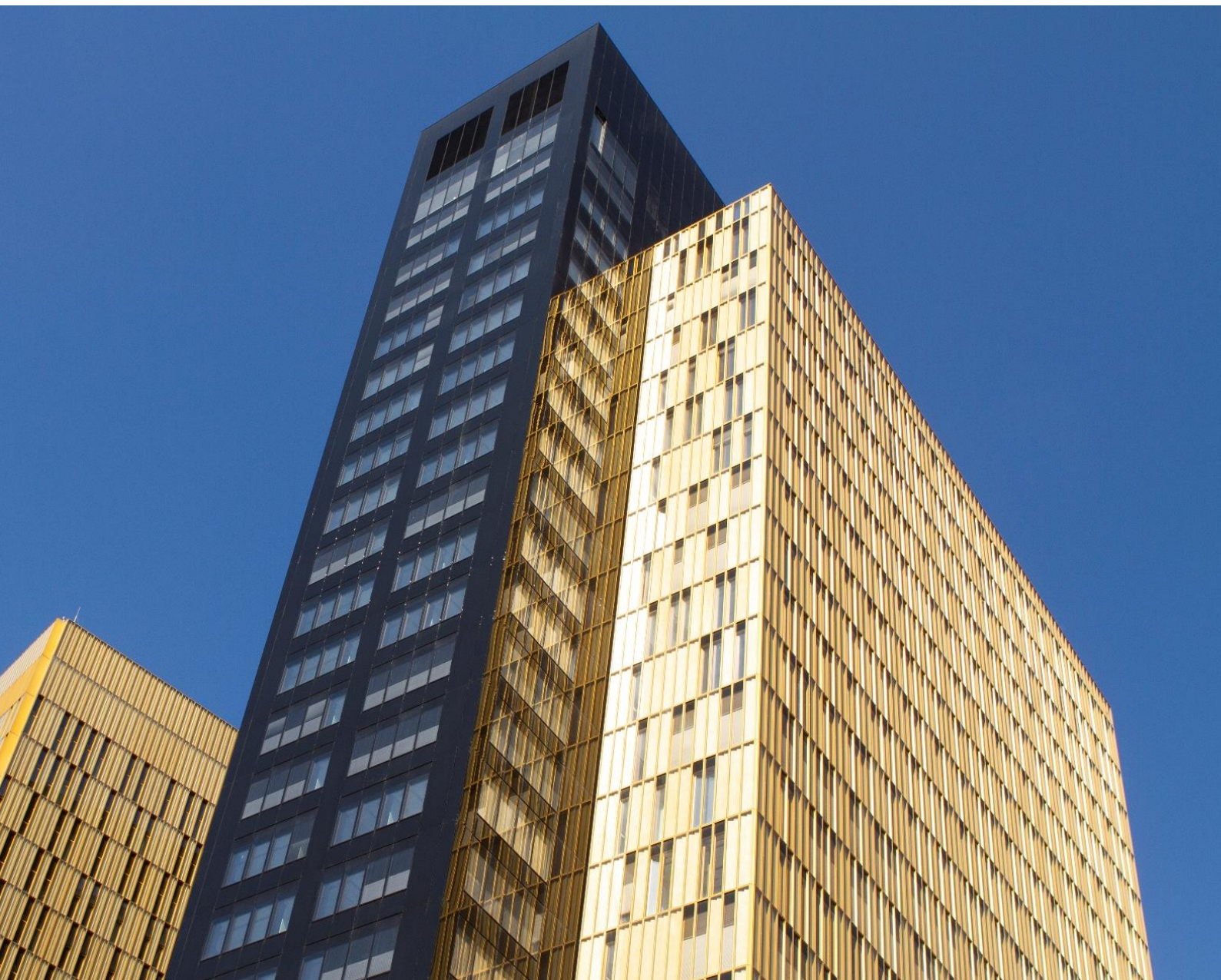




Aiheenmukainen muistio

Henkilötietojen suoja

Esipuhe

Oikeus henkilötietojen suojaan on perusoikeus, jonka noudattaminen on tärkeä tavoite Euroopan unionille.

Tämä oikeus vahvistetaan primäärioikeudessa, erityisesti Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 8 artiklassa ja Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdassa. Tämä perusoikeus liittyy kiinteästi perusoikeuskirjan 7 artiklassa vahvistettuun oikeuteen, joka koskee yksityis- ja perhe-elämän kunnioittamista.

Euroopan yhteisössä on annettu 90-luvun puolivälistä lähtien useita johdetun oikeuden säännöksiä, joilla pyritään takaamaan henkilötietojen suoja. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta annettu direktiivi 95/46/EY,¹ joka kumottiin 2018, oli ensisijainen unionin säädös tällä alalla.

Direktiiviä 95/46 täydennettiin sittemmin direktiivillä 2002/58/EY,² jolla yhdenmukaistettiin yksityisyyden suojaa koskevaa jäsenvaltioiden lainsäädäntöä erityisesti henkilötietojen käsittelyssä sähköisen viestinnän alalla.³ On huomautettava, että unionin lainsäätäjä alkoi vuodesta 2017 lähtien tarkastella kyseistä direktiiviä uudelleen⁴ teknologisen ja kaupallisen kehityksen huomioon ottamiseksi. Tämä uudelleentarkastelu jatkuu edelleen.⁵

Euroopan unioni uudisti vuonna 2016 kyseistä alaa koskevaa yleistä oikeudellista kehystä. Tuolloin annettiin henkilötietojen suojaa koskeva asetus (EU) 2016/679⁶ (jäljempänä yleinen tietosuojasetus), jolla kumottiin direktiivi 95/46 ja jota on

¹ Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annettu Euroopan parlamentin ja neuvoston direktiivi 95/46/EY (EYVL 1995, L 281, s. 31), konsolidoitu versio 20.11.2003, kumottu 25.5.2018 alkaen (ks. alaviite 6).

² Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12.7.2002 annettu Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) (EYVL 2002, L 201, s. 37), konsolidoitu versio 19.12.2009.

³ Direktiiviä 2002/58 muutettiin yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta 15.3.2006 annetulla Euroopan parlamentin ja neuvoston direktiivillä 2006/24/EY (EUVL 2006, L 105, s. 54). Unionin tuomioistuin totesi viimeksi mainitun direktiivin pätemättömäksi 8.4.2014 antamallaan tuomiolla Digital Rights Ireland ja Seitlinger ym. (C-293/12 ja C-594/12, [EU:C:2014:238](#)) sillä perusteella, että sillä loukattiin vakavasti yksityiselämän kunnioittamista koskevaa oikeutta ja oikeutta henkilötietojen suojaan (ks. jäljempänä otsikko I.1 "Unionin johdetun oikeuden yhdenmukaisuus henkilötietojen suojaa koskevan oikeuden kanssa").

⁴ Komissio antoi 10.1.2017 ehdotuksen kyseisen direktiivin korvaamiseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä annettavalla asetuksella.

⁵ Euroopan unionin neuvosto hyväksyi 10.2.2021 neuvotteluvaltuutuksen, joka koskee neuvottelujen käynnistämistä Euroopan parlamentin kanssa yksityiselämän kunnioittamista ja luottamuksellisuutta sähköisessä viestinnässä koskevien sääntöjen muuttamiseksi. Ehdotus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta annettavaksi Euroopan parlamentin ja neuvoston asetukseksi (sähköisen viestinnän tietosuojasetus) on nähtävillä internetsivulla https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN.

⁶ 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 (EUVL 2016, L 119, s. 1).

sovellettu suoraan 25.5.2018 lähtien, ja direktiivi (EU) 2016/680⁷, jolla pyritään mainittujen tietojen suojaamiseen rikosasioissa ja jonka säännöksiä on sovellettu 6.5.2018 lähtien.

EU:n toimielinten ja muiden elinten käsitellessä henkilötietoja niitä suojataan 11.12.2018 lähtien muun muassa asetuksella (EU) 2018/1725⁸. Jotta henkilötietoja suojattaisiin mahdollisimman yhdenmukaisesti unionin koko alueella, kyseisellä asetuksella pyritään saattamaan alaa koskevat säännöt mahdollisimman hyvin yleisellä tietosuoja-asetuksella luodun järjestelmän mukaisiksi.

Vastatakseen uusien teknologioiden aiheuttamiin haasteisiin unionin lainsäätäjä on vuodesta 2020 antanut uusia lainsäädäntötoimia⁹, jotka liittyvät henkilötietojen suojaan koskeviin unionin oikeuden säännöksiin.

Tässä aiheen mukaisessa muistiossa otetaan huomioon unionin tuomioistuimen rikas oikeuskäytäntö henkilötietojen suojan alalla ja esitellään valikoituja alan perustavanlaatuisia tuomioita sekä tuomioita, jotka ovat vaikuttaneet merkittävästi kyseisen oikeuskäytännön kehittymiseen, ja erityisesti unionin tuomioistuimen suuren jaoston antamia tuomioita. Tarkemmin ottaen tämän muistion on tarkoitus kattaa sekä oikeuskäytäntö, joka koskee henkilötietojen suojan alan yleistä säännöstöä ja joka liittyy direktiivin 95/46 ja yleisen tietosuoja-asetuksen tulkintaan, että oikeuskäytäntö, joka koskee alakohtaista säännöstöä muun muassa sähköisen viestinnän ja rikosoikeuden alalla. Tässä muistiossa on lisäksi tarkoitus esitellä valikoituja tuomioita, jotka koskevat monialaisia säännöstöjä, korostaen perusoikeuskirjan ratkaisevaa merkitystä oikeuskäytännön kehittämisessä.

⁷ Luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27.4.2016 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 (EUVL 2016, L 119, s. 89).

⁸ Luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta 23.10.2018 annettu Euroopan parlamentin ja neuvoston asetukset (EU) 2018/1725 (EUVL 2018, L 295, s. 39).

⁹ Tässä yhteydessä on mainittava erityisesti kolme lainsäädäntöaloitetta: i) eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta 30.5.2022 annettu Euroopan parlamentin ja neuvoston asetukset (EU) 2022/868 (datanhallinta-asetus) (EUVL 2022, L 152, s. 1) ja datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta 13.12.2023 annettu Euroopan parlamentin ja neuvoston asetukset (EU) 2023/2854 (datasäädös) (EUVL 2023, L 2854, s. 1) ii) digitaalisia palveluja ja markkinoita koskeva lainsäädäntöpaketti, joka koostuu digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta 19.10.2022 annetusta Euroopan parlamentin ja neuvoston asetuksesta (EU) 2022/2065 (digipalvelusäädös) (EUVL 2022, L 277, s. 1) ja kilpailullisista ja oikeudenmukaisista markkinoista digitaalialalla ja direktiivin (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta 14.9.2022 annetusta Euroopan parlamentin ja neuvoston asetuksesta (EU) 2022/1925 (digimarkkinasäädös) (EUVL 2022, L 265, s. 1) ja iii) ensimmäinen lainsäädäntöehdotus, jolla on tarkoitus luoda tekoälyä koskeva lainsäädäntökehys tekoälystä annetulla asetuksella (EUVL 2024, L 1689).

Sisällys

ESIPUHE	3
I. EUROOPAN UNIONIN PERUSOIKEUSKIRJASSA VAHVISTETTU OIKEUS HENKILÖTIETOJEN SUOJAAN	6
1. Unionin johdetun oikeuden yhdenmukaisuus henkilötietojen suojaa koskevan oikeuden kanssa	6
2. Henkilötietojen suojaa koskevan oikeuden noudattaminen unionin oikeuden täytäntöönpanossa	18
II. ALAN YLEISESSÄ SÄÄNNÖSTÖSSÄ TARKOITETTU HENKILÖTIETOJEN KÄSITTELY	19
1. Yleisen säännösten soveltamisala	19
2. Käsite "henkilötiedot"	25
3. Käsite "henkilötietojen käsittely"	27
4. Käsite "henkilötietojen rekisteröintijärjestelmä"	32
5. Käsite "rekisterinpitäjä"	32
6. Käsite "yhteisrekisterinpitäjä"	35
7. Henkilötietojen käsittelyn laillisuuden edellytykset	36
III. ALAKOHTAISESSA SÄÄNNÖSTÖSSÄ TARKOITETTU HENKILÖTIETOJEN KÄSITTELY	42
1. Henkilötietojen käsittely sähköisen viestinnän alalla	42
2. Henkilötietojen käsittely rikosasioissa	61
IV. HENKILÖTIETOJEN SIIRTÄMINEN KOLMANSIIN MAIHIN	64
V. HENKILÖTIETOJEN SUOJA INTERNETISSÄ	73
1. Oikeus vastustaa henkilötietojen käsittelyä ("oikeus tulla unohdetuksi")	73
2. Henkilötietojen käsittely ja immateriaalioikeudet	74
3. Henkilötietojen poistaminen hakutulosten luettelosta	76
4. Internetsivun käyttäjän suostumus tietojen tallentamiseen	85
5. Henkilötietojen käsittely verkkoyhteisöpalveluissa	87
VI. KANSALLISET VALVONTAVIRANOMAISET	90
1. Riippumattomuusvaatimuksen ulottuvuus	90
2. Sovellettavan oikeuden ja toimivaltaisen valvontaviranomaisen määrittäminen	93
3. Kansallisten valvontaviranomaisten toimivalta	95
4. Hallinnollisten seuraamusmaksujen määräämisedellytykset	100
5. Kansallisten valvontaviranomaisten toimivallan suhde muiden kansallisten viranomaisten toimivaltaan	104

I. Euroopan unionin perusoikeuskirjassa vahvistettu oikeus henkilötietojen suojaan

1. Unionin johdetun oikeuden yhdenmukaisuus henkilötietojen suojaan koskevan oikeuden kanssa

Tuomio 9.11.2010 (suuri jaosto), Volker und Markus Schecke ja Eifert (C-92/09 ja C-93/09, EU:C:2010:662)

Kyseisessä asiassa pääasian oikeudenkäynneissä olivat vastakkain eräät maanviljelijät ja Land Hessen (Hessenin osavaltio), ja asia koski Bundesanstalt für Landwirtschaft und Ernährungin (liittovaltion maatalous- ja elintarvikevirasto) internetsivustolla julkaisemia kyseisiä maanviljelijöitä koskevia henkilötietoja, jotka liittyivät tukiin, joita he saivat Euroopan maatalouden tukirahastosta (maataloustukirahasto) (FEAGA) ja Euroopan maaseudun kehittämisen maatalousrahastosta (maaseuturahasto) (Feader). Maanviljelijät vastustivat kyseistä julkaisemista ja väittivät erityisesti, ettei se ollut perusteltua pakottavan yleisen edun vuoksi. Land Hessen puolestaan katsoi, että näiden tietojen julkaiseminen perustui asetuksiin (EY) N:o 1290/2005¹⁰ ja (EY) N:o 259/2008¹¹, joilla säännellään yhteisen maatalouspolitiikan rahoitusta ja joissa edellytetään maataloustukirahastosta ja maaseuturahastosta tukea saavia luonnollisia henkilöitä koskevien tietojen julkaisemista.

Tässä tilanteessa Verwaltungsgericht Wiesbaden (Wiesbadenin hallinto-oikeus, Saksa) esitti unionin tuomioistuimelle useita ennakkoratkaisukysymyksiä asetusten N:o 1290/2005 ja N:o 259/2008 eräiden säännösten pätevyydestä. Kyseessä olevilla säännöksillä edellytettiin tällaisten tietojen saattamista yleisön saataville esimerkiksi kansallisten virastojen ylläpitämien internetsivustojen välityksellä.

Unionin tuomioistuin totesi perusoikeuskirjassa tunnustetun henkilötietojen suojaan koskevan oikeuden ja eurooppalaisia rahastoja koskevan avoimuusvelvoitteen välisestä yhteydestä, että tietojen, joissa mainitaan tuensaajien nimet ja heidän saamansa tarkat määrät, julkaisemisella internetsivustolla loukataan – koska ulkopuoliset saavat pääsyn näihin tietoihin – tuensaajien oikeutta yksityiselämäänsä ja erityisesti heidän oikeuttaan henkilötietojen suojaan.

¹⁰ Yhteisen maatalouspolitiikan rahoituksesta 21.6.2005 annettu neuvoston asetus (EY) N:o 1290/2005 (EUVL 2005, L 209, s. 1), joka on kumottu yhteisen maatalouspolitiikan rahoituksesta, hallinnoinnista ja seurannasta 17.12.2013 annetulla Euroopan parlamentin ja neuvoston asetuksella (EU) N:o 1306/2013 (EUVL 2013, L 347, s. 549).

¹¹ Asetuksen (EY) N:o 1290/2005 soveltamista koskevista yksityiskohtaisista säännöistä Euroopan maatalouden tukirahaston (maataloustukirahasto) ja Euroopan maaseudun kehittämisen maatalousrahaston (maaseuturahasto) varoja saavia tuensaajia koskevien tietojen julkaisemisen osalta 18.3.2008 annettu komission asetus (EY) N:o 259/2008 (EUVL 2008, L 76, s. 28), joka on Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1306/2013 soveltamissäännöistä maksajavirastojen ja muiden elinten, varainhoidon, tilien tarkastamisen ja hyväksymisen, tarkastuksia koskevien sääntöjen, vakuuksien ja avoimuuden osalta 6.8.2014 annetulla komission täytäntöönpanoasetuksella (EU) N:o 908/2014 (EUVL 2014, L 255, s. 59).

Tällainen loukkaaminen voisi olla oikeutettua, jos siitä säädetään lailla, jos sillä kunnioitetaan kyseisten oikeuksien ja vapauksien keskeistä sisältöä ja jos se suhteellisuusperiaatteen mukaisesti on välttämätön ja vastaa tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita. Unionin tuomioistuin katsoi tässä yhteydessä, että vaikka demokraattisessa yhteiskunnassa verovelvollisilla kyllä on oikeus saada tietoja julkisten varojen käytöstä, neuvoston ja komission piti kuitenkin arvioida kyseessä olevien eri intressien välistä tasapainoa, mikä edellytti ennen mainittujen säännösten antamista sitä, että kyseessä olevat toimielimet tutkivat, ylittikö näiden tietojen julkaiseminen yhden jäsenvaltiokohtaisen internetsivuston välityksellä sen, mikä oli tarpeen legitiimien tavoitteiden saavuttamiseksi.

Niinpä unionin tuomioistuin totesi, että eräät asetuksen N:o 1290/2005 säännökset ja asetus N:o 259/2008 kokonaisuudessaan on todettava pätemättömiksi siltä osin kuin näissä säännöksissä säädetään luonnollisten henkilöiden, jotka ovat maataloustukirahaston ja maaseuturahaston tuensaajia, osalta kutakin tuensaajaa koskevien henkilötietojen julkaisemisesta tekemättä eroa sellaisten merkityksellisten kriteerien mukaan kuin ajanjaksot, joina kyseiset luonnolliset henkilöt ovat saaneet tällaisia tukia, niiden toistuvuus tai niiden laji ja suuruus. Unionin tuomioistuin ei kuitenkaan kyseenalaistanut vaikutuksia, joita on tällaisia tuensaajia koskevien luetteloiden julkaisemisella, jonka kansalliset viranomaiset ovat toteuttaneet kyseisten säännösten nojalla tämän tuomion antamispäivää edeltäneenä ajanjaksona.

Tuomio 8.4.2014 (suuri jaosto), Digital Rights Ireland ja Seitlinger ym. (yhdistetyt asiat C-293/12 ja C-594/12, [EU:C:2014:238](#))

Kyseinen tuomio juontaa juurensa pyyntöihin arvioida tietojen säilyttämisestä annetun direktiivin 2006/24/EY pätevyyttä suhteessa perusoikeuksiin, yksityiselämän kunnioittamista koskevaan oikeuteen ja henkilötietojen suojaa koskevaan oikeuteen. Pyynnöt esitettiin kansallisissa oikeudenkäynneissä irlantilaisissa ja itävaltalaisissa tuomioistuimissa. Asiassa C-293/12 High Courtin (ylin tuomioistuin, Irlanti) ratkaistavaksi saatettiin asia, jossa vastakkain olivat Digital Rights ja Irlannin viranomaiset ja joka koski sähköiseen viestintään liittyvien tietojen säilyttämistä koskevien kansallisten säännösten lainmukaisuutta. Asiassa C-594/12 Verfassungsgerichtshofin (perustuslakituomioistuin, Itävalta) ratkaistavaksi oli saatettu useita perustuslaillisia kanteita, joissa vaadittiin kumottavaksi kansallisia säännöksiä, joilla pantiin Itävallan oikeudessa täytäntöön direktiivi 2006/24.

Irlantilainen ja itävaltalainen tuomioistuin tiedustelivat ennakkoratkaisupyynnöillään unionin tuomioistuimelta sitä, oliko direktiivi 2006/24 pätevä suhteessa perusoikeuskirjan 7, 8 ja 11 artiklaan. Täsmällisemmin sanottuna mainitut tuomioistuimet kysyivät unionin tuomioistuimelta, merkitseekö mainitussa direktiivissä yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen tarjoajille asetettu velvollisuus säilyttää tietyn ajan tietoja henkilön yksityiselämästä ja hänen viestinnästään sekä antaa toimivaltaisille kansallisille viranomaisille oikeus saada

näitä tietoja, oikeudetonta puuttumista mainittuihin perusoikeuksiin. Tiedot, joista on kyse, ovat muun muassa viestinnän lähteen ja kohteen jäljittämiseksi ja tunnistamiseksi tarvittavat tiedot, viestinnän päivämäärän, kellonajan, keston ja tyytin sekä käyttäjien viestintälaitteen määrittämiseksi tarvittavat tiedot sekä matkaviestintälaitteen sijainnin tunnistamiseksi tarvittavat tiedot, joihin kuuluu muun muassa tilaajan tai rekisteröidyn käyttäjän nimi ja osoite, soittajan puhelinnumero ja valittu numero sekä internetpalvelujen IP-protokollaosoite. Näiden tietojen avulla voidaan muun muassa saada selville, kuka on se henkilö, jonka kanssa tilaaja tai rekisteröity käyttäjä on viestinyt ja millä laitteella, sekä määrittää viestinnän ajankohta sekä paikka, josta käsin viestintä tapahtui. Niiden avulla voidaan lisäksi saada tietoon, kuinka tiheästi tilaaja tai rekisteröity käyttäjä on viestinyt tiettyjen henkilöiden kanssa tietyn ajanjakson aikana.

Unionin tuomioistuin totesi ensinnäkin, että direktiivin 2006/24 säännökset, joilla asetettiin näille palveluntarjoajille tällaisia velvoitteita, merkitsivät erityisen vakavaa puuttumista yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin, jotka taataan perusoikeuskirjan 7 ja 8 artiklassa. Unionin tuomioistuin tosin katsoi, että tämä puuttuminen saattoi olla oikeutettua yleisen edun mukaisella tavoitteella, kuten järjestäytyneen rikollisuuden torjumisella. Se totesi tästä ensinnäkin, että direktiivissä edellytetty tietojen säilyttäminen ei ole omiaan aiheuttamaan haittaa yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevien perusoikeuksien keskeiselle sisällölle, koska direktiivissä ei sallita tiedon saamista sähköisen viestinnän sisällöstä sellaisenaan ja koska siinä säädetään, että palveluntarjoajien on noudatettava tiettyjä tietosuojaa ja tietoturvaa koskevia periaatteita. Toiseksi unionin tuomioistuin huomautti, että tietojen säilyttämisellä niiden mahdolliseksi luovuttamiseksi toimivaltaisille kansallisille viranomaisille kuitenkin pyrittiin tosiasiallisesti yleisen edun mukaiseen tavoitteeseen, eli vakavan rikollisuuden torjumiseen ja loppujen lopuksi yleiseen turvallisuuteen.

Unionin tuomioistuin kuitenkin katsoi, että antaessaan tietojen säilyttämistä koskevan direktiivin unionin lainsäätäjä oli ylittänyt suhteellisuusperiaatteen kunnioittamisen asettamat rajat. Näin ollen se totesi direktiivin pätemättömäksi ja katsoi, ettei direktiivin sisältämää laajaperäistä ja erityisen vakavaa puuttumista perusoikeuksiin ollut rajoitettu riittävän tarkasti, jotta voidaan taata, että tämä puuttuminen todella rajoitetaan täysin välttämättömään. Direktiivi 2006/24 nimittäin kattaa yleisesti kaikki henkilöt ja kaikki sähköiset viestintävälineet sekä kaikki liikennetiedot ilman, että tehtäisiin mitään erottelua, rajoituksia tai poikkeuksia vakavan rikollisuuden torjunnan tavoitteen perusteella. Direktiivissä 2006/24 ei myöskään säädetä mistään objektiivisesta perusteesta, jonka nojalla voitaisiin rajoittaa toimivaltaisten kansallisten viranomaisten oikeus saada tietoja ja käyttää niitä pelkästään sellaisten rikosten estämiseen, selvittämiseen tai syyteharkintaan, jotka voidaan katsoa riittävän vakaviksi, jotta ne oikeuttavat tällaisen puuttumisen, eikä aineellisista ja menettelyllisistä edellytyksistä tällaisen tietojen saamiselle ja käyttämiselle. Direktiivissä säädettiin vähintään kuuden kuukauden ajasta tietojen säilyttämiseksi tekemättä minkäänlaista eroa sen mukaan,

kuinka hyödyllisiä ne mahdollisesti ovat tavoitellun päämäärän kannalta, tai kyseessä olevien henkilöiden mukaan.

Perusoikeuskirjan 8 artiklan 3 kohdasta aiheutuvien vaatimusten osalta unionin tuomioistuimien katsoi, ettei direktiivissä säädetä riittävästä takeista, joilla voidaan varmistaa säilytettyjen tietojen tehokas suoja väärinkäytön vaaraa vastaan sekä näiden tietojen kaikenlaista laiton saantia ja käyttöä vastaan, eikä siinä myöskään edellytetä tietojen säilyttämistä unionin alueella.

Näin ollen mainitulla direktiivillä ei taattu täysimääräisesti riippumattoman viranomaisen suorittamaa suojaa ja turvaa koskevien vaatimusten noudattamista koskevaa valvontaa.

Tuomio 21.6.2022 (suuri jaosto), Ligue des droits humains (C-817/19, [EU:C:2022:491](#))

PNR-tiedot (Passenger Name Record) ovat tietoja, joita lentoliikenteen harjoittajat tallentavat varausjärjestelmiinsä ja lähtöselvitysjärjestelmiinsä. PNR-direktiivissä¹² veloitetaan kyseiset liikenteenharjoittajat siirtämään kolmannen maan ja Euroopan unionin välillä suoritettavaa EU:n ulkopuolista lentoa käyttävien kaikkien matkustajien tiedot kyseisen lennon määräpaikan tai lähtöpaikan jäsenvaltion matkustajatietoyksikölle terrorismin ja vakavan rikollisuuden torjumiseksi. Matkustajatietoyksikkö nimittäin arvioi näin siirretyt PNR-tiedot etukäteen,¹³ minkä jälkeen tiedot säilytetään asianomaisen jäsenvaltion tai toisen jäsenvaltion toimivaltaisten viranomaisten mahdollisesti suorittamaa myöhempää arviointia varten. Jäsenvaltiot voivat päättää soveltaa tätä direktiiviä myös EU:n sisäisiin lentoihin.¹⁴

Ligue des droits humains nosti Cour de constitutionnellessa (perustuslakituomioistuin, Belgia) kumoamiskanteen Belgian laista, jolla sekä PNR-direktiivi että API-direktiivi¹⁵ saatettiin osaksi kansallista oikeusjärjestystä. Kantajan mukaan kyseinen laki loukkaa oikeutta yksityiselämän kunnioittamiseen ja henkilötietojen suojaan. Se arvosteli yhtäältä sitä, että PNR tiedot ovat erittäin laajoja, ja toisaalta sitä, että niiden kerääminen, siirtäminen ja käsittely on luonteeltaan yleistä. Kantajan mukaan laki loukkaa myös henkilöiden vapaata liikkuvuutta, koska sillä palautetaan välillisesti rajatarkastukset ulottamalla PNR-järjestelmä EU:n sisäisiin lentoihin ja muilla liikennemuodoilla unionin alueella tehtyihin matkoihin.

¹² Matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten 27.4.2016 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/681 (EUVL 2016, L 119, s. 132) (jäljempänä PNR-direktiivi).

¹³ Etukäteisarvioinnin tarkoituksena on yksilöidä henkilöt, joista toimivaltaisten viranomaisten on tehtävä lisätutkimuksia, kun otetaan huomioon se, että kyseiset henkilöt saattavat olla osallisina terrorismirikoksiin tai vakavaan rikollisuuteen. Sitä toteutetaan järjestelmällisesti ja automatisoiduin keinoin vertaamalla PNR-tietoja "olennaisiin tietokantoihin" tai käsittelemällä niitä PNR-direktiivin 6 artiklan 2 kohdan a alakohdassa ja 3 kohdassa määritettyjen kriteerien mukaisesti.

¹⁴ Käyttäen PNR-direktiivin 2 artiklassa säädettyä mahdollisuutta.

¹⁵ Liikenteenharjoittajien velvollisuudesta toimittaa tietoja matkustajista 29.4.2004 annettu neuvoston direktiivi 2004/82/EY (EUVL 2004, L 261, s. 24) (jäljempänä API-direktiivi). Kyseisellä direktiivillä säädellään sitä, että lentoliikenteen harjoittajat toimittavat toimivaltaisille kansallisille viranomaisille matkustajia koskevat tiedot (kuten käytetyn matkustusasiakirjan numero ja tyyppi sekä kansalaisuus) etukäteen rajatarkastusten tehostamiseksi ja laittoman maahanmuuton torjumiseksi.

Tässä yhteydessä Belgian perustuslakituomioistuin esitti unionin tuomioistuimelle ennakkoratkaisukysymyksiä, jotka koskivat muun muassa PNR-direktiivin pätevyyttä.

Unionin tuomioistuin vahvisti suuren jaoston kokoonpanossa antamassaan tuomiossa PNR-direktiivin pätevyyden siltä osin kuin sitä voidaan tulkita perusoikeuskirjan mukaisesti.

Unionin tuomioistuin totesi tuomiossaan, että koska unionin tuomioistuimen omaksuma PNR-direktiivin säännösten tulkitseminen Euroopan unionin perusoikeuskirjan 7, 8 ja 21 artiklassa sekä 52 artiklan 1 kohdassa¹⁶ taattujen perusoikeuksien mukaisesti varmistaa tämän direktiivin yhdenmukaisuuden perusoikeuskirjan kyseisten artiklojen kanssa, esitettyjä kysymyksiä tutkittaessa ei ole tullut esille mitään, mikä vaikuttaisi mainitun direktiivin pätevyyteen.

Unionin tuomioistuin muistutti aluksi, että unionin toimea on tulkittava niin pitkälle kuin mahdollista tavalla, joka ei aseta sen pätevyyttä kyseenalaiseksi, ja kaiken primaarioikeuden sekä erityisesti perusoikeuskirjan määräysten mukaisesti, joten jäsenvaltioiden on myös varottava tukeutumasta sellaiseen kyseisen toimen tulkintaan, joka johtaisi ristiriitaan unionin oikeusjärjestyksellä suojattujen perusoikeuksien tai muiden unionin oikeusjärjestyksessä tunnustettujen yleisten periaatteiden kanssa. PNR-direktiivin osalta unionin tuomioistuin täsmensi, että useissa kyseisen direktiivin johdanto osan perustelukappaleissa ja säännöksissä edellytetään perusoikeuksien mukaista tulkintaa, sekä korosti merkitystä, jonka unionin lainsäätäjät antaa perusoikeuskirjassa taattujen perusoikeuksien täysimääräiselle kunnioittamiselle viitatessaan tietosuojan korkeaan tasoon.

Unionin tuomioistuin totesi, että PNR-direktiiviin sisältyy selvästi vakavia puuttumisia perusoikeuskirjan 7 ja 8 artiklassa taattuihin oikeuksiin erityisesti siltä osin kuin sen tarkoituksena on ottaa käyttöön jatkuva, kohdentamaton ja järjestelmällinen valvontajärjestelmä, johon kuuluu kaikkien lentoliikennepalveluja käyttävien henkilöiden henkilötietojen automaattinen arviointi. Se muistutti, että jäsenvaltioiden mahdollisuutta oikeuttaa tällainen puuttuminen on arvioitava mittaamalla puuttumisen vakavuus ja tarkastamalla, että yleisen edun mukaisen tavoitteen tärkeys on suhteessa tähän vakavuuteen.

Unionin tuomioistuin katsoi, että kyseisessä direktiivissä säädetyn PNR-tietojen siirron, käsittelyn ja säilyttämisen voidaan katsoa olevan rajoitettuja siihen, mikä on ehdottoman välttämätöntä terrorismirikosten ja vakavan rikollisuuden torjumiseksi, edellyttäen että mainitussa direktiivissä säädettyjä toimivaltuuksia tulkitaan suppeasti. Tuomiossa todetaan tältä osin muun muassa seuraavaa:

¹⁶ Kyseisen määräyksen mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Lisäksi näille oikeuksille ja vapauksille voidaan säätää rajoituksia ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

- PNR-direktiivillä käyttöön otettu järjestelmä saa koskea vain kyseisen direktiivin liitteessä I mainittuja tietoja, jotka ovat selvästi tunnistettavissa ja rajattuja ja joilla on suora yhteys suoritettuun lentoon ja asianomaiseen matkustajaan, mikä edellyttää tiettyjen kyseisessä liitteessä olevien nimikkeiden osalta sitä, että järjestelmä koskee vain nimenomaisesti mainittuja tietoja.¹⁷
- PNR-direktiivillä käyttöön otetun järjestelmän soveltaminen on rajoitettava terrorismirikoksiin ja ainoastaan sellaisiin vakavan rikollisuuden muotoihin, joilla on vähintään välillinen objektiivinen yhteys matkustajalentoliikenteeseen. Tällaisten vakavan rikollisuuden muotojen osalta järjestelmän soveltamista ei saada ulottaa sellaisiin rikoksiin, jotka täyttävät kyseisessä direktiivissä säädetyn vakavuuskynnystä koskevan kriteerin ja joita direktiivin liitteessä II muun muassa tarkoitetaan mutta jotka kuitenkin kansallisen rikosoikeusjärjestelmän erityispiirteet huomioon ottaen kuuluvat tavanomaisen rikollisuuden alaan.
- Mahdollinen PNR-direktiivin soveltamisen ulottaminen kaikkiin tai joihinkin EU:n sisäisiin lentoihin, mistä jäsenvaltio voi päättää käyttämällä kyseisessä direktiivissä säädettyä mahdollisuutta, on rajattava siihen, mikä on ehdottoman välttämätöntä. Tätä varten tuomioistuimen tai riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, on voitava kohdistaa tällaiseen soveltamiseen tehokasta valvontaa. Tältä osin unionin tuomioistuin täsmentää seuraavaa:
 - Vain siinä tapauksessa, että mainittu jäsenvaltio toteaa, että on olemassa riittävän konkreettisia seikkoja, joiden perusteella voidaan katsoa, että jäsenvaltioon kohdistuu todellinen ja välitön tai ennakoitavissa oleva terroriuhka, kyseisen direktiivin soveltaminen kaikkiin EU:n sisäisiin lentoihin, jotka lähtevät kyseisestä jäsenvaltiosta tai saapuvat sinne, täysin välttämättömäksi rajoitettuna ajanjaksona, jota voidaan kuitenkin jatkaa, ei ylitä ehdottomasti välttämättömän rajoja.¹⁸
 - Silloin, kun tällaista terroriuhkaa ei ole, mainitun direktiivin soveltamista ei saa ulottaa kaikkiin EU:n sisäisiin lentoihin vaan soveltaminen on rajoitettava tiettyihin EU:n sisäisiin lentoihin, jotka liittyvät muun muassa tiettyihin lentoyhteyksiin tai matkustusjärjestelyihin tai tiettyihin lentoasemiin, joiden osalta on asianomaisen jäsenvaltion arvion mukaan olemassa viitteitä, jotka

¹⁷ Muun muassa "Kaikki maksutapaa koskevat tiedot" (liitteessä oleva nimike 6) voivat koskea ainoastaan lentolipun maksutapaa ja laskutusta koskevia tietoja eikä mitään muita tietoja, jotka eivät suoraan liity lentoon, ja "Yleiset huomautukset" (nimike 12) voivat koskea ainoastaan kyseisessä nimikkeessä nimenomaisesti lueteltuja tietoja, jotka liittyvät alaikäisiin lentomatikustajiin.

¹⁸ Tällaisen uhan olemassaolo on sellaisenaan omiaan osoittamaan tämän yhteyden olemassaolon asianomaisten tietojen siirtämisen ja käsittelyn ja terrorismin torjunnan välillä. Näin ollen PNR-direktiivin soveltaminen kaikkiin EU:n sisäisiin lentoihin, jotka lähtevät kyseisestä jäsenvaltiosta tai saapuvat sinne, rajoitettuna ajanjaksona ei ylitä ehdottomasti välttämättömän rajoja, ja tuomioistuimen tai riippumattoman hallinnollisen elimen on voitava valvoa päätöstä, jolla tällaisesta soveltamisesta määrätään.

voivat oikeuttaa tämän soveltamisen. Kysymystä siitä, onko järjestelmän soveltaminen näin valittuihin EU:n sisäisiin lentoihin täysin välttämätöntä, on tarkasteltava säännöllisin väliajoin uudelleen niiden valitsemisen perusteina olleiden seikkojen kehittymisen mukaan.

- PNR tietojen etukäteisarviointia varten, jonka tarkoituksena on tunnistaa henkilöt, joista on tehtävä lisätutkimuksia ennen heidän saapumistaan tai lähtöään, ja joka tehdään ensi vaiheessa tietojen automaattisella käsittelyllä, matkustajatietoyksikkö saa vertailla näitä tietoja vain tietokantoihin, jotka koskevat etsittyjä tai kuulutuksen kohteena olevia henkilöitä tai esineitä.¹⁹ Kyseisten tietokantojen on oltava syrjimättömiä, ja toimivaltaisten viranomaisien on käytettävä niitä terrorismirikosten ja sellaisen vakavan rikollisuuden, jolla on ainakin välillinen objektiivinen yhteys matkustajalentoliikenteeseen, torjuntaa koskevassa tehtävässään. Siltä osin kuin kyse on toisaalta etukäteisarvioinnista ennalta määritetyin perustein, matkustajatietoyksikkö ei saa käyttää tekoälyteknologiaa koneoppimiseen (machine learning) perustuvissa järjestelmissä, jotka voivat ilman ihmisen puuttumista ja valvontaa muuttaa arviointiprosessia ja erityisesti arviointikriteereitä, joihin kyseisen prosessin soveltamisen tulos perustuu, sekä näiden kriteerien painotusta. Mainitut perusteet on määritettävä siten, että ne kohdistuvat selvästi henkilöihin, joiden voidaan perustellusti epäillä olevan osallisina terrorismirikoksissa tai vakavassa rikollisuudessa, ja siten, että otetaan huomioon sekä asianomaista henkilöä "vastaan" että hänen "puolestaan" puhuvat seikat, ja samalla siten, ettei tämä johda välittömään eikä välilliseen syrjintään.²⁰
- Kun otetaan huomioon PNR-tietojen automaattisiin käsittelyihin liittyvä virheprosentti ja erityisesti niitä vuosina 2018 ja 2019 sovellettaessa saatujen "väärin positiivisten" tulosten varsin huomattava määrä, PNR-direktiivillä perustetun järjestelmän soveltuvuus riippuu olennaisesti siitä, että näiden käsittelyjen perusteella saatujen positiivisten tulosten tarkistaminen matkustajatietoyksikön toimesta toisessa vaiheessa muilla kuin automaattisilla keinoilla toimii asianmukaisesti. Tältä osin jäsenvaltioiden on säädettävä selkeistä ja täsmällisistä säännöistä, joilla voidaan ohjata ja säännellä yksittäin suoritettavasta tarkistuksesta vastaavan matkustajatietoyksikön toimihenkilöiden tekemää analyysiä,

¹⁹ Eli PNR-direktiivin 6 artiklan 3 kohdan a alakohdassa tarkoitettuihin etsittyjä tai kuulutuksen kohteena olevia henkilöitä tai esineitä koskeviin tietokantoihin. Sen sijaan analyysit eri tietokannoista saattavat tapahtua tiedonlouhinnan (data mining) muodossa ja saattaisivat johtaa kyseisten tietojen suhteettomaan käyttämiseen, mikä antaisi keinot kyseessä olevien henkilöiden täsmälliseen profilointiin pelkästään siksi, että he aikovat matkustaa lentokoneella.

²⁰ Ennalta määritettyjen kriteerien on oltava kohdennettuja, oikeasuhteisia ja selkeitä, ja niitä on tarkasteltava uudelleen säännöllisesti (PNR-direktiivin 6 artiklan 4 kohta). Ennalta määritettyjen kriteerien mukaisesti tapahtuva etukäteisvalvonta on toteutettava syrjimättömästi. PNR-direktiivin 6 artiklan 4 kohdan neljännen virkkeen mukaan kriteerit eivät missään olosuhteissa saa perustua henkilön rotuun tai etniseen alkuperään, poliittisiin mielipiteisiin, uskonnolliseen tai filosofiseen vakaumukseen, ammattiliiton jäsenyyteen eivätkä terveydentilaa, sukupuolielämää tai sukupuolista suuntautuneisuutta koskeviin tietoihin.

jotta voidaan varmistaa, että perusoikeuskirjan 7, 8 ja 21 artiklassa vahvistettuja perusoikeuksia kunnioitetaan täysimääräisesti, ja erityisesti taata matkustajatietoyksikön hallintokäytännön johdonmukaisuus syrjintäkiellon periaatetta noudattaen. Jäsenvaltioiden on muun muassa varmistettava, että matkustajatietoyksikkö vahvistaa objektiiviset tarkistuskriteerit, joiden avulla sen toimihenkilöt voivat tarkistaa yhtäältä sen, koskeeko – ja jos koskee niin missä määrin – osuma (hit) tosiasiallisesti henkilöä, joka voi olla osallisena terrorismirikoksissa tai vakavassa rikollisuudessa, sekä toisaalta sen, että automaattiset käsittelyt ovat syrjimättömiä. Tässä yhteydessä unionin tuomioistuimien korostaa vielä, että toimivaltaisten viranomaisten on varmistettava, että asianomainen henkilö voi ymmärtää ennalta määritetyt kriteerit ja niiden soveltamiseen käytettyjen ohjelmien toimintatavan siinä määrin, että hän voi päättää kaikista asiaan vaikuttavista seikoista tietoisena, käyttääkö hän oikeuttaan oikeudellisiin muutoksenhakukeinoihin. Vastaavasti tällaisen oikeussuojakeinon yhteydessä tuomioistuimen, jonka tehtävänä on toimivaltaisten viranomaisten tekemän päätöksen laillisuuden tutkiminen, sekä, jollei tästä aiheudu uhkaa valtion turvallisuudelle, myös asianomaisen itsensä on voitava saada tieto sekä kaikista perusteista että kaikista selvitysaineistosta, joiden perusteella kyseinen päätös on tehty, mukaan lukien etukäteen määritetyt kriteerit ja niiden soveltamiseen käytettyjen ohjelmien toimintatapa.

- PNR-tietojen luovuttaminen ja arviointi myöhemmin eli asianomaisen henkilön saapumisen tai lähdön jälkeen on sallittua vain sellaisten uusien olosuhteiden ja objektiivisten seikkojen perusteella, jotka joko antavat perustellun aiheen epäillä asianomaisen henkilön olevan osallisena terrorismirikoksissa tai vakavassa rikollisuudessa, jolla on ainakin välillinen objektiivinen yhteys matkustajalentoliikenteeseen, taikka joiden perusteella voidaan katsoa, että PNR-tiedot voivat konkreettisesti tapauksessa tosiasiallisesti myötävaikuttaa sellaisen terrorismirikollisuuden torjumiseen, jolla on tällainen yhteys. Lähtökohtaisesti PNR-tietojen luovuttaminen myöhempää arviointia varten edellyttää asianmukaisesti perusteltuja kiireellisiä tapauksia lukuun ottamatta joko tuomioistuimen tai riippumattoman hallintoelimen etukäteisvalvontaa ja sitä, että kyseisen tuomioistuimen tai elimen ratkaisu annetaan perustellusta pyynnöstä siitä riippumatta, onko pyyntö esitetty ennen tietojen siirtämisestä alkavan kuuden kuukauden määräajan päättymistä vai sen jälkeen²¹.

²¹ PNR-direktiivin 12 artiklan 1 ja 3 kohdan mukaan tällainen valvonta koskee nimenomaisesti ainoastaan PNR-tietojen luovutuspyyntöjä, jotka on esitetty sen kuuden kuukauden määräajan jälkeen, joka alkaa kyseisten tietojen siirrosta matkustajatietoyksikölle.

Tuomio 22.11.2022 (suuri jaosto), Luxembourg Business Registers (C-37/20 ja C-601/20, [EU:C:2022:912](#))

Rahanpesudirektiivin²² mukaan jäsenvaltioiden on rahanpesun ja terrorismin rahoituksen torjumiseksi ja estämiseksi pidettävä rekisteriä, joka sisältää tietoja niiden alueelle perustettujen yhtiöiden ja muiden oikeushenkilöiden tosiasiallisista omistajista ja edunsaajista.²³ Sen jälkeen, kun tätä direktiiviä muutettiin direktiivillä 2018/843²⁴, eräät näistä tiedoista on kaikissa tapauksissa saatettava suuren yleisön saataville. Näin muutetun rahanpesudirektiivin (jäljempänä muutettu rahanpesudirektiivi) nojalla Luxemburgin lainsäädännössä otettiin käyttöön tosiasiallisten omistajien ja edunsaajien rekisteri (jäljempänä RBE), jossa on tarkoitus säilyttää ja asettaa saataville useita rekisteröityjen yhteisöjen tosiasiallisia omistajia ja edunsaajia koskevia tietoja, joihin kuka tahansa voi tutustua.

Tässä asiayhteydessä tribunal d'arrondissement de Luxembourgissa (Luxemburgin piirituomioistuin, Luxemburg) kanteen nostivat kahdessa eri asiassa WM ja Sovim SA, jotka riitauttavat sen, että RBE:n rekisterinpitäjä Luxembourg Business Registers hylkäsi niiden pyynnön siitä, että suuren yleisön ei annettaisi päästä tutustumaan tietoihin, jotka ensimmäisessä asiassa koskevat WM:ää kiinteistöalan siviilyhtiön tosiasiallisena omistajana ja edunsaajana ja toisessa asiassa koskevat Sovim SA:n tosiasiallista omistajaa ja edunsaajaa. Koska tribunal d'arrondissement de Luxembourgilla oli kyseisessä kahdessa asiassa epäilyjä unionin oikeuden niiden säännösten pätevyydestä, joilla luodaan järjestelmä, jossa suurella yleisöllä on pääsy tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin, se esitti unionin tuomioistuimelle ennakkoratkaisukysymyksen pätevyyden arvioimiseksi.

Tuomiossaan, joka on annettu suuressa jaostossa, unionin tuomioistuin totesi direktiivin 2018/843 pätemättömäksi siltä osin kuin sillä on muutettu rahanpesudirektiiviä siten, että jäsenvaltioiden on varmistettava, että niiden alueelle perustettujen yhtiöiden ja muiden oikeushenkilöiden tosiasiallisia omistajia ja edunsaajia koskevat tiedot ovat kaikissa tapauksissa suuren yleisön saatavilla.²⁵

Ensimmäiseksi unionin tuomioistuin totesi, että muutetussa rahanpesudirektiivissä säädetty suuren yleisön pääsy tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin merkitsee vakavaa puuttumista Euroopan unionin perusoikeuskirjan (jäljempänä

²² Rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2005/60/EY ja komission direktiivin 2006/70/EY kumoamisesta 20.5.2015 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/849 (EUVL 2015, L 141, s. 73, jäljempänä rahanpesudirektiivi).

²³ Rahanpesudirektiivin 3 artiklan 6 kohdan mukaan tosiasiallisella omistajalla ja edunsaajalla tarkoitetaan luonnollista henkilöä, joka viime kädessä omistaa asiakkaan tai käyttää siinä määräysvaltaa, ja/tai luonnollista henkilöä, jonka lukuun liiketoimi suoritetaan tai toimintaa harjoitetaan.

²⁴ Rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun direktiivin (EU) 2015/849 ja direktiivien 2009/138/EY ja 2013/36/EU muuttamisesta 30.5.2018 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843 (EUVL 2018, L 156, s. 43).

