



Aiheenmukainen tutkimusmuistio

HENKILÖTIETOJEN SUOJA

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

Tämä oikeus vahvistetaan Euroopan unionin perusoikeuskirjassa (jäljempänä perusoikeuskirja), jonka 8 artiklassa määrätään seuraavaa:

”1. Jokaisella on oikeus henkilötietojensa suojaan.

2. Tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.

3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.”

Tämä perusoikeus liittyy kiinteästi saman perusoikeuskirjan 7 artiklassa vahvistettuun oikeuteen, joka koskee yksityis- ja perhe-elämän kunnioittamista.

Henkilötietojen suojasta säädetään myös Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdassa, jolla korvattiin tältä osin EY 286 artikla.

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 perustuu EY 100 A artiklaan, oli ensisijainen unionin säädös tällä alalla.

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).

Mainitussa direktiivissä säädettiin henkilötietojen käsittelyn laillisuuden yleisistä edellytyksistä ja kyseessä olevien henkilöiden oikeuksista, ja siinä säädettiin muun muassa itsenäisten valvontaviranomaisten perustamisesta jäsenvaltioihin.

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 aikoo tarkastella tätä direktiiviä uudelleen. Tässä tarkoituksessa komissio antoi 10.1.2017 ehdotuksen kyseisen direktiivin korvaamiseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä annettavalla asetuksella.⁴

Vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen osalta (entiset SEU 30 ja SEU 31 artikla) puitepääöksellä 2008/977/YOS⁵ säänneltiin toukokuuhun 2018 asti rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamista.

Euroopan unioni uudisti vuonna 2016 kyseistä alaa koskevaa yleistä oikeudellista kehystä. Tuolloin annettiin tietosuojaa koskeva asetus (EU) 2016/679⁶ (jäljempänä yleinen tietosuojasetus), jolla kumottiin direktiivi 95/46 ja jota on sovellettu suoraan 25.5.2018 lähtien, ja direktiivi (EU) 2016/680,⁷ jolla pyritään mainittujen tietojen suojaamiseen rikosasioissa ja jolla kumotaan puitepääötös 2008/977/YOS. Määräaika direktiivin täytäntöön panemiseksi päättyi 6.5.2018.

Asetuksella (EY) N:o 45/2001⁸ puolestaan varmistettiin aluksi henkilötietojen suoja, kun niitä käsittelevät EU:n toimielimet ja elimet. Mainitun asetuksen ansiosta muun muassa luotiin vuonna 2004 Euroopan tietosuojavaltuutettu. Vuonna 2018 Euroopan unionissa kyseisellä alalla tuli voimaan uusi oikeudellinen kehys erityisesti, kun annettiin asetus (EU) 2018/1725,⁹ jolla kumotaan asetus (EY) N:o 45/2001 ja päätös N:o 1247/2002/EY¹⁰ ja jota on sovellettu 11.12.2018 lähtien. Jotta henkilötietoja suojattaisiin mahdollisimman yhdenmukaisesti unionin

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 1.1 "Unionin johdetun oikeuden yhdenmukaisuus henkilötietojen suojaa koskevan oikeuden kanssa").

⁴ Ehdotus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta annettavaksi Euroopan parlamentin ja neuvoston asetukseksi (sähköisen viestinnän tietosuojasetus), [COM/2017/010 final – 2017/03 \(COD\)](#).

⁵ Rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta 27.11.2008 tehty neuvoston puitepääötös 2008/977/YOS (EUVL 2008, L 350, s. 60), joka on kumottu 6.5.2018 lähtien (ks. alaviite 7).

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).

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 puitepääötöksen 2008/977/YOS kumoamisesta 27.4.2016 annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 (EUVL 2016, L 119, s. 89).

⁸ Yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18.12.2000 annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 (EYVL 2001, L 8, s. 1).

⁹ 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 asetus (EU) 2018/1725.

¹⁰ Euroopan tietosuojavaltuutetun tehtävien hoitamista koskevasta ohjesäännöstä ja yleisistä ehdoista 1.7.2002 annettu Euroopan parlamentin, neuvoston ja komission päätös N:o 1247/2002/EY (EYVL 2002, L 183, s. 1).

koko alueella, tällä uudella asetuksella pyritään saattamaan alaa koskevat säännöt mahdollisimman hyvin yleisellä tietosuojasetuksella luodun järjestelmän mukaisiksi.

SISÄLLYS

I. EUROOPAN UNIONIN PERUSOIKEUSKIRJASSA TUNNUSTETTU OIKEUS HENKILÖTIETOJEN SUOJAAN	5
1. Unionin johdetun oikeuden yhdenmukaisuus henkilötietojen suojaa koskevan oikeuden kanssa.....	5
2. Henkilötietojen suojaa koskevan oikeuden noudattaminen unionin oikeuden täytäntöönpanossa.....	9
II. ALAN YLEISESSÄ SÄÄNNÖSTÖSSÄ TARKOITETTU HENKILÖTIETOJEN KÄSITTELY	10
1. Direktiivin N:o 95/46 soveltamisalan ulkopuolelle jäävä henkilötietojen käsittely	10
2. Henkilötietojen käsite	13
3. Henkilötietojen käsittelyn käsite.....	15
4. Käsite ”henkilötietojen rekisteröintijärjestelmä”	20
5. Käsite ”rekisterinpitäjä”.....	20
6. Henkilötietojen käsittelyn laillisuuden edellytykset.....	23
III. DIREKTIIVISSÄ 2002/58 TARKOITETTU HENKILÖTIETOJEN KÄSITTELY	32
IV. HENKILÖTIETOJEN SIIRTÄMINEN KOLMANSIIN MAIHIN	38
V. HENKILÖTIETOJEN SUOJA INTERNETISSÄ	45
1. Oikeus vastustaa henkilötietojen käsittelyä (”oikeus tulla unohdetuksi”).....	45
2. Henkilötietojen käsittely ja immateriaalioikeudet.....	46
3. Henkilötietojen poistaminen hakutulosten luettelosta.....	50
4. Internetsivun käyttäjän suostumus tietojen tallentamiseen tai tietojen käyttämiseen evästeiden avulla.....	55
VI. KANSALLISET VALVONTAVIRANOMAISET	56
1. Riippumattomuusvaatimuksen ulottuvuus	56
2. Sovellettavan oikeuden ja toimivaltaisen valvontaviranomaisen määrittäminen	59
3. Kansallisten valvontaviranomaisten toimivalta	60
VII. UNIONIN LAINSÄÄDÄNNÖN ALUEELLINEN SOVELTAMISALA	64
VIII. YLEISÖN OIKEUS TUTUSTUA EUROOPAN UNIONIN TOIMIELINTEN ASIAKIRJOIHIN JA HENKILÖTIETOJEN SUOJA	65

I. Euroopan unionin perusoikeuskirjassa tunnustettu oikeus henkilötietojen suojaan

1. Unionin johdetun oikeuden yhdenmukaisuus henkilötietojen suojaa koskevan oikeuden kanssa

[Tuomio 9.11.2010 \(suuri jaosto\), Volker und Markus Schecke ja Eifert \(C-92/09 ja C-93/09, EU:C:2010:662\)](#)¹¹

Tässä 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 (maaloustukirahasto) (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 1290/2005¹² ja (EY) N:o 259/2008,¹³ joilla säännellään yhteisen maatalouspolitiikan rahoitusta ja joissa edellytetään maaloustukirahastosta 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 pätevydestä. Kyseessä olevilla säännöksillä edellytettiin tällaisten tietojen saattamista yleisön saataville esimerkiksi kansallisten virastojen ylläpitämien internetsivustojen välityksellä.

Unionin tuomioistuin totesi perusoikeuskirjassa tunnustetun henkilötietojen suojaa 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 yksityiselämään ja erityisesti heidän oikeuttaan henkilötietojen suojaan (56–64 kohta).

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 (65 kohta). Unionin tuomioistuin katsoi tässä yhteydessä, että vaikka demokraattisessa

¹¹ Mainittu tuomio on esitetty vuoden 2010 vuosikertomuksessa, s. 11.

¹² 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).

¹³ Asetuksen (EY) N:o 1290/2005 soveltamista koskevista yksityiskohtaisista säännöistä Euroopan maatalouden tukirahaston (maaloustukirahasto) 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).

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 (77, 79, 85 ja 86 kohta).

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 (92 kohta ja tuomiolauselman 1 kohta). 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 (94 kohta ja tuomiolauselman 2 kohta).

