Kohtulahendite kogumik

KOHTUJURISTI ETTEPANEK
GIOVANNI PITRUZZELLA
esitatud 27. aprillil 2023 [1]

Kohtuasi C-340/21

VB

versus

Natsionalna agentsia za prihodite

(eelotsusetaotlus, mille on esitanud Varhoven administrativen sad (Bulgaaria kõrgeim halduskohus))

Eelotsusetaotlus – Isikuandmete kaitse – Määrus (EL) 2016/679 – Vastutava töötleja vastutus – Töötlemise turvalisus – Isikuandmete töötlemise turvalisuse rikkumine – Mittevaraline kahju, mille põhjustas vastutava töötleja tegevusetus – Kahju hüvitamise nõue

Kas avalik-õigusliku asutuse valduses olevate isikuandmete ebaseaduslik avalikustamine häkkerite rünnaku tõttu võib anda alust mittevaralise kahju hüvitamiseks isikule, kelle andmetega on tegemist, üksnes seepärast, et ta kardab, et tema andmeid võidakse tulevikus kuritarvitada? Missuguste kriteeriumide põhjal loetakse vastutavaks vastutavat töötajat? Kuidas jaguneb tõendamiskoormis kohtumenetluses? Missuguse ulatusega on kohtulik kontroll?

I. Õiguslik raamistik

1. Määruse 2016/679 [2] (edaspidi „määrus“) artiklis 4 „Mõisted“ on sätestatud:

„Käesolevas määruses kasutatakse järgmisi mõisteid:

[…]

12) „isikuandmetega seotud rikkumine“ – turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu;

[…]“.

[1] Algkeel: itaalia.

[2] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

2. Artiklis 5 „Isikuandmete töötlemise põhimõtted“ on nähtud ette:

„1. Isikuandmete töötlemisel tagatakse, et

[…]

f) isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“);

2. Lõike 1 täitmise eest vastutab ja on võimeline selle täitmist tõendama vastutav töötleja („vastutus“).“

3. Määruse artiklis 24 „Vastutava töötleja vastutus“ on sätestatud:

„1. Arvestades töötlemise laadi, ulatust, konteksti ja eesmärke, samuti füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte, rakendab vastutav töötleja asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada isikuandmete töötlemist kooskõlas käesoleva määrusega. Vajaduse korral vaadatakse need meetmed läbi ja ajakohastatakse neid.

2. Kui see on proportsionaalne isikuandmete töötlemise toimingutega, hõlmavad lõikes 1 osutatud meetmed asjakohaste andmekaitsepõhimõtete rakendamist vastutava töötleja poolt.

3. Vastutava töötleja kohustuste järgimise tõendamise elemendina võib kasutada artiklis 40 osutatud heakskiidetud toimimisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist.“

4. Artiklis 32 „Töötlemise turvalisus“ on nähtud ette:

„1. Võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning arvestades isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele, rakendavad vastutav töötleja ja volitatud töötleja ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, hõlmates muu hulgas vastavalt vajadusele järgmist:

[…]

2. Vajaliku turvalisuse taseme hindamisel võetakse eelkõige arvesse isikuandmete töötlemisest tulenevaid ohte, eelkõige edastatavate, salvestatavate või muul viisil töödeldavate isikuandmete juhuslikku või ebaseaduslikku hävitamist, kaotsiminekut, muutmist ja loata avalikustamist või neile juurdepääsu.

3. Käesoleva artikli lõikes 1 osutatud nõuete järgimise tõendamise elemendina võib kasutada artiklis 40 osutatud heakskiidetud toimimisjuhendite või artiklis 42 osutatud heakskiidetud sertifitseerimismehhanismi järgimist.

[…]“.

5. Selle määruse artiklis 82 „Õigus hüvitisele ja vastutus“ on sätestatud:

„1. Igal isikul, kes on kandnud käesoleva määruse rikkumise tulemusel materiaalset või mittemateriaalset kahju, on õigus saada vastutavalt töötlejalt või volitatud töötlejalt hüvitist tekitatud kahju eest.

2. Kõnealuse töötlemisega seotud vastutav töötleja vastutab kahju eest, mis on tekkinud sellise töötlemise tulemusel, millega rikutakse käesolevat määrust. […].

3. Vastutav töötleja või volitatud töötleja vabastatakse vastutusest lõike 2 kohaselt, kui ta tõendab, et ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest.“

II. Faktilised asjaolud, menetlus ja eelotsuse küsimused

6. Bulgaaria meedia teavitas 15. juulil 2019 avalikkust, et Natsionalna agentsia za prihodite (riigi maksuamet, Bulgaaria; edaspidi „NAP“[3]) infosüsteemile on saadud loata juurdepääs ning et miljonite kodanike ja välismaalaste mitmesugune maksu- ja sotsiaalkindlustusalane teave on internetis avalikustatud.

7. Paljud isikud, nende hulgas VB, kes on põhikohtuasja kassaator, esitasid seega kohtule NAP vastu kahju hüvitamise nõude, et neile hüvitataks nende mittevaraline kahju.

8. Käsitletaval juhul pöördus põhikohtuasja kassaator Administrativen sad Sofia-gradi (Sofia linna halduskohus, Bulgaaria; edaspidi „ASSG“) poole, väites, et NAP oli rikkunud riigisisest õigust ja kohustust töödelda vastutava töötlejana isikuandmeid viisil, mis „tagab asjakohase turvalisuse“, rakendades asjakohaseid tehnilisi ja korralduslikke meetmeid määruse 2016/679 artiklite 24 ja 32 tähenduses. Seejärel kinnitas kassaator, et on kandnud mittevaralist kahju, mis väljendub mures ja kartuses tema isikuandmete tulevase kuritarvitamise pärast.

9. Vastaspool rõhutas vastupidi, et põhikohtuasja kassaator ei küsinud mingit teavet selle kohta, millistele konkreetsetele isikuandmetele loata juurde pääseti. Lisaks kutsus ta rünnakuteate peale kokku kohtumised ekspertidega kodanike õiguste ja huvide kaitse eesmärgil. NAP sõnul puudus põhjuslik seos küberrünnaku ja väidetava kahju vahel, sest ta on sisse seadnud protsesside haldamise süsteemid ja infoturbe haldamise süsteemid, nagu on nõutud selles valdkonnas kehtivates rahvusvahelistes õigusnormides.

10. Esimese astme kohus, ASSG, jättis nõude rahuldamata, asudes seisukohale, et andmete avalikustamises ei saa pidada vastutavaks NAPd; et tõendamiskoormis võetud meetmete asjakohasuse küsimuses lasub kassaatoril ning et ei hüvitata mingit mittevaralist kahju.

11. Esimese astme kohtu otsus vaidlustati seejärel Varhoven administrativen sadis (Bulgaaria kõrgeim halduskohus). Esitatud väidete hulgas rõhutas põhikohtuasja kassaator, et esimese astme kohus jaotas turvameetmete võtmata jätmise tõendamisel tõendamiskoormise vääralt. Ka ei peaks tõendamiskoormis hõlmama mittevaralist kahju, sest tegemist on tegeliku, mitte hüpoteetilise mittevaralise kahjuga.

[3] NAP on vastutav töötleja määruse artikli 4 punkti 7 tähenduses. Riigisisese õiguse kohaselt on ta konkreetse pädevusega haldusasutus rahandusministeeriumi haldusalas ning tema ülesanne on rahaliste vahendite tuvastamine, tagamine ja sissenõudmine ning avalik-õiguslike ning seadusega sätestatud eraõiguslike riigi nõuete tuvastamine, tagamine ja sissenõudmine. Talle delegeeritud avalik-õiguslike volituste täitmisel töötleb ta isikuandmeid.

12. NAP kordas, et võttis vastutava töötlejana vajalikud tehnilised ja korralduslikud meetmed, ning vaidles vastu sellele, et tegelikku mittevaralist kahju on tõendatud. Mure ja hirm on nimelt emotsionaalsed seisundid, mida ei pea hüvitama.

13. Eelotsusetaotluse esitanud kohus tuvastas mitu kohtulahendit seoses üksikmenetlustega, mille kahju kannatanud olid eraldi NAP vastu esile kutsunud, et saada hüvitist mittevaralise kahju eest.

14. Selles olukorras peatas eelotsusetaotluse esitanud kohus menetluse ja esitas Euroopa Kohtule järgmised eelotsuse küsimused:

„1. Kas [Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)] artikleid 24 ja 32 tuleb tõlgendada nii, et võetud tehniliste ja korralduslike meetmete mitteasjakohasuse eeldamiseks piisab sellest, et isikuandmete loata avalikustamine või neile juurdepääs kõnealuse määruse artikli 4 punkti 12 tähenduses on põhjustatud isikute poolt, kes ei ole vastutava töötleja administratsiooni töötajad ega allu tema kontrollile?

