GENERALINIO ADVOKATO
GIOVANNI PITRUZZELLA IŠVADA,
pateikta 2023 m. balandžio 27 d.[1]

Byla C-340/21

VB
prieš
Natsionalna agentsia za prihodite

(*Varhoven administrativen sad* (Bulgarijos Aukščiausias administracinis teismas) prašymas priimti prejudicinį sprendimą)

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų apsauga – Reglamentas (ES) 2016/679 – Duomenų valdytojo atsakomybė – Duomenų tvarkymo saugumas – Asmens duomenų tvarkymo saugumo pažeidimas – Neturtinė žala, patirta dėl duomenų valdytojo neveikimo – Ieškinys dėl žalos atlyginimo“

Ar neteisėtas viešosios institucijos turimų asmens duomenų atskleidimas dėl įsilaužimo gali būti pagrindas atlyginti neturtinę žalą duomenų subjektui vien dėl to, kad šis nuogąstauja dėl galimo būsimo piktnaudžiavimo jo duomenimis? Kokie yra atsakomybės priskyrimo duomenų valdytojui kriterijai? Kaip paskirstoma įrodinėjimo pareiga nagrinėjant ginčą? Kokia yra teisminės kontrolės apimtis?

I. Teisinis pagrindas

1. Reglamento (ES) 2016/679[2] (toliau – reglamentas) 4 straipsnyje „Apibrėžtys“ numatyta:

„Šiame reglamente:

<…>

12) asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga;

<…>“

[1] Originalo kalba: italų.

[2] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

2. 5 straipsnyje „Su asmens duomenų tvarkymu susiję principai“ nurodyta:

„1. Asmens duomenys turi būti:

<…>

f) tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

2. Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi 1 dalies, ir turi sugebėti įrodyti, kad jos laikomasi (atskaitomybės principas).“

3. To paties reglamento 24 straipsnyje ‚Duomenų valdytojo atsakomybė“ nustatyta:

„1. Atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos.

2. Kai tai proporcinga duomenų tvarkymo veiklos atžvilgiu, 1 dalyje nurodytos priemonės apima duomenų valdytojo įgyvendinamą atitinkamą duomenų apsaugos politiką.

3. Tuo, kad laikomasi patvirtintų elgesio kodeksų, kaip nurodyta 40 straipsnyje, arba patvirtintų sertifikavimo mechanizmų, kaip nurodyta 42 straipsnyje, gali būti remiamasi kaip vienu iš elementų, kuriuo siekiama įrodyti, kad duomenų valdytojas vykdo prievoles.“

4. 32 straipsnyje „Duomenų tvarkymo saugumas“ numatyta:

„1. Atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, *inter alia*, jei reikia:

<…>

2. Nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

3. Tuo, kad laikomasi patvirtinto elgesio kodekso, kaip nurodyta 40 straipsnyje, arba patvirtinto sertifikavimo mechanizmo, kaip nurodyta 42 straipsnyje, gali būti remiamasi kaip vienu iš elementų, kuriuo siekiama įrodyti, kad laikomasi šio straipsnio 1 dalyje nustatytų reikalavimų.

<…>“

5. To paties reglamento 82 straipsnyje „Teisė į kompensaciją ir atsakomybė“ nurodyta:

„1. Bet kuris asmuo, patyręs materialinę ar nematerialinę žalą dėl šio reglamento pažeidimo, turi teisę iš duomenų valdytojo arba duomenų tvarkytojo gauti kompensaciją už patirtą žalą.

2. Tvarkant duomenis dalyvaujantis duomenų valdytojas atsako už žalą, padarytą dėl vykdyto duomenų tvarkymo pažeidžiant šį reglamentą. <…>

3. Duomenų valdytojas arba duomenų tvarkytojas atleidžiami nuo atsakomybės pagal 2 dalį, jeigu jis įrodo, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala.“

II. Faktinės aplinkybės, procesas ir prejudiciniai klausimai

6. 2019 m. liepos 15 d. Bulgarijos žiniasklaida plačiajai visuomenei pranešė, kad buvo neteisėtai prisijungta prie *Natsionalna agentsia za prihodite* (Nacionalinė pajamų agentūra, Bulgarija; toliau – NPA[3]) kompiuterinės sistemos ir kad internete buvo paskelbta įvairūs milijonų žmonių, tiek piliečių, tiek užsieniečių, mokesčių ir socialinio draudimo duomenys.

7. Taigi daugybė asmenų, tarp jų ir ieškovė pagrindinėje byloje V. B., pareiškė ieškinius NPA dėl neturtinės žalos atlyginimo.

8. Šioje byloje ieškovė pagrindinėje byloje pareiškė ieškinį *Administrativen sad Sofia-grad* (Sofijos miesto administracinis teismas, Bulgarija; toliau – ASSG), teigdama, kad NPA pažeidė nacionalinės teisės normas ir savo, kaip duomenų valdytojos, pareigą tvarkyti asmens duomenis tokiu būdu, kad taikant tinkamas techninės ir organizacines priemones būtų užtikrintas „tinkamas asmens duomenų saugumas“, kaip tai suprantama pagal Reglamento (ES) 2016/679 24 ir 32 straipsnius. Ieškovė teigė patyrusi neturtinę žalą, kuri pasireiškė susirūpinimu ir nuogąstavimais dėl galimo būsimo piktnaudžiavimo jos asmens duomenimis.

9. Kita vertus, atsakovė pabrėžė, kad ieškovė pagrindinėje byloje neprašė jokios informacijos apie tai, kokie konkretūs asmens duomenys buvo pasisavinti. Be to, sužinojusi apie įsilaužimą, atsakovė suorganizavo susitikimus su ekspertais, kad apsaugotų piliečių teises ir interesus. NPA teigimu, taip pat nebuvo priežastinio ryšio tarp kibernetinio išpuolio ir tariamai patirtos žalos, nes agentūra buvo įdiegusi visas procesų valdymo ir informacijos saugumo sistemas pagal atitinkamus šioje srityje galiojančius tarptautinius standartus.

10. Pirmosios instancijos teismas, ASSG, atmetė ieškinį nurodydamas, kad duomenų atskleidimas nėra susijęs su agentūra, kad įrodinėjimo pareiga dėl taikytų priemonių tinkamumo tenka ieškovei ir, galiausiai, kad ji nepatyrė jokios atlygintinos neturtinės žalos.

11. Pirmosios instancijos teismo sprendimas buvo apskųstas *Varhoven administrativen sad* (Vyriausiasis administracinis teismas, Bulgarija). Kaip vieną iš pateiktų argumentų ieškovė pagrindinėje byloje pabrėžė tai, kad pirmosios instancijos teismas neteisingai paskirstė

[3] NPA yra duomenų valdytoja, kaip tai suprantama pagal reglamento 4 straipsnio 7 dalį. Pagal nacionalinę teisę ji yra finansų ministrui pavaldi specializuota administracinė įstaiga, atsakinga už valstybės reikalavimų, kylančių iš viešosios teisės, ir teisės aktais nustatytų iš privatinės teisės kylančių valstybės reikalavimų nustatymą, užtikrinimą ir išieškojimą. Vykdydama jai pavestas viešosios valdžios funkcijas ji tvarko asmens duomenis.

įrodinėjimo pareigą, susijusią su tuo, kad nebuvo imtasi saugumo priemonių. Neturtinė žala taip pat neturėtų būti įrodinėjimo pareigos objektas, nes tai yra faktiškai patirta, o ne tik galima neturtinė žala.

12. NPA savo ruožtu pakartotinai patvirtino, kad, kaip duomenų valdytoja, ji ėmėsi būtinų techninių ir organizacinių priemonių, ir ginčijo faktinės neturtinės žalos įrodymų buvimą. Susirūpinimas ir nuogąstavimai yra emocinės būsenos, kurios nėra pakankamas pagrindas žalai atlyginti.

13. Prašymą priimti prejudicinį sprendimą pateikęs teismas atkreipė dėmesį į tai, kad teismo procesų, kuriuos nukentėjusiosios šalys atskirai inicijavo prieš NPA dėl neturtinės žalos atlyginimo, baigtis buvo įvairi.

14. Šiomis aplinkybėmis prašymą priimti prejudicinį sprendimą pateikęs teismas nutarė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar [2016 m. balandžio 27 d. Europos Parlamento ir Tarybos] reglamento (ES) 2016/679 [dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)] 24 ir 32 straipsniai aiškintini taip, jog aplinkybės, kad asmens duomenis be leidimo atskleidė arba be leidimo gavo prieigą prie jų, kaip tai suprantama pagal Reglamento (ES) 2016/679 4 straipsnio 12 punktą, asmenys, kurie nėra duomenų valdytojo administracijos darbuotojai ir kurių jis nekontroliuoja, pakanka, kad būtų galima daryti prielaidą, jog taikytos techninės ir organizacinės priemonės yra netinkamos?

2. Jeigu į pirmąjį klausimą būtų atsakyta neigiamai, koks turėtų būti teisminės teisėtumo kontrolės dalykas ir apimtis vertinant, ar techninės ir organizacinės priemonės, kurių ėmėsi duomenų valdytojas, yra tinkamos pagal Reglamento (ES) 2016/679 32 straipsnį?

