Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
GIOVANNIJA PITRUZZELLE
od 27. travnja 2023. [1]

Predmet C-340/21

VB
protiv
Nacionalne agencije za prihodite

(zahtjev za prethodnu odluku koji je uputio Vrhoven administrativen sad (Vrhovni upravni sud, Bugarska))

„Zahtjev za prethodnu odluku – Zaštita osobnih podataka – Uredba (EU) 2016/679 – Odgovornost voditelja obrade – Sigurnost obrade – Povreda sigurnosti obrade osobnih podataka – Nematerijalna šteta pretrpljena zbog nedjelovanja voditelja obrade – Tužba za naknadu štete”

Može li nezakonito širenje osobnih podataka kojima raspolože javnopravna agencija i koje je posljedica hakerskog napada dovesti do toga da osobi čiji se podaci obrađuju treba nadoknaditi nematerijalnu štetu samo zato što ta osoba strahuje zbog moguće buduće zlouporabe njezinih podataka? Koji su kriteriji za pripisivanje odgovornosti voditelju obrade? Kako se teret dokaza raspodjeljuje u okviru sudskog postupka? Koji je opseg ispitivanja koje provodi sud?

I. Pravni okvir

1. Člankom 4. Uredbe 2016/679 [2] (u daljnjem tekstu: Uredba), naslovljenim „Definicije”, određuje se:

„Za potrebe ove Uredbe:

[…]

12. ‚povreda osobnih podataka’ znači kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani;

[…]”.

[1] Izvorni jezik: talijanski

[2] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)

2. Članak 5., naslovljen „Načela obrade osobnih podataka”, glasi:

„1. Osobni podaci moraju biti:

[…]

(f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera (‚cjelovitost i povjerljivost’);

2. Voditelj obrade odgovoran je za usklađenost sa stavkom 1. te je mora biti u mogućnosti dokazati (‚pouzdanost’)”.

3. Člankom 24. te uredbe, naslovljenim „Obveze voditelja obrade”, utvrđuje se:

„1. Uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, kao i rizike različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada provodi u skladu s ovom Uredbom. Te se mjere prema potrebi preispituju i ažuriraju.

2. Ako su razmjerne u odnosu na aktivnosti obrade, mjere iz stavka 1. uključuju provedbu odgovarajućih politika zaštite podataka od strane voditelja obrade.

3. Poštovanje odobrenih kodeksa ponašanja iz članka 40. ili odobrenih mehanizama certificiranja iz članka 42. može se iskoristiti kao element za dokazivanje sukladnosti s obvezama voditelja obrade”.

4. Člankom 32., naslovljenim „Sigurnost obrade”, predviđa se:

„1. Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

[…]

2. Prilikom procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja osobnih podataka ili neovlaštenog pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani.

3. Poštovanje odobrenog kodeksa ponašanja iz članka 40. ili odobrenog mehanizma certificiranja iz članka 42. može se iskoristiti kao element za dokazivanje sukladnosti sa zahtjevima iz stavka 1. ovog članka.

[…]”.

5. Člankom 82. navedene uredbe, naslovljenim „Pravo na naknadu štete i odgovornost”, određuje se:

„1. Svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog kršenja ove Uredbe ima pravo na naknadu od voditelja obrade ili izvršitelja obrade za pretrpljenu štetu.

2. Svaki voditelj obrade koji je uključen u obradu odgovoran je za štetu prouzročenu obradom kojom se krši ova Uredba. […].

3. Voditelj obrade ili izvršitelj obrade izuzet je od odgovornosti na temelju stavka 2. ako dokaže da nije ni na koji način odgovoran za događaj koji je prouzročio štetu”.

II. Činjenice, postupak i prethodna pitanja

6. Bugarski mediji objavili su 15. srpnja 2019. vijest da je došlo do neovlaštenog pristupa informatičkom sustavu Nacionalne agencije za prihodite (Nacionalna agencija za javne prihode, u daljnjem tekstu: NAP [3]) i da su na internetu objavljene razne informacije o porezima i socijalnom osiguranju milijuna pojedinaca, kako bugarskih državljana, tako i stranaca.

7. Nakon toga, brojne osobe, među kojima i VB, tužitelj iz glavnog postupka, podnijele su tužbu protiv NAP-a radi naknade nematerijalne štete.

8. U ovom slučaju tužitelj iz glavnog postupka pokrenuo je postupak pred Administrativen sadom Sofia-grad (Upravni sud u Sofiji, Bugarska, u daljnjem tekstu: ASSG), pri čemu je tvrdio da je NAP povrijedio nacionalna pravna pravila, kao i obvezu da u svojstvu voditelja obrade obrađuje osobne podatke na način koji „jamči odgovarajuću sigurnost” primjenom odgovarajućih tehničkih i organizacijskih mjera u skladu s člancima 24. i 32. Uredbe 2016/679. Tužitelj je zatim naveo da je pretrpio nematerijalnu štetu koja se ogleda u zabrinutosti i bojazni od buduće zlouporabe njegovih osobnih podataka.

9. Druga strana naglasila je pak da od tužitelja iz glavnog postupka nije zaprimila nijedan zahtjev u kojem se navodi kojim se točno osobnim podacima pristupilo. Osim toga, nakon vijesti o napadu druga strana sazvala je sastanke sa stručnjacima kako bi se zaštitila prava i interesi građana. NAP je također smatrao da ne postoji uzročno-posljedična veza između kibernetičkog napada i istaknute navodne nematerijalne štete jer je agencija provela sve sustave upravljanja procesima i sustave upravljanja sigurnošću informacija u skladu s međunarodnim normama koje su na snazi u tom području.

10. Prvostupanjski sud, odnosno ASSG, odbio je zahtjev, pri čemu je smatrao da agencija nije odgovorna za širenje podataka, da je na tužitelju teret dokaza u pogledu toga jesu li provedene mjere bile odgovarajuće te, naposljetku, da se ne može dodijeliti naknada za nematerijalnu štetu.

[3] NAP je voditelj obrade u smislu članka 4. točke 7. Uredbe. U skladu s nacionalnim pravom, NAP je posebno osposobljeno upravno tijelo, podređeno ministru financija, koje je nadležno za utvrđivanje, osiguravanje i naplatu javnih financija te za utvrđivanje, osiguravanje i naplatu javnih i privatnih zakonom određenih državnih potraživanja. Pri izvršavanju prenesenih mu ovlasti to tijelo obrađuje osobne podatke.

11. Protiv prvostupanjske presude zatim je podnesena žalba Vrhoven administrativen sadu (Vrhovni upravni sud, Bugarska). U okviru iznesenih navoda tužitelj iz glavnog postupka naglasio je da prvostupanjski sud nije pravilno raspodijelio teret dokaza u pogledu činjenice da nisu provedene sigurnosne mjere. Ni nematerijalna šteta ne bi trebala biti predmet tereta dokaza, s obzirom na to da je riječ o stvarnoj, a ne samo mogućoj nematerijalnoj šteti.

12. S druge strane, NAP je ponovio da je u svojstvu voditelja obrade proveo potrebne tehničke i organizacijske mjere te je osporavao da postoji dokaz o nastanku stvarne nematerijalne štete. Naime, zabrinutost i bojazan duševna su stanja za koja se ne može odrediti naknada štete.

13. Sud koji je uputio zahtjev utvrdio je da su pojedinačni postupci koje su oštećenici zasebno pokrenuli protiv NAP-a radi naknade nematerijalne štete imali različite ishode.

14. U tim je okolnostima sud koji je uputio zahtjev prekinuo postupak i uputio Sudu sljedeća prethodna pitanja:

„1. Treba li članak 24. i članak 32. Uredbe (EU) 2016/679 [Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka)] tumačiti na način da je za pretpostavku da poduzete tehničke i organizacijske mjere nisu odgovarajuće dovoljno ako neovlašteno otkrivanje osobnih podataka ili neovlašteni pristup osobnim podacima u smislu članka 4. točke 12. Uredbe (EU) 2016/679 počine osobe koje nisu osoblje uprave voditelja obrade i koje ne podliježu njegovoj kontroli?