2. Juhul, kui vastus esimesele küsimusele on eitav, siis millised peavad olema õiguspärasuse kohtuliku kontrolli ese ja ulatus hindamaks, kas vastutava töötleja võetud tehnilised ja korralduslikud meetmed on määruse (EL) 2016/679 artikli 32 kohaselt asjakohased?

3. Juhul, kui vastus esimesele küsimusele on eitav, siis kas vastutuse põhimõtet, mis on sätestatud määruse (EL) 2016/679 artikli 5 lõikes 2 ja artiklis 24 koostoimes põhjendusega 74, tuleb tõlgendada nii, et kõnealuse määruse artikli 82 lõike 1 kohases kaebemenetluses lasub vastutaval töötlejal kohustus tõendada, et määruse artikli 32 kohaselt võetud tehnilised ja korralduslikud meetmed on asjakohased? Kas eksperdiarvamuse küsimist võib pidada vajalikuks ja piisavaks tõendiks, et tuvastada, kas vastutava töötleja võetud tehnilised ja korralduslikud meetmed olid asjakohased niisugusel juhul nagu käesolevas asjas, mil isikuandmetele loata juurdepääs ja nende avalikustamine toimusid nn häkkerite rünnaku tagajärjel?

4. Kas määruse (EL) 2016/679 artikli 82 lõiget 3 tuleb tõlgendada nii, et isikuandmete loata avalikustamine või neile juurdepääs kõnealuse määruse artikli 4 punkti 12 tähenduses, mille – nagu käesoleval juhul – oli põhjustanud nn häkkerite rünnak, mille korraldasid isikud, kes ei ole vastutava töötleja administratsiooni töötajad ega allu tema kontrollile, kujutab endast asjaolu, mille eest ei ole vastutav töötleja mingil viisil vastutav ja mis annab õiguse vastutusest vabastamiseks?

5. Kas määruse (EL) 2016/679 artikli 82 lõikeid 1 ja 2 koostoimes põhjendustega 85 ja 146 tuleb tõlgendada nii, et niisugusel juhul nagu käesolevas asjas, mil isikuandmete kaitse rikkumine seisnes isikuandmetele loata juurdepääsus ja nende levitamises nn häkkerite rünnaku tagajärjel, kuuluvad üksnes andmesubjekti kogetud mure, kartus ja hirm isikuandmete võimaliku tulevase kuritarvitamise pärast mittevaralise kahju laialt tõlgendatava mõiste alla ning annavad õiguse nõuda kahju hüvitamist, kui niisugust kuritarvitust ei ole tuvastatud ja/või andmesubjektile ei ole tekkinud muud kahju?“

III. Õiguslik analüüs

A. Sissejuhatavad märkused

15. Käesolev kohtuasi puudutab huvitavaid ja osaliselt siiani käsitlemata küsimusi, milles palutakse tõlgendada määruse mitmesuguseid sätteid.[4]

16. Need viis eelotsuse küsimust pöörlevad kõik ümber sama küsimuse: tingimused, mis peavad olema täidetud, et hüvitada mittevaraline kahju isikule, kelle isikuandmeid, mis on ametiasutuse valduses, on avalikustatud internetis häkkerite rünnaku tulemusena.

17. Esitluse mugavuse huvides teen ettepaneku anda eelotsusetaotluses esitatud eelotsuse küsimustele eraldi ülevaatlikud vastused, ehkki olen teadlik teatavatest kontseptuaalsetest kattuvustest, sest esimese nelja küsimusega püütakse kõigiga kindlaks teha eeldusi, mille esinemise korral saab määruse sätete rikkumise eest vastutavaks pidada andmete vastutavat töötlejat,[5] ja viies puudutab täpsemalt mõistet „mittevaraline kahju“ seoses hüvitamisega[6].

18. Juhin tähelepanu, et määruse artikli 82 teemal on praegu Euroopa Kohtus pooleli mitu kohtuasja ning ühes nendest on juba ette loetud kohtujuristi ettepanek, mida ma käesolevas analüüsis arvesse võtan.[7]

19. Enne tõstatatud küsimuste käsitlemist pean vajalikuks teha mõne sissejuhatava märkuse määruse põhimõtete ja eesmärkide kohta, mis osutuvad üksikutele eelotsuse küsimustele vastamisel vajalikuks.

20. Määruse artiklis 24 on üldises sõnastuses sätestatud vastutava töötleja kohustus võtta asjakohased tehnilised või korralduslikud meetmed selle tagamiseks, et isikuandmete töötlemine oleks kooskõlas määrusega, ning olla võimeline seda tõendama, samas kui artiklis 32 on sätestatud sama kohustus konkreetsemalt osas, mis puudutab töötlemise turvalisust. Artiklites 24 ja 32 on reguleeritud konkreetsemalt seda, mis on ette nähtud juba artikli 5 lõikes 2, milles on just „isikuandmete töötlemise põhimõtete“ hulgas sätestatud „vastutuse põhimõte“. See järgneb loogiliselt artikli 5 lõike 1 punktis f ette nähtud „usaldusväärsuse ja konfidentsiaalsuse põhimõttele“ ning täiendab seda ning neid mõlemaid tuleb tõlgendada, lähtudes riskipõhisest lähenemisest, millel määrus rajaneb.

4 Artikli 5 lõiget 2 (mis käsitleb iga isikuandmete vastutava töötleja vastutuse põhimõtet), artiklit 24 (mis käsitleb meetmeid, mida see vastutav töötleja on kohustatud võtma selle tagamiseks, et tema töötlemine oleks määrusega kooskõlas), artiklit 32 (mis käsitleb seda kohustust konkreetselt töötlemise turvalisuse osas) ning artikli 82 lõikeid 1–3 (mis käsitlevad määruse rikkumisega põhjustatud kahju hüvitamist ja vastutava töötleja võimalust võtta meetmeid selle tagamiseks, et määrust järgitakse) ning põhjendusi 74, 85 ja 146, mis on nende artiklitega seotud.

5 a) esimese eesmärk on vastata küsimusele, kas ainuüksi süsteemide rikkumisest võib järeldada, et eelnevad meetmed ei olnud asjakohased; b) teine käsitleb nende meetmete asjakohasuse üle teostatava kohtuliku kontrolli ulatust; c) kolmandas on nimetatud tõendamiskoormist selle asjakohasuse tõendamisel ning teatavaid tehnilisi meetodeid tõendite kogumisel; d) neljas on küsimus, kas vastutusest vabastamisel on asjakohane asjaolu, et süsteemi rünnati väljastpoolt.

6 Mis puudutab määruse viidatud sätteid, siis esimesed kolm küsimust käsitlevad vastutava töötleja vastutuse aspekte seoses nende meetmete asjakohasusega, mis võtta tuleb (artiklid 5, 24 ja 32); neljas ja viies vastutusest vabastamise tingimusi ja mõistet „hüvitatav mittevaraline kahju“ (artikkel 82).

7 Vt kohtujurist Campos Sánchez-Bordona ettepanek kohtuasjas Österreichische Post (isikuandmete töötlemisega seotud mittevaraline kahju) (C-300/21, EU:C:2022:756).

21. Vastutuse põhimõte on üks määruse nurgakivisid ja üks selle märkimisväärsemaid uuendusi. Sellega on vastutavale töötlejale kehtestatud kohustus võtta proaktiivseid meetmeid, et järgida määrust ja olla valmis seda ka tõendama. [8]

22. Õigusteoorias on kõneldud tõelisest kultuurilisest muutusest, mis on „vastutamise kohustuse üldise ulatuse“ tagajärg. [9] Vastutavat töötlejat ei vabasta vastutusest mitte niivõrd õigusliku kohustuse või konkreetse meetme formaalne järgimine kui ettevõtja tervikstrateegia, sest ta järgib (*compliant*) andmekaitseregulatsiooni.

23. Tehnilised ja korralduslikud meetmed, mille võtmist vastutuse põhimõte eeldab, peavad olema „asjakohased“, arvestades artiklis 24 täpsustatud tegureid: töötlemise laadi, ulatust, konteksti ja eesmärke, samuti füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte.

24. Artikkel 24 kohustab seega võtma asjakohaseid meetmeid, et oleks võimalik tõendada töötlemise vastavust määruses sätestatud põhimõtetele ja selle eesmärkidele.

25. Artiklis 32 on vastutuse põhimõtet käsitletud vastupidi nende konkreetsete meetmete vaatevinklist, mis tuleb võtta „ohule vastava turvalisuse taseme“ tagamiseks. Seejuures on selle artikliga lisatud juba ette nähtud teguritele, mida tuleb tehniliste ja korralduslike meetmete eelneval kindlaksmääramisel arvesse võtta, teaduse ja tehnoloogia viimane areng ning rakendamiskulud.

