ārpus tā kontroles sfēras esošiem subjektiem, nav pietiekams, lai atbrīvotu pārzini no atbildības.

28. Regulas 24. pantā nav ietverts izsmeļošs "atbilstīgu" pasākumu saraksts: to izvērtējums jāveic katrā konkrētajā gadījumā. Tas ir saskanīgi ar Regulas filozofiju, kas atklāj, kā priekšroka tika dota tam, lai veicamās procedūras tiktu izvēlētas, balstoties uz konkrētās situācijas rūpīgu izvērtējumu, tā, lai šie pasākumi būtu pēc iespējas efektīvāki [12].

B. Pirmais prejudiciālais jautājums

29. Ar pirmo jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai Regulas 24. un 32. pants ir jāinterpretē tādējādi, ka jau ar "personas datu aizsardzības pārkāpuma", kā definēts 4. panta 12. punktā, konstatējumu vien ir pietiekami, lai secinātu, ka pārziņa īstenotie tehniskie un organizatoriskie pasākumi nav bijuši "atbilstīgi", lai nodrošinātu datu aizsardzību.

30. No Regulas 24. un 32. panta formulējuma izriet, ka pārzinim, izvēloties tehniskos un organizatoriskos pasākumus, kas tam jāīsteno, lai nodrošinātu atbilstību Regulai, ir jāņem vērā virkne iepriekš atgādināto minētajos pantos noteikto vērtējuma faktoru.

31. Pārzinim ir zināma rīcības brīvība piemērotāko pasākumu noteikšanā, ievērojot tā īpašo situāciju, bet šī izvēle tomēr ir pakļauta iespējamai pārbaudei tiesā jautājumā par īstenoto pasākumu atbilstību visiem Regulā noteiktajiem pienākumiem un tās mērķiem.

32. Ciktāl 32. panta 1. punkts attiecas uz drošības pasākumiem, it īpaši tas liek pārzinim ņemt vērā "tehnikas līmeni" jeb tehniskās iespējas. Tas nozīmē veicamo pasākumu tehnoloģiskā līmeņa ierobežojumu līdz tādam, kāds ir saprātīgi iespējams pasākumu veikšanas brīdī, proti, pasākuma piemērotība riska novēršanai ir jābūt samērīgai ar risinājumiem, ko piedāvā pašreizējais zinātnes, tehnikas, tehnoloģijas un pētniecības attīstības līmenis, ņemot vērā arī, kā redzēsim, īstenošanas izmaksas.

33. Pasākumi var kādā noteiktā brīdī būt "atbilstīgi", tomēr kibernoziedznieki tos var apiet, izmantodami ļoti izsmalcinātus rīkus, kuri var pārkāpt arī tehnikas attīstības līmenim atbilstošus drošības pasākumus.

34. Turklāt šķiet neloģiski uzskatīt, ka Savienības likumdevēja nodoms būtu bijis noteikt pārzinim pienākumu nepieļaut nevienu personas datu pārkāpumu, neatkarīgi no rūpības drošības pasākumu plānošanā [13].

35. Kā jau teicu, Regula neparedz nekādu automātiskumu, pieprasot paaugstinātu pārskatatbildību no pārziņa; tas tomēr nedrīkst pārzinim liegt uzskatāmi parādīt, ka tas ir pareizi pildījis tam noteiktos pienākumus.

[12] L. Bolognini, E. Pelino, "Codice della disciplina privacy", Giuffrè, 2019, 201. lpp. Tātad Eiropas likumdevējs atsakās no domas, ka apstrādes drošība būtu atkarīga no iepriekš noteiktu drošības pasākumu esamības, un pieņem starptautiskajiem standartiem raksturīgo uz riskiem balstītas (*risk-based*) informātikas sistēmu pārvaldības metodiku: šī metodika paredz identificēt risku mazināšanas pasākumus, kas nav atkarīgi no iepriekš konfigurētiem un vispārīgi piemērojamiem kontrolsarakstiem (*checklists*). Tāpēc ir jāizmanto starptautiskās vadlīnijas un standarti. Tātad šāda risku izvērtējuma rezultāts kļūst saistošs brīdī, kad organizācija pieņem lēmumus identificēto risku mazināšanai, tādējādi uzņemoties pārskatatbildību.

[13] Atbilstības jēdziens nepārprotami parāda nodomu nepiešķirt nozīmi visiem teorētiski iespējamajiem tehniskajiem un organizatoriskajiem pasākumiem. Šajā nozīmē skat. M. Gambini, "Responsabilità e risarcimento nel trattamento dei dati personali", no: V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, 1059. lpp.

36. Turklāt 32. panta 1. punktā ir paredzēts, ka jāņem vērā, kā jau sacīts, aplūkojamo tehnisko un organizatorisko pasākumu "īstenošanas izmaksas". No tā izriet, ka minēto pasākumu atbilstīguma vērtējumā datu subjekta intereses, kas mēdz tiekties pēc augstāka aizsardzības līmeņa, ir jāsamēro ar pārziņa ekonomiskajām interesēm un tehnoloģiskajām spējām, kas dažkārt liek tiekties pēc zemāka līmeņa aizsardzības. Šajā samērošanā jāievēro vispārējā samērīguma principa prasības.

37. Sistēmiski interpretējot, jāpiebilst, ka likumdevējs ir ņēmis vērā iespēju, ka var notikt sistēmu uzlaušana; 32. pantā ierosināto pasākumu skaitā ietilpst 1. punkta c) apakšpunktā minētā spēja laikus atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums. Šādas iespējas iekļaušana starp drošības pasākumiem, kas nodrošina riskam atbilstošu drošības līmeni, būtu bezjēdzīga, ja sistēmu uzlaušana pati par sevi tiktu uzskatīta par pasākumu neatbilstības pierādījumu.

C. Otrais prejudiciālais jautājums

38. Ar otro jautājumu iesniedzējtiesa būtībā vaicā, kas un kādā apjomā ir jāpārbauda tiesā, izvērtējot personas datu apstrādes pārziņa īstenoto tehnisko un organizatorisko pasākumu atbilstīgumu saskaņā ar Regulas 32. pantu.

39. Ievērojot, ka praksē var rasties daudz dažādu situāciju, Regulā, kā jau teicu, nav paredzēti saistoši noteikumi par to, kā nosakāmi tehniskie un organizatoriskie pasākumi, kas pārzinim jāveic, lai atbilstu Regulas prasībām. Veikto pasākumu atbilstīgums tātad būs jāvērtē katrā atsevišķajā gadījumā, pārbaudot, vai konkrētie pasākumi ir bijuši piemēroti, lai saprātīgi novērstu risku un līdz minimumam samazinātu pārkāpuma negatīvās sekas.