2. U slučaju niječnog odgovora na prvo pitanje, koji bi predmet i opseg trebao imati sudski nadzor zakonitosti prilikom ispitivanja jesu li tehničke i organizacijske mjere koje je voditelj obrade proveo u skladu s člankom 32. Uredbe (EU) 2016/679 odgovarajuće?

3. U slučaju niječnog odgovora na prvo pitanje, treba li načelo pouzdanosti u skladu s člankom 5. stavkom 2. i člankom 24. u vezi s uvodnom izjavom 74. Uredbe (EU) 2016/679 tumačiti na način da je u sudskom postupku u skladu s člankom 82. stavkom 1. Uredbe (EU) 2016/679 na voditelju obrade teret dokaza da su u skladu s člankom 32. Uredbe provedene tehničke i organizacijske mjere odgovarajuće? Može li se pribavljanje nalaza i mišljenja vještaka smatrati potrebnim i dostatnim dokazom za utvrđenje jesu li tehničke i organizacijske mjere koje je proveo voditelj obrade bile odgovarajuće u slučaju poput onog o kojem je riječ u ovom predmetu ako su neovlašteni pristup osobnim podacima i neovlašteno otkrivanje osobnih podataka posljedica ‚hakerskog napada'?

4. Treba li članak 82. stavak 3. Uredbe (EU) 2016/679 tumačiti na način da neovlašteno otkrivanje osobnih podataka ili neovlašteni pristup osobnim podacima u smislu članka 4. točke 12. Uredbe (EU) 2016/679 kao u ovom predmetu, uslijed ‚hakerskog napada' koji su počinile osobe koje nisu osoblje uprave voditelja obrade i ne podliježu njegovoj kontroli, predstavlja događaj za koji voditelj obrade ni u kojem pogledu nije odgovoran i koji daje pravo na izuzimanje od odgovornosti?

5. Treba li članak 82. stavke 1. i 2. u vezi s uvodnim izjavama 85. i 146. Uredbe (EU) 2016/679 tumačiti na način da su u slučaju poput onog o kojem je riječ u ovom predmetu u kojem postoji povreda osobnih podataka, koja se ogleda u neovlaštenom pristupu osobnim podacima i širenju osobnih podataka uslijed ‚hakerskog napada', zabrinutost, bojazan i strahovi koje je ispitanik pretrpio zbog moguće buduće zlouporabe osobnih podataka već

sami po sebi obuhvaćeni pojmom nematerijalne štete koji se treba široko tumačiti i daju pravo na naknadu štete, ako takva zlouporaba nije utvrđena i/ili tom ispitaniku nije nastala nikakva daljnja šteta?"

III. Pravna analiza

A. Uvodna razmatranja

15. Ovaj predmet odnosi se na zanimljiva pitanja koja se u jednom dijelu do sada nisu razmatrala, a odnose se na tumačenje raznih odredbi Uredbe [4].

16. Svih je pet prethodnih pitanja povezano s istim problemom koji se odnosi na uvjete za naknadu nematerijalne štete osobi čiji su osobni podaci, kojima je raspolagala javnopravna agencija, objavljeni na internetu nakon hakerskog napada.

17. Radi praktičnosti u izlaganju predložit ću sažete zasebne odgovore na sva prethodna pitanja iz rješenja kojim se upućuje zahtjev za prethodnu odluku, iako sam svjestan da postoje određena konceptualna preklapanja, s obzirom na to da se prvim četirima prethodnim pitanjima nastoje utvrditi uvjeti pod kojima je voditelj obrade odgovoran za povredu odredbi Uredbe [5], dok se peto prethodno pitanje odnosi, konkretnije, na pojam nematerijalne štete u svrhu naknade štete [6].

18. Ističem da su u pogledu članka 82. Uredbe pred Sudom trenutačno u tijeku razni postupci i da je u jednom od tih postupaka već izneseno mišljenje nezavisnog odvjetnika koje ću uzeti u obzir u ovoj analizi [7].

19. Prije nego što se ispitaju postavljena pitanja smatram da su potrebna određena uvodna razmatranja o načelima i ciljevima Uredbe koja će biti korisna za odgovor na pojedinačna prethodna pitanja.

20. Člankom 24. Uredbe općenito se utvrđuje obveza voditelja obrade da provodi odgovarajuće tehničke i organizacijske mjere kako bi osigurao i mogao dokazati da se obrada osobnih podataka provodi u skladu sa samom Uredbom, dok se člankom 32. ta obveza konkretnije određuje s obzirom na sigurnost obrade. Člancima 24. i 32. konkretnije se određuje ono što se već predviđa člankom 5. stavkom 2., kojim se upravo među „načela obrade osobnih podataka" uvodi „načelo

[4] Članak 5. stavak 2. (koji se odnosi na načelo odgovornosti svakog voditelja obrade osobnih podataka), članak 24. (koji se odnosi na mjere koje je taj voditelj obrade dužan provesti kako bi osigurao da se obrada provodi u skladu s tom uredbom), članak 32. (koji se odnosi na navedenu obvezu osobito s obzirom na sigurnost obrade) i članak 82. stavci 1. do 3. (koji se odnosi na naknadu štete koja proizlazi iz povrede navedene uredbe i na mogućnost za voditelja obrade da provodi mjere kojima se osigurava poštovanje te uredbe), kao i uvodne izjave 74., 85. i 146. koje su povezane s navedenim člancima.

[5] (a) prvim prethodnim pitanjem nastoji se utvrditi može li se samo na temelju činjenice da je došlo do povrede sustava zaključiti da predviđene mjere nisu odgovarajuće; (b) drugo prethodno pitanje odnosi se na proširenje sudskog nadzora nad time jesu li navedene mjere odgovarajuće, (c) treće prethodno pitanje odnosi se na teret dokaza u pogledu same činjenice jesu li navedene mjere odgovarajuće i na neke tehničke metode prikupljanja dokaza; (d) četvrto prethodno pitanje odnosi se na to je li za izuzimanje od odgovornosti relevantna okolnost da je riječ o napadu na sustav izvana.

[6] Kad je riječ o odredbama Uredbe na koje se upućuje, prva tri pitanja odnose se na aspekte odgovornosti voditelja obrade s obzirom na to jesu li mjere koje treba provesti odgovarajuće (članci 5., 24. i 32.), a četvrto i peto pitanje odnose se na uvjete za izuzimanje od odgovornosti i na pojam nadoknadive nematerijalne štete (članak 82.)

[7] Vidjeti mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone u predmetu Österreichische Post (Nematerijalna šteta povezana s obradom osobnih podataka) (C-300/21, EU:C:2022:756).

pouzdanosti". To načelo logički slijedi iz „načela cjelovitosti i povjerljivosti" predviđenog člankom 5. stavkom 1. točkom (f) i služi kao dopuna tom načelu, a oba ta načela treba tumačiti s obzirom na pristup koji je zasnovan na riziku na kojem se temelji Uredba.

21. Načelo pouzdanosti jedan je od temelja Uredbe i jedna od njezinih najznačajnijih inovacija. Tim se načelom voditelju obrade pripisuje odgovornost za provedbu proaktivnih mjera kako bi osigurao i mogao dokazati da se obrada provodi u skladu s Uredbom [8].

22. U pravnoj teoriji bila je riječ o stvarnoj i pravoj kulturološkoj promjeni kao posljedici „globalnog dosega obveze odgovornosti" [9]. Do izuzimanja voditelja obrade od odgovornosti zato što djeluje u skladu (*compliant*) s propisima o zaštiti podataka ne dovodi toliko formalno poštovanje pravne obveze ili posebne mjere, nego cjelokupna primijenjena poslovna strategija.

23. Tehničke i organizacijske mjere koje se zahtijevaju načelom pouzdanosti trebaju biti „odgovarajuće" s obzirom na čimbenike navedene u članku 24., odnosno: prirodu, opseg, kontekst i svrhe obrade, kao i vjerojatnosti i ozbiljnost rizika za prava i slobode pojedinaca.

24. Člankom 24. stoga se nalaže da mjere trebaju biti odgovarajuće kako bi se moglo dokazati da je obrada usklađena s načelima i odredbama Uredbe.