26. Mõiste „asjakohasus“ eeldab, et infosüsteemide kaitseks kasutatavad lahendused on vastuvõetaval tasemel nii tehnilisest (meetmete asjakohasus) kui ka kvalitatiivsest seisukohast (kaitse tõhusus). Et tagada vajaduse, asjakohasuse ja proportsionaalsuse põhimõtte järgmine, peab töötlemine olema mitte üksnes asjakohane, vaid ka taotletavate eesmärkide seisukohast piisav. Selle loogika kohaselt on võimalikult väheste andmete kogumise põhimõttel otsustav roll, sest nimetatud põhimõtte järgi tuleb andmete töötlemise kõikides etappides pidevalt püüelda selle poole, et turvalisust ähvardavaid ohte vähendatakse miinimumini. [10]

27. Kogu määrus on suunatud ohu ennetamisele ja vastutava töötleja vastutusele ning seega teleoloogilisele lähenemisele, mille eesmärk on saavutada võimalikult hea tulemus tõhususe seisukohast – mis jääb seega üsna kaugele formalistlikust loogikast, mis seondub lihtsalt kohustusega järgida konkreetseid menetlusi, et sellest vastutusest vabaneda. [11]

[8] Docksey, C., *Article 24. Responsibility of the controller*, Kuner, C., Bygrave, L. A., Docksey, C., ja Drechsler, L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, lk 561. Andmekaitset käsitlevates õigusnormides sätestatud põhimõtted ja kohustused peaksid pigem põimuma organisatsioonide kultuurikangasse kõikidel tasanditel, kui pidada neid teatavaks õiguslike nõuete kogumiks, mille täitmist õigusosakond peab kontrollima.

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

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

[11] Seepärast – nagu näeme – saab esimesele ja neljandale eelotsuse küsimusele vastata ainult eitavalt. Määruse sätetest ei saa tuletada mingit automaatsust: ei piisa ainuüksi asjaolust, et on aset leidnud isikuandmete avalikustamine, asumaks seisukohale, et võetud tehnilised ja korralduslikud meetmed ei ole asjakohased, kuid ei piisa ka asjaolust, et see avalikustamine leidis aset väljapoole vastutava töötleja organisatsiooni ja kontrolli jäävate isikute tegevuse tagajärjel, et teda vastutusest vabastada.

28. Artikkel 24 ei sisalda „asjakohaste“ meetmete ammendavat loetelu: neid tuleb hinnata igal üksikul juhul eraldi. See on kooskõlas määruse filosoofiaga, mis näitab, et on soovitav, et menetlused, mis tuleb kehtestada, valitakse konkreetse olukorra hoolika hindamise tulemusena, mis on nii konkreetne, et saab olla võimalikult tõhus. [12]

B. Esimene eelotsuse küsimus

29. Esimese küsimusega soovib eelotsusetaotluse esitanud kohus sisuliselt teada, kas määruse artikleid 24 ja 32 tuleb tõlgendada nii, et „isikuandmetega seotud rikkumise“ esinemisest niisugusena, nagu see on määratletud artikli 4 punktis 12, piisab iseenesest järeldamaks, et vastutava töötleja võetud tehnilised ja korralduslikud meetmed ei olnud andmekaitse tagamisel „asjakohased“.

30. Määruse artiklite 24 ja 32 tekstist ilmneb, et kui vastutav töötleja valib tehnilisi ja korralduslikke meetmeid, mille ta peab määruse järgimiseks võtma, on ta kohustatud arvesse võtma teatavat hulka hindamistegureid, mis on nendes artiklites loetletud ja mida on eespool meenutatud.

31. Vastutaval töötlejal on teatav kaalutlusruum kõige asjakohasemate meetmete kindlaksmääramisel enda konkreetsest olukorrast lähtudes, kuid selle valiku puhul on siiski võimalik kohtulik kontroll selle üle, kas rakendatavad meetmed on kooskõlas kõigi määruses sätestatud kohustuste ja eesmärkidega.

32. Konkreetselt turvameetmete puhul kohustab artikli 32 lõige 1 vastutavat töötlejat arvesse võtma „teaduse ja tehnoloogia viimast arengut“. See tähendab, et võetavate meetmete tehnoloogilist taset on piiratud sellega, mis on mõistlikult võimalik hetkel, mil meetmeid võetakse: see, kas meede suudab ohu ära hoida, on seega vastavuses lahendustega, mida pakub selle hetke teaduse, tehnika, tehnoloogia ja teadusuuringute arengutase, võttes – nagu näeme – arvesse ka rakendamise kulusid.

33. Teatavad meetmed võivad olla teataval hetkel „asjakohased“ ja sellest hoolimata võivad nendest jagu saada küberkurjategijad, kes kasutavad väga arenenud vahendeid, mille abil on võimalik mööda hiilida ka turvameetmetest, mis vastavad teaduse ja tehnoloogia viimasele arengule.

34. Teisalt näib ebaloogiline arvata, et liidu seadusandjal oli kavatsus kehtestada vastutavale töötlejale kohustus hoida ära isikuandmete ükskõik missugune rikkumine, olenemata hoolikusest turvameetmete eelneval kindlaksmääramisel. [13]

35. Nagu eespool märgitud, ei ole selles määruses kaugeltki silmas peetud automaatsust, nõudes vastutava töötleja suurt vastutust, mis ei saa siiski viia selleni, et viimasel on võimatu tõendada, et ta on talle kehtestatud kohustused täitnud nõuetekohaselt.

[12] Bolognini, L., ja Pelino, E., *Codice della disciplina privacy*, Giuffrè, 2019, lk 201. Liidu seadusandja on läinud seega kaugemale töötlemise turvalisuse kontseptsioonist, mis põhineb ette kindlaks määratud turvameetmete olemasolul, ning on valinud rahvusvahelistele standarditele omase metodoloogia, mis seisneb *ohupõhises* infosüsteemide haldamises: ta on näinud ette, et tuleb kindlaks määrata ohtude leevendamise meetmed, mis lähevad kaugemale ette kindlaks määratud ja üldiselt kohaldatavate meetmete *checklist*'ist. Tuleb siiski lähtuda rahvusvahelistest suunistest ja standarditest. Niisuguse ohtude hindamise tulemus muutub seega siduvaks hetkel, mil organisatsoon teeb otsuseid, et vähendada kindlaks tehtud ohte, muutes end *vastutavaks*.

[13] Asjakohasuse kontseptsioon näitab üheselt soovi mitte pidada asjakohaseks kõiki tehnilisi ja korralduslikke meetmeid, mis on teoreetiliselt võimalikud. Vt selle kohta Gambini, M., *Responsabilità e risarcimento nel trattamento dei dati personali*, Cuffaro, V., D'Orazio, R., ja Ricciuto, V., *I dati personali nel diritto europeo, Giappichelli*, 2019, lk 1059.

36. Lisaks on artikli 32 lõikes 1 ette nähtud, et arvesse tuleb võtta – nagu märgitud – asjaomaste tehniliste ja korralduslike meetmete „rakendamise kulusid“. Sellest järeldub, et niisuguste meetmete asjakohasuse hindamine peab põhinema kaalumisel, kummad on ülekaalus, kas andmesubjekti huvid, mis tavaliselt eeldavad kõrgemat kaitstuse taset, või vastutava töötleja ärihuvid ja tehnoloogiline suutlikkus, mis mõnikord tähendab madalamat kaitstuse taset. Sellise kaalumise puhul tuleb järgida proportsionaalsuse üldpõhimõtte nõudeid.

37. Sellele tuleb nüüd süstemaatilist tõlgendamist silmas pidades lisada, et seadusandja on käsitlenud võimalust, et niisugused süsteemi sisse häkkimised toimuvad; artikli 32 lõike 1 punktis c on väljapakutud meetmete hulgas nimetatud võimet taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele füüsilise või tehnilise vahejuhtumi korral. Seda võimet ei oleks mõtet ette näha turvameetmete hulgas, mis tagavad ohule vastava turvalisuse taseme, kui arvataks, et ainuüksi süsteemi sisse häkkimine ise kujutab endast tõendit sellest, et need meetmed ei olnud asjakohased.

C. Teine eelotsuse küsimus

38. Teise küsimusega soovib eelotsusetaotluse esitanud kohus sisuliselt teada, missugused peavad olema kohtuliku kontrolli ese ja ulatus selle kontrollimisel, kas vastutava töötleja võetud tehnilised ja korralduslikud meetmed olid asjakohased määruse artikli 32 tähenduses.