40. Kaut arī katrā ziņā ir taisnība, ka minēto pasākumu izvēle un īstenošana ietilpst pārziņa subjektīvajā vērtējumā, tā kā Regulā šie pasākumi ir minēti tikai piemēra pēc, tiesas izvērtējums nevar aprobežoties ar pārbaudi, vai pārzinis ir izpildījis no 24. un 32. panta izrietošos pienākumus, proti, ka tas ir (formāli) paredzējis noteiktus tehniskos un organizatoriskos pasākumus. Tiesai ir konkrēti jāizanalizē minēto pasākumu saturs, veids, kādā tie pielietoti un to praktiskās sekas, pamatojoties uz tās rīcībā esošajiem pierādījuma elementiem un konkrētā gadījuma apstākļiem. Kā pamatoti norādījusi Portugāles valdība, "veids, kādā pārzinis izpildījis savus pienākumus, šķiet nesaraujami saistīts ar veikto pasākumu saturu, lai pierādītu, ka, ņemot vērā datu specifisko apstrādi (to raksturu, tvērumu, kontekstu un mērķus), pieejamo tehnoloģiju attīstības līmeni un to izmaksas, kā arī riskus pilsoņu tiesībām un brīvībām, pārzinis ir veicis visus pasākumus, kas nepieciešami un atbilstoši, lai nodrošinātu tādu drošības līmeni, kas atbilst iespējamajam riskam" [14].

41. Tāpēc tiesā veicamajā pārbaudē būs jāņem vērā visi faktori, kas minēti 24. un 32. pantā, kuros, kā jau teicu, tiek uzskaitīta virkne kritēriju atbilstīguma izvērtēšanai un sniegti par atbilstīgiem atzīstamu pasākumu piemēri. Turklāt, kā norāda Komisija un visas par otro jautājumu apsvērumus sniegušās dalībvalstis, 32. panta 1.–3. punktā ir uzsvērta nepieciešamība "[nodrošināt] tādu drošības līmeni, kas atbilst riskam", norādot citus šajā ziņā nozīmīgos faktorus, kā, piemēram, to, ka pārzinis, iespējams, ir pieņēmis apstiprinātu rīcības kodeksu vai apstiprinātu sertifikācijas sistēmu, kā paredzēts attiecīgi Regulas 40. un 42. pantā.

[14] Rakstveida apsvērumi, 31. punkts.

42. Rīcības kodeksu vai sertifikācijas sistēmu pieņemšana var būt noderīgs vērtēšanas elements, pildot pierādīšanas pienākumu un veicot saistīto pārbaudi tiesā. Tomēr ar precizējumu – nav pietiekami, ka pārzinis pieņem rīcības kodeksu, tam ir pienākums atbilstoši pārskatatbildības principam pierādīt, ka tas ir konkrēti veicis kodeksā paredzētos pasākumus. Savukārt sertifikācija jau "pati par sevi ir pierādījums veiktās apstrādes atbilstīgumam regulai, kaut arī to var praksē apstrīdēt"[15].

43. Visbeidzot jānorāda, ka minētie pasākumi saskaņā ar 24. panta 1. punktu ir jāpārskata un vajadzības gadījumā jāmodernizē. Arī tas būs jāizvērtē valsts tiesai. Proti, Regulas 32. panta 1. punktā[16] pārzinim ir noteikts pienākums pastāvīgi, preventīvi un secīgi kontrolēt apstrādes darbības, kā arī uzturēt un, iespējams, modernizēt veiktos pasākumus tālab, lai novērstu pārkāpumus un – gadījumā, ja tie notikuši, – mazinātu to sekas.

44. Tomēr uzskatu, ka taisāmajā spriedumā nebūtu lietderīgi ietvert tādu materiāltiesisku elementu uzskaitījumu kā Portugāles valdības ierosinātais[17]. Tas varētu atstāt vietu pretrunīgām interpretācijām, jo saraksts acīmredzami nekad nevarētu būt izsmeļošs.

D. Trešais prejudiciālais jautājums

45. Ar trešā jautājuma pirmo daļu iesniedzējtiesa būtībā vaicā Tiesai, vai, ņemot vērā Regulas 5. panta 2. punktā un 24. pantā – lasot tos kopsakarā ar tās 74. apsvērumu[18] – noteikto pārskatatbildības principu, regulas 82. pantā paredzētās prasības par kaitējuma atlīdzību ietvaros tehnisko un organizatorisko pasākumu atbilstīgums 32. panta izpratnē ir jāpierāda personas datu pārzinim.

46. Iepriekš izklāstītie apsvērumi ļauj man īsumā uz šo jautājumu atbildēt apstiprinoši.

47. Regulas formulējums, konteksts un mērķi viennozīmīgi liecina, ka pierādīšanas pienākums ir pārzinim.

48. No vairāku Regulas normu formulējuma izriet, ka pārzinim ir "jāspēj" "uzskatāmi parādīt" /"pierādīt", ka tas ir īstenojis šim nolūkam atbilstīgus pasākumus, kā norādīts 74. apsvērumā, 5. panta 2. punktā un 24. panta 1. punktā. Kā uzsver Portugāles valdība, minētajā 74. apsvērumā ir precizēts, ka pārzinim tādējādi noteiktajam pierādīšanas pienākumam ir jāietver konkrētais pierādījums, ka "pasākumi ir iedarbīgi".

[15] M. Gambini, "Responsabilità", minēts iepriekš, 1067. lpp. Tāpēc sertifikācijas ceļā pierādīšanas pienākums tiek apvērsts par labu pārzinim, kuram ir vieglāk pierādīt, ka tas ir darbojies, ievērojot Regulā noteiktās prasības.

[16] Konkrēti nosakot d) apakšpunktā, ka atbilstības vērtējums attiecas arī uz veikto pasākumu efektivitāti, kas ir regulāri jātestē, jāizvērtē un jānovērtē – gan sākotnēji, gan periodiski –, lai nodrošinātu visu apstrādes veidu faktisku drošību neatkarīgi no to riska līmeņa; un vēl, konkrēti paredzot c) apakšpunktā, ka īstenotajiem tehniskajiem un organizatoriskajiem pasākumiem ir jāuzrāda spēja laikus atjaunot personas datu pieejamību un piekļuvi tiem gadījumā, ja ir noticis fizisks vai tehnisks negadījums. Skat. M. Gambini, "Responsabilità", minēts iepriekš, 1064.–1065. lpp.