²⁵ Direktiivin 2018/843 1 artiklan 15 kohdan c alakohdan, jolla muutetaan rahanpesudirektiivin 30 artiklan 5 kohdan ensimmäisen alakohdan c alakohtaa, pätemättömyys.

perusoikeuskirja) 7 artiklassa vahvistettua yksityiselämän kunnioitusta ja perusoikeuskirjan 8 artiklassa vahvistettua henkilötietojen suojaa koskeviin perusoikeuksiin.

Unionin tuomioistuimien huomautti tältä osin, että koska asianomaiset tiedot sisältävät tietoja tunnistetuista luonnollisista henkilöistä eli jäsenvaltioiden alueelle perustettujen yhtiöiden ja muiden oikeushenkilöiden tosiasiallisista omistajista ja edunsaajista, suuren yleisön pääsy niihin vaikuttaa yksityiselämän kunnioitusta koskevaan perusoikeuteen. Mainittujen tietojen suuren yleisön saataville saattamisessa on lisäksi kyse henkilötietojen käsittelystä. Se totesi vielä, että tällainen suuren yleisön saataville saattaminen merkitsee puuttumista kahteen edellä mainittuun perusoikeuteen välitettyjen tietojen myöhemmästä käytöstä riippumatta.

Unionin tuomioistuimien totesi tämän puuttumisen vakavuudesta, että siltä osin kuin suuren yleisön saataville saatetut tiedot liittyvät tosiasiallisen omistajan ja edunsaajan henkilöllisyyteen sekä hänellä yhtiöissä tai muissa oikeushenkilöissä olevien tosiasiallisten intressien luonteeseen ja laajuuteen, niiden avulla voidaan laatia profiili tietyistä tunnistamisen mahdollistavista henkilötiedoista, asianomaisen henkilön varallisuustilanteesta sekä niistä talouden aloista, maista ja nimenomaisista yrityksistä, joihin tosiasiallinen omistaja ja edunsaaja on investoinut. Nämä tiedot ovat lisäksi mahdollisesti rajoittamattoman henkilömäärän käytettävissä, joten tällainen henkilötietojen käsittely on omiaan mahdollistamaan sen, että myös henkilöt, jotka pyrkivät kyseisellä toimenpiteellä olevasta tavoitteesta poikkeavista syistä saamaan tietoja tosiasiallisen omistajan ja edunsaajan etenkin aineellisesta tilanteesta ja finanssitilanteesta, saavat nämä tiedot vapaasti käyttöön. Tämä mahdollisuus on sitäkin helpompi, kun kyseessä oleviin tietoihin voidaan tutustua internetissä. Niitä seurauksia, joita rekisteröidyille voi aiheutua heidän tietojensa mahdollisesta väärinkäytöstä, pahentaa lisäksi se, että kun nämä tiedot on kerran saatettu suuren yleisön saataville, niihin voidaan tutustua vapaasti ja niitä voidaan myös säilyttää ja levittää ja että näiden henkilöiden on vieläkin vaikeampaa tai jopa hyödytöntä puolustautua tehokkaasti väärinkäytöksiä vastaan.

Toiseksi unionin tuomioistuimien huomautti kyseessä olevan puuttumisen oikeuttamisen tutkinnan yhteydessä ensinnäkin, että käsiteltävässä asiassa on noudatettu laillisuusperiaatetta. Edellä mainittujen perusoikeuksien käytön rajoituksesta, joka aiheutuu siitä, että suurella yleisöllä on pääsy tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin, säädetään näet lainsäätäjäräjestyksessä hyväksytyssä unionin toimessa eli muutetussa rahanpesudirektiivissä. Kyseisessä direktiivissä yhtäältä täsmennetään, että näiden tietojen on oltava riittävät, tarkat ja ajantasaiset, ja luetellaan nimenomaisesti tiettä näistä tiedoista, joihin suurelle yleisölle on sallittava pääsy. Siinä toisaalta vahvistetaan edellytykset, joilla jäsenvaltiot voivat säätää poikkeuksista tällaiseen pääsyyn.

Unionin tuomioistuimien täsmensi toiseksi, että kyseessä olevalla puuttumisella ei loukata perusoikeuskirjan 7 ja 8 artiklassa taattujen perusoikeuksien keskeistä sisältöä. Vaikka

on totta, että muutetussa rahanpesudirektiivissä ei ole tyhjentävää luetteloa tiedoista, joihin suurelle yleisölle on sallittava pääsy, ja että jäsenvaltiot voivat säätää pääsystä lisätietoihin, kuitenkin vain riittävät tiedot tosiasiallisista omistajista ja edunsaajista sekä heillä olevista tosiasiallisista intresseistä voidaan hankkia, pitää hallussa ja siis mahdollisesti saattaa yleisön saataville, millä suljetaan pois muun muassa tiedot, joilla ei ole riittävää yhteyttä muutetun rahanpesudirektiivin tavoitteisiin. Ei kuitenkaan ole ilmeistä, että sellaisten tietojen saattaminen suuren yleisön saataville, joilla on tällainen yhteys, loukkaisi jollain tavalla kyseessä olevien perusoikeuksien keskeistä sisältöä.

Unionin tuomioistuimien korosti kolmanneksi, että säätäessään suuren yleisön pääsystä tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin unionin lainsäätäjät pyrkii torjumaan rahanpesua ja terrorismin rahoittamista luomalla laajemman avoimuuden avulla ympäristön, jota epätodennäköisemmin käytetään näihin tarkoituksiin, mikä on yleisen edun mukainen tavoite, joka voi oikeuttaa jopa vakavat puuttumiset perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin.

Unionin tuomioistuimien totesi neljänneksi kyseessä olevan puuttumisen soveltuvuuden, tarpeellisuuden ja oikeasuhteisuuden tutkinnan yhteydessä, että pitää tosin paikkansa, että suuren yleisön pääsillä tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin voidaan edistää kyseisen tavoitteen saavuttamista.

Se oli kuitenkin sitä mieltä, että tämän puuttumisen ei voida katsoa rajoittuvan täysin välttämättömään. Yhtäältä sitä, että mainittu puuttuminen on täysin välttämätöntä, ei voida osoittaa tukeutumalla siihen, että oikeutetun edun – joka rahanpesudirektiivin, sellaisena kuin se oli ennen kuin sitä muutettiin direktiivillä 2018/843, mukaan oli oltava kaikilla henkilöillä, jotka halusivat päästä tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin – kriteeriä oli vaikea panna täytäntöön ja sen soveltaminen saattoi johtaa mielivaltaisiin ratkaisuihin. Se, että on mahdollisesti vaikea määrittää tarkasti niitä tilanteita ja edellytyksiä, joiden toteutuessa yleisöllä voi olla oikeus saada tietoja todellisista omistajista ja edunsaajista, ei näet voi oikeuttaa sitä, että unionin lainsäätäjät säätää suuren yleisön pääsystä näihin tietoihin.

Toisaalta myöskään direktiivissä 2018/843 esitetyt selitykset eivät voi osoittaa, että kyseessä oleva puuttuminen on täysin välttämätöntä.²⁶

Siltä osin kuin näiden selitysten mukaan sen ansiosta, että suurella yleisöllä on pääsy tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin, kansalaisyhteiskunnalla ja erityisesti lehdistöllä tai kansalaisjärjestöillä on luultavasti paremmat mahdollisuudet tutkia tietoja unionin tuomioistuimien huomauttaa, että sekä lehdistöllä että kansalaisjärjestöillä, jotka ovat yhteydessä rahanpesun ja terrorismin rahoituksen estämiseen ja torjumiseen, on oikeutettu etu päästä asianomaisiin tietoihin. Sama koskee henkilöitä, jotka haluavat tietää, ketkä ovat jonkun yhtiön tai muun oikeushenkilön tosiasiallisia omistajia tai edunsaajia, koska he mahdollisesti suorittavat

²⁶ Kyse on direktiivin 2018/843 30 perustelukappaleessa esitetystä selityksestä.

liiketoimia heidän kanssaan, tai rahanpesua tai terrorismin rahoitusta koskevien rikosten torjuntaan osallistuvia finanssilaitoksia ja viranomaisia.

Kyseessä oleva puuttuminen ei myöskään ole oikeasuhteinen. Unionin tuomioistuin totesi tältä osin, että aineelliset säännöt, joilla rajoitetaan tätä puuttumista, eivät täytä selkeyden ja täsmällisyyden vaatimusta. Muutetussa rahanpesudirektiivissä näet säädetään, että suurella yleisöllä on pääsy ”vähintään” siinä tarkoitettuihin tietoihin, ja sen mukaan jäsenvaltiot voivat säätää pääsystä lisätietoihin, joihin on sisällyttävä ”vähintään” tiedot kyseessä olevan tosiasiallisen omistajan ja edunsaajan syntymäajasta tai hänen yhteystietonsa. Kun kyseisessä direktiivissä käytetään ilmaisua ”vähintään”, siinä sallitaan kuitenkin sellaisten tietojen saattaminen yleisön saataville, joita ei ole riittävästi määritelty ja jotka eivät ole yksilöitävissä.

Siltä osin kuin on kyse tämän puuttumisen vakavuuden punnitsemisesta suhteessa kyseessä olevan yleisen edun mukaisen tavoitteen tärkeyteen, unionin tuomioistuin katsoi, että tällä tavoitteella voidaan, kun otetaan huomioon sen tärkeys, oikeuttaa vakavatkin puuttumiset perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin.

Yhtäältä rahanpesun ja terrorismin rahoittamisen torjuminen kuuluu kuitenkin ensisijaisesti viranomaisille ja luottolaitosten tai finanssilaitosten kaltaisille tahoille, joille on niiden toiminnan vuoksi asetettu tätä koskevia erityisiä velvollisuuksia. Tästä syystä muutetussa rahanpesudirektiivissä säädetään, että tosiasiallisia omistajia ja edunsaajia koskevien tietojen on kaikissa tapauksissa oltava toimivaltaisten viranomaisten ja rahanpesun selvittelykeskusten saatavilla rajoituksitta ja ilmoitusvelvollisten saatavilla asiakkaan tuntemisvelvollisuutta koskevissa puitteissa.²⁷

Toisaalta verrattuna aikaisempaan järjestelmään, jossa säädettiin paitsi toimivaltaisten viranomaisten ja tiettyjen tahojen myös sellaisten henkilöiden tai järjestöjen pääsystä tosiasiallisia omistajia ja edunsaajia koskeviin tietoihin, jotka pystyvät osoittamaan tietojen koskevan niiden oikeutettua etua, direktiivillä 2018/843 käyttöön otettu järjestelmä merkitsee huomattavasti vakavampaa perusoikeuskirjan 7 ja 8 artiklassa taattujen perusoikeuksien loukkausta, eikä tätä vakavampaa loukkausta ole kompensoitu viimeksi mainitusta järjestelmästä ensimmäiseksi mainittuun verrattuna mahdollisesti saatavilla eduilla rahanpesun ja terrorismin rahoituksen torjunnan osalta.

²⁷ Muutetun rahanpesudirektiivin 30 artiklan 5 kohdan ensimmäisen alakohdan a ja b alakohta.

2. Henkilötietojen suojaa koskevan oikeuden noudattaminen unionin oikeuden täytäntöönpanossa

Tuomio 21.12.2016 (suuri jaosto), Tele2 Sverige (yhdistetyt asiat C-203/15 ja C-698/15, [EU:C:2016:970](#))

Sen jälkeen, kun tuomiolla Digital Rights Ireland ja Seitlinger ym. julistettiin pätemättömäksi direktiivi 2006/24 (ks. edellä), unionin tuomioistuimen ratkaistavaksi saatettiin kaksi asiaa, jotka koskivat Ruotsissa ja Isossa-Britanniassa sähköisten viestintäpalvelujen tarjoajille asetettua yleistä velvoitetta säilyttää tätä viestintää koskevat tiedot, joiden säilyttämisestä säädettiin pätemättömäksi julistetussa direktiivissä.

Tuomion Digital Rights Ireland ja Seitlinger ym. antamista seuraavana päivänä Tele2 Sverige -niminen teleyritys ilmoitti Ruotsin posti- ja telehallitukselle päätöksestään lakata säilyttämästä tietoja sekä aikomuksestaan hävittää jo tallennetut tiedot (asia C-203/15). Ruotsin oikeudessa nimittäin veloitettiin sähköisten viestintäpalvelujen tarjoajat säilyttämään systemaattisesti ja jatkuvasti ilman mitään poikkeuksia kaikkien tilaajien ja rekisteröityjen käyttäjien kaikki liikenne- ja paikkatiedot kaikkien sähköisten viestintävälineiden osalta. Asiassa C-698/15 kolme henkilöä nosti kanteen Ison-Britannian tietojen säilyttämistä koskevasta järjestelmästä, jossa sallittiin sisäministerin velvoittavan yleisen televerkon operaattorit säilyttämään kaikki viestintätiedot enintään 12 kuukauden ajan. Viestinnän sisältöä ei kuitenkaan saanut säilyttää.

Kammarrätten i Stockholm (Tukholman kamarioikeus, Ruotsi) ja Court of Appeal (England and Wales) (Civil Division) (Englannin ja Walesin ylioikeus (siviilioikeudellisten asioiden jaosto), Yhdistynyt kuningaskunta) pyysivät unionin tuomioistuinta tulkitsemaan direktiivin 2002/58 – ns. sähköisen viestinnän tietosuojadirektiivi – 15 artiklan 1 kohtaa, jossa sallitaan jäsenvaltioiden ottavan käyttöön eräitä poikkeuksia mainitussa direktiivissä säädettyyn veloitteeseen varmistaa sähköisen viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuus.

Unionin tuomioistuin totesi antamassaan tuomiossa ensinnäkin, että direktiivin 2002/58 15 artiklan 1 kohta, kun sitä luetaan perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on esteenä Ruotsin säännösten kaltaiselle kansalliselle säännöstölle, jossa rikollisuuden torjumiseksi säädetään kaikkien tilaajien ja rekisteröityjen käyttäjien liikenne- ja paikannustietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä kaikkien sähköisten viestintävälineiden osalta. Unionin tuomioistuimen mukaan tällaisella säännöstöllä ylitetään täysin välttämättömän rajat, eikä sitä voida pitää perusteltuna demokraattisessa yhteiskunnassa siten kuin edellytetään direktiivin 2002/58 15 artiklan 1 kohdassa, kun se luetaan perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa.

Samainen säännös, kun sitä luetaan perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, on myös esteenä kansalliselle säännöstölle, jossa säännellään liikenne- ja paikkatietojen suoja ja turvaa, erityisesti toimivaltaisten kansallisten viranomaisten oikeutta saada säilytettäviä tietoja, ja jossa ei rikollisuuden torjumisen puitteissa rajoiteta tätä tietojen saantia vain vakavan rikollisuuden torjumisen tarkoitukseen, eikä tietojen saannin edellytykseksi aseteta tuomioistuimen tai riippumattoman hallintoviranomaisen suorittamaa ennakkovalvontaa, eikä vaadita, että kyseessä olevat tiedot säilytetään unionin alueella.

Unionin tuomioistuin sen sijaan katsoi, että direktiivin 2002/58 15 artiklan 1 kohta ei ole esteenä säännöstölle, jossa sallitaan ennaltaehkäisevästi liikenne- ja paikkatietojen kohdennettu säilyttäminen vakavan rikollisuuden torjumiseksi sillä edellytyksellä, että näiden tietojen säilyttäminen on, siltä osin kuin kyse on säilytettävistä tietoluokista, tarkoitetuista viestintävälineistä, asianomaisista henkilöistä ja aiotun säilytyksen kestosta, rajoitettu täysin välttämättömään. Näiden vaatimusten täyttämiseksi kyseisessä kansallisessa säännöstössä on ensinnäkin oltava selvät ja täsmälliset säännöt, joiden avulla voidaan tehokkaasti suojata tietoja väärinkäytön vaaroja vastaan. Säännöstössä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksillä tietojen säilyttämistoimenpide voidaan toteuttaa ennaltaehkäisevästi, jotta taataan, että toimenpide rajoittuu täysin välttämättömään. Toiseksi siltä osin kuin kyse on aineellisista edellytyksistä, jotka kansallisen säännösten on täytettävä, jotta taataan, että se rajoittuu täysin välttämättömään, unionin tuomioistuin totesi, että tietojen säilyttämisen on aina oltava sellaisten objektiivisten perusteiden mukaista, joilla luodaan yhteys säilytettävien tietojen ja asetetun tavoitteen välille. Näiden edellytysten on erityisesti oltava käytännössä sellaisia, että niissä rajataan tehokkaasti toimenpiteen laajuus ja tätä kautta asianomainen yleisö. Siltä osin kuin kyse on tästä rajaamisesta, kansallisen säännösten on perustuttava objektiivisiin seikkoihin, joiden perusteella voidaan kohdentaa yleisö, jonka tiedot voivat paljastaa ainakin välillisen yhteyden vakavaan rikollisuuteen, myötävaikuttaa tavalla tai toisella vakavan rikollisuuden torjumiseen tai ehkäistä yleistä turvallisuutta koskeva uhka.

II. Alan yleisessä säännöstössä tarkoitettu henkilötietojen käsittely

1. Yleisen säännösten soveltamisala

Tuomio 30.5.2006 (suuri jaosto), parlamentti v. neuvosto (C-317/04 ja C-318/04, [EU:C:2006:346](#))

Heti 11.9.2001 tapahtuneiden terroristi-iskujen jälkeen Yhdysvalloissa hyväksyttiin lainsäädäntö, jonka mukaan lentoyhtiöiden, jotka harjoittavat lentoliikennettä

Yhdysvalloista tai Yhdysvaltoihin, on tarjottava Yhdysvaltojen viranomaisille sähköinen pääsy tietoihin, jotka sisältyvät niiden varaus- ja valvontajärjestelmiin ja joista käytetään nimitystä Passenger Name Records (jäljempänä PNR).

Komissio katsoi, että kyseiset säännökset saattoivat olla ristiriidassa henkilötietojen suojaa koskevan eurooppalaisen ja jäsenvaltioiden lainsäädännön kanssa, ja aloitti neuvottelut Yhdysvaltojen viranomaisten kanssa. Näiden neuvottelujen päätteeksi komissio teki 14.5.2004 päätöksen 2004/535/EY²⁸, jossa todettiin että Yhdysvaltojen tulli- ja rajavartiolaitos (United States Bureau of Customs and Border Protection, jäljempänä CBP) varmisti yhteisöstä toimitettavien PNR-tietojen suojan riittävän tason (jäljempänä vastaavuuspäätös). Neuvosto teki tämän jälkeen 17.5.2004 päätöksen 2004/496/EY,²⁹ jolla hyväksyttiin lentoyhtiöiden PNR-tietojen käsitlemistä ja siirtämistä CBP:lle koskevan yhteisön ja Yhdysvaltojen välisen sopimuksen tekeminen.

Euroopan parlamentti vaati unionin tuomioistuinta kumoamaan edellä mainitut kaksi päätöstä ja väitti muun muassa, että vastaavuuspäätös oli tehty ultra vires (ilman toimivaltaa) ja että EY 95 artikla (josta on tullut SEUT 114 artikla) ei ollut asianmukainen oikeudellinen perusta sopimuksen tekemisen sallivan päätöksen tekemiseksi ja että joka tapauksessa perusoikeuksia oli loukattu.

Vastaavuuspäätöksen osalta unionin tuomioistuin tutki ensimmäiseksi sen, oliko komissio voinut pätevästi tehdä päätöksensä direktiivin 95/46 perusteella. Se totesi tässä yhteydessä, että vastaavuuspäätöksestä ilmeni, että PNR-tietojen siirto CBP:lle on käsittelyä, joka koskee yleistä turvallisuutta ja rikosoikeuden alalla tapahtuvaa valtion toimintaa. Unionin tuomioistuin totesi, että vaikka lentoyhtiöt ovat alun perin keränneet PNR-tiedot unionin oikeuden alaan kuuluvan toiminnan eli palveluun oikeuttavien lentolippujen myynnin yhteydessä, tietojen käsittely, joka on otettu huomioon suojan riittävää tasoa koskevassa päätöksessä, on kuitenkin luonteeltaan aivan toisenlaista. Mainitussa päätöksessä ei ollut kyse tietojen käsittelystä, joka on tarpeen palvelujen tarjoamiseksi, vaan tietojen käsittelystä, jota pidetään tarpeellisena yleisen turvallisuuden suojelemiseksi ja lainvalvontatarkoituksia varten.

Unionin tuomioistuin totesi tästä, ettei se seikka, että yksityiset toimijat keräävät tiettyjä henkilötietoja kaupalliseen tarkoitukseen ja että ne järjestävät kyseisten tietojen siirron kolmanteen valtioon, estä kyseisen siirron pitämistä direktiivin soveltamisalan ulkopuolelle jäävänä tietojen käsittelynä. Tämä siirto nimittäin tapahtuu julkishallinnon asettamissa puitteissa, jotka liittyvät yleiseen turvallisuuteen. Näin ollen unionin tuomioistuin katsoi, että vastaavuuspäätös ei kuulunut direktiivin soveltamisalaan, koska se koski henkilötietojen käsittelyä, joka on suljettu soveltamisalan ulkopuolelle. Unionin tuomioistuin kumosi täten vastaavuuspäätöksen.

²⁸ Yhdysvaltojen tulli- ja rajavartiolaitokselle toimitettavien lentomatkustajia koskevaan matkustajarekisteriin sisältyvien henkilötietojen suojan riittävästä tasosta 14.5.2004 tehty komission päätös 2004/535/EY (EUVL 2004, L 235, s. 11).

²⁹ Lentoyhtiöiden PNR-tietojen käsitlemistä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriön alaiselle tulli- ja rajavartiolaitokselle koskevan Euroopan yhteisön ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä 17.5.2004 tehty neuvoston päätös 2004/496/EY (EUVL 2004, L 183, s. 83 ja oikaisu EUVL 2005, L 255, s. 168).

Neuvoston päätöksestä unionin tuomioistuin katsoi, että EY 95 artikla, luettuna yhdessä direktiivin 95/46 25 artiklan kanssa, ei voi olla perusteena yhteisön toimivallalle kyseessä olevan sopimuksen tekemiseksi Yhdysvaltojen kanssa. Sopimus koskee nimittäin samaa tietojen siirtoa kuin suojan riittävää tasoa koskeva päätös ja siis tietojen käsittelyä, joka on suljettu direktiivin soveltamisalan ulkopuolelle. Näin ollen unionin tuomioistuin kumosi neuvoston päätöksen, jolla sallittiin sopimuksen tekeminen.

Tuomio 13.5.2014 (suuri jaosto), Google Spain ja Google (C-131/12, [EU:C:2014:317](#))

Eräs Espanjan kansalainen teki vuonna 2010 Agencia Española de Protección de Datosille (Espanjan tietosuojaviranomainen, jäljempänä AEPD) kantelun laajalevikkistä sanomalehteä Espanjassa julkaisevasta La Vanguardia Ediciones SL:stä sekä Google Spainista ja Googlesta. Kyseinen henkilö väitti, että kun internetin käyttäjä syöttää hänen nimensä Google-konsernin hakukoneeseen, hän saa linkit La Vanguardian sanomalehden kahdelle vuodelta 1998 olevalle sivulle, joilla on ilmoitus, jossa mainitaan muun muassa saatavien perimiseksi suoritettuun takavarikkoon liittyvän kiinteän omaisuuden huutokauppa. Mainittu henkilö vaati kantelussaan yhtäältä, että La Vanguardia veloitetaan poistamaan mainitut sivut tai muuttamaan niitä taikka käyttämään tiettyjä hakukoneiden tarjoamia välineitä kyseisten tietojen suojaamiseksi. Hän vaati toisaalta, että Google Spain tai Google veloitetaan poistamaan tai kätkemään hänen henkilötietonsa, jotta ne eivät näkyisi enää hakutuloksissa eivätkä sisältyisi enää La Vanguardian linkkeihin.

AEPD hylkäsi La Vanguardiaa vastaan tehdyn kantelun, koska se katsoi, että se oli julkaissut kyseessä olevat tiedot laillisesti. Se kuitenkin hyväksyi kantelun Google Spainin ja Googlen osalta ja vaati, että mainitut kaksi yhtiötä toteuttavat tarvittavat toimenpiteet tietojen poistamiseksi rekisteristään ja pääsyn estämiseksi niihin tulevaisuudessa. Mainitut kaksi yhtiötä nostivat AEPD:n päätöksen kumoamiseksi kanteen Audiencia Nacionalissa (ylimmän oikeusasteen tuomioistuin, Espanja), joka puolestaan esitti unionin tuomioistuimelle joukon ennakkoratkaisukysymyksiä.

Kyseisessä tuomiossa unionin tuomioistuin lausui myös direktiivin 95/46 alueellisesta soveltamisalasta.

Unionin tuomioistuin totesi, että henkilötietojen käsittely suoritetaan jäsenvaltion alueella sijaitsevassa rekisterinpitäjän toimipaikassa tapahtuvan toiminnan yhteydessä direktiivissä 95/46 tarkoitetulla tavalla, kun hakukoneen ylläpitäjä, jolla on kotipaikka kolmannes valtiossa, perustaa jäsenvaltioon sivuliikkeen tai tytäryhtiön, jonka tehtävänä on markkinoida ja myydä hakukoneen tarjoamia mainospaikkoja ja jonka toiminta kohdistuu kyseisen jäsenvaltion asukkaisiin.

Tällaisessa tilanteessa näet hakukoneen ylläpitäjän toiminnot ja sen asianomaisen jäsenvaltion alueella sijaitsevan toimipaikan toiminnot liittyvät erottamattomasti toisiinsa, koska mainospaikkoja koskevat toiminnot ovat keino tehdä kyseisestä

hakukoneesta taloudellisesti kannattava ja koska kyseinen hakukone on samanaikaisesti väline, jolla nuo toiminnot voidaan suorittaa.

Tuomio 11.12.2014, Ryneš (C-212/13, [EU:C:2014:2428](#))

Toistuvien väkivallanteiden vuoksi Ryneš oli asentanut taloonsa valvontakameran. Hänen talonsa jouduttua jälleen hyökkäyksen kohteeksi mainitun kameran tallenteiden ansiosta voitiin tunnistaa kaksi epäiltyä, joita vastaan aloitettiin rikosoikeudelliset menettelyt. Kun yksi näistä epäillyistä oli riitauttanut valvontakameran tallentamien tietojen käsittelyn laillisuuden Tšekin tietosuojavirastossa, kyseinen virasto totesi, että Ryneš oli rikkonut henkilötietojen suojaa koskevia sääntöjä ja määräsi tälle sakon.

Nejvyšší správní soud (ylin hallintotuomioistuin, Tšekki), jonka käsiteltävänä oli Rynešin valitus Městský soud v Praze (Prahan käräjäoikeus, Tšekki) tuomiosta, jolla vahvistettiin tietosuojaviraston päätös, tiedusteli unionin tuomioistuimelta, oliko tallenne, jonka Ryneš oli tallentanut suojatakseen henkeään, terveyttään ja omaisuuttaan tietojenkäsittelyä, joka ei kuulu direktiivin 95/46 soveltamisalaan, koska kyseisen tallentamisen on tehnyt luonnollinen henkilö yksinomaan henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa mainitun direktiivin 3 artiklan 2 kohdan toisessa luetelmakohdassa tarkoitettu tavoin.

Unionin tuomioistuin totesi, että sellaisen kamerajärjestelmän käyttämisen, joka tekee henkilöistä kuvataallenteen, joka tallennetaan kovalevyn kaltaiselle jatkuvasti tallentavalle laitteelle, ja jonka luonnollinen henkilö on asentanut kotitaloonsa suojatakseen talon omistajien omaisuutta, terveyttä ja henkeä, kun tällä järjestelmällä valvotaan myös julkista tilaa, ei ole katsottava olevan tietojenkäsittelyä, joka suoritetaan yksinomaan henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa kyseisessä säännöksessä tarkoitettu tavoin.

Se muistutti tältä osin, että perusoikeuskirjan 7 artiklassa taattu yksityiselämän kunnioittamista koskevan perusoikeuden suoja edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset on toteutettava täysin välttämättömän rajoissa. Koska niitä direktiivin 95/46 säännöksiä, joilla säännellään henkilötietojen käsittelyä, joka saattaa loukata perusvapauksia ja varsinkin oikeutta yksityisyyteen, on välttämättä tulkittava perusoikeuksien valossa, jotka sisältyvät perusoikeuskirjaan, kyseisen direktiivin 3 artiklan 2 kohdan toisessa luetelmakohdassa säädettyä poikkeusta on tulkittava suppeasti. Jo mainitun säännöksen sanamuodossa suljetaan direktiivin 95/46 ulkopuolelle tietojenkäsittely, joka suoritetaan "yksinomaan" henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa. Siltä osin kuin videovalvonta ulottuu vaikka osittainkin julkiseen tilaan ja kohdistuu tämän vuoksi tietojä tällä tavoin käsittelevän tahon yksityisen piirin ulkopuolelle, sitä ei voida pitää yksinomaan "henkilökohtaisena tai kotitaloutta koskevana" toimintana mainitussa säännöksessä tarkoitettu tavoin.

Tuomio 16.1.2024 (suuri jaosto), Österreichische Datenschutzbehörde (C-33/22, [EU:C:2024:46](#))

Selvittääkseen, kohdistuuko Bundesamt für Verfassungsschutz und Terrorismusbekämpfungiin (liittovaltion perustuslainsuojelu- ja terrorismintorjuntavirasto, Itävalta)³⁰ mahdollisesti poliittista vaikuttamista, Nationalrat (kansallisneuvosto, Itävalta) perusti tutkintavaliokunnan (jäljempänä BVT-tutkintavaliokunta). Kyseinen tutkintavaliokunta kuuli WK:ta todistajana. Vaikka WK oli pyytänyt tunnistetietojen poistamista, hänen kuulemisestaan laadittu pöytäkirja, jossa mainittiin hänen suku- ja etunimensä täydellisinä, julkaistiin Parlament Österreichin (Itävallan parlamentti) internetsivustolla. WK väitti, että tällainen hänen henkilöllisyytensä paljastaminen on vastoin yleistä tietosuoja-asetusta ja Itävallan lainsäädäntöä, ja teki kantelun Österreichische Datenschutzbehörde (tietosuojaviranomainen, Itävalta) (jäljempänä Datenschutzbehörde). Datenschutzbehörde katsoi 18.9.2019 tehdyssä päätöksessä, ettei sillä ole toimivaltaa ratkaista kantelua, ja totesi, että vallanjakoperiaatteen mukaan ei ole mahdollista, että se voisi toimeenpanovallan elimenä valvoa BVT-tutkintavaliokuntaa, joka kuuluu lainsäädäntövaltaan.

Bundesverwaltungsgerichtin (liittovaltion hallintotuomioistuin, Itävalta) antaman ratkaisun, jolla WK:n kantelu hyväksyttiin ja Datenschutzbehörde päätös kumottiin, johdosta Datenschutzbehörde teki ylimmälle hallintotuomioistuimelle Revision-valituksen liittovaltion hallintotuomioistuimen ratkaisusta.

Ennakkoratkaisua pyytänyt tuomioistuin tiedusteli tässä yhteydessä unionin tuomioistuimelta, kuuluuko jäsenvaltion parlamentin perustaman tutkintavaliokunnan toiminta yleisen tietosuoja-asetuksen soveltamisalaan ja sovelletaanko kyseistä asetusta, kun tämä toiminta koskee kansallisen turvallisuuden suojaamista.

Ensimmäiseksi unionin tuomioistuin huomautti, että yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan a alakohdan, jonka mukaan kyseistä asetusta ei sovelleta henkilötietojen käsittelyyn, jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan, ainoana tarkoituksena on sulkea asetuksen soveltamisalan ulkopuolelle henkilötietojen käsittely, jota valtion viranomaiset suorittavat sellaisen toiminnan yhteydessä, jonka tarkoituksena on kansallisen turvallisuuden turvaaminen tai joka kuuluu samaan ryhmään. Pelkästään se seikka, että jokin toiminto on valtiolle tai viranomaiselle ominaista, ei siis ole riittävä, jotta tällainen toiminta voisi automaattisesti jäädä yleisen tietosuoja-asetuksen ulkopuolelle.

³⁰ Kyseisestä virastosta tuli 1.12.2021 Direktion Staatsschutz und Nachrichtendienst (valtion turvallisuudesta ja tiedustelupalvelusta vastaava osasto, Itävalta).

Tämä tulkinta, joka perustuu siihen, ettei eroa tehdä asianomaisen käsittelyn suorittajan henkilöllisyyden perusteella, saa vahvistuksen kyseisen asetuksen 4 artiklan 7 alakohdasta.³¹

Unionin tuomioistuin täsmensi, että BVT-tutkintavaliokunnan parlamentaarinen luonne ei merkitse sitä, että sen toiminta jää yleisen tietosuoja-asetuksen soveltamisalan ulkopuolelle. Kyseisen asetuksen 2 artiklan 2 kohdan a alakohdassa säädetty poikkeus liittyy yksinomaan sellaisen toiminnan ryhmiin, joka ei luonteensa vuoksi kuulu unionin oikeuden soveltamisalaan, eikä se liity henkilöiden ryhmiin. Näin ollen sen perusteella, että henkilötietoja käsittelee jäsenvaltion parlamentin toimeenpanoa koskevaa valvontavaltaansa käyttäessään perustama tutkintavaliokunta, ei sellaisenaan voida katsoa, että kyseinen käsittely suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan.

Toiseksi unionin tuomioistuin huomautti, että vaikka jäsenvaltioiden asiana on määritellä keskeiset turvallisuusasetukset ja toteuttaa turvallisuutensa varmistamiseen soveltuvat toimenpiteet,³² pelkästään se, että kansallinen toimenpide on toteutettu kansallisen turvallisuuden suojaamiseksi, ei voi johtaa siihen, ettei unionin oikeutta sovelleta, ja vapauttaa jäsenvaltioita velvollisuudesta noudattaa unionin oikeutta. Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan a alakohdassa säädetty poikkeus liittyy kuitenkin yksinomaan sellaisen toiminnan ryhmiin, joka ei luonteensa vuoksi kuulu unionin oikeuden soveltamisalaan. Tältä osin se, että rekisterinpitäjä on viranomainen, jonka pääasiallisena toimintana on varmistaa kansallinen turvallisuus, ei sellaisenaan voi riittää siihen, että kyseisen viranomaisen muun toimintansa yhteydessä suorittama henkilötietojen käsittely jätetään yleisen tietosuoja-asetuksen soveltamisalan ulkopuolelle.

Käsiteltävässä asiassa BVT-tutkintavaliokunnan suorittama poliittinen valvonta ei näytä sellaisenaan olevan toimintaa, jonka tarkoituksena on kansallisen turvallisuuden turvaaminen tai joka kuuluu samaan ryhmään. Jollei ennakkoratkaisua pyytäneen tuomioistuimen selvityksestä muuta johdu, tämä toiminta ei siis jää yleisen tietosuoja-asetuksen soveltamisalan ulkopuolelle.

Parlamentarisella tutkintavaliokunnalla voi kuitenkin olla pääsy henkilötietoihin, joille on kansalliseen turvallisuuteen liittyvistä syistä annettava erityistä suojaa. Lainsäädäntötoimenpiteillä voidaan tältä osin rajoittaa yleisestä tietosuoja-asetuksesta ilmeneviä velvollisuuksia ja oikeuksia etenkin kansallinen turvallisuuden varmistamiseksi.³³ Tällä perusteella oikeutettuja voisivat siten olla rajoitukset, joissa on kyse henkilötietojen keräämisestä, tietojen ilmoittamisesta rekisteröidyille ja rekisteröityjen pääsystä näihin tietoihin tai näiden tietojen luovuttamisesta ilman

³¹ Sen mukaan "rekisterinpitäjällä" tarkoitetaan "luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot".

³² SEU 4 artiklan 2 kohdan mukaan.

³³ Yleisen tietosuoja-asetuksen 23 artiklan mukaan.

rekisteröityjen suostumusta muille henkilöille kuin rekisterinpitäjälle, sillä edellytyksellä, että niissä noudatetaan keskeisiltä osin rekisteröityjen perusoikeuksia ja -vapauksia ja ne ovat demokraattisessa yhteiskunnassa välttämättömiä ja oikeasuhteisia toimenpiteitä.

Unionin tuomioistuin huomautti kuitenkin, ettei sen käytössä olevista tiedoista ilmene, että BVT-tutkintavaliokunta olisi väittänyt, että rekisteröidyn henkilötietojen luovuttaminen olisi ollut tarpeen kansallisen turvallisuuden suojaamiseksi ja perustuisi tätä varten säädettyyn kansalliseen lainsäädäntötoimenpiteeseen, mikä ennakkoratkaisua pyytänyt tuomioistuimen on mahdollisesti kuitenkin selvitettävä.

2. Käsite "henkilötiedot"

Tuomio 19.10.2016, Breyer (C-582/14, [EU:C:2016:779](#))

Breyer oli nostanut saksalaisessa siviilituomioistuimessa kanteen, jossa vaadittiin, että Saksan liittotasavalta veloitetaan olemaan tallentamatta tai antamatta sivullisen tallennettavaksi tietokonetietoja, jotka välittyivät Saksan liittovaltion laitosten internetsivujen käytön yhteydessä. Verkkohyökkäyksiltä suojautumista ja hyökkääjien rikosoikeudelliseen vastuuseen saattamista varten Saksan liittovaltion verkkomediapalvelujen tarjoajat tallensivat tiedot, jotka koostuivat dynaamisesta IP-osoitteesta – joka on IP-osoite, joka vaihtuu jokaisen uuden internetyhteyden ottamisen myötä – ja internetsivustolla käynnin päivämäärästä ja kellonajasta. Toisin kuin staattiset IP-osoitteet, dynaamiset IP-osoitteet eivät mahdollista yleisesti saatavilla olevien tiedostojen avulla yhteyden toteuttamista tietyn tietokoneen ja internetpalvelun tarjoajan käyttämän fyysisen verkkoliittymän välillä. Tallennetut tiedot eivät yksinään antaneet verkkomediapalvelujen tarjoajalle mahdollisuutta tunnistaa käyttäjää. Internetyhteyden tarjoajalla puolestaan oli käytettävissä lisätietoja, joiden perusteella on mahdollista tunnistaa tämä käyttäjä, kun niihin yhdistetään kyseinen IP-osoite.

Tässä tilanteessa Bundesgerichtshof (liittovaltion ylin tuomioistuin, Saksa), jonka käsiteltävänä oli Revision-valitus, tiedusteli unionin tuomioistuimelta, onko IP-osoite, jonka verkkomediapalvelujen tarjoaja tallentaa, kun sen internetsivulla käydään, palveluntarjoajan kannalta henkilötieto.

Unionin tuomioistuin totesi ensimmäiseksi, että jotta tietoa voitaisiin pitää direktiivin 95/46/EY 2 artiklan a alakohdassa tarkoitettuna henkilötietona, ei edellytetä, että kaikki tiedot, joiden perusteella rekisteröity voidaan tunnistaa, ovat yhden ainoan tahon hallussa. Se, että internetsivuston käyttäjän tunnistamiseksi tarvittavat lisätiedot eivät ole verkkomediapalvelujen tarjoajan vaan kyseisen käyttäjän internetyhteyden tarjoajan hallussa, ei siis näytä sulkevan pois sitä, että verkkomediapalvelujen tarjoajan tallentamat dynaamiset IP-osoitteet ovat sen kannalta direktiivin 95/46 2 artiklan a alakohdassa tarkoitettuja henkilötietoja.

Näin ollen unionin tuomioistuin katsoi, että dynaaminen IP-osoite, jonka verkkomediapalvelujen tarjoaja tallentaa henkilön käydessä tämän palveluntarjoajan yleisön saataville asettamalla internetsivustolla, on tähän palveluntarjoajaan nähden direktiivin 95/46/EY 2 artiklan a alakohdassa tarkoitettu henkilötieto, jos palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa kyseisen henkilön sellaisten lisätietojen avulla, jotka ovat tämän henkilön internetyhteyden tarjoajan käytettävissä.

Tuomio 20.12.2017, Nowak (C-434/16, [EU:C:2017:994](#))

Nowak, joka oli kirjanpitäjäharjoittelija, oli osallistunut Irlannin tilintarkastajien järjestön järjestämään kokeeseen ja epäonnistunut siinä. Hän esitti tietosuojalain 4 artiklan mukaisen pyynnön saada tutustua kaikkiin henkilötietoihinsa, jotka olivat tilintarkastajien järjestön hallussa. Tilintarkastajien järjestö toimitti Nowakille eräitä asiakirjoja mutta kieltäytyi luovuttamasta hänelle hänen koepaperiaan sillä perusteella, että siihen ei sisältynyt tietosuojalaissa tarkoitettuja henkilötietoja.

Koska tietosuojavaltuutettu ei samoista syistä myöskään hyväksynyt Nowakin pyyntöä, hän saattoi asian kansallisen tuomioistuimen käsiteltäväksi. Supreme Court (ylin tuomioistuin, Irlanti), jonka käsiteltävänä oli Nowakin tekemä valitus, tiedusteli unionin tuomioistuimelta, onko direktiivin 95/46/EY 2 artiklan a alakohtaa tulkittava siten, että pääasiassa kyseessä olevien kaltaisissa olosuhteissa ammatilliseen kokeeseen osallistujan laatimat kirjalliset vastaukset ja mahdolliset tarkastajan niihin tekemät merkinnät ovat kyseisessä säännöksessä tarkoitettuja henkilötietoja.

Unionin tuomioistuin totesi ensimmäiseksi, että jotta tietoa voitaisiin pitää direktiivin 95/46/EY 2 artiklan a alakohdassa tarkoitettuna henkilötietona, ei edellytetä, että kaikki tiedot, joiden perusteella rekisteröity voidaan tunnistaa, ovat yhden ainoan tahon hallussa. On lisäksi riidatonta, että tilanteessa, jossa kokeeseen osallistujan henkilöllisyys ei ole tarkastajan tiedossa hänen arvostellessaan tämän kokeessa laatimia vastauksia, kokeen järjestävällä taholla – tässä tapauksessa tilintarkastajien instituutilla – sen sijaan on käytössään tarpeelliset tiedot, jotta kokeeseen osallistuja voidaan tunnistaa vaikeuksitta tai ilman epäilyksiä henkilönumeron perusteella, joka on merkitty koepaperiin tai tämän paperin kansilehdelle, ja näin yhdistää vastaukset häneen.

Toiseksi unionin tuomioistuin totesi, että ammatilliseen kokeeseen osallistujan laatimat kirjalliset vastaukset ovat hänen henkilöönsä liittyviä tietoja. Ensiksikin näiden vastausten sisältö ilmentää osallistujan tietojen ja taitojen tasoa tietyllä alalla ja tarvittaessa hänen päättelyprosessiaan, harkintakykyään ja kriittistä ajatteluaan. Mainittujen vastausten keräämisen tarkoituksena on arvioida kokeeseen osallistujan ammattitaitoa ja hänen soveltuvuuttaan kyseessä olevan ammatin harjoittamiseen. Näiden tietojen käyttö, joka ilmenee muun muassa siinä, läpäiseekö osallistuja asianomaisen kokeen vai ei, voi vaikuttaa osallistujan oikeuksiin ja etuihin, koska se voi määrittää esimerkiksi hänen mahdollisuutensa päästä haluamaansa ammattiin tai

työhön tai vaikuttaa näihin mahdollisuuksiin. Toteamus, jonka mukaan ammatilliseen kokeeseen osallistujan laatimat kirjalliset vastaukset ovat tätä osallistujaa koskevia tietoja sisältönsä, tarkoituksensa ja vaikutuksensa vuoksi, pätee lisäksi myös silloin, kun kyse on – kuten käsiteltävässä asiassa – kokeesta, jossa on mahdollista käyttää kirjallista materiaalia.

Kolmanneksi unionin tuomioistuin totesi osallistujan vastauksiin liittyvistä tarkastajan tekemistä merkinnöistä, että ne ovat osallistujan kokeessa laatimien vastausten tavoin tätä osallistujaa koskevia tietoja, koska ne ilmentävät korjaajan näkemystä tai arviota osallistujan yksilöllisestä suorituksesta ja erityisesti tämän tiedoista ja taidoista kyseisellä alalla. Näiden merkintöjen tarkoituksena on lisäksi nimenomaan antaa tietoja siitä, miten kokeen korjaaja on arvioinut osallistujan suoritusta, ja niillä voi olla vaikutuksia osallistujaan.

Neljänneksi unionin tuomioistuin totesi, että osallistujan ammatillisessa kokeessa laatimat kirjalliset vastaukset ja mahdolliset niihin liittyvät tarkastajan merkinnät voidaan tarkistaa muun muassa niiden paikkansapitävyyden ja säilyttämisen tarpeen osalta direktiivin 95/46/EY 6 artiklan 1 kohdan d ja e alakohdan nojalla, ja niitä voidaan oikaista tai ne voidaan poistaa direktiivin 12 artiklan b alakohdan nojalla. Se, että kokeeseen osallistujalle annetaan oikeus tutustua näihin vastauksiin ja näihin merkintöihin direktiivin 12 artiklan a alakohdan nojalla, palvelee direktiivin tavoitetta, joka on osallistujan yksityisyyden suojelu häntä koskevien tietojen käsittelyssä, ja näin on riippumatta siitä, onko kokeeseen osallistujalla tällainen tiedonsaantioikeus myös koemenettelyyn sovellettavan kansallisen säännösten nojalla. Unionin tuomioistuin kuitenkin korosti, että direktiivin 95/46/EY 12 artiklan a ja b alakohdan mukainen tietojen saantia ja oikaisua koskeva oikeus ei ulotu koekysymyksiin, jotka sellaisinaan eivät ole kokeeseen osallistujan henkilötietoja.

Näiden seikkojen perusteella unionin tuomioistuin katsoi, että pääasiassa kyseessä olevien kaltaisissa olosuhteissa ammatilliseen kokeeseen osallistujan laatimat kirjalliset vastaukset ja mahdolliset tarkastajan niihin tekemät merkinnät ovat direktiivin 95/46/EY 2 artiklan a alakohdassa tarkoitettuja henkilötietoja.

3. Käsite ”henkilötietojen käsittely”

Tuomio 6.11.2003 (suuri jaosto), Lindqvist (C-101/01, [EU:C:2003:596](#))

Lindqvist, joka teki vapaaehtoistyötä Ruotsin protestanttisen kirkon seurakunnan palveluksessa, oli luonut omalla tietokoneellaan internetsivuston, jossa julkaistiin henkilötietoja henkilöistä, jotka olivat hänen kanssaan vapaaehtoistyössä kyseisen seurakunnan palveluksessa. Lindqvist oli veloitettu maksamaan sakko sillä perusteella, että hän oli käyttänyt henkilötietoja automaattisessa käsittelyssä ilman

Datainspektionille (automaattisessa tietojenkäsittelyssä välitettyjen tietojen suojaaja valvova viranomainen) tehtävää kirjallista ennakkoilmoitusta, että hän oli siirtänyt nämä tiedot ilman lupaa kolmanteen valtioon ja että hän oli käsitellyt arkaluonteisia henkilötietoja.

Lindqvist valitti tästä päätöksestä Göta hovrättiin (hovioikeus, Ruotsi), joka tiedusteli unionin tuomioistuimelta erityisesti, oliko Lindqvist suorittanut direktiivissä 95/46 tarkoitettua ”kokonaan tai osittain automatisoitua henkilötietojen käsittelyä”.

Unionin tuomioistuin totesi, että sitä, että internetkotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumeronsa tai antamalla tietoja heidän työsuhteestaan ja harrastuksistaan, on pidettävä direktiivissä tarkoitettuna ”kokonaan tai osittain automatisoituna henkilötietojen käsittelyä”. Tällainen henkilötietojen käsittely, joka toteutetaan vapaaehtoistyön tai uskonnollisen toiminnan harjoittamiseksi, ei kuulu minkään direktiivin soveltamisalan ulkopuolelle sulkemista koskevan poikkeuksen alaan, koska se ei kuulu yleistä turvallisuutta koskevien toimintojen ryhmään eikä myöskään yksinomaan henkilökohtaista tai kotitaloutta koskevan toiminnan ryhmään, jotka on suljettu direktiivin soveltamisalan ulkopuolelle.

Tuomio 13.5.2014 (suuri jaosto), Google Spain ja Google (C-131/12, [EU:C:2014:317](#))

Kyseisessä tuomiossa (ks. myös otsikko II.1. ”Yleisen säännösten soveltamisala”) unionin tuomioistuimella oli tilaisuus täsmentää henkilötietojen käsittelyn käsitettä internetissä suhteessa direktiiviin 95/46.