39. Arvestades, kui mitmekesised on olukorrad, mis praktikas ette tulla võivad, ei ole määruses – nagu märgitud – sätestatud siduvaid õigusnorme nende tehniliste ja korralduslike meetmete kindlaksmääramiseks, mille vastutav töötleja peab võtma, et täita määruse nõudeid. Võetud meetmete asjakohasust tuleb seega hinnata konkreetselt, kontrollides, kas konkreetsed meetmed olid sobivad, et hoida oht mõistlikult ära ja vähendada rikkumise negatiivseid tagajärgi miinimumini.

40. Kuigi on kahtlemata õige, et niisuguste meetmete valik ja rakendamine sõltuvad vastutava töötleja subjektiivsest hinnangust, sest määruses nimetatud meetmed on üksnes näited, ei saa kohus piirduda selle kontrollimisega, kas vastutav töötleja on järginud artiklitest 24 ja 32 tulenevaid kohustusi, st kohustust näha (formaalselt) ette teatavad tehnilised ja korralduslikud meetmed. Ta peab konkreetselt analüüsima nende meetmete sisu, nende rakendamise viisi ja nende praktilisi tagajärgi tõendite põhjal, mis on tema käsutuses, ja arvestades konkreetse juhtumi asjaolusid. Nagu Portugali valitsus on õigesti märkinud, „näib viis, kuidas ta on täitnud oma kohustusi, olevat lahutamatu võetud meetmete sisust selle tõendamisel, et arvestades andmete konkreetset töötlemist (töötlemise laadi, ulatust, konteksti ja eesmärke), teaduse ja tehnoloogia viimast arengut ning meetmete rakendamise kulusid, samuti ohte kodanike õigustele ja vabadustele, on vastutav töötleja võtnud kõik vajalikud ja asjakohased meetmed, et tagada ohule vastav turvalisuse tase“. [14]

41. Seepärast tuleb kohtuliku kontrolli puhul arvesse võtta kõiki artiklites 24 ja 32 nimetatud tegureid, milles on – nagu märgitud – loetletud teatav hulk kriteeriume asjakohasuse hindamisel ning toodud näiteid meetmetest, mida võib lugeda asjakohaseks. Lisaks, nagu on toonitanud komisjon ja kõik teise küsimuse kohta seisukohti esitanud liikmesriigid, on artikli 32 lõigetes 1–3 rõhutatud vajadust „[tagada] ohule vastav turvalisuse tase“, näidates ära muud seejuures

[14] Kirjalikud seisukohad, punkt 31.

asjakohased tegurid, näiteks selle, kui vastutav töötleja võtab vastu heakskiidetud toimimisjuhendi või sertifitseerimismehhanismi, nagu on vastavalt ette nähtud määruse artiklites 40 ja 42.

42. Toimimisjuhendite või sertifitseerimismehhanismide vastuvõtmine võib olla hindamisel vajalik asjaolu, mis võimaldab täita tõendamiskoormise ja teostada sellega seotud kohtulikku kontrolli. Tuleb siiski täpsustada, et ei piisa sellest, kui vastutav töötleja liitub toimimisjuhendiga, vaid ta peab tõendama, et on võtnud konkreetselt selles ette nähtud meetmed kooskõlas vastutuse põhimõttega. Sertifitseerimine seevastu kujutab endast „juba iseenesest tõendit, et läbi viidud töötlemised olid määrusega kooskõlas, ehkki praktikas on võimalik, et tegevus ei ole sertifitseerimisega vastavuses“. [15]

43. Viimasena on tarvis märkida, et niisugused meetmed tuleb vajaduse korral uuesti läbi vaadata ja ajakohastada, nagu on nähtud ette artikli 24 lõikes 1. Ja ka seda hindab liikmesriigi kohus. Määruse artikli 32 lõikega 1 [16] on vastutavale töötlejale nimelt kehtestatud pideva kontrolli ja seire kohustus, mis on ennetav ja järgneb töötlemistoimingutele, kuid ka võetud meetmete säilitamise ja võimaliku ajakohustamise kohustus eesmärgiga ennetada rikkumisi või vastaval juhul piirata nende tagajärgi.

44. Kaldun siiski välistama võimaluse, et tulevane kohtuotsus sisaldab niisugust sisuliste asjaolude loetelu, nagu on välja pakkunud Portugali valitsus. [17] See võib anda alust vastuolulisteks tõlgendusteks, sest see loetelu ei saa ilmselgelt kunagi olla ammendav.

D. Kolmas eelotsuse küsimus

45. Kolmanda küsimuse esimese osaga palub eelotsusetaotluse esitanud kohus Euroopa Kohtul sisuliselt kindlaks määrata, kas võttes arvesse vastutuse põhimõtet, mis on sätestatud määruse artikli 5 lõikes 2 ja artiklis 24 koostoimes põhjendusega 74 [18], lasub artikli 82 alusel esitatud kahju esitamise nõude raames tõendamiskoormis selle tõendamisel, et võetud tehnilised ja korralduslikud meetmed olid asjakohased artikli 32 tähenduses, andmete vastutaval töötlejal.

46. Eeltoodud kaalutlused võimaldavad mul anda sellele küsimusele ülevaatlikult jaatava vastuse.

47. Määruse sõnastus, kontekst ja eesmärgid kõnelevad nimelt üheselt sellest, et tõendamiskoormis lasub vastutaval töötlejal.

[15] Gambini, M., *Responsabilità*, *op. cit.*, lk 1067. Sertifikaadi omamine avaldub seepärast tõendamiskoormise ümberpööramises vastutava töötleja kasuks, et viimasel on nii lihtsam tõendada, et ta on tegutsenud määruses sätestatud kohustusi järgides.

[16] Sätestades punktis d sõnaselgelt, et hinnang asjakohasusele hõlmab võetud meetmete tõhusust ning et neid tuleb korrapäraselt testida ja hinnata nii esialgses etapis kui ka perioodiliselt, et tagada töötlemise liikide tegelik turvalisus, ükskõik missugune on riskitase nende puhul, ning nähes ka punktis c sõnaselgelt ette, et võetud tehnilised ja korralduslikud meetmed peavad suutma taastada õigeaegselt isikuandmete kättesaadavuse ja juurdepääsu andmetele füüsilise või tehnilise vahejuhtumi korral. Vt Gambini, M., *Responsabilità*, *op. cit.*, lk 1064 ja 1065.

[17] Kirjalike seisukohtade punkt 30: „vastutav töötleja on kohustatud tõendama, kuidas ta on hinnanud kõiki asjaomase töötlemisega seotud tegureid ja asjaolusid ning konkreetselt läbiviidud ohuanalüüsi tulemust, tuvastatud ohte, nende ohtude leevendamiseks leitud konkreetseid meetmeid, valitud lahenduste põhjendatust turul olemasolevate tehnoloogiliste lahenduste seisukohast, meetmete tõhusust, seost tehniliste ja korralduslike meetmete vahel, andmeid töötlevate töötajate koolitamist, andmetöötlustoimingute sisseostmise esinemist, sh infotehnoloogiasüsteemide arendamine ja hooldamine, ning vastutava töötleja kontrolli ja töötlejatele antud täpsete juhiste olemasolu isikuandmete kaitse üldmääruse artikli 28 tähenduses selle üle/kohta, kuidas töötlejad isikuandmeid töötlevad, kuidas on hinnatud kommunikatsiooni- ja infosüsteemide tugiinfrastruktuuri ning kuidas on klassifitseeritud andmesubjektide õigusi ja vabadusi ähvardava ohu tase“.

[18] Põhjenduses 74 on märgitud: „Tuleks kehtestada vastutava töötleja vastutus tema poolt ja tema nimel toimuva isikuandmete mis tahes töötlemise eest. Eelkõige peaks vastutav töötleja olema kohustatud rakendama asjakohaseid ja tõhusaid meetmeid ning olema võimeline tõendama isikuandmete töötlemise toimingute kooskõla käesoleva määrusega, sealhulgas meetmete tõhusust. Nende meetmete puhul tuleks arvestada töötlemise laadi, ulatust, konteksti ja eesmärke ning ohtu füüsiliste isikute õigustele ja vabadustele.“

48. Määruse mitme sätte sõnastusest ilmneb, et vastutav töötleja peab olema „võimeline“ või „suutma“ „tõendada“, et on järginud määruses sätestatud kohustusi ning konkreetselt võtnud selleks kõik asjakohased meetmed, nagu on märgitud põhjenduses 74, artikli 5 lõikes 2 ja artikli 24 lõikes 1. Nagu on rõhutanud Portugali valitsus, on põhjenduses 74 täpsustatud, et nõnda vastutavale töötlejale kehtestatud tõendamiskoormis peab hõlmama „meetmete tõhusust“.