[17] Rakstveida apsvērumu 30. punkts: "Pārzinim būs jāpierāda, kā tas ir izvērtējis visus faktorus un apstākļus saistībā ar konkrēto apstrādi, un it īpaši veiktās risku analīzes rezultāts, identificētie riski, konkrētie rastie pasākumi minēto risku mazināšanai, izvēļu, kas veiktas tirgū pieejamo tehnoloģisko risinājumu gaismā, pamatojums, pasākumu iedarbīgums, korelācija starp tehniskajiem un organizatoriskajiem pasākumiem, datu apstrādes personāla apmācība, ārpakalpojumu izmantošana datu apstrādes darbību – t.sk. informātikas tehnoloģiju izstrādes un uzturēšanas – veikšanai, pārziņa veiktas kontroles esamība un apstrādātājiem saskaņā ar VDAR 28. pantu sniegtu konkrētu norādījumu esamība par to, kā tiem apstrādāt personas datus; kā ir tikusi izvērtēta komunikāciju un informācijas sistēmu atbalsta infrastruktūra un kā ir ticis klasificēts datu subjektu tiesību un brīvību apdraudējuma riska līmenis."

[18] Saskaņā ar 74. apsvērumu "būtu jāparedz pārziņa pienākumi un atbildība par ikvienu personas datu apstrādi, ko veic pārzinis vai pārziņa vārdā. Jo īpaši, pārzinim būtu jāuzliek pienākums īstenot piemērotus un efektīvus pasākumus, un viņam vajadzētu spēt uzskatāmi parādīt, ka apstrādes darbības notiek saskaņā ar šo regulu, tostarp, ka pasākumi ir iedarbīgi. Minētajos pasākumos būtu jāņem vērā apstrādes raksturs, piemērošanas joma, konteksts un nolūki un risks, ko tā rada fizisku personu tiesībām un brīvībām".

49. Šo gramatisko interpretāciju, manuprāt, apstiprina turpmākie praktiskie un teleoloģiskie apsvērumi.

50. Kas attiecas uz pierādīšanas pienākuma sadali, 82. pantā paredzētās prasības par kaitējuma atlīdzību ietvaros datu subjektam, kas cēlis prasību pret pārzini, ir jāpierāda, pirmkārt, ka ir noticis Regulas pārkāpums, otrkārt, ka viņam ir nodarīts kaitējums un, treškārt, ka pastāv cēloņsakarība starp abiem iepriekšējiem elementiem, kā uzsvērts visos rakstveida apsvērumos par piekto prejudiciālo jautājumu. Šie trīs nosacījumi ir kumulatīvi, kā izriet arī no Tiesas un Vispārējās tiesas pastāvīgās judikatūras par Savienības ārpuslīgumisko atbildību [19].

51. Tomēr uzskatu, ka kasācijas sūdzības iesniedzējas pienākums pierādīt Regulas pārkāpuma esamību nevar būt tik apjomīgs, ka tai tiktu prasīts uzskatāmi parādīt, kādā tieši veidā pārziņa īstenotie tehniskie un organizatoriskie pasākumi nav atbilstīgi 24. un 32. panta izpratnē.

52. Kā norāda Komisija, šādu pierādījumu iesniegšana praksē bieži būtu gandrīz neiespējama, jo datu subjektiem parasti nav nedz pietiekamu zināšanu šādu pasākumu analizēšanai, nedz piekļuves visai apstrīdētā pārziņa rīcībā esošajai informācijai, it īpaši attiecībā uz metodēm, kas izmantotas, lai nodrošinātu šādas apstrādes drošību. Turklāt pārzinis dažkārt varētu apgalvot, ka tā atteikums atklāt šos faktus datu subjektiem balstās uz leģitīmo pamatu nepubliskot savus iekšējos darījumus vai arī elementus, uz kuriem attiecas profesionālais noslēpums, citstarp tieši drošības apsvērumu dēļ.

53. Tāpēc, ja tiktu uzskatīts, ka pierādīšanas pienākums gulstas uz datu subjektu, praktiskais rezultāts būtu tāds, ka 82. panta 1. punktā paredzētās tiesības celt prasību zaudētu lielu daļu sava tvēruma. Manuprāt, tas nebūtu saskanīgi ar Savienības likumdevēja ieceri – ar šīs Regulas pieņemšanu nostiprināt datu subjektu tiesības un datu apstrādātāju pienākumus salīdzinājumā ar Direktīvu 95/46, kas ar šo Regulu ir aizstāta. Tāpēc ir loģiskāk un juridiski pamatoti, ka pārzinim, aizstāvoties tiesvedībā pret prasību par kaitējuma atlīdzību, ir jāpierāda, ka tas ir izpildījis visus no minētās Regulas 24. un 32. panta izrietošos pienākumus, veicot patiesi atbilstīgus pasākumus.

54. Ar trešā jautājuma otro daļu iesniedzējtiesa būtībā jautā Tiesai, vai tiesas ekspertīzi var uzskatīt par nepieciešamu un pietiekamu pierādījumu, lai izvērtētu personas datu apstrādes pārziņa īstenoto tehnisko un organizatorisko pasākumu atbilstīgumu situācijā, kurā personas datu neatļauta izpaušana un piekļuve tiem ir "hakeru uzbrukuma" (*hacking*) rezultāts.

55. Uzskatu – gluži kā (būtībā) uzsvērušas arī Bulgārijas un Itālijas valdības, Īrija un Komisija –, ka atbildei uz šiem jautājumiem ir jābalstās uz mūsu pastāvīgo judikatūru, atbilstoši kurai saskaņā ar procesuālās autonomijas principu, ja nav Savienības tiesību normu attiecīgajā jomā, katras dalībvalsts valsts tiesiskajā regulējumā ir jāregulē tiesvedību, kurās tiek aizstāvētas personu tiesības, procesuālā kārtība, tomēr ar nosacījumu, ka minētās tiesību normas Savienības tiesību regulētajās situācijās nav mazāk labvēlīgas par tām, kas regulē analoģiskas situācijas valsts tiesībās (līdzvērtības princips), un nepadara par praktiski neiespējamu vai pārmērīgi grūtu Savienības tiesību piešķirto tiesību izmantošanu (efektivitātes princips).

