Oikeustapauskokoelma

JULKISASIAMIEHEN RATKAISUEHDOTUS
GIOVANNI PITRUZZELLA
27 päivänä huhtikuuta 2023[1]

Asia C-340/21

VB
vastaan
Natsionalna agentsia za prihodite

(Ennakkoratkaisupyyntö – Varhoven administrativen sad (ylin hallintotuomioistuin, Bulgaria))

Ennakkoratkaisupyyntö – Henkilötietojen suoja – Asetus (EU) 2016/679 – Rekisterinpitäjän vastuu – Käsittelyn turvallisuus – Henkilötietoja koskeva tietoturvaloukkaus – Rekisterinpitäjän välinpitämättömyyden vuoksi aiheutunut henkinen kärsimys – Vahingonkorvauskanne

Voiko julkisen laitoksen hallussa olevien henkilötietojen lainvastainen levittäminen hakkeri-iskun vuoksi olla peruste henkisen kärsimyksen korvaamiseen oikeussubjektille, jota tiedot koskevat, pelkästään sillä perusteella, että viimeksi mainittu pelkää omien tietojensa mahdollista tulevaa väärinkäyttöä? Minkä edellytysten täyttyessä rekisterinpitäjä voidaan saattaa vastuuseen? Miten todistustaakka jaetaan tuomioistuimessa? Miten laaja on tuomioistuimen tutkintavalta?

I Asiaa koskevat oikeussäännöt

1. Asetuksen 2016/679[2] (jäljempänä yleinen tietosuoja-asetus) 4 artiklan otsikkona on ”Määritelmät”, ja siinä säädetään seuraavaa:

”Tässä asetuksessa tarkoitetaan

– –

(12) ’henkilötietojen tietoturvaloukkauksella’ tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin

– –”

[1] Alkuperäinen kieli: italia.

[2] Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annettu Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus).

2. Yleisen tietosuoja-asetuksen 5 artiklan otsikkona on ”Henkilötietojen käsittelyä koskevat periaatteet”, ja sen sanamuoto on seuraava:

”1. Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia:

– –

f) niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (’eheys ja luottamuksellisuus’).

2. Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (’osoitusvelvollisuus’).”

3. Saman asetuksen 24 artiklan otsikkona on ”Rekisterinpitäjän vastuu”, ja siinä säädetään seuraavaa:

”1. Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.

2. Kun se on oikeasuhteista käsittelytoimiin nähden, 1 kohdassa tarkoitettuihin toimenpiteisiin kuuluu, että rekisterinpitäjä panee täytäntöön asianmukaiset tietosuojaa koskevat toimintaperiaatteet.

3. Jäljempänä 40 artiklassa tarkoitettujen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että rekisterinpitäjälle asetettuja velvollisuuksia noudatetaan.”

4. Yleisen tietosuoja-asetuksen 32 artiklan otsikkona on ”Käsittelyn turvallisuus”, ja siinä säädetään seuraavaa:

”1. Ottaen huomioon uusin teknologia, toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

– –

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

3. Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 kohdassa asetettuja vaatimuksia noudatetaan.

– –”

5. Saman asetuksen 82 artiklan otsikkona on ”Vastuu ja oikeus korvauksen saamiseen”, ja siinä säädetään seuraavaa:

”1. Jos henkilölle aiheutuu tämän asetuksen rikkomisesta aineellista tai aineetonta vahinkoa, hänellä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta.

2. Kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on vastuussa vahingosta, joka on aiheutunut käsittelystä, jolla on rikottu tätä asetusta. – –

3. Rekisterinpitäjä tai henkilötietojen käsittelijä on vapautettava vastuusta 2 kohdan nojalla, jos se osoittaa, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta.”

II Tosiseikat, asian käsittelyn vaiheet ja ennakkoratkaisukysymykset

6. Bulgarian tiedotusvälineet ilmoittivat 15.7.2019, että Natsionalna agentsia za prihoditen (Bulgarian kansallinen verohallinto, jäljempänä NAP [3]) tietojärjestelmään oli päästy luvattomasti ja että miljoonien ihmisten, sekä Bulgarian kansalaisten että ulkomaalaisten, vero- ja sosiaalivakuutustietoja julkaistaisiin internetissä.

7. Useat henkilöt, muun muassa VB, joka on pääasian kantaja, haastoivat siis NAP:n oikeuteen saadakseen korvausta henkisestä kärsimyksestä.

8. Nyt käsiteltävässä asiassa pääasian oikeudenkäynnin kantaja saattoi asian Administrativen sad Sofia-gradin (Sofian kaupungin hallintotuomioistuin, Bulgaria; jäljempänä ASSG) käsiteltäväksi ja väitti NAP:n rikkoneen kansallisia oikeussääntöjä sekä laiminlyöneen velvollisuutensa käsitellä henkilötietoja rekisterinpitäjänä siten, että ”huolehditaan asianmukaisesta turvallisuudesta” toteuttamalla yleisen tietosuoja-asetuksen 24 ja 32 artiklassa tarkoitettuja asianmukaisia teknisiä ja organisatorisia toimenpiteitä. Kantaja väitti tämän jälkeen, että hänelle oli aiheutunut henkistä kärsimystä, joka ilmenee huolina ja pelkoina siitä, että hänen henkilötietojaan käytetään tulevaisuudessa väärin.

9. Vastaaja sitä vastoin korosti, ettei se ole saanut pääasian kantajalta mitään vaatimusta, jossa olisi mainittu nimenomaiset henkilötiedot, joihin olisi päästy tutustumaan. Lisäksi se oli saatuaan tiedon tietomurrosta kutsunut kokouksiin kansalaisten oikeuksien ja etujen suojelun asiantuntijat. NAP:n mukaan myös syy-yhteys tietohyökkäyksen ja väitetyn vahingon väliltä puuttui, koska laitos oli ottanut käyttöön kaikki prosessinhallintajärjestelmät ja tietoturvajärjestelmät asiaa koskevien voimassa olevien kansainvälisten standardien mukaisesti.

[3] NAP on yleisen tietosuoja-asetuksen 4 artiklan 7 kohdassa tarkoitettu rekisterinpitäjä. Kansallisen lainsäädännön perusteella se on valtiovarainministeriön alaisuudessa toimiva viranomainen, jolla on erityistä toimivaltaa ja jonka tehtävänä on todeta, varmistaa ja periä laissa määritetyt valtion julkiset ja yksityiset saatavat. Se käsittelee henkilötietoja käyttäessään sille annettua julkista toimivaltaa.

10. Ensimmäisen asteen tuomioistuin ASSG hylkäsi kanteen, koska se katsoi, että tietojen levittäminen ei johtunut NAP:stä, että todistustaakka toteutettujen toimenpiteiden asianmukaisuudesta oli kantajalla, ja lopuksi, että henkinen kärsimys ei ollut korvattavaa vahinkoa.

11. Ensimmäisessä asteessa annetusta tuomiosta valitettiin tämän jälkeen Varhoven administrativen sadiin (ylin hallintotuomioistuin, Bulgaria). Pääasian oikeudenkäynnin kantaja korosti esitetyistä seikoista, että ensimmäisen asteen tuomioistuin oli tehnyt virheen jakaessaan todistustaakan turvallisuustoimenpiteiden toteuttamatta jättämisen osalta. Henkisen kärsimyksen ei pitäisi olla todistustaakan kohteena, koska kyseessä on tosiasiallinen eikä ainoastaan mahdollinen henkinen kärsimys.

12. NAP puolestaan vastasi toteuttaneensa tarvittavat tekniset ja organisatoriset toimenpiteet rekisterinpitäjänä, ja kiisti sen, että tosiasiallinen henkinen kärsimys olisi näytetty toteen. Ahdistus ja pelot ovat näet sen mielestä tunnetiloja, joista ei voida maksaa korvausta.

13. Ennakkoratkaisua pyytänyt tuomioistuin totesi, että yksittäisissä menettelyissä, joita vahinkoa kärsineet olivat erikseen panneet vireille NAP:tä vastaan saadakseen korvausta henkisistä kärsimyksistä, oli päädytty eri lopputuloksiin.

14. Tässä yhteydessä ennakkoratkaisua pyytänyt tuomioistuin on lykännyt asian käsittelyä ja esittänyt unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

”1) Onko [luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston] asetuksen (EU) 2016/679 [(yleinen tietosuoja-asetus)] 24 ja 32 artiklaa tulkittava siten, että sen toteamiseksi, että toteutetut tekniset ja organisatoriset toimenpiteet eivät ole asianmukaisia, riittää, että kyseisen asetuksen 4 artiklan 12 kohdassa tarkoitettu luvaton henkilötietojen luovuttaminen tai pääsyn antaminen niihin johtuu henkilöistä, jotka eivät ole rekisterinpitäjän palveluksessa eivätkä kuulu sen määräysvaltaan?

2) Jos ensimmäiseen kysymykseen vastataan kieltävästi, mikä kohde ja laajuus pitäisi olla tuomioistuimen harjoittamalla laillisuusvalvonnalla tutkittaessa, ovatko rekisterinpitäjän asetuksen (EU) 2016/679 32 artiklan nojalla toteuttamat tekniset ja organisatoriset toimenpiteet asianmukaisia?

3) Jos ensimmäiseen kysymykseen vastataan kieltävästi, onko asetuksen (EU) 2016/679 5 artiklan 2 kohdassa ja 24 artiklassa tarkoitettua osoitusvelvollisuuden periaatetta, luettuna yhdessä sen johdanto-osan 74 perustelukappaleen kanssa, tulkittava siten, että asetuksen (EU) 2016/679 82 artiklan 1 kohdassa tarkoitetussa kannemenettelyssä rekisterinpitäjällä on todistustaakka siitä, että asetuksen 32 artiklan nojalla toteutetut tekniset ja organisatoriset toimenpiteet ovat asianmukaisia? Voidaanko asiantuntijalausunnon hankkimista pitää tarvittavana ja riittävänä todisteena, jotta voidaan todeta, olivatko rekisterinpitäjän toteuttamat tekniset ja organisatoriset toimenpiteet nyt käsiteltävän kaltaisessa tapauksessa asianmukaisia, kun luvaton pääsy henkilötietoihin ja niiden luvaton luovuttaminen johtuivat ’hakkeri-iskusta’?