49. Mulle tundub, et niisugust grammatilist tõlgendust kinnitavad järgnevad praktilised ja teleoloogilised kaalutlused.

50. Mis puudutab tõendamiskoormise jaotumist artikli 82 alusel esitatud kahju hüvitamise nõude raames, siis andmesubjekt, kes on vastutava töötleja vastu nõude esitanud, peab esiteks tõendama, et on leidnud aset määruse rikkumine; teiseks, et ta on kandnud kahju, ning kolmandaks, et eelmise kahe elemendi vahel eksisteerib põhjuslik seos, nagu on märgitud kõikides kirjalikes seisukohtades viienda eelotsuse küsimuse kohta. Tegemist on kolme kumulatiivse tingimusega, nagu ilmneb ka Euroopa Kohtu ja Üldkohtu väljakujunenud praktikast liidu lepinguvälise vastutuse kontekstis.[19]

51. Leian siiski, et kassaatori kohustus tõendada määruse rikkumist ei saa olla nii ulatuslik, et ta peab tõendama, mille poolest ei ole vastutava töötleja tehnilised ja korralduslikud meetmed asjakohased artiklite 24 ja 32 tähenduses.

52. Nagu rõhutab komisjon, on niisuguseid tõendeid praktikas tihti pea võimatu esitada, sest andmesubjektidel ei ole tavaliselt ei piisavaid teadmisi nende meetmete analüüsimiseks ega võimalust tutvuda kogu teabega, mis on asjaomase vastutava töötleja valduses, eelkõige mis puudutab töötlemise turvalisuse tagamiseks kasutatud meetodeid. Lisaks võib vastutav töötleja mõnikord väita, et ta keeldub neid faktilisi asjaolusid andmesubjektidele avaldamast õiguspärasel põhjusel, milleks on mitte avalikustada oma siseasju või ka ametisaladusega hõlmatud asjaolud, nende hulgas just turvalisega seotud põhjused.

53. Seepärast, kui asuda seisukohale, et tõendamiskoormis lasub andmesubjektil, on praktikas tulemuseks see, et artikli 82 lõikes 1 ette nähtud nõudeõigus kaotaks suure osa oma ulatusest. Minu arvates ei oleks see kooskõlas EL seadusandja kavatsustega, sest määrust andes soovis see seadusandja tugevdada andmesubjektide õigusi ja volitatud töötleja kohustusi võrreldes direktiiviga 95/46, mis selle määrusega asendati. Seetõttu on loogilisem ja õiguslikult vastuvõetav, et vastutav töötleja on kohustatud oma vastuse raames kahju hüvitamise nõudele tõendama, et ta on järginud määruse artiklitest 24 ja 32 tulenevaid kohustusi, sest on võtnud tõesti asjakohased meetmed.

54. Kolmanda küsimuse teise osaga palub eelotsusetaotluse esitanud kohus Euroopa Kohtul sisuliselt täpsustada, kas kohtuekspertiisi võib pidada vajalikuks ja piisavaks tõendiks selle hindamisel, kas isikuandmete vastutava töötleja tehnilised ja korralduslikud meetmed olid asjakohased olukorras, kus isikuandmetele pääseti ilma loata juurde ja need avaldati häkkerite rünnaku tulemusena.

[19] Vt konkreetselt Euroopa Kohtu 5. septembri 2019. aasta kohtuotsus Euroopa Liit *vs*. Guardian Europe ja Guardian Europe *vs*. Euroopa Liit (C-447/17 P ja C-479/17 P, EU:C:2019:672, punkt 147) ning 28. oktoobri 2021. aasta kohtuotsus Vialto Consulting *vs*. komisjon (C-650/19 P, EU:C:2021:879, punkt 138) ning Üldkohtu 13. jaanuari 2021. aasta kohtuotsus Helbert *vs*. EUIPO (T-548/18, EU:T:2021:4, punkt 116) ja 29. septembri 2021. aasta kohtuotsus Kočner *vs*. Europol (T-528/20, ei avaldata, EU:T:2021:631, punkt 61), milles on meenutatud, et täidetud peab olema kolm tingimust: „liidu institutsioonile etteheidetava tegevuse õigusvastasus, kahju tegelik tekkimine ning põhjuslik seos institutsiooni tegevuse ja viidatud kahju vahel“.

55. Nagu on (sisuliselt) rõhutanud ka Bulgaaria ja Itaalia valitsus, Iirimaa ja komisjon, olen arvamusel, et vastus nendele küsimustele peab rajanema meie väljakujunenud kohtupraktikal, mille kohaselt tuleb vastavasisuliste liidu õigusnormide puudumise korral liikmesriikide menetlusautonoomia põhimõtte kohaselt iga liikmesriigi õiguskorras kehtestada menetluskord isikutele liidu õigusest tulenevate õiguste kaitse tagamiseks, kuid selline kord ei tohi olla ebasoodsam kui sarnaste riigisiseste olukordade suhtes kohaldatav kord (võrdväärsuse põhimõte) ega muuta liidu õigusega antud õiguste kasutamist praktiliselt võimatuks ega ülemäära raskeks (tõhususe põhimõte).

56. Käsitletaval juhul märgin, et määrus ei sisalda ühtegi sätet, millega määrataks kindlaks lubatavad tõendite kogumise meetodid ja nende tõenduslik väärtus, eelkõige mis puudutab menetlustoiminguid (nagu ekspertiis), mille liikmesriigi kohtud võivad määrata või peavad määrama, et hinnata, kas isikuandmete vastutav töötleja on võtnud asjakohased meetmed määruse tähenduses. Seepärast leian, et kuna selles valdkonnas puuduvad ühtlustatud õigusnormid, määratakse menetluskord kindlaks iga liikmesriigi siseses õiguskorras, tingimusel et järgitakse võrdväärsuse ja tõhususe põhimõtet.

57. Nimetatud „tõhususe põhimõtet“, mis eeldab, et sõltumatu kohus peab läbi viima erapooletu hindamise, võidakse rikkuda, kui omadussõna „piisav“ tuleks mõista tähenduses, mille näib sellele omistavat eelotsusetaotluse esitanud kohus: ekspertiisi põhjal võib automaatselt järeldada, et vastutava töötleja võetud meetmed on asjakohased.[20]

E. Neljas eelotsuse küsimus

58. Neljanda küsimusega soovib eelotsusetaotluse esitanud kohus sisuliselt teada, kas määruse artikli 82 lõiget 3 tuleb tõlgendada nii, et määruse rikkumise korral (mis seisneb – nagu käsitletaval juhul – isikuandmete „loata avalikustamises“ või „loata juurdepääsus“ neile artikli 4 punkti 12 tähenduses) sellise isiku poolt, kes ei ole nende isikuandmete vastutava töötleja töötaja ega allu vastutava töötleja kontrollile, kujutab see rikkumine endast sündmust, mille eest ei ole mingil viisil vastutav töötleja, ja seega tema vastutusest vabastamise alust artikli 82 lõike 3 tähenduses.

59. Vastus neljandale küsimusele tuleneb otseselt sellest, mida on eespool märgitud määruse üldise filosoofia kohta: mingit automaatsust ette nähtud ei ole ning seega ei vabasta ainuüksi asjaolu, et isikuandmete loata avalikustamine ja loata juurdepääs nendele said võimalikuks isikute läbi, kes jäävad väljapoole sfääri, mida kontrollib vastutav töötleja, teda vastutusest.

60. Esiteks tuleb grammatilise tõlgenduse järgi märkida, et ei artikli 82 lõikes 3 ega põhjenduses 146 ei ole sätestatud konkreetseid tingimusi, mida on võimalik täita selleks, et vastutav töötleja vabastataks vastutusest, v.a kui ta tõendab, et „ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest“. Sellest sõnastusest ilmneb esiteks, et vastutava töötleja võib vastutusest vabastada ainult siis, kui ta tõendab, et asjaomase kahju põhjustanud sündmuse eest ei saa pidada vastutavaks teda, ning teiseks, et selles sättes nõutud tõendamise tase on kõrge, sest kasutatud on väljendit „mingil viisil“, nagu on rõhutanud komisjon.[21]

[20] Kirjalikud seisukohad, punkt 39.

[21] Vastavalt Euroopa Kohtu väljakujunenud praktikale, mille kohaselt tuleb üldreegli erandeid tõlgendada kitsalt, on artikli 82 lõikes 3 ette nähtud vastutuse erandit seega tarvis tõlgendada kitsalt. Vt analoogia alusel 15. oktoobri 2020. aasta kohtuotsus Association française des usagers de banques (C-778/18, EU:C:2020:831, punkt 53) ning 5. aprilli 2022. aasta kohtuotsus Commissioner of An Garda Síochána jt (C-140/20, EU:C:2022:258, punkt 40).