[Tuomio 17.10.2013, Schwarz \(C-291/12, EU:C:2013:670\)](#)

Schwarz oli pyytänyt, että Bochumin kaupunki (Saksa) myöntäisi hänelle passin mutta kieltäytyi tuossa yhteydessä kuitenkin antamasta sormenjälkiään. Koska Bochumin kaupunki hylkäsi Schwarzin pyynnön, tämä nosti kanteen Verwaltungsgericht Gelsenkirchenissä (Gelsenkirchenin hallinto-oikeus, Saksa) vaatien, että kyseinen kaupunki veloitettaisiin antamaan hänelle passi ilman, että häneltä otettaisiin sormenjäljet. Schwarz riitautti mainitussa tuomioistuimessa asetuksen (EY) N:o 2252/2004,¹⁴ jolla oli otettu käyttöön velvollisuus ottaa passin hakijoilta sormenjäljet, pätevyys. Hän väitti muun muassa, että asetuksella loukattiin oikeutta henkilötietojen suojaan ja oikeutta yksityiselämän kunnioittamiseen.

Verwaltungsgericht Gelsenkirchen esitti unionin tuomioistuimelle ennakkoratkaisupyynnön selvittääkseen, oliko kyseinen asetus pätevä, sikäli kuin sillä veloitettiin passin hakija antamaan sormenjälkensä ja säädettiin niiden säilyttämisestä passissa, erityisesti perusoikeuskirjan suhteen.

Unionin tuomioistuin totesi asetuksen päteväksi ja katsoi, että vaikka kansallisten viranomaisten menettelyllä, kun ne asetuksen N:o 2252/2004 1 artiklan 2 kohdassa säädetyin tavoin ottavat ja tallentavat sormenjäljet, loukataan oikeutta yksityiselämän kunnioittamiseen ja oikeutta henkilötietojen suojaan, tämä loukkaus on oikeutettua tavoitteella suojata passeja väärinkäytöksiltä.

Tällaisella lakisääteisellä rajoituksella ensinnäkin pyritään unionin hyväksymään yleisen edun mukaiseen tavoitteeseen, koska sen tarkoituksena on estää henkilöiden laitton saapuminen unionin alueelle (35–38 kohta). Sormenjälkien ottaminen ja tallentaminen myös soveltuvat tämän päämäärän toteuttamiseen. Yhtäältä, vaikka menetelmä, jonka mukaan henkilöllisyys

¹⁴ Jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista 13.12.2004 annettu neuvoston asetus (EY) N:o 2252/2004 (EUVL 2004, L 385, s. 1), sellaisena kuin se on muutettuna 6.5.2009 annetulla Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 444/2009 (EUVL 2009, L 142, s. 1).

todetaan sormenjälkien avulla, ei olekaan täysin luotettava, sillä vähennetään huomattavasti riskiä siitä, että maahan päästetään henkilöitä, joilla ei ole tähän lupaa. Toisaalta se, etteivät passinhaltijan sormenjäljet vastaa kyseiseen asiakirjaan sisällytettyjä tietoja, ei merkitse sitä, että asianomaiselta henkilöltä evättäisiin automaattisesti pääsy unionin alueelle, vaan siitä seuraa pelkästään, että kyseinen henkilö tarkastetaan perusteellisesti, jotta hänen henkilöllisyytensä voitaisiin varmasti todeta (42–45 kohta).

Tällaisen kohtelun tarpeellisuudesta unionin tuomioistuimien totesi, ettei sen tietoon ollut saatettu, että olemassa olisi riittävän tehokkaita toimenpiteitä, joilla loukattaisiin perusoikeuskirjan 7 ja 8 artiklassa tunnustettuja oikeuksia vähemmän kuin sormenjälkien ottamiseen pohjautuvalla menetelmällä (53 kohta). Asetuksen N:o 2252/2004 1 artiklan 2 kohdassa ei edellytetä otettuja sormenjälkiä käsiteltävän tavoin, joka menisi pidemmälle kuin kyseisen tavoitteen toteuttamiseksi on tarpeen. Mainitussa asetuksessa täsmennetään nimenomaisesti, että sormenjälkiä saadaan käyttää ainoastaan passin aitouden toteuttamiseksi ja sen haltijan henkilöllisyyden varmistamiseksi. Asetuksen 1 artiklan 2 kohdassa lisäksi varmistetaan suoja sitä riskiä vastaan, että sormenjäljet sisältäviä tietoja lukisivat henkilöt, joilla ei ole siihen lupaa, ja siinä säädetään, että sormenjäljet tallennetaan vain itse passiin, joka jää haltijansa yksinomaiseen hallintaan (54–57, 60 ja 63 kohta).

[Tuomio 8.4.2014 \(suuri jaosto\) Digital Rights Ireland ja Seitlinger ym. \(yhdistetyt asiat C-293/12 ja C-594/12, EU:C:2014:238\)](#)¹⁵

Tämä tuomio juontaa juurensa pyyntöihin arvioida tietojen säilyttämisestä annetun direktiivin 2006/24/EY pätevyyttä suhteessa perusoikeuksiin, yksityiselämän kunnioittamista koskevaan oikeuteen ja henkilötietojen suojaa koskevaan oikeuteen. Pyyntö 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 panttiin 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 kysivät 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 tyyppin 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

¹⁵ Mainittu tuomio on esitetty vuoden 2014 vuosikertomuksessa, s. 60.

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 (38–44 kohta).

Unionin tuomioistuin kuitenkin katsoi, että antaessaan tietojen säilyttämistä koskevan direktiivin unionin lainsäätäjällä 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 (65 kohta). 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 (57–59 kohta). 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 (60–62 kohta). 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 (63 ja 64 kohta).

Perusoikeuskirjan 8 artiklan 3 kohdasta aiheutuvien vaatimusten osalta unionin tuomioistuin katsoi, ettei direktiivissä säädetä riittävästä takeista, joilla voidaan varmistaa säilytettyjen tietojen tehokas suoja väärinkäytön vaaraa vastaan sekä näiden tietojen kaikenlaista laitonta 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 (66–68 kohta).

2. Henkilötietojen suojaa koskevan oikeuden noudattaminen unionin oikeuden täytäntöönpanossa

[Tuomio 21.12.2016 \(suuri jaosto\) Tele2 Sverige \(yhdistetyt asiat C-203/15 ja C-698/15, EU:C:2016:970\)](#)¹⁶

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 paikkatietojen 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 (99–105, 107 ja 112 kohta sekä tuomiolauselman 1 kohta).

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 suojaa ja turvaa, erityisesti toimivaltaisten kansallisten viranomaisten oikeutta

¹⁶ Mainittu tuomio on esitetty vuoden 2016 vuosikertomuksessa, s. 62.

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 ennakovalvontaa, eikä vaadita, että kyseessä olevat tiedot säilytetään unionin alueella (118–122 ja 125 kohta sekä tuomiolauselman 2 kohta).

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 säännöstön 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 säännöstön 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 (108–111 kohta).

II. Alan yleisessä säännöstössä tarkoitettu henkilötietojen käsittely

1. Direktiivin N:o 95/46 soveltamisalan ulkopuolelle jäävä henkilötietojen käsittely

[*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 suoja koskevan eurooppalaisen ja jäsenvaltioiden lainsäädännön kanssa, ja aloitti neuvottelut

Yhdysvaltojen viranomaisten kanssa. Näiden neuvottelujen päätteeksi komissio teki 14.5.2004 päätöksen 2004/535/EY,¹⁷ 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,¹⁸ 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 (56 ja 57 kohta).

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 (58 ja 59 kohta).

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. Täten unionin tuomioistuin kumosi neuvoston päätöksen, jolla sallittiin sopimuksen tekeminen (67–69 kohta).

¹⁷ Yhdysvaltojen tulli- ja rajavartiolaitokselle toimitettavien lentomatikustajia koskevaan matkustajarekisteriin sisältyvien henkilötietojen suojan riittävästä tasosta 14.5.2004 tehty komission päätös 2004/535/EY (EUVL 2004, L 235, s. 11).

¹⁸ Lentoyhtiöiden PNR-tietojen käsitlemistä ja siirtämistä Yhdysvaltojen sisäisen turvallisuuden ministeriön alaiselle tulli- ja rajavalvontalaitokselle 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).

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

Toistuvien väkivallantekojen johdosta Ryneš oli asentanut taloonsa valvontakameran. Hänen talonsa jouduttua jälleen hyökkäyksen kohteeksi mainitun kameran tallenteiden ansiosta voitiin tunnistaa kaksi epäiltyä, joita vastaan aloitettiin rikosoikeudelliset menettelyt. Yksi näistä epäillyistä riitautti valvontakameran tallentamien tietojen käsittelyn laillisuuden Tšekin tietosuojavirastossa, ja mainittu 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 mainitun tallentamisen on tehnyt luonnollinen henkilö yksinomaan henkilökohtaisessa tai kotitaloutta koskevassa toiminnassa direktiivin 3 artiklan 2 kohdan toisessa luetelmakohdassa tarkoitettu tavoin.

Unionin tuomioistuin totesi, että sellaisen kamerajärjestelmän käyttämisen, joka tekee henkilöistä kuvatallenteen, 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 (35 kohta ja tuomiolauselma).

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 (27–29 kohta). 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 tietoja tällä tavoin käsittelevän tahon yksityisen piirin ulkopuolelle, sitä ei voida pitää yksinomaan "henkilökohtaisena tai kotitaloutta koskevana" toimintana mainitussa säännöksessä tarkoitettu tavoin (30, 31 ja 33 kohta).