4) Onko asetuksen (EU) 2016/679 82 artiklan 3 kohtaa tulkittava siten, että se, että asetuksen (EU) 2016/679 4 artiklan 12 kohdassa tarkoitettu henkilötietojen luvaton luovuttaminen tai luvaton pääsy henkilötietoihin tapahtuu, kuten tässä tapauksessa, sellaisten henkilöiden suorittamalla ’hakkeri-iskulla’, jotka eivät ole rekisterinpitäjän palveluksessa eivätkä kuulu sen määräysvaltaan, on seikka, josta rekisterinpitäjä ei ole millään tavalla vastuussa ja joka oikeuttaa sen vapauttamisen vastuusta?

5) Onko asetuksen (EU) 2016/679 82 artiklan 1 ja 2 kohtaa, luettuna yhdessä sen johdanto-osan 85 ja 146 perustelukappaleen kanssa, tulkittava siten, että nyt käsiteltävän kaltaisessa tapauksessa, jossa henkilötietojen suojan loukkaaminen ilmenee siten, että henkilötietoihin päästään luvattomasti ja niitä luovutetaan ’hakkeri-iskun’ avulla, jo pelkästään rekisteröidyn huolet, pelot ja ahdistukset, jotka johtuvat henkilötietojen mahdollisesta tulevasta väärinkäytöstä, kuuluvat laajasti tulkittavan henkisen kärsimyksen käsitteen soveltamisalaan ja oikeuttavat vahingonkorvaukseen, vaikka tällaista väärinkäyttöä ei ole todettu ja/tai rekisteröidylle ei ole aiheutunut muita vahinkoja?”

III Oikeudellinen arviointi

A Alustavia huomautuksia

15. Nyt käsiteltävän asian kohteena on mielenkiintoisia ja osittain aivan uusia kysymyksiä, jotka koskevat yleisen tietosuoja-asetuksen eri säännösten tulkintaa. [4]

16. Kaikki viisi ennakkoratkaisukysymystä koskevat samaa asiaa: edellytyksiä, joiden täyttyessä henkinen kärsimys voidaan korvata oikeussubjektille, jonka henkilötiedot, jotka ovat julkisen laitoksen hallussa, on julkaistu internetissä hakkeri-iskun seurauksena.

17. Asian esittelemisen helpottamiseksi ehdotan kaikkiin ennakkoratkaisukysymyksiin erilliset tiiviit vastaukset, vaikka olen tietoinen joistakin sisällöllisistä päällekkäisyyksistä, koska kaikilla neljällä ensimmäisellä kysymyksellä pyritään selvittämään edellytyksiä, joiden täyttyessä yleisen tietosuoja-asetuksen säännösten rikkominen luetaan rekisterinpitäjän syyksi, [5] ja viides koskee erityisesti korvattavan henkisen kärsimyksen käsitettä. [6]

18. Todettakoon, että unionin tuomioistuimessa on vireillä useita yleisen tietosuoja-asetuksen 82 artiklaa koskevia asioita ja että yhdessä niistä julkisasiamies on jo antanut ratkaisuehdotuksen, jonka otan huomioon tässä tarkastelussa. [7]

[4] 5 artiklan 2 kohta (joka koskee kaikkia henkilötietojen rekisterinpitäjiä velvoittavaa osoitusvelvollisuusperiaatetta), 24 artikla (joka koskee toimenpiteitä, joita tällainen rekisterinpitäjä on velvollinen toteuttamaan varmistaakseen, että niitä käsitellään tämän asetuksen mukaisesti), 32 artikla (joka koskee tällaista velvollisuutta erityisesti käsittelyn turvallisuuden osalta) ja 82 artiklan 1–3 kohta (joka koskee tämän asetuksen rikkomisesta johtuvien vahinkojen korvaamista ja rekisterinpitäjän mahdollisuutta toteuttaa toimenpiteitä varmistaakseen tämän asetuksen noudattamisen), sekä johdanto-osan 74, 85 ja 146 perustelukappale, jotka liittyvät edellä mainittuihin artikloihin.

[5] Näistä a) ensimmäisellä pyydetään vastausta siihen, voidaanko pelkästä järjestelmiin murtautumisesta päätellä, että toteutetut toimenpiteet ovat olleet epäasianmukaisia, b) toinen koskee edellä mainittujen toimenpiteiden asianmukaisuutta koskevan tuomioistuimen harjoittaman vallan laajuutta, c) kolmas liittyy asianmukaisuutta koskevaan todistustaakkaan ja joihinkin näytön hankkimista koskeviin teknisiin yksityiskohtaisiin sääntöihin ja d) neljäs liittyy siihen, mikä merkitys on vastuusta vapautumisen kannalta sillä, että hyökkäys järjestelmään tulee ulkopuolelta.

[6] Edellä mainittujen yleisen tietosuoja-asetuksen säännösten osalta kolme ensimmäistä kysymystä koskevat rekisterinpitäjän vastuuta toteutettavien toimenpiteiden asianmukaisuudesta (5, 24 ja 32 artikla); neljäs ja viides vastuusta vapautumisen edellytyksiä ja korvattavan henkisen kärsimyksen käsitettä (82 artikla).

[7] Ks. julkisasiamies Campos Sánchez-Bordonan ratkaisuehdotus Österreichische Post (Henkilötietojen käsittelyyn liittyvä aineeton vahinko) (C-300/21, EU:C:2022:756).

19. Ennen esitettyjen kysymysten tutkimista on mielestäni asianmukaista esittää yleisen tietosuoja-asetuksen periaatteista ja tarkoituksesta muutamia alustavia näkemyksiä, jotka ovat hyödyllisiä yksittäisten ennakkoratkaisukysymysten ratkaisemisen kannalta.

20. Yleisen tietosuoja-asetuksen 24 artiklassa vahvistetaan yleisesti rekisterinpitäjän velvollisuus toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta, kun puolestaan 32 artiklassa vahvistetaan tämä sama velvollisuus tarkemmin käsittelyn turvallisuuden osalta. Edellä mainituissa 24 ja 32 artiklassa täsmennetään sitä, mitä säädetään jo 5 artiklan 2 kohdassa, jossa otetaan käyttöön "henkilötietojen käsittelyä koskevat periaatteet" ja niiden joukossa "osoitusvelvollisuusperiaate". Tämä on johdonmukainen seuraus 5 artiklan 1 kohdan f alakohdan "eheys ja luottamuksellisuus" -periaatteesta ja täydentää sitä, ja molempia on luettava asetuksen perustana olevaan riskiin perustuvan lähestymistavan valossa.

21. Osoitusvelvollisuusperiaate on yksi yleisen tietosuoja-asetuksen peruspilareista ja yksi sen merkittävimmistä uudistuksista. Sillä annetaan rekisterinpitäjälle vastuu toteuttaa ennakoivia toimia varmistaakseen asetuksen noudattamisen ja olla valmis osoittamaan se.[8]

22. Oikeuskirjallisuudessa on puhuttu tosiasiallisesta ja aidosta kulttuurin muutoksesta, joka johtuisi osoitusvelvollisuuden kaikenkattavuudesta.[9] Kyseessä ei ole niinkään lakisääteisen velvollisuuden tai täsmällisen toimenpiteen muodollinen noudattaminen kuin yrityksen strateginen kokonaisuus, jolla pyritään vapauttamaan rekisterinpitäjä vastuusta, koska se noudattaa tietosuojaa koskevaa sääntelyä.

23. Osoitusvelvollisuusperiaatteen edellyttämien teknisten ja organisatoristen toimenpiteiden on oltava ”asianmukaisia”, kun otetaan huomioon 24 artiklassa täsmennetyt tekijät: käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

24. Yleisen tietosuoja-asetuksen 24 artiklassa vaaditaan siten toimenpiteiden asianmukaisuutta, jotta kyetään osoittamaan, että tietojen käsittely on asetuksen periaatteiden ja säännösten mukaista.

25. Yleisen tietosuoja-asetuksen 32 artiklassa vahvistetaan sitä vastoin osoitusvelvollisuusperiaate, joka koskee konkreettisia toimenpiteitä, joita on toteutettava, jotta varmistetaan ”riskiä vastaava turvallisuustaso”. Tässä yhteydessä siinä lisätään niihin jo edellä mainittuihin osatekijöihin, jotka on otettava huomioon toteutettaessa teknisiä ja organisatorisia toimenpiteitä, uusin teknologia ja toteuttamiskustannukset.

26. Asianmukaisuuden käsite edellyttää, että ratkaisuilla, joita toteutetaan tietojärjestelmien toiminnan varmistamiseksi, saavutetaan hyväksyttävä taso sekä teknisesti (toimenpiteiden asiaankuuluvuus) että laadullisesti (suojan tehokkuus). Jotta varmistetaan tarpeellisuutta, asiaankuuluvuutta ja oikeasuhteisuutta koskevien periaatteiden noudattaminen, käsittelyjen on

[8] Docksey, C., “Article 24. Responsibility of the controller”, teoksessa Kuner, C., Bygrave, L. A., Docksey, C. ja Drechsler, L., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, s. 561. Tietosuojaa koskevien säännösten mukaisten periaatteiden ja velvollisuuksien pitäisi pikemminkin käsittää yritysten kulttuuri kaikilla tasoilla eikä niin, että se nähdään sarjana oikeudellisia velvoitteita, joita lainkäyttöviranomaisten pitäisi valvoa.