61. Artiklis 82 ja üldisemalt kogu määruses ette nähtud vastutuse regulatsiooni on põhjalikult käsitletud erinevate liikmesriikide õigusteoorias. See regulatsioon sisaldab nimelt traditsioonilisi elemente, mis on iseloomulikud lepinguvälisele vastutusele, kuid ka elemente, mis lähendavad seda sätete ülesehituses lepingulisele vastutusele või lausa teatavas vormis objektiivsele vastutusele andmetöötlustoimingute olemusliku ohtlikkuse tõttu. See siin ei ole õige koht teha ülevaade arutatust, kuid minu arvates ei ole artiklis 82 kindlaks määratud objektiivse vastutuse regulatsiooni. [22]

62. Isikuandmetega seotud rikkumisega põhjustatud kahju ei saa olla süüline tagajärg, mis kaasneb sellega, kui jäeti võtmata tehnilised ja korralduslikud meetmed, mis on mõistlikud ja suudavad selle kahju igal juhul ära hoida, võttes arvesse töötlemistoimingutega seotud ohte isikute õigustele ja vabadustele. Need ohud muudavad kahju ärahoidmise ja ennetamise kohustuse rangemaks, laiendades vastutaval töötlejal lasuvat hoolsuskohustust. Seepärast võib vastutavate töötlejate suhtes kohaldatavate toimimisnõuete tõlgendamisel koostoimes kahju põhjustaja kohustusega esitada tõend, mis ta vastutusest vabastab, tuletada argumendi, et tunnustatakse raskendatud süülist vastutust, mida eeldatakse määruse artiklis 82 ette nähtud juhtumil, milleks on vastutus isikuandmete ebaseadusliku töötlemise eest. [23]

63. Sellest järeldub, et vastutaval töötlejal on võimalik esitada tõend, mis ta vastutusest vabastab (objektiivse vastutuse korral ei ole võimalik). Tõendamiskoormise jaotumise alal on määruse artikli 82 lõikega 3 kehtestatud regulatsioon, mis on soodus kahju kannatanule, sätestades tõendamiskoormise ümberpööramise kahju põhjustanu süü küsimuses, [24] täielikus kooskõlas eespool mainitud tõendamiskoormise ümberpööramisega võetud meetmete asjakohasuse küsimuses. Seadusandja näitab nii, et oli teadlik ohtudest, mida peidab endas nõustumine tõendamiskoormise teistsuguse jaotumisega; et see, kui kohustada kahju kandnud füüsilist isikut tõendama kahju põhjustanu süüd, viiks selleni, et tema seisund muudetakse liiga raskeks ja tegelikkuses rikutakse seega kahju hüvitamise kui kaitse toimimist uute tehnoloogiate kasutamisega seotud õigusnormide raamistikus. Andmesubjektile võib olla eriti koormav rekonstrueerida kahju tekitamise viis ja sellele ligi pääseda ning seega vastutava töötleja süüd tõendada. Ja vastupidi, vastutav töötleja on paremas olukorras, et esitada vastutusest vabastav tõend, mis kinnitab, et ta ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest. [25]

64. Vastutav töötleja peab ka tõendama – kooskõlas eespool kirjeldatud vastutuse põhimõttega –, et tegi kõik võimaliku, et taastada õigeaegselt isikuandmete kättesaadavus ja juurdepääs andmetele.

65. Naastes eelotsusetaotluse esitanud kohtu küsimuse juurde, st kas eespool vastutava töötleja vastutuse laadi kohta märgitu põhjal võib – nagu öeldud – vastutava töötleja vastutusest vabastada, kui ta tõendab, et rikkumise põhjuse eest ei saa kuidagi vastutavaks pidada teda, siis niisuguseks tõendiks ei saa pidada üksnes asjaolu, et sündmuse kutsus esile isik, kes jääb väljapoole tema kontrollisfääri.

[22] Tsiviilvastutust kaldutakse kvalifitseerima objektiivseks alati, kui õigussubjekt on kohustatud võtma kõik teoreetiliselt võimalikud meetmed kahju ärahoidmiseks, olenemata sellest, kas ta oli kahjust ja selle majanduslikust ulatusest teadlik. Ja vastupidi, kui õigussubjekt on kohustatud võtma meetmed, mida tavapäraselt järgib selles majandussektoris tegutsev ettevõtja, et säilitada turvalisus ja hoida ära kahju, mis läbiviidava tegevusega võib kaasneda, kaldub see, kui teda peetakse selle kahju eest vastutavaks, viitama vastutuse regulatsioonile, mis on ette nähtud konkreetse süü korral. Gambini, M., *Responsabilità*, *op. cit.*, lk 1055.

[23] Gambini, M., *Responsabilità*, *op. cit.*, lk 1059. Sama mõtte, st arvamuse kohta, et seda, et võeti asjakohased meetmed, ei saa tõendada lihtsalt väitega, et ilmutati nii suurt hoolt kui võimalik, vaid tuleb tõendada faktilist asjaolu, et kahju on põhjustatud väljastpoolt ning seda ei saanud ette näha ega vältida, nagu on iseloomulik juhuslikule sündmusele ja vääramatule jõule, vt Sica, S., *Sub art. 82*, D'Orazio, R., Finocchiaro, G., Pollicino, O., ja Resta, G., *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „*kui ta tõendab*, et ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest" (artikli 82 lõige 3).

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

66. Kui vastutavale töötlejale saab osaks küberkurjategijate rünnak, võib sündmust, mis kahju tekitas, pidada sündmuseks, mille eest ei saa pidada vastutavaks vastutavat töötlejat, kuid ei ole välistatud, et selle küberrünnakuni viis andmete vastutava töötleja hooletus, hõlbustades seda rünnakut, sest puudusid isikuandmete turbe meetmed, mida vastutav töötaja peab võtma, või need ei olnud asjakohased. Tegemist on hinnangutega faktilistele asjaoludele, mis on igal juhtumil erinevad ja mida peab hindama liikmesriigi kohus, lähtudes talle esitatud tõenditest.

67. Pealegi näitab ühine kogemus, et rünnakud väljastpoolt avalik-õiguslike ja eraõiguslike isikute süsteemidele, kus on suur hulk isikuandmeid, on juba ammu palju sagedasemad kui rünnakud seestpoolt. Seepärast peab vastutav töötleja ette nägema asjakohased meetmed just oma süsteemide kaitsmiseks väljastpoolt tulevate rünnakute vastu.

68. Viimaseks tuleb teleoloogilisest seisukohast märkida, et määrusega taotletakse kõrgetasemelise kaitse eesmärki. Selle kohta on Euroopa Kohus juba rõhutanud, et määruse artikli 1 lõikest 2, tõlgendatuna koostoimes põhjendustega 10, 11 ja 13, tuleneb, et selle määrusega on kehtestatud liidu institutsioonidele, organitele ja asutustele ning liikmesriikide pädevatele asutustele kohustus tagada ELTL artiklis 16 ja harta artiklis 8 ette nähtud isikuandme kaitsega seotud õiguste kaitse kõrge tase. [26]

69. Kui Euroopa Kohus peaks valima tõlgenduse, mille kohaselt tuleb juhul, kui määruse rikkumise on pannud toime kolmas isik, vastutav töötleja automaatselt artikli 82 lõike 3 alusel vastutusest vabastada, oleks niisugusel tõlgendusel tagajärg, mis on vastuolus selle õigusakti kaitse-eesmärgiga, sest see nõrgendaks andmesubjektide õigusi, kuna piiraks seda vastutust juhtudega, mil rikkumise eest saab pidada vastutavaks isikuid, kes on vastutava töötleja töötajad ja/või tema kontrolli all.

F. Viies eelotsuse küsimus

70. Viienda küsimusega palub liikmesriigi kohus Euroopa Kohtul sisuliselt tõlgendada mõistet „mittevaraline kahju“ (määruses „mittemateriaalne“) määruse artikli 82 tähenduses. Konkreetselt küsib ta, kas määruse artikli 82 lõikeid 1 ja 2 tuleb koostoimes selle põhjendustega 85 ja 146 [27] tõlgendada nii, et olukorras, kus määruse rikkumine seisnes loata juurdepääsus isikuandmetele ja nende loata avalikustamises küberkurjategijate poolt, võib asjaolu, et andmesubjekt kardab oma isikuandmete kuritarvitamist tulevikus, juba iseenesest kujutada endast (mittevaralist) kahju, mis annab õiguse hüvitisele.