2. Henkilötietojen käsite

[Tuomio 19.10.2016, Breyer \(C-582/14, EU:C:2016:779\)¹⁹](#)

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 toteamista 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 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 sulje pois sitä, että verkkomediapalvelujen tarjoajan tallentamat dynaamiset IP-osoitteet ovat sen kannalta direktiivin 95/46 2 artiklan a alakohdassa tarkoitettuja henkilötietoja (43 ja 44 kohta).

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 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 (49 kohta ja tuomiolauselman 1 kohta).

[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 mukaisen pyynnön saada tutustua kaikkiin henkilötietoihinsa, jotka olivat tilintarkastajien järjestön hallussa. Tilintarkastajien järjestö toimitti Nowakille eräitä asiakirjoja mutta kieltäytyi luovuttamasta hänelle

¹⁹ Mainittu tuomio on esitetty vuoden 2016 vuosikertomuksessa, s. 61.

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 2 artiklan a alakohdasta 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 2 artiklan a alakohdassa tarkoitettuna henkilötietona, ei edellytetä, että kaikki tiedot, joiden perusteella rekisteröity voidaan tunnistaa, ovat yhden ainoan tahon hallussa. Tilanteessa, jossa kokeeseen osallistujan henkilöllisyys ei ole tarkastajan tiedossa hänen arvostellessaan tämän kokeessa laatimia vastauksia, kokeen järjestävällä taholla – tässä tapauksessa tilintarkastajien järjestöllä – 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. Näiden vastausten sisältö nimittäin ilmentää osallistujan tietojen ja taitojen tasoa tietyllä alalla ja tarvittaessa hänen päättelyprosessiaan, harkintakykyään ja kriittistä ajatteluaan. Mainittujen vastausten keräämisen tarkoituksena on lisäksi 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 kokeesta, jossa on mahdollista käyttää kirjallista materiaalia (31 ja 36–40 kohta).

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 (42 ja 43 kohta).

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 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 12 artiklan a ja b alakohdan mukainen tietojen saantia ja oikaisua koskeva oikeus ei ulotu koekysymyksiin, jotka sellaisinaan eivät ole kokeeseen osallistujan henkilötietoja (56 ja 58 kohta).

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 2 artiklan a alakohdassa tarkoitettuja henkilötietoja (62 kohta ja tuomiolauselma).

3. Henkilötietojen käsittelyn käsite

[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 velvoitettu maksamaan sakko sillä perusteella, että hän oli käyttänyt henkilötietoja automaattisessa käsittelyssä ilman Datainspektionille (automaattisessa tietojenkäsittelyssä välitettyjen tietojen suojaa valvova viranomainen) tehtävää kirjallista ennakoilmoitusta, 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 käsittelynä” (27 kohta ja tuomiolauselman 1 kohta). 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 (38 ja 43–48 kohta sekä tuomiolauselman 2 kohta).

[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.

Näin unionin tuomioistuimelle avautui tilaisuus täsmentää henkilötietojen käsittelyn käsitettä internetissä suhteessa direktiiviin 95/46.

Unionin tuomioistuin katsoi, että hakukoneen sellaisen toiminnan, joka käsittää sivullisten 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 (tuomiolauselman 1 kohta). 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 (29 ja 30 kohta).

[Tuomio 10.7.2018 \(suuri jaosto\), Jehovan todistajat \(C-25/17, EU:C:2018:551\)](#)²⁰

Suomen tietosuojavaltuutettu oli antanut päätöksen, jolla se kielsi Jehovan todistajat -yhdyiskuntaa keräämästä tai muutoin käsittelemästä jäsentensä ovelta ovelle -saarnaamistyössä henkilötietoja ilman, että jokin henkilötietolaissa tarkoitetuista henkilötietojen käsittelyn edellytyksistä täyttyy. Tämän yhdyskunnan jäsenet tekevät ovelta ovelle -saarnaamistyönsä yhteydessä muistiinpanoja tapaamistaan heille ja yhdyskunnalle 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

²⁰ Mainittu tuomio on esitetty vuoden 2018 vuosikertomuksessa, s. 87 ja 88.

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 (51 kohta ja tuomiolauselman 1 kohta).

[Tuomio 14.2.2019, Buivids \(C-345/17, EU:C:2019:122\)](#)

Kyseisessä asiassa unionin tuomioistuin tarkasteli tulkintaa, joka koskee ensinnäkin direktiivin 95/46 soveltamisalaa ja toiseksi kyseisen direktiivin 9 artiklassa tarkoitettua käsitettä "ainoastaan journalistisia tarkoituksia – varten toteutettua henkilötietojen käsittelyä".

Kyseisessä asiassa ennakkoratkaisua oli pyytänyt Latvian ylin tuomioistuin käsiteltäväkseen saatetussa riita-asiassa, jossa olivat vastakkain Buivids (jäljempänä valittaja) ja Latvian tietosuojaviranomainen ja joka koski kanteen, jolla vaadittiin toteamaan lainvastaiseksi kyseisen viranomaisen päätös, jonka mukaan Buivids rikkoi kansallista tietosuojalainsäädäntöä julkaisemalla internetsivustolla kuvaamansa videon erään hallinnollista rikkomusta koskevan menettelyn yhteydessä poliisiasemalla pidetystä kuulustelustaan. Sen jälkeen, kun kaksi alemmanasteista tuomioistuinta oli hylännyt hänen kanteensa, valittaja teki ylimpään tuomioistuimeen kassaatiovalituksen. Kyseisessä tuomioistuimessa hän vetosi ilmaisunvapauteensa ja esitti, että kyseessä olevalla videolla näytetään kansallisen poliisin virkamiehiä eli julkisia henkilöitä tilassa, johon yleisöllä on pääsy, minkä vuoksi näihin henkilöihin ei sovelleta henkilötietojen suojasta annetun lain säännöksiä.

Ensinnäkin direktiivin 95/46 soveltamisalasta unionin tuomioistuin huomautti yhtäältä, että kyseiselle videolle tallennetut poliisimiesten kuvat ovat henkilötietoja, ja toiseksi, että näistä henkilöistä kuvattu videokuva, joka on tallennettu valittajan käyttämän kameran muistiin, on henkilötietojen käsittelyä. Unionin tuomioistuin totesi lisäksi, että videotallenteen, johon sisältyy henkilötietoja, julkaiseminen internetin videosivustolla, jolla käyttäjät voivat katsella ja jakaa videoita, kyseisten tietojen kokonaan tai osittain automatisoitua käsittelyä. Unionin tuomioistuin korosti myös, ettei kyseinen videotallenne ja sen julkaiseminen kuulu direktiivin 95/46 soveltamisalasta säädettyjen sellaisten poikkeusten alaan, jotka koskevat muun muassa sellaisen toiminnan yhteydessä suoritettua henkilötietojen käsittelyä, joka ei kuulu kyseisen direktiivin soveltamisalaan, ja käsittelyä, joka kuuluu yksinomaan henkilökohtaiseen tai kotitaloutta koskevaan toimintaan. Näin ollen unionin tuomioistuin totesi, että kyseisen direktiivin soveltamisalaan kuuluu poliisimiesten videoiminen poliisiasemalla kuulustelutilanteessa ja näin kuvattun videon julkaiseminen internetin videosivustolla, jolle käyttäjät voivat lähettää videoita ja jolla he voivat katsoa ja jakaa niitä (31, 32, 35, 39, 42 ja 43 kohta sekä tuomiolauselman 1 kohta).

Toiseksi käsitteen "henkilötietojen käsittely journalistisia tarkoituksia varten" sisällöstä unionin tuomioistuin huomautti aluksi, että käsitteen "journalismi" laajan tulkinnan mukaisesti direktiivin 95/46 9 artiklassa säädettyjä poikkeuksia ja vapautuksia sovelletaan kaikkiin journalismia harjoittaviin henkilöihin. Unionin tuomioistuin totesi, ettei se, ettei valittaja ole ammatiltaan toimittaja, sulje pois sitä, että kyseessä olevan videon kuvaamista ja julkaisemista voidaan pitää "henkilötietojen käsittelynä journalistisia tarkoituksia varten". Lisäksi unionin tuomioistuin korosti, että direktiivin 95/46 9 artiklassa säädettyjä poikkeuksia ja vapautuksia on sovellettava vain siinä määrin, kuin on tarpeen kahden perusoikeuden eli yksityisyyden suoja ja sananvapautta koskevien oikeuksien yhteensovittamiseksi. Tältä osin unionin tuomioistuin täsmensi, ettei voida

sulkea pois sitä, että kyseessä olevan videon kuvaaminen ja julkaiseminen, jotka tapahtuivat ilman, että kyseisellä videolla näkyville poliisimiehille olisi ilmoitettu kuvaamisesta ja sen tarkoituksesta, loukkaa kyseisten henkilöiden yksityisyyden suojaa koskevaa perusoikeutta. Tämän vuoksi unionin tuomioistuin totesi, että kyseisen videon kuvaaminen ja julkaiseminen internetin videosivustolla voivat olla henkilötietojen käsittelyä journalistisia tarkoituksia varten, jos mainitusta videosta käy ilmi, että kuvaamisen ja julkaisemisen ainoana tarkoituksena oli tietojen, mielipiteiden tai ajatusten ilmaiseminen yleisölle, mikä ennakkoratkaisua pyytäneen tuomioistuimen on tutkittava (51, 52, 55, 63 ja 67 kohta sekä tuomiolauselman 2 kohta).