3. Jeigu į pirmąjį klausimą būtų atsakyta neigiamai, ar Reglamento (ES) 2016/679 5 straipsnio 2 dalyje ir 24 straipsnyje, siejamuose su to paties reglamento 74 konstatuojamąja dalimi, įtvirtintas atskaitomybės principas aiškintinas taip, kad pagal Reglamento (ES) 2016/679 82 straipsnio 1 dalį nagrinėjant ieškinį teisme duomenų valdytojui tenka pareiga įrodyti, kad taikytos techninės ir organizacinės priemonės yra tinkamos pagal to reglamento 32 straipsnį? Ar gauta eksperto išvada gali būti laikoma būtinu ir pakankamu įrodymu siekiant nustatyti, ar techninės ir organizacinės priemonės, kurių ėmėsi duomenų valdytojas, buvo tinkamos tokiu atveju, kaip šis, kai prieiga prie asmens duomenų be leidimo gauta ir duomenys be leidimo buvo atskleisti įvykdžius „programišių išpuolį“?

4. Ar Reglamento (ES) 2016/679 82 straipsnio 3 dalis aiškintina taip, kad asmens duomenų atskleidimas be leidimo arba prieigos prie jų gavimas be leidimo, kaip tai suprantama pagal to paties reglamento 4 straipsnio 12 punktą, kaip šioje byloje, kai „programišių išpuolį“ įvykdė asmenys, kurie nėra duomenų valdytojo administracijos darbuotojai ir kurių jis nekontroliuoja, yra aplinkybė, už kurią duomenų valdytojas jokiu būdu nėra atsakingas ir dėl kurios jis gali būti atleistas nuo atsakomybės?

5. Ar Reglamento (ES) 2016/679 82 straipsnio 1 ir 2 dalys kartu su 85 ir 146 konstatuojamosiomis dalimis aiškintinos taip, kad tokiu atveju, kaip šis, kai buvo padarytas asmens duomenų saugumo pažeidimas, t. y. be leidimo gauta prieiga prie asmens duomenų ir duomenys be leidimo platinti įvykdžius „programišių išpuolį“, tik duomenų subjekto patirti rūpesčiai,

nuogąstavimai ir baimė dėl galimo būsimo piktnaudžiavimo asmens duomenimis patenka į plačiai aiškintiną neturtinės žalos sąvoką ir pagrindžia jo teisę reikalauti atlyginti žalą, jeigu toks piktnaudžiavimas nebuvo nustatytas ir (arba) duomenų subjektas nepatyrė jokios papildomos žalos?“

III. Teisinis vertinimas

A. Pirminės pastabos

15. Šioje byloje keliami įdomūs ir iš dalies nauji klausimai, susiję su kelių reglamento nuostatų aiškinimu [4].

16. Penki prejudiciniai klausimai iš esmės yra susiję su vienu ir tuo pačiu aspektu: neturtinės žalos atlyginimo asmeniui, kurio duomenys, saugomi viešosios institucijos, buvo paskelbti internete po „programišių išpuolio“, sąlygomis.

17. Dėl patogumo pasiūlysiu atskirus apibendrintus atsakymus į visus prašyme priimti prejudicinį sprendimą pateiktus klausimus, nors ir manytina, kad kai kurie iš jų konceptualiai sutampa, nes pirmaisiais keturiais klausimais siekiama nustatyti sąlygas, kuriomis duomenų valdytoja galimai pažeidė reglamento nuostatas [5], o penktasis klausimas konkrečiai susijęs su neturtinės žalos sąvoka siekiant gauti kompensaciją [6].

18. Norėčiau pabrėžti, kad šiuo metu Teisingumo Teisme nagrinėjamos kelios bylos dėl reglamento 82 straipsnio ir vienoje iš jų jau buvo remtasi generalinio advokato išvada, į kurią atsižvelgsiu šioje analizėje [7].

19. Manau, kad, prieš pradedant nagrinėti nurodytus klausimus, tikslinga pateikti keletą pirminių pastabų dėl reglamento principų ir tikslų, nes jos bus naudingos atsakant į kiekvieną prejudicinį klausimą.

20. Reglamento 24 straipsnyje nustatyta bendro pobūdžio duomenų valdytojo pareiga įgyvendinti tinkamas technines ir organizacines priemones, kad jis užtikrintų ir galėtų įrodyti, kad duomenys tvarkomi laikantis šio reglamento, o 32 straipsnyje konkrečiai aptariama ta pati pareiga, susijusi su duomenų tvarkymo saugumu. 24 ir 32 straipsniuose konkrečiau išdėstoma tai, kas jau numatyta 5 straipsnio 2 dalyje; joje, kaip vienas iš „[s]u asmens duomenų tvarkymu susij[usių] princip[ų]“,

[4] 5 straipsnio 2 dalis (dėl bet kurio duomenų valdytojo atsakomybės už asmens duomenų tvarkymą principo), 24 straipsnis (dėl priemonių, kurių duomenų valdytojas turi imtis, kad užtikrintų, jog jo atliekamas duomenų tvarkymas atitinka šį reglamentą), 32 straipsnis (dėl pareigos, konkrečiai susijusios su duomenų tvarkymo saugumu) ir 82 straipsnio 1–3 dalys (dėl žalos, atsiradusios dėl šio reglamento pažeidimo, atlyginimo ir galimybės duomenų valdytojui imtis priemonių, kad būtų užtikrinta atitiktis minėtam reglamentui), taip pat 74, 85 ir 146 konstatuojamosios dalys, susijusios su minėtais straipsniais.

[5] a) pirmuoju siekiama atsakyti į klausimą, ar įgyvendintų priemonių netinkamumas gali būti konstatuotas vien dėl to, kad buvo įsilaužta į sistemas; b) antrasis klausimas susijęs su teismo atliekamos minėtų priemonių tinkamumo kontrolės apimtimi; c) trečiasis klausimas susijęs su pačia tinkamumo įrodinėjimo pareiga ir tam tikrais techniniais įrodymų rinkimo būdais; d) ketvirtuoju siekiama išsiaiškinti, ar aplinkybė, kad įsilaužimas į sistemą buvo įvykdytas iš išorės, yra svarbi atleidimo nuo atsakomybės tikslais.

[6] Atsižvelgiant į nurodomas reglamento nuostatas, pirmieji trys klausimai susiję su duomenų valdytojo atsakomybės dėl taikytinų priemonių tinkamumo aspektais (5, 24 ir 32 straipsniai); ketvirtasis ir penktasis klausimai susiję su atleidimo nuo atsakomybės sąlygomis ir atlygintinos neturtinės žalos sąvoka (82 straipsnis).

[7] Žr. generalinio advokato M. Campos Sánchez-Bordona išvadą byloje *Österreichische Post (Neturtinė žala, atsiradusi dėl neteisėto duomenų tvarkymo)* (C-300/21, EU:C:2022:756).

nustatytas „atskaitomybės [principas]“. Jis logiškai atitinka 5 straipsnio 1 dalies f punkte numatytą „vientisumo ir konfidencialumo principą“ ir jį papildo, ir abu šie principai turi būti aiškinami atsižvelgiant į rizika pagrįstą požiūrį, kuriuo grindžiamas reglamentas.

21. Atskaitomybės principas – vienas iš reglamento ramsčių ir viena iš svarbiausių jo naujovių. Pagal jį duomenų valdytojui tenka atsakomybė imtis aktyvių veiksmų, kad būtų užtikrinta atitiktis reglamentui, ir būti pasirengusiam tai įrodyti [8].

22. Doktrinoje tikri kultūriniai pokyčiai nurodomi kaip „bendros atsakomybės pareigos apimties“ poveikis [9]. Ne formalus teisinės prievolės laikymasis ar neatidėliotinos priemonės taikymas, o priimta bendra įmonės strategija yra svarbi atleidžiant duomenų valdytoją nuo atsakomybės, kadangi jis *laikosi* duomenų apsaugos taisyklių.

23. Techninės ir organizacinės priemonės, kurių reikalaujama pagal atskaitomybės principą, turi būti „tinkamos“, atsižvelgiant į 24 straipsnyje nurodytus kriterijus: duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms.

24. Taigi 24 straipsnyje reikalaujama, kad priemonės būtų tinkamos, siekiant įrodyti, jog duomenų tvarkymas atitinka reglamento principus ir nuostatas.

25. Kita vertus, 32 straipsnyje atskaitomybės principas grindžiamas konkrečiomis priemonėmis, kurių reikia imtis, kad būtų užtikrintas „pavojų atitinkančio lygio saugumas“. Šiuo atveju jau numatyti kriterijai, į kuriuos reikia atsižvelgti rengiant technines ir organizacines priemones, yra papildomi techninių galimybių išsivystymo lygiu ir įgyvendinimo sąnaudomis.

26. Pagal tinkamumo sąvoką reikalaujama, kad užtikrinant informacinių sistemų apsaugą priimti sprendimai būtų priimtini tiek techniniu (priemonių tinkamumas), tiek kokybiniu (apsaugos veiksmingumas) požiūriu. Siekiant užtikrinti būtinumo, tinkamumo ir proporcingumo principų laikymąsi, duomenų tvarkymas turi būti ne tik tinkamas, bet ir pakankamas atsižvelgiant į tikslus, kurių juo siekiama. Pagal šią logiką lemiamas vaidmuo tenka duomenų kiekio mažinimo principui; pagal jį visais duomenų tvarkymo etapais turi būti nuolat stengiamasi kuo labiau sumažinti riziką saugumui [10].