71. Ei artiklis 82 ega kahju hüvitamist käsitletavates põhjendustes ei ole esitatud selgitust selles küsimuses, kuid nendest võib leida pidepunkte, mis tulevad analüüsimisel kasuks: mittemateriaalne (ehk mittevaraline) kahju võidakse hüvitada lisaks materiaalsele (varalisele); määruse rikkumisega ei kaasne automaatselt kahju, mida on selle „tulemusel“ kantud, ehk täpsemalt „võib“ isikuandmete rikkumine „põhjustada“ füüsilise, materiaalse või mittemateriaalse

[26] Vt selle kohta 15. juuni 2021. aasta kohtuotsus Facebook Ireland jt (C-645/19, EU:C:2021:483, punktid 43 ning 44).

[27] Põhjenduses 85 on märgitud: „Isikuandmetega seotud rikkumine, kui seda asjakohaselt ja õigeaegselt ei käsitleta, võib põhjustada füüsilistele isikutele füüsilise, materiaalse või mittemateriaalse kahju[…]“. Põhjenduses 146 on juhitud tähelepanu: „Vastutav töötleja või volitatud töötleja peaks hüvitama igasuguse kahju, mida füüsilisele isikule võib põhjustada töötlemine, mis ei ole käesoleva määrusega kooskõlas. Vastutav töötleja või volitatud töötleja tuleks sellest vastutusest vabastada, kui ta tõendab, et ta ei ole kahju eest mingil viisil vastutav. Kahju mõistet tuleks Euroopa Kohtu praktikat arvestades tõlgendada laialt ja sellisel viisil, mis kajastab täielikult käesoleva määruse eesmärke. See ei mõjuta muude liidu või liikmesriigi õiguses sätestatud normide rikkumisest tuleneva kahju eest esitatavaid nõudeid. […] Andmesubjektid peaksid saama täieliku ja tõhusa hüvitise kahju eest, mida nad on kandnud. […]“.

kahju füüsilistele isikutele; mõistet „kahju“ võib tõlgendada „laialt“ Euroopa Kohtu praktikast lähtudes, st nii, et järgitakse täielikult määruse eesmärke; hüvitis kahju eest, mida isik on „kandnud“, peab olema „täielik ja tõhus“.

72. Juba määruse sätete grammatiline sisu ei jäta mingit ruumi oletusele, et tegemist võiks olla kahjuga *in re ipsa*: määruses ette nähtud tsiviilvastutuse põhieesmärk on andmesubjekti rahuldada just kantud kahju „täieliku ja tõhusa“ hüvitisega ning seega taastada selle õigusliku olukorra tasakaal, mida õiguse rikkumisega negatiivses suunas muudeti. [28]

73. Teisalt, ka süstemaatilisest seisukohast, nagu konkurentsiõiguses, on määruses ette nähtud kaks kaitsesammast: üks avalik-õiguslik, milles on ette nähtud karistused määruse sätete rikkumise puhuks; teine eraõiguslik, milles on just ette nähtud lepinguvälist laadi tsiviilvastutus, mille võib kvalifitseerida raskendatud vastutuseks eeldatava süü tõttu ja millel on eespool näidatud omadused, sh ka seoses tõendiga, mis vastutusest vabastab. [29]

74. Seepärast ei tohi mõiste „(mittevaraline) kahju“ [30] lai tõlgendus minna nii kaugele, et tuleb asuda seisukohale, et seadusandja on loobunud vajadusest, et esineks tõeline „kahju“.

75. Tegelik sisuline probleem on see, et kas olukorras, kus rikkumise ja põhjusliku seose esinemine on juba kindlaks tehtud, võib tekkida õigus hüvitisele ainuüksi andmesubjekti põhjendatud mure, ärevuse või hirmu tõttu, et tema isikuandmeid kuritarvitatakse tulevikus, kui see kuritarvitamine ei ole tuvastatud ja/või andmesubjekt ei ole kandnud mingit hilisemat kahju.

76. Euroopa Kohtu väljakujunenud praktika kohaselt tuleb mõisteid, mida on kasutatud liidu õigusnormis, milles ei ole õigusnormi tähenduse ja ulatuse kindlaksmääramise osas viidatud sõnaselgelt liikmesriikide õigusele, kogu liidus tõlgendada autonoomselt ja ühetaoliselt ning niisuguse tõlgendamise käigus ei tule arvestada mitte üksnes sätte sõnastust, vaid ka konteksti ning selle õigusakti eesmärke, mille osaks säte on. [31]

77. Euroopa Kohus ei ole – nagu meenutab kohtujurist Campos Sánchez-Bordona [32] – välja töötanud „kahju“ üldist määratlust, mis oleks ühtemoodi kohaldatav ükskõik missuguses kontekstis [33]. Mis puudutab mittevaralist kahju, siis Euroopa Kohtu praktikast võib järeldada, et

[28] Vt kohtujurist Campos Sánchez-Bordona viidatud ettepanek, punkt 29 ja 11. joonealune märkus. Samas ettepanekus võtab kohtujurist oma analüüsi grammatilisest, ajaloolisest, kontekstuaalsest ja teleoloogilisest seisukohast õigesti kokku järeldusega, et andmesubjektidele hüvitatav kahju on „karistusmeede“ artikli 82 tähenduses (punktid 27 ja 55), märkides esiteks, et liikmesriikidel „ei ole andmekaitse tagamiseks vaja (ja nad tegelikult ei saagi) VIII peatüki mehhanismide hulgast valida. Rikkumise puhul, mis kahju ei tekita, on andmesubjektil ikkagi (vähemalt) õigus esitada […] kaebus järelevalveasutusele“, ning teiseks, et „[p]ealegi stimuleeriks võimalus ilma igasuguse kahjuta hüvitist saada tõenäoliselt tsiviilõiguslikke vaidlusi, kus nõuded ei ole ehk alati põhjendatud, ning võib seetõttu pärssida huvi andmeid töödelda“ (punktid 54 ja 55).

[29] See, kui ei tunnustata õigust hüvitisele kergete ja mööduvate tunnete või emotsioonide tõttu, mis on seotud töötlemist käsitlevate õigusnormide rikkumisega, ei jäta andmesubjekti seepärast täielikult kaitsest ilma (vt selle kohta kohtujurist Campos Sánchez-Bordona viidatud ettepanek, punkt 115).

[30] Või „laialt“, kui kasutada põhjenduses 146 kasutatud väljendit.

[31] Vt 15. aprilli 2021. aasta kohtuotsus The North of England P & I Association (C-786/19, EU:C:2021:276, punkt 48) ja 10. juuni 2021. aasta kohtuotsus KRONE – Verlag (C-65/20, EU:C:2021:471, punkt 25).

[32] Vt kohtujurist Campos Sánchez-Bordona viidatud ettepanek, punkt 104.

[33] Ega ole ära näidanud tõlgendamismeetodit – autonoomselt või viitega liikmesriikide õiguskordadele –, mida tuleks eelistada: sõltub analüüsitavast teemast. Vt 10. mai 2001. aasta kohtuotsus Veedfald (C-203/99, EU:C:2001:258, punkt 27) defektsete toodete kohta, 6. mai 2010. aasta kohtuotsus Walz (C-63/09, EU:C:2010:251, punkt 21) lennuveoettevõtjate vastutuse kohta ning 10. juuni 2021. aasta kohtuotsus Van Ameyde España (C-923/19, EU:C:2021:475, punkt 37 jj), mis käsitleb tsiviilvastutust liiklusõnnetuste korral.

kui tõlgendatava õigusnormi eesmärk (või üks eesmärke) on isiku või teatud isikute kategooria kaitse,[34] peab kahju mõiste olema lai; kooskõlas selle kriteeriumiga laieneb hüvitamine mittemateriaalsele kahjule, isegi kui seda ei ole tõlgendatavas õigusnormis nimetatud[35].

78. Ehkki Euroopa Kohtu praktika võimaldab väita, et eespool esitatud sõnastuses eksisteerib liidu õiguses mittemateriaalse kahju hüvitamise põhimõte, olen ühel meelel kohtujurist Camposega, et sellest ei saa tuletada reeglit, mille põhjal on *igasugune* mittemateriaalne kahju olenemata selle tõsidusest hüvitatav.[36]

79. Selles kontekstis on asjakohane eristada hüvitatavat mittevaralist kahju ja muid *ebasoodsaid asjaolusid, mis ebaseaduslikkusest tulenevad* ega anna nende väikest ulatust arvestades tingimata õigust hüvitisele.[37]

80. Euroopa Kohus tunnustab seda erinevust, kui ta nimetab raskusi ja ebamugavust kui autonoomset kategooriat võrreldes kahju kategooriaga, mille puhul tuleb tema arvates maksta hüvitist.[38]

81. Empiiriliselt võib täheldada, et ükskõik missugune isikuandmete kaitset käsitleva õigusnormi rikkumine toob kaasa andmesubjekti negatiivse reaktsiooni. Hüvitis, mida tuleb maksta lihtsalt ebamugavustunde eest, et aset leiab veel teine seadusrikkumine, läheb kergesti segi hüvitisega, mida makstakse ilma kahjuta ja mis – nagu nägime – ei näi kujutavat endast määruse artiklis 82 kirjeldatud juhtu.