Unionin tuomioistuin katsoi, että hakukoneen sellaisen toiminnan, joka käsittää sivustallisten internetissä julkaisemien tai siihen liittämien tietojen löytämisen, automaattisen indeksoinnin ja tilapäisen tallentamisen sekä lopuksi kyseisten tietojen asettamisen internetin käyttäjien saataville tietyssä etusijajärjestyksessä, on katsottava olevan henkilötietojen käsittelyä silloin, kun näihin tietoihin sisältyy henkilötietoja. Unionin tuomioistuin myös muistutti, että direktiivissä tarkoitettuja toimia on pidettävä käsittelynä myös siinä tilanteessa, että ne koskevat yksinomaan tiedotusvälineissä julkaistua aineistoa sellaisenaan. Jos direktiivin soveltamisesta poikettaisiin yleisesti tällaisessa tilanteessa, kyseinen direktiivi olisi suurelta osin merkityksetön.

Tuomio 10.7.2018 (suuri jaosto), Jehovan todistajat (C-25/17, [EU:C:2018:551](#))

Suomen tietosuojavaltuutettu oli antanut päätöksen, jolla se kielsi Jehovan todistajat -yhdyshenkilöitä keräämästä tai muutoin käsittelemästä jäsentensä ovelta ovelle -saarnaamistyössä henkilötietoja ilman, että jokin henkilötietolaissa tarkoitetuista henkilötietojen käsittelyn edellytyksistä täyttyy. Tämän yhdyshenkilön jäsenet tekevät ovelta ovelle -saarnaamistyönsä yhteydessä muistiinpanoja tapaamistaan heille ja yhdyshenkilölle vieraista ihmisistä. Tiedot kerätään muistin tueksi ja siinä tarkoituksessa, että ne ovat löydettävissä mahdollista myöhempää käyntiä varten, ja ne kerätään ilman

kyseessä olevien henkilöiden suostumusta ja ilman, että heitä informoidaan tästä. Jehovan todistajat on antanut ohjeistusta muistiinpanojen tekemisestä ainakin saarnaamistyötä käsittelevässä lehtisessään.

Unionin tuomioistuin totesi, että henkilötietojen kerääminen, jota uskonnollisen yhdyskunnan jäsenet suorittavat ovelta ovelle -saarnaamistyön yhteydessä, ja niiden myöhempi käsittely eivät kuulu direktiivin 95/46 soveltamisalaa koskeviin poikkeuksiin, koska ne eivät ole henkilötietojen käsittelyä, joka toteutetaan kyseisen direktiivin 3 artiklan 2 kohdan ensimmäisessä luetelmakohdassa tarkoitetun toiminnan harjoittamiseksi, eivätkä kyseisen direktiivin 3 artiklan 2 kohdan toisessa luetelmakohdassa tarkoitettua luonnollisten henkilöiden suorittamaa henkilötietojen käsittelyä yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa

Tuomio 22.6.2021 (suuri jaosto), Latvijas Republikas Saeima (Liikenne rikkomuspisteet) (C-439/19, [EU:C:2021:504](#))

B:lle, joka on luonnollinen henkilö, on määrätty liikenne rikkomuspisteitä yhdestä tai useammasta tieliikenne rikkomuksesta. Ceļu satiksmes drošības direkcija (liikenneturvallisuusvirasto, Latvia; jäljempänä liikenneturvallisuusvirasto) merkitsi kyseiset liikenne rikkomuspisteet kansalliseen ajoneuvo- ja kuljettajarekisteriin.

Latvian tieliikennesäännösten³⁴ mukaan ajoneuvojen kuljettajille määrättyjä liikenne rikkomuspisteitä koskevat tiedot, jotka on merkitty kyseiseen rekisteriin, ovat yleisön saatavilla, ja liikenneturvallisuusvirasto luovuttaa ne jokaiselle, joka niitä pyytää, ilman että tämän on perusteltava erityinen intressi saada kyseiset tiedot, mukaan lukien talouden toimijoille uudelleen käyttöä varten. B pohti kyseisen säännösten lainmukaisuutta ja teki perustuslain mukaisuutta koskevan valituksen Latvijas Republikas Satversmes tiesaan (perustuslakituomioistuin, Latvia), jotta tämä tutkisi, onko kyseinen säännöstö sopusoinnussa yksityiselämän kunnioittamista koskevan oikeuden kanssa.

Perustuslakituomioistuin katsoi, että arvioidessaan kyseistä perustuslaillista oikeutta sen on otettava huomioon yleinen tietosuoja-asetus. Näin ollen se pyysi unionin tuomioistuinta selventämään useiden yleisen tietosuoja-asetuksen säännösten ulottuvuutta määrittääkseen, onko Latvian tieliikennesäännöstö sopusoinnussa kyseisen asetuksen kanssa.

Tuomiossaan, joka on annettu suuressa jaostossa, unionin tuomioistuin toteaa, että liikenne rikkomuspisteitä koskevien henkilötietojen käsittely on ”rikostuomioihin ja rikoksiin liittyvien henkilötietojen käsittelyä”,³⁵ jonka osalta yleisessä tietosuoja-asetuksessa säädetään paremmasta suojasta kyseessä olevien tietojen erityisen arkaluontoisuuden vuoksi.

³⁴ Tieliikennelain (Ceļu satiksmes likums), joka on annettu 1.10.1997, (Latvijas Vēstnesis, 1997, nro 274/276) 14¹ §:n 2 momentti.

³⁵ Yleisen tietosuoja-asetuksen 10 artikla.

Tässä yhteydessä se huomauttaa aluksi, että liikenneriikkomuspisteitä koskevat tiedot ovat henkilötietoja ja että se, että liikenneturvallisuusvirasto luovuttaa niitä kolmansille, on käsittelyä, joka kuuluu yleisen tietosuoja-asetuksen aineelliseen soveltamisalaan. Mainittu soveltamisala on nimittäin erittäin laaja eikä kyseinen käsittely kuulu mainitun asetuksen sovellettavuutta koskevien poikkeusten soveltamisalaan.

Näin ollen yhtäältä kyseinen käsittely ei kuulu sen poikkeuksen soveltamisalaan, jonka mukaan yleistä tietosuoja-asetusta ei sovelleta käsittelyyn, joka tapahtuu sellaisen toiminnan puitteissa, joka ei kuulu unionin oikeuden soveltamisalaan.³⁶ Kyseisen poikkeuksen ainoana tavoitteena on katsottava olevan sulkea mainitun asetuksen soveltamisalan ulkopuolelle sellainen henkilötietojen käsittely, jota valtion viranomaiset suorittavat sellaisen toiminnan puitteissa, jonka tarkoituksena on turvata kansallinen turvallisuus, tai sellaisen toiminnan puitteissa, joka voidaan luokitella samaan ryhmään. Kyseinen toiminta kattaa erityisesti sellaisen toiminnan, jonka tarkoituksena on suojata keskeiset valtion tehtävät ja yhteiskunnan perustavanlaatuiset edut.

Liikenneturvallisuutta koskevalla toiminnalla ei kuitenkaan tavoitella mainitunlaista päämäärää eikä sitä siten voida luokitella niiden toimintojen ryhmään, joiden tarkoituksena on turvata kansallinen turvallisuus.

Toisaalta liikenneriikkomuspisteitä koskevien henkilötietojen luovuttaminen ei ole myöskään käsittelyä, jonka kattaa poikkeus, jossa säädetään siitä, ettei yleistä tietosuoja-asetusta sovelleta sellaiseen henkilötietojen käsittelyyn, jota toimivaltaiset viranomaiset suorittavat rikosoikeuden alalla.³⁷ Unionin tuomioistuin toteaa nimittäin, ettei liikenneturvallisuusvirastoa voida mainitussa luovuttamisessa pitää mainitunlaisena "toimivaltaisena viranomaisena".³⁸

Sen määrittämiseksi, onko oikeus tutustua tieliikenneriikkomuksia koskeviin henkilötietoihin, kuten liikenneriikkomuspisteisiin, sellaisten "rikoksia"³⁹ koskevien henkilötietojen käsittelyä, jotka saavat parempaa suojaa, unionin tuomioistuin toteaa muun muassa yleisen tietosuoja-asetuksen syntyhistoriaan nojautuen, että kyseisellä käsitteellä viitataan ainoastaan rikoksiin rikosoikeudellisessa merkityksessä. Kuitenkaan se, että Latvian oikeusjärjestyksessä tieliikenneriikkomuksia pidetään hallinnollisina, ei ole määräävää sen arvioimiseksi, kuuluvatko kyseiset rikkomukset "rikoksen" rikosoikeudellisessa merkityksessä käsitteen alaan, koska kyseessä on unionin oikeuden itsenäinen käsite, joka edellyttää koko unionissa itsenäistä ja yhtenäistä tulkintaa. Näin ollen muistutettuaan kolmesta merkityksellisestä arviointiperusteesta sen arvioimiseksi, onko kyseessä rikos rikosoikeudellisessa merkityksessä, eli rikkomuksen oikeudellinen luonnehdinta kansallisessa oikeudessa, rikkomuksen luonne ja aiheutuneen

³⁶ Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan a alakohhta.

³⁷ Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan d alakohhta.

³⁸ Luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäättöksen 2008/977/YOS kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 (EUVL 2016, L 119, s. 89) 3 artiklan 7 kohta.

³⁹ Yleisen tietosuoja-asetuksen 10 artikla.

seuraamuksen ankaruus, unionin tuomioistuinin toteaa, että kyseessä olevat tieliikenneriikkomukset kuuluvat yleisessä tietosuojasetuksessa tarkoitetun ”rikoksen” käsitteen alaan. Kahdesta ensin mainitusta arviointiperusteesta unionin tuomioistuin toteaa, että vaikkei rikkomuksia luokitella ”rikosoikeudellisiksi” kansallisessa oikeudessa, mainitunlainen luonne voi johtua rikkomuksen luonteesta ja muun muassa siitä, että sillä seuraamuksella, joka rikkomuksesta voi aiheutua, on tarkoitus rangaista. Nyt käsiteltävässä asiassa liikenneriikkomuspisteiden jakamisella tieliikenneriikkomuksista, aivan kuten muillakin seuraamuksilla, joita niihin syyllystymisestä voi aiheutua, tavoitellaan muun muassa mainitunlaista päämäärää rangaista. Kolmannesta arviointiperusteesta unionin tuomioistuin huomauttaa, että vain jossain määrin vakavista tieliikenneriikkomuksista määrätään liikenneriikkomuspisteitä ja että näin ollen niistä voi aiheutua jossain määrin ankaria seuraamuksia. Lisäksi mainitunlaisten pisteiden määrääminen tulee yleensä määrätyn seuraamuksen lisäksi ja kyseisten pisteiden kertymisellä on oikeudellisia seurauksia, jotka voivat ulottua jopa ajokieltoon saakka.

Tuomio 5.12.2023 (suuri jaosto), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

Vuonna 2020 Liettuan viranomaiset päättivät järjestää tietoteknisen mobiilisovelluksen hankinnan voidakseen hallinnoida paremmin covid-19-pandemiaa. Sovelluksella oli tarkoitus parantaa epidemiologista seuranta mahdollistamalla covid-19-virukselle altistuneiden henkilöiden tietojen tallentaminen ja seuraaminen.

Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (terveysministeriön alainen kansanterveyslaitos, Liettua; jäljempänä NVSC), jonka tehtäväksi tämä hankinta oli annettu, otti tässä tarkoituksessa yhteyttä UAB ”IT sprendimai sėkmei” -nimiseen yhtiöön (jäljempänä ITSS-yhtiö) ja pyysi tätä luomaan tällaisen mobiilisovelluksen. NVSC:n työntekijät lähettivät tämän jälkeen ITSS-yhtiölle sähköpostiviestejä etenkin niistä kysymyksistä, joiden oli tarkoitus sisältyä kyseiseen sovellukseen.

ITSS-yhtiön luoma mobiilisovellus asetettiin yleisön saataville vuoden 2020 huhti- ja toukokuun välisenä aikana. Sovellusta käytti tämän jälkeen 3 802 henkilöä, jotka antoivat sovelluksessa pyydettyä heitä koskevat eri tiedot. Rahoituksen puuttuessa NVSC ei kuitenkaan tehnyt ITSS-yhtiön kanssa mitään julkista hankintasopimusta ITSS-yhtiön mobiilisovelluksen virallisesta hankkimisesta, ja se päätti sitä koskevan menettelyn.

Tällä välin kansallinen valvontaviranomainen oli aloittanut tutkinnan kyseisen sovelluksen käytöstä seuraavasta henkilötietojen käsittelystä. Valvontaviranomaisen tutkinnan päätteeksi tekemällä päätöksellä sekä NVSC:lle että ITSS-yhtiölle, jonka katsottiin olevan yhteisrekisterinpitäjä, määrättiin hallinnolliset seuraamusmaksut.

NVSC riitautti tämän päätöksen Vilniaus apygardos administracinis teismasissa (Vilnan alueellinen hallintotuomioistuin, Liettua). Koska kyseisellä tuomioistuimella on epäilyjä

useiden yleisen tietosuoja-asetuksen säännösten tulkinnasta, se esitti unionin tuomioistuimelle ennakkoratkaisupyyntöä.

Tuomiossaan, joka on annettu suuressa jaostossa, unionin tuomioistuin täsmensi muun muassa käsittelyn käsitettä. Se totesi tältä osin, että henkilötietojen käyttö mobiilisovelluksen tietoteknisiin testauksiin on yleisessä tietosuoja-asetuksessa tarkoitettua käsittelyä. Näin ei kuitenkaan ole, jos tällaisten tietojen tunnistettavuus on poistettu siten, ettei rekisteröidyn tunnistaminen ole tai ei ole enää mahdollista, tai jos kyse on fiktiivisistä tiedoista, jotka eivät liity olemassa olevaan luonnolliseen henkilöön.

Yhtäältä näet kysymyksellä siitä, käytetäänkö henkilötietoja tietoteknisiin testauksiin tai muuhun tarkoitukseen, ei ole vaikutusta toiminnon luonnehtimiseksi käsittelyksi. Toisaalta pelkästään henkilötietoihin kohdistuva käsittely voidaan luonnehtia yleisen tietosuoja-asetuksessa tarkoitetuksi käsittelyksi. Fiktiiviset tai anonyymit tiedot eivät kuitenkaan ole henkilötietoja.

4. Käsite ”henkilötietojen rekisteröintijärjestelmä”

Tuomio 10.7.2018 (suuri jaosto), Jehovan todistajat (C-25/17, [EU:C:2018:551](#))

Tässä tuomiossa (ks. myös otsikko II.3 Käsite ”henkilötietojen käsittely”) unionin tuomioistuin täsmensi direktiivin 95/46 2 artiklan c alakohdassa tarkoitettua käsitettä ”rekisteröintijärjestelmä”.

Muistutettuaan, että kyseistä direktiiviä sovelletaan ainoastaan sellaisten henkilötietojen manuaaliseen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa, unionin tuomioistuin totesi, että kyseinen käsite kattaa kaikki henkilötiedot, jotka kerätään ovelta ovelle -saarnaamistyön yhteydessä ja joihin kuuluvat nimet ja osoitteet sekä muut tavattuja henkilöitä koskevat tiedot, kun kyseiset tiedot järjestetään tiettyjen sellaisten kriteerien mukaan, joiden ansiosta ne voidaan käytännössä helposti hakea myöhempää käyttöä varten. Jotta tällainen tietojen kokonaisuus kuuluisi kyseisen käsitteen soveltamisalaan, ei ole tarpeen, että se sisältää nimenomaisia kortistoja tai luetteloja tai muita hakua palvelevia järjestelyjä.

5. Käsite ”rekisterinpitäjä”

Tuomio 10.7.2018 (suuri jaosto), Jehovan todistajat (C-25/17, [EU:C:2018:551](#))

Kyseisessä tuomiossa (ks. myös otsikko II.3 Käsite ”henkilötietojen käsittely” ja otsikko II.4 Käsite ”henkilötietojen rekisteröintijärjestelmä”) unionin tuomioistuin lausui uskonnollisen yhdyskunnan rekisterinpitäjän vastuusta sellaisen henkilötietojen käsittelyn osalta, jota harjoitetaan sellaisen ovelta ovelle -saarnaamistyön yhteydessä, jota kyseinen yhdyskunta organisoii ja koordinoi ja johon se kannustaa jäseniään.

Unionin tuomioistuin katsoi, että kunkin henkilön velvollisuutta noudattaa henkilötietojen suoja koskevia unionin oikeuden sääntöjä ei voida pitää puuttumisena uskonnollisten yhdyskuntien organisatoriseen autonomiaan. Tältä osin se totesi, että direktiivin 95/46 2 artiklan d alakohtaa, tarkasteltuna yhdessä perusoikeuskirjan 10 artiklan 1 kohdan kanssa, on tulkittava siten, että sen perusteella uskonnollista yhdyskuntaa voidaan pitää – yhdessä saarnaamistyötä harjoittavien jäsentensä kanssa – rekisterinpitäjänä henkilötietojen käsittelyn osalta, jota viimeksi mainitut harjoittavat yhdyskunnan organisoiman ja koordinoiman ovelta ovelle -saarnaamistyön, johon tämä myös kannustaa, yhteydessä, eikä ole tarpeen, että kyseisellä yhdyskunnalla on oikeus tutustua tietoihin tai että osoitetaan, että se on antanut jäsenilleen kirjallisia ohjeita tai käskyjä, jotka koskevat kyseistä käsittelyä.

Tuomio 5.6.2018 (suuri jaosto), Wirtschaftsakademie Schleswig Holstein (C-210/16, [EU:C:2018:388](#))

Saksalainen tietosuojaviranomainen oli direktiivin 95/46 28 artiklassa tarkoitettuna valvontaviranomaisena määrännyt saksalaisen yhtiön, joka on erikoistunut koulutusalaan ja tarjoaa koulutuspalveluja Facebook-nimisen verkkoyhteisön sivustolla olevan fanisivun välityksellä, poistamaan käytöstä fanisivunsa. Kyseisen viranomaisen mukaan kyseinen yhtiö tai Facebook eivät kumpikaan olleet ilmoittaneet fanisivun käyttäjille, että tämä sivu keräsi evästeiden avulla heitä koskevia henkilötietoja ja että kyseinen yhtiö ja Facebook käsittelivät tämän jälkeen näitä tietoja.

Tässä asiayhteydessä unionin tuomioistuin täsmensi käsitettä ”rekisterinpitäjä” henkilötietojen osalta. Se katsoi tältä osin, että pääasiassa kyseessä olevan yhtiön kaltainen Facebookissa olevan fanisivun hallinnoija osallistuu valitsemalla parametrit (mm. kohdeyleisönsä ja toimintansa hallinnoinnin tai edistämisen tavoitteiden mukaan) fanisivullaan kävijöiden henkilötietojen käsittelyn tarkoituksen ja keinojen määrittämiseen. Tästä syystä mainittua hallinnoijaa on unionin tuomioistuimen mukaan pidettävä direktiivin 95/46 2 artiklan d alakohdassa tarkoitettuna rekisterinpitäjänä unionissa yhdessä Facebook Irelandin (amerikkalaisen Facebook-yhtiön unionissa toimiva tytäryhtiö) kanssa.

Tuomio 29.7.2019, Fashion ID (C-40/17, [EU:C:2019:629](#))

Kyseisessä asiassa unionin tuomioistuin täsmensi käsitettä ”rekisterinpitäjä” suhteessa ”ohjelmallisäkkeen” sisällyttämiseen verkkosivustolle.

Kyseisessä asiassa saksalainen muotivaatteita verkossa myyvä yritys Fashion ID oli liittänyt verkkosivustolleen Facebookin sosiaalisen verkoston ”tykkää”-yhteisöliittännäisen. Tämän liittämisen seurauksena vaikuttaa olevan se, että kun kävijä selaa Fashion ID:n verkkosivustoa, kyseisen kävijän henkilötietoja välitetään Facebook Irelandille. Tämä tietojenvälitys näyttää tapahtuvan ilman, että mainittu kävijä on

tietoinen siitä, ja riippumatta siitä, onko hän Facebookin sosiaalisen verkoston jäsen tai onko hän klikannut Facebookin ”tykkää”-painiketta.

Verbraucherzentrale NRW, joka on kuluttajien etujen turvaamiseen pyrkivä saksalainen yleishyödyllinen yhdistys, moittii Fashion ID:tä siitä, että se on välittänyt Facebook Irelandille sivustollaan kävijöiden henkilötietoja yhtäältä ilman näiden kävijöiden suostumusta ja toisaalta henkilötietojen suojaa koskevissa säännöksissä säädettyjen informointivelvollisuuksien vastaisesti. Oberlandesgericht Düsseldorf (osavaltion ylioikeus, Düsseldorf, Saksa), jossa asia on vireillä, pyysi unionin tuomioistuinta tulkitsemaan useita direktiivin 95/46 säännöksiä.

Unionin tuomioistuin totesi aluksi, että Fashion ID:n kaltaisen verkkosivuston voidaan katsoa olevan direktiivin 95/46 2 artiklan d alakohdassa tarkoitettu rekisterinpitäjä. Tämä rekisterinpitäjän vastuu on kuitenkin rajattu henkilötietojen käsittelyä koskevaan toimintoon tai toimintojen kokonaisuuteen, jonka osalta tämä ylläpitäjä määrittelee tosiasiasa tarkoituksen ja keinot, eli kyseessä olevien tietojen keräämiseen ja niiden siirtämällä tapahtuvaan välittämiseen. Unionin tuomioistuimen mukaan Fashion ID:n on sen sijaan lähtökohtaisesti mahdotonta määritellä sellaisten myöhempien henkilötietojen käsittelytoimien tarkoitusta ja keinoja, jotka Facebook Ireland toteuttaa sen jälkeen, kun tiedot on siirretty sille, mistä syystä Fashion ID:tä ei voida pitää vastuussa näistä toiminnoista kyseisen 2 artiklan d alakohdassa tarkoitettulla tavalla.

Lisäksi unionin tuomioistuin korosti olevan välttämätöntä, että verkkosivuston ylläpitäjä ja Facebook Irelandin kaltainen yhteisöliittännäisen tarjoaja tavoittelevat kumpikin näillä käsittelytoimilla direktiivin 95/46 7 artiklan f alakohdassa tarkoitettua oikeutettua intressiä, jotta toimet olisivat oikeutettuja kummankin niistä osalta.

Lopuksi unionin tuomioistuin totesi, että verkkosivuston ylläpitäjän on saatava direktiivin 95/46 2 artiklan h alakohdassa ja 7 artiklan a alakohdassa tarkoitettu suostumus ainoastaan henkilötietojen käsittelyä koskevan toiminnon tai toimintojen kokonaisuuden osalta, jonka osalta se määrittelee tosiasiasa tarkoituksen ja keinot. Myös kyseisen direktiivin 10 artiklassa säädetty informointivelvollisuus koskee tällaisessa tilanteessa mainittua ylläpitäjää, mutta tietojen, jotka viimeksi mainitun on annettava kyseessä olevalle henkilölle, ei tarvitse kuitenkaan koskea kuin henkilötietojen käsittelyä koskevaa toimintoa tai toimintojen kokonaisuutta, jonka osalta se määrittelee tosiasiasa tarkoituksen ja keinot.

Tuomio 5.12.2023 (suuri jaosto), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

Kyseisessä asiassa (ks. myös otsikko II.3. Käsité ”henkilötietojen käsittely”), unionin tuomioistuin totesi, että rekisterinpitäjänä⁴⁰ voidaan pitää yksikköä, joka on antanut

⁴⁰ Yleisen tietosuojasetuksen 4 artiklan 7 alakohdassa tarkoitettuna rekisterinpitäjänä.

yrittäjien tehtäväksi kehittää tietoteknisen mobiilisovelluksen ja joka on tässä yhteydessä osallistunut kyseisellä sovelluksella toteutetun henkilötietojen käsittelyn tarkoitusten ja keinojen määrittämiseen. Tätä toteamusta ei kyseenalaista se, että tämä yksikkö ei ole itse suorittanut henkilötietojen käsittelytoimia, antanut nimenomaisesti lupaansa konkreettisten henkilötietojen käsittelytoimien toteuttamiseen tai kyseisen mobiilisovelluksen yleisön saataville asettamiseen eikä hankkinut mainittua mobiilisovellusta, jollei tämä yksikkö ole ennen yleisön saataville asettamista nimenomaisesti vastustanut sitä ja siitä johtuvaa henkilötietojen käsittelyä.

6. Käsite ”yhteisrekisterinpitäjä”

Tuomio 5.12.2023 (suuri jaosto), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

Kyseisessä asiassa (ks. myös otsikko II.3. Käsite ”henkilötietojen käsittely” ja otsikko II.5. Käsite ”rekisterinpitäjä”), unionin tuomioistuin huomautti, että kahden yksikön luonnehtiminen yhteisrekisterinpitäjiksi ei edellytä kyseisten yksiköiden välistä sopimusta, jossa määritettäisiin henkilötietojen käsittelyn tarkoitukset ja keinot, tai sopimusta, jossa vahvistettaisiin yhteisrekisterinpitämiseen liittyvät ehdot. Yleisen tietosuoja-asetuksen⁴¹ nojalla yhteisrekisterinpitäjien on tosin määriteltävä keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueet kyseisessä asetuksessa vahvistettujen velvoitteiden noudattamiseksi. Tällaisen järjestelyn olemassaolo ei kuitenkaan ole ennakoedellytys sille, että kaksi tai useampi yksikkö luonnehditaan yhteisrekisterinpitäjiksi, vaan se on velvollisuus, joka yleisessä tietosuoja-asetuksessa asetetaan yhteisrekisterinpitäjille sen jälkeen, kun ne on sellaisiksi luonnehdittu, niitä sitovien kyseisen asetuksen velvoitteiden noudattamisen varmistamiseksi. Tämä luonnehdinta perustuu siis pelkästään siihen, että useat yksiköt ovat osallistuneet käsittelyn tarkoitusten ja keinojen määrittämiseen.

Unionin tuomioistuin totesi sen osalta, että asianomaiset yksiköt määrittävät yhdessä käsittelyn tarkoitukset ja keinot, että näiden yksiköiden osallistuminen tähän määrittämiseen voi tapahtua eri muodoissa ja perustua sekä niiden yhteiseen päätökseen että niiden yhdenmukaisiin päätöksiin. Jälkimmäisessä tapauksessa näiden päätösten on kuitenkin täydennettävä toisiaan siten, että kukin niistä vaikuttaa konkreettisesti käsittelyn tarkoitusten ja keinojen määrittämiseen.

⁴¹ Yleisen tietosuoja-asetuksen 26 artiklan 1 kohta, kun sitä luetaan asetuksen johdanto-osan 79 perustelukappaleen valossa.

7. Henkilötietojen käsittelyn laillisuuden edellytykset

Tuomio 16.12.2008 (suuri jaosto), Huber (C-524/06, [EU:C:2008:724](#))

Saksan liittotasavallan siirtolais- ja pakolaisvirasto (Bundesamt für Migration und Flüchtlinge) hallinnoi ulkomaalaisista pidettävää keskusrekisteriä, johon kootaan tiettyjä henkilötietoja niistä ulkomaalaisista, joiden oleskelu Saksan alueella kestää yli kolme kuukautta. Rekisteriä käytetään tilastotieteellisiin tarkoituksiin ja silloin, kun turvallisuus-, poliisi- sekä oikeusviranomaiset käyttävät toimivaltaa rikollisen tai yleisen turvallisuuden vaarantavan toiminnan estämiseen tai sellaisen selvittämiseen.

Itävallan kansalainen Huber muutti Saksaan vuonna 1996 harjoittaakseen siellä itsenäisen vakuutusasiamiehen ammattia. Hän katsoi tulleen syrjityksi kyseisen rekisterin sisältämien häntä koskevien tietojen käsittelyn vuoksi erityisesti, koska tällaista tietokantaa ei pidetä Saksan kansalaisista, ja pyysi näiden tietojen poistamista.

Tässä yhteydessä oikeusriitaa käsittelevä Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Nordrhein-Westfalenin osavaltion ylemmän asteen hallintotuomioistuin, Saksa) esitti unionin tuomioistuimelle ennakkoratkaisupyyntöä siitä, oliko kyseisessä rekisterissä suoritettu henkilötietojen käsittely unionin oikeuden mukaista.

Unionin tuomioistuin muistutti ensimmäiseksi, että unionin kansalaisten oikeus oleskella sellaisen jäsenvaltion alueella, jonka kansalainen hän ei ole, ei ole ehdoton, vaan siihen voi liittyä rajoituksia. Tämän vuoksi tällaisen rekisterin käyttäminen tukemaan oleskeluoikeutta koskevan lainsäädännön soveltamisesta vastaavia viranomaisia on lähtökohtaisesti hyväksyttävää ja sen luonteen vuoksi yhteensoveltuva EY 12 artiklan ensimmäisen kohdan (josta on tullut SEUT 18 artiklan ensimmäinen kohta) sisältämän kansalaisuuden perusteella tapahtuvan syrjinnän kiellon kanssa. Tällaisessa rekisterissä saa kuitenkin olla vain ne tiedot, jotka ovat tätä varten tarpeen henkilötietojen suojasta annetussa direktiivissä tarkoitetulla tavalla.

Direktiivin 95/46 7 artiklan e alakohdassa tarkoitettu käsittelyn tarpeellisuutta koskevasta käsitteestä unionin tuomioistuin totesi ensimmäiseksi, että kyse on unionin oikeuden itsenäisestä käsitteestä, jota on tulkittava siten, että se vastaa täysimääräisesti tämän direktiivin tavoitetta, joka on määritelty sen 1 artiklan 1 kohdassa. Henkilötietojen käsittelyjärjestelmä on unionin oikeuden mukainen, jos se sisältää yksinomaan tiedot, jotka ovat tarpeen, jotta kyseiset viranomaiset voivat soveltaa tätä lainsäädäntöä, ja jos sen keskitetyn luonteen avulla tätä lainsäädäntöä voidaan soveltaa tehokkaammin sellaisten unionin kansalaisten oleskeluoikeuden osalta, jotka eivät ole tämän jäsenvaltion kansalaisia.

Direktiivin 95/46 7 artiklan e alakohdassa tarkoitetulla tavalla tarpeellisina ei missään tapauksessa voida pitää nimeltä mainittujen henkilöiden henkilötietojen tallentamista ja käsittelyä tämän kaltaisen rekisterin puitteissa tilastotieteellisiin.

Mitä tulee rekisterin sisältämien tietojen käyttöön rikollisuuden torjuntaan, unionin tuomioistuin totesi, että tämä tavoite liittyy syytteiden nostamiseen tehdyistä rikoksista ja rikkomuksista tekijöiden kansalaisuudesta riippumatta. Tämän vuoksi jäsenvaltion kannalta sen kansalaisten tilanne ei voi rikollisuuden torjunnan tavoitteen valossa olla erilainen kuin sellaisten unionin kansalaisten asema, jotka eivät ole tämän jäsenvaltion kansalaisia ja jotka oleskelevat tämän jäsenvaltion alueella. Näin ollen jäsenvaltion kansalaisten ja unionin kansalaisten erilainen kohtelu, joka johtuu siitä, että ainoastaan unionin kansalaisten, jotka eivät ole kyseessä olevan jäsenvaltion kansalaisia, henkilötietoja käsitellään järjestelmällisesti rikollisuuden torjumiseksi, merkitsee EY 12 artiklan ensimmäisessä kohdassa kiellettyä syrjintää.

Tuomio 19.10.2016, Breyer (C-582/14, [EU:C:2016:779](#))

Kyseisessä tuomiossa (ks. myös otsikko II.2. Käsite ”henkilötiedot”) unionin tuomioistuin lausui myös siitä, onko direktiivin 95/46/EY 7 artiklan f alakohta esteenä kansalliselle oikeussäännölle, jonka nojalla verkkomediapalvelun tarjoaja saa kerätä ja hyödyntää käyttäjän henkilötietoja ilman tämän suostumusta vain silloin, kun tämä on tarpeen, jotta mahdollistetaan kyseisen käyttäjän kyseisen verkkomediapalvelun tosiasiallinen käyttö ja tämän käytön laskutus, ja jonka mukaan verkkomediapalvelun yleisen toiminnan takaamisen tavoitteella ei voida oikeuttaa kulloisenkin yksittäisen käytön päättymisen jälkeistä hyödyntämistä.

Unionin tuomioistuin totesi, että direktiivin 95/46/EY 7 artiklan f alakohta ei ole esteenä kyseessä olevalle säännöstölle. Mainitun säännöksen nojalla siinä tarkoitettu henkilötietojen käsittely on laillista, jos käsittely on tarpeen rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamiseksi, paitsi milloin tämän intressin syrjäyttävät rekisteröidyn intressit ja perusoikeudet ja -vapaudet. Käsiteltävässä asiassa Saksan säännöstössä suljettiin ehdottomasti ja yleisesti pois mahdollisuus käsitellä tiettyihin tietoryhmiin kuuluvia henkilötietoja sallimatta niiden oikeuksien ja intressien punnitsemista, joista on kyse tietyssä yksittäisessä tapauksessa. Tällä tavoin sillä rajoitettiin tämän direktiivin 95/46 7 artiklan f alakohdassa vahvistetun periaatteen ulottuvuutta, kun siinä suljettiin pois se, että verkkomediapalvelun yleisen toiminnan takaamisen tavoitetta voitaisiin punnita suhteessa käyttäjien intresseihin tai perusoikeuksiin ja -vapauksiin.

Tuomio 27.9.2017, Puškár (C-73/16, [EU:C:2017:725](#))

Pääasian oikeudenkäynnissä Puškár nosti kanteen Najvyšší súd Slovenskej republikyssa (Slovakian tasavallan ylin tuomioistuin) ja vaati, että Finančné riaditeľstvo (verohallitus), kaikki sen alaiset vero toimistot ja Kriminálny úrad finančnej správy (talousrikollisuuden torjuntavirasto) veloitetaan poistamaan Puškárin nimi verohallituksen bulvaaniksi katsomien henkilöiden luettelosta, jonka verohallitus on laatinut veronkannon tarkoituksessa ja jonka päivityksestä vastaavat verohallitus, sen alaiset vero toimistot

sekä talousrikollisuuden torjuntavirasto (jäljempänä riidanalainen luettelo). Hän vaati myös poistamaan kaikki häntä koskevat merkinnät näistä luetteloista ja verohallinnon tietojärjestelmästä.

Tässä tilanteessa Najvyšší súd Slovenskej republiky tiedusteli unionin tuomioistuimelta muun muassa, voidaanko perusoikeuskirjan 7 artiklassa vahvistettua oikeutta yksityis- ja perhe-elämän, kodin sekä viestien kunnioittamiseen ja 8 artiklassa vahvistettua oikeutta henkilötietojen suojaan tulkita siten, ettei jäsenvaltio voi ilman rekisteröidyn suostumusta koota veronkannon tarpeisiin luetteloja henkilötiedoista, toisin sanoen siten, että henkilötietojen hankkimiseen viranomaisen käyttöön veropetosten torjumiseksi liittyy itsessään riskejä.

Unionin tuomioistuin katsoi, että direktiivin 95/46/EY 7 artiklan e alakohta ei ole esteenä sille, että jäsenvaltion viranomaiset suorittavat veronkannon ja veropetosten torjunnan tarkoituksessa sen kaltaista henkilötietojen käsittelyä kuin riidanalaisen luettelon laatiminen pääasiassa ilman rekisteröityjen suostumusta, edellyttäen yhtäältä, että näille viranomaisille on kansallisessa lainsäädännössä annettu kyseisessä säännöksessä tarkoitettuja yleistä etua koskevia tehtäviä, että tämän luettelon laatiminen ja rekisteröityjen nimen merkitseminen siihen ovat tosiasiallisesti soveltuvia ja tarpeen tavoiteltujen päämäärien saavuttamiseksi ja että on olemassa riittäviä indisioita olettaa, että rekisteröidyt ovat luettelossa perustellusti, ja toisaalta, että kaikki direktiivissä 95/46/EY asetetut henkilötietojen käsittelyn laillisuuden edellytykset.

Unionin tuomioistuin huomautti tästä, että ennakkoratkaisua pyytäneen tuomioistuimen on tarkistettava, onko riidanalaisen luettelon laatiminen tarpeen pääasiassa kyseessä olevien yleistä etua koskevien tehtävien suorittamiseksi, kun otetaan huomioon erityisesti riidanalaisen luettelon laatimisen täsmällinen tarkoitus, oikeusvaikutukset, jotka koskevat luettelossa mainittuja henkilöitä, sekä se, onko luettelo julkinen vai ei. Ennakkoratkaisua pyytäneen tuomioistuimen on suhteellisuusperiaatteen kannalta arvioituna tarkistettava, onko niin, että riidanalaisen luettelon laatiminen ja rekisteröityjen nimien merkitseminen luetteloon soveltuvat niillä tavoiteltujen päämäärien saavuttamiseksi ja ettei näiden päämäärien saavuttamiseksi ole olemassa lievempiä keinoja.

Unionin tuomioistuin totesi vielä, että se, että henkilö on merkitty riidanalaiseen luetteloon, voi loukata joitakin hänen oikeuksistaan. Tähän luetteloon merkitseminen voi näet vahingoittaa hänen mainettaan ja vaikuttaa hänen suhteisiinsa veroviranomaisiin. Tämä merkintä voi myös vaikuttaa kyseisen henkilön syyttömyysolettamaan, joka on vahvistettu perusoikeuskirjan 48 artiklan 1 kohdassa, sekä oikeushenkilöiden, jotka on liitetty riidanalaiseen luetteloon merkittyihin luonnollisiin henkilöihin, perusoikeuskirjan 16 artiklan mukaiseen elinkeinovapauteen. Tällainen puuttuminen voi olla asianmukainen vain, jos on riittäviä viitteitä epäilystä, että rekisteröity toimii näennäisesti häneen liitettyjen oikeushenkilöiden johtotehtävissä, mikä vaikuttaa haitallisesti veronkantoa ja veropetosten torjuntaa koskevaan yleiseen etuun.

Unionin tuomioistuin katsoi myös, että jos on olemassa syitä direktiivin 95/46/EY 13 artiklan nojalla rajoittaa joitakin sen 6 ja 10–12 artiklassa säädettyjä oikeuksia kuten rekisteröidyn oikeutta informointiin, tällaisen rajoituksen on oltava välttämätön 13 artiklan 1 kohdassa mainitun edun, kuten tärkeän taloudellisen tai rahoituksellisen edun verotusta koskeissa asioissa, varmistamiseksi, ja perustuttava lainsäädännöllisiin toimenpiteisiin.

Tuomio 11.11.2020, Orange Romania (C-61/19, [EU:C:2020:901](#))

Orange România SA tarjoaa matkaviestinpalveluja Romanian markkinoilla. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (henkilötietojen käsittelyä valvova kansallinen viranomainen, Romania) määräsi 28.3.2018 tekemällään päätöksellä Orange Românialle sakon sen vuoksi, että tämä oli säilyttänyt kopioita asiakkaidensa henkilöllisyystodistuksista ilman näiden nimenomaista suostumusta.

ANSPDCP:n mukaan Orange România oli tehnyt 1.–26.3.2018 matkaviestinpalvelujen tarjoamisesta sopimuksia, jotka sisältävät ehdon, jonka mukaan asiakkaille on ilmoitettu heidän henkilöllisyystodistustensa jäljennöksen keräämisestä ja säilyttämisestä tunnistamistarkoituksessa ja he ovat antaneet tähän suostumuksensa. Rekisterinpitäjä on merkinnyt kyseistä ehtoa koskevaan ruutuun rastin ennen sopimuksen allekirjoittamista.

Tässä asiayhteydessä Tribunalul București (Bukarestin alueellinen tuomioistuin, Romania) pyysi unionin tuomioistuinta täsmentämään niitä edellytyksiä, joiden on täyttyttävä, jotta asiakkaiden suostumusta henkilötietojen käsittelyyn voidaan pitää pätevänä.

Unionin tuomioistuin muistuttaa aluksi, että unionin oikeudessa⁴² esitetään luettelo tapauksista, joissa henkilötietojen käsittelyn voidaan katsoa olevan lainmukaista. Erityisesti rekisteröidyn suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen.⁴³ Suostumusta ei ole annettu pätevästi vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta.

Lisäksi jos rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka koskee myös muita asioita, ilmoitus on annettava helposti ymmärrettävässä ja helposti saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Jotta rekisteröidyllä olisi todellinen valinnanvapaus, sopimusmääräykset eivät saa johtaa häntä harhaan mahdollisuudesta tehdä sopimus, vaikka hän kieltäytyisi hyväksymästä tietojensa käsittelyä.

⁴² Direktiivin 95/46 7 artikla ja yleisen tietosuojasetuksen 6 artikla.

⁴³ Direktiivin 95/46 2 artiklan h alakohta ja yleisen tietosuojasetuksen 4 artiklan 11 kohta.

Unionin tuomioistuimien täsmentää, että koska Orange România on henkilötietojen rekisterinpitäjä, sen on kyettävä osoittamaan näiden tietojen käsittelyn lainmukaisuus, ja näin ollen tässä tapauksessa asiakkaidensa pätevän suostumuksen olemassaolo. Koska kyseiset asiakkaat eivät näytä itse rastineen henkilöllisyystodistustensa jäljennöksen keräämistä ja säilyttämistä koskenutta ruutua, pelkästään se seikka, että tämä ruutu on rastitettu, ei ole omiaan osoittamaan, että nämä asiakkaat olisivat ilmaisseet aktiivisesti suostumuksensa siihen. Tätä koskevien tarpeellisten selvitysten toteuttaminen kuuluu ennakkoratkaisua pyytäneelle tuomioistuimelle.

Unionin tuomioistuimen mukaan kansallisen tuomioistuimen on myös arvioitava sitä, saattoivatko pääasiassa kyseessä olevat sopimusmääräykset johtaa rekisteröityä harhaan mahdollisuudesta tehdä sopimus siitä huolimatta, että hän ei suostunut tietojensa käsittelyyn, kun tätä koskevia täsmennyksiä ei ollut. Lisäksi unionin tuomioistuin huomauttaa, että siinä tapauksessa, että asiakas ei antanut suostumusta, Orange România vaati, että kyseinen asiakas ilmoittaa kirjallisesti, ettei hän suostu henkilöllisyystodistuksensa kopion keräämiseen eikä säilyttämiseen. Unionin tuomioistuimen mukaan tällainen lisävaatimus on omiaan vaikuttamaan epäasianmukaisesti valinnanvapauteen vastustaa tällaista keräämistä ja säilyttämistä. Joka tapauksessa on niin, että koska kyseisen yhtiön on osoitettava, että sen asiakkaat ovat aktiivisella toiminnallaan ilmaisseet suostumuksensa henkilötietojensa käsittelyyn, kyseinen yhtiö ei voi vaatia, että he ilmaisevat kieltäytymisensä aktiivisesti.

Unionin tuomioistuin toteaa näin ollen, että televiestintäpalvelujen tarjoamista koskeva sopimus, johon sisältyy ehto, jonka mukaan rekisteröity on saanut tiedon henkilöllisyystodistuksensa kopion keräämisestä ja säilyttämisestä tunnistamistarkoituksessa ja hän on suostunut tähän, ei ole omiaan osoittamaan, että kyseinen henkilö olisi antanut pätevästi näissä säännöksissä tarkoitetun suostumuksensa tähän keräämiseen ja säilyttämiseen, kun rekisterinpitäjä on rastittanut tähän ehtoon liittyvän ruudun ennen sopimuksen allekirjoittamista tai kyseisen sopimuksen sopimusmääräykset saattavat johtaa rekisteröityä harhaan mahdollisuudesta tehdä kyseinen sopimus siitä huolimatta, että hän kieltäytyy antamasta suostumustaan tietojensa käsittelyyn, tai rekisterinpitäjä vaikuttaa epäasianmukaisesti valinnanvapauteen vastustaa tätä keräämistä ja säilyttämistä vaatimalla, että rekisteröidyn on suostumuksensa epäämiseksi täytettävä lisälomake, jossa kyseinen kieltäytyminen mainitaan.

Tuomio 22.6.2021 (suuri jaosto), Latvijas Republikas Saeima (Liikennevirasto)
(C-439/19, [EU:C:2021:504](#))

Tässä tuomiossa (ks. myös otsikko II.3 Käsité ”henkilötietojen käsittely”) unionin tuomioistuin totesi, että yleinen tietosuoja-asetus on esteenä lainsäädännölle, jolla veloitetaan Ceļu satiksmes drošības direkcija (liikenneturvallisuusvirasto, Latvia; jäljempänä liikenneturvallisuusvirasto) saattamaan suuren yleisön saataville tiedot, jotka koskevat ajoneuvojen kuljettajille tieliikennevirastoista määrättyjä

liikenneterikkomuspisteitä, ilman, että tietojen pyytäjän on esitettävä erityistä intressiä niiden saamiseen. Se totesi, että kun otetaan huomioon muun muassa liikenneturvallisuuden parantamisen tavoite, johon Latvian hallitus on vedonnut, tieliikenneterikkomuksista määrättyjä liikenneterikkomuspisteitä koskevien henkilötietojen luovuttamisen välttämättömyyttä ei ole osoitettu. Unionin tuomioistuimen mukaan yleisön oikeus tutustua virallisiin asiakirjoihin ja tiedonvälityksen vapaus eivät myöskään oikeuta mainitunlaista säännöstöä.

Tässä asiayhteydessä unionin tuomioistuin korosti, että liikenneturvallisuuden parantaminen, johon Latvian säännöstöllä pyritään, on unionin tunnustama yleisen edun mukainen tavoite, ja että näin ollen jäsenvaltiot voivat luokitella liikenneturvallisuuden ”yleistä etua koskevaksi tehtäväksi”.⁴⁴ Kuitenkaan sitä, että Latvian järjestelmässä on välttämätöntä luovuttaa liikenneterikkomuspisteitä koskevia henkilötietoja, jotta tavoitellun päämäärän saavuttaminen varmistetaan, ei ole osoitettu. Yhtäältä Latvian lainsäätäjällä on nimittäin käytettävissään lukuisia toimintatapoja, jotka mahdollistavat sille unionin tuomioistuimen mukaan kyseisen tavoitteen saavuttamisen muilla rekisteröityjen perusoikeuksia vähemmän rajoittavilla keinoilla. Toisaalta on otettava huomioon liikenneterikkomuspisteitä koskevien tietojen arkaluontoisuus ja se, että niiden luovuttaminen yleisölle on omiaan muodostamaan vakavan puuttumisen yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin oikeuksiin, koska se voi aiheuttaa yhteiskunnan paheksuntaa ja rekisteröidyn leimautumista.

Unionin tuomioistuin katsoi lisäksi, että kun otetaan huomioon kyseisten tietojen arkaluontoisuus ja se, miten vakavasti mainittuun kahteen perusoikeuteen puututaan, kyseiset oikeudet ovat tärkeämpiä kuin sekä virallisten asiakirjojen, kuten kansallisen ajoneuvo- ja kuljettajarekisterin, julkisuutta koskeva etu että oikeus tiedonvälityksen vapauteen.

Samoista syistä unionin tuomioistuin katsoi, että yleinen tietosuoja-asetus on esteenä Latvian säännöstölle myös siltä osin kuin siinä annetaan liikenneturvallisuusvirastolle oikeus luovuttaa ajoneuvojen kuljettajille tieliikenneterikkomuksista määrättyjä liikenneterikkomuspisteitä koskevat tiedot talouden toimijoille, jotta viimeksi mainitut voivat uudelleenkäyttää niitä ja luovuttaa ne yleisölle.

Viimeiseksi unionin tuomioistuin totesi, että unionin oikeuden ensisijaisuuden periaate on esteenä sille, että ennakkoratkaisua pyytänyt tuomioistuin, jonka käsiteltävänä on valitus Latvian säännöstöstä, jonka unionin tuomioistuin on katsonut olevan ristiriidassa unionin oikeuden kanssa, päättää pysyttää voimassa kyseisen säännöstön oikeusvaikutukset lainvoimaisen tuomionsa julistamispäivään saakka.

⁴⁴ Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan nojalla henkilötietojen käsittely on lainmukaista, jos ”käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi –”.