27. Visas reglamentas grindžiamas rizikos prevencija ir duomenų valdytojo atsakomybe; tai teleologinis požiūris, kuriuo siekiama geriausio įmanomo rezultato veiksmingumo atžvilgiu, t. y. gerokai nutolstama nuo formalios logikos, susijusios su paprasčiausia pareiga laikytis konkrečių procedūrų, kad būtų išvengta atsakomybės [11].

[8] C. Docksey, „Article 24. Responsibility of the controller“, paskelbta C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, „The ES General Data Protection Regulation (GDPR): A Commentary“, Oxford University Press, 2020 m., p. 561. Duomenų apsaugos reglamentavimo principai ir įpareigojimai turėtų atsispindėti organizacijų kultūrinėje struktūroje visais lygmenimis, o ne būti laikomi teisinių reikalavimų rinkiniu, kurį nustato teisinė institucija.

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

[10] E. Belisario, G. Riccio, G. Scorza, minėtas leidinys GDPR,. p. 380.

[11] Dėl šios priežasties, kaip paaiškės toliau, į pirmąjį ir ketvirtąjį prejudicinius klausimus galima atsakyti tik neigiamai. Iš reglamento nuostatų negalima automatiškai daryti tokios išvados: nepakanka vien to, kad buvo atskleisti asmens duomenys, siekiant konstatuoti, jog taikytos techninės ir organizacinės priemonės yra netinkamos, bet nepakanka ir aplinkybės, kad duomenys buvo atskleisti dėl asmenų, nepriklausančių duomenų valdytojo organizacijai ir jo kontrolės sričiai, įsikišimo, kad duomenų valdytojas būtų atleistas nuo atsakomybės.

28. 24 straipsnyje nepateikiamas baigtinis „tinkamų“ priemonių sąrašas: kiekvienu konkrečiu atveju reikės atlikti individualų vertinimą. Tai atitinka reglamento filosofiją, iš kurios matyti, jog pageidautina, kad taikytinos procedūros būtų pasirinktos kruopščiai įvertinus konkrečią situaciją, kad jos būtų kuo veiksmingesnės [12].

B. Pirmasis prejudicinis klausimas

29. Pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar reglamento 24 ir 32 straipsniai turi būti aiškinami taip, kad vien „asmens duomenų saugumo pažeidimo“, kaip tai suprantama pagal 4 straipsnio 12 dalį, atsiradimo pakanka, kad būtų galima daryti išvadą, jog duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės nebuvo „tinkamos“ duomenų apsaugai užtikrinti.

30. Iš reglamento 24 ir 32 straipsnių formuluotės matyti, kad duomenų valdytojas, pasirinkdamas technines ir organizacines priemones, kurias privalo įgyvendinti siekdamas užtikrinti minėto reglamento laikymąsi, turi atsižvelgti į tam tikrus šiuose straipsniuose išvardytus ir pirma minėtus vertinimo kriterijus.

31. Duomenų valdytojas turi tam tikrą veiksmų laisvę nustatyti tinkamiausias priemones, atsižvelgdamas į konkrečią situaciją, tačiau šis pasirinkimas vis dėlto gali būti teisminės kontrolės objektas, kad būtų galima patikrinti, ar taikomos priemonės atitinka visas iš minėto reglamento kylančias prievoles ir tikslus.

32. Visų pirma, kalbant apie saugumo priemones, pažymėtina, jog 32 straipsnio 1 dalyje reikalaujama, kad duomenų valdytojas atsižvelgtų į „techninių galimybių išsivystymo lygį“. Tai reiškia, kad įgyvendintinų priemonių technologinis lygis apsiriboja tuo, kas pagrįstai įmanoma priemonių įgyvendinimo metu, t. y. priemonės tinkamumas užkirsti kelią pavojui turi būti proporcingas sprendimams, kuriuos gali pateikti dabartiniai laimėjimai mokslo, technikos, technologijų ir mokslinių tyrimų srityje, taip pat atsižvelgiant, kaip bus nurodyta toliau, į įgyvendinimo sąnaudas.

33. Priemonės tam tikru metu gali būti „tinkamos“ ir, nepaisant to, jas gali apeiti kibernetiniai nusikaltėliai, naudojantys itin sudėtingus metodus, dėl kurių netgi techninių galimybių išsivystymo lygį atitinkančios saugumo priemonės gali tapti neveiksmingos.

34. Kita vertus, nelogiška manyti, kad Sąjungos teisės aktų leidėjas ketino nustatyti duomenų valdytojui pareigą užkirsti kelią bet kokiam asmens duomenų saugumo pažeidimui, neatsižvelgiant į tai, kaip stropiai jis įgyvendina saugumo priemones [13].

35. Kaip jau minėta, reglamente atsisakoma automatiškumo ir reikalaujama didelės duomenų valdytojo atsakomybės, tačiau tai nereiškia, kad pastarajam neįmanoma įrodyti, kad jis tinkamai vykdė jam nustatytas pareigas.

[12] L. Bolognini, E. Pelino, „Codice della disciplina privacy“, Giuffrè, 2019 m., p. 201. Taigi Europos teisės aktų leidėjas neapsiriboja duomenų tvarkymo saugumo samprata, grindžiama iš anksto nustatytų saugumo priemonių buvimu, ir taiko metodiką, atitinkančią tarptautinius *rizikos* vertinimu (*risk based*) pagrįsto informacinių sistemų valdymo standartus: pagal ją turi būti nustatytos rizikos mažinimo priemonės, kurios neapsiriboja iš anksto parengtais ir bendrai taikomais *kontroliniais sąrašais* (*checklist*). Šiuo atveju būtina remtis tarptautinėmis gairėmis ir standartais. Šio rizikos vertinimo rezultatai tampa privalomi, kai organizacija priima sprendimus nustatytai rizikai mažinti, taigi ir tampa *atskaitinga* (*accountable*).

[13] Tinkamumo sąvoka aiškiai rodo, kad nesiekiama suteikti reikšmės visoms teoriškai įmanomoms techninėms ir organizacinėms priemonėms. Šiuo klausimu žr. M. Gambini, „Responsabilità e risarcimento nel trattamento dei dati personali“, paskelbta V. Cuffaro, R. D'Orazio, V. Ricciuto, „I dati personali nel diritto europeo“, Giappichelli, 2019 m., p. 1059.

36. 32 straipsnio 1 dalyje taip pat numatyta, kad turi būti atsižvelgta į aptariamų techninių ir organizacinių priemonių „įgyvendinimo sąnaudas“. Darytina išvada, kad tokių priemonių tinkamumo vertinimas turi būti grindžiamas duomenų subjekto interesų, kurių apsaugos lygis paprastai yra aukštesnis, ir duomenų valdytojo ekonominių interesų bei technologinių pajėgumų, kurių apsaugos lygis kartais gali būti žemesnis, pusiausvyra. Toks pusiausvyros užtikrinimas turi atitikti bendrojo proporcingumo principo reikalavimus.

37. Be to, aiškinant sistemiškai, reikėtų pridurti, jog teisės aktų leidėjas numato, kad tokių sistemų pažeidimų gali pasitaikyti; 32 straipsnio 1 dalies c punkte tarp siūlomų priemonių nurodytas gebėjimas laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju. Saugumo priemonių, kuriomis užtikrinamas riziką atitinkantis šių pajėgumų saugumo lygis, numatymas būtų beprasmis, jei būtų teigiama, kad vien sistemų pažeidimas savaime yra tokių priemonių netinkamumo įrodymas.

C. Antrasis prejudicinis klausimas

38. Antruoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, koks turėtų būti teisminės kontrolės dalykas ir apimtis vertinant asmens duomenų valdytojo įgyvendintų techninių ir organizacinių priemonių tinkamumą pagal reglamento 32 straipsnį.

39. Atsižvelgiant į praktikoje galinčių susiklostyti situacijų įvairovę, reglamente, kaip minėta, nepateikiamos privalomos nuostatos, pagal kurias nustatomos techninės ir organizacinės priemonės, kurių turi imtis duomenų valdytojas, kad įvykdytų minėto reglamento reikalavimus. Taigi priemonių, kurių buvo imtasi, tinkamumas turės būti vertinamas *in concreto*, nagrinėjant, ar konkrečios priemonės buvo tinkamos siekiant pagrįstai užkirsti kelią rizikai ir kuo labiau sumažinti neigiamas pažeidimo pasekmes.