25. Načelo pouzdanosti prenosi se pak člankom 32. na konkretne mjere koje treba provesti kako bi se osigurala „odgovarajuć[a] razin[a] sigurnosti s obzirom na rizik". Prilikom navedenog prenošenja tim se člankom već propisanim čimbenicima koje treba uzeti u obzir prilikom predviđanja tehničkih i organizacijskih mjera dodaju i najnovija dostignuća i troškovi provedbe.

26. Pojam „odgovarajuće" zahtijeva da rješenja koja se donose kako bi se osigurali informatički sustavi dosegnu određenu razinu prihvatljivosti i u pogledu tehničkih zahtjeva (relevantnost mjera) i u pogledu zahtjeva kvalitete (učinkovitost zaštite). Kako bi se osiguralo poštovanje načela nužnosti, relevantnosti i proporcionalnosti, obrada treba biti ne samo prikladna za postizanje ciljeva koji se namjeravaju postići, nego obradom te ciljeve treba i ispuniti. Presudnu ulogu u toj logici ima načelo smanjenja količine podataka na temelju kojeg sve faze obrade podataka trebaju kontinuirano težiti tomu da se sigurnosni rizici svedu na najmanju moguću mjeru [10].

27. Cijela Uredba temelji se na sprečavanju rizika i na pouzdanosti voditelja obrade i, stoga, na teleološkom pristupu kojim se sa stajališta učinkovitosti nastoji postići najbolji mogući rezultat, odnosno na pristupu koji je daleko od formalističke logike povezane s običnom obvezom pridržavanja posebnih postupaka kako bi se moglo osloboditi od odgovornosti [11].

[8] C. Docksey, *Article 24. Responsibility of the controller*, objavljeno u C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press*, 2020., str. 561. Načela i obveze iz propisa u području zaštite podataka trebala bi prožimati kulturno tkivo organizacija na svim razinama te ih ne bi trebalo smatrati nizom pravnih zahtjeva koje treba ispuniti pravni odjel organizacije.

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

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

[11] Kao što će se to pokazati u nastavku, zbog toga na prvo i četvrto prethodno pitanje treba odgovoriti niječno. Iz odredbi Uredbe ne može se izvesti nikakav automatizam: sama činjenica da je došlo do otkrivanja osobnih podataka nije dovoljna kako bi se smatralo da provedene tehničke i organizacijske mjere nisu odgovarajuće, ali ni okolnost da je do samog otkrivanja došlo zbog djelovanja osoba koje se nalaze izvan organizacije voditelja obrade i izvan njegova područja kontrole nije dovoljna kako bi se voditelj obrade izuzeo od odgovornosti.

28. Članak 24. ne sadržava taksativan popis „odgovarajućih” mjera i stoga treba provesti ocjenu u svakom slučaju zasebno. To je u skladu s filozofijom Uredbe iz koje proizlazi da se prednost daje tomu da se postupci koje treba primijeniti odabiru na temelju pažljive ocjene posebne situacije kako bi bili što učinkovitiji [12].

B. Prvo prethodno pitanje

29. Sud koji je uputio zahtjev prvim pitanjem u biti nastoji doznati treba li članke 24. i 32. Uredbe tumačiti na način da je činjenica da je nastupila „povreda osobnih podataka”, kako se definira člankom 4. točkom 12., sama po sebi dovoljna kako bi se zaključilo da tehničke i organizacijske mjere koje je poduzeo voditelj obrade nisu bile „odgovarajuće” kako bi se osigurala zaštita podataka.

30. Iz teksta članaka 24. i 32. Uredbe proizlazi da voditelj obrade prilikom odabira tehničkih i organizacijskih mjere koje je dužan provesti kako bi osigurao usklađenost sa samom Uredbom treba uzeti u obzir niz spomenutih čimbenika ocjene koji se navode u tim člancima.

31. Kad je riječ o utvrđivanju najprikladnijih mjera s obzirom na njegovu posebnu situaciju, voditelj obrade raspolaže određenim manevarskim prostorom, ali taj odabir u svakom slučaju podliježe eventualnom sudskom nadzoru usklađenosti primijenjenih mjera sa svim obvezama i ciljevima same Uredbe.

32. Konkretno, kad je riječ o sigurnosnim mjerama, člankom 32. stavkom 1. voditelju obrade nalaže se da uzme u obzir „najnovija dostignuća”. To podrazumijeva ograničavanje tehnološke razine mjera koje treba provesti na ono što je razumno moguće u trenutku njihove provedbe, odnosno prikladnost mjere da spriječi rizik treba odgovarati rješenjima koja se nude u skladu s trenutačnim znanstvenim, tehničkim, tehnološkim i istraživačkim saznanjima, također s obzirom na troškove provedbe, kao što će se to vidjeti u nastavku.

33. Pojedine mjere mogu biti „odgovarajuće” u nekom određenom trenutku i, neovisno o tome, mogu ih zaobići kiberkriminalci koji upotrebljavaju vrlo sofisticirana sredstva kojima se mogu probiti i sigurnosne mjere koje su u skladu s najnovijim dostignućima.

34. Međutim, čini se da nije logično smatrati da je namjera zakonodavca Unije bila nametnuti voditelju obrade obvezu da spriječi svaku povredu osobnih podataka, neovisno o savjesnosti prilikom predviđanja sigurnosnih mjera [13].

35. Kao što je to navedeno, Uredba se temelji na logici koja je daleko od automatizama i njome se zahtijeva izrazita pouzdanost voditelja obrade koja, međutim, ne može biti takva da se voditelju obrade onemogući dokazivanje da je pravilno ispunio obveze koje mu se nalažu.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019., str. 201. Zakonodavac Unije stoga je uklonio koncept sigurnosti obrade koji se temelji na postojanju unaprijed utvrđenih sigurnosnih mjera i donio je vlastitu metodologiju međunarodnih standarda upravljanja informacijskim sustavima koja se temelji na riziku: tom se metodologijom predviđa utvrđivanje mjera za ublažavanje rizika koje su neovisne o unaprijed sastavljenim kontrolnim listama koje se mogu općenito primjenjivati. Zbog toga je potrebno pribjeći smjernicama i međunarodnim standardima. Rezultat takve ocjene rizika stoga je obvezujuć od trenutka u kojem je organizacija donijela odluke s ciljem ublažavanja utvrđenih rizika, pri čemu postaje odgovorna (*accountable*).

[13] Nedvosmislena namjera koncepta „odgovarajuće” jest da se ne pridaje važnost svim tehničkim i organizacijskim mjerama koje su teoretski moguće. Vidjeti u tom smislu M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, objavljeno u V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019., str. 1059.

36. Osim toga, člankom 32. stavkom 1. predviđa se da treba uzeti u obzir, kao što je navedeno, „troškove provedbe" tehničkih i organizacijskih mjera o kojima je riječ. Iz toga proizlazi da se ocjena pitanja jesu li takve mjere odgovarajuće treba temeljiti na odvagivanju interesa ispitanika, koji uglavnom teže višem stupnju zaštite, s gospodarskim interesima i tehnološkim mogućnostima voditelja obrade, koji ponekad naginju nižem stupnju zaštite. To odvagivanje treba poštovati zahtjeve općeg načela proporcionalnosti.

37. U tom pogledu valja dodatno napomenuti da, sa stajališta sustavnog tumačenja, zakonodavac predviđa mogućnost nastanka povreda sustava te se člankom 32. stavkom 1. točkom (c) u predložene mjere uključuje sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa tim podacima u slučaju fizičkog ili tehničkog incidenta. Ne bi imalo smisla predvidjeti tu sposobnost kao jednu od sigurnosnih mjera kojima se osigurava odgovarajuća razina sigurnosti s obzirom na rizik ako bi se smatralo da povreda sustava sama po sebi predstavlja dokaz da same mjere nisu odgovarajuće.

C. Drugo prethodno pitanje

38. Drugim pitanjem sud koji je uputio zahtjev u biti nastoji doznati koji bi predmet i opseg trebao imati sudski nadzor prilikom ispitivanja jesu li tehničke i organizacijske mjere koje je voditelj obrade proveo u skladu s člankom 32. Uredbe odgovarajuće.