[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 tieliikennesäännöstön²¹ 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 säännöstön lainmukaisuutta ja teki perustuslain mukaisuutta koskevan valituksen Latvijas Republikas Satversmes tiesaan (perustuslakituomioistuin, Latvia), jotta tämä tutkisi, onko kyseinen säännöstö sopu soinnussa yksityiselämän kunnioittamista koskevan oikeuden kanssa.

Perustuslakituomioistuin katsoi, että arvioidessaan kyseistä perustuslaillista oikeutta sen on otettava huomioon yleinen tietosuojasetus. Näin ollen se pysyi unionin tuomioistuinta selventämään useiden yleisen tietosuojasetuksen säännösten ulottuvuutta määrittääkseen, onko Latvian tieliikennesäännöstö sopu soinnussa 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",²² jonka osalta yleisessä tietosuojasetuksessa säädetään paremmasta suojasta kyseessä olevien tietojen erityisen arkaluontoisuuden vuoksi (10, 46, 74 ja 94 kohta sekä tuomiolauselman 1 kohta).

Tässä yhteydessä se huomauttaa aluksi, että liikenne rikkomuspisteitä koskevat tiedot ovat henkilötietoja ja että se, että liikenneturvallisuusvirasto luovuttaa niitä kolmansille, on käsittelyä, joka kuuluu yleisen tietosuojasetuksen aineelliseen soveltamisalaan. Mainittu soveltamisala on nimittäin erittäin laaja eikä kyseinen käsittely kuulu mainitun asetuksen sovellettavuutta koskevien poikkeusten soveltamisalaan (60, 61 ja 72 kohta).

²¹ Tieliikennelain (Ceļu satiksmes likums), joka on annettu 1.10.1997, (Latvijas Vēstnesis, 1997, nro 274/276) 14¹ §:n 2 momentti.

²² Yleisen tietosuojasetuksen 10 artikla.

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.²³ 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 (62 ja 66–68 kohta).

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.²⁴ Unionin tuomioistuin toteaa nimittäin, ettei liikenneturvallisuusvirastoa voida mainitussa luovuttamisessa pitää mainitunlaisena "toimivaltaisena viranomaisena"²⁵ (69–71 kohta).

Sen määrittämiseksi, onko oikeus tutustua tieliikenneriikkomuksia koskeviin henkilötietoihin, kuten liikenneriikkomuspisteisiin, sellaisten "rikoksia"²⁶ 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 seuraamuksen ankuruus, unionin tuomioistuin toteaa, että kyseessä olevat tieliikenneriikkomukset kuuluvat yleisessä tietosuoja-asetuksessa 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 syyllistymisestä 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

²³ Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan a alakohta.

²⁴ Yleisen tietosuoja-asetuksen 2 artiklan 2 kohdan d alakohta.

²⁵ 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 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 (EUVL 2016, L 119, s. 89) 3 artiklan 7 kohta.

²⁶ Yleisen tietosuoja-asetuksen 10 artikla.

seuraamuksen lisäksi ja kyseisten pisteiden kertymisellä on oikeudellisia seurauksia, jotka voivat ulottua jopa ajokieltoon saakka (77, 80, 85, 87–90 ja 93 kohta).

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 ”Henkilötietojen käsittelyn käsite”) 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 (62 kohta ja tuomiolauselman 2 kohta).

5. Käsite ”rekisterinpitäjä”

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

Kyseisessä tuomiossa (ks. myös otsikot II.3 ”Henkilötietojen käsittelyn käsite” ja 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 (74 ja 75 kohta sekä tuomiolauselman 3 kohta).

[Tuomio 5.6.2018 \(suuri jaosto\), Wirtschaftsakademie Schleswig Holstein \(C-210/16, EU:C:2018:388\)](#)²⁷

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 (39 kohta).

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

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

Kyseisessä asiassa saksalainen muotivaatteita verkossa myyvä yritys Fashion ID oli liittänyt verkkosivustolleen Facebookin sosiaalisen verkoston ”tykkää”-yhteisöliitännäisen. 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 koskeissa 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 tosiasiallisesti tarkoituksen ja keinot, eli kyseessä olevien tietojen keräämiseen ja niiden siirtämällä tapahtuvaan välittämiseen. Unionin tuomioistuimen mukaan Fashion ID:n on sen sijaan lähtökohtaisesti mahdotonta

²⁷ Mainittu tuomio on esitetty vuoden 2018 vuosikertomuksessa, s. 86 ja 87.

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 (76 ja 85 kohta sekä tuomiolauselman 2 kohta).

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 (97 kohta ja tuomiolauselman 3 kohta).

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 tosiasiallisesti 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 tosiasiallisesti tarkoituksen ja keinot (106 kohta ja tuomiolauselman 4 kohta).

[Tuomio 9.7.2020, Land Hessen, C-272/19, EU:C:2020:535](#)

Kansalainen, joka oli esittänyt vetoomuksen Hessenin osavaltion parlamentin vetoomusvaliokunnalle (Saksa), esitti kyseiselle valiokunnalle pyynnön saada pääsy omiin henkilötietoihinsa, jotka valiokunta oli tallentanut hänen vetoomuksensa käsittelyn yhteydessä. Hän tukeutui pyyntönsä tueksi yleiseen tietosuojasetukseen, jossa säädetään rekisteröidyn oikeudesta saada rekisterinpitäjältä pääsy omiin henkilötietoihinsa.

Hessenin osavaltion parlamentin puhemies hylkäsi tämän pyynnön sillä perusteella, että vetoomusmenettely on parlamentaarinen tehtävä ja että parlamentti ei kuulu yleisen tietosuojasetuksen soveltamisalaan.

Verwaltungsgericht Wiesbaden (Wiesbadenin hallintotuomioistuin, Saksa), jossa kansalainen nosti kanteen, totesi, että Saksan oikeudessa ei anneta oikeutta saada pääsy henkilötietoihin pääasiassa kyseessä olevan kaltaisen vetoomuksen yhteydessä. Verwaltungsgericht Wiesbaden katsoi kuitenkin, että tällainen oikeus voisi perustua yleiseen tietosuojasetukseen, ja esitti unionin tuomioistuimelle tätä koskevan kysymyksen. Lisäksi Verwaltungsgericht Wiesbaden epäilee omaa riippumattomuuttaan ja näin ollen toimivaltaansa esittää ennakkoratkaisukysymyksiä unionin tuomioistuimelle, ja se esitti unionin tuomioistuimelle myös tätä koskevan kysymyksen.

Tuomiossaan unionin tuomioistuin vastaa, että siltä osin kuin jäsenvaltion osavaltion parlamentin vetoomusvaliokunta määrittelee yksin tai yhdessä toisten kanssa henkilötietojen käsittelyn tarkoituksen ja keinot, kyseistä valiokuntaa on pidettävä yleisessä tietosuojasetuksessa tarkoitettuna "rekisterinpitäjänä".²⁸ Tällaisen valiokunnan suorittama henkilötietojen

²⁸ Yleisen tietosuojasetuksen 4 artiklan 7 kohta.

käsittely kuuluu siis tämän asetuksen ja erityisesti sen säännöksen soveltamisalaan, jolla rekisteröidyille annetaan oikeus saada pääsy omiin henkilötietoihinsa.²⁹

Unionin tuomioistuin toteaa muun muassa, ettei Hessenin osavaltion parlamentin vetoomusvaliokunnan toiminta kuulu yleisessä tietosuojasetuksessa säädetyn poikkeuksen piiriin. Se toteaa, että tällainen toiminta on luonteeltaan julkista ja tälle osavaltiolle ominaista, koska kyseinen valiokunta osallistuu parlamentaariseen toimintaan välillisesti, mutta korostaa, että tämä toiminta on luonteeltaan sekä poliittista että hallinnollista. Unionin tuomioistuimen käytettävissä olevasta asiakirja-aineistosta ei ilmene, että kyseinen toiminta vastaisi nyt käsiteltävässä asiassa jotain yleisessä tietosuojasetuksessa säädettyä poikkeusta (71–74 kohta ja tuomiolauselma).

6. Henkilötietojen käsittelyn laillisuuden edellytykset

*[Tuomio 16.12.2008 \(suuri jaosto\), Huber \(C-524/06, EU:C:2008:724\)](#)*³⁰

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 Obergerwaltungsgericht für das Land Nordrhein-Westfalen (Nordrhein-Westfalenin osavaltion ylemmän asteen hallintotuomioistuin, Saksa) esitti unionin tuomioistuimelle ennakkoratkaisupyynnön 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 (54, 58 ja 59 kohta).