III. Alakohtaisessa säännöstössä tarkoitettu henkilötietojen käsittely

1. Henkilötietojen käsittely sähköisen viestinnän alalla

Tuomio 2.10.2018 (suuri jaosto), Ministerio Fiscal (C-207/16, [EU:C:2018:788](#))

Tässä asiassa oli kyse siitä, että espanjalainen tutkintatuomari hylkäsi pyynnön, joka oli esitetty lompakon ja matkapuhelimen ryöstöä koskevan tutkinnan yhteydessä. Erityisesti rikospoliisi oli pyytänyt tutkintatuomarilta määräystä, jotta se saisi niiden puhelinnumeroiden haltijoista, jotka oli aktivoitu varastetulla matkapuhelimella 12 päivän ajanjaksolla ryöstöpäivästä lukien. Pyyntö oli hylätty sillä perusteella, että rikostutkinnan taustalla olevat tosiseikat eivät merkinneet ”vakavaa” rikosta – eli Espanjan oikeuden mukaan rikosta, jonka seuraamuksena on yli viiden vuoden vankeusrangaistus – sillä tunnistetiedot voitiin luovuttaa ainoastaan tällaisten rikosten osalta.

Muistutettuaan, että viranomaisen oikeus saada sähköisten viestintäpalvelujen tarjoajien säilyttämiä henkilötietoja rikostutkinnan yhteydessä kuuluu direktiivin 2002/58 soveltamisalaan, unionin tuomioistuin totesi, että oikeus saada varastetulla matkapuhelimella aktivoitujen SIM-korttien haltijoiden henkilöllisyyttä koskevia tietoja, kuten sukunimiä, etunimiä ja mahdollisesti näiden haltijoiden osoitteita, merkitsee puuttumista perusoikeuskirjassa vahvistettuihin yksityiselämän suojaa ja tietosuojaa koskeviin perusoikeuksiin, vaikka olosuhteet eivät ole sellaiset, että tätä puuttumista olisi pidettävä ”vakavana”, eikä merkitystä ole sillä, ovatko kyseessä olevat yksityiselämää koskevat tiedot arkaluonteisia vai eivät, eikä sillä, onko asianosaisille aiheutunut tästä puuttumisesta mahdollista haittaa vai ei. Unionin tuomioistuin korosti kuitenkin, ettei tämä puuttuminen ole niin vakavaa, että tätä oikeutta olisi rajoitettava rikosten ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan alalla vain vakavan rikollisuuden torjumiseen. Vaikka direktiivissä 2002/58 luetellaan tyhjentävästi ne tavoitteet, joilla voidaan perustella kansallista lainsäädäntöä, jolla säännellään viranomaisten oikeutta saada kyseessä olevia tietoja ja siten poiketaan sähköisen viestinnän luottamuksellisuuden periaatteesta, joten tietojen saannin on oltava tosiasiallisesti ja ehdottomasti näistä tavoitteista jonkin mukaista, unionin tuomioistuin huomauttaa, että kun kyse on rikosten torjunnan, tutkinnan, selvittämisen ja syyteharkinnan tavoitteesta, että direktiivin 2002/58 sanamuodossa tätä tavoitetta ei rajata vain vakaviin rikoksiin vaan se koskee ”rikoksia”.

Tässä asiayhteydessä unionin tuomioistuin täsmensi, että vaikka se katsoi tuomiossaan Tele2 Sverige ja Watson ym.⁴⁵, että vain vakavan rikollisuuden torjuminen voi oikeuttaa

⁴⁵ Tuomio 21.12.2016, Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, [EU:C:2016:970](#)).

viranomaisen tiedonsaannin viestintäpalvelujen tarjoajien säilyttämistä henkilötiedoista, joiden kokonaisuus voi mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, tämä tulkinta perustui siihen, että tätä tiedonsaantia sääntelevän lainsäädännön tavoitteella on oltava yhteys sen perusoikeuksiin puuttumisen vakavuuteen, jota tämä toimenpide merkitsee. Suhteellisuusperiaatteen mukaisesti vakava puuttuminen voi olla oikeutettu tällä alalla vain sellaisen rikollisuuden torjumisen tavoitteella, joka on myös luokiteltavissa "vakavaksi". Sen sijaan silloin, kun puuttuminen, jota tällainen tietojensaanti merkitsee, ei ole vakavaa, se voidaan oikeuttaa yleisesti "rikosten" ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan alalla.

Esillä olevassa asiassa unionin tuomioistuin katsoi, että tietojen saantia vain niistä tiedoista, joita pääasiassa esitetty pyyntö koskee, ei voida pitää "vakavana" puuttumisena niiden henkilöiden perusoikeuksiin, joiden tiedoista on kyse, sillä näiden tietojen perusteella ei voida tehdä täsmällisiä päätelmiä heidän yksityiselämästään. Unionin tuomioistuin totesi tämän perusteella, että puuttuminen, jota pääsy näihin tietoihin merkitsee, voidaan näin ollen oikeuttaa yleisesti "rikosten" ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan tavoitteella, eikä näiden rikosten luokittelu "vakaviksi" ole tarpeen.

Tuomiot 6.10.2020 (suuri jaosto), Privacy International (C-623/17, [EU:C:2020:790](#)) ja La Quadrature du Net ym. (C-511/18, C-512/18 et C-520/18, [EU:C:2020:791](#))

Henkilötietojen säilyttämistä ja oikeutta saada niitä sähköisen viestinnän alalla koskeva oikeuskäytäntö, erityisesti tuomio Tele2 Sverige ja Watson ym., jossa unionin tuomioistuin katsoi muun muassa, että jäsenvaltiot eivät voi asettaa sähköisten viestintäpalvelujen tarjoajille velvollisuutta säilyttää liikenne- ja paikkatietoja yleisesti ja erotuksetta, on aiheuttanut huolta eräille valtioille, jotka pelkäävät, että niiltä on evätty väline, jota ne pitävät tarpeellisena kansallisen turvallisuuden takaamiseksi ja rikollisuuden torjumiseksi.

Investigatory Powers Tribunalin (tutkintavaltuuksia koskevia asioita käsittelevä tuomioistuin, Yhdistynyt kuningaskunta) (Privacy International, C-623/17), Conseil d'État'n (ylin hallintotuomioistuin, Ranska) (La Quadrature du Net ym., yhdistetyt asiat C-511/18 ja C-512/18) ja Cour constitutionnelles (perustuslakituomioistuin, Belgia) (Ordre des barreaux francophones et germanophone ym., C-520/18) käsiteltäviksi on tätä taustaa vasten saatettu oikeusriitoja, jotka koskevat tiettyjen jäsenvaltioiden näillä aloilla antamien sellaisten säännösten lainmukaisuutta, joissa säädetään erityisesti sähköisten viestintäpalvelujen tarjoajien velvollisuudesta siirtää viranomaiselle käyttäjien liikenne- ja paikkatiedot tai säilyttää kyseiset tiedot yleisesti tai erotuksetta.

Unionin tuomioistuin totesi kahdessa 6.10.2020 suurena jaostona antamassaan tuomiossa ensinnäkin, että direktiiviä 2002/58 sovelletaan kansallisiin säännöksiin, joiden mukaan sähköisten viestintäpalvelujen tarjoajien on kansallisen turvallisuuden

takaamiseksi toteutettava henkilötietojen käsittelyä, kuten esimerkiksi säilytettävä liikenne- ja paikkatietoja ja siirrettävä niitä turvallisuus- ja tiedustelupalveluille.

Tämän jälkeen unionin tuomioistuin muistutti, että direktiivissä 2002/58⁴⁶ ei sallita sitä, että sähköisen viestinnän ja siihen liittyvien tietojen luottamuksellisuuden takaamista koskevasta periaatteellisesta velvollisuudesta ja näiden tietojen tallentamista koskevasta kiellosta poikkeamisesta tulisi sääntö. Tämä merkitsee sitä, että kyseisessä direktiivissä sallitaan se, että jäsenvaltiot toteuttavat muun muassa kansallisen turvallisuuden vuoksi lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan kyseisessä direktiivissä säädettyjen oikeuksien ja velvollisuuksien ulottuvuutta ja erityisesti velvollisuutta taata viestinnän ja liikennetietojen luottamuksellisuus,⁴⁷ ainoastaan, jos unionin oikeuden yleisiä periaatteita, joihin kuuluu suhteellisuusperiaate, ja perusoikeuskirjassa taattuja perusoikeuksia⁴⁸ noudatetaan.

Unionin tuomioistuin katsoi tässä yhteydessä yhtäältä asiassa *Privacy International*, että direktiivi 2002/58, luettuna perusoikeuskirjan valossa, on esteenä kansalliselle säännöstölle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on kansallisen turvallisuuden takaamiseksi siirrettävä liikenne- ja paikkatietoja yleisesti ja erotuksetta turvallisuus- ja tiedustelupalveluille. Toisaalta yhdistetyissä asioissa *La Quadrature du Net* ym. ja asiassa *Ordre des barreaux francophones et germanophone* ym. unionin tuomioistuin katsoi, että tämä sama direktiivi on esteenä lainsäädännöllisille toimenpiteille, joilla sähköisten viestintäpalvelujen tarjoajat velvoitetaan ennakoivasti säilyttämään liikenne- ja paikkatietoja yleisesti ja erotuksetta.

Nämä velvollisuudet, jotka koskevat tällaisten tietojen siirtämistä ja yleistä ja erotuksetta tapahtuvaa säilyttämistä, merkitsevät näet erityisen vakavaa puuttumista perusoikeuskirjassa taattuihin perusoikeuksiin ilman, että niiden henkilöiden, joiden tiedot ovat kyseessä, toiminta liittyisi kyseessä olevan säännösten tavoitteeseen. Unionin tuomioistuin tulkitsi yleisen tietosuoja-asetuksen 23 artiklan 1 kohtaa, luettuna perusoikeuskirjan valossa, analogisesti siten, että se on esteenä kansalliselle säännöstölle, jonka mukaan yhteyttä yleisölle tarkoitettuihin verkkoviestintäpalveluihin tarjoavien toimijoiden ja hosting-palvelujen tarjoajien on säilytettävä yleisesti ja erotuksetta muun muassa kyseisiin palveluihin liittyvät henkilötiedot.

Unionin tuomioistuin katsoi sitä vastoin, että tilanteissa, joissa asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavaksi olevaksi, direktiivi 2002/58, luettuna perusoikeuskirjan valossa, ei ole esteenä sille, että sähköisten viestintäpalvelujen tarjoajat määrätään säilyttämään liikenne- ja paikkatietoja yleisesti ja erotuksetta. Unionin tuomioistuin täsmensi tässä yhteydessä, että joko tuomioistuimen tai riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, on valvottava

⁴⁶ Direktiivin 2002/58 15 artiklan 1 ja 3 kohta.

⁴⁷ Direktiivin 2002/58 5 artiklan 1 kohta.

⁴⁸ Erityisesti perusoikeuskirjan 7, 8 ja 11 artikla sekä 52 artiklan 1 kohta.

tehokkaasti päätöstä, jolla tällainen määräys annetaan ajanjaksoksi, joka on rajoitettu täysin välttämättömään, sen tarkastamiseksi, että kyseessä on jokin näistä tilanteista ja että niitä edellytyksiä ja takeita, joista on säädetävä, noudatetaan. Mainittu direktiivi ei samoin edellytyksin ole esteenä myöskään kaikkien sähköisten viestintävälineiden käyttäjien tietojen ja muun muassa liikenne- ja paikkatietojen automaattiselle analysoinnille.

Unionin tuomioistuin totesi vielä, että direktiivi 2002/58, luettuna perusoikeuskirjan valossa, ei ole esteenä lainsäädännöllisille toimenpiteille, jotka mahdollistavat liikenne- ja paikkatietojen kohdennetun säilyttämisen, joka on ajallisesti rajoitettu täysin välttämättömään ja joka on objektiivisten ja syrjimättömien seikkojen perusteella rajattu asianomaisten henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla. Kyseinen direktiivi ei niinkään ole esteenä tällaisille toimenpiteille, joissa säädetään viestinnän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksetta tapahtuvasta säilyttämisestä, siltä osin kuin säilytysaika on rajoitettu täysin välttämättömään, eikä toimenpiteille, joissa säädetään sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen tällaisesta säilyttämisestä, ja jäsenvaltioiden ei viimeksi mainitussa tapauksessa tarvitse rajoittaa säilyttämistä ajallisesti. Mainittu direktiivi ei myöskään ole esteenä lainsäädännölliselle toimenpiteelle, jossa sallitaan palveluntarjoajien käytössä olevien tietojen säilyttämisen nopea varmistaminen silloin, kun syntyy tilanteita, joissa on välttämätöntä säilyttää mainitut tiedot lakisääteisten säilytysaikojen päättymisen jälkeen vakavien rikosten tai kansalliseen turvallisuuteen kohdistuvien loukkausten selvittämiseksi, kun nämä rikokset tai loukkaukset on jo todettu tai kun niiden olemassaoloa voidaan kohtuudella epäillä.

Unionin tuomioistuin totesi lisäksi, että direktiivi 2002/58, luettuna perusoikeuskirjan valossa, ei ole esteenä kansalliselle säännöstölle, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on kerättävä reaaliajassa muun muassa liikenne- ja paikkatietoja, kun tämä kerääminen on rajattu henkilöihin, joiden osalta on olemassa pätevä syy epäillä, että he osallistuvat tavalla tai toisella terrorismiin, ja keräämiseen kohdistuu joko tuomioistuimen tai sellaisen riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, suorittama etukäteisvalvonta, jolla varmistetaan, että tällainen tietojen kerääminen reaaliajassa sallitaan ainoastaan täysin välttämättömän rajoissa. Kiireellisessä tapauksessa valvonta on suoritettava viipymättä.

Unionin tuomioistuin tarkasteli lopuksi kysymystä unionin oikeuden vastaiseksi todetun kansallisen säännösten ajallisten vaikutusten pysyttämisestä. Se katsoi tältä osin, että kansallinen tuomioistuin ei voi soveltaa kansallisen oikeutensa säännöstä, jossa sille annetaan toimivalta rajoittaa ajallisesti sellaisen lainvastaisuutta koskevan toteamuksen vaikutuksia, joka sen on kyseisen oikeuden nojalla tehtävä kansallisesta lainsäädännöstä, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä direktiivin 2002/58, luettuna perusoikeuskirjan valossa, vastaisesti liikenne- ja paikkatietoja yleisesti ja erotuksetta.

Jotta kansalliselle tuomioistuimelle voidaan antaa hyödyllinen vastaus, unionin tuomioistuin huomautti tämän jälkeen, että sellaisten todisteiden hyväksyttävyyden arviointi, jotka on hankittu unionin oikeuden vastaisella tietojen säilyttämisellä, rikosprosessissa, joka on pantu vireille vakavista rikoksista epäiltyjä henkilöitä vastaan, kuuluu unionin oikeuden nykytilassa yksinomaan kansallisen oikeuden soveltamisalaan. Unionin tuomioistuin täsmensi kuitenkin, että sähköisen viestinnän tietosuojadirektiivissä, tulkittuna tehokkuusperiaatteen valossa, edellytetään, että kansallinen rikostuomioistuin jättää tällaisessa rikosprosessissa huomiotta todisteet, jotka on hankittu unionin oikeuden vastaisella liikenne- ja paikkatietojen yleisesti ja erotuksetta tapahtuvalla säilyttämisellä, jos rikoksista epäillyt henkilöt eivät voi tehokkaasti ilmaista käsitystään näistä todisteista

Tuomio 2.3.2021 (suuri jaosto), Prokuratuur (Sähköiseen viestintään liittyvien tietojen saannin edellytykset) (C-746/18, [EU:C:2021:152](#))

Virossa käynnistettiin H. K:ta vastaan rikosprosessi, jossa häntä syytettiin varkaudesta, toiselle kuuluvan pankkikortin käyttämisestä ja oikeudenkäyntiin osallistuviin henkilöihin kohdistuvasta väkivallasta. Alioikeus määräsi H. K:lle näistä rikoksista kahden vuoden vankeusrangaistuksen. Kyseinen päätös vahvistettiin sittemmin muutoksenhakuasteessa. Pöytäkirjat, joiden perusteella näitä rikoksia koskeva syyllisyys todettiin, laadittiin muun muassa sähköisten viestintäpalvelujen tarjoamisen yhteydessä luotujen henkilötietojen perusteella. Riigikohus (ylin tuomioistuin, Viro), johon H. K. teki kassaatiovalituksen, epäili niiden edellytysten, joilla tutkintaviranomaiset ovat saaneet näitä tietoja, yhteensopivuutta unionin oikeuden kanssa.⁴⁹

Nämä epäilykset koskivat ensiksi sitä, onko sen ajanjakson pituus, jolta tutkintaviranomaiset ovat saaneet tietoja, kriteeri, jonka perusteella voidaan arvioida kyseisten tietojen saannin muodostaman asianomaisten henkilöiden perusoikeuksiin puuttumisen vakavuutta. Jos siis mainittu ajanjakso on hyvin lyhyt tai saatujen tietojen määrä on hyvin vähäinen, ennakkoratkaisua pyytänyt tuomioistuin tiedustele, voidaanko tällainen puuttuminen oikeuttaa rikollisuuden torjunnalla yleisesti eikä yksinomaan vakavan rikollisuuden torjunnalla. Toiseksi ennakkoratkaisua pyytäneellä tuomioistuimella oli epäilyksiä siitä, voidaanko Viron syyttävaviranomaista, kun otetaan huomioon sille kansallisen lainsäädännön nojalla kuuluvat erilaiset tehtävät, pitää tuomiossa Tele2 Sverige ja Watson ym.⁵⁰ tarkoitettuna riippumattomana hallintoviranomaisena, joka voi antaa tutkintaviranomaiselle luvan saada kyseessä olevia tietoja.

Unionin tuomioistuin totesi suuressa jaostossa antamassaan tuomiossa, että direktiiviä 2002/58, kun sitä luetaan perusoikeuskirjan valossa, on tulkittava siten, että se on

⁴⁹ Tarkemmin ottaen direktiivin 2002/58 15 artiklan 1 kohdan kanssa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä perusoikeuskirjan 52 artiklan 1 kohdan valossa.

⁵⁰ Tuomio 21.12.2016, Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, [EU:C:2016:970](#), 120 kohta).

esteenä kansalliselle säännöstölle, jossa annetaan viranomaisille oikeus saada sellaisia liikenne- ja paikkatietoja, jotka ovat omiaan antamaan tietoja sähköisen viestintävälineen käyttäjän harjoittamasta viestinnästä tai tämän käyttämien päätelaitteiden sijainnista ja joista voidaan tehdä täsmällisiä tämän yksityiselämää koskevia päätelmiä, rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa varten ilman, että kyseinen tietojen saanti rajoitetaan koskemaan vain menettelyjä, joilla pyritään torjumaan vakavaa rikollisuutta tai ehkäisemään yleiseen turvallisuuteen kohdistuvia vakavia uhkia. Unionin tuomioistuimen mukaan tämä ei riipu sen ajanjakson pituudesta, jolta mainittujen tietojen saantia pyydetään, eikä tällaiselta ajanjaksolta saatavilla olevien tietojen määrästä tai luonteesta. Unionin tuomioistuin katsoi lisäksi, että sama direktiivi, kun sitä luetaan perusoikeuskirjan valossa, on esteenä kansalliselle säännöstölle, jossa annetaan syyttäjäviranomaiselle toimivalta myöntää viranomaiselle lupa liikenne- ja paikkatietojen saantiin rikostutkintaa varten.

Siltä osin kuin on kyse pääasiassa kyseessä olevalla säännöstöllä tavoitellusta rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa koskevasta tavoitteesta, unionin tuomioistuin toteaa, että ainoastaan vakavan rikollisuuden torjuminen ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen voivat suhteellisuusperiaatteen mukaisesti oikeuttaa sen, että viranomaiset saavat oikeuden saada joukon liikenne- ja paikkatietoja, joista voidaan tehdä täsmällisiä asianomaisten henkilöiden yksityiselämää koskevia päätelmiä ilman, että muista tietojen saantia koskevan pyynnön oikeasuhtaisuutta koskevista tekijöistä, kuten sen ajanjakson pituudesta, jolta tällaisten tietojen saantia pyydetään, voisi seurata, että tällainen tietojen saanti voidaan oikeuttaa rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella.

Siltä osin kuin kyse on syyttäjäviranomaisen toimivallasta myöntää viranomaiselle lupa saada liikenne- ja paikkatietoja rikostutkintaa varten, unionin tuomioistuin muistutti, että niiden edellytysten, joiden nojalla sähköisten viestintäpalvelujen tarjoajien on annettava toimivaltaisille kansallisille viranomaisille oikeus saada hallussaan olevia tietoja, määrittäminen kuuluu kansallisen oikeuden alaan. Oikeasuhteisuutta koskevan edellytyksen täyttämiseksi tällaisessa säännöstössä on joka tapauksessa säädettävä selvistä ja täsmällisistä asianomaisten toimenpiteen laajuutta ja soveltamista koskevista säännöistä, joissa asetetaan vähimmäisvaatimukset, jotta henkilöillä, joiden henkilötiedoista on kyse, on riittävät takeet, joiden avulla heidän henkilötietojaan voidaan tehokkaasti suojata väärinkäytön vaaroilta. Kyseisen säännösten on oltava kansallisen oikeuden mukaan laillisesti sitova, ja siinä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksin tällaisten tietojen käsittelyä koskeva toimenpide voidaan toteuttaa, jotta taataan, että puuttuminen rajoittuu täysin välttämättömään.

Unionin tuomioistuimen mukaan sen takaamiseksi, että näitä edellytyksiä noudatetaan käytännössä täysimääräisesti, on olennaista se, että toimivaltaisten kansallisten viranomaisten oikeus saada säilytetyjä tietoja edellyttää joko tuomioistuimen tai riippumattoman hallinnollisen elimen etukäteisvalvontaa ja sitä, että kyseisen

tuomioistuimen tai elimen ratkaisu annetaan perustellusta pyynnöstä, jonka nämä viranomaiset esittävät rikoksen estämis-, selvittämisen- tai syyteharkintamenettelyssä. Asianmukaisesti perustellussa kiireellisessä tapauksessa valvonta on suoritettava viipymättä.

Tältä osin unionin tuomioistuin täsmensi, että etukäteisvalvonta edellyttää muun muassa sitä, että mainitun valvonnan suorittamisesta vastaavalla tuomioistuimella tai elimellä on kaikki valtuudet ja kaikki takeet, jotka ovat välttämättömiä sen varmistamiseksi, että kyseessä olevat eri intressit ja oikeudet sovitetaan yhteen. Tarkemmin ottaen rikostutkinnan osalta tällainen valvonta edellyttää sitä, että kyseinen tuomioistuin tai elin pystyy turvaamaan oikeudenmukaisen tasapainon yhtäältä rikollisuuden torjumiseksi tehtävän tutkinnan tarpeisiin liittyvien intressien ja toisaalta henkilöiden, joita tietojensaanti koskee, yksityiselämän kunnioittamista ja henkilötietojen suojelua koskevien perusoikeuksien välillä. Siinä tapauksessa, että kyseisen valvonnan suorittaa tuomioistuimen sijaan riippumaton hallinnollinen elin, kyseisellä elimellä on oltava asema, jossa se voi suorittaa tehtävänsä objektiivisesti ja puolueettomasti, ja sen on tätä varten oltava suojattu kaikelta ulkopuoliselta vaikuttamiselta.

Unionin tuomioistuimen mukaan riippumattomuutta koskeva vaatimus, joka etukäteisvalvonnasta vastaavan viranomaisen on täytettävä, edellyttää sitä, että kyseinen viranomainen on ulkopuolinen siihen viranomaiseen nähden, joka pyytää kyseisten tietojen saantia, jotta ensiksi mainittu voi suorittaa kyseisen valvonnan objektiivisesti ja puolueettomasti suojattuna kaikelta ulkopuoliselta vaikuttamiselta. Erityisesti rikosasioissa riippumattomuuden vaatimus tarkoittaa, että tästä etukäteisvalvonnasta vastaava viranomainen ei yhtäältä osallistu kyseisen rikostutkinnan suorittamiseen ja toisaalta on neutraalissa asemassa rikosprosessin asianosaisiin nähden. Asia ei ole näin syyttäväviranomaisen, joka Viron syyttäväviranomaisen tapaan johtaa tutkintamenettelyä ja tarvittaessa ajaa virallista syytettä, kohdalla. Tästä seuraa, että syyttäväviranomainen ei voi suorittaa edellä mainittua etukäteisvalvontaa

Tuomio 5.4.2022 (suuri jaosto), Commissioner of An Garda Síochána ym. (C-140/20, [EU:C:2022:258](#))

Kyseisessä asiassa Supreme Court (ylin tuomioistuin, Irlanti) oli esittänyt ennakkoratkaisupyynnön siviilioikeudellisessa menettelyssä, jonka oli pannut vireille henkilö, joka oli tuomittu elinkautiseen vankeusrangaistukseen Irlannissa tehdystä murhasta. Kyseinen henkilö katsoi, että eräät sähköisen viestinnän yhteydessä syntyvien tietojen säilyttämistä koskevat kansallisen lain säännökset ovat yhteensopimattomia unionin oikeuden kanssa. Sähköisten viestintäpalvelujen tarjoajat olivat tämän lain nojalla säilyttäneet kyseisen rikoksesta tuomitun henkilön puheluiden liikenne- ja paikkatiedot ja antaneet ne poliisiin käyttöön. Ennakkoratkaisua pyytänyt tuomioistuin oli epävarma erityisesti siitä, onko näiden tietojen yleistä ja erotuksetta tapahtuvaa

säilyttämistä koskeva järjestelmä vakavan rikollisuuden torjunnan yhteydessä sähköisen viestinnän tietosuojadirektiivin, luettuna perusoikeuskirjan valossa, mukainen.

Unionin tuomioistuimen suuri jaosto vahvisti tuomioon *La Quadrature du Net* ym.⁵¹ perustuvan oikeuskäytännön ja täsmensi samalla sen ulottuvuutta muistuttaen, että sähköiseen viestintään liittyvien liikenne- ja paikkatietojen yleinen ja erotuksetta tapahtuva säilyttäminen ei ole sallittua vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien estämiseksi. Unionin tuomioistuin vahvisti myös tuomioon *Prokuratuur* (Sähköiseen viestintään liittyvien tietojen saannin edellytykset)⁵² perustuvan oikeuskäytännön erityisesti siltä osin kuin kyse on velvollisuudesta asettaa sen edellytykseksi, että toimivaltaiset kansalliset viranomaiset saavat mainittuja tietoja, ennakkovalvonnan, jonka suorittaa joko tuomioistuin tai hallintoelin, joka on riippumaton poliisivirkamieheen nähden.

Unionin tuomioistuin totesi ensinnäkin, että sähköisen viestinnän tietosuojadirektiivi, luettuna perusoikeuskirjan valossa, on esteenä lainsäädännöllisille toimenpiteille, joissa säädetään ennalta ehkäisevästi liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta tietojen säilyttämisestä vakavan rikollisuuden torjumiseksi ja yleistä turvallisuutta koskevien vakavien uhkien ehkäisemiseksi. Kun nimittäin otetaan huomioon yhtäältä, että näiden tietojen säilyttäminen voi vaikuttaa ehkäisevästi perusoikeuksien⁵³ käyttöön ja toisaalta, että tällaisesta säilyttämisestä johtuva puuttuminen on vakavaa, tämän säilyttämisen on oltava poikkeus eikä sääntö tällä direktiivillä käyttöön otetussa järjestelmässä, niin että näitä tietoja ei voida säilyttää järjestelmällisesti ja jatkuvasti. Rikollisuutta, vaikka se olisi erityisen vakavaa, ei voida rinnastaa kansallista turvallisuutta koskevaan uhkaan, koska tällainen rinnastaminen voisi merkitä uuden väliluokan käyttöön ottamista kansallisen turvallisuuden ja yleisen turvallisuuden välille, jotta ensin mainittuun liittyviä vaatimuksia voitaisiin soveltaa viimeksi mainittuun.

Sähköisen viestinnän tietosuojadirektiivi, luettuna perusoikeuskirjan valossa, ei sen sijaan ole esteenä lainsäädännöllisille toimenpiteille, joissa säädetään vakavan rikollisuuden torjumiseksi ja yleistä turvallisuutta koskevien vakavien uhkien ehkäisemiseksi liikenne- ja paikkatietojen kohdennetusta säilyttämisestä, joka on objektiivisten ja syrjimättömien seikkojen perusteella rajattu rekisteröityjen muodostamien ryhmien mukaan tai maantieteellisen kriteerin avulla ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa. Unionin tuomioistuin totesi lisäksi, että tällaisella säilyttämistoimenpiteellä, joka koskee paikkoja tai infrastruktuureja, joissa käy säännöllisesti suuri määrä ihmisiä, tai strategisia paikkoja, kuten lentoasemia, rautatieasemia, merisatamia tai tietuallalueita, annetaan toimivaltaisille viranomaisille mahdollisuus kerätä tietoja sellaisten henkilöiden

⁵¹ Tuomio 6.10.2020, *La Quadrature du Net* ym. (C-511/18, C-512/18 ja C-520/18, [EU:C:2020:791](#)).

⁵² Tuomio 2.3.2021, *Prokuratuur* (Sähköiseen viestintään liittyvien tietojen saannin edellytykset) (C-746/18, [EU:C:2021:152](#)).

⁵³ Perusoikeuskirjan 7–11 artiklassa vahvistetut perusoikeudet.

läsnäolosta näillä paikoilla tai maantieteellisillä alueilla, jotka käyttävät siellä sähköistä viestintävälinettä, ja tehdä niistä vakavan rikollisuuden torjumiseksi päätelmiä heidän läsnäolostaan ja toiminnastaan näillä paikoilla tai maantieteellisillä alueilla. Joka tapauksessa se, että on mahdollisesti vaikea määrittää tarkasti niitä tilanteita ja edellytyksiä, joiden toteutuessa kohdennettu säilyttäminen voidaan toteuttaa, ei voi oikeuttaa jäsenvaltioita muuttamaan poikkeusta säännöksi siten, että ne säätävät liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä.

Kyseinen direktiivi, luettuna perusoikeuskirjan valossa, ei myöskään ole esteenä lainsäädännöllisille toimenpiteille, joissa säädetään liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksetta tapahtuvasta säilyttämisestä ajanjaksoksi, joka on rajattu täysin välttämättömään, ja sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä. Unionin tuomioistuinin totesi viimeksi mainitun seikan osalta erityisesti, ettei sähköisen viestinnän tietosuojadirektiivi eikä mikään muukaan unionin oikeuden toimi ole esteenä kansalliselle lainsäädännölle, jonka tavoitteena on vakavan rikollisuuden torjunta ja jonka nojalla etukäteen maksetun SIM-kortin kaltaisen sähköisen viestintävälineen hankinta edellyttää sellaisten virallisten asiakirjojen tarkistamista, jotka osoittavat ostajan henkilöllisyyden, ja sitä, että myyjä rekisteröi tästä saadut tiedot, ja myyjällä on tarvittaessa velvollisuus antaa nämä tiedot toimivaltaisille kansallisille viranomaisille.

Toisin ei ole sellaisten lainsäädännöllisten toimenpiteiden osalta, joissa edelleen vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi säädetään siitä, että sähköisten viestintäpalvelujen tarjoajat määrätään toimivaltaisen viranomaisen päätöksellä, johon kohdistuu tehokas tuomioistuinvalvonta, varmistamaan nopeasti (quick freeze) kyseisten palveluntarjoajien käytössä olevien liikenne- ja paikkatietojen säilyttäminen tietyn ajan. Ainoastaan vakavan rikollisuuden torjunta ja varsinkin kansallisen turvallisuuden takaaminen voivat näet oikeuttaa tällaisen säilyttämisen, sillä edellytyksellä, että tämä toimenpide ja näin säilytettyjen tietojen saanti tapahtuvat täysin välttämättömän rajoissa. Unionin tuomioistuin muistutti, että tällainen säilyttämisen nopea varmistaminen voidaan ulottaa koskemaan muihin kuin sellaisiin henkilöihin liittyviä liikenne- ja paikkatietoja, joiden epäillään suunnitelleen vakavaa rikosta tai kansalliseen turvallisuuteen kohdistuvaa loukkausta taikka syyllistyneen tällaiseen rikokseen tai loukkaukseen, siltä osin kuin kyseisillä tiedoilla voidaan objektiivisten ja syrjimättömien seikkojen perusteella myötävaikuttaa tällaisen rikoksen tai tällaisen kansalliseen turvallisuuteen kohdistuvan loukkauksen selvittämiseen; tällaisia tietoja ovat esimerkiksi rikoksen uhria ja hänen sosiaalista tai ammatillista lähipiiriään koskevat tiedot.

Unionin tuomioistuin totesi kuitenkin, että kaikissa edellä mainituissa toimenpiteissä on varmistettava selvin ja täsmällisin säännöin, että kyseessä olevien tietojen säilyttämisen ehtona on, että näihin toimenpiteisiin liittyviä aineellisia ja menettelyllisiä edellytyksiä noudatetaan, ja että asianomaisilla henkilöillä on tehokkaat takeet väärinkäytön vaaroja

vastaan. Eri liikenne- ja paikkatietojen säilyttämistoimenpiteitä voidaan soveltaa yhdessä kansallisen lainsäätäjän valinnan mukaan ja täysin välttämättömän rajoissa.

Unionin tuomioistuin täsmensi lisäksi, että vakavan rikollisuuden torjumiseksi tällaisten yleisesti ja erotuksetta säilytettyjen tietojen saannin salliminen todelliseen ja olemassa olevaan tai ennakoitavissa olevaan kansallista turvallisuutta koskevaan uhkaan vastaamiseksi olisi niiden yleisen edun mukaisten tavoitteiden hierarkian vastaista, joilla voidaan oikeuttaa sähköisten viestinnän tietosuojadirektiivin nojalla toteutettava toimenpide. Tämä merkitsisi nimittäin sen sallimista, että tietojen saanti voitaisiin oikeuttaa tavoitteella, joka on tavoitteiden hierarkiassa alempana kuin se, joka oikeutti säilyttämisen, eli kansallisen turvallisuuden suojaaminen, jolloin vaarana siis olisi, että vietäisiin kaikki tehokas vaikutus kielloilta, joka koskee yleistä ja erotuksetta tapahtuvaa tietojen säilyttämistä vakavan rikollisuuden torjumiseksi.

Toiseksi unionin tuomioistuin totesi, että sähköisen viestinnän tietosuojadirektiivi, luettuna perusoikeuskirjan valossa, on esteenä kansalliselle lainsäädännölle, jonka nojalla poliisin vakavien rikosten tutkinnan ja syytetoimien yhteydessä esittämien, sähköisten viestintäpalvelujen tarjoajien säilyttämien tietojen saantia koskevien pyyntöjen keskitetty käsittely kuuluu poliisivirkamiehelle, myös silloin, kun häntä avustaa poliisin sisäinen yksikkö, jolla on tietty itsenäisyys tehtävänsä suorittaessaan, ja jonka päätökset voivat myöhemmin olla tuomioistuinvalvonnan kohteena. Tällainen virkamies ei nimittäin yhtäältä täytä riippumattomuutta ja puolueettomuutta koskevia vaatimuksia, joita sovelletaan hallintoviranomaiseen, joka valvoo etukäteen toimivaltaisten kansallisten viranomaisten esittämiä pyyntöjä saada tutustua tietoihin, koska hän ei ole ulkopuolinen näihin viranomaisiin nähden. Toisaalta on niin, että vaikka tällaisen virkamiehen päätökseen voidaan kohdistaa tuomioistuinvalvontaa jälkikäteen, tällä jälkikäteisellä valvonnalla ei voida korvata vaatimusta riippumattomasta valvonnasta ja, jollei kyse ole asianmukaisesti perustellusta kiireellisestä tapauksesta, etukäteisvalvonnasta.

Kolmanneksi unionin tuomioistuin vahvisti lopuksi oikeuskäytäntönsä, jonka mukaan unionin oikeus on esteenä sille, että kansallinen tuomioistuin rajoittaa ajallisesti sellaisen pätemättömyyttä koskevan toteamuksen vaikutuksia, joka sen on kansallisen oikeuden nojalla tehtävä kansallisesta lainsäädännöstä, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä liikenne- ja paikkatiedot yleisesti ja erotuksetta, sen vuoksi, että tämä lainsäädäntö ei ole yhteensopiva sähköisen viestinnän tietosuojadirektiivin kanssa. Unionin tuomioistuin muistutti kuitenkin, että tällaisen säilyttämisen avulla saatujen todisteiden hyväksyttävyyys kuuluu jäsenvaltioiden menettelyllisen itsemääräämisoikeuden periaatteen mukaisesti kansallisen oikeuden alaan, edellyttäen, että erityisesti vastaavuus- ja tehokkuusperiaatteita noudatetaan.

Tuomio 20.9.2022 (suuri jaosto), VD ja SR (C-339/20 ja C-397/20, [EU:C:2022:703](#))

Ranskan rahoitusmarkkinaviranomaisen (Autorité des marchés financiers (AMF)) suorittaman tutkinnan jälkeen VD:tä ja SR:ää, jotka ovat luonnollisia henkilöitä, vastaan käynnistettiin rikosoikeudelliset menettelyt, jotka koskivat sisäpiiritiedon väärinkäyttöä, kätkemisrikosta, avunantoa, lahjontaa ja rahanpesua. AMF käytti tutkinnassaan VD:n ja SR:n soittamiin puheluihin perustuvia henkilötietoja, jotka oli saatu postista ja sähköisestä viestinnästä annetun koodeksin (code des postes et des communications électroniques) nojalla tarjottaessa sähköisiä viestintäpalveluja.

Koska tutkinnat perustuivat AMF:n toimittamiin tietoliikennetietoihin, VD ja SR nostivat kumpikin kanteen cour d'appel de Paris'ssa (Pariisin ylioikeus, Ranska) ja vetosivat muun muassa kanneperusteeseen, joka perustui pääasiallisesti direktiivin 2002/58 15 artiklan 1 kohdan, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, rikkomiseen. Tukeutuen tuomioon Tele2 Sverige ja Watson ym.⁵⁴ perustuvaan oikeuskäytäntöön VD ja SR riitauttivat erityisesti sen, että AMF perusti tietojen keräämisen kyseessä oleviin kansallisiin säännöksiin, vaikka nämä säännökset eivät heidän mukaansa ensinnäkään olleet unionin oikeuden mukaisia siltä osin kuin niissä säädettiin yhteystietojen yleisesti ja erotuksetta tapahtuvasta säilyttämisestä ja vaikka kyseisissä säännöksissä ei toiseksi rajoitettu AMF:n tutkijoiden valtuuksia vaatia säilytettyjä tietoja.

Cour d'appel de Paris hylkäsi VD:n ja SR:n kanteet 20.12.2018 ja 7.3.2019 antamillaan tuomioilla. Hylätessään edellä mainitun kanneperusteen asiakysymystä käsitelleet tuomioistuimet tukeutuivat muun muassa siihen, että markkinoiden väärinkäyttöasetuksessa⁵⁵ sallitaan se, että toimivaltaiset viranomaiset vaativat kansallisen lainsäädännön sallimissa puitteissa sähköisten viestintäpalvelujen tarjoajien hallussa olevia tietoliikennetietoja, jos voidaan perustellusti epäillä sisäpiirikauppoja koskevan kiellon rikkomista ja jos näillä tiedoilla saattaa olla merkitystä tutkittaessa tällaista rikkomista.

VD ja SR valittivat näistä tuomioista Cour de cassationiin (ylin tuomioistuin, Ranska), joka on pääasioissa ennakkoratkaisua pyytänyt tuomioistuin.

Tässä yhteydessä ennakkoratkaisua pyytänyt tuomioistuin pohti sitä, miten sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohta, luettuna perusoikeuskirjan valossa, sopii yhteen markkinoiden väärinkäyttödirektiivin⁵⁶ 12 artiklan 2 kohdan a ja d alakohdasta ja markkinoiden väärinkäyttöasetuksen 23 artiklan 2 kohdan g ja h alakohdasta ilmenevien vaatimusten kanssa. Tämän kysymyksen taustalla ovat pääasiassa kyseessä olevat lainsäädäntötoimenpiteet, joiden mukaan sähköisten

⁵⁴ Tuomio 21.12.2016, Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, [EU:C:2016:970](#)).

⁵⁵ Euroopan parlamentin ja neuvoston direktiivin 2003/6/EY ja komission direktiivien 2003/124/EY, 2003/125/EY ja 2004/72/EY kumoamisesta 16.4.2014 annettu Euroopan parlamentin ja neuvoston asetusta (EU) N:o 596/2014 (EUVL 2014, L 173, s. 1).

⁵⁶ Sisäpiirikaupoista ja markkinoiden manipuloinnista (markkinoiden väärinkäyttö) 28.1.2003 annettu Euroopan parlamentin ja neuvoston direktiivi 2003/6/EY (EUVL 2003, L 96, s. 16).

viestintäpalvelujen tarjoajien on säilytettävä ennaltaehkäisevästi markkinoiden väärinkäyttöön liittyvien rikosten, joihin sisäpiirikaupat kuuluvat, torjumiseksi tietoliikennetietoja yleisesti ja erotuksetta vuoden ajan niiden tallennuspäivästä. Sitä tapausta varten, että unionin tuomioistuimien katsoisi, että pääasioissa kyseessä oleva yhteystietojen säilyttämistä koskeva lainsäädäntö ei ole unionin oikeuden mukainen, ennakkoratkaisua pyytänyt tuomioistuin esittää kysymyksen kyseisen lainsäädännön vaikutusten väliaikaisesta voimassa pitämisestä, jotta vältettäisiin oikeudellinen epävarmuus ja jotta aiemmin kerättyjä ja säilytettyjä tietoja voitaisiin käyttää sisäpiirikauppojen selvittämiseen ja syyteharkintaan.

Unionin tuomioistuimen suuri jaosto totesi tuomiossaan, että se, että sähköisten viestintäpalvelujen tarjoajat veloitetaan ennaltaehkäisevästi markkinoiden väärinkäyttöön liittyvien rikosten, joihin sisäpiirikaupat kuuluvat, torjumiseksi säilyttämään tietoliikennetietoja yleisesti ja erotuksetta vuoden ajan niiden tallennuspäivästä, ei ole sallittua. Lisäksi unionin tuomioistuin vahvisti oikeuskäytännön, jonka mukaan unionin oikeus on esteenä sille, että kansallinen tuomioistuin rajoittaa ajallisesti sellaisen pätemättömyyttä koskevan toteamuksen vaikutuksia, joka koskee unionin oikeuden kanssa ristiriidassa olevia kansallisia säännöksiä.

Unionin tuomioistuin muistutti aluksi, että unionin oikeuden säännöksen tulkitsemiseksi on otettava huomioon sen sanamuodon lisäksi sen asiayhteys sekä sillä säännöstöllä tavoitellut päämäärät, jonka osa se on.

Unionin tuomioistuin totesi ennakkoratkaisukysymyksissä tarkoitettujen säännösten sanamuodosta, että markkinoiden väärinkäyttödirektiivin 12 artiklan 2 kohdan d alakohdassa viitataan AMF:n valtuuksiin "vaatia olemassa olevia tallenteita puheluista ja tietoliikenteestä", kun taas markkinoiden väärinkäyttöasetuksen 23 artiklan 2 kohdan g ja h alakohdassa viitataan kyseisen viranomaisen valtuuksiin yhtäältä pyytää "sijoituspalveluyritysten, luottolaitosten tai rahoituslaitosten hallussa olevia – tietoliikennetietoja" ja toisaalta vaatia "kansallisen lainsäädännön sallimissa puitteissa televiestintäoperaattorin hallussa olevia tietoliikennetietoja". Unionin tuomioistuimen mukaan näiden säännösten sanamuodosta ilmenee yksiselitteisesti, että niissä vain rajoitetaan AMF:n valtuuksia "vaatia" tai "pyytää" kyseisten operaattoreiden hallussa olevia tietoja, mikä vastaa näiden tietojen saantia. Lisäksi viittaus "olemassa oleviin" tallenteisiin, kuten ne, jotka ovat kyseisten operaattoreiden "hallussa", antaa ymmärtää, että unionin lainsäätäjän tarkoituksena ei ole ollut säännellä kansallisen lainsäätäjän mahdollisuutta asettaa tällaisille tiedoille säilyttämisvelvollisuutta. Unionin tuomioistuimen mukaan tätä tulkintaa tukevat sen säännöstön asiayhteys ja sillä säännöstöllä tavoitellut päämäärät, joiden osa kyseiset säännökset ovat.

Unionin tuomioistuin huomautti asiayhteydestä, johon ennakkoratkaisukysymyksissä tarkoitetut säännökset kuuluvat, että vaikka markkinoiden väärinkäyttödirektiivin ja

markkinoiden väärinkäyttöasetuksen merkityksellisten säännösten⁵⁷ mukaan on niin, että unionin lainsäätäjän tarkoituksena on ollut velvoittaa jäsenvaltiot toteuttamaan tarvittavat toimenpiteet sen varmistamiseksi, että rahoitusalan toimivaltaisilla viranomaisilla on tehokkaat keinot, valtuudet ja resurssit sekä kaikki tehtäviensä tehokkaan hoitamisen edellyttämät valvonta- ja tutkintavaltuudet, kyseisissä säännöksissä ei kuitenkaan säädetä jäsenvaltioiden mahdollisuudesta ottaa käyttöön tätä tarkoitusta varten sähköisten viestintäpalvelujen tarjoajille asetettua velvollisuutta säilyttää tietoliikennetietoja yleisesti ja erotuksetta eikä sellaisista edellytyksistä, joiden täyttyessä kyseisten operaattoreiden on säilytettävä nämä tiedot toimittaakseen ne tarvittaessa toimivaltaisille viranomaisille.

Kyseessä olevan säännösten päämääristä unionin tuomioistuin huomautti, että markkinoiden väärinkäyttödirektiivistä ja markkinoiden väärinkäyttöasetuksesta⁵⁸ ilmenee, että näiden säädösten tarkoituksena on varmistaa unionin rahoitusmarkkinoiden luotettavuus ja lujittaa sijoittajien luottamusta kyseisiin markkinoihin, johon vaikuttaa muun muassa se seikka, että sijoittajia kohdellaan yhdenvertaisesti ja suojataan sisäpiiritiedon väärinkäytöltä. Kyseisissä säädöksissä⁵⁹ säädetyn sisäpiirikauppojen kiellon tarkoituksena on siten taata, että tietyn pörssissä tehtävän kaupan osapuolia kohdellaan yhdenvertaisesti, estämällä se, että sellainen osapuoli, jolla on hallussaan sisäpiiritietoa ja joka näin ollen on edullisemmassa asemassa muihin sijoittajiin nähden, hyötyy kyseisestä tiedosta sellaisten henkilöiden vahingoksi, joilla tätä tietoa ei ole. Vaikka markkinoiden väärinkäyttöasetuksen⁶⁰ mukaan yhteystiedot ovat ratkaisevan tärkeitä ja toisinaan ainoita todisteita, joiden avulla sisäpiirikaupat ja markkinoiden manipulointi voidaan havaita ja todistaa, tässä perustelukappaleessa viitataan kuitenkin vain sähköisten viestintäpalvelujen tarjoajien ”hallussa oleviin” tietoihin sekä rahoitusalan toimivaltaisen viranomaisen oikeuteen ”vaatia” kyseisiltä operaattoreilta ”olemassa olevia” tietoja. Kyseisestä tekstistä ei siis mitenkään ilmene, että unionin lainsäätäjän tarkoituksena olisi ollut tällä asetuksella antaa jäsenvaltioille toimivalta asettaa sähköisten viestintäpalvelujen tarjoajille yleinen tietojensäilyttämisvelvollisuus. Tästä seuraa, että markkinoiden väärinkäyttödirektiivi ja markkinoiden väärinkäyttöasetus eivät voi muodostaa oikeusperustaa sähköisten viestintäpalvelujen tarjoajien hallussa olevien tietoliikennetietojen yleiselle säilyttämisvelvollisuudelle rahoitusalan toimivaltaiselle viranomaiselle kyseisten säädösten nojalla annettujen valtuuksien käyttämiseksi.

Tämän jälkeen unionin tuomioistuin muistutti, että sähköisen viestinnän tietosuoja-direktiivi on perussäädös silloin, kun on kyse henkilötietojen säilyttämisestä ja yleisemmin niiden käsittelystä sähköisen viestinnän alalla, joten unionin tuomioistuimen

⁵⁷ Markkinoiden väärinkäyttödirektiivin 12 artiklan 1 kohta ja markkinoiden väärinkäyttöasetuksen 23 artiklan 3 kohta, luettuna yhdessä asetuksen 62 perustelukappaleen kanssa.

⁵⁸ Markkinoiden väärinkäyttödirektiivin 2 ja 12 perustelukappale ja markkinoiden väärinkäyttöasetuksen 1 artikla, luettuna yhdessä asetuksen 2 ja 24 perustelukappaleen kanssa.

⁵⁹ Markkinoiden väärinkäyttödirektiivin 2 artiklan 1 kohta ja markkinoiden väärinkäyttöasetuksen 8 artiklan 1 kohta.