40. Be abejo, tokių priemonių pasirinkimas ir įgyvendinimas priklauso subjektyviam duomenų valdytojo vertinimui, nes reglamente nurodytos priemonės yra tik pavyzdinės, todėl teisminė kontrolė negali apsiriboti tik patikrinimu, ar duomenų valdytojas laikosi savo pareigų pagal 24 ir 32 straipsnius, t. y. ar jis (formaliai) numatė tam tikras technines ir organizacines priemones. Jis turi atlikti konkrečią šių priemonių turinio, jų taikymo būdo ir praktinio poveikio analizę, remdamasis turimais įrodymais ir nagrinėjamo atvejo aplinkybėmis. Kaip tinkamai pažymėjo Portugalijos vyriausybė, „būdas, kuriuo jis įvykdė savo pareigas, atrodo neatsiejamas nuo priimtų priemonių turinio, siekiant įrodyti, kad, atsižvelgdamas į konkretų duomenų tvarkymą (jo pobūdį, apimtį, kontekstą ir tikslus), techninių galimybių išsivystymo lygį ir jų įgyvendinimo sąnaudas, taip pat į pavojų piliečių teisėms ir laisvėms, duomenų valdytojas ėmėsi visų būtinų ir tinkamų priemonių, kad būtų užtikrintas pavojų atitinkančio lygio saugumas“ [14].

41. Taigi atliekant teisminę kontrolę reikės atsižvelgti į visus kriterijus, nurodytus 24 ir 32 straipsniuose, kuriuose, kaip minėta, išvardyti tam tikri tinkamumo vertinimo kriterijai ir pateikti priemonių, kurios gali būti laikomos tinkamomis, pavyzdžiai. Be to, kaip nurodė Komisija ir visos valstybės narės, pateikusios pastabas dėl antrojo klausimo, 32 straipsnio 1–3 dalyse pabrėžiama būtinybė užtikrinti „pavojų atitinkančio lygio saugum[ą]“, pažymint kitus šiuo atveju svarbius kriterijus, pavyzdžiui, galimą duomenų tvarkytojo patvirtinto elgesio kodekso priėmimą ar patvirtinto sertifikavimo mechanizmo nustatymą, kaip numatyta atitinkamai reglamento 40 ir 42 straipsniuose.

[14] Rašytinių pastabų 31 punktas.

42. Elgesio kodeksų priėmimas ar sertifikavimo mechanizmų nustatymas gali būti naudingas vertinimo kriterijus įrodinėjimo pareigos ir su tuo susijusios teisminės kontrolės vykdymo tikslais. Vis dėlto vertėtų patikslinti, kad duomenų valdytojui nepakanka laikytis elgesio kodekso, bet jis turi ir pareigą įrodyti, kad iš tikrųjų ėmėsi jame numatytų priemonių, vadovaudamasis atskaitomybės principu. Kita vertus, sertifikavimas „pats savaime yra įrodymas, kad vykdomos duomenų tvarkymo operacijos atitinka reglamentą, net jeigu jį praktiškai galima paneigti“ [15].

43. Galiausiai reikia pažymėti, kad tos priemonės prireikus turi būti peržiūrimos ir atnaujinamos pagal 24 straipsnio 1 dalį. Ir tai taip pat turės įvertinti nacionalinis teismas. Pagal reglamento 32 straipsnio 1 dalį [16] duomenų valdytojui tenka pareiga ne tik atlikti nuolatinę kontrolę ir stebėseną prieš duomenų tvarkymą ir po jo, bet ir prižiūrėti ir galbūt atnaujinti priimtas priemones, kad būtų užkirstas kelias pažeidimams, o jų padarius – sumažintas jų poveikis.

44. Vis dėlto esu linkęs atmesti galimybę, kad būsimame sprendime bus pateiktas esminių kriterijų sąrašas, kaip antai pasiūlytas Portugalijos vyriausybės [17]. Tai galėtų sukelti prieštaringų aiškinimų, nes akivaizdu, kad sąrašas niekada nebus baigtinis.

D. Trečiasis prejudicinis klausimas

45. Pirma savo trečiojo klausimo dalimi prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės prašo Teisingumo Teismo nustatyti, ar, atsižvelgiant į reglamento 5 straipsnio 2 dalyje ir 24 straipsnyje, siejamame su 74 konstatuojamąja dalimi [18], įtvirtintą atskaitomybės principą, nagrinėjant ieškinį dėl žalos atlyginimo pagal 82 straipsnį įrodinėjimo pareiga dėl techninių ir organizacinių priemonių tinkamumo pagal 32 straipsnį tenka asmens duomenų valdytojui.

46. Remiantis pirma išdėstytais argumentais, galima apibendrintai teigiamai atsakyti į šį klausimą.

47. Iš tiesų teisės akto tekstas, kontekstas ir reglamento tikslai vienareikšmiškai patvirtina duomenų valdytojui tenkančią įrodinėjimo pareigą.

48. Iš įvairių reglamento nuostatų formuluočių matyti, kad duomenų valdytojas turi „galėti“ arba „gebėti“ „įrodyti“, kad jis laikosi savo įsipareigojimų pagal reglamentą, ir visų pirma tai, kad jis šiuo tikslu įgyvendino tinkamas priemones, kaip numatyta 74 konstatuojamojoje dalyje,

[15] M. Gambini, minėtas leidinys „Responsabilità“, p. 1067. Taigi turint sertifikavimo dokumentus įrodinėjimo pareiga perkeliama jų turėtojui, kuriam palengvinama galimybė įrodyti, kad jis veikė laikydamasis reglamente nustatytų pareigų.

[16] Šios dalies d punkte aiškiai nustatyta, kad sprendimas dėl tinkamumo apima ir priimtų priemonių veiksmingumą, kuris turi būti reguliariai tikrinamas ir vertinamas tiek pradiniu etapu, tiek periodiškai, siekiant užtikrinti veiksmingą visų rūšių duomenų tvarkymo operacijų saugumą, neatsižvelgiant į jų rizikos lygį; be to, c punkte aiškiai nustatyta, kad įgyvendintos techninės ir organizacinės priemonės turi būti tokios, kad fizinio ar techninio incidento atveju būtų užtikrintas gebėjimas laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis. Žr. M. Gambini, minėtas leidinys „Responsabilità“, p. 1064–1065.

[17] Rašytinių pastabų 30 punktas: „duomenų valdytojas turi įrodyti, kaip įvertino visus su nagrinėjamu duomenų tvarkymu susijusius kriterijus ir aplinkybes, visų pirma atliktos rizikos analizės rezultatus, nustatytą riziką, konkrečias priemones šiai rizikai sumažinti, pasirinktų galimybių pagrindimą atsižvelgiant į rinkoje prieinamus technologinius sprendimus, priemonių veiksmingumą, techninių ir organizacinių priemonių ryšį, duomenis tvarkančių darbuotojų mokymą, duomenų tvarkymo operacijų užsakomąsias paslaugas, įskaitant informacinių technologijų diegimą ir priežiūrą, ir tai, ar duomenų tvarkytojas vykdo duomenų tvarkymo kontrolę ir teikia tikslius nurodymus duomenų tvarkymą atliekantiems asmenims, kaip tai suprantama pagal BDAR 28 straipsnį, dėl pastarųjų atliekamo duomenų tvarkymo, taip pat tai, kaip buvo įvertinta ryšių ir informacinių sistemų rėmimo infrastruktūra ir kaip buvo nustatytas pavojaus duomenų subjektų teisėms ir laisvėms lygis“.

[18] Kaip išdėstyta 74 konstatuojamojoje dalyje, „turėtų būti nustatyta duomenų valdytojo atsakomybė už bet kokį duomenų valdytojo arba jo vardu vykdomą asmens duomenų tvarkymą. Duomenų valdytojas visų pirma turėtų būti įpareigotas įgyvendinti tinkamas ir veiksmingas priemones ir galėti įrodyti, kad duomenų tvarkymo veikla atitinka šį reglamentą, įskaitant priemonių veiksmingumą. Tomis priemonėmis turėtų būti atsižvelgta į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat į pavojų fizinių asmenų teisėms ir laisvėms.“

5 straipsnio 2 dalyje ir 24 straipsnio 1 dalyje. Kaip nurodo Portugalijos vyriausybė, minėtoje 74 konstatuojamojoje dalyje patikslinama, kad šiuo atveju duomenų valdytojui tenkanti įrodinėjimo pareiga turi apimti atitinkamų „priemonių veiksmingumo“ įrodymą.

49. Man atrodo, kad tokį pažodinį aiškinimą patvirtina toliau nurodomi praktiniai ir teleologiniai argumentai.

50. Kiek tai susiję su įrodinėjimo pareigos paskirstymu, nagrinėjant 82 straipsniu grindžiamą ieškinį dėl žalos atlyginimo duomenų subjektas, pareiškęs ieškinį duomenų valdytojui, turi įrodyti, pirma, kad buvo padarytas reglamento pažeidimas, antra, kad jis patyrė žalą, ir, trečia, kad tarp dviejų pirmesnių elementų yra priežastinis ryšys, kaip pažymėta visos rašytinėse pastabose dėl penktojo prejudicinio klausimo. Šios trys sąlygos yra kumuliatyvios, kaip matyti ir iš Teisingumo Teismo suformuotos jurisprudencijos, ir Bendrojo Teismo praktikos Sąjungos deliktinės atsakomybės srityje [19].

51. Vis dėlto manau, kad ieškovo pareiga įrodyti reglamento pažeidimo faktą negali būti tokia plati, kad jis privalėtų įrodyti, kodėl duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės yra netinkamos, kaip tai suprantama pagal 24 ir 32 straipsnius.