[19] It īpaši skat. Tiesas spriedumus, 2019. gada 5. septembris, Eiropas Savienība/*Guardian Europe* un *Guardian Europe*/Eiropas Savienība (C-447/17 P un C-479/17 P, EU:C:2019:672, 147. punkts), un 2021. gada 28. oktobris, *Vialto Consulting*/Komisija (C-650/19 P, EU:C:2021:879, 138. punkts), kā arī Vispārējās tiesas spriedumus, 2021. gada 13. janvāris, *Helbert*/*EUIPO* (T-548/18, EU:T:2021:4, 116. punkts), un 2021. gada 29. septembris, *Kočner*/*Europol* (T-528/20, nav publicēts, EU:T:2021:631, 61. punkts), kuros atgādināts, ka ir jābūt izpildītam trim šādiem nosacījumiem: "Savienības iestādei pārmestā rīcība ir prettiesiska, zaudējumi ir reāli un pastāv cēloņsakarība starp iestādes rīcību un apgalvoto kaitējumu".

56. Šajā lietā jākonstatē, ka Regulā nav neviena noteikuma, kā noteikt pieļaujamās pierādīšanas metodes un to pierādījuma spēku, it īpaši attiecībā uz pierādījumu vākšanas pasākumiem (kā, piemēram, ekspertīze), ko valstu tiesas var uzdot vai ko tām ir jāuzdod tālab, lai izvērtētu, vai personas datu pārzinis ir īstenojis atbilstīgus pasākumus minētās Regulas izpratnē. Tāpēc uzskatu, ka, tā kā nav saskaņotu tiesību normu šajā jomā, minētā procesuālā kārtība – nodrošinot līdzvērtības un efektivitātes principu ievērošanu – ir jānosaka katras dalībvalsts valsts tiesiskajā regulējumā.

57. Minētais "efektivitātes princips", kas nozīmē, ka neatkarīgai tiesai ir jāveic objektīvs vērtējums, varētu tikt apdraudēts, ja apzīmējums "pietiekams" būtu saprotams tādā nozīmē, kādu tam to, manuprāt, piešķir iesniedzējtiesa, un, proti, ka no kādas ekspertīzes var automātiski secināt, ka pārziņa veiktie pasākumi ir atbilstīgi [20].

E. Ceturtais prejudiciālais jautājums

58. Ar ceturto jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai Regulas 82. panta 3. punkts ir jāinterpretē tādējādi, ka tāda minētās Regulas pārkāpuma gadījumā (kas, piemēram, šajā lietā izpaužas kā personas datu "neatļauta izpaušana" vai "neatļauta piekļuve" tiem 4. panta 12. punkta izpratnē), kuru izdarījušas personas, kas nav minēto datu pārziņa darbinieki un nav viņa kontrolē, tas ir notikums, par kuru pārzinis nekādā veidā nav atbildīgs, un tātad ir pamats viņa atbrīvošanai no atbildības saskaņā ar 82. panta 3. punktu.

59. Atbilde uz šo jautājumu lineāri izriet no tā, ko iepriekš izklāstīju par Regulas vispārējo filozofiju, proti, tajā nav paredzēti automātiskumi, un tātad tikai fakts, ka personas datu neatļauta izpaušana vai piekļuve tiem ir notikusi tādu subjektu dēļ, kuri atrodas ārpus pārziņa kontroles jomas, neatbrīvo pārzini no atbildības.

60. Vispirmām kārtām par formulējumu ir jānorāda, ka nedz 82. panta 3. punktā, nedz 146. apsvērumā nav noteikti nekādi specifiski nosacījumi, kas būtu jāizpilda, lai pārzinis varētu tikt atbrīvots no atbildības, tālab tam ir tikai jāpierāda, ka tas "nekādā veidā nav atbildīgs par notikumu, ar ko nodarīts attiecīgais kaitējums". No šā formulējuma izriet, pirmkārt, ka pārzinis var tikt atbrīvots no atbildības tikai tad, ja tas pierāda, ka nav atbildīgs par notikumu, ar ko nodarīts konkrētais kaitējums, un, otrkārt, ka šajā noteikumā prasītais pierādījuma līmenis ir augsts, ievērojot termina "nekādā veidā" izmantošanu, kā uzsvērusi Komisija [21].

61. Par Regulas 82. pantā un vispārīgāk visā Regulā paredzēto atbildības režīmu ir notikušas plašas debates dažādu dalībvalstu juridiskās literatūras autoru starpā. Tajā ir ietverti ne tikai elementi, kas tradicionāli raksturīgi ārpuslīgumiskajai atbildībai, bet arī elementi, kuri noteikumu struktūrā pietuvina to līgumiskajai atbildībai vai pat kādam objektīvās jeb bezvainas atbildības veidam datu apstrādes darbībai piemītošās bīstamības dēļ. Šeit būtu nevietā šīs debates atreferēt, taču, manuprāt, nešķiet, ka 82. pants identificē bezvainas atbildības režīmu [22].

[20] Rakstveida apsvērumi, 39. punkts.

[21] Saskaņā ar Tiesas pastāvīgo judikatūru – atbilstoši kurai izņēmumi no vispārīgas normas ir jāinterpretē šauri – 82. panta 3. punktā paredzētais iespējamais atbrīvojums no atbildības ir jāinterpretē šauri. Pēc analoģijas skat. spriedumus, 2020. gada 15. oktobris, *Association française des usagers de banques* (C-778/18, EU:C:2020:831, 53. punkts), un 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c. (C-140/20, EU:C:2022:258, 40. punkts).

[22] Civiltiesiskā atbildība mēdz tikt kvalificēta kā objektīva [jeb "atbildība bez vainas", "atbildība neatkarīgi no vainas", "bezvainas atbildība"] ikreiz, kad darbības subjektam ir jāveic visi teorētiski iespējamie pasākumi kaitējuma nepieļaušanai, neatkarīgi no tā, vai tie tam ir zināmi un ir finansiāli paveicami. Savukārt tad, kad darbības subjektam ir noteikts pienākums rīkoties tā, kā parasti dara attiecīgās saimnieciskās nozares uzņēmējs, lai uzturētu drošību un nepieļautu kaitējumu, ko var radīt veiktā darbība, saukšana pie atbildības par kaitējumu mēdz notikt "atbildības specifiskas vainas dēļ" režīmā. M. Gambini, "Responsabilità", minēts iepriekš, 1055. lpp.