²⁹ Yleisen tietosuojasetuksen 15 artikla.

³⁰ Mainittu tuomio on esitetty vuoden 2008 vuosikertomuksessa, s. 45.

Direktiivin 95/46 7 artiklan e alakohdassa tarkoitettua 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 tarkoitettulla tavalla tarpeellisina ei missään tapauksessa voida pitää nimeltä mainittujen henkilöiden henkilötietojen tallentamista ja käsittelyä tämän kaltaisen rekisterin puitteissa tilastotieteellisiin tarkoituksiin (52, 66 ja 68 kohta).

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 (78–80 kohta).

[Tuomio 24.11.2011, ASNEF ja FECEMD \(C-468/10 ja C-469/10, EU:C:2011:777\)](#)

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) olivat molemmat tehneet Tribunal Supremossa (ylin oikeusaste, Espanja) hallintovalituksen useista kuninkaan asetuksen nro 1720/2007 pykälistä. Mainitulla asetuksella pantiin täytäntöön laki nro 15/1999, jolla saatettiin direktiivi 95/46 osaksi Espanjan oikeutta.

ASNEF ja FECEMD katsoivat erityisesti, että Espanjan oikeudessa – henkilötietojen käsittelyn sallimiseksi ilman kyseisen henkilön suostumusta – säädettiin edellytyksestä, jota ei ollut direktiivissä 95/46, ja edellytettiin, että mainitut tiedot ovat yleisön saatavilla olevissa lähteissä sellaisina kuin ne luetellaan lain nro 15/1999 3 §:n j alakohdassa. Ne väittivät tältä osin, että mainitulla lailla ja kuninkaan asetuksella nro 1720/2007 rajoitettiin direktiivin 95/46 7 artiklan f alakohdan ulottuvuutta, sillä viimeksi mainitussa säännöksessä säädetään henkilötietojen käsittelemiseksi kyseessä olevan henkilön suostumuksen puuttuessa ainoastaan yhdestä edellytyksestä, joka koskee yksinomaan rekisterinpitäjän tai tiedot saavan sivullisen oikeutetun intressin toteuttamista.

Unionin tuomioistuin totesi tästä ensinnäkin, että direktiivissä 95/46 säädetään tyhjentävästä luettelosta, johon on rajattu tilanteet, joissa henkilötietojen käsittelyn voidaan katsoa olevan laillista kyseessä olevan henkilön suostumuksen puuttuessa. Jäsenvaltiot eivät täten voi direktiivin 5 artiklan perusteella ottaa käyttöön muita henkilötietojen käsittelyn laillistamista koskevia periaatteita kuin ne, jotka mainitaan 7 artiklassa, eivätkä lisävaatimuksilla muuttaa mainitussa artiklassa säädettyjen periaatteiden ulottuvuutta. Kyseisessä 5 artiklassa annetaan

jäsenvaltioille lupa ainoastaan määritellä henkilötietojen käsittelyn laillisuuden edellytykset direktiivin II luvussa eli näin siis sen 7 artiklassa säädetyissä rajoissa (30, 32 ja 33 kohta).

Erityisesti on niin, että jäsenvaltioilla on mahdollisuus vahvistaa periaatteellisia ohjeita direktiivin 95/46 7 artiklan f alakohdassa tarkoitettun, asiassa vastakkain olevien oikeuksien ja intressien edellyttämän punnitsemisen suorittamiseksi. Ne voivat myös ottaa huomioon sen, että rekisteröidyn perusoikeuksiin häntä koskevien tietojen käsittelyn vuoksi kohdistuvan loukkauksen vakavuus voi vaihdella sen mukaan, ovatko kyseessä olevat tiedot mahdollisesti jo yleisön saatavilla olevassa lähteessä vai eivät (44 ja 46 kohta).

Unionin tuomioistuin kuitenkin katsoi, että jos kansallisella lainsäädännöllä suljetaan kokonaan pois tiettyjen henkilötietoryhmien osalta mahdollisuus niiden käsittelyyn vahvistamalla näiden ryhmien osalta lopullisesti se, mikä vastakkaisten oikeuksien ja intressien punnitsemisen tulos on, sallimatta muunlaista tulosta tiettyjen konkreettisissa tapauksessa vallitsevien erityisten olosuhteiden perusteella, kyseessä ei ole enää pelkkä direktiivin 95/46 5 artiklassa tarkoitettu täsmennys. Näin ollen unionin tuomioistuin totesi, että direktiivin 95/46 7 artiklan f alakohta on esteenä sille, että jäsenvaltio sulkee ehdottomasti ja yleisesti pois mahdollisuuden käsitellä tiettyihin tietoryhmiin kuuluvia henkilötietoja sallimatta niiden oikeuksien ja intressien punnitsemista, joista on kyse tietyssä yksittäisessä tapauksessa (47 ja 48 kohta).

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

Tässä tuomiossa (ks. myös otsikko II.2 "Henkilötietojen käsite") unionin tuomioistuin otti kantaa myös siihen, onko direktiivin 95/46 7 artiklan f alakohta esteenä sellaiselle kansalliselle säännökselle, jonka mukaan verkkomediapalvelujen 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.

Se totesi, että direktiivin 95/46 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 rajoitettiin laittomasti kyseisen direktiivin 95/46 7 artiklan f alakohdassa säädetyin periaatteen ulottuvuutta, koska näin suljettiin pois se, että verkkomediapalvelun yleisen toiminnan takaamisen tavoitetta voitaisiin punnita suhteessa näiden käyttäjien intresseihin tai perusoikeuksiin ja -vapauksiin (62–64 kohta ja tuomiolauselman 2 kohta).

[Tuomio 4.5.2017, Rīgas satiksme \(C-13/16, EU:C:2017:336\)](#)

Tässä asiassa oli kyse oikeusriidasta, jossa vastakkain olivat Latvian poliisi ja Rīgas satiksme, joka on Riian kaupungin johdinautoyrittäjä, ja jossa oli kyse pyynnöstä saada tietoja onnettomuuden

aiheuttaneen henkilön tunnistamista varten. Käsiteltävässä asiassa taksinkuljettaja oli liikenneonnettomuuden yhteydessä pysäyttänyt autonsa ajoväylän reunaan. Rīgas satiksmen johdinauton ohittaessa taksia taksin takapenkillä istunut matkustaja avasi oven, joka osui johdinautoon ja vahingoitti sitä. Siviilioikeudellisen kanteen nostamiseksi Rīgas satiksme pyysi poliisilta tietoja onnettomuuden aiheuttaneen henkilön tunnistamista varten. Poliisi kieltäytyi antamasta matkustajan henkilönnumeroa ja osoitetta ja asiakirjoja, jotka koskivat onnettomuudessa mukana olleiden henkilöiden selvityksiä, sillä perusteella, että hallinnollisen seuraamusmenettelyn asiakirjat voidaan luovuttaa vain kyseisen menettelyn osapuolille ja että henkilötietojen suojasta annettu laki kieltää luonnollisten henkilöiden henkilönnumeron ja osoitteen luovuttamisen.

Tässä tilanteessa Augstākās tiesas Administratīvo lietu departaments (ylimmän tuomioistuimen hallintoasioita käsittelevä osasto, Latvia) päätti tiedustella unionin tuomioistuimelta, asetetaanko direktiivin 95/46 7 artiklan f alakohdassa velvollisuus luovuttaa henkilötietoja sivulliselle, jotta tämä voi nostaa siviilioikeudellisen vahingonkorvauskanteen vaatiakseen kyseisen henkilön, jota henkilötietosuoja koskee, aiheuttaman vahingon korvaamista, ja voiko sillä seikalla, että kyseinen henkilö on alaikäinen, olla vaikutusta tämän säännöksen tulkintaan.

Unionin tuomioistuin katsoi, että direktiivin 95/46 7 artiklan f alakohtaa on tulkittava siten, ettei siinä aseteta velvollisuutta luovuttaa henkilötietoja sivulliselle, jotta tämä voi nostaa siviilioikeudellisen vahingonkorvauskanteen vaatiakseen henkilön, jota henkilötietosuoja koskee, aiheuttaman vahingon korvaamista. Mainittu säännös ei kuitenkaan ole esteenä tällaiselle luovuttamiselle siinä tapauksessa, että luovuttaminen tapahtuu kansallisen oikeuden nojalla ja tässä säännöksessä säädettyjä edellytyksiä noudattaen (27 ja 34 kohta sekä tuomiolauselman).

Unionin tuomioistuin huomautti tästä, ettei ole perusteltua – mikä kansallisen tuomioistuimen on varmistettava – kieltäytyä sellaisten henkilötietojen luovuttamisesta vahinkoa kärsineelle osapuolelle, jotka ovat tarpeen vahingonkorvauskanteen nostamiseksi vahingon aiheuttanutta henkilöä vastaan tai mahdollisesti huoltajia vastaan sen vuoksi, että vahingon aiheuttanut henkilö on alaikäinen (33 kohta).