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

oltava paitsi asianmukaisia, myös tyydyttäviä siihen tavoitteeseen nähden, joka niillä pyritään saavuttamaan. Tämän perusteella ratkaiseva merkitys on minimointiperiaatteella, jonka nojalla kaikissa tietojenkäsittelyn vaiheissa on jatkuvasti pyrittävä turvallisuusriskien minimoimiseen. [10]

27. Koko yleiselle tietosuoja-asetukselle on ominaista riskin estäminen ja rekisterinpitäjän osoitusvelvollisuus ja siten teleologinen tulkinta, jolla pyritään tehokkuuden kannalta parhaaseen mahdolliseen tulokseen, mikä on siis hyvin kaukana muodollisesta logiikasta, joka liittyisi pelkkään velvollisuuteen noudattaa erityisiä menettelyjä vastuusta vapautumista varten. [11]

28. Yleisen tietosuoja-asetuksen 24 artiklaan ei sisälly tyhjentävää luetteloa asianmukaisista toimenpiteistä: on tehtävä tapauskohtainen arviointi. Tämä vastaa kyseisen asetuksen filosofiaa, jonka mukaan pidettiin parempana sitä, että toteutettavat menettelyt valittaisiin kunkin yksittäistilanteen tarkan arvioinnin perusteella, jotta ne voisivat olla mahdollisimman tehokkaita. [12]

B Ensimmäinen ennakkoratkaisukysymys

29. Ennakkoratkaisua pyytänyt tuomioistuin tiedustelee ensimmäisellä kysymyksellään lähinnä, onko yleisen tietosuoja-asetuksen 24 ja 32 artiklaa tulkittava siten, että 4 artiklan 12 kohdassa määritellyn ”henkilötietojen tietoturvaloukkauksen” toteutumiseksi lähtökohtaisesti riittää, että todetaan, että rekisterinpitäjän toteuttamat tekniset ja organisatoriset toimenpiteet eivät olleet ”asianmukaisia” tietosuojan varmistamiseksi.

30. Yleisen tietosuoja-asetuksen 24 ja 32 artiklan sanamuodosta ilmenee, että kun rekisterinpitäjä valitsee tekniset ja organisatoriset toimenpiteet, joita se on velvollinen toteuttamaan varmistaakseen, että ne ovat kyseisen asetuksen mukaisia, sen on otettava huomioon useita arviointiperusteita, jotka on lueteltu kyseisissä ja edellä mainituissa artikloissa.

31. Rekisterinpitäjällä on käytettävissään tiettyä harkintavaltaa asianmukaisimpien toimenpiteiden määrittämisessä sen erityisen tilanteen perusteella, mutta tähän valintaan kohdistetaan kuitenkin mahdollista tuomioistuimen harjoittamaa valvontaa, joka koskee sovellettavien toimenpiteiden yhteensopivuutta saman asetuksen kaikkien velvoitteiden ja tavoitteiden kanssa.

32. Erityisesti turvallisuustoimenpiteiden osalta 32 artiklan 1 kohdassa asetetaan rekisterinpitäjälle velvollisuus ottaa huomioon ”uusin teknologia”. Tämä edellyttää sitä, että rajoitetaan toteutettavien toimenpiteiden teknologinen taso siihen, mikä on kohtuudella mahdollista ajankohtana, jona toimenpiteet toteutetaan: toimenpiteen soveltuvuutta estämään

[10] Em. Belisario, E., Riccio, G. ja Scorza, G., *GDPR*, s. 380.

[11] Kuten jäljempänä havaitaan, ensimmäiseen ja neljänteen ennakkoratkaisukysymykseen voidaan tästä syystä vastata vain kieltävästi. Yleisen tietosuoja-asetuksen säännöksistä ei voida johtaa mitään automaatiota: pelkästään sillä perusteella, että henkilötietoja on luovutettu, ei voida katsoa, että toteutetut tekniset ja organisatoriset toimenpiteet eivät ole asianmukaisia, mutta myöskään se, että tiedot on luovutettu sellaisten rekisterinpitäjän organisaation ulkopuolisten oikeussubjektien toimesta, jotka eivät kuulu sen valvonnan piiriin, ei riitä vapauttamaan sitä vastuusta.

[12] Bolognini, L. ja Pelino, E., *Codice della disciplina privacy*, Giuffrè, 2019, s. 201. Unionin lainsäätäjä ylittää siis käsittelyn turvallisuuden käsitteen, joka perustuu siihen, että on olemassa ennalta määritettyjä turvallisuustoimenpiteitä, ja ottaa käyttöön kansainvälisiä standardeja koskevan oman metodologian, jota sovelletaan riskiperusteiseen tietojärjestelmien hallinnointiin: sen mukaan on yksilöitävä riskiä lieventäviä toimenpiteitä, joissa jätetään ennalta määritetyt ja yleisesti sovellettavat tarkistuslistat tarkastelun ulkopuolelle. On näin ollen turvauduttava kansainvälisiin suuntaviivoihin ja standardeihin. Tällaisen riskienarvioinnin lopputuloksesta tulee siis sitova sillä hetkellä, jona organisaatio panee päätökset täytäntöön lieventääkseen riskejä, ja tekee itsestään vastuussa olevan tahon.

riskin toteutuminen on siis arvioitava niihin ratkaisuihin nähden, jotka tieteen, tekniikan, teknologian ja senhetkisen tutkimuksen kehitys tarjoaa, mutta, kuten jäljempänä havaitaan, myös toteuttamiskustannukset otetaan huomioon.

33. Toimenpiteet voivat olla ”asianmukaisia” tiettynä ajankohtana, ja siitä huolimatta kyberrikolliset saattavat kiertää ne käyttämällä erittäin edistyksellisiä keinoja, joilla voidaan murtaa myös uusimman teknologian mukaiset turvallisuustoimenpiteet.

34. Toisaalta tuntuisi epäjohdonmukaiselta katsoa, että unionin lainsäätäjän aikomuksena olisi ollut asettaa rekisterinpitäjälle velvoite estää kaikki henkilötietojen tietoturvaloukkaukset riippumatta sen valppaudesta turvallisuustoimenpiteiden käyttöönotossa. [13]

35. Kuten edellä todettiin, yleisellä tietosuoja-asetuksella ei missään tapauksessa pyritä automaatioon vaan edellytetään rekisterinpitäjältä huomattavaa osoitusvelvollisuutta, joka ei voi kuitenkaan merkitä sitä, että viimeksi mainitun olisi mahdotonta osoittaa noudattaneensa sille asetettuja velvollisuuksia oikein.

36. Lisäksi 32 artiklan 1 kohdassa säädetään, että kuten edellä mainitsin, on otettava huomioon tutkittavien teknisten ja organisatoristen toimenpiteiden ”toteuttamiskustannukset”. Tästä seuraa, että tällaisten toimenpiteiden asianmukaisuuden arvioinnin on perustuttava siihen, että verrataan keskenään rekisteröidyn intressejä, jotka yleensä puoltavat korkeampaa suojan tasoa, sekä rekisterinpitäjän taloudellisia intressejä ja teknologisia kykyjä, jotka toisinaan puoltavat heikompaa suojan tasoa. Tällaisessa vertailussa on noudatettava yleisen suhteellisuusperiaatteen asettamia vaatimuksia.

37. Lisättäköön tähän vielä systemaattisen tulkinnan näkökulmasta, että lainsäätäjä ottaa huomioon sen mahdollisuuden, että järjestelmiin murtaudutaan; ehdotettuihin toimenpiteisiin sisältyy 32 artiklan 1 kohdan c alakohdassa kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa. Olisi turhaa säätää tällaisesta kyvystä yhtenä turvallisuustoimenpiteistä, joilla varmistetaan turvallisuuden taso, joka on asianmukaisessa suhteessa riskiin, jos katsottaisiin, että järjestelmiin murtautuminen osoittaisi jo sellaisenaan näiden toimenpiteiden epäasianmukaisuuden.

C Toinen ennakkoratkaisukysymys

38. Ennakkoratkaisua pyytänyt tuomioistuin tiedustelee toisella kysymyksellään lähinnä, mikä kohde ja laajuus pitää olla tuomioistuimen harjoittamalla valvonnalla tutkittaessa, ovatko henkilötietojen rekisterinpitäjän yleisen tietosuoja-asetuksen 32 artiklan nojalla toteuttamat tekniset ja organisatoriset toimenpiteet asianmukaisia.

39. Koska tilanteet, joita voi käytännössä ilmetä, ovat moninaisia, yleisessä tietosuoja-asetuksessa ei, kuten edellä todettiin, vahvisteta sitovia säännöksiä niiden teknisten ja organisatoristen toimenpiteiden määrittämiseksi, joita rekisterinpitäjän on toteutettava täyttääkseen asetuksen vaatimukset. Toteutettavien toimenpiteiden asianmukaisuutta on siten arvioitava konkreettisesti ja selvitettävä, ovatko tietyt toimenpiteet olleet soveltuvia estämään kohtuudella riskin ja minimoimaan tietomurron kielteiset vaikutukset.

[13] Asianmukaisuuden käsite osoittaa yksiselitteisesti aikomuksen olla antamatta merkitystä kaikille teknisille ja organisatorisille toimenpiteille, jotka olisivat abstraktisti mahdollisia. Ks. vastaavasti Gambini, M., Responsabilità e risarcimento nel trattamento dei dati personali, teoksessa Cuffaro, V., D’Orazio, R. ja Ricciuto, V., I dati personali nel diritto europeo, Giappichelli, 2019, s. 1059.