52. Kaip nurodo Komisija, tokių įrodymų pateikti praktikoje dažnai beveik neįmanoma, nes duomenų subjektai paprastai neturi nei pakankamai žinių, kad galėtų analizuoti tokias priemones, nei galimybės susipažinti su visa ginčijamus duomenų tvarkymo veiksmus atliekančio valdytojo turima informacija, visų pirma susijusia su metodais, taikomais siekiant užtikrinti tokio duomenų tvarkymo saugumą. Be to, kartais duomenų valdytojas galėtų teigti, kad jo atsisakymas atskleisti šiuos faktus duomenų subjektams grindžiamas teisėtu pagrindu neatskleisti savo vidaus reikalų ar netgi informacijos, kuri laikoma profesine paslaptimi, be kita ko, būtent dėl saugumo.

53. Taigi teigiant, kad įrodinėjimo pareiga tenka duomenų subjektui, praktinis rezultatas būtų toks, kad nebūtų galima įgyvendinti visos teisės pareikšti ieškinį pagal 82 straipsnio 1 dalį. Mano nuomone, tai neatitiktų Sąjungos teisės aktų leidėjo ketinimų, nes jis, priimdamas šį reglamentą, siekė sustiprinti duomenų subjektų teises ir duomenų valdytojų pareigas, palyginti su Direktyva 95/46/EB, kurią jis pakeitė. Todėl logiškiau ir teisiškai pagrįsčiau teigti, kad duomenų valdytojas, gindamasis nuo ieškinio dėl žalos atlyginimo, privalo įrodyti, kad jis įvykdė savo pareigas pagal to reglamento 24 ir 32 straipsnius ir veiksmingai ėmėsi tinkamų priemonių.

54. Trečiojo klausimo antra dalimi prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės prašo Teisingumo Teismo išaiškinti, ar teismo eksperto išvada gali būti laikoma būtinu ir pakankamu įrodymu siekiant įvertinti asmens duomenų valdytojo įgyvendintų techninių ir organizacinių priemonių tinkamumą tuo atveju, kai prieiga prie asmens duomenų ir jų atskleidimas be leidimo yra *įsilaužimo* pasekmė.

55. Manau, kad, kaip (iš esmės) pabrėžė Bulgarijos ir Italijos vyriausybės, taip pat Airija ir Komisija, atsakymas į šiuos klausimus turi būti grindžiamas suformuota jurisprudencija; pagal ją, remiantis procesinės autonomijos principu, nesant Sąjungos taisyklių šiuo klausimu, būtent kiekvienos valstybės narės vidaus teisės sistema turi nustatyti išsamias procesines taisykles,

[19] Žr., be kita ko, Teisingumo Teismo sprendimus: 2019 m. rugsėjo 5 d. Sprendimą *Europos Sąjunga / Guardian Europe ir Guardian Europe* / *Europos Sąjunga* (C-447/17 P ir C-479/17 P, EU:C:2019:672, 147 punktas) ir 2021 m. spalio 28 d. Sprendimą *Vialto Consulting Kft.* / *Komisija* (C-650/19 P, EU:C:2021:879, 138 punktas), taip pat Bendrojo Teismo sprendimus: 2021 m. sausio 13 d. Sprendimą *Helbert* / *EUIPO* (T-548/18, EU:T:2021:4, 116 punktas) ir 2021 m. rugsėjo 29 d. Sprendimą *Kočner* / *Europolas* (T-528/20, nepaskelbtas Rink., EU:T:2021:631, 61 punktas); juose primenama, kad turi būti įvykdytos trys sąlygos, t. y. „veiksmų, kuriais kaltinama Sąjungos institucija, neteisėtum[as], žalos realum[as] ir priežastinio ryšio tarp institucijos veiksmų ir nurodytos žalos buvim[as]“.

kuriomis reglamentuojami teisminiai procesai, skirti asmenų teisių apsaugai, tačiau su sąlyga, kad šios taisyklės Sąjungos teisės reglamentuojamose situacijose nėra mažiau palankios nei taisyklės, reglamentuojančios panašias situacijas pagal nacionalinę teisę (lygiavertiškumo principas), ir kad dėl jų praktiškai netampa neįmanoma arba pernelyg sunku naudotis Sąjungos teisės suteiktomis teisėmis (veiksmingumo principas).

56. Šiuo atveju pažymiu, kad reglamente nėra nuostatų, kuriomis būtų siekiama nustatyti leistinus įrodinėjimo būdus ir jų įrodomąją vertę, ypač kiek tai susiję su tyrimo veiksmais (pavyzdžiui, eksperto išvada), kuriuos nacionaliniai teismai gali arba turi nurodyti atlikti, kad galėtų įvertinti, ar duomenų valdytojas ėmėsi tinkamų priemonių, kaip tai suprantama pagal reglamentą. Todėl manau, kad, nesant suderintų taisyklių šiuo klausimu, šią procesinę tvarką, laikantis lygiavertiškumo ir veiksmingumo principų, turi nustatyti kiekvienos valstybės narės vidaus teisės sistema.

57. Minėtas „veiksmingumo principas“, kuris reiškia, kad nepriklausomas teisėjas turi atlikti nešališką vertinimą, galėtų būti pažeistas, jei būdvardis „pakankamas“ būtų suprantamas taip, kad prašymą priimti prejudicinį sprendimą pateikęs teismas gali automatiškai iš eksperto išvados nustatyti, jog duomenų valdytojo priimtos priemonės yra tinkamos [20].

E. Ketvirtasis prejudicinis klausimas

58. Ketvirtuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar reglamento 82 straipsnio 3 dalis turi būti aiškinama taip, kad aplinkybė, jog šio reglamento pažeidimą (kuris, kaip šioje byloje, yra asmens duomenų „atskleidimas be leidimo“ arba prie jų „be leidimo gaunama prieiga“, kaip tai suprantama pagal 4 straipsnio 12 punktą) padarė asmenys, kurie nėra šių duomenų valdytojo darbuotojai ir nėra jo kontroliuojami, t. y. buvo įvykdytas pažeidimas, kuris jokiu būdu nepriskirtinas duomenų valdytojui, yra pagrindas atleisti jį nuo atsakomybės, kaip tai suprantama pagal 82 straipsnio 3 dalį.

59. Atsakymas į klausimą tiesiogiai kyla iš to, kas buvo išdėstyta pirma dėl bendros reglamento filosofijos: automatiškumas nenumatytas, todėl vien tai, kad asmens duomenis be leidimo atskleidė arba prie jų be leidimo gavo prieigą asmenys, nepriklausantys duomenų valdytojo kontrolės sričiai, neatleidžia to valdytojo nuo atsakomybės.

60. Pirma, aiškinant pažodžiui reikėtų pažymėti, kad nei 82 straipsnio 3 dalyje, nei 146 konstatuojamojoje dalyje nenustatyta jokių konkrečių sąlygų, kurios gali būti įvykdytos, kad duomenų valdytojas būtų atleistas nuo atsakomybės, išskyrus įrodymą, kad jis „jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala“. Iš šios formuluotės matyti, kad, pirma, duomenų valdytojas gali būti atleistas nuo atsakomybės tik tuo atveju, jeigu įrodo, kad už įvykį, dėl kurio patirta atitinkama žala, jis nėra atsakingas, ir, antra, šioje nuostatoje reikalaujamų įrodymų lygis yra aukštas, atsižvelgiant į sąvokos „jokiu būdu“ vartojimą, kaip tai nurodė Komisija [21].

61. 82 straipsnyje ir apskritai visame reglamente numatytas atsakomybės režimas sukėlė daug diskusijų įvairių valstybių narių doktrinoje. Iš tikrųjų jame yra tradicinių nesutartinės atsakomybės elementų, kaip ir elementų, kurie pagal nuostatų struktūrą priartina šią atsakomybę prie sutartinės

[20] Rašytinių pastabų 39 punktas.

[21] Tai atitinka Teisingumo Teismo suformuotą jurisprudenciją; pagal ją bendrosios taisyklės išimtys turi būti aiškinamos siaurai, todėl bet koks atleidimas nuo atsakomybės pagal 82 straipsnio 3 dalį turi būti aiškinamas siaurai. Pagal analogiją žr. 2020 m. spalio 15 d. Sprendimą *Association française des usagers de banques* (C-778/18, EU:C:2020:831, 53 punktas) ir 2022 m. balandžio 5 d. Sprendimą *Commissioner of the Garda Síochána ir kt.* (C-140/20, EU:C:2022:258, 40 punktas).

atsakomybės arba netgi prie atsakomybės be kaltės formos, atsižvelgiant į duomenų tvarkymo veiklai būdingą pavojingumą. Šioje išvadoje negali būti išsamiai aptartos minėtos diskusijos, tačiau, mano nuomone, 82 straipsnyje atsakomybės be kaltės forma nenustatyta [22].