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

Pääasian oikeudenkäynnissä Puškár nosti kanteen Najvyšší súd Slovenskej republikyssa (ylin tuomioistuin, Slovakia) 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 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 indisoita olettaa, että rekisteröidyt ovat luettelossa perustellusti, ja toisaalta, että kaikki direktiivissä 95/46 asetetut henkilötietojen käsittelyn laillisuuden edellytykset täyttyvät (117 kohta ja tuomiolauselman 3 kohta).

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 (111, 112 ja 113 kohta).

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 syyttömysolettamaan, 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 näin ollen 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 (114 kohta).

Unionin tuomioistuin katsoi myös, että jos on olemassa syitä direktiivin 95/46 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 koskevista asioista, varmistamiseksi, ja perustuttava lainsäädännöllisiin toimenpiteisiin (116 kohta).

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

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

Românille 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 täyttyvä, jotta asiakkaiden suostumusta henkilötietojen käsittelyyn voidaan pitää pätevänä.

Unionin tuomioistuin muistuttaa aluksi, että unionin oikeudessa³¹ esitetään luettelo tapauksista, joissa henkilötietojen käsittelyyn voidaan katsoa olevan lainmukaista. Erityisesti rekisteröidyn suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen.³² Suostumusta ei ole annettu pätevästi vaikenemalla, valmiiksi rastitetuilla ruuduilla tai jättämällä jokin toimi toteuttamatta (34, 36, 37 ja 39 kohta).

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 (34, 36, 37, 39 ja 41 kohta).

Unionin tuomioistuin 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 (42 ja 46 kohta).

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

³¹ Direktiivin 95/46 7 artikla ja yleisen tietosuoja-asetuksen 6 artikla.

³² Direktiivin 95/46 2 artiklan h alakohta ja yleisen tietosuoja-asetuksen 4 artiklan 11 kohta.

toiminnallaan ilmaisseet suostumuksensa henkilötietojensa käsittelyyn, kyseinen yhtiö ei voi vaatia, että he ilmaisevat kieltäytymisensä aktiivisesti (49–51 kohta).

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 (52 kohta ja tuomiolauselma).

[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 yleissopimuksen³³ 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

³³ Tarkastusten asteittaisesta lakkauttamisesta yhteisillä rajoilla Benelux-talousoiiton valtioiden, Saksan liittotasavallan ja Ranskan tasavallan hallitusten välinen, Schengenissä 14.6.1985 allekirjoitettu sopimus (EYVL 2000, L 239, s. 13) (jäljempänä Schengenin sopimuksen soveltamisesta tehty yleissopimus).

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 2016/680³⁴ säännösten vastaista.

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 toteaa suuren jaoston kokoonpanossa antamassaan tuomiossa muun muassa, että direktiivin 2016/680 säännöksiä, luettuina 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 (121 kohta ja tuomiolauselman 2 kohta).

Kysymyksestä, joka koskee Interpolin punaiseen ilmoitukseen sisältyviä henkilötietoja, unionin tuomioistuin toteaa, että kaikki kyseisiin tietoihin kohdistuva toiminta, kuten niiden tallentaminen jäsenvaltion etsittyjen henkilöiden tietokantoihin, on direktiivin 2016/680 soveltamisalaan kuuluvaa henkilötietojen käsittelyä.³⁵ Se katsoo 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.³⁶ Jäsenvaltioiden viranomaisten suorittama henkilötietojen käsittely voi osoittautua välttämättömäksi juuri sen tarkistamiseksi, sovelletaanko kyseistä periaatetta (111, 114, 116, 117 ja 119 kohta).

Näissä olosuhteissa unionin tuomioistuin toteaa 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 varten³⁷ (121 kohta ja tuomiolauselman 2 kohta).

³⁴ 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).

³⁵ Direktiivin 2016/680 2 artiklan 1 kohta ja 3 artiklan 2 kohta.

³⁶ Direktiivin 2016/680 4 artiklan 1 kohdan b alakohta ja 8 artiklan 1 kohta.

³⁷ Ks. direktiivin 2016/680 1 artiklan 1 kohta ja 8 artiklan 1 kohta.

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 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 (120 kohta).

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

Kyseisessä tuomiossa (ks. myös otsikko II.3 ”Henkilötietojen käsittelyn käsite”) unionin tuomioistuin toteaa, että yleinen tietosuojasetus on esteenä säännöstölle, jolla Ceļu satiksmes drošības direkcijai (liikenneturvallisuusvirasto, Latvia; jäljempänä liikenneturvallisuusvirasto) asetetaan velvollisuus saattaa yleisön saataville ajoneuvojen kuljettajille tieliikenneturvallisuudesta määrättyjä liikenneturvallisuuspisteitä koskevat tiedot ilman, että henkilön, joka niitä pyytää, olisi perusteltava erityinen intressi saada kyseiset tiedot. Se toteaa, ettei ole osoitettu, että tieliikenneturvallisuudesta määrättyjä liikenneturvallisuuspisteitä koskevien henkilötietojen luovuttamisjärjestelmä olisi välttämätön erityisesti Liettuan mainitseman liikenneturvallisuuden parantamisen tavoitteen valossa. Unionin tuomioistuimen mukaan virallisten asiakirjojen julkisuus tai oikeus tiedonvälityksen vapauteen eivät kumpikaan oikeuta tällaista säännöstöä (113, 120–122 kohta ja tuomiolauselman 2 kohta).

Tässä asiayhteydessä unionin tuomioistuin korostaa, että Liettuan säännöstössä tavoiteltu liikenneturvallisuuden parantaminen on unionin tunnustama yleisen edun mukainen tavoite ja että näin ollen jäsenvaltiot voivat luokitella liikenneturvallisuuden ”yleistä etua koskevaksi tehtäväksi”.³⁸ Ei ole kuitenkaan osoitettu, että Liettuan järjestelmässä liikenneturvallisuuspisteitä koskevien henkilötietojen luovuttaminen olisi välttämätöntä tavoitteen saavuttamiseksi. Yhtäältä Liettuan lainsäätäjällä on nimittäin kyseisen tavoitteen saavuttamiseksi käytettävissään useita muita, rekisteröityjen perusoikeuksia vähemmän rajoittavia keinoja. Toisaalta on otettava huomioon liikenneturvallisuuspisteitä koskevien tietojen arkaluontoisuus ja se, että niiden luovuttaminen yleisölle on omiaan muodostamaan vakavan puuttumisen yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin, koska se voi aiheuttaa yhteiskunnan paheksuntaa ja rekisteröidyn leimautumista (109–113 kohta).

Lisäksi unionin tuomioistuin katsoo, että kun otetaan huomioon näiden tietojen arkaluontoisuus ja tämän perusoikeuksiin puuttumisen vakavuus, mainitut oikeudet ovat tärkeämpiä kuin virallisten asiakirjojen, muun muassa kansallisen ajoneuvo- ja kuljettajarekisterin, julkisuutta koskeva etu ja oikeus tiedonvälityksen vapauteen (120 ja 121 kohta).

Samasta syystä unionin tuomioistuin toteaa, että yleinen tietosuojasetus on esteenä myös Liettuan lainsäädännölle, jossa liikenneturvallisuusvirastolle annetaan oikeus luovuttaa

³⁸ Yleisen tietosuojasetuksen 6 artiklan 1 kohdan e alakohdan nojalla henkilötietojen käsittely on lainmukaista, jos ”käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi –”.

ajoneuvojen kuljettajille tieliikenne rikkomuksista määrättyjä liikenne rikkomuspisteitä koskevat tiedot talouden toimijoille, jotta viimeksi mainitut pystyvät uudelleenkäyttämään niitä ja luovuttamaan ne yleisölle (126 kohta ja tuomiolauselman 3 kohta).

Lopuksi unionin tuomioistuin toteaa, että unionin oikeuden ensisijaisuuden periaate on esteenä sille, että ennakkoratkaisua pyytänyt tuomioistuin, jonka käsiteltävänä on valitus Liettuan lainsäädännöstä, jonka unionin tuomioistuin luonnehtii unionin oikeuden vastaiseksi, päättää, että kyseisen lainsäädännön oikeusvaikutukset pysytetään voimassa sen tuomion julistamispäivään saakka, jolla se ratkaisee kyseisen valituksen lainvoimaisesti (137 kohta ja tuomiolauselman 4 kohta).

III. Direktiivissä 2002/58 tarkoitettu henkilötietojen käsittely

[*Tuomio 2.10.2018 \(suuri jaosto\), Ministerio Fiscal \(C-207/16, EU:C:2018:788\)*](#)³⁹

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 tyhjentyvästi 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" yleisesti (38, 42 ja 59–63 kohta sekä tuomiolauselma).

³⁹ Mainittu tuomio on esitetty vuoden 2018 vuosikertomuksessa, s. 88 ja 89.