40. Vaikka on ilman muuta niin, että tällaisten toimenpiteiden valinta ja täytäntöönpano kuuluvat rekisterinpitäjän subjektiivisen arvioinnin piiriin, koska yleisessä tietosuoja-asetuksessa mainitut toimenpiteet ovat vain esimerkkejä, tuomioistuimen arviointi ei voi rajoittua vain siihen, että valvotaan, että rekisterinpitäjä on noudattanut 24 ja 32 artiklassa johtuvia velvoitteita eli että se on (muodollisesti) määrännyt tietyistä teknisistä ja organisatorisista toimenpiteistä. Sen on tarkasteltava konkreettisesti tällaisten toimenpiteiden sisältöä, tapaa, jolla niitä sovelletaan, ja niiden käytännön vaikutuksia käytettävissään olevien todisteiden ja tapaukseen liittyvien olosuhteiden perusteella. Kuten Portugalin hallitus on aivan oikein huomauttanut, ”tapaa, jolla se on täyttänyt velvollisuutensa, ei ilmeisesti voida erottaa toteutettujen toimenpiteiden sisällöstä, jos tarkoituksena on osoittaa, että kun otetaan huomioon tietojen erityinen käsittely (sen luonne, laajuus, asiayhteys ja tavoitteet), käytettävissä oleva uusin teknologia ja sen kustannukset sekä kansalaisten oikeuksiin ja vapauksiin kohdistuvat riskit, rekisterinpitäjä on toteuttanut kaikki tarvittavat ja asianmukaiset toimenpiteet varmistaakseen taustalla olevaan riskiin nähden asianmukaisen turvallisuuden tason”. [14]

41. Tuomioistuimen harjoittaman valvonnan yhteydessä on näin ollen otettava huomioon kaikki tekijät, jotka sisältyvät 24 ja 32 artiklaan, joissa edellä mainitulla tavalla luetellaan useita perusteita, joiden mukaan asianmukaisuutta on arvioitava, ja esitetään esimerkkejä toimenpiteistä, joita voidaan pitää asianmukaisina. Lisäksi, kuten komissio ja kaikki toisesta kysymyksestä huomautuksia esittäneet jäsenvaltiot ovat korostaneet, 32 artiklan 1–3 kohdassa painotetaan tarvetta ”riskiä vastaavan turvallisuustason” varmistamiseen ja mainitaan muita tämän kannalta merkityksellisiä tekijöitä, kuten se, että rekisterinpitäjä mahdollisesti vahvistaa hyväksytyt käytännesäännöt tai hyväksytyn sertifiointijärjestelmän, kuten 40 artiklassa vahvistetaan ensin mainittujen ja 42 artiklassa jälkimmäisten osalta.

42. Käytännesääntöjen tai sertifiointijärjestelmän hyväksyminen voi tarjota hyödyllisen arviointiperusteen, kun ratkaistaan todistustaakkaa ja siihen liittyvää tuomioistuimen harjoittamaa valvontaa koskeva kysymys. Tätä on kuitenkin täsmennettävä siten, että ei riitä, että rekisterinpitäjä hyväksyy käytännesäännöt, vaan sillä on osoitusvelvollisuusperiaatteen mukaisesti todistustaakka sen osoittamiseksi, että se on konkreettisesti toteuttanut niiden mukaiset toimenpiteet. Sertifiointi on sitä vastoin ”sellaisenaan osoitus siitä, että tietoja on käsitelty asetuksen mukaisesti, mutta tämä voidaan kiistää käytännön tasolla”. [15]

43. Huomautettakoon lopuksi, että tällaisia toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa 24 artiklan 1 kohdan nojalla. Kansallinen tuomioistuin arvioi myös tätä. Yleisen tietosuoja-asetuksen 32 artiklan 1 kohdassa [16] määrätään näet rekisterinpitäjälle jatkuvaa valvontaa ja seurantaa koskeva velvollisuus, joka edeltää ja seuraa käsittelytoimintaa, mutta myös ylläpitoa ja toteutettujen toimenpiteiden mahdollista päivitystä koskeva velvollisuus, jolla pyritään sekä estämään tietomurrot että mahdollisesti rajoittamaan niiden vaikutuksia.

[14] Kirjalliset huomautukset, 31 kohta.

[15] Em. Gambini, M., Responsabilità, s. 1067. Todistuksen hallussapito merkitsee näin ollen todistustaakan kääntämistä sellaisen rekisterinpitäjän hyväksi, joka on auttanut osoittamaan, että se on toiminnassaan noudattanut yleisen tietosuoja-asetuksen mukaisia velvoitteita.

[16] Kyseisen artiklan d alakohdassa säädetään nimenomaisesti, että menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi sekä alkuvaiheessa että aika ajoin, riippumatta siitä, mikä on niiden riskin taso; ja sen c alakohdassa säädetään vielä nimenomaisesti, että teknisillä ja organisatorisilla toimenpiteillä on oltava kyky palauttaa nopeasti tietojen saatavuus ja pääsy henkilötietoihin fyysisen tai teknisen vian sattuessa. Ks. em. Gambini, M., Responsabilità, s. 1064–1065.

44. Haluaisin kuitenkin sulkea pois sen mahdollisuuden, että seuraava tuomio sisältäisi Portugalin hallituksen ehdottaman kaltaisen luettelon aineellisista osatekijöistä.[17] Tämä saattaisi mahdollistaa ristiriitaiset tulkinnat, koska luettelo ei tietenkään voi koskaan olla tyhjentävä.

D Kolmas ennakkoratkaisukysymys

45. Ennakkoratkaisua pyytänyt tuomioistuin pyytää kolmannen kysymyksensä ensimmäisessä osassa unionin tuomioistuinta lähinnä ratkaisemaan, onko yleisen tietosuoja-asetuksen 5 artiklan 2 kohdassa ja 24 artiklassa tarkoitetun osoitusvelvollisuuden periaatteen, luettuna yhdessä yleisen tietosuoja-asetuksen johdanto-osan 74 perustelukappaleen[18] kanssa, perusteella 82 artiklassa tarkoitetun vahingonkorvauskanteen yhteydessä rekisterinpitäjällä todistustaakka siitä, että yleisen tietosuoja-asetuksen 32 artiklan nojalla toteutetut tekniset ja organisatoriset toimenpiteet ovat asianmukaisia.

46. Edellä esitetyn perusteella pystyn vastaamaan tähän kysymykseen lyhyesti myöntävällä tavalla.

47. Lain sanamuoto, asiayhteys ja asetuksen tarkoitus puoltavat näet yksiselitteisesti sitä, että todistustaakka on rekisterinpitäjällä.

48. Yleisen tietosuoja-asetuksen eri säännösten sanamuodosta ilmenee, että rekisterinpitäjän on ”pystyttävä” tai ”kyettävä” ”osoittamaan” asetuksessa säädettyjen velvollisuuksien noudattaminen ja erityisesti se, että se on toteuttanut tätä vastaavat asianmukaiset toimenpiteet, kuten todetaan johdanto-osan 74 perustelukappaleessa, 5 artiklan 2 kohdassa ja 24 artiklan 1 kohdassa. Kuten Portugalin hallitus korostaa, edellä mainitussa johdanto-osan 74 perustelukappaleessa täsmennetään, että rekisterinpitäjälle tällä tavoin asetetun todistustaakan on katettava kyseisten ”toimenpiteiden tehokkuus”.

49. Tätä sanamuodon mukaista tulkintaa tukevat mielestäni seuraavat käytännölliset ja teleologiset seikat.

50. Todistustaakan jakamisen osalta 82 artiklaan perustuvan vahingonkorvauskanteen yhteydessä rekisteröidyn, joka on nostanut kanteen rekisterinpitäjää vastaan, on ensinnäkin osoitettava, että yleistä tietosuoja-asetusta on rikottu, toiseksi, että vahinkoa on syntynyt, ja kolmanneksi, että kahden edellä mainitun seikan välillä on syy-yhteys, kuten kaikissa viidettä ennakkoratkaisukysymystä koskevissa kirjallisissa huomautuksissa on korostettu. Nämä kolme

[17] Kirjallisten huomautusten 30 kohta: ”on rekisterinpitäjän tehtävänä osoittaa, miten se on arvioinut kaikkia kyseiseen käsittelyyn liittyviä tekijöitä ja olosuhteita sekä erityisesti suoritetun riskinarvioinnin tulosta, havaittuja riskejä, konkreettisia toimenpiteitä, joita on löydetty tällaisten riskien lieventämiseksi, valittujen vaihtoehtojen perusteluja markkinoilla käytettävissä olevien teknologisten ratkaisujen valossa, toimenpiteiden tehokkuutta, teknisten ja organisatoristen toimenpiteiden välistä yhteyttä, tietoja käsittelevän henkilöstön koulutusta, tietojenkäsittelytoimintojen ulkoistamista, mukaan lukien tietotekniikan kehitys ja ylläpito, sekä rekisterinpitäjän harjoittama valvonta ja täsmälliset ohjeet, joita on annettu yleisen tietosuoja-asetuksen 28 artiklassa tarkoitetuille henkilötietojen käsittelijöille siitä, miten näiden on käsiteltävä henkilötietoja; miten on arvioitu tieto- ja viestintäjärjestelmien tukirakennetta ja miten on luokiteltu rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin taso”.

[18] Johdanto-osan 74 perustelukappaleen sanamuoto on seuraava: ”Olisi vahvistettava rekisterinpitäjän vastuu tämän suorittamasta tai rekisterinpitäjän puolesta suoritetusta henkilötietojen käsittelystä. Erityisesti rekisterinpitäjällä olisi oltava velvollisuus toteuttaa asianmukaisia ja tehokkaita toimenpiteitä, ja sen olisi voitava osoittaa, että käsittelytoimet ovat tämän asetuksen mukaisia, toimenpiteiden tehokkuus mukaan luettuna. Näitä toimenpiteitä toteutettaessa olisi otettava huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski.”

edellytystä ovat päällekkäisiä, kuten ilmenee myös unionin tuomioistuimen ja unionin yleisen tuomioistuimen sopimussuhteen ulkopuolista vastuuta unionissa koskevasta oikeuskäytännöstä. [19]

51. Katson kuitenkin, että kantajan velvollisuus osoittaa yleisen tietosuoja-asetuksen rikkominen ei voi ulottua niin pitkälle, että edellytettäisiin hänen osoittavan, millä tavoin rekisterinpitäjän tekniset ja organisatoriset toimenpiteet eivät ole 24 ja 32 artiklan perusteella asianmukaisia.