62. Žala, atsiradusi dėl asmens duomenų saugumo pažeidimo, gali atsirasti kaip neatsargumo pasekmė dėl to, kad nebuvo imtasi pagrįstų ir bet kuriuo atveju tinkamų techninių ir organizacinių priemonių, kad būtų užkirstas kelias pažeidimui, atsižvelgiant į su duomenų tvarkymo veikla susijusį pavojų asmenų teisėms ir laisvėms. Dėl šio pavojaus pareiga užkirsti kelią žalai ir jos išvengti tampa griežtesnė, išplečiant duomenų valdytojui tenkančią rūpestingumo pareigą. Taigi, suderintai vertinant duomenų valdytojams tenkančias elgesio pareigas ir nuostatą dėl teisinančių įrodymų, kuriuos turi pateikti žalą padaręs subjektas, galima pateikti argumentų, kuriais remiantis pripažįstamas griežtesnis preziumuojama kalte grindžiamos atsakomybės už neteisėtą asmens duomenų tvarkymą, kaip numatyta reglamento 82 straipsnyje, pobūdis [23].

63. Tai reiškia, kad duomenų valdytojas gali pateikti pateisinamųjų įrodymų, kuriais remiantis jis būtų atleistas nuo atsakomybės (tokie įrodymai neleistini atsakomybės be kaltės atveju). Dėl įrodinėjimo pareigos paskirstymo reglamento 82 straipsnio 3 dalyje nustatyta nukentėjusiajai šaliai palanki procedūra; pagal ją numatoma tam tikra nukentėjusiosios šalies įrodinėjimo pareigos perkėlimo forma [24], kuri visiškai atitinka minėtą įrodinėjimo pareigos perkėlimą, kiek tai susiję su priemonių, kurių buvo imtasi, tinkamumu. Taip teisės aktų leidėjas parodo, kad suvokia pavojus, kylančius pritarus skirtingam įrodinėjimo pareigos paskirstymui; jeigu jis žalą padariusios šalies kaltės įrodinėjimo pareigą perkeltų nukentėjusiam fiziniam asmeniui, tai pernelyg apsunkintų jo padėtį ir būtų faktiškai pakenkta žalos atlyginimo instituto veiksmingumui, atsižvelgiant į taisykles, susijusias su naujų technologijų naudojimu. Duomenų subjektui gali būti itin sudėtinga atkurti žalos atsiradimo aplinkybes ir gauti informacijos apie tai, taigi ir įrodyti duomenų valdytojo kaltę. Priešingai, duomenų valdytojas turi geriausias galimybes pateikti pateisinamuosius įrodymus, kad jis jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala [25].

64. Duomenų valdytojas, vadovaudamasis pirma aptartu atskaitomybės principu, taip pat turės įrodyti, jog jis ėmėsi visų įmanomų veiksmų, kad laiku atkurtų sąlygas ir galimybes naudotis asmens duomenimis.

65. Grįžtant prie prašymą priimti prejudicinį sprendimą pateikusio teismo klausimo ir atsižvelgiant į pateiktus argumentus dėl duomenų valdytojo atsakomybės pobūdžio, pažymėtina, kad, jei, kaip minėta, duomenų valdytojas gali būti atleistas nuo atsakomybės, jam įrodžius, kad pažeidimas įvykdytas dėl visiškai nuo jo nepriklausančios aplinkybės, tokia aplinkybe negali būti laikomas vien faktas, kad įvykį sukėlė asmuo, kurio jis negali kontroliuoti.

[22] Civilinė atsakomybė paprastai kvalifikuojama kaip atsakomybė be kaltės, kai subjekto atstovas privalo imtis visų abstrakčiai įmanomų priemonių žalai išvengti, neatsižvelgiant į tai, ar jis faktiškai apie ją žinojo, ar į šių priemonių ekonominį tvarumą. Ir priešingai, kai subjekto atstovas privalo imtis priemonių, kurių paprastai turi imtis atitinkamo ekonomikos sektoriaus ekonominės veiklos vykdytojas, kad būtų užtikrintas saugumas ir išvengta žalos, kuri gali atsirasti dėl vykdomos veiklos, pačios žalos priskyrimui labiau taikytinas konkrečia kalte grindžiamos atsakomybės režimas. M. Gambini, minėtas leidinys „Responsabilità“, p. 1055.

[23] M. Gambini, minėtas leidinys „Responsabilità“, p. 1059. Pagal analogiją pateiktinas požiūris, jog įrodant, kad buvo imtasi tinkamų priemonių, nepakanka teigti, kad buvo laikomasi didžiausio įmanomo rūpestingumo, bet turi būti įrodytas ir trečiasis žalą sukėlęs veiksnys, kuriam būdingos nenuspėjamumo ir neišvengiamumo savybės, įprastai pasireiškiančios nenumatytų aplinkybių arba *force majeure* atvejais; S. Sica, „Sub art. 82“, paskelbta R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta leidinyje „Codice della privacy e data protection“, Giuffrè, 2021 m.

[24] „<…> jeigu jis *įrodo*, kad jokiu būdu nėra atsakingas už įvykį, dėl kurio patirta žala“ (82 straipsnio 3 dalis).

[25] M. Gambini, minėtas leidinys „Responsabilità“, p. 1060.

66. Kai duomenų valdytojas tampa kibernetinių nusikaltėlių išpuolių auka, galėtų būti laikoma, kad duomenų valdytojas nėra kaltas dėl žalą sukėlusio įvykio, tačiau negalima atmesti galimybės, kad duomenų valdytojo aplaidumas galėjo būti atitinkamo išpuolio, kurį palengvino asmens duomenų saugumo priemonių, kurias duomenų valdytojas privalėjo įgyvendinti, nebuvimas arba netinkamumas, priežastis. Tai kiekvieno atskiro atvejo faktinių aplinkybių vertinimas, kurį atlieka bylą nagrinėjantis nacionalinis teismas, atsižvelgdamas į jam pateiktus įrodymus.

67. Be to, bendra patirtis rodo, kad išpuoliai iš išorės prieš viešojo ar privačiojo sektoriaus subjektų, saugančių didelius kiekius asmens duomenų, sistemas yra kur kas dažnesni nei vidiniai išpuoliai. Vadinasi, duomenų valdytojas turi imtis tinkamų priemonių, kad galėtų kovoti visų pirma su išpuoliais iš išorės.

68. Galiausiai teleologiniu požiūriu reikia pažymėti, kad reglamentu siekiama aukšto apsaugos lygio tikslo. Šiuo klausimu Teisingumo Teismas jau pažymėjo, kad, kaip matyti iš reglamento 1 straipsnio 2 dalies, siejamos su jo 10, 11 ir 13 konstatuojamosiomis dalimis, šiame reglamente Sąjungos institucijoms, įstaigoms ir organams bei kompetentingoms valstybių narių institucijoms nustatyta užduotis užtikrinti aukštą SESV 16 straipsnyje ir Chartijos 8 straipsnyje garantuojamų su asmens duomenų apsauga susijusių teisių apsaugos lygį [26].

69. Jeigu Teisingumo Teismas pasirinktų aiškinimą, kad tuo atveju, kai reglamento pažeidimą padarė trečiasis asmuo, duomenų valdytojas turėtų būti automatiškai atleidžiamas nuo atsakomybės pagal 82 straipsnio 3 dalį, toks aiškinimas būtų nesuderinamas su šiuo teisės aktu siekiamu apsaugos tikslu, nes būtų susilpnintos duomenų subjektų teisės, kadangi ši atsakomybė būtų taikoma tik tais atvejais, kai pažeidimą įvykdo asmenys, kurie yra pavaldūs šiam duomenų valdytojui ir (arba) yra jo kontroliuojami.

F. Penktasis prejudicinis klausimas

70. Penktuoju klausimu nacionalinis teismas iš esmės prašo Teisingumo Teismo išaiškinti „neturtinės žalos“ (reglamente – „nematerialinės“) sąvoką, kaip ji suprantama pagal reglamento 82 straipsnį. Visų pirma jis siekia išsiaiškinti, ar reglamento 82 straipsnio 1 ir 2 dalių, siejamų su jo 85 ir 146 konstatuojamosiomis dalimis [27], nuostatos turi būti aiškinamos taip, kad tuo atveju, kai šio reglamento pažeidimas pasireiškė be leidimo gaunama prieiga prie asmens duomenų ir kibernetinių nusikaltėlių įvykdytu šių duomenų atskleidimu be leidimo, aplinkybė, kad duomenų subjektas baiminasi dėl galimo būsimo piktnaudžiavimo jo asmens duomenimis, savaime gali būti laikoma (neturtine) žala, suteikiančia jam teisę į kompensaciją.

71. Nei 82 straipsnyje, nei konstatuojamosiose dalyse dėl kompensacijos nepateikiama aiškaus atsakymo į šį klausimą, tačiau iš jų galima daryti keletą analizei naudingų prielaidų: neturtinė (arba moralinė) žala gali būti atlyginama kartu su turtine (arba pinigine) žala; reglamento pažeidimas nėra automatiškai siejamas su „padaryta“ žala, arba, konkrečiai kalbant, asmens duomenų apsaugos pažeidimas „gali sukelti“ fizinę, turtinę arba neturtinę žalą fiziniams

[26] Šiuo klausimu žr. 2021 m. birželio 15 d. Sprendimą *Facebook Ireland ir kt.* (C-645/19, EU:C:2021:483, 44 ir 45 punktai).