⁶⁰ Markkinoiden väärinkäyttöasetuksen 62 perustelukappale.

kyseisestä direktiivistä tekemä tulkinta koskee myös sähköisten viestintäpalvelujen tarjoajien hallussa olevia tietoliikennetietoja, joita markkinoiden väärinkäyttödirektiivissä ja markkinoiden väärinkäyttöasetuksessa⁶¹ tarkoitetut rahoitusalan toimivaltaiset viranomaiset voivat niiltä pyytää. Sähköisten viestintäpalvelujen tarjoajien hallussa olevien tallenteiden⁶² käsittelyn laillisuutta on siten arvioitava sähköisen viestinnän tietosuojadirektiivissä säädettyjen edellytysten ja unionin tuomioistuimen kyseisestä direktiivistä tekemän tulkinnan valossa.

Näin ollen unionin tuomioistuin totesi, että markkinoiden väärinkäyttödirektiivi ja markkinoiden väärinkäyttöasetus, luettuina yhdessä sähköisen viestinnän tietosuojadirektiivin kanssa ja perusoikeuskirjan valossa, ovat esteenä lainsäädäntötoimenpiteille, joiden mukaan sähköisten viestintäpalvelujen tarjoajien on ennaltaehkäisevästi markkinoiden väärinkäyttöön liittyvien rikosten, joihin sisäpiirikaupat kuuluvat, torjumiseksi säilytettävä tietoliikennetietoja rajoitetun ajan, eli vuoden ajan niiden tallennuspäivästä, mutta yleisesti ja erotuksetta.

Lopuksi unionin tuomioistuin vahvisti oikeuskäytännön, jonka mukaan unionin oikeus on esteenä sille, että kansallinen tuomioistuin rajoittaa ajallisesti sellaisen pätemättömyyttä koskevan toteamuksen vaikutuksia, joka sen on tehtävä kansallisen oikeuden nojalla sellaisten kansallisen säännösten osalta, joiden mukaan sähköisten viestintäpalvelujen tarjoajien on yhtäältä säilytettävä tietoliikennetietoja yleisesti ja erotuksetta ja joissa toisaalta sallitaan tällaisten tietojen toimittaminen rahoitusalan toimivaltaiselle viranomaiselle edellyttämättä tuomioistuimen tai riippumattoman hallintoviranomaisen ennakkolupaa, sen vuoksi, että kyseiset säännökset ovat ristiriidassa sähköisen viestinnän tietosuojadirektiivin, luettuna perusoikeuskirjan valossa, kanssa. Unionin tuomioistuin muistutti kuitenkin, että tällaisen säilyttämisen avulla saatujen todisteiden hyväksyttävyyys kuuluu jäsenvaltioiden menettelyllisen itsemääräämisoikeuden periaatteen mukaisesti kansallisen oikeuden alaan, edellyttäen, että erityisesti vastaavuus- ja tehokkuusperiaatteita noudatetaan. Tehokkuusperiaate velvoittaa kansallisen rikostuomioistuimen jättämään huomiotta tiedot ja todisteet, jotka on hankittu unionin oikeuden vastaisella tietojen yleisesti ja erotuksetta tapahtuvalla säilyttämisellä, jos kyseiset henkilöt eivät voi tehokkaasti ilmaista käsitystään näistä tiedoista ja todisteista, jotka ovat peräisin alalta, jota tuomarit eivät tunne, ja jotka voivat vaikuttaa ratkaisevalla tavalla tosiseikkojen arviointiin.

Tuomio 30.4.2024 (täysistunto), La Quadrature du Net ym. (Henkilötiedot ja oikeudenloukkausten torjuminen) (C-470/21, [EU:C:2024:370](#))

Unionin tuomioistuin, jolle Conseil d'État (ylin hallintotuomioistuin, Ranska) esitti ennakkoratkaisupyyntö, kehitti täysistunnossa direktiiviä 2002/58/EY koskevaa

⁶¹ Markkinoiden väärinkäyttödirektiivin 11 artikla ja markkinoiden väärinkäyttöasetuksen 22 artikla.

⁶² Markkinoiden väärinkäyttödirektiivin 12 artiklan 2 kohdan d alakohdassa ja markkinoiden väärinkäyttöasetuksen 23 artiklan 2 kohdan g ja h alakohdassa tarkoitetut tallenteet.

oikeuskäytäntöä esittämällä täsmennyksiä, jotka koskevat yhtäältä edellytyksiä, joiden täyttyessä sen, että sähköisten viestintäpalvelujen tarjoajat säilyttävät yleisesti IP-osoitteita, ei voida katsoa merkitsevän vakavaa puuttumista perusoikeuskirjassa⁶³ taattuihin yksityiselämän kunnioittamista, henkilötietojen suojaa ja sananvapautta koskeviin oikeuksiin, ja toisaalta viranomaisen mahdollisuutta saada pääsy tiettyihin henkilötietoihin, jotka säilytetään tällaisia edellytyksiä noudattaen, teollis- ja tekijänoikeuksien verkossa tapahtuvien loukkausten torjumisen yhteydessä.

Nyt käsiteltävässä asiassa neljä yhdistystä esitti pääministerille (Ranska) vaatimuksen henkilötietojen automaattisesta käsittelystä annetun asetuksen⁶⁴ kumoamisesta. Koska näin ei tapahtunut, nämä yhdistykset nostivat Conseil d'État'ssa kanteen, jossa ne vaativat tämän implisiittisen hylkäyspäätöksen kumoamista. Niiden mukaan kyseisellä asetuksella ja sen oikeusperustan muodostavilla säännöksillä⁶⁵ rikotaan unionin oikeutta.

Ranskan lainsäädännön mukaan internetissä tapahtuvasta teosten jakelusta ja oikeuksien suojaamisesta vastaavalla korkealla viranomaisella (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet; Hadopi) on verkossa tehdyistä tekijänoikeuksien tai lähioikeuksien loukkauksista vastuussa olevien henkilöiden tunnistamiseksi oikeus saada pääsy tietoihin, joita sähköisten viestintäpalvelujen tarjoajien on säilytettävä. Nämä ovat oikeudenhaltijoita edustavien järjestöjen ennalta keraamia IP-osoitteita vastaavia rekisteröidyn henkilöllisyyttä koskevia tietoja. Kun tällaista loukkausta merkitsevään toimintaan käytetyn IP-osoitteen haltija on tunnistettu, Hadopi noudattaa niin sanottua porrastetun reagoinnin menettelyä. Käytännössä sillä on oikeus lähettää kyseiselle henkilölle kaksi varoituksen kaltaista suositusta ja, jos toiminta jatkuu, kirje, jossa hänelle ilmoitetaan, että hänen toimintansa saattaa johtaa rikossyytteisiin. Sillä on myös oikeus saattaa asia virallisen syyttäjän käsiteltäväksi kyseisen henkilön asettamiseksi syytteeseen⁶⁶.

Tässä yhteydessä Conseil d'État pyysi unionin tuomioistuinta tulkitsemaan sähköisen viestinnän tietosuojadirektiiviä perusoikeuskirjan valossa luettuna⁶⁷.

Ensinnäkin henkilöllisyyttä koskevien tietojen ja niitä vastaavien IP-osoitteiden säilyttämisestä unionin tuomioistuin korosti, että IP-osoitteiden yleinen ja erotuksetta tapahtuva säilyttäminen ei välttämättä merkitse vakavaa puuttumista

⁶³ Perusoikeuskirjan 7, 8 ja 11 artikla.

⁶⁴ Teollis- ja tekijänoikeuskoodeksin L. 331-29 §:ssä sallitusta henkilötietojen automaattisesta käsittelystä, josta käytetään nimitystä "Système de gestion des mesures pour la protection des œuvres sur internet" (teosten suojaamista internetissä koskevien toimenpiteiden hallintajärjestelmä), 5.3.2010 annettu asetus nro 2010-236 (JORF nro 56, 7.3.2010, teksti nro 19), sellaisena kuin se on muutettuna hallinnointielimen toteuttamasta tekijänoikeuksien ja lähioikeuksien hallinnoinnista sekä teollis- ja tekijänoikeuskoodeksin muuttamisesta 6.5.2017 annetulla asetuksella nro 2017-924 (JORF nro 109, 10.5.2017, teksti nro 176).

⁶⁵ Erityisesti teollis- ja tekijänoikeuskoodeksin L. 331-21 §:n 3-5 momentti.

⁶⁶ Hadopi ja toinen riippumaton viranomainen Conseil supérieur de l'audiovisuel (audiovisuaalisen alan neuvosto) (CSA) yhdistyivät 1.1.2022 ja muodostivat Autorité de régulation de la communication audiovisuelle et numérique (audiovisuaalisen ja digitaalisen viestinnän sääntelystä vastaava viranomainen; ARCOM). Porrastetun reagoinnin menettely säilyi kuitenkin olennaisilta osin muuttumattomana.

⁶⁷ Direktiivin 2002/58/EY 15 artiklan 1 kohta.

perusoikeuskirjassa taattuun yksityiselämän kunnioittamista, henkilötietojen suoja ja sananvapautta koskeviin oikeuksiin.

Velvollisuus varmistaa tällainen säilyttäminen voidaan oikeuttaa rikosten torjuntaa yleisesti koskevalla tavoitteella, kun on tosiasiallisesti suljettu pois se, että tämä säilyttäminen voisi merkitä vakavaa puuttumista rekisteröidyn yksityiselämään, koska olisi mahdollista tehdä häntä koskevia täsmällisiä päätelmiä muun muassa yhdistämällä nämä IP-osoitteet joukkoon liikenne- ja paikkatietoja.

Näin ollen jäsenvaltion, joka aikoo asettaa sähköisten viestintäpalvelujen tarjoajille tällaisen velvollisuuden, on varmistuttava siitä, että kyseisten tietojen säilytysmenetelmät sulkevat pois sen, että voitaisiin tehdä täsmällisiä päätelmiä rekisteröityjen yksityiselämästä.

Unionin tuomioistuin täsmensi, että säilytysmenetelmien on koskettava itse säilyttämisen rakennetta, joka on pääasiallisesti toteutettava siten, että taataan säilytettyjen eri tietoryhmien tosiasiallinen erottelu. Näitä menetelmiä koskevilla kansallisilla säännöillä on varmistettava, että kutakin tietoryhmää, mukaan lukien henkilöllisyyttä koskevat tiedot ja IP-osoitteet, säilytetään täysin erillään muista säilytettävien tietojen ryhmistä ja että tämä erottelu tapahtuu tosiasiallisesti aukottomasti suojatun ja luotettavan tietojärjestelmän avulla. Lisäksi siltä osin kuin näissä säännöissä säädetään mahdollisuudesta yhdistää säilytetyt IP-osoitteet rekisteröidyn henkilöllisyyden kanssa rikosten torjumiseksi, niissä on sallittava tällainen yhdistäminen ainoastaan käyttämällä tehokasta teknistä menettelyä, joka ei vaaranna näiden tietoryhmien aukottoman erottelun tehokkuutta. Kolmannen viranomaisen on säännöllisesti valvottava tämän erottelun luotettavuutta. Mikäli sovellettavassa kansallisessa lainsäädännössä säädetään tällaisista tiukoista vaatimuksista, IP-osoitteiden säilyttämisestä johtuvaa puuttumista ei voida pitää vakavana.

Näin ollen unionin tuomioistuin katsoi, että kun on olemassa säännös, jolla taataan, ettei minkään tietojen yhdistelmän perusteella voida tehdä täsmällisiä päätelmiä niiden henkilöiden yksityiselämästä, joiden tietoja säilytetään, sähköisen viestinnän tietosuojadirektiivi, luettuna perusoikeuskirjan valossa, ei ole esteenä sille, että jäsenvaltio asettaa velvollisuuden säilyttää IP-osoitteet yleisesti ja erotuksetta rikosten torjuntaan yleisesti liittyvän tavoitteen saavuttamiseksi.

Toiseksi unionin tuomioistuin totesi IP-osoitteita vastaaviin henkilöllisyyttä koskeviin tietoihin pääsystä, että sähköisen viestinnän tietosuojadirektiivi, luettuna perusoikeuskirjan valossa, ei lähtökohtaisesti ole esteenä kansalliselle säännöstölle, jossa annetaan hallintoviranomaiselle pääsy näihin tietoihin, joita yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat ovat säilyttäneet erillään ja tosiasiallisesti aukottomasti, vain sitä varten, että tämä viranomainen voi yksilöidä näiden osoitteiden haltijat, joiden epäillään syyllistyneen näihin oikeudenloukkauksiin, ja ryhtyä heitä koskeviin toimenpiteisiin. Tällaisessa tapauksessa kansallisessa lainsäädännössä on kiellettävä työntekijöitä, joilla on pääsy tällaisiin tietoihin, ensinnäkin paljastamasta

missään muodossa tietoja osoitteiden haltijoiden käyttämien tiedostojen sisällöstä paitsi ainoastaan asian saattamiseksi syyttäjän käsiteltäväksi, toiseksi jäljittämästä näiden henkilöiden selailupolkua ja kolmanneksi käyttämästä näitä IP-osoitteita muihin tarkoituksiin kuin näiden toimenpiteiden toteuttamiseksi.

Tässä yhteydessä unionin tuomioistuin muistutti erityisesti, että vaikka sananvapaus ja henkilötietojen luottamuksellisuus ovat keskeisiä huolenaiheita, nämä perusoikeudet eivät kuitenkaan ole ehdottomia. Kun kyseessä ovat oikeudet ja edut on punnittu, niiden on nimittäin toisinaan väistytävä muiden perusoikeuksien ja yleisen edun mukaisten pakottavien syiden kuten yleisen järjestyksen säilyttämisen ja rikosten estämisen tai muiden henkilöiden oikeuksien ja vapauksien suojelemisen tieltä. Näin on erityisesti silloin, kun näille keskeisille huolenaiheille annettu etusija on omiaan haittaamaan rikostutkinnan tehokkuutta muun muassa tekemällä rikoksentekijän tunnistamisen ja hänelle määrättävän seuraamuksen mahdolltomaksi tai liiallisen vaikeaksi.

Unionin tuomioistuin viittasi tässä samassa yhteydessä myös oikeuskäytäntöönsä, jonka mukaan verkossa tapahtuvasta tekijänoikeuksia tai lähioikeuksia loukkaavasta toiminnasta rangaistavien rikosten torjunnassa se seikka, että pääsy IP-osoitteisiin voi olla ainoa tutkintakeino, jonka avulla voidaan tunnistaa asianomainen henkilö, on omiaan osoittamaan, että näiden osoitteiden säilyttäminen ja niihin pääsy ovat ehdottoman välttämättömiä tavoitellun päämäärän saavuttamiseksi ja vastaavat näin ollen oikeasuhteisuuden vaatimusta. Se, ettei tällaista pääsyä tietoihin anneta, sisältäisi lisäksi todellisen riskin siitä, että rankaisematta jäisivät järjestelmällisesti rikokset, jotka on tehty verkossa tai joiden tekemistä tai valmistelua internetin ominaispiirteet helpottavat. Tällaisen riskin olemassaolo on merkityksellinen seikka arvioitaessa kyseessä olevien eri oikeuksien ja intressien punninnan yhteydessä sitä, onko puuttuminen yksityiselämän kunnioittamisesta, henkilötietojen suojaan ja sananvapautta koskeviin oikeuksiin oikeasuhteinen toimenpide rikosten torjuntaa koskevaan tavoitteeseen nähden.

Kolmanneksi lausuessaan siitä, edellyttääkö viranomaisen pääsy IP-osoitteita vastaaviin henkilöllisyyttä koskeviin tietoihin tuomioistuimen tai riippumattoman hallinnollisen elimen suorittama etukäteisvalvontaa, unionin tuomioistuin totesi, että vaatimus tällaisesta valvonnasta on välttämätön silloin, kun kansallisen säännösten yhteydessä tämä pääsy sisältää vaaran vakavasta puuttumisesta asianomaisen henkilön perusoikeuksiin siten, että se voisi mahdollistaa sen, että kyseinen viranomainen voi tehdä täsmällisiä päätelmiä tämän henkilön yksityiselämästä ja tarvittaessa laatia hänestä yksityiskohtaisen profiilin. Käänteisesti tätä etukäteisvalvontaa koskevaa vaatimusta ei voida soveltaa silloin, kun perusoikeuksiin puuttumista ei voida pitää vakavana.

Tältä osin unionin tuomioistuin täsmensi, että jos on otettu käyttöön säilytysmenetelmä, jolla varmistetaan säilytettyjen tietojen tosiasiallisesti aukoton erottelu, viranomaisen pääsy näin säilytettyjä IP-osoitteita vastaaviin henkilöllisyyttä koskeviin tietoihin ei

lähtökohtaisesti edellyttä etukäteisvalvontaa. Tällainen pääsy, jonka ainoana tarkoituksena on yksilöidä IP-osoitteen haltija, ei nimittäin pääsääntöisesti merkitse vakavaa puuttumista edellä mainittuihin oikeuksiin.

Unionin tuomioistuin ei kuitenkaan sulkenut pois sitä, että epätyypillisissä tilanteissa on olemassa vaara siitä, että viranomaisen voi pääasiassa kyseessä olevan porrastetun reagoinnin menettelyn kaltaisessa menettelyssä tehdä täsmällisiä asianomaisten henkilöiden yksityiselämää koskevia päätelmiä muun muassa silloin, kun henkilö harjoittaa vertaisverkossa toistuvasti tai jopa laajamittaisesti tekijänoikeuksia tai lähioikeuksia loukkaavaa toimintaa, joka liittyy tietäntyyppisiin suojattuihin teoksiin, jotka voivat paljastaa mahdollisesti arkaluonteisia tietoja hänen yksityiselämänsä liittyvistä seikoista.

Nyt käsiteltävässä asiassa IP-osoitteen haltija voi olla erityisen alttiina tällaiselle riskille, kun viranomaisen on päätettävä siitä, saattaako se asian syyttäjälle mahdollisen syytteen nostamiseksi tätä haltijaa vastaan. Yksityiselämän kunnioittamista koskevan oikeuden loukkauksen vakavuus voi nimittäin kasvaa sitä mukaa kuin porrastetun reagoinnin menettelyä, jossa noudatetaan vaiheittaista prosessia, toteutetaan sen muodostavissa eri vaiheissa. Se, että toimivaltaisella viranomaisella on pääsy kaikkiin menettelyn eri vaiheissa kertyneisiin rekisteröityä koskeviin tietoihin, voi näiden tietojen yhdistämisen myötä mahdollistaa tarkkojen päätelmien tekemisen rekisteröidyn yksityiselämästä. Näin ollen kansallisessa säännöstössä on säädettävä etukäteisvalvonnasta, jonka on tapahduttava ennen kuin toimivaltainen viranomainen voi yhdistää henkilöllisyyttä koskevat tiedot näihin muihin tietoihin ja ennen sellaisen tiedoksiantokirjeen mahdollista lähettämistä, jossa todetaan, että kyseinen henkilö on syyllistynyt toimintaan, joka saattaa johtaa rikossyytteisiin. Tämän valvonnan on lisäksi turvattava porrastetun reagoinnin menettelyn tehokkuus siten, että sen avulla voidaan erityisesti yksilöidä tapaukset, joissa kyseessä oleva tekijänoikeuksia tai lähioikeuksia loukkaava toiminta toistetaan. Kyseinen menettely on näin ollen järjestettävä ja jäsenneltävä siten, että toimivaltaisessa viranomaisessa tosiseikkojen tutkinnasta vastaavat henkilöt eivät pysty automaattisesti yhdistämään internetistä aiemmin kerättyjä IP-osoitteita vastaavia henkilön henkilöllisyyttä koskevia tietoja tiedostoihin, jotka sisältävät tietoja, jotka ovat jo tämän viranomaisen käytettävissä ja joiden perusteella voidaan tehdä täsmällisiä päätelmiä tämän henkilön yksityiselämästä.

Unionin tuomioistuin totesi lisäksi etukäteisvalvonnan kohteesta, että tapauksissa, joissa rekisteröidyn epäillään syyllistyneen rikkomukseen, joka yleisesti on rangaistava teko, tuomioistuimen tai riippumattoman hallinnollisen elimen, joka vastaa tästä valvonnasta, on evättävä pääsy tietoihin, jos pääsy antaisi viranomaiselle mahdollisuuden tehdä täsmällisiä päätelmiä rekisteröidyn yksityiselämästä. Sitä vastoin jopa pääsy, joka mahdollistaa tällaisten täsmällisten päätelmien tekemisen, olisi sallittava tapauksissa, joissa voidaan epäillä, että rekisteröity on syyllistynyt oikeudenloukkaukseen, jonka osalta asianomainen jäsenvaltio katsoo, että se vaarantaa yhteiskunnan olennaisen edun ja kuuluu näin ollen vakavaan rikollisuuteen.

Unionin tuomioistuimien täsmäsi myös, että etukäteisvalvonta ei kuitenkaan voi missään tapauksessa olla täysin automatisoitua, koska rikostutkinnan osalta tällainen valvonta edellyttää yhtäältä rikollisuuden torjuntaan liittyvien oikeutettujen intressien ja toisaalta yksityiselämän ja henkilötietojen suojan kunnioittamisen punnintaa. Tämä vertailu edellyttää luonnollisen henkilön toimintaa, ja tämä on tarpeen sitä suuremmalla syyllä, kun kyseessä olevan tietojenkäsittelyn automaattisuudesta ja laaja-alaisuudesta aiheutuu vaaraa yksityiselämälle.

Unionin tuomioistuimien päätteli näin ollen, että se, että kyseisessä viranomaisessa tosiseikkojen tutkinnasta vastaavilla henkilöillä on mahdollisuus yhdistää tällaiset tiedot tiedostoihin, jotka sisältävät tietoja, joiden perusteella voidaan saada selville niiden suojattujen teosten nimet, joiden internetiin saataville asettaminen on oikeuttanut sen, että oikeudenhaltijoita edustavat järjestöt ovat keränneet IP-osoitteet, edellyttää tilanteessa, jossa sama henkilö toistaa tekijänoikeuksia tai lähioikeuksia loukkaavan toiminnan, tuomioistuimen tai riippumattoman hallinnollisen elimen suorittamaa valvontaa. Tämä valvonta ei voi olla täysin automatisoitua, ja sen on tapahduttava ennen tällaista yhdistämistä, kun tällainen yhdistäminen voi tällaisissa tilanteissa mahdollistaa täsmällisten päätelmien tekemisen kyseisen henkilön, jonka IP-osoitetta on käytetty toiminnassa, joka saattaa loukata tekijänoikeuksia tai lähioikeuksia, yksityiselämästä.

Neljänneksi ja viimeiseksi unionin tuomioistuimien huomautti, että viranomaisen käyttämän tietojenkäsittelyjärjestelmän tarkastaa säännöllisin väliajoin riippumaton elin, joka on kyseiseen viranomaiseen nähden kolmas osapuoli. Tämän valvonnan tarkoituksena on varmistaa järjestelmän eheys, mukaan lukien tehokkaat suojatoimet näiden tietojen väärinkäytön riskin ja lainvastaisen tietoihin pääsyn ja tietojen käytön estämiseksi, sekä sen tehokkuus ja luotettavuus mahdollisten rikkomusten havaitsemisessa.

Unionin tuomioistuimien huomautti tässä yhteydessä, että nyt käsiteltävässä asiassa henkilötietojen automaattinen käsittely, jonka viranomainen suorittaa oikeudenhaltijoita edustavien järjestöjen havaitsemia oikeudenloukkauksia koskevien tietojen perusteella, voi sisältää tietyn määrän vääriä positiivisia tapauksia ja ennen kaikkea riskin siitä, että kolmannet käyttävät väärin tai lainvastaisiin tarkoituksiin mahdollisesti hyvin suurta määrää henkilötietoja, minkä vuoksi tällainen valvonta on välttämätöntä. Lisäksi tässä henkilötietojen käsittelyssä on noudatettava direktiivissä 2016/680 säädettyjä näiden tietojen suojaa koskevia erityisiä sääntöjä. Nyt käsiteltävässä asiassa on nimittäin niin, että vaikka viranomaisella ei sovellettavan kansallisen oikeuden nojalla ole omaa päätösvaltaa, kun se käsittelee henkilötietoja porrastetun reagoinnin menettelyssä, sitä on pidettävä viranomaisena, joka osallistuu rikosten ehkäisemiseen ja paljastamiseen, ja se kuuluu näin ollen kyseisen direktiivin soveltamisalaan. Tällaisen menettelyn kohteena olevilla henkilöillä on siten oltava käytettävissään joukko direktiivissä 2016/680 säädettyjä aineellisia ja menettelyllisiä takeita, joiden osalta ennakkoratkaisua pyytäneen tuomioistuimen on tarkastettava, että niistä on säädetty kansallisessa lainsäädännössä.

2. Henkilötietojen käsittely rikosasioissa

Tuomio 12.5.2021 (suuri jaosto), Bundesrepublik Deutschland (Interpolin punainen ilmoitus) (C-505/19, [EU:C:2021:376](#))

Vuonna 2012 Kansainvälinen rikospoliisijärjestö (jäljempänä Interpol) julkaisi Amerikan yhdysvaltojen pyynnöstä ja kyseisen maan toimivaltaisten viranomaisten antaman pidätysmääräyksen perusteella Saksan kansalaista WS:ää koskevan punaisen ilmoituksen hänen mahdollista Yhdysvaltoihin luovuttamistaan varten. Kun tällaisen ilmoituksen kohteena olevan henkilön olinpaikka Interpolin jäsenvaltion alueella selvitetään, kyseisen valtion on lähtökohtaisesti otettava hänet kiinni, otettava hänet säilöön tai rajoitettava hänen liikkumistaan.

Jo ennen kyseisen punaisen ilmoituksen julkaisemista Saksassa oli kuitenkin aloitettu WS:ää koskeva esitutkintamenettely, joka ennakkoratkaisua pyytäneen tuomioistuimen mukaan koski samoja tekoja kuin kyseinen ilmoitus. Kyseinen menettely oli päätetty lopullisesti vuonna 2010 sen jälkeen, kun WS oli suorittanut tietyn rahasumman Saksan rikosoikeudessa säädetyn tietyn sovittelumenettelyn mukaisesti. Tämän jälkeen Bundeskriminalamt (liittovaltion rikospoliisivirasto, Saksa) ilmoitti Interpolille katsovansa, että kyseisen aiemman menettelyn vuoksi nyt esillä olevassa asiassa oli sovellettava ne bis in idem -periaatetta. Kyseinen Schengenin sopimuksen soveltamisesta tehdyn yleissopimuksen⁶⁸ 54 artiklassa ja perusoikeuskirjan 50 artiklassa vahvistettu periaate on esteenä muun muassa sille, että henkilöä, jota koskevassa asiassa on jo annettu lainvoimainen tuomio, syytetään uudelleen samasta teosta.

Vuonna 2017 WS nosti kanteen Saksan liittotasavaltaa vastaan Verwaltungsgericht Wiesbadenissa (Wiesbadenin hallintotuomioistuin, Saksa), jotta kyseinen jäsenvaltio veloitetaan toteuttamaan kaikki tarvittavat toimenpiteet mainitun punaisen ilmoituksen poistamiseksi. Tältä osin WS vetoaa ne bis in idem -periaatteen loukkaamisen lisäksi siihen, että hänen SEUT 21 artiklassa vahvistettua oikeuttaan vapaaseen liikkuvuuteen on loukattu, koska hän ei voi matkustaa Schengenin sopimuksen sopimuspuolena olevaan valtioon tai jäsenvaltioon ilman vaaraa joutua otetuksi kiinni. Hän katsoo myös, että kyseisten loukkausten vuoksi hänen mainittuun punaiseen ilmoitukseen sisältyvien henkilötietojensa käsittely on henkilötietojen suojaa rikosasioissa koskevan direktiivin 2016/680⁶⁹ säännösten vastaista.

⁶⁸ Tarkastusten asteittaisesta lakkauttamisesta yhteisillä rajoilla Benelux-talousliiton valtioiden, Saksan liittotasavallan ja Ranskan tasavallan hallitusten välinen, Schengenissä 14.6.1985 allekirjoitettu sopimus (EYVL 2000, L 239, s. 19) (jäljempänä Schengenin sopimuksen soveltamisesta tehty yleissopimus).

⁶⁹ Luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27.4.2016 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 (EUVL 2016, L 119, s. 89).

Tässä asiayhteydessä Verwaltungsgericht Wiesbaden päätti kysyä unionin tuomioistuimelta ne bis in idem -periaatteen soveltamisesta ja tarkemmin ottaen mahdollisuudesta ottaa kiinni henkilö, josta on annettu punainen ilmoitus, pääasiassa kyseessä olevan kaltaisessa tilanteessa. Mikäli kyseistä periaatetta voidaan soveltaa, kyseinen tuomioistuin pyrkii lisäksi selvittämään, miten se vaikuttaa siihen, että jäsenvaltiot käsittelevät tällaisen ilmoituksen sisältämiä tietoja.

Unionin tuomioistuin totesi suuren jaoston kokoonpanossa antamassaan tuomiossa muun muassa, että direktiivin 2016/680 säännöksiä, luettuna Schengenin sopimuksen soveltamisesta tehdyn yleissopimuksen 54 artiklan ja perusoikeuskirjan 50 artiklan valossa, on tulkittava siten, että ne eivät ole esteenä Interpolin antamaan punaiseen ilmoitukseen sisältyvien henkilötietojen käsittelylle, jollei lainvoimaisessa tuomioistuinratkaisussa ole todettu, että ne bis in idem -periaatetta sovelletaan tekoihin, joihin tämä ilmoitus perustuu, kunhan tämä käsittely täyttää kyseisessä direktiivissä säädetyt edellytykset.

Kysymyksestä, joka koskee Interpolin punaiseen ilmoitukseen sisältyviä henkilötietoja, unionin tuomioistuin totesi, että kaikki kyseisiin tietoihin kohdistuva toiminta, kuten niiden tallentaminen jäsenvaltion etsittyjen henkilöiden tietokantoihin, on direktiivin 2016/680 soveltamisalaan kuuluvaa henkilötietojen käsittelyä.⁷⁰ Se katsoi lisäksi yhtäältä, että kyseistä käsittelyä tehdään laillisia tarkoituksia varten, ja toisaalta, ettei sitä voida pitää lainvastaisena pelkästään siksi, että ne bis in idem -periaatetta voidaan soveltaa tosiseikkoihin, joihin punainen ilmoitus perustuu.⁷¹ Jäsenvaltioiden viranomaisten suorittama henkilötietojen käsittely voi osoittautua välttämättömäksi juuri sen tarkistamiseksi, sovelletaanko kyseistä periaatetta.

Näissä olosuhteissa unionin tuomioistuin totesi samoin, että direktiivi 2016/680, luettuna Schengenin sopimuksen soveltamisesta tehdyn yleissopimuksen 54 artiklan ja perusoikeuskirjan 50 artiklan valossa, ei ole esteenä punaiseen ilmoitukseen sisältyvien henkilötietojen käsittelylle, jollei lainvoimaisessa tuomioistuinratkaisussa ole todettu, että ne bis in idem -periaatetta sovelletaan nyt esillä olevassa asiassa. Tämän käsittelyn on kuitenkin täytettävä kyseisessä direktiivissä säädetyt edellytykset. Sen on erityisesti oltava tarpeen toimivaltaisen viranomaisen tehtävän suorittamiseksi rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.⁷²

Sen sijaan, kun ne bis in idem -periaatetta sovelletaan, Interpolin punaiseen ilmoitukseen sisältyvien henkilötietojen tallentaminen jäsenvaltioiden etsittyjen henkilöiden tietokantoihin ei ole enää tarpeen, koska tähän henkilöön ei voida enää kohdistaa syytetoimia kyseisen ilmoituksen kattamista teoista eikä häntä tämän vuoksi voida enää ottaa kiinni näiden tekojen perusteella. Tästä seuraa, että rekisteröidyn on

⁷⁰ Direktiivin 2016/680 2 artiklan 1 kohta ja 3 artiklan 2 kohta.

⁷¹ Direktiivin 2016/680 4 artiklan 1 kohdan b alakohhta ja 8 artiklan 1 kohta.

⁷² Ks. direktiivin 2016/680 1 artiklan 1 kohta ja 8 artiklan 1 kohta.

voitava pyytää rekisterinpitäjältä henkilötietojensa poistamista. Jos tämä rekisteröinti kuitenkin pidetään voimassa, siihen on liitettävä maininta siitä, että kyseistä henkilöä ei voida enää syyttää samoista teoista jäsenvaltiossa tai sopimusvaltiossa ne bis in idem -periaatteen vuoksi.

Tuomio 21.6.2022 (suuri jaosto), Ligue des droits humains (C-817/19, [EU:C:2022:491](#))

Kyseisessä asiassa (ks. myös otsikko II.1. "Yleisen säännösten soveltamisala") unionin tuomioistuin totesi PNR-direktiivin olevan pätevä ja täsmäsi, miten tiettyjä sen säännöksiä on tulkittava.⁷³

Se totesi ensinnäkin, että direktiivissä luetellaan tyhjentävästi PNR-tietojen käsittelyllä tavoitellut päämäärät. Kyseinen direktiivi on näin ollen esteenä kansalliselle lainsäädännölle, jossa sallitaan PNR-tietojen käsittely muihin tarkoituksiin kuin terrorismirikosten ja vakavan rikollisuuden torjuntaan. Näin ollen kansallinen lainsäädäntö, jossa sallitaan PNR-tietojen käsittelyn tarkoituksiksi myös tiedustelu- ja turvallisuuspalvelujen toimintojen seuranta, saattaa jättää huomiotta sen, että luettelo on tyhjentävä. PNR-direktiivillä käyttöön otetusta järjestelmästä ei voida myöskään säätää rajatarkastusten parantamiseksi ja laittoman maahanmuuton torjumiseksi. Tästä seuraa myös, että PNR-tietoja ei saa säilyttää sellaisessa yhtenäisessä tietokannassa, johon voidaan tehdä hakuja sekä PNR-direktiivin tavoitteisiin että muunlaisiin tavoitteisiin pyrittäessä.

Toiseksi unionin tuomioistuin selvensi sellaisen riippumattoman kansallisen viranomaisen käsitettä, jolla on toimivalta tarkistaa, täyttyvätkö PNR-tietojen toimittamisen edellytykset niiden myöhempää arviointia varten, ja hyväksyä tällainen luovuttaminen. Erityisesti matkustajatietoyksiköksi perustettua viranomaista ei voida luokitella sellaiseksi viranomaiseksi, koska se ei ole ulkopuolinen siihen viranomaiseen nähden, joka pyytää oikeutta tutustua tietoihin. Koska matkustajatietoyksikön henkilöstöön kuuluvat voivat olla tällaisen tutustumisoikeuden hakemiseen oikeutettujen viranomaisten lähettämiä toimihenkilöitä, matkustajatietoyksiköllä on ilmeisesti välttämättä yhteys näihin viranomaisiin. Näin ollen PNR-direktiivi on esteenä kansalliselle lainsäädännölle, jonka mukaan matkustajatietoyksiköksi perustettu viranomainen on samalla toimivaltainen kansallinen viranomainen, jolla on toimivalta hyväksyä PNR-tietojen luovuttaminen näiden tietojen matkustajatietoyksikölle siirtämisestä alkavan kuuden kuukauden ajanjakson päätyttyä.

Kolmanneksi unionin tuomioistuin totesi PNR-tietojen säilytysajasta, että PNR-direktiivin 12 artikla, luettuna perusoikeuskirjan 7 ja 8 artiklan ja 52 artiklan 1 kohdan valossa, on esteenä kansalliselle lainsäädännölle, jossa säädetään PNR-tietojen viiden vuoden pituisesta yleisestä säilytysajasta, jota sovelletaan erotuksetta kaikkiin lentomatikustajiin.

⁷³ Erityisesti direktiivin 2 artikla ("[Direktiivin] soveltaminen EU:n sisäisiin lentoihin"), 6 artikla ("PNR-tietojen käsittely") ja 12 artikla ("Tietojen säilytysaika ja tunnistamisen mahdollistavien tiedonosien erottaminen").

Unionin tuomioistuin nimittäin katsoi, että PNR-tietojen säilyttäminen kuuden kuukauden alkuperäisen ajanjakson jälkeen ei ilmeisesti rajoitu täysin välttämättömään niiden lentomatkestajien osalta, joiden osalta etukäteisarviointi, kuuden kuukauden jakson aikana suoritettavat mahdolliset tarkistukset tai mikään muukaan seikka ei ole osoittanut sellaisten objektiivisten seikkojen – kuten esimerkiksi sen seikan, että asianomaisten matkestajien PNR-tiedot ovat tuottaneet etukäteisarvioinnin yhteydessä tarkistetun osuman – olemassaoloa, joiden perusteella voitaisiin todeta terrorismirikoksiin tai vakavaan rikollisuuteen liittyvä riski, jolla on ainakin välillinen objektiivinen yhteys kyseisten matkestajien suorittamaan lentomatkkaan. Sen sijaan unionin tuomioistuin katsoi, että kaikkien kyseisellä direktiivillä käyttöön otetun järjestelmän soveltamisalaan kuuluvien lentomatkestajien PNR-tietojen säilyttäminen kuuden kuukauden alkuperäisen jakson ajan ei lähtökohtaisesti näytä ylittävän ehdottomasti välttämättömän rajoja.

Neljänneksi unionin tuomioistuin antoi ohjeita PNR-direktiivin mahdollisesta soveltamisesta muihin matkestajia unionissa kuljettaviin liikennemuotoihin terrorismirikosten ja vakavan rikollisuuden torjumiseksi. Direktiivi, luettuna SEU 3 artiklan 2 kohdan, SEUT 67 artiklan 2 kohdan ja perusoikeuskirjan 45 artiklan valossa, on esteenä järjestelmälle, jossa siirretään ja käsitellään kaikilla liikennemuodoilla unionin alueella suoritettavien kuljetusten PNR-tietoja silloinkin, kun kyseessä olevaan jäsenvaltioon ei kohdistu todellista ja konkreettista tai ennakoitavissa olevaa terrorismiuhkaa. Tällaisessa tilanteessa PNR-direktiivillä käyttöön otettua järjestelmää on nimittäin sovellettava EU:n sisäisten lentojen tavoin ainoastaan sellaisten kuljetusten PNR-tietojen siirtoon ja käsittelyyn, jotka liittyvät muun muassa tiettyihin reitteihin tai matkestusjärjestelyihin tai tiettyihin lentoasemiin, rautatieasemiin tai merisatamiin, joiden osalta on olemassa viitteitä, jotka voivat oikeuttaa tämän soveltamisen. Asianomaisen jäsenvaltion tehtävänä on valita ne kuljetukset, joiden osalta tällaisia viitteitä on olemassa, ja tarkastella mainittua soveltamista säännöllisesti uudelleen näiden kuljetusten valinnan perusteena olleiden olosuhteiden kehityksen mukaan.

IV. Henkilötietojen siirtäminen kolmansiin maihin

Tuomio 6.11.2003 (suuri jaosto), Lindqvist (C-101/01, [EU:C:2003:596](#))

Tässä tuomiossa (ks. myös otsikko II.3 Käsité ”henkilötietojen käsittely”) ennakkoratkaisua pyytänyt tuomioistuin halusi erityisesti selvittää, oliko Lindqvist suorittanut mainitussa direktiivissä tarkoitetun henkilötietojen siirron kolmansiin maihin.

Unionin tuomioistuin katsoi, että direktiivin 95/46 25 artiklassa tarkoitetusta ”henkilötietojen siirrosta kolmansiin maihin” ei ole kyse silloin, kun tietyssä

jäsenvaltiossa oleva henkilö laittaa henkilötietoja internetsivulle, joka on tallennettu sellaisen luonnollisen tai oikeushenkilön palvelimelle, joka säilyttää sitä internetsivustoa, jolta kyseistä sivua voidaan lukea ja joka toimii samassa tai jossakin toisessa jäsenvaltiossa, saattaen tiedot näin kaikkien sellaisten henkilöiden saataville, jotka kytkeytyvät internetiin, kolmansissa maissa olevat henkilöt mukaan lukien.

Kun näet otetaan huomioon internetin kehitysaste silloin kun direktiiviä 95/46 laadittiin, sekä se, että sen IV luvussa, johon mainittu 25 artikla kuuluu, ei ole internetin käyttöön soveltuvia kriteereitä, joiden tarkoituksena on turvata se, että jäsenvaltiot kykenevät valvomaan henkilötietojen siirtämistä kolmansiin maihin ja kieltämään nämä henkilötietojen siirrot silloin, kun tällaisissa maissa voimassa oleva tietosuojaki ei ole riittävä, ei voida olettaa yhteisöjen lainsäätäjän aikoneen tulevaisuuden varalta sisällyttää käsitteeseen ”henkilötietojen siirto kolmansiin maihin” tällaista tilannetta, jossa henkilötietoja laitetaan internetsivulle, vaikka tiedot saatetaankin tällä tavoin sellaisten kolmansissa maissa olevien henkilöiden saataville, joilla on tähän tarvittavat tekniset välineet.

Tuomio 6.10.2015 (suuri jaosto), Schrems (C-362/14, [EU:C:2015:650](#))

Schrems, joka on Itävallan kansalainen ja Facebook-verkkoyhteisöpalvelun käyttäjä, oli tehnyt kantelun Data Protection Commissionerille (tietosuojavaltuutettu, Irlanti) siitä syystä, että Facebook Ireland siirsi Yhdysvaltoihin käyttäjiensä henkilötietoja ja säilytti niitä mainitussa valtiossa sijaitsevilla palvelimilla. Tietoja myös käsiteltiin tuolla. Schremsin mukaan Yhdysvaltojen oikeus ja siellä noudatetut käytännöt eivät tarjonneet riittävää suojaa sitä vastaan, että julkisviranomaiset valvovat kyseiseen valtioon siirrettyjä tietoja. Data Protection Commissioner kieltäytyi tutkimasta kantelua muun muassa sillä perusteella, että komissio oli päätöksessään 2000/520/EY⁷⁴ katsonut, että safe harbour -järjestelmän⁷⁵ ansiosta Yhdysvallat takaa siirrettyjen henkilötietojen suojan riittävän tason.

Tässä tilanteessa High Court (ylin tuomioistuin, Irlanti) esitti unionin tuomioistuimelle kysymyksen siitä, kuinka tulkita direktiivin 95/46 25 artiklan 6 kohtaa, jonka nojalla komissio voi todeta, että kolmas maa turvaa siirrettyjen tietojen suojan riittävän tason, sekä kysymyksen, jolla pyrittiin selvittämään, oliko komission mainitun 25 artiklan 6 kohdan nojalla tekemä päätös 2000/520 pätevä.

Unionin tuomioistuin julkisti komission päätöksen pätemättömäksi kokonaisuudessaan ja korosti ensinnäkin, että päätöksen tekeminen edellytti komission asianmukaisin perusteluin tekemää toteamusta siitä, että asianomainen kolmas maa tosiasiallisesti

⁷⁴ Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbour -periaatteiden antaman suojan riittävydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä 26.7.2000 tehty komission päätös 2000/520/EY (EYVL 2000, L 215, s. 7).

⁷⁵ Safe harbour -järjestelmä sisältää joukon henkilötietojen suojaa koskevia periaatteita, joiden noudattamiseen amerikkalaiset yritykset voivat vapaaehtoisesti sitoutua.

takaa perusoikeuksien suojan sellaisen tason, joka pääosiltaan vastaa unionin oikeusjärjestyksessä taattua tasoa. Koska komissio ei ole tätä todennut päätöksessään 2000/520, tämän päätöksen 1 artiklassa jätetään huomiotta vaatimukset, joista säädetään direktiivin 95/46 25 artiklan 6 kohdassa, luettuna perusoikeuskirjan valossa, joten kyseinen 1 artikla on pätemätön. Safe harbour -periaatteita nimittäin sovelletaan vain oman varmennuksensa antaneisiin henkilötietoja unionista saaviin yhdysvaltalaisiin organisaatioihin, mutta vaatimuksena ei ole, että Yhdysvaltain viranomaiset noudattaisivat kyseisiä periaatteita. Lisäksi päätös 2000/520 mahdollistaa puuttumisen niiden henkilöiden perusoikeuksiin, joiden henkilötiedot siirretään tai voitaisiin siirtää unionista Yhdysvaltoihin, sisältämättä toteamusta siitä, että Yhdysvalloissa olisi valtiollisia sääntöjä, joilla olisi tarkoitus rajoittaa mahdollista puuttumista kyseisiin oikeuksiin, ja sisältämättä mainintaa, että tällaista puuttumista vastaan on olemassa tehokasta oikeussuojaa.

Unionin tuomioistuinin julisti pätemättömäksi myös päätöksen 2000/520 3 artiklan, siltä osin kuin se estää kansallisia valvontaviranomaisia käyttämästä valtuuksia, jotka niillä on direktiivin 95/46 28 artiklan nojalla, kun henkilö esittää seikkoja, jotka voivat kyseenalaistaa komission päätöksen, jossa on todettu kolmannen maan takaavan tietosuojan riittävän tason, yhteensoveltuvuuden henkilöiden yksityiselämän sekä perusvapauksien ja -oikeuksien suojan kanssa. Unionin tuomioistuin katsoi, että päätöksen 2000/520 1 ja 3 artiklan pätemättömyys vaikuttaa koko päätöksen pätevyyyteen.

Sikäli kuin kyse on mahdottomuudesta perustella tällaista puuttumista, unionin tuomioistuin huomautti ensinnäkin, että unionin säännöstössä, jolla puututaan perusoikeuskirjan 7 ja 8 artiklassa taattuihin perusoikeuksiin, on säädettävä selvistä ja täsmällisistä toimenpiteiden laajuutta ja soveltamista koskevista säännöistä, joissa asetetaan vähimmäisvaatimukset, jotta henkilöillä, joiden henkilötiedot ovat kyseessä, on riittävät takeet, joiden avulla heidän tietonsa voidaan tehokkaasti suojata väärinkäytön vaaroilta sekä kaikenlaiselta näiden tietojen laittomalta saannilta ja käytöltä. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti ja on olemassa huomattava vaara laittomasta pääsystä näihin tietoihin.

Lisäksi ja varsinkin on huomattava, että yksityiselämän kunnioitusta koskevan perusoikeuden suoja unionin tasolla edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset toteutetaan sen rajoissa, mikä on ehdottomasti tarpeen. Siihen, mikä on ehdottomasti tarpeen, ei siis rajoitu säännöstö, jossa sallitaan yleisesti kaikkien henkilöiden, joiden henkilötiedot on siirretty unionista, kaikkien henkilötietojen säilyttäminen tekemättä mitään erottelua, rajoitusta tai poikkeusta tavoiteltavan päämäärän mukaan ja säätämättä objektiivisesta perusteesta, jolla voitaisiin rajoittaa viranomaisten pääsyä tietoihin ja rajata niiden myöhempi käyttö tarkoituksiin, jotka ovat täsmällisiä, täysin rajallisia ja omiaan oikeuttamaan puuttumisen, jota niin henkilötietoihin pääsy kuin niiden käyttökin merkitsevät. Säännöstöstä, jonka nojalla

viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön, on erityisesti katsottava, että sillä loukataan yksityiselämän kunnioitusta koskevan perusoikeuden keskeistä sisältöä. Myöskään säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi, ei ole tehokasta oikeussuojaa koskevan perusoikeuden, sellaisena kuin se vahvistetaan perusoikeuskirjan 47 artiklassa, keskeisen sisällön mukainen.

Lausunto 1/15 (EU:n ja Kanadan välinen matkustajarekisterisopimus) 26.7.2017 (suuri jaosto)
([EU:C:2017:592](#))

Unionin tuomioistuimien lausui 26.7.2017 ensimmäistä kertaa kansainvälisen sopimusluonnoksen yhteensoveltuvuudesta perusoikeuskirjan ja erityisesti siinä olevien yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevien määräysten kanssa.

Euroopan unioni ja Kanada ovat neuvotelleet sopimuksen matkustajatietojen (PNR-tiedot) siirtämisestä ja käsittelystä (PNR-sopimus), joka allekirjoitettiin 2014. Euroopan unionin neuvosto pyysi Euroopan parlamenttia hyväksymään sopimuksen, mutta viimeksi mainittu päätti saattaa asian unionin tuomioistuimen käsiteltäväksi selvittääkseen, oliko suunniteltu sopimus unionin oikeuden mukainen.