52. Kuten komissio korostaa, tällaisten todisteiden esittäminen olisi käytännössä lähes mahdotonta, koska asianosaisilla ei ole yleensä riittävää osaamista, jotta he voisivat arvioida tällaisia toimenpiteitä, eikä pääsyä kaikkiin vastaajana olevan rekisterinpitäjän hallussa oleviin tietoihin erityisesti tietojen käsittelyn turvallisuuden varmistamiseksi käytettyjen menetelmien osalta. Lisäksi rekisterinpitäjä voisi toisinaan väittää, että sen kieltäytyminen antamasta näitä tietoja asianosaisille perustuu hyväksyttävään syyhyn, jonka vuoksi se ei julkaise omia sisäisiä asioitaan tai muitakaan liikesalaisuuden piiriin kuuluvia seikkoja muun muassa turvallisuussyistä.

53. Jos siis katsottaisiin, että todistustaakka kuuluu rekisteröidylle, tästä seuraisi, että 82 artiklan 1 kohdassa säädetty kanneoikeus menettäisi suuren osan merkityksestään. Tämä ei mielestäni vastaisi unionin lainsäätäjän tarkoituksia, koska se on antaessaan yleisen tietosuoja-asetuksen pyrkinyt vahvistamaan rekisteröityjen oikeuksia ja rekisterinpitäjän velvollisuuksia sillä korvattuun direktiiviin 95/46 nähden. On siis johdonmukaisempaa ja oikeudellisesti kestävämpää, että rekisterinpitäjä on puolustautuessaan vahingonkorvauskannetta vastaan velvollinen osoittamaan noudattaneensa kyseisen asetuksen 24 ja 32 artiklasta johtuvia velvoitteitaan toteuttamalla tosiasiallisesti asianmukaisia toimenpiteitä.

54. Ennakkoratkaisua pyytänyt tuomioistuin tiedustelee unionin tuomioistuimelta kolmannen kysymyksensä toisessa osassa lähinnä, voidaanko oikeudellista asiantuntijalausuntoa pitää tarvittavana ja riittävänä todisteena arvioitaessa henkilötietojen rekisterinpitäjän toteuttamien teknisten ja organisatoristen toimenpiteiden asianmukaisuutta tilanteessa, jossa luvaton pääsy henkilötietoihin ja niiden luvaton luovuttaminen johtuvat hakkeri-iskusta.

55. Kuten myös Bulgarian ja Italian hallitukset, Irlanti ja komissio ovat (olennaisilta osin) korostaneet, katson, että näihin kysymyksiin annettavan vastauksen on perustuttava unionin tuomioistuimen vakiintuneeseen oikeuskäytäntöön, josta seuraa, että kun kyseessä olevasta alasta ei ole annettu unionin sääntöjä, kunkin jäsenvaltion on annettava sisäisessä oikeusjärjestyksessään menettelysäännöt sellaisia oikeussuojakeinoja varten, joilla pyritään turvaamaan yksityisten oikeudet menettelyllistä itsemääräämisoikeutta koskevan periaatteen nojalla, kuitenkin sillä edellytyksellä, että nämä menettelysäännöt eivät ole epäedullisempia kuin ne, jotka koskevat samankaltaisia kansallisen oikeuden piiriin kuuluvia tilanteita (vastaavuusperiaate), eivätkä ne ole sellaisia, että unionin oikeudessa vahvistettujen oikeuksien käyttäminen on käytännössä mahdotonta tai suhteettoman vaikeaa (tehokkuusperiaate).

56. Huomauttakoon tässä tapauksessa, että yleiseen tietosuoja-asetukseen ei sisälly yhtään säännöstä, jossa määritettäisiin hyväksyttävät todistelukeinot ja niiden todistusarvo, erityisesti sellaisten tutkinta-asiakirjojen (kuten asiantuntijalausunto) osalta, joita kansalliset tuomioistuimet voivat tai niiden pitää määrätä esitettäviksi arvioidakseen, onko henkilötietojen

[19] Ks. erityisesti unionin tuomioistuimen 5.9.2019 antama tuomio Euroopan unioni v. Guardian Europe ja Guardian Europe v. Euroopan unioni (C-447/17 P ja C-479/17 P, EU:C:2019:672, 147 kohta) ja 28.10.2021 antama tuomio Vialto Consulting v. komissio (C-650/19 P, EU:C:2021:879, 138 kohta) sekä unionin yleisen tuomioistuimen 13.1.2021 antama tuomio Helbert v. EUIPO (T-548/18, EU:T:2021:4, 116 kohta) ja 29.9.2021 antama tuomio Kočner v. Europol (T-528/20, ei julkaistu, EU:T:2021:631, 61 kohta), jossa muistutetaan, että kolmen edellytyksen on täytyttävä eli ”unionin toimielimen moitittu toiminta on lainvastaista, vahinko on tosiasiassa syntynyt ja toimielimen toiminnan ja väitetyn vahingon välillä on syy-yhteys”.

rekisterinpitäjä toteuttanut tässä asetuksessa tarkoitettuja asianmukaisia toimenpiteitä. Katson näin ollen, että koska tätä alaa koskevia yhdenmukaistettuja oikeussääntöjä ei ole annettu, kunkin jäsenvaltion sisäisessä oikeusjärjestyksessä on annettava tällaiset yksityiskohtaiset menettelysäännöt, kuitenkin sillä edellytyksellä, että vastaavuus- ja tehokkuusperiaatteita noudatetaan.

57. Niin kutsuttu ”tehokkuusperiaate”, joka edellyttää sitä, että riippumattoman tuomioistuimen on suoritettava puolueeton arviointi, saattaisi vaarantua, jos adjektiivi ”riittävä” pitäisi ymmärtää siten kuin ennakkoratkaisua pyytänyt tuomioistuin mielestäni sen ymmärtää ja jos siis asiantuntijalausunnosta voitaisiin automaattisesti päätellä, että rekisterinpitäjän toteuttamat toimenpiteet ovat asianmukaisia. [20]

E Neljäs ennakkoratkaisukysymys

58. Ennakkoratkaisua pyytänyt tuomioistuin tiedustelee neljännellä kysymyksellään lähinnä, onko yleisen tietosuoja-asetuksen 82 artiklan 3 kohtaa tulkittava siten, että jos kyseistä asetusta ovat rikkoneet (kuten tässä tapauksessa, 4 artiklan 12 kohdassa tarkoitetulla tavalla henkilötietojen ”luvattomalla luovuttamisella” tai ”luvattomalla pääsyllä tietoihin”) henkilöt, jotka eivät ole tällaisten tietojen rekisterinpitäjän palveluksessa eivätkä kuulu sen määräysvaltaan, tämä on seikka, josta rekisterinpitäjä ei ole millään tavalla vastuusta ja joka siten oikeuttaa sen vapauttamiseen vastuusta 82 artiklan 3 kohdassa tarkoitetulla tavalla.

59. Vastaus kysymykseen seuraa suoraan siitä, mitä edellä esitettiin yleisen tietosuoja-asetuksen yleisestä filosofiasta: automaatiosta ei ole säädetty, joten pelkästään se seikka, että henkilötietojen luvatun luovuttaminen tai luvaton pääsy tietoihin on johtunut rekisterinpitäjän määräysvaltaan kuulumattomista henkilöistä, ei vapauta viimeksi mainittua vastuusta.

60. Huomautettakoon ensinnäkin sanamuodon perusteella, että 82 artiklan 3 kohdassa sen enempää kuin johdanto-osan 146 perustelukappaleessakaan ei vahvisteta erityisiä edellytyksiä, jotka voitaisiin täyttää, jotta rekisterinpitäjä vapautuisi vastuusta, lukuun ottamatta sen osoittamista, ettei ”se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta”. Tästä sanamuodosta ilmenee yhtäältä, että rekisterinpitäjä voidaan vapauttaa vastuusta vain, jos osoitetaan, että tapahtuma, joka on aiheuttanut kyseisen vahingon, ei johdu siitä, ja toisaalta, että kyseisessä säännöksessä edellytetty näytön taso on korkea, koska on käytetty ilmaisua ”millään tavoin”, kuten komissio on korostanut. [21]

61. Yleisen tietosuoja-asetuksen 82 artiklassa ja yleisemmin koko asetuksessa säädettyä vastuujärjestelyä on käsitelty laajasti eri jäsenvaltioiden oikeuskirjallisuudessa. Se sisältää näet sopimussuhteen ulkopuoliselle vastuulle ominaisia perinteisiä osatekijöitä mutta myös osatekijöitä, jotka säännösten rakenteessa muistuttavat sopimussuhteeseen perustuvaa vastuuta tai jopa eräänlaista objektiivista vastuuta, kun otetaan tietojenkäsittelytoimintaan

[20] Kirjalliset huomautukset, 39 kohta.