39. Budući da su slučajevi koji mogu nastati u praksi raznoliki, kao što je već navedeno, Uredbom se ne utvrđuju obvezujuće odredbe za određivanje tehničkih i organizacijskih mjera koje voditelj obrade treba provesti kako bi ispunio zahtjeve iz same Uredbe. Pitanje jesu li provedene mjere odgovarajuće stoga treba ocijeniti konkretno, pri čemu se provjerava je li se posebnim mjerama opravdano mogao spriječiti rizik i jesu li se mogli ublažiti negativni učinci povrede.

40. Ako je točno da su odabir i provedba tih mjera obuhvaćeni subjektivnom ocjenom voditelja obrade, s obzirom na to da su mjere navedene u Uredbi samo primjeri, ispitivanje koje provodi sud ne može se ograničiti na to da se kontrolira poštuje li voditelj obrade obveze koje proizlaze iz članaka 24. i 32., odnosno na to da se kontrolira je li (formalno) predvidio određene tehničke i organizacijske mjere. Taj sud treba provesti konkretnu analizu sadržaja tih mjera, načina na koji se primjenjuju i njihovih učinaka u praksi na temelju dokaza kojima raspolaže i okolnosti konkretnog slučaja. Kao što je to točno napomenula portugalska vlada, „čini se da je način na koji je ispunio svoje obveze neodvojiv od sadržaja provedenih mjera te je voditelj obrade, kako bi dokazao da je uzimajući u obzir posebnu obradu podataka (njezinu prirodu, opseg, kontekst i svrhe), najnovija dostignuća dostupnih tehnologija i njihov trošak te rizike za prava i slobode građana, proveo sve potrebne i prikladne mjere radi osiguravanja odgovarajuće razine sigurnosti s obzirom na povezani rizik" [14].

41. U okviru sudskog nadzora trebat će stoga uzeti u obzir sve čimbenike sadržane u člancima 24. i 32. u kojima se, kao što je navedeno, nabraja niz kriterija za ocjenu jesu li mjere odgovarajuće i pružaju primjeri mjera koje se mogu smatrati odgovarajućima. Osim toga, kao što su to istaknule Komisija i sve države članice koje su podnijele očitovanja u pogledu drugog pitanja, u članku 32. stavcima 1. do 3. naglašava se potreba da se „osigur[a] odgovarajuć[a] razin[a] sigurnosti s obzirom na rizik", pri čemu se navode i drugi čimbenici koji su relevantni u tu svrhu, poput mogućnosti da voditelj obrade donese odobreni kodeks ponašanja ili odobreni sustav certificiranja, kao što se to predviđa člankom 40. odnosno člankom 42. Uredbe.

[14] Točka 31. pisanih očitovanja

42. Donošenje kodeksa ponašanja ili sustava certificiranja može pružiti koristan element ocjene za potrebe ispunjenja obveze tereta dokaza i povezanog sudskog nadzora. Međutim, valja pojasniti da za voditelja obrade nije dovoljno da poštuje kodeks ponašanja, nego je na njemu teret da dokaže da je konkretno proveo mjere koje se predviđaju tim kodeksom, u skladu s načelom pouzdanosti. Certificiranje pak predstavlja „samo po sebi dokaz da je obrada koja se provodi u skladu s Uredbom, iako je moguće da se to u praksi opovrgne” [15].

43. Na kraju valja napomenuti da na temelju članka 24. stavka 1. te mjere treba prema potrebi preispitivati i ažurirati. To također treba ocijeniti nacionalni sud. Naime, člankom 32. stavkom 1. Uredbe [16] voditelju obrade nalaže se obveza stalne kontrole i nadzora, prije i nakon aktivnosti obrade, ali i obveza održavanja i mogućeg ažuriranja provedenih mjera, u svrhu sprečavanja povreda i eventualnog ograničivanja učinaka povreda.

44. Međutim, sklon sam isključiti mogućnost da će sljedeća presuda sadržavati popis bitnih elemenata kao što je to popis koji je predložila portugalska vlada [17]. To bi moglo stvoriti priliku za oprečna tumačenja, s obzirom na to da je očito da popis nikad ne može biti taksativan.

D. Treće prethodno pitanje

45. Prvim dijelom trećeg pitanja sud koji je uputio zahtjev u biti traži od Suda da utvrdi, uzimajući u obzir načelo pouzdanosti u skladu s člankom 5. stavkom 2. i člankom 24. u vezi s uvodnom izjavom 74. [18] Uredbe, je li u okviru tužbe za naknadu štete u skladu s člankom 82. na voditelju obrade osobnih podataka teret dokaza da su u skladu s člankom 32. provedene tehničke i organizacijske mjere odgovarajuće.

46. Prethodna razmatranja omogućuju mi da na to pitanje sažeto odgovorim potvrdno.

47. Naime, tekst zakona, kontekst i ciljevi Uredbe nedvosmisleno idu u prilog tomu da je teret dokaza na voditelju obrade.

48. Iz teksta raznih odredbi Uredbe proizlazi da voditelj obrade treba „biti u mogućnosti” ili treba „moći” „dokazati” da je poštovao obveze predviđene Uredbom i, konkretno, da je u tu svrhu proveo odgovarajuće mjere, kao što se to navodi u uvodnoj izjavi 74., članku 5. stavku 2. i

[15] M. Gambini, *Responsabilità*, *op. cit.*, str. 1067. Posjedovanje certifikata stoga dovodi do prebacivanja tereta dokaza u korist voditelja obrade kojem se olakšava dokazivanje da je djelovao poštujući obveze iz Uredbe.

[16] U čijoj se točki (d) izričito određuje da se ocjena jesu li mjere odgovarajuće proširuje na učinkovitost mjera koje se provode i koje redovno treba testirati, preispitivati i ocjenjivati i na početku i periodično kako bi se osigurala stvarna sigurnost svih vrsta obrade, neovisno o njihovu stupnju rizika i, nadalje, u čijoj se točki (c) izričito predviđa da tehničke i organizacijske mjere koje se provode trebaju moći pravodobno ponovno uspostaviti dostupnost osobnih podataka i pristup tim podacima u slučaju fizičkog ili tehničkog incidenta. Vidjeti M. Gambini, Responsabilità, *op. cit.*, str. 1064. i 1065.

[17] Točka 30. pisanih očitovanja: „na voditelju je obrade da dokaže kako je ocijenio sve čimbenike i okolnosti koji se odnose na obradu o kojoj je riječ i, konkretno, rezultat provedene analize rizika, utvrđene rizike, konkretne mjere kako bi se ublažili ti rizici, opravdanje odabranih mogućnosti s obzirom na tehnološka rješenja koja su dostupna na tržištu, učinkovitost mjera, povezanost tehničkih i organizacijskih mjera, obuku osoblja koje obrađuje podatke, postojanje eksternalizacije postupaka obrade podataka, uključujući razvoj i održavanje informatičke tehnologije, i postojanje kontrole koju provodi voditelj obrade te preciznih uputa koje se osobama zaduženima za obradu u skladu s člankom 28. OUZP-a daju u pogledu obrade osobnih podataka koju provode, način na koji je ocijenjena potporna infrastruktura komunikacijskih i informacijskih sustava te kako je klasificiran stupanj rizika za prava i slobode ispitanika”.

[18] U skladu s uvodnom izjavom 74.: „Trebalo bi uspostaviti dužnost i odgovornosti voditelja obrade za svaku obradu osobnih podataka koju provede sâm voditelj obrade ili netko drugi u ime voditelja obrade. Osobito, voditelj obrade trebao bi imati obvezu provođenja odgovarajućih i djelotvornih mjera te biti u mogućnosti dokazati usklađenost aktivnosti obrade s ovom Uredbom uključujući i djelotvornost mjera. Tim bi mjerama u obzir trebalo uzeti prirodu, opseg, kontekst i svrhe obrade te rizik za prava i slobode pojedinaca”.

članku 24. stavku 1. Kao što to ističe portugalska vlada, u navedenoj uvodnoj izjavi 74. pojašnjava se da teret dokaza koji na taj način ima voditelj obrade treba obuhvaćati i dokaz „djelotvornost[i] mjera" o kojima je riječ.

49. Čini mi se da to doslovno tumačenje podupiru i sljedeća praktična i teleološka razmatranja.