Suunniteltu sopimus mahdollistaa kaikkien lentomatkustajien PNR-tietojen järjestelmällisen ja jatkuvan siirtämisen Kanadan viranomaisille näiden tietojen käyttämiseksi ja säilyttämiseksi sekä niiden mahdollisen edelleen siirtämisen muille viranomaisille ja muille kolmansille maille terrorismin ja vakavan kansainvälisen rikollisuuden torjumiseksi. Suunnitellussa sopimuksessa määrätään muun muassa viiden vuoden ajasta tietojen säilyttämiseksi ja asetetaan erityisvaatimuksia, jotka koskevat PNR-tietojen turvallisuutta ja koskemattomuutta, kuten arkaluontoisten tietojen välitön poistaminen, ja siinä määrätään myös oikeudesta tutustua näihin tietoihin, korjata ja poistaa niitä sekä hallinnollisista ja oikeudellisista muutoksenhakukeinoista.

Suunnitellussa sopimuksessa tarkoitetut PNR-tiedot sisältävät matkustajan nimen ja yhteystietojen lisäksi muun muassa varausta varten tarpeelliset tiedot, kuten matkustuspäivät ja matkareitin, tiedot lipunnumeroista, samalla varaustunnuksella matkustavista henkilöryhmistä, maksutavasta tai laskutuksesta, matkatavaroista ja matkustajia koskevista yleisistä huomautuksista.

Unionin tuomioistuimien katsoi lausunnossaan, että PNR-sopimusta ei voida tehdä sen tämänhetkisessä muodossa, koska useat sen määräyksistä ovat ristiriidassa unionin tunnustamien perusoikeuksien kanssa.

Se totesi ensimmäiseksi, että sekä PNR-tietojen siirtäminen unionista Kanadan toimivaltaisille viranomaisille että unionin Kanadan kanssa neuvotteleva järjestelmä ehdoista, jotka koskevat näiden tietojen säilyttämistä, käyttöä ja mahdollista siirtämistä

edelleen muille Kanadan viranomaisille, Europolille, Eurojustille, jäsenvaltioiden oikeus- tai poliisiviranomaisille tai jopa muiden kolmansien maiden viranomaisille, muodosti perusoikeuskirjan 7 artiklassa taattuihin oikeuksiin puuttumisen. Nämä toimet merkitsevät myös puuttumista perusoikeuskirjan 8 artiklassa taattuun henkilötietojen suojan perusoikeuteen, koska ne merkitsevät henkilötietojen käsittelyä.

Unionin tuomioistuimien korosti myös, että vaikka jotkin PNR-tiedoista eivät erikseen tarkasteltuina näytä voivan paljastaa merkittäviä tietoja asianomaisten henkilöiden yksityiselämästä, kyseiset tiedot voivat yhdessä tarkasteltuina muun muassa paljastaa koko matkareitin, matkustustottumuksia, kahden tai useamman henkilön välisiä suhteita sekä tietoja lentomatkustajien taloudellisesta tilanteesta, heidän ravintotottumuksistaan tai heidän terveydentilastaan, ja ne voisivat jopa välittää näistä matkustajista suunnitellun sopimuksen 2 artiklan e alakohdassa määritellyn kaltaisia arkaluonteisia tietoja (tietoja, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista vakaumusta jne.).

Se katsoi tämän osalta, että vaikka kyseessä olevat puuttumiset voidaan oikeuttaa pyrkimyksellä yleistä etua koskevaan tavoitteeseen (yleisen turvallisuuden takaaminen terrorismin ja vakavan kansainvälisen rikollisuuden torjumisessa), useat sopimusmääräykset eivät rajoitu pelkästään tarpeelliseen eikä niissä ole selviä ja täsmällisiä sääntöjä.

Unionin tuomioistuimien totesi erityisesti, että kun otetaan huomioon vaara syrjintäkiellon vastaisesta käsittelystä, arkaluontoisten tietojen siirtäminen Kanadaan edellyttää täsmällistä ja erityisen pätevää oikeutusperustetta, joka perustuu muihin perusteisiin kuin yleisen turvallisuuden takaamiseen terrorismia ja vakavaa kansainvälistä rikollisuutta vastaan. Tässä tapauksessa tällaista oikeuttamisperustetta ei kuitenkaan ole. Unionin tuomioistuimien katsoi, että sopimusmääräykset, jotka koskevat arkaluontoisten tietojen siirtämistä Kanadaan ja niiden säilyttämistä, ovat perusoikeuksien vastaisia.

Toiseksi unionin tuomioistuimien katsoi, että lentomatkustajien lähdettyä Kanadasta kaikkien lentomatkustajien niiden PNR-tietojen säilyttäminen, joka sopimuksessa sallitaan, ei rajoitu pelkästään tarpeelliseen. Siltä osin kuin kyse on lentomatkustajista, joiden osalta riskiä terrorismista tai vakavasta kansainvälisestä rikollisuudesta ei ole tunnistettu heidän Kanadaan saapumisensa ajankohdasta siihen asti, kun he lähtevät tästä maasta, heidän PNR-tietojensa ja suunnitellun sopimuksen tavoitteen välillä ei heidän kyseisestä maasta lähdettyään ole edes sellaista välillistä yhteyttä, joka oikeuttaisi kyseisten tietojen säilyttämisen. Sen sijaan PNR-tietojen säilyttäminen lentomatkustajista, joiden osalta on tunnistettu objektiivisia seikkoja, joiden perusteella voidaan katsoa, että he voisivat Kanadasta lähdettyäänkin merkitä riskiä terrorismin ja vakavan kansainvälisen rikollisuuden torjunnan kannalta, on hyväksyttävää jopa viiden vuoden ajan heidän Kanadassa oleskelunsa päättymisenkin jälkeen.

Kolmanneksi unionin tuomioistuin katsoi, että perusoikeuskirjan 7 artiklassa vahvistettu perusoikeus yksityiselämän kunnioittamiseen edellyttää, että asianomainen henkilö voi varmistua henkilötietojensa käsittelyn paikkansapitävyydestä ja laillisuudesta. Kyseisellä henkilöllä on oltava oikeus tutustua itseään koskeviin käsiteltäviin tietoihin voidakseen suorittaa tarpeelliset tarkastukset.

Unionin tuomioistuin korosti, että suunnitellussa sopimuksessa on tärkeää, että lentomatkestajia informoidaan heidän PNR-tietojensa siirrosta kyseiseen kolmanteen maahan ja näiden tietojen käytöstä heti, kun tällainen tiedoksianto ei ole omiaan vaarantamaan suunnitellussa sopimuksessa tarkoitettuja viranomaisten suorittamia tutkimuksia. Tällainen informointi nimittäin on välttämätöntä, jotta lentomatkestajat voivat käyttää oikeuttaan saada tutustua PNR-tietoihinsa ja tarvittaessa oikeuttaan pyytää niiden oikaisua sekä perusoikeuskirjan 47 artiklan ensimmäisen kohdan mukaista oikeuttaan tehokkaihin oikeussuojakeinoihin tuomioistuimessa.

Niinpä tapauksissa, joissa esiintyy objektiivisia seikkoja, jotka oikeuttavat PNR-tietojen käytön terrorismin ja vakavan kansainvälisen rikollisuuden torjumiseksi ja jotka edellyttävät oikeusviranomaisen tai riippumattoman hallintoelimen etukäteen antamaa lupaa, lentomatkestajien henkilökohtainen informointi osoittautuu tarpeelliseksi. Sama pätee tapauksiin, joissa lentomatkestajien PNR-tiedot luovutetaan muille viranomaisille tai yksityishenkilöille. Tällainen informaatio on kuitenkin annettava vasta, kun se ei ole omiaan vaarantamaan suunnitellussa sopimuksessa tarkoitettuja viranomaisten suorittamia tutkimuksia.

Tuomio 16.7.2020 (suuri jaosto), Facebook Ireland ja Schrems (C-311/18, [EU:C:2020:559](#))

Yleisessä tietosuojasetuksessa säädetään, että henkilötietojen siirto johonkin kolmanteen maahan voidaan lähtökohtaisesti toteuttaa ainoastaan, jos kyseinen kolmas maa varmistaa riittävän tietosuojan tason. Kyseisen asetuksen mukaan komissio voi päättää, että kolmas maa varmistaa kansallisen lainsäädäntönsä tai kansainvälisten sitoumuksiensa perusteella riittävän tietosuojan tason.⁷⁶ Jollei tällaista tietosuojan riittävyttä koskevaa päätöstä ole tehty, henkilötietoja voidaan siirtää kolmanteen maahan vain, jos unioniin sijoittautunut henkilötietojen siirtäjä on toteuttanut asianmukaiset suojatoimet, joita voivat olla muun muassa komission antamat tietosuoja koskevat vakiolausekkeet, ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.⁷⁷ Yleisessä tietosuojasetuksessa vahvistetaan lisäksi täsmällisesti edellytykset, joilla tällainen siirto voidaan toteuttaa, jos tietosuojan tason riittävyttä koskevaa päätöstä ei ole tehty tai asianmukaisia suojatoimia ei ole toteutettu.⁷⁸

⁷⁶ Yleisen tietosuojasetuksen 45 artikla.

⁷⁷ Yleisen tietosuojasetuksen 46 artiklan 1 kohta ja 2 kohdan c alakohhta.

⁷⁸ Yleisen tietosuojasetuksen 49 artikla.

Maximillian Schrems, joka on Itävallan kansalainen ja asuu Itävallassa, on ollut Facebookin käyttäjä vuodesta 2008. Samoin kuin muiden unionin alueella asuvien Facebookin käyttäjien henkilötiedot, Facebook Ireland siirtää myös Schremsin henkilötiedot kokonaan tai osittain käsiteltäviksi Facebook Inc:lle kuuluville palvelimille, jotka sijaitsevat Yhdysvaltojen alueella. Schrems teki Irlannin tietosuojavaltuutetulle kantelun, jossa hän pääasiallisesti vaati tätä kieltämään nämä siirrot. Hän väitti, että Yhdysvalloissa voimassa olevat oikeussäännöt ja käytännöt eivät takaa sinne siirretyille henkilötiedoille riittävää suojaa sitä vastaan, että viranomaiset pääsevät tutustumaan niihin. Tämä kantelu hylättiin erityisesti sillä perusteella, että komissio oli päätöksessään 2000/520⁷⁹ todennut, että Yhdysvalloissa taataan riittävä tietosuojan taso. Unionin tuomioistuin, jolle High Court (ylin tuomioistuin, Irlanti) oli esittänyt ennakkoratkaisukysymyksen, totesi 6.10.2015 antamallaan tuomiolla, että kyseinen päätös oli pätemätön (jäljempänä ”tuomio Schrems I”).⁸⁰

Sen jälkeen, kun tuomio Schrems I oli annettu ja Irlannin ylin oikeusaste oli hylännyt päätöksen, jolla Schremsin kantelu oli hylätty, Irlannin valvontaviranomainen pyysi häntä muotoilemaan kantelunsa uudelleen ottaen huomioon sen, että unionin tuomioistuin oli todennut päätöksen 2000/520 pätemättömäksi. Uudelleen muotoillussa kantelussaan Schrems väitti, etteivät Yhdysvallat takaa riittävää suojaa sinne siirretyille tiedoille. Schrems vaati, että jatkossa hänen henkilötietojensa siirtämistä unionista Yhdysvaltoihin, jota Facebook Ireland harjoittaa päätöksen 2010/87/EU⁸¹ liitteessä olevien tietosuojaa koskevien vakiolausekkeiden perusteella, lykätään tai se kielletään. Koska Irlannin tietosuojavaltuutettu katsoi, että Schremsin kantelun käsittely riippuu muun muassa päätöksen 2010/87 pätevydestä, hän saattoi High Courtissa vireille menettelyn, jotta tämä esittäisi unionin tuomioistuimelle ennakkoratkaisupyynnön. Tämän menettelyn vireille saattamisen jälkeen komissio antoi päätöksen (EU) 2016/1250 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävästä.⁸²

Ennakkoratkaisua pyytänyt tuomioistuin kysyi ennakkoratkaisupyynnössään unionin tuomioistuimelta, voidaanko yleistä tietosuojaa-asetusta soveltaa henkilötietojen siirtoihin, jotka perustuvat päätöksessä 2010/87 oleviin tietosuojaa koskeviin vakiolausekkeisiin, minkä tasoista suojaa kyseisessä asetuksessa edellytetään tällaisen siirron yhteydessä ja mitä velvollisuuksia valvontaviranomaisilla on tässä yhteydessä. High Court otti lisäksi esiin kysymyksen sekä päätöksen 2010/87 että päätöksen 2016/1250 pätevydestä.

⁷⁹ Direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbour -periaatteiden antaman suojan riittävästä ja niihin liittyvistä Yhdysvaltojen kauppatieteiden ministeriön julkaisemista tavallisimmista kysymyksistä 26.7.2000 tehty komission päätös 2000/520/EY (EUVL 2000, L 215, s. 7).

⁸⁰ Tuomio 6.10.2015, Schrems, C-362/14, [EU:C:2015:650](#).

⁸¹ Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen siirtoa varten kolmansiin maihin sijoittautuneille henkilötietojen käsittelijöille 5.2.2010 annettu komission päätös 2010/87/EU (EUVL 2010, L 39, s. 5), sellaisena kuin se on muutettuna 16.12.2016 annetulla komission täytäntöönpanopäätöksellä (EU) 2016/2297 (EUVL 2016, L 344, s. 100).

⁸² Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävästä 12.7.2016 annettu komission täytäntöönpanopäätös (EU) 2016/1250 (EUVL 2016, L 207, s. 1).

Unionin tuomioistuin totesi, että päätöksen 2010/87 perusoikeuskirjan perusteella suoritettussa tarkastelussa ei ole tullut esiin mitään seikkaa, joka vaikuttaisi tämän päätöksen pätevyyyteen. Sen sijaan päätöksen 2016/1250 se totesi pätemättömäksi.

Aivan aluksi unionin tuomioistuin katsoi, että unionin oikeutta ja muun muassa yleistä tietosuoja-asetusta sovelletaan henkilötietojen siirtoon, jonka jäsenvaltioon sijoittautunut talouden toimija toteuttaa kaupallisissa tarkoituksissa toiselle talouden toimijalle, joka on sijoittautunut kolmanteen maahan, vaikka kyseisen kolmannen maan viranomaiset käsittelevät näitä tietoja siirron yhteydessä tai sen jälkeen yleistä turvallisuutta, puolustusta ja valtion turvallisuutta varten. Se täsmensi, että tällainen siirto ei voi jäädä yleisen tietosuoja-asetuksen soveltamisalan ulkopuolelle siksi, että kyseisen kolmannen maan viranomaiset käsittelevät tietoja tällä tavoin.

Tällaisen siirron yhteydessä edellytetyn suojan tasosta unionin tuomioistuin totesi, että yleisen tietosuoja-asetuksen säännöksissä tältä osin asetettuja edellytyksiä, jotka liittyvät asianmukaisiin suojatoimenpiteisiin, täytäntöönpanokelpoisiin oikeuksiin ja tehokkaisiin oikeussuojakeinoin, on tulkittava siten, että niillä on varmistettava, että henkilöt, joiden henkilötietoja siirretään kolmanteen maahan tietosuojaa koskevien vakiolausekkeiden perusteella, saavat edukseen sellaisen tietosuojan tason, joka pääosiltaan vastaa tasoa, joka taataan unionissa tällä asetuksella, luettuna perusoikeuskirjan valossa. Unionin tuomioistuin täsmensi, että tällaisen siirron yhteydessä varmistetun suojan tason arvioinnissa on muun muassa otettava huomioon yhtäältä unioniin sijoittautuneen henkilötietojen siirtäjän ja asianomaiseen kolmanteen maahan sijoittautuneen siirron vastaanottajan välillä sovitut sopimusmääräykset ja toisaalta, siltä osin kuin kyse on tämän kolmannen maan viranomaisten mahdollisesta pääsystä näin siirrettyihin henkilötietoihin, tämän maan oikeusjärjestelmään liittyvät merkitykselliset tekijät.

Valvontaviranomaisten velvollisuuksista tällaisen siirron yhteydessä unionin tuomioistuin totesi, että jollei komissio ole pätevästi tehnyt tietosuojan riittävyttä koskevaa päätöstä, toimivaltaisen valvontaviranomaisen on keskeytettävä tai kiellettävä komission antamiin tietosuojaa koskeviin vakiolausekkeisiin perustuva henkilötietojen siirto kolmanteen maahan, jos tämä valvontaviranomainen katsoo kaikkien tämän siirron olosuhteiden valossa, että tietosuojaa koskevia vakiolausekkeitä ei noudateta tai voida noudattaa tässä kolmannessa maassa ja että unionin oikeudessa vaadittua siirrettyjen tietojen suojaa ei voida varmistaa muilla keinoilla, siltä osin kuin unioniin sijoittautunut tietojen siirtäjä ei itse ole keskeyttänyt tai lopettanut siirtoa.

Unionin tuomioistuin tutki tämän jälkeen päätöksen 2010/87 pätevyyttä. Unionin tuomioistuimen mukaan pelkästään se, että siihen sisältyvät tietosuojaa koskevat vakiolausekkeet eivät sido sen kolmannen maan viranomaisia, johon henkilötietoja voidaan siirtää, ei voi saattaa tämän päätöksen pätevyyttä kyseenalaiseksi. Sen mukaan tämä pätevyys sen sijaan riippuu siitä, sisältyykö tällaiseen päätökseen tehokkaita mekanismeja, jotka käytännössä varmistavat, että unionin oikeudessa edellytettyä tietosuojan tasoa noudatetaan ja että tällaisiin lausekkeisiin perustuvat henkilötietojen

siirrot keskeytetään tai kielletään, jos näitä lausekkeitä rikotaan tai niiden noudattaminen on mahdotonta. Unionin tuomioistuin totesi, että päätöksessä 2010/87 säädetään tällaisista mekanismeista. Se korosti tältä osin, että tässä päätöksessä asetetaan tietojen siirtäjälle ja henkilötietojen siirron vastaanottajalle velvollisuus varmistaa ennalta, että asianomaisessa kolmannessa maassa noudatetaan unionin oikeudessa edellytettyä tietosuojan tasoa, ja siirron vastaanottajalle velvollisuus ilmoittaa tietojen siirtäjälle, jos se ei voi noudattaa tietosuojaa koskevia vakiolausekkeitä, jolloin viimeksi mainitun on keskeytettävä tietojen siirto ja/tai irtisanottava sopimus.

Unionin tuomioistuin tutki lopuksi päätöksen 2016/1250 pätevyyttä yleisestä tietosuojasetuksesta johtuvien velvoitteiden suhteen, luettuna perusoikeuskirjan niiden määräysten valossa, joissa taataan yksityis- ja perhe-elämän kunnioittaminen, henkilötietojen suojaaminen ja oikeus tehokkaaseen oikeussuojaan. Tältä osin unionin tuomioistuin korosti, että kyseisessä päätöksessä vahvistetaan, kuten päätöksessä 2000/520, Yhdysvaltojen kansallisen turvallisuuden ja yleisen edun tai sisäisen lainsäädännön vaatimusten ensisijaisuus, joka mahdollistaa siten puuttumisen niiden henkilöiden perusoikeuksiin, joiden henkilötietoja siirretään Yhdysvaltoihin. Unionin tuomioistuimen mukaan Yhdysvaltojen sisäisestä säännöstöstä, joka koskee Yhdysvaltojen viranomaisten pääsyä unionista Yhdysvaltoihin siirrettyihin henkilötietoihin ja näiden tietojen käyttöä, johtuvia henkilötietojen suojan rajoituksia, joita komissio on arvioinut päätöksessä 2016/1250, ei ole rajattu tavalla, joka täyttäisi vaatimukset, jotka pääosiltaan vastaavat vaatimuksia, jotka unionin oikeudessa liittyvät suhteellisuusperiaatteeseen, sillä näihin säännöksiin perustuvia tarkkailuohjelmia ei ole rajattu vain täysin välttämättömään. Unionin tuomioistuin tukeutui kyseisessä päätöksessä esitettyihin toteamuksiin ja korosti, että tiettyjen tarkkailuohjelmien osalta kyseisestä säännöstöstä ei ilmene millään tavalla, että olisi olemassa rajoituksia sen sisältämään valtuutukseen, joka koskee näiden tarkkailuohjelmien käyttöönottoa, eikä myöskään, että ei-yhdysvaltalaisia henkilöitä varten, joita nämä ohjelmat mahdollisesti koskevat, olisi olemassa suojatoimia. Unionin tuomioistuin totesi lisäksi, että vaikka kyseisessä säännöstössä asetetaan vaatimuksia, joita on noudatettava kyseisiä tarkkailuohjelmia täytäntöön pantaessa, niissä ei anneta rekisteröidyille oikeuksia, joihin voitaisiin vedota Yhdysvaltojen viranomaisia vastaan tuomioistuimissa.

Tuomioistuinvalvonnan vaatimuksesta unionin tuomioistuin totesi, että toisin kuin komissio katsoi päätöksessä 2016/1250, siinä tarkoitettu oikeusasiamiesmekanismi ei merkitse oikeussuojakeinoa sellaisessa elimessä, joka antaa näille henkilöille takeet, jotka pääosiltaan vastaavat unionin oikeudessa edellytetyjä takeita, jolla taattaisiin sekä tässä mekanismissa tarkoitettu oikeusasiamiehen riippumattomuus että sellaisten säännösten olemassaolo, jolla oikeusasiamiehelle annettaisiin toimivalta tehdä Yhdysvaltojen tiedustelupalveluja sitovia päätöksiä. Näillä perusteilla unionin tuomioistuin totesi päätöksen 2016/1250 pätemättömäksi.

V. Henkilötietojen suoja internetissä

1. Oikeus vastustaa henkilötietojen käsittelyä ("oikeus tulla unohdetuksi")

Tuomio 13.5.2014 (suuri jaosto), Google Spain ja Google (C-131/12, [EU:C:2014:317](#))

Kyseisessä tuomiossa (ks. myös otsikko II.1 "Yleisen säännösten soveltamisala" ja otsikko II.3 Käsité "henkilötietojen käsittely") unionin tuomioistuin täsmensi laajuutta, joka on direktiivissä 95/46 säädetyllä oikeudella tutustua henkilötietoihin ja oikeudella vastustaa niiden käsittelyä internetissä.

Niinpä lausueessaan kysymyksestä, joka koski internetin hakukoneen ylläpitäjän vastuun laajuutta, unionin tuomioistuin totesi, että direktiivin 95/46 12 artiklan b alakohdassa ja 14 artiklan ensimmäisen kohdan a alakohdassa taattujen tiedonsaantia ja vastustusta koskevien oikeuksien kunnioittamiseksi – ja kunhan noissa säännöksissä säädetyt edellytykset täyttyvät – hakukoneen ylläpitäjä on tietyin edellytyksin velvollinen poistamaan henkilön nimellä suoritettua haun johdosta näkyvästä hakutulosten luettelosta linkit sivullisten julkaisemiin internetsivuihin, joissa on kyseistä henkilöä koskevaa tietoa. Unionin tuomioistuin täsmensi, että tällainen velvollisuus voi olla myös siinä tilanteessa, että kyseistä nimeä tai kyseisiä tietoja ei ole poistettu ensin tai poisteta samanaikaisesti näiltä internetsivuilta, ja näin on tilanteen mukaan jopa silloin, kun niiden julkaiseminen mainituilla sivuilla on itsessään laillista.

Unionin tuomioistuin, jolta tiedusteltiin myös, onko kyseessä olevalla henkilöllä direktiivin nojalla oikeus vaatia poistamaan tällaisesta luettelosta linkit internetsivuihin sillä perusteella, että hän haluaa niiden tulevan "unohdetuiksi" tietyn ajan kuluttua, totesi ensimmäiseksi, että jopa paikkansapitävien tietojen alun perin laillinen käsittely voi ajan myötä muuttua kyseisen direktiivin kanssa yhteensopimattomaksi, jos kyseiset tiedot eivät ole enää tarpeen siihen tarkoitukseen, johon ne on kerätty ja jossa niitä on käsitelty, etenkin silloin, kun ne eivät ole asianmukaisia, kun ne eivät ole tai eivät enää ole olennaisia taikka kun ne ovat liian laajoja näihin tarkoituksiin tai niitä on säilytetty liian pitkään. Näin ollen tilanteessa, jossa kyseisen henkilön tekemän vaatimuksen johdosta todetaan, että näiden linkkien sisällyttäminen hakutulosten luetteloon on direktiivin vastaista, mainitun hakutulosten luettelon asianomaiset tiedot ja linkit on poistettava. Tässä yhteydessä on korostettava, että rekisteröidyllä siihen olevan oikeuden toteaminen, ettei hänen henkilöään koskevia tietoja liitetä enää hänen nimeensä hakutulosten luettelossa, ei edellytä sitä, että kyseessä olevien tietojen sisällyttäminen hakutulosten luetteloon aiheuttaa vahinkoa.

Unionin tuomioistuin täsmensi vielä, että kun rekisteröity voi hänellä perusoikeuskirjan 7 ja 8 artiklan nojalla olevien perusoikeuksiensa suhteen vaatia, ettei kyseessä olevia tietoja aseteta enää suuren yleisön saataville sisällyttämällä ne tällaiseen hakutulosten luetteloon, on katsottava, että kyseiset oikeudet syrjäyttävät lähtökohtaisesti paitsi hakukoneen ylläpitäjän taloudellisen intressin myös suurella yleisöllä olevan intressin

löytää mainitut tiedot tehdessään haun rekisteröidyn nimellä. Tästä ei kuitenkaan olisi kyse, jos ilmenee, että rekisteröidyllä julkisuudessa olevan aseman kaltaisista erityisistä syistä puuttuminen rekisteröidyn perusoikeuksiin on perusteltavissa sillä ensisijaisella intressillä, joka suurella yleisöllä on saada nuo tiedot saataviinsa.

2. Henkilötietojen käsittely ja immateriaalioikeudet

Tuomio 29.1.2008 (suuri jaosto), Promusicae (C-275/06, [EU:C:2008:54](#))

Promusicae, joka on espanjalainen voittoa tavoittelematon yhdistys, jonka jäsenet ovat musiikkitalenteiden ja musiikkia sisältävien audiovisuaalisten tallenteiden tuottajia ja julkaisijoita, oli nostanut espanjalaisessa tuomioistuimessa kanteen, jossa se vaati, että internetyhteyksiä tarjoavan espanjalaisen Telefónica de España SAU:n on paljastettava eräiden sellaisten internetin käyttäjien henkilöllisyys ja kotiosoite, joille Telefónica on tarjonnut internetyhteyksipalvelua ja joiden IP-osoite sekä yhteydenoton päivämäärä ja kellonaika olivat tiedossa. Promusicaen mukaan kyseiset henkilöt käyttivät tiedostojenjakohjelmaa (nk. peer-to-peer tai P2P), joka on avoin, riippumaton ja hajautettu sisällönjakoväline, jossa on pitkälle kehitetyt haku- ja lataustoiminnot ja jonka avulla on mahdollista päästä heidän henkilökohtaisen tietokoneensa jaetun hakemiston kautta äänitteisiin, joiden käyttöön liittyvät taloudelliset oikeudet kuuluivat Promusicaen jäsenille. Se vaati näin ollen edellä mainittujen tietojen luovuttamista voidakseen panna asianomaisia vastaan vireille siviiliprosessit.

Tässä tilanteessa Juzgado de lo Mercantil nº 5 de Madrid (Madridin markkinatuomioistuin nro 5, Espanja) tiedusteli unionin tuomioistuimelta sitä, edellytetäänkö unionin säännöstössä jäsenvaltioiden säätävän velvollisuudesta luovuttaa henkilötietoja tekijänoikeuden tehokkaan suojan varmistamiseksi siviiliprosessin yhteydessä.

Unionin tuomioistuimen mukaan kyseinen ennakkoratkaisupyyntö toi esiin kysymyksen eri perusoikeuksien eli yhtäältä yksityisyyden kunnioittamista koskevan oikeuden ja toisaalta omaisuudensuojaa ja tehokkaita oikeussuojakeinoja koskevien oikeuksien suojaan liittyvien vaatimusten välttämättömästä yhteensovittamisesta.

Se katsoi tästä, että tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista (direktiivi sähköisestä kaupankäynnistä) annetussa direktiivissä 2000/31/EY,⁸³ tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa annetussa direktiivissä 2001/29/EY⁸⁴, teollis- ja tekijänoikeuksien noudattamisen varmistamisesta

⁸³ Tietoyhteiskunnan palveluja, erityisesti sähköistä kaupankäyntiä, sisämarkkinoilla koskevista tietyistä oikeudellisista näkökohdista (direktiivi sähköisestä kaupankäynnistä) 8.6.2000 annettu Euroopan parlamentin ja neuvoston direktiivi 2000/31/EY (EYVL 2000, L 178, s. 1).

⁸⁴ Tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa 22.5.2001 annettu Euroopan parlamentin ja neuvoston direktiivi 2001/29/EY (EYVL 2001, L 167, s. 10).

annetussa direktiivissä 2004/48/EY⁸⁵ ja direktiivissä 2002/58 ei edellytetä jäsenvaltioita säätämään pääasiassa kyseessä olevan kaltaisessa tilanteessa velvollisuudesta luovuttaa henkilötietoja tekijänoikeuden tehokkaan suojan varmistamiseksi siviiliprosessin yhteydessä. Unionin oikeuden mukaan mainittujen valtioiden on kuitenkin pannessaan täytäntöön kyseisiä direktiivejä huolehdittava siitä, että ne nojautuvat sellaiseen kyseisten direktiivien tulkintaan, jolla voidaan varmistaa unionin oikeusjärjestyksessä suojattujen eri perusoikeuksien välinen asianmukainen tasapaino. Jäsenvaltioiden viranomaisten ja tuomioistuinten on pannessaan täytäntöön mainittujen direktiivien noudattamisen edellyttämiä toimenpiteitä tulkittava kansallista oikeuttaan näiden samojen direktiivien mukaisesti, ja tämän lisäksi ne eivät myöskään saa nojautua sellaiseen kyseisten direktiivien tulkintaan, joka johtaisi ristiriitaan mainittujen perusoikeuksien kanssa tai muiden yhteisön oikeuden yleisten periaatteiden, kuten suhteellisuusperiaatteen, kanssa.

Tuomio 19.4.2012, Bonnier Audio ym. (C-461/10, [EU:C:2012:219](#))

Högsta domstolen (ylin tuomioistuin, Ruotsi) esitti unionin tuomioistuimelle ennakkoratkaisupyynnön direktiivien 2002/58 ja 2004/48 tulkinnasta oikeudenkäynnissä, jossa vastakkain olivat yhtäältä Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB ja Storyside AB (jäljempänä Bonnier Audio ym.) ja toisaalta Perfect Communication Sweden AB (jäljempänä ePhone) ja jossa viimeksi mainittu vastustaa Bonnier Audio ym.:iden vaatimusta tietojenantomääräyksestä.

Bonnier Audio ym. ovat kustantamoja, joilla on yksinoikeus valmistaa kappaleita 27:stä äänikirjan muodossa olevasta teoksesta, julkaista niitä ja saattaa niitä yleisön saataville. Bonnier Audio ym. katsovat, että niiden yksinoikeuksia on loukattu siten, että kyseistä 27:ää teosta on ilman niiden suostumusta levitetty yleisölle käyttäen FTP-palvelinta (file transfer protocol), joka mahdollistaa tiedostojen jakamisen ja tietojen siirron internetissä tietokoneiden välillä. Niinpä ne hakivat ruotsalaiselta tuomioistuimelta tietojenantomääräystä, jossa veloitettaisiin ilmoittamaan sen henkilön nimi ja osoite, joka käyttää IP-osoitetta, jonka kautta kyseiset tiedostot oletettavasti on lähetetty.

Tässä tilanteessa kassaatiovalitusta käsittelevä Högsta domstolen tiedusteli unionin tuomioistuimelta, onko unionin oikeus esteenä sellaisen kansallisen säännöksen soveltamiselle, joka on annettu direktiivin 2004/48 8 artiklan nojalla ja jonka mukaan internetyhteyden tarjoaja voidaan määrätä antamaan internetyhteyden tilaajan tai käyttäjän tunnistamista varten tekijänoikeuden haltijalle tai tämän oikeudenomistajalle tieto sen tilaajan nimestä ja osoitteesta, jolle on rekisteröity IP-osoite, josta tekijänoikeutta väitetään loukatun. Kysymyksessä edellytetään, että määräyksen hakija

⁸⁵ Teollis- ja tekijänoikeuksien noudattamisen varmistamisesta 29.4.2004 annettu Euroopan parlamentin ja neuvoston direktiivi 2004/48/EY (EUVL 2004, L 157, s. 45 ja oikaisu EUVL 2004, L 195, s. 16).

saattaa tekijänoikeuteen kohdistuneen loukkauksen todennäköiseksi ja että toimenpide on oikeasuhteinen.

Unionin tuomioistuin muistutti ensinnäkin, että direktiivin 2004/48 8 artiklan 3 kohta, kun sitä tulkitaan yhdessä direktiivin 2002/58 15 artiklan 1 kohdan kanssa, ei ole esteenä sille, että jäsenvaltiot säätävät velvollisuudesta luovuttaa yksityisille henkilötietoja, jotta siviilituomioistuimissa voidaan panna vireille menettely tekijänoikeuksien loukkauksien vuoksi, mutta siinä ei myöskään aseteta näille valtioille velvollisuutta säätää tällaista velvollisuutta. Jäsenvaltioiden viranomaisten ja tuomioistuinten on kuitenkin tulkittava kansallista oikeuttaan näiden samojen direktiivien mukaisesti, ja tämän lisäksi ne eivät myöskään saa nojautua sellaiseen kyseisten direktiivien tulkintaan, joka johtaisi ristiriitaan mainittujen perusoikeuksien kanssa tai muiden unionin oikeuden yleisten periaatteiden, kuten suhteellisuusperiaatteen, kanssa.

Se huomautti tästä, että kyseessä olevassa kansallisessa lainsäädännössä edellytetään muun muassa, että jotta kyseessä olevien tietojen antamista koskeva määräys voidaan antaa, tiettyyn teokseen liittyvän immateriaalioikeuden loukkaus on saatettava todennäköiseksi, että pyydetyt tiedot voivat helpottaa tekijänoikeuden loukkauksen tai rikkomisen tutkintaa ja että tätä määräystä puoltavien syiden on oltava merkittävämpiä kuin vahinko tai muu haitta, jota siitä aiheutuu sille, jolle se osoitetaan, tai jollekin muulle vastakkaiselle edulle.

Näin ollen unionin tuomioistuin totesi, ettei direktiivien 2002/58 ja 2004/48 kanssa ole ristiriidassa pääasiassa kyseessä olevan kaltainen kansallinen lainsäädäntö, koska kansallinen tuomioistuin, jonka käsiteltäväksi on saatettu asiavaltuuden omaavan henkilön vaatimus henkilötietojen antamista koskevasta määräyksestä, voi tämän lainsäädännön nojalla punnita asiaan liittyviä vastakkaisia etuja jokaisen yksittäistapauksen olosuhteiden mukaan ja ottaen asianmukaisesti huomioon suhteellisuusperiaatteesta johtuvat vaatimukset.

3. Henkilötietojen poistaminen hakutulosten luettelosta

Tuomio 24.9.2019 (suuri jaosto), GC ym. (Arkaluonteisten tietojen poistaminen hakutulosten luettelosta) (C-136/17, [EU:C:2019:773](#))

Kyseisessä tuomiossa unionin tuomioistuin, joka kokoontui suuressa jaostossa, täsmensi hakukoneen ylläpitäjän velvollisuuksia, kun kyse on pyynnöstä poistaa arkaluonteisia tietoja hakutulosten luettelosta.

Google oli hylännyt neljän henkilön esittämät pyynnot poistaa hakutulosten luettelosta, jonka hakukone antoi vastauksena heidän nimillään tehtyyn hakuun, useita linkkejä, jotka johtivat sivullisten julkaisemille internetsivuille, muun muassa lehtiartikkeleihin. Sen jälkeen, kun nämä neljä henkilöä olivat tehneet kanteluja, Commission nationale de l'informatique et des libertés (CNIL) (tietojenkäsittelystä ja perusvapauksista vastaava

kansallinen elin, Ranska) kieltäytyi vaatimasta Googlea toteuttamaan pyydetty hakutulosten luettelosta poistamiset. Conseil d'État (ylin hallintotuomioistuin, Ranska), jonka käsiteltäväksi asia tuli, pyysi unionin tuomioistuinta täsmentämään velvoitteita, joita hakukoneen ylläpitäjällä on direktiivin 95/46 nojalla käsitellessään hakutulosten luettelosta poistamista koskevaa pyyntöä.

Ensimmäiseksi unionin tuomioistuin muistutti, että sellaisten henkilötietojen käsittely, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta tai ammattiliittoon kuulumista, sekä terveyteen ja seksuaaliseen käyttäytymiseen liittyvien tietojen käsittely on kiellettyä⁸⁶ tietyin poikkeuksin. Rikoksiin, tuomioihin tai turvaamistoimiin liittyvää tietojenkäsittelyä voidaan lähtökohtaisesti suorittaa ainoastaan julkisen viranomaisen valvonnassa tai jos kansallisessa lainsäädännössä säädetään erityisistä tarpeellisista suojatoimista.⁸⁷

Unionin tuomioistuin totesi, että näitä erityisiä tietoryhmiä koskevaan tietojenkäsittelyyn sovellettavia kieltoa ja rajoituksia sovelletaan hakukoneen ylläpitäjään samoin kuin kaikkiin henkilötietojen käsittelyä suorittaviin rekisterinpitäjiin. Näiden kieltojen ja rajoitusten tarkoituksena nimittäin on varmistaa parempi suoja tällaista käsittelyä vastaan, joka kyseisten tietojen erityisen arkaluonteisuuden vuoksi voi merkitä erityisen vakavaa puuttumista yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin.

Hakukoneen ylläpitäjä ei ole kuitenkaan vastuussa siitä, että henkilötiedot ovat sivullisen julkaisemalla internetsivulla, vaan se on vastuussa kyseisen sivun lisäämisestä hakutulosten luetteloon. Arkaluonteisten tietojen käsittelyyn sovellettavia kieltoja ja rajoituksia voidaan näin ollen soveltaa kyseiseen ylläpitäjään vain tämän hakutulosten luetteloon lisäämisen vuoksi ja siis sellaisen tarkastuksen välityksellä, joka on suoritettava toimivaltaisten kansallisten viranomaisten valvonnassa kyseessä olevan henkilön esittämän pyynnön perusteella.

Toiseksi unionin tuomioistuin katsoi, että kun hakukoneen ylläpitäjälle on esitetty arkaluonteisia tietoja koskeva hakutulosten luettelosta poistamista koskeva pyyntö, se on lähtökohtaisesti velvollinen – tietyin poikkeuksin – hyväksymään tämän pyynnön. Kun kyse on näistä poikkeuksista, hakukoneen ylläpitäjä voi muun muassa kieltäytyä hyväksymästä hakutulosten luettelosta poistamista koskevan pyynnön, jos se toteaa, että kyseessä olevat linkit johtavat sisältöihin, joissa on henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi,⁸⁸ kunhan tällaisten linkkien luettelointi täyttää kaikki muut kyseisessä direktiivissä asetetut henkilötietojen käsittelyn laillisuutta koskevat edellytykset ja jollei rekisteröidyllä ole oikeutta vastustaa mainittua käsittelyä henkilökohtaiseen tilanteeseensa liittyvien syiden vuoksi.⁸⁹

⁸⁶ Direktiivin 95/46 8 artiklan 1 kohta ja asetuksen 2016/679 9 artiklan 1 kohta.

⁸⁷ Direktiivin 95/46 8 artiklan 5 kohta ja asetuksen 2016/679 10 artikla.

⁸⁸ Direktiivin 95/46 8 artiklan 2 kohdan e alakohta ja asetuksen 2016/679 9 artiklan 2 kohdan e alakohta.

⁸⁹ Direktiivin 95/46 14 artiklan ensimmäisen kohdan a alakohta ja asetuksen 2016/679 21 artiklan 1 kohta.

Hakukoneen ylläpitäjän on joka tapauksessa silloin, kun sille on esitetty hakutulosten luettelosta poistamista koskeva pyyntö, tarkastettava, onko internetsivulle, jolla arkaluonteisia tietoja on julkaistu, johtavan linkin sisällyttäminen rekisteröidyn nimellä suoritettun haun johdosta näkyvään luetteloon tarpeen sitä tiedonvälityksen vapautta koskevan oikeuden käyttämiseen, joka on internetin käyttäjillä, jotka ovat mahdollisesti kiinnostuneita saamaan kyseisen internetsivun tällaisella haullla saataviinsa. Tältä osin unionin tuomioistuin korosti, että vaikka yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevat oikeudet syrjäyttävät pääsääntöisesti internetin käyttäjien tiedonvälityksen vapauden, tuo tasapaino voi kuitenkin riippua erityistapauksissa kyseessä olevien tietojen luonteesta ja niiden arkaluonteisuudesta rekisteröidyn yksityiselämän kannalta sekä yleisöllä olevasta intressistä saada kyseiset tiedot käyttöönsä, ja jälkimmäinen intressi voi olla erilainen muun muassa kyseisellä henkilöllä julkisuudessa olevan aseman perusteella.

Kolmanneksi unionin tuomioistuin totesi, että hakukoneen ylläpitäjän on arvioitava sellaisen hakutulosten luettelosta poistamista koskevan pyynnön yhteydessä, joka koskee rekisteröidyn osalta rikosasiassa vireille pantua tuomioistuinmenettelyä koskevia tietoja, jotka liittyvät kyseisen menettelyn aikaisempaan vaiheeseen eivätkä vastaa enää tämänhetkistä tilannetta, onko rekisteröidyllä kaikkien sellaisten käsiteltävään tapaukseen liittyvien olosuhteiden perusteella oikeus siihen, että kyseessä olevia tietoja ei enää kyseisen arvioinnin ajankohtana liitetä hänen nimeensä hänen nimellään suoritettun haun johdosta näkyvässä hakutulosten luettelossa. Vaikka hakukoneen ylläpitäjän olisi todettava, ettei näin ole siitä syystä, että kyseessä olevan linkin sisällyttäminen osoittautuu ehdottoman tarpeelliseksi rekisteröidyllä yksityiselämän kunnioittamiseen ja tietojen suojaan olevien oikeuksien sovittamiseksi yhteen mahdollisesti kiinnostuneilla internetin käyttäjillä olevan tiedonvälityksen vapauden kanssa, kyseisen ylläpitäjän on joka tapauksessa viimeistään hakutulosten luettelosta poistamista koskevan pyynnön esittämisen yhteydessä muutettava hakutulosten luetteloa siten, että internetin käyttäjän siitä saama kokonaisvaikutelma ilmentää tämänhetkistä oikeudellista tilannetta, mikä edellyttää muun muassa, että linkit internetsivuille, jotka sisältävät tätä asiaa koskevia tietoja, näkyvät kyseisessä luettelossa ensimmäisinä.

Tuomio 24.9.2019 (suuri jaosto), Google (Hakutulosten luettelosta poistamista koskevan oikeuden alueellinen ulottuvuus) (C-507/17, [EU:C:2019:772](#))

Commission nationale de l'informatique et des libertés (CNIL) (tietojenkäsittelystä ja perusvapauksista vastaava kansallinen elin, Ranska) kehotti Googlea silloin, kun se hyväksyy hakutulosten luettelosta poistamista koskevan pyynnön, poistamaan kyseessä olevan henkilön nimellään suoritettun haun johdosta näkyvästä hakutulosten luettelosta sellaisille internetsivuille, jotka sisältävät hänen henkilötietojaan johtavat linkit, kaikkien hakukoneensa verkkotunnuspäätteiden osalta. Kun Google ei noudattanut tätä kehotusta, CNIL määräsi tälle 100 000 euron suuruisen seuraamuksen. Conseil d'État

(ylin hallintotuomioistuin, Ranska), johon Google oli valittanut, pyysi unionin tuomioistuinta täsmentämään hakukoneen ylläpitäjällä olevan sen velvollisuuden alueellista ulottuvuutta, joka koskee hakutulosten luettelosta poistamista koskevan oikeuden täytäntöön panemista direktiivin 95/46 mukaisesti.

Aluksi unionin tuomioistuin muistutti luonnollisten henkilöiden mahdollisuudesta vedota unionin oikeuden nojalla hakutulosten luettelosta poistamista koskevaan oikeuteensa sellaista hakukoneen ylläpitäjää vastaan, jolla on yksi tai useampi toimipaikka unionin alueella, riippumatta siitä, suoritetaanko henkilötietojen käsittely (tässä tapauksessa luettelo linkeistä internetsivuille, joilla on sitä henkilöä, joka vetoaa tähän oikeuteen, koskevia henkilötietoja) unionin alueella vai ei.⁹⁰

Hakutulosten luettelosta poistamista koskevan oikeuden ulottuvuudesta unionin tuomioistuin katsoi, että hakukoneen ylläpitäjä ei ole velvollinen toteuttamaan hakutulosten luettelosta poistamista hakukoneensa kaikkien versioiden osalta, vaan se on velvollinen toteuttamaan sen sellaisten kansallisten versioiden osalta, jotka vastaavat kaikkia jäsenvaltioita. Se totesi tältä osin, että vaikka hakutulosten luettelosta poistaminen kaikista versioista täyttäisi, kun otetaan huomioon internetin ja hakukoneiden ominaispiirteet, täysin unionin lainsäätäjän tavoitteen varmistaa henkilötietojen korkeatasoinen suojeleminen kaikkialla unionissa, unionin oikeudesta⁹¹ ei kuitenkaan lainkaan ilmene, että tällaisen tavoitteen saavuttamiseksi lainsäätäjä olisi valinnut antaa hakutulosten luettelosta poistamista koskevalle oikeudelle ulottuvuuden, joka ulottuisi jäsenvaltioiden alueen ulkopuolelle. Vaikka unionin oikeudessa säädetään jäsenvaltioiden valvontaviranomaisten yhteistyömekanismeista, joiden avulla ne voivat tehdä yhteisen päätöksen, joka perustuu yksityiselämän kunnioittamista ja henkilötietojen suojaamista koskevan oikeuden ja eri jäsenvaltioiden yleisöllä olevan, jonkin tiedon saamista koskevan intressin väliseen punnintaan, unionin oikeudessa ei säädetä tällä hetkellä tällaisista yhteistyömekanismeista siltä osin kuin on kyse hakutulosten luettelosta poistamisen ulottuvuudesta unionin ulkopuolella.

Unionin oikeuden nykytilassa hakukoneen ylläpitäjän ei ole toteutettava pyydettyä hakutulosten luettelosta poistamista ainoastaan hakukoneen sen version osalta, joka vastaa sitä jäsenvaltiota, jossa hakutulosten luettelosta poistamista koskevan oikeuden haltija asuu, vaan hakukoneen niiden versioiden osalta, jotka vastaavat jäsenvaltioita, ja tämä erityisesti henkilötietojen yhdenmukaisen ja korkeatasoisen suojelun varmistamiseksi koko unionissa. Tämän ylläpitäjän asiana on lisäksi toteuttaa tarvittaessa riittävän tehokkaat toimenpiteet, joilla on estettävä tai ainakin tehtävä merkittävästi vähemmän houkuttelevaksi se, että internetin käyttäjät unionin jäsenvaltioissa saavat kyseessä olevat linkit saatavilleen mahdollisesti hakukoneen kolmatta valtiota vastaavasta versiosta, ja kansallisen tuomioistuimen asiana on valvoa, täyttävätkö ylläpitäjän toteuttamat toimenpiteet tämän vaatimuksen.

⁹⁰ Direktiivin 95/46 4 artiklan 1 kohdan a alakohta ja asetuksen 2016/679 3 artiklan 1 kohta.

⁹¹ Direktiivin 95/46 12 artiklan b alakohta ja 14 artiklan ensimmäisen kohdan a alakohta sekä asetuksen 2016/679 17 artiklan 1 kohta.

Lopuksi unionin tuomioistuin korosti, että vaikka unionin oikeudessa ei aseteta hakukoneen ylläpitäjälle velvollisuutta toteuttaa hakutulosten luettelosta poistamista hakukoneensa kaikkien versioiden osalta, sitä ei myöskään kielletä. Näin ollen jäsenvaltion valvontaviranomainen tai tuomioistuinviranomainen on edelleen toimivaltainen punnitsemaan perusoikeuksien suojan kansallisen tason valossa yhtäältä rekisteröidyn henkilön oikeutta yksityiselämänsä kunnioittamiseen ja häntä koskevien henkilötietojen suojaan ja toisaalta oikeutta tiedonvälityksen vapauteen ja tämän punninnan päätteeksi määräämään tarvittaessa kyseisen hakukoneen ylläpitäjän toteuttamaan hakutulosten luettelosta poistamisen mainitun hakukoneen kaikkien versioiden osalta.