Tässä asiayhteydessä unionin tuomioistuin täsmensi, että vaikka se katsoi tuomiossaan Tele2 Sverige ja Watson ym.,⁴⁰ että vain vakavan rikollisuuden torjuminen voi oikeuttaa 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 (54–57 kohta).

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 (61 ja 62 kohta).

[Tuomio 6.10.2020 \(suuri jaosto\), Privacy International \(C-623/17, EU:C:2020:790\) ja tuomio 6.10.2020, La Quadrature du Net ym. \(C-511/18, C-512/18 ja C-520/18, EU:C:2020:791\)](#)⁴¹

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 constitutionnelle (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 toteaa 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

⁴⁰ Tuomio 21.12.2016, Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, EU:C:2016:970).

⁴¹ Mainitut tuomiot on esitetty vuoden 2020 vuosikertomuksessa, s. 29–32.

henkilötietojen käsittelyä, kuten esimerkiksi säilytettävä liikenne- ja paikkatietoja ja siirrettävä niitä turvallisuus- ja tiedustelupalveluille (tuomion Privacy International 49 kohta ja tuomiolauselman 1 kohta sekä tuomion La Quadrature du Net ym. 104 kohta).

Tämän jälkeen unionin tuomioistuin muistuttaa, että direktiivissä 2002/58⁴² 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,⁴³ ainoastaan, jos unionin oikeuden yleisiä periaatteita, joihin kuuluu suhteellisuusperiaate, ja perusoikeuskirjassa taattuja perusoikeuksia⁴⁴ noudatetaan (tuomion Privacy International 59 ja 60 kohta sekä tuomion La Quadrature du Net ym. 111 ja 113 kohta).

Unionin tuomioistuin katsoo 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 katsoo, että tämä sama direktiivi on esteenä lainsäädännöllisille toimenpiteille, joilla sähköisten viestintäpalvelujen tarjoajat veloitetaan 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 tulkitsee yleisen tietosuojasetuksen 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 (tuomion Privacy International 71 ja 82 kohta ja tuomiolauselman 2 kohta sekä tuomion La Quadrature du Net ym. 146, 168, 174, 177 ja 212 kohta sekä tuomiolauselman 1 ja 3 kohta).

Unionin tuomioistuin katsoo 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 täsmentää tässä yhteydessä, että joko tuomioistuimen tai riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, on valvottava tehokkaasti päätöstä, jolla tällainen määräys annetaan ajanjaksoksi, joka on rajoitettu täysin välttämättömään, sen tarkastamiseksi, että kyseessä on jokin näistä tilanteista ja että niitä

⁴² Direktiivin 2002/58 15 artiklan 1 ja 3 kohta.

⁴³ Direktiivin 2002/58 5 artiklan 1 kohta.

⁴⁴ Erityisesti perusoikeuskirjan 7, 8 ja 11 artikla sekä 52 artiklan 1 kohta.

edellytyksiä ja takeita, joista on säädettävä, noudatetaan. Mainittu direktiivi ei samoin edellytyksin ole esteenä myöskään kaikkien sähköisten viestintävälineiden käyttäjien tietojen ja muun muassa liikenne- ja paikkatietojen automaattiselle analysoinnille (tuomion La Quadrature du Net ym. 137–139 ja 177–179 kohta sekä tuomiolauselman 1 ja 2 kohta).

Unionin tuomioistuin toteaa 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 lakisäätteisten 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 (tuomion La Quadrature du Net ym. 161, 163 ja 168 kohta sekä tuomiolauselman 1 kohta).

Unionin tuomioistuin toteaa 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 (tuomion La Quadrature du Net ym. 192 kohta ja tuomiolauselman 2 kohta).

Unionin tuomioistuin tarkastelee lopuksi kysymystä unionin oikeuden vastaiseksi todetun kansallisen säännösten ajallisten vaikutusten pysyttämisestä. Se katsoo 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 huomauttaa tämän jälkeen, että sellaisten todisteiden hyväksyttävyyden ja 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 täsmentää 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

erotukset tapahtuvalla säilyttämisellä, jos rikoksista epäillyt henkilöt eivät voi tehokkaasti ilmaista käsitystään näistä todisteista (tuomion La Quadrature du Net ym. 222 ja 228 kohta sekä tuomiolauseلمان 4 kohta).

[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, epäilee niiden edellytysten, joilla tutkintaviranomaiset ovat saaneet näitä tietoja, yhteensopivuutta unionin oikeuden kanssa.⁴⁵

Nämä epäilykset koskevat 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 tiedustelee, voidaanko tällainen puuttuminen oikeuttaa rikollisuuden torjunnalla yleisesti eikä yksinomaan vakavan rikollisuuden torjunnalla. Toiseksi ennakkoratkaisua pyytäneellä tuomioistuimella on epäilyksiä siitä, voidaanko Viron syyttäviviranomaisista, kun otetaan huomioon sille kansallisen lainsäädännön nojalla kuuluvat erilaiset tehtävät, pitää tuomiossa Tele2 Sverige ja Watson ym.⁴⁶ tarkoitettuna riippumattomana hallintoviranomaisena, joka voi antaa tutkintaviranomaiselle luvan saada kyseessä olevia tietoja.

Union tuomioistuin toteaa suuressa jaostossa antamassaan tuomiossa, että direktiiviä 2002/58, kun sitä luetaan perusoikeuskirjan valossa, on tulkittava siten, että se on 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 katsoo lisäksi, että sama direktiivi, kun sitä luetaan perusoikeuskirjan valossa, on esteenä kansalliselle säännöstölle, jossa annetaan syyttäviviranomaiselle toimivalta myöntää viranomaiselle lupa liikenne- ja paikkatietojen saantiin rikostutkintaa varten (45 ja 59 kohta sekä tuomiolauseلمان 1 ja 2 kohta).

⁴⁵ Tarkemmin ottaen direktiivin 2002/58 15 artiklan 1 kohdan kanssa, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa.

⁴⁶ Tuomio 21.12.2016, Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, EU:C:2016:970, 120 kohta).

Siltä osin kuin on kyse pääasiassa kyseessä olevalla säännöstöllä tavoitellusta rikosten ehkäisemisestä, 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 ehkäisemisestä, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella (33 ja 35 kohta).

Siltä osin kuin kyse on syyttäväviranomaisen toimivallasta myöntää viranomaiselle lupa saada liikenne- ja paikkatietoja rikostutkintaa varten, unionin tuomioistuin muistuttaa, että niiden edellytysten, joiden nojalla sähköisten viestintäpalvelujen tarjoajien on annettava toimivaltaisille kansallisille viranomaisille oikeus saada hallussaan olevia tietoja, määrittäminen kuuluu kansallisen oikeuden alaan. Oikeasuhtaisuutta koskevan edellytyksen täyttämiseksi tällaisessa säännöstössä on joka tapauksessa säädettävä selvistä ja täsmällisistä asianomaisten toimenpiteiden laajuutta ja soveltamista koskevista säännöistä, joissa asetetaan vähimmäisvaatimukset, jotta henkilöillä, joiden henkilötiedoista on kyse, on riittävät takeet, joiden avulla heidän henkilötietojensa 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 (48 kohta).

Unionin tuomioistuimen mukaan sen takaamiseksi, että näitä edellytyksiä noudatetaan käytännössä täysimääräisesti, on olennaista se, että toimivaltaitten kansallisten viranomaisten oikeus saada säilytetyt 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 estämisen, selvittämisen tai syyteharkintamenettelyssä. Asianmukaisesti perustellussa kiireellisessä tapauksessa valvonta on suoritettava viipymättä (51 kohta).

Tältä osin unionin tuomioistuin täsmentää, 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 sovitaan 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 (52 ja 53 kohta).

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 viranomaisen 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 syyttäväviranomaisen ei voi suorittaa edellä mainittua etukäteisvalvontaa (54, 55 ja 57 kohta).

IV. Henkilötietojen siirtäminen kolmansiin maihin

[*Tuomio 6.11.2003 \(suuri jaosto\), Lindqvist \(C-101/01, EU:C:2003:596\)⁴⁷*](#)

Tässä tuomiossa (ks. myös otsikko II.3 "Henkilötietojen käsittelyn käsite") 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 (71 kohta ja tuomiolauselman 4 kohta).

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 tietosuojaja 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 (63, 64 ja 68 kohta).

[*Tuomio 6.10.2015 \(suuri jaosto\), Schrems \(C-362/14, EU:C:2015:650\)⁴⁸*](#)

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

⁴⁷ Mainittu tuomio on esitetty vuoden 2003 vuosikertomuksessa, s. 67.

⁴⁸ Mainittu tuomio on esitetty vuoden 2015 vuosikertomuksessa, s. 53.

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/EY⁴⁹ katsonut, että safe harbour -järjestelmän⁵⁰ 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 julisti komission päätöksen pätemättömäksi kokonaisuudessaan ja korosti ensinnäkin, että päätöksen tekeminen edellytti komission asianmukaisin perusteluin tekemää toteamusta siitä, että asianomainen kolmas maa tosiasiallisesti 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 (82, 87–89 ja 96–98 kohta sekä tuomiolauselman 2 kohta).