62. Personas datu apstrādes pārkāpuma rezultātā nodarītais kaitējums var tikt kvalificēts kā sekas, kādas izriet no vainojamas rīcības, neveicot tehniskos un organizatoriskos pasākumus, kas būtu saprātīgi un katrā ziņā piemēroti kaitējuma novēršanai, ievērojot ar apstrādes darbību saistītos personu tiesību un brīvību apdraudējuma riskus. Šādi riski padara kaitējuma prevencijas un novēršanas pienākumu stingrāku, paplašinot pārziņa rūpības pienākuma apjomu. Tāpēc, pārziņu pienākumus skatot kopsakarā ar kaitējumu nodarījušajam doto iespēju iesniegt vainu atspēkojošu pierādījumu, var izdarīt secinājumu par labu tādas atbildības atzīšanai, kas prezumētās vainas dēļ Regulas 82. pantā aprakstītās atbildības par personas datu nelikumīgu apstrādi gadījumā kvalificējama kā smagāka [23].

63. No tā izriet pārziņa iespēja iesniegt vainu atspēkojošu pierādījumu (kas nav atļauts bezvainas atbildības režīmā). Attiecībā uz pierādīšanas pienākuma formulējumu Regulas 82. panta 3. punktā ir noteikts kaitējumā cietušajam labvēlīgs režīms, nosakot kaitējumu nodarījušā vainas pierādīšanas pienākuma apvērstu formu [24], gluži simetriski iepriekš minētā pierādīšanas pienākuma apvērstajai formai par veikto pasākumu atbilstīgumu. Tādējādi likumdevējs parāda, ka apzinās briesmas, kādas raksturīgas pierādīšanas pienākuma atšķirīga sadalījuma atzīšanai; ka tad, ja fiziskajai personai, kam nodarīts kaitējums, tiktu uzlikts pienākums pierādīt kaitējumu nodarījušās personas vainu, tas galu galā pārmērīgi apgrūtinātu viņa stāvokli un tātad faktiski apdraudētu kaitējuma atlīdzības operativitāti jauno tehnoloģiju izmantošanu reglamentējošo tiesību normu ietvaros. Īpaši grūti datu subjektam varētu būt rekonstruēt kaitējuma radīšanas gaitu un piekļūt tai, un līdz ar to pierādīt pārziņa vainu. Savukārt datu apstrādes pārzinis ir vislabākajā stāvoklī, lai piedāvātu vainu atspēkojošus pierādījumus un uzskatāmi parādītu, ka par kaitējumu izraisījušo notikumu tas nekādi nav atbildīgs [25].

64. Atbilstoši iepriekš aprakstītajam pārskatatbildības principam pārzinim būs arī jāpierāda, ka tas ir darījis visu iespējamo, lai laikus atjaunotu personas datu pieejamību un piekļuvi tiem.

65. Atgriežoties pie iesniedzējtiesas jautājuma, jānorāda, ka, pamatojoties uz līdz šim izklāstīto par pārziņa atbildības raksturu – lai arī, kā jau teicu, pārzinis var tikt atbrīvots no atbildības, ja tas pierāda, ka pārkāpuma iemesls ir tāds, par ko pārzinis nekādā veidā nav atbildīgs –, par šādu iemeslu nav uzskatāms tikai fakts, ka notikumu izraisījis ārpus pārziņa kontroles sfēras esošs subjekts.

66. Kad pārzinis cieš no kibernoziedznieku uzbrukuma, tas var arī netikt uzskatīts par atbildīgu par kaitējumu izraisījušo notikumu, taču nav izslēgts, ka datu pārziņa nolaidība ir bijusi konkrētā uzbrukuma pamatā, un viņš ir to veicinājis, jo personas datu aizsardzības drošības pasākumi, kas tam ir jāveic, ir bijuši neatbilstīgi vai to nav bijis vispār. Runa ir par katrā konkrētajā gadījumā specifisku faktu izvērtējumiem, kas lietu izskatošajai valsts tiesai jāveic, ņemot vērā tai iesniegtos pierādījumus.

67. Vispārēja pieredze liecina, ka publisko vai privāto tiesību subjektu – pārziņu – sistēmām, kurās glabājas milzums personas datu, daudz biežāk tiek uzbrukts no ārpuses, nekā no iekšienes. Tāpēc pārzinim ir jāizplāno atbilstīgi pasākumi it īpaši ārējo uzbrukumu atvairīšanai.

[23] M. Gambini, "Responsabilità", minēts iepriekš, 1059. lpp. Analoģiski par viedokli, ka atbilstīgu pasākumu veikšana ir pierādāma nevis gluži vienkārši apgalvojot, ka ir ievērota visa pienācīgā rūpība, bet gan pierādot, ka kaitējums radies kādu tādu no subjekta gribas neatkarīgu apstākļu dēļ, kuriem piemīt nepārvaramai varai vai neparedzamiem apstākļiem raksturīgā neparedzamība un nenovēršamība, S. Sica, "Sub art. 82", no: R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] "ja tas *pierāda*, ka nekādā veidā nav atbildīgs par notikumu, ar ko nodarīts attiecīgais kaitējums" (82. panta 3. punkts).

[25] M. Gambini, "Responsabilità", minēts iepriekš, 1060. lpp.

68. Visbeidzot, no teleoloģiskā viedokļa jāpiebilst, ka Regulas mērķis ir nodrošināt augstu aizsardzības līmeni. Šajā ziņā Tiesa jau ir uzsvērusi, ka no Regulas 1. panta 2. punkta, lasot to kopsakarā ar tās 10., 11. un 13. apsvērumu, izriet, ka ar šo regulu Savienības iestādēm, struktūrām, aģentūrām un kompetentajām iestādēm ir uzlikts pienākums nodrošināt augstu LESD 16. pantā un Hartas 8. pantā garantēto tiesību aizsardzības līmeni [26].

69. Ja Tiesa izvēlēsies interpretāciju, atbilstoši kurai gadījumā, kad Regulas pārkāpumu ir izdarījusi kāda trešā persona, pārzinis būtu automātiski jāatbrīvo no atbildības saskaņā ar 82. panta 3. punktu, šai interpretācijai būtu ar minētajā instrumentā izvirzīto aizsardzības mērķi nesaderīgas sekas, jo tā vājinātu datu subjektu tiesības, ierobežojot šādu atbildību līdz gadījumiem, kad pārkāpumu ir izdarījušas personas, kas atrodas minētā pārziņa pakļautībā un/vai kontrolē.