Tuomio 8.12.2022 (suuri jaosto), Google (Väitetysti virheellisen sisällön poistaminen hakutulosten luettelosta) (C-460/20, [EU:C:2022:962](#))

Pääasian valittajat, TU, joka on vastuutehtävissä eri yhtiöissä ja omistaa niiden osuuksia, ja RE, joka oli hänen avopuolisonsa ja toukokuuhun 2015 asti prokuristi yhdessä näistä yhtiöistä, olivat kohteena kolmessa artikkelissa, jotka G LLC julkaisi vuonna 2015 ylläpitämällään internetsivustolla. Näissä artikkeleissa, joista yhden kuvituksena oli neljä kantajia esittävää valokuvaa, joissa annettiin ymmärtää heidän viettävän yleistä elämää, käsiteltiin kriittisesti useiden heidän yhtiöidensä toteuttamaa sijoitusmallia. Näihin artikkeleihin saattoi saada pääsyn, kun Google LLC:n (jäljempänä Google) ylläpitämään hakukoneeseen syötettiin pääasian valittajien etu- ja sukunimet sekä erikseen että tiettyjen yhtiöiden nimien yhteydessä. Hakutulosten luettelo ohjasi kyseisiin artikkeleihin linkin välityksellä sekä pikkukuvina (”thumbnails”) näytettäviin valokuviin.

Pääasian valittajat vaativat Googlea sen hakukoneella toteutetun henkilötietojen käsittelyn rekisterinpitäjän ominaisuudessa yhtäältä poistamaan hakutulosten luettelosta linkit kyseessä oleviin artikkeleihin sillä perusteella, että ne sisältävät heidän mukaansa virheellisiä väittämiä ja kunniaa loukkaavia mielipiteitä, ja toisaalta poistamaan pikkukuvat hakutulosten luettelosta. Google kieltäytyi hyväksymästä tätä pyyntöä.

Pääasian valittajien vaatimukset hylättiin ensimmäisessä oikeusasteessa ja muutoksenhakuasteessa, joten he tekivät Bundesgerichtshofiin (liittovaltion ylin tuomioistuin, Saksa) Revision-valituksen, jonka yhteydessä Bundesgerichtshof esitti unionin tuomioistuimelle ennakkoratkaisupyynnön yleisen tietosuoja-asetuksen ja direktiivin 95/46⁹² tulkinnasta.

Suuressa jaostossa antamassaan tuomiossa unionin tuomioistuin kehitti oikeuskäytäntöä edellytyksistä, joita sovelletaan hakukoneen ylläpitäjälle esitettyihin hakutulosten luettelosta poistamista koskeviin pyyntöihin henkilötietojen suoja

⁹² Yleisen tietosuoja-asetuksen 17 artiklan 3 kohdan a alakohta ja direktiivin 95/46 12 artiklan b alakohta ja 14 artiklan ensimmäisen kohdan a alakohta.

koskevien sääntöjen perusteella. Se tutki erityisesti yhtäältä niiden velvollisuuksien ja vastuiden laajuutta, jotka hakukoneen ylläpitäjällä on käsitellessään hakutulosten luettelosta poistamista koskevaa pyyntöä, joka perustuu hakutulosten luettelossa olevaan sisältöön kuuluvien tietojen väitettyyn virheellisyyteen, ja toisaalta rekisteröidyn kyseistä virheellisyyttä koskevaa näyttötaakkaa. Se lausui lisäksi siitä, onko tutkittaessa hakukoneen ylläpitäjälle esitettyä hakutulosten luettelosta poistamista koskevaa pyyntöä, jolla pyritään saamaan poistetuksi kuvahaun tuloksista pikkukuvina näytettävät valokuvat, otettava huomioon kyseisten kuvien internetissä julkaisemisen alkuperäinen asiayhteys.

Ensiksi unionin tuomioistuin totesi, että yhtäältä yksityiselämän kunnioittamista ja henkilötietojen suoja koskevien oikeuksien ja toisaalta sananvapautta ja tiedonvälityksen vapautta koskevien oikeuksien⁹³ välisessä punninnassa, joka tehdään tutkittaessa hakukoneen ylläpitäjälle esitettyä hakutulosten luettelosta poistamista koskevaa pyyntöä, jolla pyritään saamaan poistetuksi hakutulosten luettelosta linkki sisältöön, johon kuuluu väitetysti virheellisiä väitteitä, kyseinen hakutulosten luettelosta poistaminen ei edellytä sitä, että hakutulosten luettelossa olevan sisällön paikkansapitävyyttä koskeva kysymys on ratkaistu vähintäänkin väliaikaisesti pyynnön esittäjän sisällöntarjoajaa vastaan nostaman kanteen yhteydessä.

Aluksi sen selvittämiseksi, millä edellytyksillä hakukoneen ylläpitäjä on velvollinen hyväksymään hakutulosten luettelosta poistamista koskevan pyynnön ja siis poistamaan rekisteröidyn nimellä suoritettun haun johdosta näkyvästä hakutulosten luettelosta linkin internetsivulle, jolla on kyseisen henkilön virheellisinä pitämiä väitteitä, unionin tuomioistuin palautti mieleen erityisesti seuraavaa:

- koska hakukoneen toiminta voi vaikuttaa huomattavasti ja internetsivustojen julkaisijoiden toimintaan nähden suuremmassa määrin yksityiselämän kunnioittamista ja henkilötietojen suoja koskeviin perusoikeuksiin, hakukoneen ylläpitäjän on kyseisen toiminnan tarkoituksen ja keinot määrittelevänä henkilönä varmistettava vastuidensa, valtuuksiensa ja mahdollisuuksiensa puitteissa se, että direktiivissä 95/46 ja yleisessä tietosuojasetuksessa asetetut takeet voivat saavuttaa täyden vaikutuksensa ja rekisteröityjen tehokas ja kattava suojele voidaan tosiasiallisesti turvata;
- hakukoneen ylläpitäjän on silloin, kun sille on esitetty hakutulosten luettelosta poistamista koskeva pyyntö, tarkastettava, onko kysymyksessä olevalle internetsivulle johtavan linkin sisällyttäminen hakutulosten luetteloön tarpeen sen tiedonvälityksen vapautta koskevan oikeuden käyttämiseen, joka on internetin käyttäjillä, jotka ovat mahdollisesti kiinnostuneita saamaan pääsyn kyseiselle internetsivulle tällaisella haulla, jota sananvapauden ja tiedonvälityksen vapaus suojaavat;

⁹³ Perusoikeuskirjan 7, 8 ja 11 artiklassa taatut perusoikeudet.

- tietosuoja-asetuksessa vahvistetaan nimenomaisesti yhtäältä yksityiselämän kunnioittamista ja henkilötietojen suoja koskevien perusoikeuksien ja toisaalta tiedonvälityksen vapautta koskevan perusoikeuden punnintaa koskeva vaatimus.

Aluksi unionin tuomioistuin totesi, että vaikka rekisteröidyn yksityiselämän kunnioittamista ja henkilötietojen suoja koskevat oikeudet syrjäyttävät pääsääntöisesti internetin käyttäjien perustellun intressin saada pääsy kyseisiin tietoihin, tämä tasapaino voi kuitenkin riippua kunkin tapauksen merkityksellisistä olosuhteista, erityisesti kyseisten tietojen luonteesta ja niiden arkaluonteisuudesta rekisteröidyn yksityiselämän kannalta sekä yleisöllä olevasta intressistä saada kyseiset tiedot käyttöönsä, ja jälkimmäinen intressi voi olla erilainen muun muassa kyseisellä henkilöllä julkisuudessa olevan aseman perusteella.

Hakutulosten luettelossa olevan sisällön paikkansapitävyys on myös keskeinen tekijä arvioinnissa. Tietyissä olosuhteissa internetin käyttäjien tiedonsaantioikeus ja sisällöntarjoajan sananvapaus voidaan asettaa etusijalle rekisteröidyn yksityiselämän kunnioittamista ja henkilötietojen suoja koskeviin oikeuksiin nähden erityisesti silloin, kun rekisteröidyllä on näkyvä asema julkisessa elämässä. Kyseinen suhde kääntyy kuitenkin päinvastaiseksi, jos hakutulosten luettelosta poistamista koskevan pyynnön kohteena olevien tietojen vähintäänkin sellainen osa, joka ei ole vähäinen suhteessa kokonaissisältöön, osoittautuu virheelliseksi. Tällaisessa tilanteessa ei voida ottaa huomioon tiedonanto-oikeutta ja tiedonsaantioikeutta, koska niihin ei voi kuulua oikeutta levittää tällaisia tietoja ja saada niihin pääsyä.

Seuraavaksi unionin tuomioistuin täsmensi hakutulosten luettelossa olevan sisällön paikkansapitävyyden tai virheellisyyden osoittamista koskevista velvollisuuksista, että hakutulosten luettelosta poistamista kyseisten tietojen virheellisyyden vuoksi koskevan pyynnön esittäjän on osoitettava tällaisten tietojen tai vähintäänkin sellaisen näiden tietojen osan, joka ei ole vähäinen suhteessa kokonaissisältöön, ilmeinen virheellisyys. Kuitenkin sen välttämiseksi, että kyseiselle henkilölle aiheutetaan kohtuuton taakka, joka voi haitata hakutulosten luettelosta poistamista koskevan oikeuden tehokasta vaikutusta, hänen on esitettävä ainoastaan sellainen näyttö, joka häneltä voidaan kohtuudella vaatia tapauksen olosuhteet huomioon ottaen. Kyseistä henkilöä ei voida lähtökohtaisesti vaatia esittämään oikeudenkäyntiä edeltävässä vaiheessa hakutulosten luettelosta poistamista koskevan pyyntönsä tueksi kyseessä olevaa internetsivuston julkaisijaa vastaan saatua tuomioistuimen ratkaisua, ei edes välitoimipäätöstä.

Toiseksi unionin tuomioistuin korosti hakukoneen ylläpitäjän velvollisuuksista ja vastuista, että on totta, että kyseisen ylläpitäjän on sen tarkistamiseksi, voidaanko sisältö pysyttää sen hakukoneella suoritettujen hakujen tulosten luettelossa hakutulosten luettelosta poistamista koskevan pyynnön jälkeen, käytettävä perusteena kaikkia asiaan liittyviä oikeuksia ja intressejä sekä kaikkia tapaukseen liittyviä olosuhteita. Kyseistä hakukoneen ylläpitäjää ei kuitenkaan voida velvoittaa selvittämään tosiseikkoja ja järjestämään tätä varten sisällöntarjoajan kanssa kontradiktorista näkemystenvaihtoa, jolla pyritään saamaan hakutulosten luettelossa olevan sisällön paikkansapitävyyttä

koskevat puuttuvat tiedot. Velvollisuudella myötävaikuttaa hakutulosten luettelossa olevan sisällön paikkansapitävyyden tai virheellisuuden toteamiseen asetettaisiin kyseiselle ylläpitäjälle taakka, joka ylittää sen, mitä siltä voidaan kohtuudella odottaa sen vastuiden, valtuuksien ja mahdollisuuksien osalta. Tähän ratkaisuun sisältyisi vakava vaara siitä, että sisältöjä, jotka vastaavat ensisijaiseen ja oikeutettuun yleisön tiedonvälityksen tarpeeseen, poistettaisiin hakutulosten luetteloista ja näin ollen niitä olisi tämän jälkeen vaikea löytää internetistä. Olisi siis todellinen vaara siitä, että sananvapauden ja tiedonvälityksen vapauden käyttämiseen vaikutettaisiin heikentävästi, jos tällainen hakukoneen ylläpitäjä ryhtyisi hakutulosten luettelosta poistamiseen lähes järjestelmällisesti välttääkseen taakan, joka aiheutuisi merkityksellisten tosiseikkojen selvittämisestä sen toteamiseksi, pitääkö hakutulosten luettelossa oleva sisältö paikkansa.

Näin ollen on niin, että jos hakutulosten luettelosta poistamista koskevan pyynnön esittänyt henkilö esittää asianmukaisen ja riittävän näytön, josta käy ilmi hakutulosten luettelossa olevien tietojen tai vähintäänkin sellaisen tietojen osan, joka ei ole vähäinen suhteessa kokonaissisältöön, ilmeinen virheellisyys, hakukoneen ylläpitäjän on hyväksyttävä tämä pyyntö. Sama koskee tilannetta, jossa kyseisen pyynnön esittäjä toimittaa internetsivuston julkaisijaa koskevan tuomioistuinratkaisun, joka perustuu toteamukseen siitä, että hakutulosten luettelossa olevaan sisältöön kuuluvat tiedot, jotka eivät ole vähäisiä suhteessa kokonaissisältöön, ovat ainakin ensi näkemältä virheellisiä. Jos tällaisten hakutulosten luettelossa olevaan sisältöön kuuluvien tietojen virheellisyys ei sitä vastoin ole ilmiselvää pyynnön tekijän toimittaman näytön perusteella, hakukoneen ylläpitäjällä ei ole velvollisuutta hyväksyä tällaista hakutulosten luettelosta poistamista koskevaa pyyntöä ilman tällaista tuomioistuinratkaisua. Kun kyseiset tiedot ovat omiaan myötävaikuttamaan yleisen edun mukaiseen keskusteluun, sananvapautta ja tiedonvälityksen vapautta koskevaa oikeutta on painotettava erityisesti ottaen huomioon kaikki kyseiseen tapaukseen liittyvät seikat.

Unionin tuomioistuin totesi lopuksi, että jos hakukoneen ylläpitäjä ei ryhdy hakutulosten luettelosta poistamista koskevan pyynnön johdosta toimenpiteisiin, rekisteröidyn on voitava siirtää asia valvontaviranomaiselle tai lainkäyttöviranomaiselle, jotta tämä suorittaisi välttämättömät tarkastukset ja velvoittaisi kyseisen ylläpitäjän toteuttamaan tarvittavat toimenpiteet. Tältä osin nimenomaan lainkäyttöviranomaisten on suoritettava kilpailevien intressien punninta, koska ne voivat parhaiten toteuttaa monitahoisen ja perusteellisen vertailun, jossa otetaan huomioon kaikki merkityksellisessä oikeuskäytännössä vahvistetut edellytykset ja seikat.

Toiseksi unionin tuomioistuin totesi, että asianomaisten perusoikeuksien välisessä punninnassa, joka on tehtävä tutkittaessa hakutulosten luettelosta poistamista koskevaa pyyntöä, jolla pyritään saamaan poistetuksi luonnollisen henkilön nimellä tehdyn kuvahaun tulosten luettelosta pikkukuvina näytettävät kyseistä henkilöä esittävät valokuvat, on otettava huomioon kyseisten valokuvien informaatioarvo siitä riippumatta, mikä on niiden julkaisemisen asiayhteys internetsivulla, jolta ne ovat lähtöisin. On

kuitenkin otettava huomioon tekstielementit, joita on välittömästi hakutulosten luettelossa olevien valokuvien yhteydessä ja jotka ovat omiaan selkeyttämään niiden informaatioarvoa.

Unionin tuomioistuin korosti tämän päätelmän taustasta, että henkilön nimellä hakukoneen avulla internetissä tehtyihin kuvahakuihin sovelletaan samoja periaatteita kuin internetsivuja ja niihin sisältyviä tietoja koskeviin hakuihin. Se totesi, että rekisteröityä esittävien valokuvien näyttäminen pikkukuvina nimellä tehdyn haun seurauksena voi merkitä erityisen huomattavaa puuttumista kyseisen henkilön yksityiselämän ja henkilötietojen suojaa koskevaan oikeuteen.

Hakukoneen ylläpitäjän on siis silloin, kun sille on esitetty hakutulosten luettelosta poistamista koskeva pyyntö, jolla pyritään saamaan poistetuksi luonnollisen henkilön nimellä tehdyn kuvahaun tulosten luettelosta pikkukuvina näytettävät kyseistä henkilöä esittävät valokuvat, tarkistettava, onko kyseisten valokuvien näyttäminen tarpeen sitä tiedonvälityksen vapautta koskevan oikeuden käyttämiseen, joka on internetin käyttäjillä, jotka ovat mahdollisesti kiinnostuneita saamaan pääsyn näihin valokuviin tällaisen haun avulla.

Siltä osin kuin hakukone näyttää rekisteröityä esittäviä valokuvia erillään siitä asiayhteydestä, jossa ne on julkaistu hakutulosten luettelossa olevalla internetsivulla – useimmiten kyseisen sivun sisältämien tekstielementtien kuvittamistarkoituksessa –, on määritettävä, onko kyseinen asiayhteys kuitenkin otettava huomioon tehtävässä kilpailevien oikeuksien ja intressien punninnassa. Tässä yhteydessä se, onko kyseisessä arvioinnissa otettava huomioon myös valokuvan, jonka pikkukuvana näyttämisen lopettamista on pyydetty, sisältävän internetsivun sisältö, riippuu kyseessä olevan käsittelyn kohteesta ja luonteesta.

Unionin tuomioistuin totesi ensinnäkin kyseessä olevan käsittelyn kohteesta, että valokuvien julkaisemisella voi sanattoman viestinnän välineenä olla vahvempi vaikutus internetin käyttäjiin kuin tekstijulkaisuilla. Valokuvat itsessään ovat nimittäin tärkeä internetin käyttäjien huomion kiinnittämisen menetelmä, ja ne voivat herättää kiinnostusta tutustua artikkeleihin, joiden kuvituksena ne ovat. Erityisesti siitä syystä, että niitä voidaan usein tulkita monilla tavoilla, niiden pikkukuvana näyttämisestä hakutulosten luettelossa voi seurata huomattavan vakava puuttuminen rekisteröidyn kuvansa suojaamista koskevaan oikeuteen, mikä on otettava huomioon kilpailevien oikeuksien ja intressien punninnassa. On tehtävä erilainen punninta riippuen siitä, onko kyse yhtäältä internetsivun julkaisijan artikkelien yhteydessä julkaisemista valokuvista, jotka alkuperäisessä asiayhteydessään kuvittavat kyseisten artikkelien sisältämiä tietoja ja niissä ilmaistuja mielipiteitä, ja toisaalta valokuvista, jotka hakukoneen ylläpitäjä näyttää pikkukuvina hakutulosten luettelossa erillään siitä asiayhteydestä, jossa ne on julkaistu alkuperäisellä internetsivulla.

Unionin tuomioistuin muistutti tältä osin, että sen lisäksi, ettei peruste, joka oikeuttaa julkaisemaan henkilötiedon internetsivustolla, ole välttämättä sama kuin se peruste, jota

sovelletaan hakukoneiden toimintaan, on myös niin, että vaikka peruste olisi sama, kyseessä olevien oikeuksien ja intressien punninnan, joka on suoritettava, tulos voi olla erilainen sen mukaan, onko kyse hakukoneen ylläpitäjän suorittamasta käsittelystä vai internetsivun julkaisijan suorittamasta käsittelystä. Yhtäältä kyseiset käsittelyt perustelevat oikeutetut intressit voivat olla erilaisia ja toisaalta seuraukset, jotka mainituista käsittelyistä aiheutuvat rekisteröidylle ja erityisesti hänen yksityiselämälleen, eivät välttämättä ole samat.

Toiseksi unionin tuomioistuin totesi hakukoneen ylläpitäjän suorittaman käsittelyn luonteesta, että kun hakukoneen ylläpitäjä noutaa internetissä julkaistuja luonnollisia henkilöitä esittäviä valokuvia ja näyttää ne erikseen pikkukuvina kuvahaun tulosten luettelossa, se tarjoaa palvelun, jossa henkilötietoja käsitellään itsenäisesti ja erillisenä internetsivun, jolta valokuvat on otettu, julkaisijan suorittamasta käsittelystä sekä kyseisen sivun hakemistoon lisäämiseen liittyvästä käsittelystä, josta kyseinen hakukoneen ylläpitäjä on myös vastuussa.

Näin ollen on arvioitava itsenäisesti hakukoneen ylläpitäjän toimintaa, joka koostuu kuvahaun tulosten näyttämisestä pikkukuvina, koska tällaisesta toiminnasta aiheutuva perusoikeuksien lisäloukkaus voi olla erityisen voimakas, mikä johtuu nimishaun yhteydessä tapahtuvasta rekisteröityä koskevien internetissä olevien tietojen kokoamisesta. Tässä itsenäisessä arvioinnissa on otettava huomioon se, että tämä näyttäminen pikkukuvina on sellaisenaan internetin käyttäjän tavoitteleva tulos riippumatta hänen mahdollisesta myöhemmästä päätöksestään vierailla alkuperäisellä internetsivulla.

Unionin tuomioistuin totesi kuitenkin, että tällainen erityinen punninta, jossa otetaan huomioon hakukoneen ylläpitäjän suorittaman käsittelyn itsenäinen luonne, ei vaikuta tekstielementtien, joita voi olla välittömästi hakutulosten luettelossa olevan valokuvan yhteydessä, mahdolliseen merkitykseen, koska tällaiset elementit ovat omiaan selkeyttämään tällä valokuvalla yleisölle olevaa informaatioarvoa ja näin ollen vaikuttamaan käsillä olevien oikeuksien ja intressien punnintaan.

4. Internetsivun käyttäjän suostumus tietojen tallentamiseen

Tuomio 1.10.2019 (suuri jaosto), Planet49 (C-673/17, [EU:C:2019:801](#))

Tässä tuomiossa unionin tuomioistuin totesi, että suostumusta tietojen tallentamiseen tai tietojen käyttämiseen internetsivun käyttäjän päätelaitteelle tallennettujen evästeiden avulla ei ole annettu pätevästi, jos lupa annetaan valmiiksi rastitetulla ruudulla, riippumatta siitä, ovatko kyseessä olevat tiedot henkilötietoja vai eivät. Unionin tuomioistuin totesi lisäksi, että palveluntarjoajan on ilmoitettava internetsivun käyttäjälle evästeiden toiminta-aika sekä se, onko kolmansilla mahdollisuus käyttää näitä evästeitä.

Kansallisessa tuomioistuimessa vireillä ollut riita-asia koski Planet49:n mainostarkoituksessa järjestämää arvontaa internetsivustolla www.dein-macbook.de. Internetkäyttäjien, jotka halusivat osallistua tähän arvontaan, oli syötettävä nimensä ja osoitteensa internetsivulla, jolla oli rastitettavia ruutuja. Ruutu, jolla annettiin lupa evästeiden tallentamiseen, oli rastitettu valmiiksi. Bundesgerichtshof (liittovaltion ylin tuomioistuin, Saksa), jonne Saksan kuluttajaneuvontajärjestöjen keskusjärjestö oli valittanut, oli epävarma käyttäjiltä valmiiksi rastitetun ruudun avulla saaman suostumuksen pätevydestä sekä palveluntarjoajan ilmoittamisvelvollisuuden laajuudesta.

Ennakkoratkaisupyyntö koski lähinnä direktiivissä 2002/58,⁹⁴ luettuna yhdessä direktiivin 95/46⁹⁵ sekä yleisen tietosuoja-asetuksen⁹⁶ kanssa, tarkoitetun ”suostumuksen” käsitteen tulkintaa.

Ensinnäkin unionin tuomioistuin huomautti, että direktiivin 95/46 2 artiklan h alakohdassa, johon direktiivin 2002/58 2 artiklan f alakohdassa viitataan, määritellään, että ”rekisteröidyn suostumuksella” tarkoitetaan ”kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdon ilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn”. Se korosti, että vaatimus rekisteröidyn tahdon ”ilmaisusta” viittaa selvästi aktiiviseen eikä passiiviseen toimintaan. Valmiiksi rastitetulla ruudulla annettu suostumus ei merkitse internetsivuston käyttäjän aktiivista toimintaa. Lisäksi direktiivin 2002/58 5 artiklan 3 kohdan, jossa säädetään direktiivillä 2009/136/EY tehdyn muutoksen jälkeen, että käyttäjän on pitänyt ”antaa suostumuksensa” evästeiden tallentamiseen, syntyhistoriasta ilmenee, että käyttäjän ei voida vastedes enää olettaa antaneen suostumustaan vaan suostumuksen on perustuttava käyttäjän aktiiviseen toimintaan. Yleisessä tietosuoja-asetuksessa säädetään siten vastedes nimenomaisesti aktiivisesta suostumuksesta,⁹⁷ ja sen 4 artiklan 11 kohdassa edellytetään tahdonilmaisua, joka esitetään erityisesti ”selkeästi suostumusta ilmaisevan toimen” muodossa, ja sen 32 perustelukappaleessa suljetaan nimenomaisesti pois se mahdollisuus, että suostumus on annettu ”vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta”.

Unionin tuomioistuin totesi näin ollen, että suostumus ei ole pätevästi annettu, kun lupa tietojen tallentamiseen tai internetsivuston käyttäjän päätelaitteelle jo tallennettujen tietojen käyttämiseen on annettu valmiiksi rastitetulla ruudulla, josta käyttäjän on poistettava rasti evätkseen suostumuksensa. Se totesi lisäksi, että se, että käyttäjä napsauttaa kyseisen mainostarkoituksessa järjestetyn arvonnän osallistumispainiketta, ei ole riittävää, jotta voitaisiin katsoa, että käyttäjä on pätevästi antanut suostumuksensa evästeiden tallentamiseen.

⁹⁴ Direktiivin 2002/58, sellaisena kuin se on muutettuna 25.11.2009 annetulla Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY (EUVL 2009, L 337, s. 11) 2 artiklan f alakohta ja 5 artiklan 3 kohta.

⁹⁵ Direktiivin 95/46 2 artiklan h alakohta.

⁹⁶ Asetuksen 2016/679 6 artiklan 1 kohdan a alakohta.

⁹⁷ IDEM.

Toiseksi unionin tuomioistuin totesi, että direktiivin 2002/58 5 artiklan 3 kohdalla pyritään suojelemaan käyttäjää hänen yksityisyytensä loukkaamiselta riippumatta siitä, koskeeko tämä loukkaus henkilötietoja vai muita tietoja. Tästä seuraa, että ”suostumuksen” käsitettä ei ole tulkittava eri tavoin sen mukaan, ovatko internetsivuston käyttäjän päätelaitteelle tallennetut tai sieltä haetut tiedot henkilötietoja vai eivät.

Kolmanneksi unionin tuomioistuin korosti, että direktiivin 2002/58 5 artiklan 3 kohdassa edellytetään, että käyttäjä on antanut suostumuksensa saatuaan selkeät ja kattavat tiedot muun muassa käsittelyn tarkoituksesta. Käyttäjän on voitava selkeiden ja kattavien tietojen avulla helposti määrittää mahdollisesti antamansa suostumuksen seuraukset, ja näillä tiedoilla on voitava taata käyttäjälle se, että tämä suostumus annetaan täysin tietoisena asiasta. Tältä osin unionin tuomioistuin katsoi, että evästeiden toiminta-aika sekä se, onko kolmansilla mahdollisuus käyttää näitä evästeitä, kuuluvat selkeisiin ja kattaviin tietoihin, jotka palveluntarjoajan on annettava internetsivun käyttäjälle.

5. Henkilötietojen käsittely verkkoyhteisöpalveluissa

Tuomio 4.7.2023 (suuri jaosto), Meta Platforms ym. (Yhteisöpalvelun yleiset käyttöehdot) (C-252/21, [EU:C:2023:537](#))

Yhtiö Meta Platforms omistaa Facebook-verkkoyhteisöpalvelun, joka on maksuton yksityiskäyttäjille. Tämän yhteisöpalvelun taloudellinen malli perustuu sen yksittäisille käyttäjille räätälöidystä verkkomainonnasta saatavaan rahoitukseen. Tällaisen mainonnan tekee teknisesti mahdolliseksi yhteisöpalvelun ja Meta-konsernin tarjoamien verkkopalvelujen käyttäjien yksityiskohtaisten profiilien automatisoitu laatiminen. Jotta he voivat käyttää tätä yhteisöpalvelua, käyttäjien on rekisteröityessään hyväksyttävä Meta Platformsin laatimat yleiset ehdot, joissa viitataan tämän yhtiön vahvistamiin tietosuoja- ja evästekäytäntöihin. Kyseisten käytäntöjen nojalla Meta Platforms kerää niiden tietojen lisäksi, jotka käyttäjät antavat suoraan rekisteröityessään, myös tietoja näiden käyttäjien toiminnasta yhteisöpalvelussa ja sen ulkopuolella ja yhdistää kyseiset tiedot asianomaisten käyttäjien Facebook-tileihin. Näissä yhteisöpalvelun ulkopuolista toimintaa koskevissa tiedoissa, joita kutsutaan myös off Facebook -tiedoiksi, on kyse tiedoista, jotka koskevat yhtäältä kolmansien verkkosivustoilla ja sovelluksissa käymistä ja toisaalta muiden Meta-konserniin kuuluvien verkkopalvelujen (mukaan luettuna Instagram ja WhatsApp) käyttöä. Näin kerättyjen tietojen kokonaisuuden perusteella voidaan tehdä yksityiskohtaisia päätelmiä näiden käyttäjien mieltymyksistä ja mielenkiinnon kohteista.

Bundeskartellamt (liittovaltion kilpailuviranomainen, Saksa) kielsi 6.2.2019 tehdyllä päätöksellään Meta Platformsia yhtäältä asettamasta tuolloin voimassa olleissa yleisissä ehdoissaan Saksassa asuvien yksityiskäyttäjien Facebook-yhteisöpalvelun käytön edellytykseksi sitä, että heidän off Facebook -tietojaan käsitellään, ja toisaalta

käsittelmästä kyseisiä tietoja ilman heidän suostumustaan. Lisäksi liittovaltion kilpailuviranomainen velvoitti sen muuttamaan yleisiä ehtojaan siten, että niistä käy selkeästi ilmi, että mainittuja tietoja ei kerätä, yhdistetä Facebook-käyttäjätileihin eikä käytetä ilman asianomaisen käyttäjän suostumusta. Lopuksi tämä viranomainen korosti, että tällainen suostumus ei ole pätevä, jos se on yhteisöpalvelun käytön edellytys. Se perusteli päätöstään sillä seikalla, että asianomaisten tietojen käsittelyä, joka ei ollut yleisen tietosuoja-asetuksen mukaista, oli pidettävä Meta Platformsilla verkkoyhteisöpalvelujen markkinoilla olevan määräävän aseman väärinkäyttönä.

Meta Platforms valitti tästä päätöksestä Oberlandesgericht Düsseldorfin (Düsseldorfissa sijaitseva osavaltion ylioikeus, Saksa). Oberlandesgericht Düsseldorf, jolla oli epäilyjä muun muassa yleisen tietosuoja-asetuksen tiettyjen säännösten tulkinnasta ja soveltamisesta, esitti unionin tuomioistuimelle ennakkoratkaisupyyntö.

Suuressa jaostossa antamassaan tuomiossa unionin tuomioistuin esitti täsmennyksiä, jotka koskevat yhteisöpalvelun ylläpitäjän mahdollisuutta käsitellä käyttäjiensä arkaluontoisia henkilötietoja, tällaisen ylläpitäjän suorittaman tietojenkäsittelyn lainmukaisuuden edellytyksiä sekä sitä, onko näiden käyttäjien kansallisilla verkkoyhteisöpalvelujen markkinoilla määräävässä asemassa olevalle yritykselle tällaista käsittelyä varten antama suostumus pätevä.

Unionin tuomioistuin totesi erityisiä henkilötietoryhmiä koskevan käsittelyn osalta,⁹⁸ että tilanteessa, jossa verkkoyhteisöpalvelun käyttäjä käy verkkosivustoilla tai sovelluksissa, joilla on liittymä yhteen tai useampaan tällaiseen henkilötietoryhmään, ja tarvittaessa syöttää niihin tietoja rekisteröitymällä tai tekemällä verkkotilauksia, tämän verkkoyhteisöpalvelun ylläpitäjän suorittamaa henkilötietojen käsittelyä⁹⁹ on pidettävä yleisen tietosuoja-asetuksen 9 artiklan 1 kohdassa tarkoitettuna erityisiä henkilötietoryhmiä koskevana käsittelynä, kun kyseisestä henkilötietojen käsittelystä voi ilmetä johonkin näistä ryhmistä kuuluvia tietoja, riippumatta siitä, koskevatko kyseiset tiedot palvelun käyttäjää tai ketä tahansa muuta luonnollista henkilöä. Tällainen tietojenkäsittely on lähtökohtaisesti kiellettyä tietyin poikkeuksin.¹⁰⁰

⁹⁸ Yleisen tietosuoja-asetuksen 9 artiklan 1 kohta. Tämän säännöksen mukaan "sellaisien henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys, sekä geneettisten tietojen käsittely, biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely on kiellettyä."

⁹⁹ Tämä käsittely muodostuu rajapintojen, evästeiden tai vastaavien tallennusteknologioiden avulla toteutettavasta kyseisillä sivustoilla ja kyseisissä sovelluksissa käymisestä lähtöisin olevien tietojen sekä käyttäjän syöttämien tietojen keräämisestä, kaikkien näiden tietojen yhdistämisestä hänen yhteisöpalvelutiliinsa ja kyseisen ylläpitäjän toteuttamasta näiden tietojen käyttämisestä.

¹⁰⁰ Yleisen tietosuoja-asetuksen 9 artiklan 2 kohta. Kyseisen säännöksen sanamuoto on seuraava: "Edellä olevaa 1 kohtaa ei sovelleta, jos sovelletaan jotakin seuraavista:

- a) rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä säädetään, että 1 kohdassa tarkoitettua kieltoa ei voida kumota rekisteröidyn suostumuksella --
- e) käsittely koskee henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi;
- f) käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi tai aina, kun tuomioistuimet suorittavat lainkäyttötehtäviään

--".

Unionin tuomioistuimien täsmäsi tältä osin, että kun verkkoyhteisöpalvelun käyttäjä käyttää verkkosivustolla tai sovelluksessa, joilla on liittymä yhteen tai useampaan erityiseen henkilötietoryhmään, hän ei nimenomaisesti saata julkiseksi¹⁰¹ tätä käyntiä koskevia tietoja, joita tämän verkkoyhteisöpalvelun ylläpitäjä kerää evästeiden tai vastaavien tallennusteknologioiden avulla. Lisäksi on niin, että kun käyttäjä syöttää tietoja tällaisille verkkosivustoille tai tällaisiin sovelluksiin tai kun hän käyttää niihin sisältyviä valintapainikkeita, kuten "tykkää"- ja "jaa"-painikkeita tai painikkeita, joiden avulla hän voi tunnistautua näille sivustoille tai näihin sovelluksiin käyttämällä verkkoyhteisöpalvelun käyttäjätiliinsä, puhelinnumeroonsa tai sähköpostiosoitteeseensa liittyviä kirjautumistunnuksia, hän nimenomaisesti saattaa julkiseksi näin syötetyt tai näiden painikkeiden käyttämisestä lähtöisin olevat tiedot ainoastaan siinä tapauksessa, että hän on nimenomaisesti ilmaissut etukäteen, tarvittaessa täysin tietoisesti tehdyn yksilöllisten asetusten säätämisen avulla, valintansa saattaa häntä koskevat tiedot rajoittamattoman henkilökunnan saataville julkisesti.

Yleisemmin henkilötietojen käsittelyn lainmukaisuuden edellytyksistä unionin tuomioistuimien muistutti, että yleisen tietosuojasetuksen mukaan tietojenkäsittely on lainmukaista jos ja vain siltä osin kuin rekisteröity on antanut suostumuksensa siihen yhtä tai useampaa erityistä tarkoitusta varten.¹⁰² Jos tällainen suostumus puuttuu tai sitä ei ole annettu vapaaehtoisesti, yksilöidysti, tietoisesti ja yksiselitteisesti, tällainen käsittely on kuitenkin oikeutettua, jos sen osalta täyttyy jokin käsittelyn välttämättömyyttä koskevista edellytyksistä,¹⁰³ joita on tulkittava suppeasti. Verkkoyhteisöpalvelun ylläpitäjän suorittaman henkilötietojen käsittelyn voidaan katsoa olevan tarpeen sellaisen sopimuksen täyttämiseksi, jossa nämä käyttäjät ovat osapuolena, ainoastaan sillä edellytyksellä, että tämä käsittely on objektiivisesti välttämätöntä sellaisen tarkoituksen toteuttamiseksi, joka on näille käyttäjille tarkoitettuna sopimusperusteisen suorituksen olennainen osa, joten sopimuksen pääkohdetta ei voida toteuttaa ilman tätä käsittelyä.

Lisäksi unionin tuomioistuimen mukaan kyseessä olevan tietojenkäsittelyn voidaan katsoa olevan tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi ainoastaan sillä edellytyksellä, että kyseinen ylläpitäjä on ilmoittanut tietojen keräämisen kohteena olleille käyttäjille niiden käsittelyllä tavoiteltavasta oikeutetusta edusta, että käsittely suoritetaan tämän oikeutetun edun toteuttamiselle täysin välttämättömän rajoissa ja että vastakkaisten etujen punninnasta käy ilmi, kun otetaan huomioon kaikki merkitykselliset olosuhteet, että näiden käyttäjien edut tai perusoikeudet- ja vapaudet eivät syrjäytä kyseistä rekisterinpitäjän tai kolmannen

¹⁰¹ Yleisen tietosuojasetuksen 9 artiklan 2 kohdan e alakohdassa tarkoitettussa merkityksessä.

¹⁰² Yleisen tietosuojasetuksen 6 artiklan 1 kohdan ensimmäisen alakohdan a alakohdan sanamuoto.

¹⁰³ Mainittu yleisen tietosuojasetuksen 6 artiklan 1 kohdan ensimmäisen alakohdan b–f alakohdassa. Näiden säännösten mukaan käsittely on lainmukaista ainoastaan jos ja siltä osin kuin se on tarpeen sellaisen sopimuksen täyttämiseksi, jossa rekisteröity on osapuolena (yleisen tietosuojasetuksen 6 artiklan 1 kohdan ensimmäisen alakohdan b alakohta), rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi (yleisen tietosuojasetuksen 6 artiklan 1 kohdan ensimmäisen alakohdan c alakohta) tai rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi (yleisen tietosuojasetuksen 6 artiklan 1 kohdan ensimmäisen alakohdan f alakohta).

osapuolen oikeutettua etua. Unionin tuomioistuin katsoi erityisesti, että tilanteessa, jossa nämä käyttäjät eivät ole antaneet suostumustaan, heidän etunsa ja perusoikeutensa syrjäyttävät verkkoyhteisöpalvelun ylläpitäjä edun, joka liittyy sen toiminnan rahoituslähteenä olevan mainonnan personointiin.

Lopuksi unionin täsmensi, että kyseessä olevien tietojen käsittely on oikeutettua, kun se on tosiasiallisesti tarpeen, jotta rekisterinpitäjä voi noudattaa unionin oikeussäännökseen tai asianomaisten jäsenvaltion oikeuteen perustuvaa lakisääteistä velvoitettaan, kun tämä oikeusperusta täyttää yleisen edun mukaisen tavoitteen ja on oikeasuhteinen sillä tavoiteltuun oikeutettuun päämäärään nähden ja kun tämä käsittely suoritetaan täysin välttämättömän rajoissa.

Siitä, onko asianomaisten käyttäjien suostumus heitä koskevien tietojen käsittelyyn pätevä yleisen tietosuojasetuksen nojalla, unionin tuomioistuin totesi, että se, että verkkoyhteisöpalvelun ylläpitäjä on määräävässä asemassa yhteisöpalvelujen markkinoilla, ei estä sellaisenaan sitä, että tällaisen palvelun käyttäjät voivat pätevästi antaa suostumuksensa tämän ylläpitäjän suorittamaan heitä koskevien henkilötietojen käsittelyyn. Kun otetaan huomioon, että tällainen asema voi vaikuttaa kyseisellä käyttäjällä olevaan vapaan valinnan mahdollisuuteen ja synnyttää rekisteröidyn ja rekisterinpitäjän välille selkeän epäsuhdan, se on kuitenkin tärkeä tekijä määritettäessä, onko suostumus tosiasiallisesti annettu pätevästi ja erityisesti vapaaehtoisesti, mikä tämän ylläpitäjän on osoitettava.¹⁰⁴

Näillä kyseessä olevan yhteisöpalvelun käyttäjillä on erityisesti oltava sopimusmenettelyn yhteydessä vapaus kieltäytyä tapauskohtaisesti antamasta suostumustaan erityisiin tietojenkäsittelytoimiin, jotka eivät ole välttämättömiä sopimuksen täyttämiseksi, ilman, että heidän on samalla luovuttava kokonaan tämän verkkoyhteisöpalvelun käyttämisestä, mikä tarkoittaa, että näille käyttäjille on tarjottava, tarvittaessa asianmukaista korvausta vastaan, vastaava vaihtoehto, johon ei liity tällaisia tietojenkäsittelytoimia. Lisäksi off Facebook -tietojen käsittelyyn on voitava antaa erillinen suostumus.

VI. Kansalliset valvontaviranomaiset

1. Riippumattomuusvaatimuksen ulottuvuus

Tuomio 9.3.2010 (suuri jaosto), komissio v. Saksa (C-518/07, [EU:C:2010:125](#))

Komissio vaati kanteessaan unionin tuomioistuinta toteamaan, että Saksan liittotasavalta ei ole noudattanut direktiivin 95/46 28 artiklan 1 kohdan toisen alakohdan

¹⁰⁴ Yleisen tietosuojasetuksen 7 artiklan 1 kohdan nojalla.

mukaisia velvoitteitaan, koska se oli asettanut valtion valvonnan alaiseksi valvontaviranomaiset, jotka ovat toimivaltaisia valvomaan henkilötietojen käsittelyä muulla kuin julkisella sektorilla eri osavaltioissa, ja pannut näin ollen virheellisesti täytäntöön näiden tietojen suojan takaamisesta vastaavien viranomaisten ”täydellisen itsenäisyyden” vaatimuksen.

Saksan liittotasavalta puolestaan katsoi, että direktiivin 95/46 28 artiklan 1 kohdan toisessa alakohdassa edellytetään valvontaviranomaisten toiminnallista itsenäisyyttä siten, että näiden viranomaisten on oltava riippumattomia valvontansa kohteena olevasta muusta kuin julkisesta sektorista ja että ne eivät saa olla alttiina ulkopuoliselle vaikuttamiselle. Sen mukaan valtion Saksan osavaltioissa harjoittama valvonta ei sellaisenaan ollut ulkopuolista vaikuttamista vaan hallinnon sisäinen valvontamekanismi, jonka täytäntöönpanijoina olivat valvontaviranomaisten kanssa samaan hallintokoneistoon kuuluvat viranomaiset, joiden on ensin mainittujen tavoin täytettävä direktiivin 95/46 tavoitteet.

Unionin tuomioistuimien katsoi, että direktiivissä 95/46 tarkoitetulla kansallisten valvontaviranomaisten itsenäisyyden takaamisella pyritään varmistamaan yksilöiden suojelua henkilötietojen käsittelyssä koskevien säännösten ja määräysten noudattamisen valvonnan tehokkuus ja luotettavuus, ja sitä on tulkittava tämän tavoitteen valossa. Tätä taetta ei ole otettu käyttöön sen vuoksi, että itse näille viranomaisille tai niiden toimihenkilöille annettaisiin erityinen asema, vaan sen vuoksi, että niille henkilöille ja elimille, joita niiden päätökset koskevat, annettavaa suojaa vahvistettaisiin, ja valvontaviranomaisten on näin ollen tehtäviään hoitaessaan toimittava objektiivisesti ja puolueettomasti.

Unionin tuomioistuimen mukaan näiden valvontaviranomaisten, jotka ovat toimivaltaisia valvomaan henkilötietojen käsittelyä, on oltava itsenäisiä siten, että ne voivat suorittaa tehtävänsä vapaina ulkoisesta vaikuttamisesta. Tämä itsenäisyys sulkee pois paitsi kaiken vaikuttamisen valvonnan kohteena olevien elinten taholta myös kaikki sellaiset määräykset ja kaiken muun ulkoisen vaikuttamisen, olipa se sitten suoraa tai välillistä, jotka saattaisivat asettaa kyseenalaiseksi sen, että nämä viranomaiset täyttävät tehtävänsä, joka on oikean tasapainon saavuttaminen yksityisyyden suojan ja henkilötietojen vapaan liikkuvuuden välillä. Pelkästään riski siitä, että valvovat viranomaiset voivat vaikuttaa poliittisesti toimivaltaisten valvontaviranomaisten päätöksiin, riittää estämään sen, että viimeksi mainitut voisivat suorittaa tehtävänsä itsenäisesti. Yhtäältä on niin, että ne saattavat ikään kuin ennakoiden noudattaa valvovien viranomaisten päätöskäytäntöä. Toisaalta valvontaviranomaisten rooli yksityisyyden suojan vartijoina edellyttää, että niiden päätökset – ja siis ne itse – ovat kaiken puolueellisuutta koskevan epäilyn yläpuolella. Unionin tuomioistuimen mukaan valvonta, jota valtio harjoittaa kansallisiin valvontaviranomaisiin nähden, ei täten ole yhteensopiva itsenäisyyden vaatimuksen kanssa.

Tuomio 16.10.2012 (suuri jaosto), komissio v. Itävalta (C-614/10, [EU:C:2012:631](#))

Komissio vaati kanteellaan unionin tuomioistuinta toteamaan, että Itävallan tasavalta ei ole noudattanut direktiivin 95/46 28 artiklan 1 kohdan toisen alakohdan mukaisia velvoitteitaan, koska se ei ole antanut kaikkia tarpeellisia säännöksiä ja määräyksiä, jotta Itävallassa voimassa oleva lainsäädäntö täyttäisi itsenäisyysvaatimuksen henkilötietojen suojaajaa valvovaksi viranomaiseksi perustetun Datenschutzkommissionin (tietosuojalautakunta) osalta.

Unionin tuomioistuin totesi, että Itävallan tasavalta ei ollut noudattanut jäsenyyssoveltoitteitaan, ja katsoi, että direktiivin 95/46 mukaista edellytystä valvovan viranomaisen itsenäisyydestä ei täytä jäsenvaltio, joka on ottanut käyttöön säännösten, jonka perusteella mainitun viranomaisen hallinnosta vastaava jäsen on liittovaltion virkamies, johon kohdistetaan valvontaa, viranomaisen toimisto on liittokanslerinviraston yhteydessä ja liittokanslerilla on ehdoton tiedonsaantioikeus kaikista viranomaisen hallintoa koskevista seikoista.

Unionin tuomioistuin muistutti ensimmäiseksi, että direktiivin 95/46 28 artiklan 1 kohdan toisen alakohdan ilmaisu ”itsenäisesti” on tulkittava siten, että valvovilla viranomaisilla on oltava sellainen itsenäisyys, että ne voivat hoitaa tehtäviään ilman ulkopuolista vaikuttamista. Se, että tällainen viranomainen on toiminnallisesti itsenäinen siten, että sen jäsenet ovat riippumattomia eikä mikään ohje sido heitä heidän hoitaessaan tointansa, ei yksinään riitä suojaamaan valvontaviranomaista kaikelta ulkopuoliselta vaikuttamiselta. Tässä yhteydessä edellytetyllä itsenäisyydellä pyritään kuitenkin sulkemaan pois paitsi suora vaikuttaminen ohjeiden muodossa myös kaikenlainen välillinen vaikuttaminen, joka voi ohjata valvontaviranomaisen päätöksiä. Valvontaviranomaisten rooli yksityisyyden suojan vartijoina edellyttää lisäksi, että niiden päätökset – ja siis ne itse – ovat kaiken puolueellisuutta koskevan epäilyn yläpuolella.

Unionin tuomioistuin täsmensi, että jotta henkilötietojen suojaajaa valvova viranomainen voisi täyttää direktiivin 95/46 edellä mainitussa säännöksessä ilmaistun itsenäisyysvaatimuksen, sillä ei tarvitse olla talousarviossa erillistä kohtaa, jollaisesta säädetään asetuksen N:o 45/2001 43 artiklan 3 kohdassa. Jäsenvaltiot eivät ole velvollisia saattamaan osaksi kansallisia lainsäädäntöjään asetuksen N:o 45/2001 V luvun säännösten kanssa analogisia säännöksiä kyseisten jäsenvaltioiden valvontaviranomaisen tai -viranomaisten täyden itsenäisyyden takaamiseksi, ja ne voivat näin ollen säätää, että budjettioikeudelliselta kannalta valvontaviranomainen kuuluu tietyn ministeriön alaisuuteen. Tarpeellisten henkilöstövoimavarojen ja aineellisten voimavarojen antaminen tällaisen viranomaisen käyttöön ei saa kuitenkaan estää sitä hoitamasta tehtäviään direktiivin 95/46 28 artiklan 1 kohdan toisessa alakohdassa tarkoitetulla tavalla ”itsenäisesti”.