[27] Kaip išdėstyta 85 konstatuojamojoje dalyje, „dėl asmens duomenų saugumo pažeidimo, jei dėl jo laiku nesiimama tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą <…>“. Pagal 146 konstatuojamąją dalį „bet kokią žalą, kurią asmuo gali patirti dėl duomenų tvarkymo pažeidžiant šį reglamentą, turėtų atlyginti duomenų valdytojas arba duomenų tvarkytojas. Duomenų valdytojas arba duomenų tvarkytojas turėtų būti atleisti nuo atsakomybės, jeigu jie įrodo, kad jokiu būdu nėra atsakingi už žalą. Žalos sąvoka turėtų būti aiškinama plačiai, atsižvelgiant į Teisingumo Teismo praktiką, taip, kad būtų visapusiškai atspindėti šio reglamento tikslai. Tai nedaro poveikio jokiems reikalavimams dėl žalos atlyginimo, kurie pareiškiami dėl kitų taisyklių, nustatytų Sąjungos ar valstybės narės teisėje <…>. Duomenų subjektai už patirtą žalą turėtų gauti visą ir veiksmingą kompensaciją <…>“

asmenims; žalos sąvoka turėtų būti aiškinama „plačiai“, atsižvelgiant į Teisingumo Teismo jurisprudenciją, kad būtų visapusiškai atspindėti reglamento tikslai; už „patirtą“ žalą turėtų būti gaunama „visa ir veiksminga“ kompensacija.

72. Pati reglamento nuostatų formuluotė neleidžia daryti jokių galimų prielaidų dėl žalos atsiradimo *in re ipsa*: pagrindinis reglamente numatytos civilinės atsakomybės tikslas – patenkinti duomenų subjekto interesus, būtent „visiškai ir veiksmingai“ kompensuojant patirtą žalą, ir taip atkurti dėl teisės pažeidimo neigiamai pasikeitusios (pažeistos) teisinės padėties pusiausvyrą [28].

73. Kita vertus, taip pat vertinant sistemiškai, kaip ir antimonopolinėje teisėje, reglamente numatyti du apsaugos ramsčiai: vienas – viešosios teisės pobūdžio, numatant sankcijas reglamento nuostatų pažeidimo atveju, ir kitas – privatinės teisės pobūdžio, numatant būtent nesutartinę civilinę atsakomybę, kuri gali būti kvalifikuojama kaip sunkesnė dėl numanomos kaltės, kuriai būdingos tam tikromis savybės, taip pat atsižvelgiant į pirma minėtus pateisinamuosius įrodymus [29].

74. Taigi, (neturtinės) žalos sąvoką aiškinant plačiai [30], negalima daryti išvados, kad teisės aktų leidėjas atsisakė būtinybės įrodyti, kad buvo padaryta reali „žala“.

75. Esminė problema yra klausimas, ar, nustačius pažeidimo faktą ir priežastinį ryšį, teisė į kompensaciją gali atsirasti vien tik dėl duomenų subjekto jaučiamo susirūpinimo, baimės ir nuogąstavimų dėl galimo būsimo piktnaudžiavimo jo asmens duomenimis, kai toks piktnaudžiavimas nebuvo nustatytas ir (arba) duomenų subjektas nepatyrė jokios papildomos žalos.

76. Remiantis Teisingumo Teismo suformuota jurisprudencija, tuo atveju, kai Sąjungos teisės nuostatoje aiškiai nedaroma nuorodos į valstybių narių teisę, norint nustatyti šios nuostatos prasmę ir apimtį, jos reikšmė visoje Sąjungoje paprastai turi būti aiškinama autonomiškai ir vienodai, atsižvelgiant ne tik į aptariamos nuostatos formuluotę, bet ir jos kontekstą ir nagrinėjamu teisės aktu, kuriame ši nuostata yra, siekiamą tikslą, taip pat į tokios nuostatos genezę [31].

[28] Žr. minėtos generalinio advokato M. Campos Sánchez-Bordona išvados 29 punktą ir 11 išnašą. Toje pačioje išvadoje generalinis advokatas teisingai užbaigia savo analizę pažodiniu, istoriniu, kontekstiniu ir teleologiniu požiūriais ir atmeta „baudos pobūdžio“ kompensaciją duomenų subjektams pagal 82 straipsnį (27–55 punktai), pažymėdamas, kad, pirma, valstybės narės „neturi (ir iš tiesų negali) rinktis vieno iš VIII skyriuje numatytų mechanizmų, siekdamos užtikrinti duomenų apsaugą. Jeigu dėl pažeidimo nepadaryta žalos, duomenų subjektas vis tiek (bent jau) turi teisę pateikti skundą priežiūros institucijai“; ir, antra, „perspektyva gauti kompensaciją, neatsižvelgiant į tai, ar padaryta žala, tikriausiai paskatintų civilinį bylinėjimąsi ir būtų reiškiami galbūt ne visada pagrįsti reikalavimai; tai galėtų atgrasyti nuo duomenų tvarkymo veiklos“ (54 ir 55 punktai).

[29] Taigi teisės į kompensaciją už tai, kad dėl duomenų tvarkymo taisyklių pažeidimo buvo patirti nestiprūs ir trumpalaikiai jausmai ar emocijos, paneigimas nereiškia, kad duomenų subjektas lieka visiškai neapsaugotas (šiuo atveju žr. minėtos generalinio advokato M. Campos Sánchez-Bordona išvados 115 punktą).

[30] Arba „plačiai“, kaip nurodyta 146 konstatuojamojoje dalyje.

[31] Žr. 2021 m. balandžio 15 d. Sprendimą *The North of England P & I Association* (C-786/19, EU:C:2021:276, 48 punktas) ir 2021 m. birželio 10 d. Sprendimą *KRONE – Verlag* (C-65/20, EU:C:2021:471, 25 punktas).

77. Teisingumo Teismas, kaip priminė generalinis advokatas M. Campos Sánchez-Bordona [32], nepateikė jokios bendros „žalos“ apibrėžties, vienodai taikytinos bet kuriomis aplinkybėmis [33]. Dėl neturtinės žalos, remiantis Teisingumo Teismo jurisprudencija, galima daryti tokią išvadą: žalos atlyginimo sąvoka turi būti plati, kai aiškinamos nuostatos tikslas (arba vienas iš tikslų) yra apsaugoti asmenį arba tam tikrą asmenų grupę [34]; laikantis šios taisyklės, kompensacija apima ir neturtinę žalą, net jei aiškinamoje nuostatoje ši žala neminima [35].

78. Nors atsižvelgiant į Teisingumo Teismo jurisprudenciją galima teigti, kad, kaip nurodyta pirma, Sąjungos teisėje egzistuoja neturtinės žalos atlyginimo principas, vis dėlto pritariu generaliniam advokatui M. Campos Sánchez-Bordona, kad remiantis šia jurisprudencija negalima suformuluoti taisyklės, pagal kurią kompensuotina *visa* neturtinė žala, nepaisant jos dydžio [36].

79. Šiomis aplinkybėmis svarbu atskirti atlygintiną neturtinę žalą ir kitus *nepatogumus, atsirandančius dėl teisės aktų nesilaikymo*, kurie, atsižvelgiant į jų nedidelį mastą, nebūtinai suteiktų teisę į kompensaciją [37].

80. Teisingumo Teismas pripažįsta šį skirtumą, nurodydamas nemalonumus ir nepatogumus kaip savarankišką kategoriją, palyginti su žala, patiriama tose srityse, kuriose, jo nuomone, ji turėtų būti kompensuota [38].

[32] Žr. minėtos generalinio advokato M. Campos Sánchez-Bordona išvados 104 punktą.

[33] Jis taip pat nenurodė, kuris aiškinimo metodas – savarankiškas ar pagrįstas nacionalinės teisės sistemomis – yra priimtinesnis: tai priklauso nuo nagrinėjamo dalyko. Žr. 2001 m. gegužės 10 d. Sprendimą *Veedfald* (C-203/99, EU:C:2001:258, 27 punktas) dėl gaminių su trūkumais, 2010 m. gegužės 6 d. Sprendimą *Walz* (C-63/09, EU:C:2010:251, 21 punktas) dėl oro vežėjų atsakomybės arba 2021 m. birželio 10 d. Sprendimą *Van Ameyde España SA* (C-923/19, EU:C:2021:475, 37 ir paskesni punktai) dėl motorinių transporto priemonių valdytojų civilinės atsakomybės už sukeltus draudžiamuosius įvykius.

[34] Pavyzdžiui, produktų vartotojus arba nuo eismo įvykių nukentėjusius asmenis.

[35] Kelionės paslaugų paketų srityje žr. 2002 m. kovo 12 d. Sprendimą *Leitner* (C-168/00, EU:C:2002:163); motorinių transporto priemonių valdytojų civilinės atsakomybės srityje žr. 2013 m. spalio 24 d. Sprendimą *Haasová* (C-22/12, EU:C:2013:692, 47–50 punktai), 2013 m. spalio 24 d. Sprendimą *Drozdovs* (C-277/12, EU:C:2013:685, 40 punktas) ir 2014 m. sausio 23 d. Sprendimą *Petillo* (C-371/12, EU:C:2014:26, 35 punktas).