F. Piektais prejudiciālais jautājums

70. Ar piekto jautājumu iesniedzējtiesa būtībā lūdz Tiesu interpretēt "nemateriālā kaitējuma" jēdzienu Regulas 82. panta izpratnē. Konkrēti tā jautā, vai Regulas 82. panta 1. un 2. punkts, lasot tos kopsakarā ar tās pašas regulas 85. un 146. apsvērumu [27], ir jāinterpretē tādējādi, ka tādā situācijā, kurā minētās regulas pārkāpums izpaudies kā kibernoziedznieku veikta neatļauta piekļuve personas datiem un šādu datu neatļauta izpaušana, fakts, ka datu subjekts baidās no iespējamas viņa personas datu ļaunprātīgas izmantošanas nākotnē, var pats par sevi veidot (nemateriālu) kaitējumu, kas dod tiesības uz atlīdzinājumu.

71. Nedz 82. pantā, nedz apsvērumos par kaitējuma atlīdzināšanu nav sniegta skaidra atbilde uz šo jautājumu, bet no tiem var iegūt vairākus analīzei noderīgus elementus: nemateriālais (jeb nemantiskais) kaitējums var tikt atlīdzināts papildus materiālajam (jeb mantiskajam) kaitējumam; regulas pārkāpums nenozīmē, ka katrā ziņā sekos tā "izraisīts" kaitējums vai, precīzāk, personas datu aizsardzības pārkāpums "var izraisīt" fiziskām personām fizisku, materiālu vai nemateriālu kaitējumu; kaitējuma jēdziens ir jāinterpretē "plaši" Tiesas judikatūras gaismā tā, lai pilnībā atspoguļotu Regulas mērķus; "nodarītā" kaitējuma atlīdzībai būtu jābūt "pilnīgai un efektīvai".

72. Jau pats Regulas normu formulējums izslēdz jebkādu iespējamu mājienu uz kaitējumu *in re ipsa*: Regulā paredzētās civiltiesiskās atbildības galvenais mērķis ir atlīdzināt datu subjektam par kaitējumu tieši ar "pilnīgu un efektīvu" tam nodarītā kaitējuma kompensāciju un, tātad, atjaunot ar tiesību pārkāpumu negatīvi mainītās juridiskās situācijas līdzsvaru [28].

[26] Šajā nozīmē skat. spriedumu, 2021. gada 15. jūnijs, *Facebook Ireland* u.c. (C-645/19, EU:C:2021:483, 44. un 45. punkts).

[27] Saskaņā ar 85. apsvērumu, "ja uz personas datu aizsardzības pārkāpumu nereaģē pienācīgi un savlaicīgi, tas fiziskām personām var izraisīt [..] fizisku, materiālu vai nemateriālu kaitējumu [..]". Saskaņā ar 146. apsvērumu "pārzinim vai apstrādātājam būtu jākompensē jebkurš kaitējums, kurš personai var būt nodarīts tādas apstrādes rezultātā, kura pārkāpj šo regulu. Pārzinis vai apstrādātājs būtu jāatbrīvo no atbildības, ja tas pierāda, ka nekādā veidā nav atbildīgs par kaitējumu. Kaitējuma jēdziens būtu plaši jāinterpretē, ņemot vērā Tiesas judikatūru, tādā veidā, kas pilnībā atbilst šīs regulas mērķiem. Tas neskar prasības par kaitējumu, kas izriet no citu Savienības vai dalībvalstu tiesību aktu noteikumu pārkāpumiem. [..]. Datu subjektiem būtu jāsaņem pilna un iedarbīga kompensācija par tiem nodarīto kaitējumu. [..]".

[28] Skat. ģenerāladvokāta M. Kamposa Sančesa-Bordonas secinājumus, kas minēti šo secinājumu 29. punktā un 11. zemsvītras piezīmē. Tajos ģenerāladvokāts gramatiskās, vēsturiskās, kontekstuālās un teleoloģiskās analīzes noslēgumā pamatoti izslēdz, ka datu subjektiem saskaņā ar 82. pantu atlīdzināmais kaitējums pēc sava rakstura būtu "sods" (27.–55. punkts), norādot, pirmkārt, ka dalībvalstīm "nav jāizvēlas (un patiesībā tās nemaz nedrīkst izvēlēties) starp VIII nodaļā paredzētajiem datu aizsardzības nodrošināšanas mehānismiem. Kaitējumu neizraisoša pārkāpuma gadījumā datu subjektam ir vēl paredzētas (vismaz) tiesības iesniegt sūdzību uzraudzības iestādē" un, otrkārt, ka "izredzes saņemt kompensāciju, nepastāvot kaitējumam, iespējams, veicinātu civillietas ar prasībām, kas varbūt ne vienmēr būtu pamatotas [..] un tādējādi varētu atturēt no nodarbošanās ar datu apstrādi" (54. un 55. punkts).

73. Turklāt arī no sistēmiskā aspekta – gluži tāpat kā konkurences tiesībās – Regula nodrošina divus aizsardzības pīlārus: publiski tiesisko aizsardzību, paredzot sodus Regulas noteikumu pārkāpuma gadījumā, un privāttiesisko aizsardzību, paredzot ārpuslīgumiska rakstura civiltiesisko atbildību, kas kvalificējama kā smagāka prezumētās vainas dēļ, ietverot iepriekš minētās īpašības vainu atspēkojoša pierādījuma ziņā [29].

74. Tāpēc (nemateriālā) kaitējuma jēdziena plaša [30] interpretācija nevar mudināt likt uzskatīt, ka likumdevējs būtu atteicies no prasības, ka "kaitējumam" jābūt faktiskam.

75. Jautājums būtībā ir par to, vai tad, kad ir konstatēta pārkāpuma un cēloņsakarības esamība, var rasties tiesības uz atlīdzinājumu tikai datu subjekta rūpju, bažu un baiļu dēļ, ko tas izjūt saistībā ar tā personas datu iespējamu ļaunprātīgu izmantošanu nākotnē, ja šāda ļaunprātīga izmantošana nav konstatēta un/vai datu subjektam vēlāk nav nodarīts nekāds cits kaitējums.

76. Saskaņā ar Tiesas pastāvīgo judikatūru Savienības tiesību normās rodamie jēdzieni, kuru jēgas un tvēruma noskaidrošanai nav konkrēti norādīts uz dalībvalstu tiesībām, parasti ir jāinterpretē autonomi un visā Savienībā vienveidīgi, ņemot vērā ne tikai konkrētās tiesību normas tekstu, bet arī kontekstu, kurā tā iekļaujas, mērķus, kādi ir tiesību aktam, kurā tā iekļaujas, un minētās tiesību normas rašanās vēsturi [31].