50. Kad je riječ o raspodjeli tereta dokaza, u okviru tužbe za naknadu štete koja se temelji na članku 82., ispitanik koji je podnio tužbu protiv voditelja obrade treba dokazati, kao prvo, da je došlo do povrede Uredbe, kao drugo, da je pretrpio štetu i, kao treće, da postoji uzročno-posljedična veza između prethodnih dvaju elementa, kao što se to navodi u svim pisanim očitovanjima koja se odnose na peto prethodno pitanje. Riječ je o trima kumulativnim uvjetima, kao što to proizlazi i iz ustaljene sudske prakse Suda i Općeg suda u kontekstu izvanugovorne odgovornosti Unije [19].

51. Međutim, smatram da se obveza dokazivanja postojanja povrede Uredbe koju ima tužitelj ne može proširiti sve do toga da se zahtijeva dokazivanje da tehničke i organizacijske mjere koje provodi voditelj obrade nisu odgovarajuće u skladu s člancima 24. i 32.

52. Kao što je to naglasila Komisija, podnošenje takvih dokaza u praksi je često gotovo nemoguće, s obzirom na to da ispitanici obično nemaju ni dostatna znanja kako bi mogli analizirati te mjere niti imaju pristup svim informacijama koje posjeduje sporni voditelj obrade, posebno kad je riječ o metodama koje se primjenjuju kako bi se osigurala sigurnost te obrade. Osim toga, voditelj obrade može ponekad tvrditi da se njegovo odbijanje otkrivanja tih činjenica ispitanicama temelji na zakonitom razlogu neobjavljivanja vlastitih internih poslova ili, također, elemenata koji su obuhvaćeni poslovnom tajnom, i to, među ostalim, upravo zbog sigurnosnih razloga.

53. Stoga, kad bi se smatralo da je teret dokaza na ispitaniku, to bi u praksi rezultiralo time da bi pravo na tužbu predviđeno člankom 82. stavkom 1. bilo lišeno velikog dijela svojeg dosega. Smatram da navedeno nije u skladu s namjerama zakonodavca Unije koji je donošenjem te uredbe nastojao ojačati prava ispitanika i obveze izvršitelja obrade u odnosu na one iz Direktive 95/46 koju je Uredba zamijenila. Stoga je logičnije i pravno održivo da je voditelj obrade taj koji u okviru svoje obrane od tužbe za naknadu štete treba dokazati da je poštovao obveze koje proizlaze iz članaka 24. i 32. te uredbe provedbom mjera koje su zaista odgovarajuće.

54. Drugim dijelom trećeg pitanja sud koji je uputio zahtjev u biti pita Sud može li se pribavljanje nalaza i mišljenja vještaka smatrati potrebnim i dostatnim dokazom za utvrđenje jesu li tehničke i organizacijske mjere koje je proveo voditelj obrade osobnih podataka bile odgovarajuće u slučaju u kojem su neovlašteni pristup osobnim podacima i neovlašteno otkrivanje osobnih podataka posljedica hakerskog napada.

55. Kao što su to (u biti) naglasile i bugarska i talijanska vlada, Irska i Komisija, smatram da se odgovor na ta pitanja treba temeljiti na našoj ustaljenoj sudskoj praksi u skladu s kojom, na temelju načela postupovne autonomije, u slučaju kad ne postoje pravila prava Unije u tom području, nacionalnim pravnim sustavom svake države članice treba urediti postupovna pravila sudskih postupaka čiji je cilj zaštita prava pojedinaca, ali pod uvjetom da ta pravna pravila u

[19] Vidjeti konkretno presude Suda od 5. rujna 2019., Europska unija/Guardian Europe i Guardian Europe/Europska unija (C-447/17 P i C-479/17 P, EU:C:2019:672, t. 147.) i od 28. listopada 2021., Vialto Consulting protiv Komisije (C-650/19 P, EU:C:2021:879, t. 138.), kao i presude Općeg suda od 13. siječnja 2021., Helbert/EUIPO(T-548/18, EU:T:2021:4, t. 116.) i od 29. rujna 2021., Kočner/Europol (T-528/20, neobjavljena, EU:T:2021:631, t. 61.), u kojoj se podsjeća da trebaju biti ispunjena tri uvjeta, odnosno „da je postupanje koje se pripisuje instituciji Unije protupravno, da je šteta stvarna i da postoji uzročno-posljedična veza između postupanja te institucije i štete na koju se poziva".

situacijama uređenima pravom Unije nisu nepovoljnija od onih kojima se uređuju slične situacije koje podliježu nacionalnom pravu (načelo ekvivalentnosti) te da u praksi ne onemogućuju ili pretjerano ne otežavaju ostvarivanje prava dodijeljenih pravom Unije (načelo djelotvornosti).

56. U ovom slučaju napominjem da Uredba ne sadržava nijednu odredbu čiji je cilj utvrditi prihvatljive metode dokazivanja i njihovu dokaznu vrijednost, osobito u pogledu istražnih radnji (poput vještačenja) koje nacionalni sudovi mogu ili moraju naložiti kako bi ocijenili je li voditelj obrade osobnih podataka proveo mjere koje su odgovarajuće u smislu te uredbe. Stoga smatram da, u slučaju da u tom području ne postoje ujednačena pravna pravila, nacionalnim pravnim sustavom svake države članice treba odrediti ta postupovna pravila, ne dovodeći u pitanje poštovanje načela ekvivalentnosti i djelotvornosti.

57. Navedeno „načelo djelotvornosti", koje podrazumijeva da neovisan sud treba provesti nepristranu ocjenu, može se dovesti u pitanje ako se pridjev „dostatno" tumači u smislu za koji mi se čini da mu pridaje sud koji je uputio zahtjev, odnosno na način da se iz mišljenja vještaka može automatski zaključiti da su mjere koje provodi voditelj obrade odgovarajuće [20].

E. Četvrto prethodno pitanje

58. Četvrtim pitanjem sud koji je uputio zahtjev u biti nastoji doznati treba li članak 82. stavak 3. Uredbe tumačiti na način da slučaj povrede te uredbe (koji se kao u ovom predmetu odnosi na „neovlašteno otkrivanje" ili „neovlašteni pristup" osobnim podacima u smislu članka 4. točke 12.), od strane osoba koje nisu osoblje voditelja obrade i ne podliježu njegovoj kontroli, predstavlja događaj za koji voditelj obrade ni u kojem pogledu nije odgovoran i stoga predstavlja razlog da se izuzme od svoje odgovornosti u skladu s člankom 82. stavkom 3.

59. Odgovor na pitanje izravno proizlazi iz onoga što se navodi u pogledu opće filozofije Uredbe: ne predviđa se nikakav automatizam i stoga sama činjenica da je do neovlaštenog otkrivanja ili neovlaštenog pristupa osobnim podacima došlo zbog osoba koje ne podliježu kontroli voditelja obrade ne izuzima voditelja obrade od odgovornosti.

60. Kao prvo, s obzirom na tekst, valja napomenuti da se ni člankom 82. stavkom 3. ni uvodnom izjavom 146. ne utvrđuju posebni uvjeti koji se mogu ispuniti kako bi se voditelja obrada izuzelo od odgovornosti, osim ako ne dokaže da „nije ni na koji način odgovoran za događaj koji je prouzročio štetu". S jedne strane, iz tog teksta proizlazi da se voditelj obrade može izuzeti od odgovornosti samo ako dokaže da nije odgovoran za događaj koji je prouzročio štetu o kojoj je riječ i, s druge strane, da je dokazni standard koji se zahtijeva tom odredbom visok, s obzirom na to da se upotrebljava izraz „ni na koji način", kao što je to naglasila Komisija [21].

61. O sustavu odgovornosti predviđenom člankom 82. i, općenitije, cijelom Uredbom, opsežno se raspravljalo u pravnoj teoriji raznih država članica. Naime, taj sustav sadržava tradicionalne elemente svojstvene izvanugovornoj odgovornosti, ali i elemente koje ga u strukturi odredbi približavaju ugovornoj odgovornosti ili čak nekoj vrsti objektivne odgovornosti zbog toga što je

[20] Točka 39. pisanih očitovanja

[21] U skladu s ustaljenom sudskom praksom Suda, prema kojoj iznimke od općeg pravnog pravila treba usko tumačiti, eventualno izuzimanje od odgovornosti predviđeno člankom 82. stavkom 3. treba usko tumačiti. Vidjeti po analogiji presude od 15. listopada 2020., Association française des usagers de banques (C-778/18, EU:C:2020:831, t. 53.) i od 5. travnja 2022., Commissioner of An Garda Síochána i drugi (C-140/20, EU:C:2022:258, t. 40.).

aktivnost obrade podataka po svojoj prirodi opasna. Ovo nije postupak u kojem treba opravdati spomenutu raspravu, ali smatram da se ne čini da se člankom 82. određuje sustav objektivne odgovornosti [22].