82. Sellest, et niisugustel asjaoludel nagu põhikohtuasjas on isikuandmete kuritarvitamine ainult võimalik, mitte tegelik, piisab asumaks seisukohale, et andmesubjekt võis kanda määruse rikkumise kaudu mittevaralist kahju, tingimusel et andmesubjekt tõendab, et niisuguse kuritarvitamise hirm on konkreetselt ja tõesti põhjustanud tegeliku ja kindla emotsionaalse kahju.[39]

[34] Näiteks toodete tarbijad või liiklusõnnetuste ohvrid.

[35] Pakettreiside kohta vt 12. märtsi 2002. aasta kohtuotsus Leitner (C-168/00, EU:C:2002:163), mootorsõiduki kasutamisega kaasneva tsiviilvastutuse kohta vt 24. oktoobri 2013. aasta kohtuotsus Haasová (C-22/12, EU:C:2013:692, punktid 47 ja 50), 24. oktoobri 2013. aasta kohtuotsus Drozdovs (C-277/12, EU:C:2013:685, punkt 40) ning 23. jaanuari 2014. aasta kohtuotsus Petillo (C-371/12, EU:C:2014:26, punkt 35).

[36] Vt kohtujurist Campos Sánchez-Bordona viidatud ettepanek, punkt 105. Euroopa Kohus on näiteks nõustunud, et liidu õigusnormidega on kooskõlas riigisisene seadus, milles on hüvitise arvutamisel õnnetuses saadud kehavigastustega seotud mittevaraliste kahjude vahel vahet tehtud olenevalt õnnetuse põhjusest; vt 23. jaanuari 2014. aasta kohtuotsuse Petillo (C-371/12, EU:C:2014:26) resolutsioon: liidu õigusega „ei ole vastuolus niisugused siseriiklikud õigusnormid, […] mis näevad ette liiklusõnnetustest põhjustatud kergetest kehavigastustest tuleneva mittevaralise kahju hüvitamise erikorra, piirates selle kahju eest ette nähtud hüvitist võrreldes hüvitisega, mida peetakse kohaseks muudel põhjustel kui niisuguste õnnetuste tõttu tekkinud samasuguse kahju puhul“.

[37] Niisugust vahetegemist võib kohata mõnes liikmesriigi kohtu määruses, sest see käib ühiskonnaeluga vältimatult kaasas. Hiljuti tegid andmekaitse valdkonnas Itaalias Tribunale di Palermo (Palermo esimese astme kohus) I tsiviilkoda 5. oktoobri 2017. aasta kohtuotsuse nr 5261 ning Corte suprema di cassazione (kassatsioonikohus) VI tsiviilkolleegium kohtumääruse nr 17383/2020. Vt Saksamaal *inter alia* AG Diez, 07.11.2018 – 8 C 130/18; LG Karlsruhe, 02.08.2019 – 8 O 26/19, ja AG Frankfurt am Main, 10.07.2020 – 385 C 155/19 (70). Vt Austrias OGH 6 Ob 56/21k.

[38] Vt 23. oktoobri 2012. aasta kohtuotsus Nelson jt (C-581/10 ja C-629/10, EU:C:2012:657, punkt 51), mis puudutab Montréalis 28. mail 1999 sõlmitud rahvusvahelise õhuveo nõuete ühtlustamise konventsiooni artikli 19 tähenduses mõistetud „kahju“ eristamist „ebamugavusest“ määruse nr 261/2004 tähenduses, mis on hüvitatav selle määruse artikli 7 alusel 19. novembri 2009. aasta kohtuotsuse Sturgeon jt (C-402/07 ja C-432/07, EU:C:2009:716) kohaselt. Selles sektoris – nagu ka meritsi ja siseveeteedel reisijate vedamise sektoris, mida käsitleb määrus nr 1177/2010 – võis seadusandja tunnustada ühte abstraktset kategooriat kui asjaolu, mis määrab ära ebamugavuse, ja selle olemust, mis on kõikide reisijate puhul samasugused. Ei usu, et seda oleks võimalik järeldada andmekaitse alal.

[39] Iirimaa sõnul on need kaalutlused praktikas eriti olulised küberkuritegevuse kontekstis, sest kui igal isikul, keda rikkumine kas või veidigi puudutab, oleks õigus mittevaralise kahju hüvitamisele, oleks sellel tugev mõju – eelkõige avaliku sektori andmete vastutavatele töötlejatele, keda rahastatakse piiratud avalik-õiguslikest vahenditest ja kes peaksid pigem teenima kollektiivseid huve, sh isikuandmete turvalisuse parandamine (kirjalikud seisukohad, punkt 72).

83. Piir lihtsa ärrituse (mis ei ole hüvitatav) ning tõelise mittevaralise kahju (mis on hüvitatav) vahel on mõistagi õrn, kuid liikmesriikide kohtud, kelle ülesanne on igal üksikul juhul see piir kindlaks määrata, peavad tähelepanelikult hindama kõiki asjaolusid, mille on esitanud andmesubjekt, kes hüvitist nõuab ning kellel on kohustus näidata täpselt ja mitte üldsõnaliselt ära konkreetsed asjaolud, mille tõttu võib esineda „mittevaraline kahju, mida on tegelikult kantud“ isikuandmetega seotud rikkumise kaudu, ilma et see siiski oleks ette kindlaks määratud konkreetse raskusastmega: olulised on see, et tegemist ei ole lihtsalt subjektiivse tajuga, mis võib muutuda ning sõltub ka iseloomu- ja isiksuseomadustest, vaid ebamugavus on objektiivne ja kuigi kerge, siis ikkagi tõendatav isiku füüsilises või psüühilises sfääris või tema suhetes; asjasse puutuvate isikuandmete laad ja tähtsus, mis neil on andmesubjekti elus, ning võib-olla ka see, kuidas tajub ühiskond sel hetkel seda konkreetset andmete rikkumisega seotud ebamugavust. [40]

IV. Ettepanek

84. Kõikide eeltoodud kaalutluste põhjal teen Euroopa Kohtule ettepaneku vastata esitatud eelotsuse küsimustele järgmiselt:

Määruse 2016/679 artikleid 5, 24, 32 ja 82 tuleb tõlgendada nii, et

ainuüksi artikli 4 punktis 12 määratletud „isikuandmetega seotud rikkumise“ esinemisest ei piisa iseenesest asumaks seisukohale, et vastutava töötleja võetud tehnilised ja korralduslikud meetmed ei olnud „asjakohased“ nende andmete kaitse tagamisel;

selle kontrollimisel, kas isikuandmete vastutava töötleja võetud tehnilised ja korralduslikud meetmed on adekvaatsed, peab liikmesriigi kohus, kelle poole on pöördutud, viima läbi kontrolli, mis hõlmab nii nende meetmete sisu kui ka rakendamise viisi ning nende praktiliste tagajärgede konkreetset analüüsi;

isikuandmete kaitse üldmääruse artikli 82 alusel esitatud kahju hüvitamise nõude raames on isikuandmete vastutaval töötlejal tõendamiskoormis selle määruse artikli 32 tähenduses rakendatud meetmete asjakohasuse tõendamise küsimuses;

kooskõlas menetlusautonoomia põhimõttega tuleb iga liikmesriigi siseses õiguskorras kindlaks määrata lubatavad tõendamismeetodid ja nende tõenduslik väärtus, sh menetlustoimingud, mida liikmesriikide kohtud võivad määrata ja peavad määrama hindamaks, kas isikuandmete vastutav töötleja on võtnud asjakohased meetmed selle määruse tähenduses, järgides liidu õiguses kindlaks määratud võrdväärsuse ja tõhususe põhimõtet;

asjaolu, et asjaomase kahju põhjustanud määruse rikkumise pani toime kolmas isik, ei kujuta endast iseenesest vastutava töötaja vastutusest vabastamise alust ning vabastuse saamiseks selle õigusnormi alusel peab vastutav töötleja tõendama, et ta ei ole rikkumise eest mingil viisil vastutav;

kahju, mis seisneb isiku hirmus, et tema andmeid võidakse tulevikus kuritarvitada, mille olemasolu andmesubjekt on tõendanud, võib kujutada endast mittevaralist kahju, mis annab õiguse hüvitisele, tingimusel et andmesubjekt tõendab, et kandis isiklikult tegelikku ja kindlat emotsionaalset kahju, kusjuures seda asjaolu peab liikmesriigi kohus igal üksikul juhul kontrollima.

[40] Vt kohtujurist Campos Sánchez-Bordona viidatud ettepanek, punkt 116.