77. Tiesa, kā atgādinājis ģenerāladvokāts M. Kamposs Sančess-Bordona [32], nav izstrādājusi vispārēju "kaitējuma" jēdziena definīciju, kas būtu vienlīdz piemērojama visās jomās [33]. Attiecībā uz nemateriālo kaitējumu no Tiesas judikatūras var secināt, ka tad, ja viens no interpretējamās tiesību normas mērķiem ir indivīda vai noteiktas indivīdu kategorijas [34] aizsardzība, kaitējuma jēdzienam ir jābūt plašam; saskanīgi ar minēto kritēriju atlīdzināms ir arī nemateriālais kaitējums, pat ja tas nav minēts interpretētajā tiesību normā [35].

78. Kaut gan Tiesas judikatūra atļauj apgalvot, ka iepriekš minētajā izpratnē Savienības tiesībās pastāv nemateriālā kaitējuma atlīdzības princips, piekrītu ģenerāladvokātam M. Kamposam Sančesam-Bordonam, ka no tā nevar izsecināt noteikumu, uz kura pamata būtu atlīdzināms *ikviens* nemateriālais kaitējums neatkarīgi no tā, cik tas ir būtisks [36].

[29] Tāpēc, liedzot tiesības uz atlīdzinājumu par vieglām vai pārejošām sajūtām vai emocijām saistībā ar apstrādes noteikumu pārkāpumu, datu subjekts nepaliktu pavisam neaizsargāts (šajā nozīmē skat. ģenerāladvokāta M. Kamposa Sančesa-Bordonas secinājumus, minēti iepriekš, 115. punkts).

[30] Skat. Regulas 146. apsvērumu.

[31] Skat. spriedumus, 2021. gada 15. aprīlis, *The North of England P & I Association* (C-786/19, EU:C:2021:276, 48. punkts), un 2021. gada 10. jūnijs, *KRONE – Verlag* (C-65/20, EU:C:2021:471, 25. punkts).

[32] Skat. ģenerāladvokāta M. Kamposa Sančesa-Bordonas secinājumus, minēti iepriekš, 104. punkts.

[33] Tā nav norādījusi arī vēlamo interpretācijas metodi, proti, vai interpretācija ir veicama autonomi vai ar atsauci uz valstu tiesiskajiem regulējumiem, jo tas ir atkarīgs no aplūkojamās jomas. Skat. spriedumus, 2001. gada 10. maijs, *Veedfald* (C-203/99, EU:C:2001:258, 27. punkts), defektīvu preču jomā, 2010. gada 6. maijs, *Walz* (C-63/09, EU:C:2010:251, 21. punkts), gaisa pārvadātāju atbildības jomā, un 2021. gada 10. jūnijs, *Van Ameyde España* (C-923/19, EU:C:2021:475, 37. un nākamie punkti), par civiltiesisko atbildību saistībā ar mehānisko transportlīdzekļu izmantošanu.

[34] Piemēram, preču patērētāji vai ceļu satiksmes negadījumos cietušie.

[35] "Komplekso" ceļojumu jomā skat. spriedumu, 2002. gada 12. marts, *Leitner* (C-168/00, EU:C:2002:163); par civiltiesisko atbildību saistībā ar mehānisko transportlīdzekļu izmantošanu skat. spriedumus, 2013. gada 24. oktobris, *Haasová* (C-22/12, EU:C:2013:692, 47.–50. punkts), 2013. gada 24. oktobris, Drozdovs (C-277/12, EU:C:2013:685, 40. punkts), un 2014. gada 23. janvāris, *Petillo* (C-371/12, EU:C:2014:26, 35. punkts).

[36] Skat. ģenerāladvokāta M. Kamposa Sančesa-Bordonas secinājumus, minēti iepriekš, 105. punkts. Par saderīgu ar Savienības tiesību normām Tiesa ir atzinusi, piemēram, tādu valsts tiesisko regulējumu, kas atlīdzinājuma aprēķināšanas nolūkos nemateriālo kaitējumu, kas saistīts ar ceļu satiksmes negadījuma rezultātā nodarītajiem miesas bojājumiem, nošķir atkarībā no tā izcelsmes; skat. spriedumu, 2014. gada 23. janvāris, *Petillo* (C-371/12, EU:C:2014:26), rezolutīvā daļa: Savienības tiesībām pretrunā nav "tāds [..] valsts tiesiskais regulējums, ar kuru tiek paredzēts konkrēts režīms attiecībā uz atlīdzināmā nemateriālā kaitējuma, kas radies ceļu satiksmes negadījumu rezultātā radītiem viegliem miesas bojājumiem, apmēru, ierobežojot šī kaitējuma atlīdzības apmēru, salīdzinot ar to, kas tiek piešķirts kā atlīdzība par identiska kaitējuma, kas radies citu iemeslu dēļ, nevis konkrēto negadījumu rezultātā, nodarīšanu".

79. Minētajos apstākļos nozīme ir nošķiršanai starp atlīdzināmu nemateriālo kaitējumu un citām *neērtībām, kuras izriet no tiesiskuma neievērošana* un kuras, ņemot vērā to nebūtiskumu, ne vienmēr obligāti dotu tiesības uz atlīdzinājumu [37].

80. Tiesa atzīst šo atšķirību, kad tā norāda uz neērtībām un sarežģījumiem kā autonomu kategoriju salīdzinājumā ar zaudējumu kategoriju jomās, kurās tā uzskata, ka tie ir jāatlīdzina [38].

81. Empīriski ir vērojams, ka ikviens pārkāpums personas datu aizsardzības jomā izraisa negatīvu reakciju no datu subjekta puses. Atlīdzinājums tikai par nepatīkamu sajūtu citas personas veiktas likuma neievērošanas dēļ būtu viegli sajaucams ar kompensāciju bez kaitējuma, kas, kā jau teicu, Regulas 82. pantā minētajā situācijā nešķiet esam paredzēts.

82. Fakts, ka tādos apstākļos kā pamatlietā personas datu ļaunprātīga izmantošana ir tikai potenciāla, nevis faktiska, ir pietiekams, lai uzskatītu, ka datu subjektam, iespējams, ir nodarīts Regulas pārkāpuma dēļ izraisīts nemateriāls kaitējums, ja vien datu subjekts pierāda, ka bailes no šādas ļaunprātīgas izmantošanas viņam ir faktiski un konkrēti radījušas reālu un skaidru emocionālo kaitējumu [39].