62. Šteta zbog povrede osobnih podataka može nastati kao posljedica toga što namjerno nisu provedene razumne tehničke i organizacijske mjere, odnosno mjere koje su u svakom slučaju prikladne za izbjegavanje štete, uzimajući u obzir rizike za prava i slobode pojedinaca povezane s aktivnostima obrade. Ti rizici dovode do toga da obveza sprečavanja i izbjegavanja štete postaje stroža, pri čemu se proširuje obveza dužne pažnje koju ima voditelj obrade. Stoga se iz usklađenog tumačenja obveza u pogledu postupanja koje imaju voditelji obrade i predviđanja oslobađajućeg dokaza koji treba podnijeti počinitelj štete može izvesti argumenti u prilog priznavanju toga da odgovornost zbog nezakonite obrade osobnih podataka određena člankom 82. Uredbe ima prirodu strože odgovornosti na temelju pretpostavljene krivnje [23].

63. Iz toga proizlazi da voditelj obrade ima mogućnost podnijeti oslobađajući dokaz (koja nije dopuštena u slučaju objektivne odgovornosti). Kad je riječ o raspodjeli tereta dokaza, člankom 82. stavkom 3. Uredbe određuje se sustav koji je povoljan za oštećenika, pri čemu se propisuje oblik prebacivanja tereta dokaza u pogledu krivnje počinitelja štete [24], koji je potpuno usklađen s navedenim prebacivanjem tereta dokaza u pogledu toga jesu li provedene mjere odgovarajuće. Na taj način zakonodavac pokazuje da je svjestan opasnosti koje proizlaze iz prihvaćanja drukčije raspodjele tereta dokaza koja bi, u slučaju da je teret dokaza krivnje počinitelja štete na fizičkoj osobi, odnosno oštećeniku, dovela do toga da se ta osoba nalazi u previše nepovoljnom položaju, a time bi zapravo dovela u pitanje i funkcioniranje zaštite u obliku naknade štete u okviru pravnih pravila povezanih s uporabom novih tehnologija. Naime, ispitaniku bi moglo biti osobito teško utvrditi postupke koji su doveli do nastanka štete i imati pristup tim postupcima te, posljedično, dokazati krivnju voditelja obrade. Suprotno tomu, voditelj obrade nalazi se u boljem položaju kad treba pružiti oslobađajući dokaz kako bi potvrdio da nije ni na koji način odgovoran za događaj koji je prouzročio štetu [25].

64. Voditelj obrade također će trebati dokazati, u skladu s opisanim načelom pouzdanosti, da je učinio sve što je bilo moguće kako bi pravodobno ponovno uspostavio dostupnost osobnih podataka i pristup tim podacima.

65. Da se vratim na pitanje suda koji je uputio zahtjev, na temelju onog što se navodi o prirodi odgovornosti voditelja obrade u slučaju kad se, kao što je navedeno, voditelj obrade može izuzeti od odgovornosti ako dokaže da je do povrede došlo zbog razloga za koji on ni na koji način nije odgovoran, taj razlog ne može biti sama činjenica da je događaj prouzročila osoba koja ne podliježe njegovoj kontroli.

[22] Građanskopravna odgovornost obično se kvalificira kao objektivna odgovornost uvijek kad je osoba koja djeluje dužna donijeti sve teoretski moguće mjere kako bi se izbjegla šteta, neovisno o stvarnim saznanjima koje ima o tim mjerama ili njihovoj gospodarskoj održivosti. Suprotno tomu, kad se osobi koja djeluje nalaže donošenje mjera koje subjekt u referentnom gospodarskom sektoru obično može ispuniti kako bi se održala sigurnost i kako bi se spriječili negativni učinci koji mogu proizaći iz djelatnosti koja se obavlja, odgovornost za samu štetu bliža je sustavu odgovornosti na temelju određene vrste krivnje. M. Gambini, *Responsabilità*, *op. cit.*, str. 1055.

[23] M. Gambini, *Responsabilità*, *op. cit.*, str. 1059. U istom smislu, u pogledu mišljenja u skladu s kojim se dokaz da su provedene prikladne mjere ne sastoji samo od obične tvrdnje u prilog osobito savjesnom postupanju koje se zahtijeva, nego od dokazivanja neke druge činjenice koja je dovela do nastanka štete i koja je po svojoj prirodi nepredvidljiva i neizbježna, što je svojstveno nepredvidljivim okolnostima i višoj sili, vidjeti S. Sica, *Sub art. 82*, objavljeno u R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „[A]ko *dokaže* da nije ni na koji način odgovoran za događaj koji je prouzročio štetu" (članak 82. stavak 3.).

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

66. Kad je voditelj obrade žrtva napada kiberkriminalaca, može se smatrati da za događaj koji je doveo do nastanka štete ne odgovara voditelj obrade, ali nije isključeno da je nemar voditelja obrade podataka uzrok napada o kojem je riječ jer je napad učinio lakšim zbog toga što su izostale mjere sigurnosti u pogledu osobnih podatka koje je voditelj obrade trebao provoditi ili one nisu bile odgovarajuće. Riječ je o činjeničnim ocjenama koje su posebne u svakom pojedinom slučaju i koje nacionalni sud pred kojim je pokrenut postupak treba provesti s obzirom na dokaze koji su mu podneseni.

67. Isto tako, uobičajeno je da su napadi izvana na sustave javnih ili privatnih subjekata koji su voditelji obrade velikih količina osobnih podataka učestaliji od unutarnjih napada. Voditelj obrade stoga treba predvidjeti odgovarajuće mjere osobito za sprečavanje napada izvana.

68. Naposljetku, s teleološkog stajališta valja napomenuti da se Uredbom nastoji postići cilj visoke razine zaštite. U tom pogledu, Sud je već naglasio da iz članka 1. stavka 2. Uredbe, u vezi s njezinim uvodnim izjavama 10., 11. i 13., proizlazi da se tom uredbom institucijama, tijelima, uredima i agencijama Unije te nadležnim tijelima država članica nalaže da osiguraju visoku razinu zaštite prava povezanih sa zaštitom osobnih podataka i zajamčenih člankom 16. UFEU-a i člankom 8. Povelje [26].

69. Ako se Sud opredijeli za tumačenje u skladu s kojim, u slučaju kad je povredu Uredbe počinila treća osoba, voditelja obrade automatski treba izuzeti od odgovornosti u skladu s člankom 82. stavkom 3., učinak tog tumačenja ne bi bio u skladu s ciljem zaštite koji se tim sredstvom nastoji postići jer bi oslabio prava ispitanika zato što bi se ta odgovornost ograničila na slučajeve u kojima su povredu počinile osobe koje su podređene tom voditelju obrade i/ili koje podliježu njegovoj kontroli.

F. Peto prethodno pitanje

70. Petim pitanjem nacionalni sud u biti traži od Suda da tumači pojam „nematerijalna šteta” u smislu članka 82. Uredbe. Konkretno, nacionalni sud nastoji doznati treba li odredbe članka 82. stavaka 1. i 2. u vezi s uvodnim izjavama 85. i 146. Uredbe [27] tumačiti na način da, u slučaju u kojem se povreda te uredbe sastoji od neovlaštenog pristupa kiberkriminalaca osobnim podacima i neovlaštenog širenja osobnih podataka, činjenica da ispitanik trpi bojazan zbog moguće buduće zlouporabe osobnih podataka već sama po sebi predstavlja (nematerijalnu) štetu koja daje pravo na naknadu štete.