[21] Unionin tuomioistuimen vakiintuneessa oikeuskäytännössä, jonka mukaan yleissäännöstä tehtäviä poikkeuksia on tulkittava suppeasti, esitetyn mukaisesti 82 artiklan 3 kohdassa säädettyä mahdollisuutta vapautua vastuusta on tulkittava suppeasti. Ks. analogisesti tuomio 15.10.2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, 53 kohta) ja tuomio 5.4.2022, Commissioner of An Garda Síochána ym. (C-140/20, EU:C:2022:258, 40 kohta).

erottamattomasti liittyvät vaarat huomioon. Tämä ei ole mielestäni tilanne, jossa käyty keskustelu olisi otettava huomioon, sillä 82 artiklassa ei mielestäni vahvisteta objektiivisen vastuun mukaista järjestelyä. [22]

62. Henkilötietojen tietoturvaloukkauksesta aiheutuva vahinko voi olla tuottamuksellinen seuraus siitä, että kohtuullisten teknisten ja organisatoristen toimenpiteiden toteuttaminen on laiminlyöty, vaikka niillä olisi voitu estää vahinko, kun otetaan tietojen käsittelyyn liittyvät ihmisten oikeuksille ja vapauksille aiheutuvat riskit huomioon. Tällaiset riskit tekevät velvollisuudesta estää ja välttää vahinko ankaramman ja laajentavat rekisterinpitäjälle kuuluvaa huolellisuusvelvoitetta. Kun rekisterinpitäjien toimimisvelvollisuuksia ja säännöstä, joka koskee näyttöä, joka vahingon aiheuttajan on esitettävä vapautuakseen vastuusta, luetaan yhdessä, on siis mahdollista puoltaa sitä, että tunnustetaan oletetusta tuottamuksesta johtuva tiukempi vastuu yleisen tietosuoja-asetuksen 82 artiklassa tarkoitetun henkilötietojen lainvastaiseen käsittelyyn liittyvän vastuun yhteydessä. [23]

63. Tästä seuraa rekisterinpitäjän mahdollisuus esittää vapauttava näyttö (jota ei sallita objektiivisen vastuun yhteydessä). Todistustaakan osalta yleisen
tietosuoja-asetuksen 82 artiklan 3 kohdassa vahvistetaan vahinkoa kärsineelle edullinen järjestelmä, kun siinä säädetään eräänlaisesta todistustaakan kääntämisestä, kun on osoitettava vahingon aiheuttajan tuottamus, [24] mikä vastaa täysin edellä mainittua todistustaakan kääntämistä toteutettujen toimenpiteiden asianmukaisuuden osalta. Lainsäätäjä osoittaa siten olevansa tietoinen vaaroista, joita liittyy siihen, että hyväksytään erilainen todistustaakan jako; jos vahinkoa kärsinyt luonnollinen henkilö velvoitettaisiin osoittamaan vahingon aiheuttajan tuottamus, hänen asemaansa heikennettäisiin liikaa ja vaarannettaisiin siis tosiasiallisesti vahingonkorvaussuojan toimivuus uuden teknologian käyttöön liittyvien oikeussääntöjen yhteydessä. Saattaisi näet osoittautua rekisteröidylle erityisen hankalaksi selvittää vahingon aiheutumiseen liittyvät yksityiskohtaiset tiedot ja saada tutustua niihin sekä osoittaa siten rekisterinpitäjän tuottamus. Rekisterinpitäjä on sitä vastoin paremmassa asemassa esittämään vapauttavan näytön osoittaakseen, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta. [25]

64. Rekisterinpitäjän on niin ikään osoitettava edellä kuvatun osoitusvelvollisuuden periaatteen mukaisesti tehneensä kaiken mahdollisen palauttaakseen nopeasti henkilötietojen saatavuuden ja pääsyn tietoihin.

[22] Siviilioikeudellista vastuuta luonnehditaan yleensä objektiiviseksi vastuuksi aina kun oikeussubjekti on velvollinen toteuttamaan kaikki abstraktisti mahdolliset toimenpiteet välttääkseen vahingon, riippumatta siitä, onko asianomainen todellisuudessa tiennyt niistä tai niiden taloudellisesta kestävyydestä. Toisaalta silloin kun oikeussubjekti on velvollinen toteuttamaan toimenpiteitä, jotka vastaavan talouden alan toimija normaalisti ottaa huomioon säilyttääkseen turvallisuuden ja estääkseen vahingot, joita harjoitetusta toiminnasta saattaa aiheutua, vahingon syyksilukeminen siirtyy yleensä erityistä tuottamusta edellyttävän vastuujärjestelyn piiriin. Em. Gambini, M., Responsabilità, s. 1055.

[23] Em. Gambini, M., Responsabilità, s. 1059. Ks. vastaavasti mielipide, jonka mukaan näyttö siitä, että asianmukaisia toimenpiteitä on toteutettu, ei voi koostua pelkästään siitä, että väitetään, että suurinta vaadittavissa olevaa huolellisuutta on noudatettu, vaan myös siitä, että osoitetaan vahingon aiheuttanut ulkopuolinen tekijä, joka on ollut ennakoimaton ja väistämätön, koska tapaus on ollut sattumanvarainen ja force majeure -tapahtuma, Sica, S., ”Sub art. 82”, teoksessa D’Orazio, R., Finocchiaro, G., Pollicino, O. ja Resta, G., Codice della privacy e *data protection*, Giuffrè, 2021.

[24] “Jos se *osoittaa*, ettei se ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta” (82 artiklan 3 kohta).

[25] Em. Gambini, M., Responsabilità, s. 1060.

65. Palatakseni ennakkoratkaisua pyytäneen tuomioistuimen kysymykseen sen perusteella, mitä tähän mennessä olen esittänyt rekisterinpitäjän vastuun luonteesta, totean, että vaikka rekisterinpitäjä voi edellä mainitulla tavalla vapautua vastuusta osoittamalla, että tietomurto johtuu seikasta, josta se ei ole millään tavalla vastuussa, tällaisena osoituksena ei voida pitää pelkästään sitä, että tapahtuman on aiheuttanut oikeussubjekti, joka ei kuulu sen määräysvaltaan.

66. Kun rekisterinpitäjä on joutunut kyberrikollisten hyökkäyksen kohteeksi, voitaisiin katsoa, että vahingon taustalla oleva tapahtuma ei johdu rekisterinpitäjästä, mutta ei ole mahdotonta, että rekisterinpitäjän huolimattomuus on kyseisen hyökkäyksen taustalla sen vuoksi, että se on helpottanut hyökkäystä, koska henkilötietojen turvallisuuden varmistavia toimenpiteitä, joita viimeksi mainittu on velvollinen toteuttamaan, ei ole toteutettu tai ne eivät ole olleet asianmukaisia. Kyseessä ovat kunkin yksittäistapauksen osalta erikseen suoritettavat tosiseikkoja koskevat arvioinnit, jotka kuuluvat asiaa käsittelevän kansallisen tuomioistuimen tehtäväksi sille esitettyjen todisteiden valossa.

67. Todettakoon tämän jälkeen, että yleisen kokemuksen mukaan julkisten tai yksityisten oikeussubjektien järjestelmiin, joissa on suuria määriä henkilötietoja, kohdistuvat ulkoiset hyökkäykset ovat huomattavasti yleisempiä kuin sisäiset hyökkäykset. Rekisterinpitäjän on näin ollen toteutettava asianmukaiset toimenpiteet estääkseen erityisesti ulkoiset hyökkäykset.

68. Huomautettakoon lopuksi teleologisesta näkökulmasta, että yleisen tietosuoja-asetuksen tavoitteena on korkea suojan taso. Unionin tuomioistuin on jo korostanut tältä osin, että asetuksen 1 artiklan 2 kohdasta, luettuna yhdessä sen johdanto-osan 10, 11 ja 13 perustelukappaleen kanssa, seuraa, että kyseisessä asetuksessa asetetaan unionin toimielimille, elimille ja laitoksille sekä jäsenvaltioiden toimivaltaisille viranomaisille tehtäväksi varmistaa SEUT 16 artiklassa ja perusoikeuskirjan 8 artiklassa taattujen oikeuksien suojan korkea taso.[26]

69. Mikäli unionin tuomioistuin valitsisi tulkinnan, jonka mukaan silloin, kun yleistä tietosuoja-asetusta on rikkonut jokin kolmas osapuoli, rekisterinpitäjä pitäisi automaattisesti vapauttaa 82 artiklan 3 kohdan mukaisesta vastuusta, tällaisen tulkinnan vaikutus ei sopisi yhteen kyseisen säännöksen mukaisen suojelun tavoitteen kanssa, koska sillä heikennettäisiin rekisteröityjen oikeuksia rajoittamalla tällainen vastuu koskemaan vain tapauksia, joissa rikkominen johtuu henkilöistä, jotka kuuluvat tämän rekisterinpitäjän alaisuuteen ja/tai määräysvaltaan.

F Viides ennakkoratkaisukysymys

70. Kansallinen tuomioistuin pyytää viidennellä kysymyksellään unionin tuomioistuinta lähinnä tulkitsemaan yleisen tietosuoja-asetuksen 82 artiklan käsitettä ”henkinen kärsimys” (josta asetuksessa käytetään nimitystä ”aineeton vahinko”). Se tiedustelee erityisesti, onko asetuksen 82 artiklan 1 ja 2 kohdan säännöksiä, luettuina yhdessä sen johdanto-osan 85

[26] Ks. vastaavasti tuomio 15.6.2021, Facebook Ireland ym. (C-645/19, EU:C:2021:483, 44 ja 45 kohta).

ja 146 perustelukappaleen kanssa,[27] tulkittava siten, että tilanteessa, jossa tämän asetuksen rikkominen johtui siitä, että kyberrikolliset olivat päässeet luvattomasti henkilötietoihin ja luovuttaneet tällaisia tietoja luvattomasti, rekisteröidyn pelko henkilötietojensa mahdollisesta tulevasta väärinkäytöstä voi sellaisenaan merkitä vahinkoa (henkistä kärsimystä), joka antaa oikeuden korvaukseen.