83. Starp gluži vienkāršu sarūgtinājumu vien (par ko atlīdzinājums nepienākas) un patiesu nemateriālu kaitējumu (par ko atlīdzinājums pienākas) esošā robeža katrā ziņā ir smalka, bet valstu tiesām, kurām ir uzdevums novilkt robežu katrā konkrētajā gadījumā, būtu uzmanīgi jāizvērtē visa informācija, ko sniedz atlīdzinājumu prasošais datu subjekts, kuram ir konkrēti, nevis vispārīgi jānorāda konkrētie elementi, kas var pierādīt "faktiski nodarīta nemateriālā kaitējuma" esamību personas datu aizsardzības pārkāpuma dēļ, kaut arī tam nav obligāti jāsasniedz noteiktas pakāpes smagums: nozīme ir tam, ka runa nav par gluži subjektīvu uztveri, kas mainās un ir atkarīga arī no rakstura un personīgiem faktoriem, bet neērtības – kaut vieglas, taču uzskatāmi parādāmas, datu subjekta fiziskajai vai psihiskajai neaizskaramībai vai attiecībām – tiek objektivizētas; iesaistīto personas datu raksturam un nozīmei, kāda tiem ir datu subjekta dzīvē, un, iespējams, arī tam, kā sabiedrība katrā konkrētā brīdī uztver šo konkrēto ar datu aizsardzības pārkāpumu saistīto neērtību [40].

[37] Šāds nošķirums ir sastopams vairāku valstu tiesiskajos regulējumos kā nenovēršamas sekas, kas izriet no dzīves sabiedrībā. Nesen datu aizsardzības jomā Itālijā *Tribunale di Palermo, sez. I civile, sentenza* 05/10/2017 Nr. 5261, kā arī *Cass Civ. Ord. Sez VI*, Nr. 17383/2020. Vācijā tostarp *AG Diez*, 07.11.2018 – 8 C 130/18; *LG Karlsruhe*, 02.08.2019. – 8 O 26/19; un *AG Frankfurt am Main*, 10.07.2020. – 385 C 155/19 (70). Austrijā *OGH 6 Ob 56/21k*.

[38] Skat. spriedumu, 2012. gada 23. oktobris, *Nelson* u.c. (C-581/10 un C-629/10, EU:C:2012:657, 51. punkts), par atšķirību starp "zaudējumiem" Monreālā 1999. gada 28. maijā noslēgtās Konvencijas par dažu starptautiskā gaisa transporta noteikumu unifikāciju 19. panta izpratnē un "neērtībām" Regulas Nr. 261/2004 izpratnē, kas ir kompensējamas saskaņā ar minētās regulas 7. pantu atbilstoši 2009. gada 19. novembra spriedumam *Sturgeon* u.c. (C-402/07 un C-432/07, EU:C:2009:716). Šajā nozarē, tāpat kā pasažieru transportā pa jūru un iekšzemes ūdensceļiem, uz ko attiecas Regula Nr. 1177/2010, likumdevējs ir varējis noteikt teorētisku kategoriju tāpēc, ka neērtības izraisošais faktors un tā būtība ir vienāda visu cietušo gadījumā. Nedomāju, ka šādu secinājumu izdarīt būtu iespējams datu aizsardzības jomā.

[39] Īrijas ieskatā, praksē šie apsvērumi ir īpaši svarīgi kibernoziedzības kontekstā, jo, ja ikvienai personai, ko – kaut arī tikai nedaudz – ir skāris pārkāpums, būtu tiesības uz nemateriālā kaitējuma atlīdzinājumu, tam būtu spēcīga ietekme, it īpaši uz publiskā sektora datu pārziņiem, ko finansē no ierobežotiem publiskajiem līdzekļiem un kam būtu jākalpo visupirms kolektīvajam interesēm, ieskaitot personas datu drošības uzlabošanu (rakstveida apsvērumi, 72. punkts).

[40] Skat. ģenerāladvokāta M. Kamposa Sančesa-Bordonas secinājumus, minēti iepriekš, 116. punkts.

IV. Secinājumi

84. Ņemot vērā visus iepriekš izklāstītos apsvērumus, iesaku Tiesai uz uzdotajiem prejudiciālajiem jautājumiem atbildēt šādi:

Regulas 2016/679 5., 24., 32. un 82. pants

ir jāinterpretē tādējādi, ka

ar "personas datu aizsardzības pārkāpuma", kā definēts 4. panta 12. punktā, konstatējumu vien nav pietiekami, lai secinātu, ka pārziņa īstenotie tehniskie un organizatoriskie pasākumi nav bijuši "atbilstīgi", lai nodrošinātu konkrēto datu aizsardzību;

pārbaudot personas datu apstrādes pārziņa īstenoto tehnisko un organizatorisko pasākumu atbilstību, valsts tiesai, kas skata lietu, būs jāveic pārbaude, kuras ietvaros konkrēti jāizanalizē gan minēto pasākumu saturs, gan veids, kādā tie piemēroti, un to konkrētās praktiskās sekas;

VDAR 82. pantā paredzētās prasības par kaitējuma atlīdzību ietvaros personas datu pārzinim ir pienākums pierādīt, ka pasākumi, ko tas īstenojis atbilstoši minētās regulas 32. pantam, ir atbilstīgi;

saskaņā ar procesuālās autonomijas principu katras dalībvalsts valsts tiesiskajā regulējumā ir jānosaka pieļaujamie pierādīšanas līdzekļi un to pierādījuma spēks, ieskaitot pierādījumu vākšanas pasākumus, ko valstu tiesas var uzdot vai ko tām ir jāuzdod tālab, lai izvērtētu, vai personas datu pārzinis ir īstenojis atbilstīgus pasākumus minētās regulas izpratnē, ievērojot Savienības tiesībās noteiktos līdzvērtības un efektivitātes principus;

fakts, ka minētās regulas pārkāpumu, kas izraisījis konkrēto kaitējumu, ir izdarījusi kāda trešā persona, pats par sevi nav pamats, lai atbrīvotu pārzini no atbildības, un, lai gūtu labumu no minētajā tiesību normā paredzētā atbrīvojuma, pārzinim ir jāpierāda, ka par pārkāpumu tas nekādā veidā nav atbildīgs;

kaitējums, kas izpaužas kā bailes no kāda datu subjekta personas datu iespējamas ļaunprātīgas izmantošanas nākotnē, kuras iespējamību datu subjekts ir pierādījis, var veidot nemateriālu kaitējumu, kas dod tiesības uz atlīdzinājumu, ja vien datu subjekts pierāda, ka viņam individuāli ir nodarīts reāls un skaidrs emocionālais kaitējums; un šis apstāklis katrā konkrētajā gadījumā ir jāizvērtē valsts tiesai, kura skata attiecīgo prasību.