71. Ni članak 82. ni uvodne izjave koje se odnose na naknadu štete ne daju jasan odgovor na pitanje, ali se iz njih mogu izvesti određeni korisni elementi za analizu: neimovinska (ili nematerijalna) šteta može se nadoknaditi zajedno s materijalnom (ili imovinskom) štetom; iz povrede Uredbe automatski ne proizlazi šteta koju bi ta povreda „prouzročila” ili, konkretnije, povreda osobnih podataka „može prouzročiti” fizičku, materijalnu ili nematerijalnu štetu

[26] Vidjeti u tom smislu presudu od 15. lipnja 2021., Facebook Ireland i dr. (C-645/19, EU:C:2021:483, t. 43. i 44.).

[27] U skladu s uvodnom izjavom 85.: „Ako se povreda osobnih podataka ne rješava na odgovarajući način i pravodobno, ona može prouzročiti fizičku, materijalnu ili nematerijalnu štetu pojedincima […]”. U skladu s uvodnom izjavom 146.: „Voditelj obrade ili izvršitelj obrade trebao bi nadoknaditi svaku štetu koju osoba može pretrpjeti zbog obrade kojom se krši ova Uredba. Voditelj obrade ili izvršitelj obrade trebao bi biti izuzet od odgovornosti ako dokaže da nije ni na koji način odgovoran za štetu. Pojam štete trebalo bi široko tumačiti s obzirom na sudsku praksu Suda tako da se u potpunosti odražavaju ciljevi ove Uredbe. Time se ne dovode u pitanje zahtjevi za naknadu štete koja proizlazi iz kršenja drugih pravila prava Unije ili prava države članice. […]. Ispitanici bi trebali dobiti potpunu i učinkovitu naknadu za štetu koju su pretrpjeli […]”.

pojedincima; pojam štete trebalo bi „široko" tumačiti s obzirom na sudsku praksu Suda tako da se u potpunosti odražavaju ciljevi Uredbe; trebalo bi dobiti „potpunu i učinkovitu" naknadu za štetu koja se „pretrpjel[a]".

72. Već se tekstom odredbi Uredbe uklanja bilo kakva mogućnost upućivanja na štetu koja se podrazumijeva: glavni cilj građanskopravne odgovornosti predviđene Uredom jest obeštetiti ispitanika upravo na temelju „potpun[e] i učinkovit[e]" naknade za pretrpljenu štetu i, stoga, ponovno uravnotežiti pravnu situaciju na koju je negativno utjecala povreda prava [28].

73. S druge strane, i sa sustavnog stajališta, kao što je to u slučaju propisa o suzbijanju zabranjenih sporazuma, Uredbom se predviđaju dva temelja zaštite: jedan je javne prirode i njime se predviđaju sankcije u slučaju povreda odredbi Uredbe, a drugi je privatne prirode te se upravo njime predviđa građanskopravna izvanugovorna odgovornost koja se može kvalificirati kao stroža odgovornost na temelju pretpostavljene krivnje i koja ima navedena obilježja, također s obzirom na oslobađajući dokaz [29].

74. Stoga se šire tumačenje [30] pojma (nematerijalne) štete ne može proširiti toliko da se smatra da je zakonodavac odustao od potrebe da treba postojati stvarna i prava „šteta".

75. Pravi suštinski problem jest može li, ako se utvrdi postojanje povrede i uzročno-posljedične veze, nastati pravo na naknadu štete uslijed obične zabrinutosti, bojazni i strahova koje ispitanik trpi zbog moguće buduće zlouporabe osobnih podataka ako takva zlouporaba nije utvrđena i/ili ispitaniku nije nastala nikakva daljnja šteta.

76. Prema ustaljenoj sudskoj praksi Suda, pojmovi iz odredbe prava Unije koja ne sadržava nikakvo izričito upućivanje na pravo država članica za utvrđivanje njezina smisla i dosega u cijeloj Europskoj uniji trebaju se tumačiti na autonoman i ujednačen način, pri čemu prilikom tog tumačenja treba uzeti u obzir ne samo tekst odredbe o kojoj je riječ, nego i kontekst u kojem se nalazi, cilj koji se želi postići propisom kojeg je ona dio i nastanak te odredbe [31].

77. Kao što je to napomenuo nezavisni odvjetnik Campos Sánchez-Bordona [32], Sud nije dao opću definiciju „štete" koja je bez razlike primjenjiva u svim područjima [33]. Kad je riječ o nematerijalnoj šteti, iz sudske prakse Suda može se zaključiti da ako je jedan od ciljeva odredbe koja se tumači

[28] Vidjeti navedeno mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone, t. 29. i bilješku 11. U tom mišljenju nezavisni odvjetnik pravilno je zaključio svoju analizu s doslovnog, povijesnog, kontekstualnog i teleološkog stajališta, pri čemu je isključio „kaznenu" prirodu štete koja se ispitanicima nadoknađuje u skladu s člankom 82. (t. 27. do 55.) te je istaknuo, s jedne strane, da države članice „ne trebaju odabrati (niti to zapravo mogu) određeni mehanizam iz poglavlja VIII. kako bi osigurale zaštitu podataka. Ako postoji povreda koja ne stvara štetu, ispitaniku se i dalje (kao minimalna zaštita) daje pravo na podnošenje pritužbe nadzornom tijelu" i, s druge strane, da bi „mogućnost dobivanja naknade štete neovisno o tome postoji li bilo kakva šteta vjerojatno […] potaknula građanskopravne postupke, u kojima tužbe možda ne bi uvijek bile opravdane, te bi ona, u tom smislu, mogla odvratiti od djelatnosti obrade podataka"(t. 54. i 55.).

[29] Uskraćivanje prava na naknadu štete zbog slabih i prolaznih osjećaja koji su povezani s povredom pravila o obradi ne dovodi stoga do potpune nezaštićenosti ispitanika (vidjeti u tom smislu navedeno mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone, t. 115.).

[30] Ili, prema riječima iz uvodne izjave 146., „široko" tumačiti

[31] Vidjeti presude od 15. travnja 2021., The North of England P & I Association (C-786/19, EU:C:2021:276, t. 48.) i od 10. lipnja 2021., KRONE - Verlag (C-65/20, EU:C:2021:471, t. 25.).

[32] Vidjeti navedeno mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone, t. 104.

[33] Nije naveo ni metodu tumačenja – autonomnog ili upućivanjem na nacionalne pravne poretke – kojoj se daje prednost: ovisi o području koje se ispituje. Usporediti presude od 10. svibnja 2001., Veedfald (C-203/99, EU:C:2001:258, t. 27.), u području neispravnih proizvoda, od 6. svibnja 2010., Walz (C-63/09, EU:C:2010:251, t. 21.), o odgovornosti zračnih prijevoznika ili od 10. lipnja 2021., Van Ameyde España (C-923/19, EU:C:2021:475, t. 37. i sljedeće), u pogledu građanskopravne odgovornosti koja se primjenjuje na nezgode izazvane upotrebom motornih vozila.

zaštita pojedinca ili određene kategorije pojedinaca [34], pojam štete treba biti širok i da, u skladu s tim kriterijem, naknada štete obuhvaća nematerijalnu štetu, čak i ako se u odredbi koja se tumači ne navodi ta šteta [35].

78. Iako je na temelju sudske prakse Suda moguće zagovarati da, u navedenim uvjetima, u pravu Unije postoji načelo naknade nematerijalne štete, slažem se s nezavisnim odvjetnikom M. Camposom da iz nje ne može proizaći pravilo na temelju kojeg je nadoknadiva *svaka* nematerijalna šteta, neovisno o njezinoj ozbiljnosti [36].

79. U tom kontekstu, relevantno je razlikovanje nadoknadive nematerijalne štete od *drugih neugodnosti koje proizlaze iz nepoštovanja zakonitosti* te koje zbog svoje neznatnosti ne dovode nužno do prava na naknadu štete [37].

80. Sud priznaje tu razliku kad upućuje na probleme i neugodnosti kao samostalnu kategoriju u odnosu na kategoriju štete, u područjima u kojima smatra da ih treba nadoknaditi [38].

81. Empirijski, valja napomenuti da svaka povreda pravnog pravila o zaštiti osobnih podataka dovodi do određene negativne reakcije ispitanika. Naknada štete koja proizlazi iz običnog osjećaja nezadovoljstva zbog toga što je netko drugi prekršio zakon lako se može zamijeniti za naknadu u slučaju da šteta ne postoji za što se čini, kao što je navedeno, da nije moguće u slučaju koji se navodi u članku 82. Uredbe.