[36] Žr. minėtos generalinio advokato M. Campos Sánchez-Bordona išvados 105 punktą. Pavyzdžiui, Teisingumo Teismas pripažino, kad nacionalinės teisės aktai, pagal kuriuos, siekiant apskaičiuoti kompensaciją, su kūno sužalojimu per nelaimingą atsitikimą susijusi neturtinė žala diferencijuojama pagal nelaimingo atsitikimo kilmę, atitinka Europos teisės normas; žr. 2014 m. sausio 23 d. Sprendimą *Petillo* (C-371/12, EU:C:2014:26), kurio rezoliucinėje dalyje nustatyta, kad pagal Sąjungos teisę nedraudžiami „nacionalinės teisės aktai, <…> kuriuose numatyta specifinė neturtinės žalos, kurią lemia nesunkūs kūno sužalojimai, patirti per kelių eismo įvykius, atlyginimo sistema, pagal kurią šios žalos atlyginimas apribotas, palyginti su leidžiamu tokios pačios žalos, atsiradusios ne per tokius įvykius, atlyginimu“.

[37] Kai kuriose nacionalinės teisės sistemose toks atskyrimas suvokiamas kaip neišvengiama gyvenimo visuomenėje pasekmė. Neseniai Italijoje duomenų apsaugos klausimu *Tribunale di Palermo* (Palermo teismas) I civilinių bylų skyrius 2017 m. spalio 5 d. priėmė Sprendimą Nr. 5261, taip pat Kasacinio teismo VI civilinių bylų kolegija priėmė Nutartį Nr. 17383/2020. Vokietijoje, be kita ko, priimtas 2018 m. lapkričio 7 d. *Amtsgericht Diez* (Dyco apylinkės teismas) sprendimas Nr. 8 C 130/18, 2019 m. rugpjūčio 2 d. *Landgericht Karlsruhe* (Karlsrūhės apygardos teismas) sprendimas Nr. 8 O 26/19 ir 2020 m. liepos 10 d. *Amtsgericht Frankfurt am Main* (Frankfurto prie Maino apylinkės teismas) sprendimas Nr. 385 C 155/19 (70). Austrijoje priimtas *Oberster Gerichtshof* (Aukščiausiasis Teismas) Sprendimas OGH 6 Ob 56/21k.

[38] Žr. 2012 m. spalio 23 d. Sprendimą *Nelson ir kt.* (C-581/10 ir C-629/10, EU:C:2012:657, 51 punktas) dėl skirtumo tarp „žalos“, kaip ji suprantama pagal 1999 m. gegužės 28 d. Monrealyje sudarytos Konvencijos dėl tam tikrų tarptautinio vežimo oru taisyklių suvienodinimo 19 straipsnį, ir „nepatogumų“, kaip tai suprantama pagal Reglamentą Nr. 261/2004, kurie turi būti atlyginti pagal šio reglamento 7 straipsnį, kaip tai suprantama pagal 2009 m. lapkričio 19 d. Sprendimą *Sturgeon ir kt.* (C-402/07 ir C-432/07, EU:C:2009:716). Šiame sektoriuje, kaip ir keleivių vežimo jūra ir vidaus vandenų keliais sektoriuje, kuriam taikomas Reglamentas Nr. 1177/2010, teisės aktų leidėjas galėjo pripažinti bendrą kategoriją, nes nemalonumų sukeliantis veiksnys ir nemalonumų esmė visiems nukentėjusiems asmenims yra vienodi. Manau, kad duomenų apsaugos srityje negalima daryti tokios išvados.

81. Empiriniu požiūriu pažymėtina, kad bet koks asmens duomenų apsaugos taisyklės pažeidimas sukelia tam tikrą neigiamą duomenų subjekto reakciją. Kompensaciją, kylančią iš paprasto nepasitenkinimo jausmo dėl kito asmens įvykdyto įstatymų nesilaikymo, lengva supainioti su kompensacija, kai žalos nepadaryta, o tai, kaip jau minėta, neatrodo įmanoma pagal reglamento 82 straipsnį, atsižvelgiant į bylos aplinkybes.

82. Tai, kad pagrindinėje byloje susiklosčiusiomis aplinkybėmis piktnaudžiavimas asmens duomenimis yra tik potencialus, o ne realus, yra pakankamas pagrindas pripažinti, kad duomenų subjektas galėjo patirti neturtinę žalą dėl šio reglamento pažeidimo, jeigu duomenų subjektas įrodo, kad baimė dėl tokio piktnaudžiavimo jam iš tikrųjų ir konkrečiai sukėlė realią ir tikrą emocinę žalą [39].

83. Paprastą nepasitenkinimą (nekompensuotiną) ir tikrą neturtinę žalą (kompensuotiną) skirianti riba neabejotinai yra plona, tačiau valstybių narių teismai, kurių užduotis yra kiekvienu konkrečiu atveju nustatyti šią ribą, turėtų atidžiai įvertinti visas aplinkybes, nurodytas kompensacijos prašančio duomenų subjekto, kuriam tenka pareiga tiksliai, o ne bendrai nurodyti konkrečius elementus, kuriais remiantis galima nustatyti, kad dėl asmens duomenų saugumo pažeidimo jis patyrė „realią neturtinę žalą“, net jei ji nesiekia iš anksto nustatytos ypač didelės sunkumo ribos: svarbu, kad tai būtų ne tik subjektyvus suvokimas, kuris kinta ir priklauso nuo charakterio bei asmeninių savybių, bet ir objektyvus nepatogumas, nors ir nedidelis, bet įrodomas, daromas asmens fizinei ar psichinei būklei arba jo socialiniams ryšiams; svarbus ir susijusių asmens duomenų pobūdis bei jų reikšmė atitinkamo asmens gyvenime, taip pat galbūt tuo metu visuomenėje vyraujantis suvokimas apie šiuos konkrečius nepatogumus, susijusius su duomenų saugumo pažeidimu [40].

IV. Išvada

84. Atsižvelgdamas į tai, kas išdėstyta, siūlau Teisingumo Teismui taip atsakyti į pateiktus prejudicinius klausimus:

„Reglamento (ES) 2016/679 5, 24, 32 ir 82 straipsniai turi būti aiškinami taip:

vien tik „asmens duomenų saugumo pažeidimo“, kaip jis apibrėžiamas 4 straipsnio 12 punkte, nepakanka, kad būtų galima daryti išvadą, jog duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės nebuvo „tinkamos“ nagrinėjamų duomenų apsaugai užtikrinti;

vertindamas, ar asmens duomenų valdytojo įgyvendintos techninės ir organizacinės priemonės yra tinkamos, nacionalinis teismas, į kurį kreiptasi, turi atlikti vertinimą, apimantį konkrečią tokių priemonių turinio, jų taikymo būdo ir praktinio poveikio analizę;

nagrinėjant ieškinį dėl kompensacijos pagal BDAR 82 straipsnį, asmens duomenų valdytojas privalo įrodyti, kad priemonės, kurias jis įgyvendino pagal šio reglamento 32 straipsnį, yra tinkamos;

[39] Airijos teigimu, šie argumentai yra ypač svarbūs praktiniu požiūriu, kiek tai susiję su kibernetiniais nusikaltimais, nes jei bet kuris asmuo, nors ir mažai nukentėjęs nuo pažeidimo, turėtų teisę į neturtinės žalos atlyginimą, tai turėtų didelį poveikį visų pirma viešojo sektoriaus duomenų valdytojams, kurie finansuojami ribotomis viešojo sektoriaus lėšomis ir turėtų verčiau tarnauti bendriems interesams, įskaitant asmens duomenų saugumo didinimą (rašytinių pastabų 72 punktas).

[40] Žr. minėtos generalinio advokato M. Campos Sánchez-Bordona išvados 116 punktą.

pagal procesinės autonomijos principą kiekvienos valstybės narės vidaus teisinėje sistemoje turi būti nustatyti leistini įrodinėjimo būdai ir jų įrodomoji vertė, įskaitant tyrimo veiksmus, kuriuos nacionaliniai teismai gali arba turi nurodyti atlikti, kad galėtų įvertinti, ar duomenų valdytojas ėmėsi tinkamų priemonių, kaip tai suprantama pagal reglamentą, laikantis Sąjungos teisėje apibrėžtų lygiavertiškumo ir veiksmingumo principų;

aplinkybė, kad šio reglamento pažeidimą, sukėlusį minėtą žalą, padarė trečiasis asmuo, savaime nėra pagrindas atleisti duomenų valdytoją nuo atsakomybės, o siekdamas pasinaudoti šioje nuostatoje numatyta išimtimi duomenų valdytojas turi įrodyti, kad jis jokiu būdu nėra atsakingas už pažeidimą;

žala, patirta dėl baimės dėl galimo būsimo piktnaudžiavimo asmens duomenimis, jeigu jos buvimą duomenų subjektas įrodė, gali būti laikoma neturtine žala, suteikiančia teisę į kompensaciją, jeigu duomenų subjektas įrodo, kad jis individualiai patyrė realią ir tikrą emocinę žalą, kurią kiekvienu konkrečiu atveju turi įvertinti nacionalinis teismas, į kurį kreiptasi.“