71. Yleisen tietosuoja-asetuksen 82 artiklassa sen enempää kuin vahingonkorvausta koskevissa johdanto-osan perustelukappaleissakaan ei anneta selvää vastausta tähän kysymykseen, mutta niistä voidaan johtaa joitakin tarkastelun kannalta hyödyllisiä seikkoja: aineeton vahinko (tai henkinen kärsimys) voidaan korvata aineellisen vahingon (tai omaisuusvahingon) lisäksi; kyseisen asetuksen rikkomista ei automaattisesti seuraa vahinko, jonka se on ”aiheuttanut”, tai, tarkemmin sanoen, henkilötietojen tietoturvaloukkaus ”voi aiheuttaa” fyysisiä, aineellisia tai aineettomia vahinkoja luonnollisille henkilöille; vahingon käsitettä pitäisi tulkita ”laajasti” unionin tuomioistuimen oikeuskäytännön valossa siten, että kunnioitetaan kaikilta osin yleisen tietosuoja-asetuksen tavoitteita; ”aiheutuneen” vahingon korvauksen on oltava ”täysi ja tosiasiallinen”.

72. Jo yleisen tietosuoja-asetuksen säännösten sanamuoto poistaa sen mahdollisuuden, että voitaisiin viitata vahinkoihin in re ipsa: asetuksessa säädetyn siviilioikeudellisen vastuun pääasiallisena tavoitteena on täyttää rekisteröidyn vaatimukset nimenomaan myöntämällä kärsitystä vahingosta ”täysi ja tosiasiallinen” korvaus ja palauttamalla sen oikeudellisen tilanteen tasapaino, jota oikeuden loukkaaminen on kielteisesti muuttanut.[28]

73. Toisaalta myös systemaattisesta näkökulmasta yleisessä tietosuoja-asetuksessa säädetään, kuten kartellilainsäädännössä, kahdesta suojan tukipilarista: ensinnäkin julkisoikeudellisesta määräämällä seuraamuksista siltä varalta, että kyseisen asetuksen säännöksiä rikotaan, toiseksi yksityisoikeudellisesta määräämällä nimenomaan sopimussuhteen ulkopuolisesta siviilioikeudellisesta vastuusta, jota voidaan pitää ankarana tiukennettuna myös vapauttavan näytön esittämisen osalta silloin, kun kyseessä katsotaan olevan edellä mainitun kaltainen tuottamus.[29]

74. Näin ollen vahingon (henkisen kärsimyksen) käsitteen laajentava[30] tulkinta ei voi ulottua niin pitkälle, että lainsäätäjä olisi luopunut vaatimasta sitä, että varsinaista ”vahinkoa” on aiheutunut.

[27] Yleisen tietosuoja-asetuksen johdanto-osan 85 perustelukappale: ”Jos henkilötietojen tietoturvaloukkaukseen ei puututa riittävän tehokkaasti ja nopeasti, siitä voi aiheutua luonnollisille henkilöille fyysisiä, aineellisia tai aineettomia vahinkoja – –”. Johdanto-osan 146 perustelukappale: ”Rekisterinpitäjän tai henkilötietojen käsittelijän olisi korvattava luonnollisille henkilöille vahingot, jotka ovat aiheutuneet tietojenkäsittelystä, jossa on rikottu tätä asetusta. Rekisterinpitäjä tai henkilötietojen käsittelijä olisi vapautettava korvausvelvollisuudesta, jos se osoittaa, ettei se ole millään tavalla vastuussa kyseisestä vahingosta. Vahingon käsite olisi tulkittava laajasti unionin tuomioistuimen oikeuskäytännön perusteella ja tavalla, jossa tämän asetuksen tavoitteet otetaan kaikilta osin huomioon. Tämä ei vaikuta korvausvaatimuksiin, jotka johtuvat unionin oikeuden tai jäsenvaltion lainsäädännön muiden sääntöjen rikkomisesta. – – Rekisteröityjen olisi saatava täysi ja tosiasiallinen korvaus aiheutuneesta vahingosta – –”.

[28] Ks. em. julkisasiamies Campos Sánchez-Bordonan ratkaisuehdotus, 29 kohta ja alaviite 11. Julkisasiamies päättää perustellusti sanamuotoon, syntyhistoriaan, asiayhteyteen ja teleologiseen tulkintaan perustuvan tarkastelunsa siten, että hän poissulkee sen, että 82 artiklan perusteella rekisteröidyille vahingoista suoritettava korvaus olisi “rangaistusluonteinen” (27–55 kohta), ja korostaa yhtäältä, että jäsenvaltioiden “ei tietosuojan takaamiseksi tarvitse (eivätkä ne todellisuudessa voi) valita VIII lukuun sisältyvien mekanismien välillä. Kun kyseessä on rikkominen, josta ei aiheudu vahinkoa, rekisteröidylle on vielä (vähintäänkin) annettava oikeus tehdä kantelu valvontaviranomaiselle”, ja toisaalta, että ”mahdollisuus saada korvausta ilman minkäänlaista vahinkoa kannustaisi todennäköisesti panemaan vireille siviilioikeudellisia riita-asioita, joissa esitetyt vaatimukset eivät välttämättä aina olisi perusteltuja, ja se voisi tältä osin tehdä tietojenkäsittelytoiminnasta vähemmän houkuttelevaa” (54 ja 55 kohta).

[29] Korvauksen epääminen rekisteröidyltä sen vuoksi, että tietojenkäsittelyä koskevien sääntöjen rikkomiseen liittyvät tunteet tai tuntemukset ovat vähäisiä tai ohimeneviä, ei näin ollen merkitse rekisteröidyn täydellistä sivuuttamista. Ks. em. julkisasiamies Campos Sánchez-Bordonan ratkaisuehdotus, 115 kohta).

[30] Tai tulkinta ”laajasti”, kuten johdanto-osan 146 kohdassa todetaan.

75. Todellinen ja merkittävä ongelma liittyy siihen, voiko sen jälkeen, kun tietomurto ja syy-yhteys on todettu, syntyä oikeus korvaukseen pelkästään sillä perusteella, että rekisteröity huolestuu, on ahdistunut ja pelkää sen vuoksi, että hänen henkilötietojaan mahdollisesti käytetään väärin tulevaisuudessa, kun tällaista väärinkäyttöä ei ole todettu ja/tai rekisteröidylle ei ole aiheutunut mitään muuta vahinkoa.

76. Unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan silloin, kun unionin oikeussääntö ei sisällä nimenomaista viittausta jäsenvaltioiden oikeuteen säännöksen merkityksen ja ulottuvuuden määrittämiseksi, sitä on yleensä tulkittava itsenäisesti ja yhtenäisesti koko unionissa, ja sen tulkitsemisessa on otettava huomioon sen sanamuoto, asiayhteys, johon se kuuluu, ja toimella, jonka osa se on, tavoiteltavat päämäärät sekä kyseisen oikeussäännön syntyhistoria.[31]

77. Kuten julkisasiamies Campos Sánchez-Bordona on muistuttanut,[32] unionin tuomioistuin ei ole laatinut yleistä vahingon määritelmää, jota sovellettaisiin erotuksetta millä tahansa alalla.[33] Henkisen kärsimyksen osalta sen oikeuskäytännöstä voidaan johtaa seuraavaa: kun yksi tulkittavan säännöksen tavoitteista on yksilön tai tietyn yksilöiden ryhmän[34] suojelu, vahingon käsitteen on oltava laaja; tämän perusteen mukaisesti korvaus ulottuu aineettomaan vahinkoon silloinkin, kun tätä ei ole mainittu tulkittavassa oikeussäännössä.[35]

78. Vaikka unionin tuomioistuimen oikeuskäytännön perusteella voidaan katsoa, että edellä esitetyn mukaisesti unionin oikeudessa on olemassa aineettoman vahingon korvaamista koskeva periaate, olen julkisasiamies Campos Sánchez-Bordonan kanssa samaa mieltä siitä, että siitä ei voida johtaa sääntöä, jonka mukaisesti *kaikki* aineeton vahinko olisi sen vakavuudesta riippumatta korvattava.[36]

79. Tässä yhteydessä on merkityksellistä erottaa toisistaan korvattava aineeton vahinko ja muut *lain rikkomisesta aiheutuvat haitat*, jotka eivät vähäisyytensä vuoksi välttämättä antaisi oikeutta korvaukseen.[37]

[31] Ks. tuomio 15.4.2021, The North of England P & I Association (C-786/19, EU:C:2021:276, 48 kohta) ja tuomio 10.6.2021, KRONE - Verlag (C-65/20, EU:C:2021:471, 25 kohta).

[32] Ks. em. julkisasiamies Campos Sánchez-Bordonan ratkaisuehdotus, 104 kohta.

[33] Se ei myöskään ole todennut, kumpi tulkintatapa – itsenäinen vai viittaus kansallisiin oikeusjärjestyksiin – on suositeltavampi: se riippuu tutkittavasta aiheesta. Vrt. viallisten tuotteiden osalta tuomio 10.5.2001, Veedfald (C-203/99, EU:C:2001:258, 27 kohta), lentoliikenteen harjoittajien vastuun osalta tuomio 6.5.2010, Walz (C-63/09, EU:C:2010:251, 21 kohta) ja autoiluista johtuvista vahingoista aiheutuvan siviilivastuun osalta tuomio 10.6.2021, Van Ameyde España (C-923/19, EU:C:2021:475, 37 kohta ja sitä seuraavat kohdat).

[34] Esim. tuotteiden kuluttajat tai liikenneonnettomuuksien uhrit.

[35] Ks. valmismatkojen osalta tuomio 12.3.2002, Leitner (C-168/00, EU:C:2002:163) ja moottoriajoneuvojen käyttöön liittyvän vastuun alalla tuomio 24.10.2013, Haasová (C-22/12, EU:C:2013:692, 47–50 kohta), tuomio 24.10.2013, Drozdovs (C-277/12, EU:C:2013:685, 40 kohta) ja tuomio 23.1.2014, Petillo (C-371/12, EU:C:2014:26, 35 kohta).