Tuomio 8.4.2014 (suuri jaosto), komissio v. Unkari (C-288/12, [EU:C:2014:237](#))

Tässä asiassa komissio vaati unionin tuomioistuinta toteamaan, ettei Unkari ollut noudattanut direktiivin 95/46 mukaisia velvoitteitaan, koska se on päättänyt henkilötietojen suojaan valvovan viranomaisen toimikauden ennenaikaisesti.

Unionin tuomioistuin katsoi, että jäsenvaltio, joka päättää henkilötietojen suojaan valvovan viranomaisen toimikauden ennenaikaisesti, ei noudata direktiivin 95/46 mukaisia velvoitteitaan.

Valvontaviranomaisten, jotka ovat toimivaltaisia valvomaan henkilötietojen käsittelyä, itsenäisyys nimittäin sulkee pois kaikki sellaiset määräykset ja kaiken muun missä muodossa tahansa tapahtuvan ulkoisen vaikuttamisen, olipa se sitten suoraa tai välillistä, jotka saattaisivat ohjata niiden päätöksiä ja voisivat näin asettaa kyseenalaiseksi sen, että nämä viranomaiset täyttävät tehtävänsä, joka on oikean tasapainon saavuttaminen yksityisyyden suojan ja henkilötietojen vapaan liikkuvuuden välillä.

Unionin tuomioistuin muistutti lisäksi, että toiminnallinen itsenäisyys ei kuitenkaan yksinään riitä suojaamaan valvontaviranomaisia kaikelta ulkopuoliselta vaikuttamiselta, koska pelkästään riski siitä, että valtion valvovat viranomaiset voivat vaikuttaa poliittisesti valvontaviranomaisten päätöksiin, riittää estämään sen, että viimeksi mainitut voisivat suorittaa tehtävänsä itsenäisesti. Jos kukin jäsenvaltio saisi päättää valvontaviranomaisen toimikauden päättämisestä ennen sen alun perin määritettyä päättymistä noudattamatta sovellettavassa lainsäädännössä tätä varten ennalta säädettyjä sääntöjä ja takeita, tällaisen ennenaikaisen päättämisen uhka, joka olisi tällöin ilmassa kaiken aikaa tämän viranomaisen hoitaessa tehtäväänsä, voisi johtaa siihen, että tämä viranomainen tietyllä tavalla noudattaisi poliittisen vallan tahtoa, mikä ei ole kyseisen itsenäisyysvaatimuksen mukaista. Tällaisessa tilanteessa ei myöskään voida katsoa, että valvontaviranomainen voisi toimia joka tilanteessa kaiken puolueellisuutta koskevan epäilyn yläpuolella.

2. Sovellettavan oikeuden ja toimivaltaisen valvontaviranomaisen määrittäminen

Tuomio 1.10.2015, Weltimmo (C-230/14, [EU:C:2015:639](#))

Nemzeti Adatvédelmi és Információszabadság Hatóság (tietosuojasta ja tiedonvälityksen vapaudesta vastaava kansallinen virasto, Unkari) oli määrännyt Slovakiaan sijoittautuneelle Weltimmo-nimiselle yhtiölle, joka ylläpitää internetsivuja, joilla julkaistaan ilmoituksia Unkarissa sijaitsevista kiinteistöistä, sakon sillä perusteella, että ei ollut poistanut ilmoittajien henkilötietoja sivuiltaan heidän pyynnöistään huolimatta ja että se oli ilmoittanut nämä tiedot perintätoimistoille maksun saamiseksi

maksamattomista laskuista. Unkarin valvontaviranomaisen mukaan Weltimmo oli näin toimiessaan rikkonut Unkarin lakia, jolla pantiin täytäntöön direktiivi 95/46.

Kassaatiovalitusta käsitellyt Kúria (ylin tuomioistuin, Unkari) oli epävarma sovellettavasta lainsäädännöstä ja Unkarin valvontaviranomaisen toimivallasta direktiivin 95/46 4 artiklan 1 kohdan ja 28 artiklan kannalta. Se esitti täten unionin tuomioistuimelle useita ennakkoratkaisukysymyksiä.

Sovellettavasta kansallisesta lainsäädännöstä unionin tuomioistuin totesi, että direktiivin 95/46 4 artiklan 1 kohdan a alakohdan nojalla on mahdollista soveltaa henkilötietojen suojaa koskevaa lainsäädäntöä, joka on muun jäsenvaltion lainsäädäntö kuin sen, jossa näiden tietojen rekisterinpitäjä on rekisteröity, kunhan rekisterinpitäjä harjoittaa kyseisen valtion alueella olevan kiinteän toimipaikan välityksin aitoa ja todellista, vaikka vähäistäkin, toimintaa, jonka yhteydessä tämä tietojenkäsittely suoritetaan. Sen määrittämiseksi, onko tilanne tällainen, ennakkoratkaisua pyytänyt tuomioistuin voi erityisesti ottaa huomioon yhtäältä sen, että kyseisen rekisterinpitäjän toiminta, jonka yhteydessä käsittely on suoritettu, muodostuu sellaisten internetsivustojen ylläpitämisestä, joilla on ilmoituksia tämän jäsenvaltion alueella sijaitsevista kiinteistöistä ja jotka on laadittu sen kielellä ja että se on siis tämän vuoksi pääasiallisesti tai jopa täysin kohdistettu tähän jäsenvaltioon. Ennakkoratkaisua pyytänyt tuomioistuin voi toisaalta ottaa huomioon sen, että tällä rekisterinpitäjällä on kyseisessä jäsenvaltiossa edustaja, jonka tehtävänä on periä tästä toiminnasta aiheutuneet saatavat ja edustaa rekisterinpitäjää asianomaisten tietojen käsittelyä koskevissa hallinnollisissa menettelyissä ja tuomioistuinmenettelyissä. Unionin tuomioistuin täsmensi, että henkilöiden, joita tämä tietojenkäsittely koskee, kansalaisuudella ei sen sijaan ole merkitystä.

Valvontaviranomaisen, jolle kantelu tehdään direktiivin 95/46 28 artiklan 4 kohdan mukaisesti, toimivallasta unionin tuomioistuin katsoi, että kyseinen viranomainen voi käyttää tutkintavaltuuksiaan riippumatta sovellettavasta kansallisesta oikeudesta ja jopa ennen kuin tiedetään, mitä kansallista oikeutta kyseessä olevaan käsittelyyn sovelletaan. Jos se kuitenkin tulee siihen tulokseen, että jonkin toisen jäsenvaltion oikeutta sovelletaan, se ei voi määrätä seuraamuksia jäsenvaltionsa alueen ulkopuolella. Tällaisessa tilanteessa sen on direktiivin 28 artiklan 6 kohdassa säädetyn yhteistyövelvollisuuden mukaisesti pyydettävä tämän toisen jäsenvaltion valvontaviranomaista toteamaan mahdollinen tämän jäsenvaltion oikeuden rikkominen ja määräämään seuraamuksia, jos kyseinen oikeus sen mahdollistaa, niin että se nojautuu tarvittaessa ensimmäisen jäsenvaltion valvontaviranomaisen sille toimittamiin tietoihin.

3. Kansallisten valvontaviranomaisten toimivalta

Tuomio 6.10.2015 (suuri jaosto), Schrems (C-362/14, [EU:C:2015:650](#))

Tässä asiassa (ks. myös otsikko IV ”Henkilötietojen siirtäminen kolmansiin maihin”) unionin tuomioistuin katsoi muun muassa, että kansalliset valvontaviranomaiset ovat toimivaltaisia valvomaan henkilötietojen siirtoa kolmansiin maihin.

Unionin tuomioistuin totesi ensinnäkin, että kansallisilla valvontaviranomaisilla on laaja valikoima toimivaltuuksia, ja näitä valtuuksia, jotka luetellaan – muttei tyhjentävästi – direktiivin 95/46 28 artiklan 3 kohdassa, on pidettävä tarvittavina keinoina kyseisten viranomaisten tehtävien suorittamiseksi. Niinpä näillä viranomaisilla on muun muassa tutkintavaltuudet, kuten valtuudet kerätä kaikki valvontatehtävänsä suorittamiseksi tarvittavat tiedot, tehokkaat toimintavaltuudet, kuten valtuudet kieltää tietojen käsittely väliaikaisesti tai lopullisesti, tai valtuudet olla asianosaisena oikeudenkäynnissä.

Siltä osin kuin kyse on toimivallasta valvoa henkilötietojen siirtoja kolmansiin maihin, unionin tuomioistuin totesi, että direktiivin 95/46 28 artiklan 1 ja 6 kohdasta tosin ilmenee, että kansallisten valvontaviranomaisten toimivalta koskee jäsenvaltion, johon nämä viranomaiset kuuluvat, alueella toteutettuja henkilötietojen käsittelyjä, joten niillä ei ole mainitun 28 artiklan nojalla toimivaltaa kolmannen maan alueella toteutettujen henkilötietojen käsittelyjen osalta.

On kuitenkin niin, että toimenpiteessä, jolla henkilötietoja siirretään jäsenvaltiosta kolmanteen maahan, on sellaisenaan kyse henkilötietojen käsittelystä jäsenvaltion alueella. Kansallisilla valvontaviranomaisilla on perusoikeuskirjan 8 artiklan 3 kohdan ja direktiivin 95/46 28 artiklan mukaisesti tehtävänä valvoa yksilöiden suoja henkilötietojen käsittelyssä koskevien unionin sääntöjen noudattamista, joten kukin niistä on toimivaltainen selvittämään, onko henkilötietojen siirto kolmanteen maahan jäsenvaltiosta, johon kyseinen viranomainen kuuluu, mainitussa direktiivissä säädettyjen vaatimusten mukaista.

Tuomio 5.6.2018 (suuri jaosto), Wirtschaftsakademie Schleswig-Holstein (C-210/16, [EU:C:2018:388](#))

Tässä tuomiossa (ks. myös otsikko II.5 Käsité ”rekisterinpitäjä”), joka koskee muun muassa direktiivin 95/46 4 ja 28 artiklan tulkintaa, unionin tuomioistuin lausui sen toimivallan laajuudesta, joka valvontaviranomaisilla on sellaisen henkilötietojen käsittelyn osalta, johon osallistuu useita toimijoita.

Unionin tuomioistuin totesi, että silloin kun Euroopan unionin ulkopuolelle sijoittautuneella yrityksellä (kuten amerikkalaisella Facebook-yhtiöllä) on useita toimipaikkoja eri jäsenvaltioissa, jäsenvaltion valvontaviranomainen on toimivaltainen käyttämään sillä kyseisen direktiivin 28 artiklan 3 kohdan mukaan olevia toimivaltuuksia

mainitun yrityksen kyseisen jäsenvaltion alueella sijaitsevan toimipaikan osalta (nyt esillä olevassa asiassa Facebook Germany), vaikka konsernin sisäisen tehtävänjaon mukaan yhtäältä kyseinen toimipaikka vastaa vain mainospaikkojen myynnistä ja muusta markkinoinnista kyseisen jäsenvaltion alueella ja toisaalta yksinomainen vastuu henkilötietojen keräämisestä ja käsittelystä koko unionin alueella on jonkin toisen jäsenvaltion alueella sijaitsevalla toimipaikalla (nyt esillä olevassa asiassa Facebook Ireland).

Unionin tuomioistuin täsmensi lisäksi, että silloin, kun jäsenvaltion valvontaviranomainen aikoo käyttää kyseisen jäsenvaltion alueelle sijoittautuneen elimen suhteen direktiivin 95/46 28 artiklan 3 kohdassa tarkoitettuja toimintavaltuuksia sen vuoksi, että henkilötietojen käsittelystä vastuussa oleva sivullinen, jonka kotipaikka on jossakin toisessa jäsenvaltiossa (nyt esillä olevassa asiassa Facebook Ireland), on rikkonut henkilötietojen suojaa koskevia sääntöjä, kyseinen valvontaviranomainen on toimivaltainen arvioimaan viimeksi mainitun jäsenvaltion valvontaviranomaiseen nähden itsenäisesti mainittujen tietojen käsittelyn lainmukaisuutta ja voi käyttää toimintavaltuuksiaan alueelleen sijoittautuneen elimen suhteen pyytämättä ensin kyseisen toisen jäsenvaltion valvontaviranomaista toimimaan

Tuomio 15.6.2021 (suuri jaosto), Facebook Ireland ym. (C-645/19, [EU:C:2021:483](#))

Belgian yksityisyydensuojakomission puheenjohtaja nosti 11.9.2015 kieltokanteen Facebook Irelandia, Facebook Inc:tä ja Facebook Belgiumia vastaan Nederlandstalige rechtbank van eerste aanleg Brusselissa (Brysselin hollanninkielinen alioikeus, Belgia). Kanteen tarkoituksena oli saada lopetetuksi Facebookin väitetyt tietosuojalainsäädännön rikkomiset. Nämä rikkomiset muodostuivat erityisesti belgialaisten internetin käyttäjien – sekä Facebook-tilin haltijoiden että henkilöiden, joilla ei tällaista tiliä ole – selailukäyttäytymistä koskevien tietojen keräämisestä ja käyttämisestä evästeiden, yhteisöliitännäisten¹⁰⁵ tai jäljitteiden kaltaisten tekniikoiden avulla.

Kyseinen tuomioistuin totesi 16.2.2018 olevansa toimivaltainen ratkaisemaan mainitun kanteen ja totesi asiakysymyksen osalta, että verkkoyhteisö Facebook ei ollut tiedottanut riittävällä tavalla belgialaisille internetin käyttäjille kyseessä olevien tietojen keräämisestä ja käytöstä. Internetin käyttäjien kyseisten tietojen keräämiseen ja käsittelyyn antama suostumus katsottiin lisäksi pätemättömäksi.

Facebook Ireland, Facebook Inc. ja Facebook Belgium valittivat tästä tuomiosta 2.3.2018 hof van beroep te Brusseliin (Brysselin ylioikeus, Belgia), joka on tässä asiassa ennakkoratkaisupyynnön esittänyt tuomioistuin. Belgian tietosuojaviranomainen (GBA) toimi kyseisessä tuomioistuimessa kieltokanteen nostaneen

¹⁰⁵ Esimerkiksi painikkeet ”tykkää” tai ”jaa”.

yksityisyydensuojakomission puheenjohtajan laillisena seuraajana. Ennakkoratkaisua pyytänyt tuomioistuin totesi olevansa toimivaltainen ratkaisemaan valituksen ainoastaan Facebook Belgiumia koskevilta osin.

Ennakkoratkaisua pyytäneellä tuomioistuimella on epäilyjä yleisessä tietosuoja-asetuksessa¹⁰⁶ säädetyn ”yhden luukun” järjestelmän soveltamisen vaikutuksesta GBA:n toimivaltaan, ja se pohtii erityisesti kysymystä siitä, voiko GBA 25.5.2018 jälkeen tapahtuneiden tosiseikkojen osalta nostaa kanteen Facebook Belgiumia vastaan, kun Facebook Ireland on yksilöity kyseisten tietojen osalta rekisterinpitäjäksi. Kyseisestä ajankohdasta lähtien ja yleisessä tietosuoja-asetuksessa säädetyn ”yhden luukun” periaatteen nojalla vaikuttaa näet siltä, että ainoastaan Irlannin tietosuojavaltuutettu olisi toimivaltainen nostamaan kieltokanteen Irlannin tuomioistuinten.

Unionin tuomioistuimen suuri jaosto täsmentää tuomiossaan kansallisten valvontaviranomaisten valtuudet yleisen tietosuoja-asetuksen puitteissa. Se katsoo erityisesti, että tässä asetuksessa sallitaan tietyin edellytyksin se, että jäsenvaltion valvontaviranomainen käyttää valtuuksiaan saattaa kaikki yleisen tietosuoja-asetuksen väitetyt rikkomiset tämän valtion tuomioistuimen tietoon ja tarvittaessa panna vireille tai käynnistää muulla tavoin oikeustoimet siltä osin kuin kyse on rajatylittävästä tietojenkäsittelystä,¹⁰⁷ vaikka se ei ole johtava valvontaviranomainen tämän käsittelyn osalta.

Unionin tuomioistuin täsmentää ensiksi edellytykset, joita noudattaen kansallisen valvontaviranomaisen, joka ei ole johtava valvontaviranomainen rajatylittävän tietojenkäsittelyn osalta, on käytettävä valtuuksiaan saattaa kaikki yleisen tietosuoja-asetuksen väitetyt rikkomiset jäsenvaltion tuomioistuimen tietoon ja tarvittaessa panna vireille tai käynnistää muulla tavoin oikeustoimet tämän asetuksen soveltamisen varmistamiseksi. Niinpä yhtäältä yleisessä tietosuoja-asetuksessa on annettava tälle valvontaviranomaiselle toimivalta tehdä päätös, jossa todetaan mainitun käsittelyn olevan asetuksen sääntöjen vastaista, ja toisaalta näitä valtuuksia on käytettävä mainitussa asetuksessa säädettyjä yhteistyö- ja yhdenmukaisuusmenettelyjä noudattaen.¹⁰⁸

Yleisessä tietosuoja-asetuksessa säädetään nimittäin ”yhden luukun” järjestelmästä,¹⁰⁹ joka perustuu toimivallan jakoon johtavan valvontaviranomaisen ja muiden osallistuvien kansallisten valvontaviranomaisten välillä. Tämä järjestelmä edellyttää näiden viranomaisten välistä tiivistä, lojaalia ja tehokasta yhteistyötä henkilötietojen suojelua koskevien sääntöjen johdonmukaisen ja yhtenäisen soveltamisen varmistamiseksi ja tämän järjestelyn tehokkaan vaikutuksen säilyttämiseksi. Yleisessä tietosuoja-

¹⁰⁶ Yleisen tietosuoja-asetuksen 56 artiklan 1 kohdassa säädetään seuraavaa: ”Rekisterinpitäjän tai henkilötietojen käsittelijän päätoimipaikan tai ainoan toimipaikan valvontaviranomaisella on toimivalta toimia johtavana valvontaviranomaisena kyseisen rekisterinpitäjän tai henkilötietojen käsittelijän toteuttaman rajatylittävän käsittelyn osalta – –, sanotun kuitenkin rajoittamatta 55 artiklan soveltamista.”

¹⁰⁷ Yleisen tietosuoja-asetuksen 4 artiklan 23 kohta.

¹⁰⁸ Yleisen tietosuoja-asetuksen 56 ja 60 artikla.

¹⁰⁹ Yleisen tietosuoja-asetuksen 56 artiklan 1 kohta.

asetuksessa annetaan johtavalle valvontaviranomaiselle lähtökohtainen toimivalta tehdä päätös, jossa todetaan, että rajatylittävällä käsittelyllä rikotaan tässä asetuksessa vahvistettuja sääntöjä,¹¹⁰ kun taas poikkeuksena on muiden osallistuvien valvontaviranomaisten toimivalta tehdä tällainen päätös, edes väliaikainen.¹¹¹ Johtava valvontaviranomainen ei toimivaltaansa käyttäessään kuitenkaan voi laiminlyödä välttämätöntä vuoropuhelua sekä lojaalia ja tehokasta yhteistyötä muiden osallistuvien valvontaviranomaisten kanssa. Näin ollen johtava valvontaviranomainen ei voi tämän yhteistyön puitteissa jättää muiden osallistuvien valvontaviranomaisten näkemyksiä huomiotta, ja jos jokin viimeksi mainituista viranomaisista esittää merkityksellisen ja perustellun vastalauseen, johtavan valvontaviranomaisen päätösehdotuksen hyväksyminen estyy ainakin väliaikaisesti.

Unionin tuomioistuimien täsmentää lisäksi, että se, että jäsenvaltion valvontaviranomainen, joka ei ole rajatylittävän tietojenkäsittelyn osalta johtava valvontaviranomainen, voi käyttää valtuuksiaan saattaa kaikki tämän asetuksen väitetyt rikkomiset tämän valtion tuomioistuimen tietoon ja panna vireille oikeustoimet vain sillä edellytyksellä, että noudatetaan johtavan valvontaviranomaisen ja muiden valvontaviranomaisten välisen päätöksentekotoimivallan jakamista koskevia sääntöjä,¹¹² on yhteensopivaa Euroopan unionin perusoikeuskirjan 7, 8 ja 47 artiklan kanssa, joissa taataan rekisteröidylle oikeus henkilötietojensa suojaan ja oikeus tehokkaisiin oikeussuojakeinoihin.

Unionin tuomioistuimien katsoo toiseksi, että rajatylittävän tietojenkäsittelyn tilanteessa jäsenvaltion valvontaviranomaisen, joka ei ole johtava valvontaviranomainen, oikeudellisen menettelyn vireille panemista koskevien valtuuksien käyttäminen¹¹³ ei edellytä, että henkilötietojen rajatylittävää käsittelyä suorittavan rekisterinpitäjän tai henkilötietojen käsittelijän, jota vastaan kyseinen oikeudellinen menettely pannaan vireille, päätoimipaikka tai muu toimipaikka on tämän jäsenvaltion alueella. Näiden valtuuksien käyttämisen on kuitenkin kuuluttava yleisen tietosuoja-asetuksen alueelliseen soveltamisalaan,¹¹⁴ mikä edellyttää, että rajatylittävää käsittelyä suorittavalla rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka unionin alueella.

Unionin tuomioistuimien toteaa kolmanneksi, että rajatylittävän tietojenkäsittelyn tilanteessa jäsenvaltion valvontaviranomaisen, joka ei ole johtava valvontaviranomainen, valtuuksia, jotka koskevat yleisen tietosuoja-asetuksen väitettyjen rikkomisten saattamista tämän valtion tuomioistuimen tietoon ja tarvittaessa oikeustoimien vireille panemista tai muulla tavoin käynnistämistä, voidaan käyttää sekä rekisterinpitäjän päätoimipaikkaa, joka sijaitsee tämän viranomaisen omassa jäsenvaltiossa, vastaan että

¹¹⁰ Yleisen tietosuoja-asetuksen 60 artiklan 7 kohta.

¹¹¹ Yleisen tietosuoja-asetuksen 56 artiklan 2 kohdassa ja 66 artiklassa säädetään johtavan valvontaviranomaisen päätöksentekotoimivallan periaatteesta tehtävistä poikkeuksista.

¹¹² Yleisen tietosuoja-asetuksen 55 ja 56 artikla, luettuina yhdessä asetuksen 60 artiklan kanssa.

¹¹³ Yleisen tietosuoja-asetuksen 58 artiklan 5 kohdan nojalla.

¹¹⁴ Yleisen tietosuoja-asetuksen 3 artiklan 1 kohdassa säädetään, että "tätä asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei".

tämän rekisterinpitäjän muuta toimipaikkaa vastaan, jos oikeudellinen menettely koskee tietojenkäsittelyä, joka suoritetaan tässä toimipaikassa tapahtuvan toiminnan yhteydessä, ja mainitulla viranomaisella on toimivalta käyttää näitä valtuuksia.

Unionin tuomioistuin täsmentää, että näiden valtuuksien käyttäminen edellyttää kuitenkin, että yleinen tietosuoja-asetus on sovellettavissa. Käsiteltävässä asiassa Facebook-konsernin Belgiassa sijaitsevan toimipaikan toimintojen on katsottava liittyvän erottamattomasti pääasiassa kyseessä olevaan henkilötietojen käsittelyyn, jonka osalta Facebook Ireland on unionin alueella rekisterinpitäjä. On siis katsottava, että tällainen käsittely suoritetaan rekisterinpitäjän toimipaikassa tapahtuvan toiminnan yhteydessä ja se kuuluu siis yleisen tietosuoja-asetuksen soveltamisalaan.

Unionin tuomioistuin katsoo neljänneksi, että kun jäsenvaltion valvontaviranomainen, joka ei ole johtava valvontaviranomainen, on pannut vireille henkilötietojen rajatylittävää käsittelyä koskevan oikeudellisen menettelyn ennen kuin yleinen tietosuoja-asetus tuli voimaan, tätä menettelyä voidaan unionin oikeuden näkökulmasta jatkaa niiden säännösten perusteella, joista säädetään tietosuojadirektiivissä, jota sovelletaan edelleen siinä säädettyjen sääntöjen rikkomisiin, jotka on tehty kyseisen direktiivin kumoamisajankohtaan mennessä. Tämä viranomainen voi lisäksi panna vireille mainitun menettelyn yleisen tietosuoja-asetuksen voimaantuloajankohdan jälkeen tehdyistä rikkomisista, jos kyseessä on jokin niistä tilanteista, joissa kyseisessä asetuksessa poikkeuksellisesti annetaan tälle samalle viranomaiselle toimivalta tehdä päätös, jossa todetaan kyseessä olevan tietojenkäsittelyn olevan vastoin mainitun asetuksen sääntöjä, ja edellyttäen, että samassa asetuksessa säädettyjä yhteistyö- ja yhdenmukaisuusmenettelyjä noudatetaan.

Unionin tuomioistuin toteaa viidenneksi ja viimeiseksi, että yleisen tietosuoja-asetuksen säännöksellä, jonka mukaan kunkin jäsenvaltion on säädettävä laissa siitä, että sen valvontaviranomaisella on valtuudet saattaa tämän asetuksen rikkomiset lainkäyttöviranomaisten tietoon ja tarvittaessa panna vireille tai käynnistää muulla tavoin oikeustoimet, on välitön oikeusvaikutus. Näin ollen kansallinen valvontaviranomainen voi vedota mainittuun säännökseen pannakseen vireille oikeudellisen menettelyn yksityisiä vastaan tai jatkaakseen sitä, vaikka tätä säännöstä ei olisi nimenomaisesti pantu täytäntöön asianomaisen jäsenvaltion lainsäädännössä.

Tuomio 16.1.2024 (suuri jaosto), Österreichische Datenschutzbehörde (C-33/22, [EU:C:2024:46](#))

Kyseisessä tuomiossa (ks. myös otsikko II.1. ”Yleisen säännösten soveltamisala”) unionin tuomioistuin totesi, että yleisen tietosuoja-asetuksen säännökset, jotka koskevat kansallisten valvontaviranomaisten toimivaltaa ja oikeutta tehdä kantelu,¹¹⁵ eivät edellytä kansallisten täytäntöönpanotoimenpiteiden toteuttamista ja ne ovat riittävän

¹¹⁵ Yleisen tietosuoja-asetuksen 55 artiklan 1 kohta ja 77 artiklan 1 kohta.

selkeitä, täsmällisiä ja ehdottomia, jotta niillä voidaan katsoa olevan välitön oikeusvaikutus. Tästä seuraa, että vaikka yleisessä tietosuoja-asetuksessa jätetään jäsenvaltioille harkintavaltaa sen suhteen, kuinka monta valvontaviranomaista luodaan,¹¹⁶ siinä vahvistetaan niiden yleisen tietosuoja-asetuksen soveltamisen valvontaa koskevan toimivallan laajuus. Jos jäsenvaltio päättää perustaa yhden ainoan valvontaviranomaisen, tälle on välttämättä annettava kaikki se toimivalta, josta kyseisessä asetuksessa säädetään. Muunlainen tulkinta kyseenalaistaisi kyseisten säännösten tehokkaan vaikutuksen ja saattaisi heikentää kaikkien yleisten tietosuoja-asetuksen sellaisten muiden säännösten tehokasta vaikutusta, joita kantelu voi koskea.

Unionin tuomioistuimien korosti siitä seikasta, että perustuslaintasoisissa kansallisissa säännöksissä suljetaan pois valvontaviranomaisen, joka on osa toimeenpanovaltaa, mahdollisuus valvoa sitä, miten lainsäädäntövaltaan kuuluva elin soveltaa yleistä tietosuoja-asetusta, että yleisessä tietosuoja-asetuksessa vaaditaan jäsenvaltioilta juuri niiden perustuslakia kunnioittaen ainoastaan, että ne perustavat ainakin yhden valvontaviranomaisen, samalla kun siinä annetaan niille mahdollisuus perustaa useampia valvontaviranomaisia. Kyseisessä asetuksessa jokaiselle jäsenvaltiolle annetaan siis harkintavaltaa, jonka nojalla se voi perustaa juuri niin monta valvontaviranomaista kuin muun muassa sen perustuslakiin liittyvät vaatimukset edellyttävät.

Se, että jäsenvaltio vetoaa kansallisen oikeuden säännöksiin, ei myöskään saa vahingoittaa unionin oikeuden yhtenäisyyttä ja tehokkuutta. Unionin oikeuden ensisijaisuuden periaatteen vaikutukset näet koskevat kaikkia jäsenvaltion elimiä kansallisten säännösten – mukaan lukien perustuslaintasoiset säännökset – voimatta tätä estää.

Jos jäsenvaltio on harkintavaltansa puitteissa päättänyt perustaa yhden ainoan valvontaviranomaisen, se ei siis voi vedota kansallisen oikeuden säännöksiin – vaikka ne olisivatkin perustuslaintasoisia – jättääkseen yleisen tietosuoja-asetuksen soveltamisalaan kuuluvan henkilötietojen käsittelyn kyseisen valvontaviranomaisen valvonnan ulkopuolelle.

4. Hallinnollisten seuraamusmaksujen määräämisedellytykset

Tuomio 5.12.2023 (suuri jaosto), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

Kyseisessä asiassa (ks. myös otsikot II.3. Käsité ”henkilötietojen käsittely”, II.5. Käsité ”rekisterinpitäjä” ja II.6. Käsité ”yhteisrekisterinpitäjä”) unionin tuomioistuimien totesi, että yleisen tietosuoja-asetuksen 83 artiklan nojalla hallinnollinen seuraamusmaksu voidaan

¹¹⁶ Yleisen tietosuoja-asetuksen 51 artiklan 1 kohdan mukaisesti.

määrätä rekisterinpitäjälle yksinomaan, jos se on tahallisesti tai tuottamuksellisesti rikkonut kyseisen asetuksen säännöksiä.¹¹⁷

Unionin tuomioistuin täsmentää tältä osin, että unionin lainsäätäjä ei ole jättänyt jäsenvaltioille harkintavaltaa niiden aineellisten edellytysten osalta, joita valvontaviranomaisen on noudatettava, kun se päättää määrätä rekisterinpitäjälle hallinnollisen seuraamusmaksun kyseisen säännöksen nojalla. Se, että yleisessä tietosuoja-asetuksessa annetaan jäsenvaltioille mahdollisuus säätää poikkeuksista suhteessa viranomaisiin ja julkishallinnon elimiin kyseisissä jäsenvaltioissa¹¹⁸ ja vaatimuksista, jotka koskevat sitä menettelyä, jota valvontaviranomaisten on noudatettava hallinnollista seuraamusmaksua määrätessään,¹¹⁹ ei merkitse millään tavalla sitä, että jäsenvaltioilla olisi myös toimivalta säätää tällaisista aineellisista edellytyksistä.

Unionin tuomioistuin huomauttaa näistä edellytyksistä, että niihin yleisessä tietosuoja-asetuksessa lueteltuihin seikkoihin, joiden valossa valvontaviranomainen määrää rekisterinpitäjälle hallinnollisen seuraamusmaksun, kuuluu ”rikkomuksen tahallisuus tai tuottamuksellisuus”.¹²⁰ Sitä vastoin mikään kyseisessä säännöksessä luetelluista seikoista ei viittaa minkäänlaiseen mahdollisuuteen saattaa rekisterinpitäjä vastuuseen, jos rekisterinpitäjä ei ole toiminut tuottamuksellisesti. Ainoastaan rekisterinpitäjän tahallisesti tai tuottamuksellisesti tekemät yleisen tietosuoja-asetuksen säännösten rikkomiset voivat johtaa hallinnollisen seuraamusmaksun määräämiseen rekisterinpitäjälle kyseisen asetuksen 83 artiklan nojalla.

Unionin tuomioistuin lisää, että yleisen tietosuoja-asetuksen yleinen rakenne ja tarkoitus tukevat tätä tulkintaa. Se täsmentää tässä yhteydessä, että yleisen tietosuoja-asetuksen mukaisen seuraamusjärjestelmän olemassaolo, joka mahdollistaa hallinnollisen seuraamusmaksun määräämisen kunkin tapauksen erityisten olosuhteiden perusteella, luo rekisterinpitäjille ja henkilötietojen käsittelijöille kannustimen noudattaa kyseistä asetusta, ja että hallinnollisilla seuraamusmaksuilla tehostetaan kyseessä olevien henkilöiden suojelua niiden varoittavan vaikutuksen avulla. Unionin lainsäätäjä ei kuitenkaan ole pitänyt tällaisen korkeatasoisen suojan varmistamiseksi tarpeellisena säätää hallinnollisten seuraamusmaksujen määräämisestä myös silloin, kun kyse ei ole tuottamuksesta. Kun otetaan huomioon se, että yleisellä tietosuoja-asetuksella pyritään yhdenmukaiseen ja yhtenäiseen tietosuojan tasoon ja että sitä on tätä varten sovellettava johdonmukaisesti koko unionissa, olisi tämän tavoitteen vastaista antaa jäsenvaltioille mahdollisuus säätää tällaisesta järjestelmästä seuraamusmaksun määräämisen osalta.

¹¹⁷ Yleisen tietosuoja-asetuksen 83 artiklan 4–6 kohdassa tarkoitettulla tavalla.

¹¹⁸ Yleisen tietosuoja-asetuksen 83 artiklan 7 kohdan nojalla, jonka mukaan ”kukin jäsenvaltio voi asettaa sääntöjä siitä, voidaanko viranomaisille tai julkishallinnon elimille määrätä kyseisessä jäsenvaltiossa hallinnollisia seuraamusmaksuja ja missä määrin –”.

¹¹⁹ Yleisen tietosuoja-asetuksen 83 artiklan 8 kohdan, luettuna yhdessä sen 129 perustelukappaleen kanssa, nojalla.

¹²⁰ Yleisen tietosuoja-asetuksen 83 artiklan 2 kohdan b alakohhta.

Unionin tuomioistuimien päätteelee lisäksi, että tällainen seuraamusmaksu voidaan määrätä rekisterinpitäjälle henkilötietojen käsittelijän sen lukuun suorittamien henkilötietojen käsittelytoimien osalta, paitsi jos näiden toimien yhteydessä henkilötietojen käsittelijä on käsitellyt henkilötietoja omia tarkoituksiaan varten tai se on käsitellyt henkilötietoja vastoin rekisterinpitäjän määrittämiä ohjeita tai käsittelytapoja taikka sellaisella tavalla, ettei voida kohtuudella katsoa, että rekisterinpitäjä on antanut siihen suostumuksensa. Tässä tilanteessa henkilötietojen käsittelijää on pidettävä tällaisen käsittelyn suhteen rekisterinpitäjänä.

Tuomio 5.12.2023 (suuri jaosto), Deutsche Wohnen (C-807/21, [EU:C:2023:950](#))

Deutsche Wohnen SE (jäljempänä DW) on kiinteistöyhtiö, joka omistaa välillisesti eri yhtiöissä omistamiensa yhtiöosuuksien välityksellä useita liike- ja asuinhuoneistoja. Se käsittelee liiketoimintansa yhteydessä kyseisten huoneistojen vuokralaisten henkilötietoja.

Kahden paikalla vuosina 2017 ja 2019 tehdyn tarkastuksen jälkeen Berliner Beauftragte für den Datenschutz (tietosuojasta Berliinissä vastaava viranomainen) totesi useita yleisen tietosuojasetuksen rikkomisia, joihin DW oli syyllistynyt. Tietosuojaviranomainen määräsi 30.10.2019 tekemällään päätöksellä DW:lle tämän vuoksi hallinnollisen seuraamusmaksun.

DW nosti kyseisestä päätöksestä kanteen Landgericht Berlinissä (Berliinin alueellinen alioikeus, Saksa), joka tämän jälkeen lopetti menettelyn. Kyseinen tuomioistuin totesi, että Saksan lain¹²¹ mukaan ainoastaan luonnollisen henkilön, eikä oikeushenkilön, voidaan todeta syyllistyneen hallinnolliseen rikkomukseen. Lisäksi oikeushenkilön voidaan katsoa olevan vastuussa ainoastaan sen hallintoelimiin kuuluvan tai sitä edustavan henkilön toimista. Staatsanwaltschaft Berlin (Berliinin syyttäväviranomainen, Saksa) valitti kyseisestä ratkaisusta Kammergericht Berliniin (Berliinin osavaltion ylioikeus, Saksa). Tässä yhteydessä kyseinen tuomioistuin esitti unionin tuomioistuimelle ennakkoratkaisupyyntönsä yleisen tietosuojasetuksen tulkinnasta.

Unionin tuomioistuimen suuri jaosto otti tuomiossaan kantaa yleisen tietosuojasetuksen mukaisten hallinnollisten seuraamusmaksujen määrittämisen edellytyksiin. Ensinnäkin se tarkasteli kysymystä siitä, voivatko jäsenvaltiot asettaa oikeushenkilölle määrättävän hallinnollisen seuraamusmaksun edellytykseksi sen, että kyseisen asetuksen rikkominen luetaan ensin yksilöidyn luonnollisen henkilön syyksi. Toiseksi se tarkasteli, samoin kuin tuomiossa Nacionalinis visuomenès sveikatos centros (ks. edellä), kysymystä siitä, onko yleisen tietosuojasetuksen säännösten rikkomisen, josta on määrätty seuraamus, oltava tahallista tai tuottamuksellista.

¹²¹ Hallinnollisista rikkomuksista 24.5.1968 annettu laki (Gesetz über Ordnungswidrigkeiten) (BGBl. 1968 I, s. 481), sellaisena kuin se on 19.2.1987 julkaistussa tiedonannossa (BGBl. 1987 I, s. 602), sellaisena kuin se on muutettuna 19.6.2020 annetulla lailla (BGBl. 2020 I, s. 1350).

Siltä osin kuin on kyse hallinnollisen seuraamusmaksun määräämisestä oikeushenkilölle yleisen tietosuoja-asetuksen nojalla, unionin tuomioistuin totesi aluksi, että yleisessä tietosuoja-asetuksessa säädetyt periaatteet, kiellot ja velvoitteet koskevat erityisesti ”rekisterinpitäjää”, jonka vastuu ulottuu kaikkeen henkilötietojen käsittelyyn, jota ne suorittavat itse tai joka suoritetaan niiden puolesta. Juuri tämä vastuu muodostaa yleisen tietosuoja-asetuksen säännösten rikkomisen tapauksessa perustan hallinnollisen seuraamusmaksun määräämiselle rekisterinpitäjälle kyseisen asetuksen 83 artiklan nojalla. Unionin lainsäätäjä ei ole kuitenkaan ole tehnyt kyseisen asetuksen mukaisen vastuun määrittämiseksi eroa luonnollisten henkilöiden ja oikeushenkilöiden välillä, vaan tämän vastuun edellytyksenä on ainoastaan se, että kyseiset henkilöt yksin tai yhdessä toisten kanssa määrittävät henkilötietojen käsittelyn tarkoituksen ja keinot.¹²² Näin ollen lähtökohtaisesti kaikki kyseisen edellytyksen täyttävät henkilöt vastaavat kaikista yleisen tietosuoja-asetuksen rikkomisista, joihin ne ovat syyllistyneet itse tai joihin on syyllistytty niiden puolesta. Tämä merkitsee yhtäältä sitä, että oikeushenkilöt ovat vastuussa paitsi niiden edustajien, johtajien tai hallintoelimen jäsenten tekemistä rikkomuksista myös kaikkien muiden henkilöiden, jotka toimivat kyseisten oikeushenkilöiden liiketoiminnan yhteydessä ja niiden lukuun, tekemistä rikkomuksista. Toisaalta yleisen tietosuoja-asetuksen 83 artiklassa tällaisista rikkomuksista säädetyt hallinnolliset seuraamusmaksut on voitava määrätä suoraan oikeushenkilöille, jos niitä voidaan pitää kyseessä olevina rekisterinpitäjinä.

Unionin tuomioistuin huomautti tämän jälkeen, että minkään yleisen tietosuoja-asetuksen säännöksen perusteella ei voida katsoa, että hallinnollisen seuraamusmaksun määrääminen oikeushenkilölle rekisterinpitäjänä edellyttäisi sitä, että ensin todettaisiin, että tähän rikkomiseen on syyllistynyt yksilöity luonnollinen henkilö. Unionin lainsäätäjä ei myöskään ole jättänyt jäsenvaltioille tältä osin harkintavaltaa. Se, että yleisessä tietosuoja-asetuksessa annetaan jäsenvaltioille mahdollisuus säätää vaatimuksista, jotka koskevat menettelyä, jonka mukaisesti valvontaviranomaiset voivat määrätä hallinnollisen seuraamusmaksun,¹²³ ei merkitse sitä, että niillä olisi myös toimivalta säätää yleisessä tietosuoja-asetuksessa määrättyihin edellytyksiin nähden ylimääräisistä aineellisista edellytyksistä.

Unionin tuomioistuin täsmensi tältä osin, että se, että jäsenvaltioiden sallittaisiin edellyttää yksipuolisesti ja välttämättömänä edellytyksenä hallinnollisen seuraamusmaksun määräämiselle yleisen tietosuoja-asetuksen 83 artiklan nojalla rekisterinpitäjälle, joka on oikeushenkilö, että kyseessä oleva rikkominen on ensin luettava tai voitava lukea yksilöidyn luonnollisen henkilön syyksi, olisi yleisen tietosuoja-asetuksen tämän tarkoituksen vastaista. Lisäksi tällaisella lisävaatimuksella saatettaisiin viime kädessä heikentää rekisterinpitäjinä toimiville oikeushenkilöille määrättyjen hallinnollisten seuraamusmaksujen tehokkuutta ja varoittavaa vaikutusta.

¹²² Yleisen tietosuoja-asetuksen 4 artiklan 7 kohta.

¹²³ Kuten yleisen tietosuoja-asetuksen 58 artiklan 4 kohdasta ja 83 artiklan 8 kohdasta, luettuna asetuksen 129 perustelukappaleen valossa, ilmenee.

Lopuksi unionin tuomioistuin korosti, että SEUT 101 ja SEUT 102 artiklassa¹²⁴ tarkoitetulla yrityksen käsitteellä ei ole vaikutusta siihen, voidaanko hallinnollinen sakko määrätä yleisen tietosuoja-asetuksen nojalla rekisterinpitäjälle, joka on oikeushenkilö, ja millä edellytyksillä sillä on merkitystä ainoastaan määritettäessä tällaisen sakon määrää.

Näin ollen unionin tuomioistuin totesi, että yleinen tietosuoja-asetus¹²⁵ on esteenä kansalliselle säännöstölle, jonka mukaan oikeushenkilölle voidaan rekisterinpitäjän ominaisuudessaan määrätä hallinnollinen seuraamusmaksu kyseisen asetuksen rikkomisesta¹²⁶ vain, jos rikkominen on aiemmin luettu yksilöidyn luonnollisen henkilön syyksi.

Siitä, voivatko jäsenvaltiot säätää hallinnollisen seuraamusmaksun määräämisestä silloinkin, kun rikkominen, josta on määrätty seuraamus, ei ole tahallista tai tuottamuksellista, unionin tuomioistuin muistutti aluksi, että aineelliset edellytykset, joita valvontaviranomaisen on noudatettava määrätessään tällaisen seuraamusmaksun rekisterinpitäjälle, kuuluvat yksinomaan unionin oikeuden soveltamisalaan, ja että jäsenvaltioilla ei ole tältä osin lainkaan harkintavaltaa. Noudattaen samanlaista päättelyä kuin edellä mainitussa tuomiossa *Nacionalinis visuomenės sveikatos centras* unionin tuomioistuin totesi, että yleisen tietosuoja-asetuksen 83 artiklan nojalla voidaan määrätä hallinnollinen seuraamusmaksu yksinomaan, jos osoitetaan, että rekisterinpitäjä, joka on oikeushenkilö ja yritys, on syylistynyt tahallaan tai tuottamuksellisesti kyseiseen asetukseen sisältyvien sääntöjen rikkomiseen.

5. Kansallisten valvontaviranomaisten toimivallan suhde muiden kansallisten viranomaisten toimivaltaan

Tuomio 4.7.2023 (suuri jaosto), Meta Platforms ym. (Yhteisöpalvelun yleiset käyttöehdot) (C-252/21, [EU:C:2023:537](#))

Tässä asiassa (ks. myös otsikko V.5. ”Henkilötietojen käsittely verkkoyhteisöpalveluissa”) unionin tuomioistuin lausui kilpailuviranomaisen toimivallasta todeta henkilötietojen käsittelyn olevan yleisen tietosuoja-asetuksen vastaista ja totesi, että tällainen viranomaisen voi sillä edellytyksellä, että se noudattaa henkilötietojen suojasta vastaavien viranomaisten kanssa tehtävää vilpittöntä yhteistyötä koskevaa velvollisuuttaan¹²⁷, todeta tutkiessaan, onko yritys väärinkäyttänyt määräävää asemaa,¹²⁸ että kyseisen yrityksen laatimat henkilötietojen käsittelyä koskevat yleiset käyttöehdot ja niiden soveltaminen eivät ole yleisen tietosuoja-asetuksen mukaisia, jos tällainen toteamus on tarpeen tällaisen väärinkäytön toteamiseksi. Kun kansallinen

¹²⁴ Johon yleisen tietosuoja-asetuksen 150 perustelukappaleessa viitataan.

¹²⁵ Yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan i alakohhta ja 83 artiklan 1–6 kohta.

¹²⁶ Yleisen tietosuoja-asetuksen 83 artiklan 4–6 kohta.

¹²⁷ Vahvistettu SEU 4 artiklan 3 kohdassa.

¹²⁸ SEUT 102 artiklassa tarkoitetussa merkityksessä.

kilpailuviranomainen toteaa määräävän aseman väärinkäytön toteamisen yhteydessä, että yleistä tietosuojasetusta on rikottu, se ei kuitenkaan korvaa valvontaviranomaisia.

Kun otetaan huomioon vilpittömyyden yhteistyötä koskeva periaate, on siis niin, että kun kilpailuviranomaisten on tehtäviensä hoitamisen yhteydessä tutkittava, onko yrityksen käyttäytyminen yleisen tietosuojasetuksen säännösten mukaista, niiden on sovittava toimintansa yhteen osallistuvien kansallisten valvontaviranomaisten tai johtavan valvontaviranomaisen kanssa ja tehtävä vilpittömyyden yhteistyötä niiden kanssa. Kaikkien näiden viranomaisten on siis toimittava omien valtuuksiensa ja toimivaltansa puitteissa, jotta sekä yleisestä tietosuojasetuksesta johtuvia velvoitteita että kyseisen asetuksen tavoitteita noudatetaan ja niiden tehokas vaikutus säilytetään. Tästä seuraa, että jos kilpailuviranomainen katsoo tutkinnan, jonka tarkoituksena on todeta, onko yritys väärinkäyttänyt määräävää asemaa, yhteydessä, että on välttämätöntä tutkia, onko mainitun yrityksen käyttäytyminen yleisen tietosuojasetuksen säännösten mukaista, tämän viranomaisen on selvitettävä, onko toimivaltainen kansallinen valvontaviranomainen tai johtava valvontaviranomainen taikka unionin tuomioistuin jo tutkinut kyseistä käyttäytymistä tai samankaltaista käyttäytymistä tai tehnyt tällaista käyttäytymistä koskevan ratkaisun. Jos asia on näin, kilpailuviranomainen ei voi poiketa siitä, mutta se voi vapaasti tehdä sen perusteella omat päätelmänsä kilpailuoikeuden soveltamisen näkökulmasta.

Jos kansallisella kilpailuviranomaisella on epäilyjä toimivaltaisen kansallisen valvontaviranomaisen tai johtavan valvontaviranomaisen toteuttaman arvioinnin ulottuvuudesta, jos kyseiset viranomaiset tutkivat samaan aikaan asianomaista käyttäytymistä tai samankaltaista käyttäytymistä tai jos mainittujen viranomaisten tutkinnan puuttuessa kilpailuviranomainen katsoo, että yrityksen käyttäytyminen ei ole yleisen tietosuojasetuksen säännösten mukaista, kansallisen kilpailuviranomaisen on kuultava kyseistä viranomaista ja pyydettävä niitä tekemään yhteistyötä epäilyjensä poistamiseksi tai sen määrittämiseksi, onko odotettava asianomaisen valvontaviranomaisen päätöstä ennen kuin se tekee oman arvionsa. Jos ne eivät vastusta asiaa tai eivät vastaa kohtuullisen määräajan kuluessa, kilpailuviranomainen voi jatkaa omaa tutkintaansa.



EUROOPAN UNIONIN
TUOMIOISTUIN

Tutkimus ja dokumentaatio-osasto

Heinäkuu 2024