82. Činjenica da je, u okolnostima kao što su one u glavnom postupku, zlouporaba osobnih podataka samo moguća, a ne već stvarna, dovoljna je kako bi se smatralo da je ispitanik pretrpio nematerijalnu štetu koju je prouzročila povreda Uredbe, pod uvjetom da ispitanik dokaže da mu je bojazan od takve zlouporabe konkretno i određeno prouzročila stvarnu i izvjesnu emocionalnu štetu [39].

[34] Primjerice, potrošača proizvoda ili žrtava prometnih nezgoda

[35] U području putovanja u paket aranžmanima, vidjeti presudu od 12. ožujka 2002., Leitner (C-168/00, EU:C:2002:163); u području građanskopravne odgovornosti u pogledu upotrebe motornih vozila, presude od 24. listopada 2013., Haasová (C-22/12, EU:C:2013:692, t. 47. do 50.), od 24. listopada 2013., Drozdovs (C-277/12, EU:C:2013:685, t. 40.) i od 23. siječnja 2014., Petillo (C-371/12, EU:C:2014:26, t. 35.).

[36] Vidjeti navedeno mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone, t. 105. Primjerice, Sud je priznao da je u skladu s pravilima prava Unije nacionalni zakon u kojem se, u svrhu izračuna naknade štete, nematerijalna šteta povezana s tjelesnim ozljedama zbog nezgode razlikuje ovisno o uzroku te štete; vidjeti presudu od 23. siječnja 2014., Petillo (C-371/12, EU:C:2014:26), izreka: pravu Unije ne protivi se „nacionalno zakonodavstvo […] koje predviđa poseban sustav naknade nematerijalne štete nastale zbog lakših tjelesnih ozljeda uzrokovanih prometnim nezgodama u cestovnom prometu, ograničavajući naknadu navedene štete u odnosu na ono što je dopušteno na području naknade istovjetne štete uzrokovane na drukčiji način, a ne tim nezgodama".

[37] Takva se razlika može uočiti u nacionalnim pravnim porecima kao neizbježna posljedica života u društvu. Nedavno, u području zaštite podataka, u Italiji, Tribunale di Palermo (Sud u Palermu, Italija), prvo građansko vijeće, presuda br. 5261 od 5. listopada 2017., te Corte suprema di cassazione (Vrhovni kasacijski sud, Italija), građanski odjel, šesto vijeće, br. 17383/2020. U Njemačkoj, među ostalim, AG Diez, 07.11.2018 – 8 C 130/18; LG Karlsruhe, 02.08.2019 – 8 O 26/19, i AG Frankfurt am Main, 10.07.2020 – 385 C 155/19 (70). U Austriji, OGH 6 Ob 56/21k.

[38] Vidjeti presudu od 23. listopada 2012., Nelson i dr. (C-581/10 i C-629/10, EU:C:2012:657, t. 51.), u pogledu razlike između „štete" u smislu članka 19. Konvencije o ujednačavanju određenih pravila u međunarodnom zračnom prijevozu, sklopljene u Montrealu 28. svibnja 1999., i „neugodnosti" u smislu Uredbe br. 261/2004, koje su nadoknadive na temelju njezina članka 7., u skladu s presudom od 19. studenoga 2009., Sturgeon i dr. (C-402/07 i C-432/07, EU:C:2009:716). U tom području, kao i u području prijevoza putnika morem ili plovnim putovima na koji se upućuje u Uredbi br. 1177/2010, zakonodavac je mogao priznati apstraktnu kategoriju zahvaljujući činjenici da su čimbenik koji uzrokuje problem i njegova bit istovjetni za sve oštećene osobe. Ne smatram da je takav zaključak moguć u području zaštite podataka.

[39] Irska smatra da su ta razmatranja osobito važna u praksi u kontekstu kiberkriminala jer kad bi svaka osoba na koju utječe povreda, pa čak i neznatno, imala pravo na naknadu nematerijalne štete, to bi snažno utjecalo osobito na voditelje obrade podataka u javnom sektoru koji se financiraju iz ograničenih javnih sredstava i koji bi zapravo trebali služiti kolektivnim interesima, uključujući poboljšanje sigurnosti osobnih podataka (pisana očitovanja, t. 72.).

83. Granica između običnog nezadovoljstva (koje nije nadoknadivo) te stvarne i prave nematerijalne štete (koja je nadoknadiva) svakako je neznatna, ali nacionalni sudovi, koji imaju zadaću da u svakom slučaju zasebno utvrde tu granicu, trebaju pažljivo ocijeniti sve dokaze koje je podnio ispitanik koji zahtijeva naknadu štete i koji je obvezan točno, a ne samo općenito, navesti konkretne elemente koji mogu dovesti do nastanka „stvarno pretrpljene nematerijalne štete" zbog povrede osobnih podataka, ali ta šteta ne mora dostići unaprijed određen i osobito ozbiljan stupanj: ono što je bitno jest da nije riječ samo o subjektivnom doživljaju koji je promjenjiv i koji također ovisi o karakternim i osobnim elementima, nego i o objektivizaciji tjelesne ili psihičke neugodnosti odnosno neugodnosti u odnosima, koja je dokaziva, iako je blaga, a bitna je i priroda osobnih podataka o kojima je riječ te njihova relevantnost u životu ispitanika te možda čak i predodžba koju društvo u tom trenutku ima u pogledu te posebne neugodnosti povezane s povredom podataka [40].

IV. Zaključak

84. Na temelju svih prethodnih razmatranja, predlažem Sudu da na upućena prethodna pitanja odgovori na sljedeći način:

„Članke 5., 24., 32. i 82. Uredbe 2016/679 treba tumačiti na način da:

činjenica da samo postoji ‚povreda osobnih podataka', kako se definira člankom 4. točkom 12., sama po sebi nije dovoljna kako bi se zaključilo da tehničke i organizacijske mjere koje je poduzeo voditelj obrade nisu bile „odgovarajuće" kako bi se osigurala zaštita podataka o kojima je riječ;

prilikom ispitivanja jesu li tehničke i organizacijske mjere koje je proveo voditelj obrade osobnih podataka odgovarajuće, nacionalni sud pred kojim je pokrenut postupak treba provesti nadzor koji obuhvaća konkretnu analizu i sadržaja tih mjera i načina na koji se primjenjuju te njihovih učinaka u praksi;

u okviru tužbe za naknadu štete u skladu s člankom 82. OUZP-a, na voditelju je obrade osobnih podataka teret dokaza da su u skladu s člankom 32. te uredbe mjere koje je proveo odgovarajuće;

u skladu s načelom postupovne autonomije, nacionalnim pravnim sustavom svake države članice treba utvrditi prihvatljive metode dokazivanja i njihovu dokaznu vrijednost, uključujući istražne radnje koje nacionalni sudovi mogu ili moraju naložiti kako bi ocijenili je li voditelj obrade osobnih podataka proveo mjere koje su odgovarajuće u smislu te uredbe, pri čemu se poštuju načela ekvivalentnosti i djelotvornosti utvrđena pravom Unije,

činjenica da je povredu te uredbe koja je prouzročila štetu o kojoj je riječ počinila treća osoba sama po sebi ne predstavlja razlog da se voditelja obrade izuzme od odgovornosti te, kako bi ostvario pravo na izuzimanje od odgovornosti predviđeno tom odredbom, voditelj obrade treba dokazati da ni na koji način nije odgovoran za povredu;

[40] Vidjeti navedeno mišljenje nezavisnog odvjetnika M. Camposa Sánchez-Bordone, t. 116.

šteta koja se sastoji od bojazni zbog moguće buduće zlouporabe vlastitih osobnih podataka za koju je ispitanik dokazao da postoji može predstavljati nematerijalnu štetu koja daje pravo na naknadu štete, pod uvjetom da ispitanik dokaže da je on kao pojedinac pretrpio stvarnu i izvjesnu emocionalnu štetu, što je okolnost koju nacionalni sud pred kojim je pokrenut postupak treba provjeriti u svakom slučaju zasebno".