[36] Ks. em. julkisasiamies Campos Sánchez-Bordonan ratkaisuehdotus, 105 kohta. Unionin tuomioistuin on todennut unionin oikeussääntöjen mukaiseksi esimerkiksi kansallisen lain, jossa laskettaessa korvausta erotetaan toisistaan onnettomuudesta aiheutuneisiin henkilövahinkoihin liittyvät aineettomat vahingot onnettomuuden syyn mukaan; ks. 23.1.2014 annetun tuomion Petillo (C-371/12, EU:C:2014:26) tuomiolauselma: unionin oikeus ei ole esteenä "kansalliselle lainsäädännölle, jossa säädetään lievistä terveyteen kohdistuvista henkilövahingoista, jotka ovat aiheutuneet moottoriajoneuvojen käyttöön liittyvistä tieliikenneonnettomuuksista, johtuvien aineettomien vahinkojen korvaamista koskevasta erityisestä järjestelmästä ja rajoitetaan näiden vahinkojen korvaamista verrattuna muista syistä kuin tieliikenneonnettomuuksista aiheutuneiden samanlaisten vahinkojen korvaamiseen".

[37] Tämä erottelu on tehty joissain kansallisissa oikeusjärjestyksissä, koska se välttämättä liittyy yhteiskunnassa elämiseen. Ks. tietosuojan osalta äskettäin Italiassa annettu Tribunale di Palermon (Palermon alioikeus) siviilioikeudellisten asioiden I jaoston tuomio 5.10.2017, nro 5261 ja Cass. Civ., Ord. (ylin tuomioistuin) siviilioikeudellisten asioiden VI jaoston määräys nro 17383/2020. Saksassa mm. AG Diez (Diezin alioikeus), 7.11.2018 – 8 C 130/18; LG Karlsruhe (Karlsruhen alueellinen alioikeus), 02.08.2019 – 8 O 26/19, ja AG Frankfurt am Main (Frankfurt am Mainin alioikeus), 10.7.2020 – 385 C 155/19 (70). Itävallassa OGH (ylin tuomioistuin) 6 Ob 56/21k.

80. Unionin tuomioistuin tunnustaa tämän eron, kun se viittaa haittoihin ja vaivoihin erillisenä ryhmänä vahinkojen ryhmään nähden aloilla, joilla se katsoo, että ne on korvattava. [38]

81. Empiirisesti voidaan havaita, että mikä tahansa henkilötietojen suojaa koskevan säännöksen rikkominen aiheuttaa rekisteröidyssä kielteisen reaktion. Korvaus, joka pitäisi suorittaa pelkästään pahasta mielestä, joka johtuu siitä, että toinen henkilö ei ole noudattanut lakia, sekoittuisi helposti korvaukseen, joka suoritettaisiin ilman vahinkoa, mikä, kuten edellä olen todennut, ei vaikuttaisi olevan mahdollinen yleisen tietosuoja-asetuksen 82 artiklan mukaisessa tilanteessa.

82. Se, että pääasian kohteena olevien kaltaisissa olosuhteissa henkilötietojen väärinkäyttö on vain mahdollista mutta ei vielä tosiasiallista, riittää siihen, että voidaan katsoa, että rekisteröidylle on voinut aiheutua henkistä kärsimystä yleisen tietosuoja-asetuksen rikkomisesta, sillä edellytyksellä, että rekisteröity osoittaa, että tällaisen väärinkäytön pelko on konkreettisesti ja erityisesti aiheuttanut hänen tunne-elämälleen todellista ja varmaa vahinkoa. [39]

83. Pelkkien harmien (jotka eivät ole korvattavia) ja varsinaisten aineettomien vahinkojen (jotka ovat korvattavia) välinen raja on ilman muuta hiuksenhieno, mutta kansallisten tuomioistuinten, joiden tehtävänä on vetää tämä raja tapauskohtaisesti, pitäisi arvioida tarkasti kaikkia korvausta vaativan rekisteröidyn esittämiä tietoja, sillä hänen tehtävänään on esittää täsmällisesti, eikä vain yleisesti, konkreettisia seikkoja, jotka voivat johtaa siihen, että henkilötietojen tietoturvaloukkauksen voidaan katsoa ”tosiasiallisesti aiheuttaneen henkistä kärsimystä”, vaikka tämä ei ylitä ennalta määrättyä erityisen vakavuuden kynnystä: ratkaisevaa on, että kyseessä ei ole pelkkä subjektiivinen, vaihteleva ja myös muista luonteenpiirteistä ja henkilökohtaisista ominaisuuksista johtuva kokemus, vaan objektiivinen arvio haitasta, joka on kylläkin lievä mutta konkretisoitavissa oleva ja jota aiheutuu omalle fyysisestä tai psyykkiselle hyvinvoinnille tai omalle elämänpiirille; kyseessä olevien henkilötietojen luonne ja niiden merkitys rekisteröidyn elämässä ja kenties myös yhteiskunnassa kyseisellä hetkellä vallitseva käsitys kyseisestä nimenomaisesta tietoturvaloukkaukseen liittyvästä haitasta. [40]

IV Ratkaisuehdotus

84. Edellä esitetyn perusteella ehdotan, että unionin tuomioistuin vastaa esitettyihin ennakkoratkaisukysymyksiin seuraavasti:

Asetuksen 2016/679 5, 24, 32 ja 82 artiklaa on tulkittava siten, että

[38] Ks. tuomio 23.10.2012, Nelson ym. (C-581/10 ja C-629/10, EU:C:2012:657, 51 kohta), joka koskee tiettyjen kansainvälistä ilmakuljetusta koskevien sääntöjen yhtenäistämisestä Montrealissa 28.5.1999 tehdyn yleissopimuksen 19 tarkoitettujen ”vahinkojen” ja asetuksen N:o 261/2004 tarkoitettujen ”haittojen”, jotka on 19.11.2009 annetun tuomion Sturgeon ym. (C-402/07 ja C-432/07, EU:C:2009:716) mukaan korvattava sen 7 artiklan nojalla, välistä eroa. Tällaisella alalla, kuten kuljetettaessa matkustajia meri- ja sisävesiliikenteessä, mihin viitataan asetuksessa N:o 1177/2010, lainsäätäjä on voinut tunnustaa abstraktin ryhmän haitan määrittäväksi osatekijäksi, ja sellaisen puuttuessa ne ovat samoja kaikille asianomaisille henkilöille. Mielestäni tällainen päätelmä ei ole mahdollinen tietosuojan yhteydessä.

[39] Irlannin mukaan nämä seikat ovat käytännössä erityisen tärkeitä kyberrikollisuuden yhteydessä, koska jos jokaisella henkilöllä, johon tietomurto on – vähäisimmissäkin määrin – vaikuttanut, olisi oikeus saada korvausta aineettomista vahingoista, tällä olisi vahva vaikutus erityisesti julkisen sektorin tietojen rekisterinpitäjiin, joiden toimintaa rahoitetaan rajallisista julkisista varoista ja joiden pitäisi pikemminkin palvella yhteisiä etuja, mukaan lukien henkilötietojen turvallisuuden parantaminen (kirjalliset huomautukset, 72 kohta).

[40] Ks. em. julkisasiamies Campos Sánchez-Bordonan ratkaisuehdotus, 116 kohta.

pelkkä 4 artiklan 12 kohdassa määritellyn ”henkilötietojen tietoturvaloukkauksen” olemassaolo ei sellaisenaan riitä siihen, että voitaisiin päätellä, että rekisterinpitäjän toteuttamat tekniset ja organisatoriset toimenpiteet eivät olleet ”asianmukaisia” varmistamaan kyseisten tietojen suojaa;

selvittäessään henkilötietojen rekisterinpitäjän toteuttamien teknisten ja organisatoristen toimenpiteiden asianmukaisuuden asiaa käsittelevän kansallisen tuomioistuimen on harjoitettava valvontaa, joka sisältää sekä tällaisten toimenpiteiden sisällön että niiden soveltamistavan ja käytännön vaikutusten konkreettisen arvioinnin;

henkilötietojen rekisterinpitäjällä on yleisen tietosuoja-asetuksen 82 artiklassa tarkoitetun vahingonkorvauskanteen yhteydessä todistustaakka siitä, että sen tämän asetuksen 32 artiklan nojalla toteuttamat toimenpiteet ovat asianmukaisia;

menettelyllistä itsemääräämisoikeutta koskevan periaatteen mukaisesti kunkin jäsenvaltion kansallisessa oikeusjärjestyksessä on määritettävä hyväksyttävät todistelukeinot ja niiden todistusarvo, mukaan lukien asian selvittämistoimet, joista kansalliset tuomioistuimet voivat määrätä tai niiden on määrättävä, jotta voidaan arvioida, onko rekisterinpitäjä toteuttanut tässä asetuksessa tarkoitettuja asianmukaisia toimenpiteitä, noudattamalla unionin oikeudessa määriteltyjä vastaavuus- ja tehokkuusperiaatteita;

se, että tätä asetusta on rikkonut kyseisen vahingon aiheuttaneella tavalla jokin kolmas osapuoli, ei sellaisenaan ole peruste vapauttaa rekisterinpitäjä vastuusta ja, jotta rekisterinpitäjä voisi saada kyseisen säännöksen mukaisen vapautuksen, sen on osoitettava, ettei se ole millään tavoin vastuussa tietoturvaloukkauksesta;

vahinko, joka koostuu rekisteröidyn pelosta, jonka olemassaolon rekisteröity on osoittanut ja joka koskee hänen henkilötietojensa mahdollista tulevaa väärinkäyttöä, voi merkitä henkistä kärsimystä, joka antaa oikeuden korvaukseen, sillä edellytyksellä, että rekisteröity osoittaa, että hänen tunne-elämälleen on aiheutunut erikseen todellista ja varmaa vahinkoa, mikä asiaa käsittelevän kansallisen tuomioistuimen on jokaisessa yksittäistapauksessa selvitettävä.