Unionin tuomioistuin 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 (102–104 kohta). Unionin tuomioistuin katsoi, että päätöksen 2000/520 1 ja 3 artiklan pätemättömyys vaikuttaa koko päätöksen pätevyys (105 ja 106 kohta).

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

⁴⁹ 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).

⁵⁰ Safe harbour -järjestelmä sisältää joukon henkilötietojen suojaa koskevia periaatteita, joiden noudattamiseen amerikkalaiset yritykset voivat vapaaehtoisesti sitoutua.

saannilta ja käytöltä. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti ja on olemassa huomattava vaara laittomasta pääsystä näihin tietoihin (91 kohta).

Lisäksi ja varsinkin on huomattava, että yksityiselämän kunnioitusta koskevan perusoikeuden suoja unionin tasolla edellyttää, että henkilötietojen suoja koskevat poikkeukset ja rajoitukset toteutetaan sen rajoissa, mikä on ehdottomasti tarpeen (92 kohta). 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 (93 kohta). 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 (94 ja 95 kohta).

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

Unionin tuomioistuin lausui 26.7.2017 ensimmäistä kertaa kansainvälisen sopimusluonnoksen yhteensoveltuvuudesta perusoikeuskirjan ja erityisesti siinä olevien yksityiselämän kunnioittamista ja henkilötietojen suoja 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 muutoksenhakekeinoista.

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 tuomioistuin 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 neuvottelema 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 (125 ja 126 kohta).

Unionin tuomioistuin 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.) (128 kohta).

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 tuomioistuin 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 tuomioistuin katsoi, että sopimusmääräykset, jotka koskevat arkaluontoisten tietojen siirtämistä Kanadaan ja niiden säilyttämistä, ovat perusoikeuksien vastaisia (165 ja 232 kohta).

Toiseksi unionin tuomioistuin 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 (205–207 ja 209 kohta).

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 lentomatrustajia 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 lentomatrustajat voivat käyttää oikeuttaan saada tutustua PNR-tietoihinsa ja tarvittaessa oikeuttaan pyytää niiden oikaisua sekä perusoikeuskirjan 47 artiklan ensimmäisen kohdan mukaista oikeuttaan tehokkaiisiin 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, lentomatrustajien henkilökohtainen informointi osoittautuu tarpeelliseksi. Sama pätee tapauksiin, joissa lentomatrustajien 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 (219, 220, 223 ja 224 kohta).

[*Tuomio 16.7.2020 \(suuri jaosto\), Facebook Ireland ja Schrems \(C-311/18, EU:C:2020:559\)*⁵¹](#)

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.⁵² 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 tietosuojaa koskevat vakiolausekkeet, ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.⁵³ 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.⁵⁴

⁵¹ Mainittu tuomio on esitetty vuoden 2020 vuosikertomuksessa, s. 26–29.

⁵² Yleisen tietosuojasetuksen 45 artikla.

⁵³ Yleisen tietosuojasetuksen 46 artiklan 1 kohta ja 2 kohdan c alakohta.

⁵⁴ 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 2000/520⁵⁵ 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")⁵⁶ (52 ja 53 kohta).

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/EU⁵⁷ 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 riittävydestä⁵⁸ (54, 55 ja 57 kohta).

Ennakkoratkaisua pyytänyt tuomioistuin kysyy 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.

Unionin tuomioistuin totesi 16.7.2020 antamassaan tuomiossa, että päätöksen 2010/87 perusoikeuskirjan perusteella suoritettua tarkastelua ei ole tullut esiin mitään seikkaa, joka vaikuttaisi tämän päätöksen pätevyteen. Sen sijaan päätöksen 2016/1250 se totesi pätemättömäksi (tuomiolauselman 4 ja 5 kohta).

⁵⁵ Direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbour -periaatteiden antaman suojan riittävydestä ja niihin liittyvistä Yhdysvaltojen kauppanäyttämisen julkaisemista tavallisimmista kysymyksistä 26.7.2000 tehty komission päätös 2000/520/EY (EUVL 2000, L 215, s. 7).

⁵⁶ Tuomio 6.10.2015, Schrems, C-362/14, [EU:C:2015:650](#) (ks. myös lehdistötiedote nro 117/15).

⁵⁷ 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).

⁵⁸ Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävydestä 12.7.2016 annettu komission täytäntöönpanopäätös (EU) 2016/1250 (EUVL 2016, L 207, s. 1).

Aivan aluksi unionin tuomioistuin katsoi, että unionin oikeutta ja muun muassa yleistä tietosuojasetusta 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 tietosuojasetuksen soveltamisalan ulkopuolelle siksi, että kyseisen kolmannen maan viranomaiset käsittelevät tietoja tällä tavoin (86, 88 ja 89 kohta sekä tuomiolauselman 1 kohta).

Tällaisen siirron yhteydessä edellytetyn suojan tasosta unionin tuomioistuin totesi, että yleisen tietosuojasetuksen säännöksissä tältä osin asetettuja edellytyksiä, jotka liittyvät asianmukaisiin suojoitoimenpiteisiin, täytäntöönpanokelpoisiin oikeuksiin ja tehokkaisiin oikeussuojakeinoihin, on tulkittava siten, että niillä on varmistettava, että henkilöt, joiden henkilötietoja siirretään kolmanteen maahan tietosuoja 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 (105 kohta ja tuomiolauselman 2 kohta).

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 tietosuoja koskeviin vakiolausekkeisiin perustuva henkilötietojen siirto kolmanteen maahan, jos tämä valvontaviranomainen katsoo kaikkien tämän siirron olosuhteiden valossa, että tietosuoja 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 (121 kohta ja tuomiolauselman 3 kohta).

Unionin tuomioistuin tutki tämän jälkeen päätöksen 2010/87 pätevyyttä. Unionin tuomioistuimen mukaan pelkästään se, että siihen sisältyvät tietosuoja 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 tietosuoja koskevia vakiolausekkeitä, jolloin viimeksi mainitun on keskeytettävä tietojen siirto ja/tai irtisanottava sopimus (132, 136, 137, 142 ja 148 kohta sekä tuomiolauselman 4 kohta).

Unionin tuomioistuin tutki lopuksi päätöksen 2016/1250 pätevyyttä yleisestä tietosuojasetuksesta johtuvien veloitteiden 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 suhteellisuusperiaatteeeseen, 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 suojoitoimia. 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 (164, 165, 180–182, 184 ja 185 kohta).

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 mekaniisissa 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 (195–197 ja 201 kohta sekä tuomiolauselman 5 kohta).

V. Henkilötietojen suoja internetissä

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

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

Tässä tuomiossa (ks. myös otsikko II.3 "Henkilötietojen käsittelyn käsite") unionin tuomioistuin täsmensi laajuutta, joka on direktiivissä 95/46 säädetyllä oikeudella tutustua henkilötietoihin ja oikeudella vastustaa niiden käsittelyä internetissä.

Niinpä lausuaan 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 suoritetun 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 internetsivuilla, ja näin on tilanteen mukaan jopa silloin, kun niiden julkaiseminen mainituilla sivuilla on itsessään laillista (88 kohta ja tuomiolauselman 3 kohta).

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 (93 kohta). 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 (94 kohta). Tässä yhteydessä on korostettava, että rekisteröidyllä siihen olevan oikeuden toteaminen, ettei hänen henkilöönsä koskevia tietoja liitetä enää hänen nimeensä hakutulosten luettelossa, ei edellytä sitä, että kyseessä olevien tietojen sisällyttäminen hakutulosten luetteloon aiheuttaa vahinkoa (96 kohta ja tuomiolauselman 4 kohta).

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 (97 kohta ja tuomiolauselman 4 kohta).

2. Henkilötietojen käsittely ja immateriaalioikeudet

[*Tuomio 29.1.2008 \(suuri jaosto\), Promusicae \(C-275/06, EU:C:2008:54\)*](#)⁵⁹

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-

⁵⁹ Mainittu tuomio on esitetty vuoden 2008 vuosikertomuksessa, s. 46.

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 säännöstyössä 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,⁶⁰ tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa annetussa direktiivissä 2001/29/EY,⁶¹ teollis- ja tekijänoikeuksien noudattamisen varmistamisesta annetussa direktiivissä 2004/48/EY⁶² 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 (70 kohta ja tuomiolauselma).

[Tuomio 24.11.2011, Scarlet Extended \(C-70/10, EU:C:2011:771\)](#)⁶³

Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) oli todennut, että Scarlet Extended SA -nimisen internetyhteyden tarjoajan (jäljempänä Scarlet) palveluja käyttävät internetin käyttäjät lataavat internetistä ilman lupaa ja tekijänoikeuskorvauksia maksamatta sen teosvalikoiman teoksia käyttämällä vertaisverkkoja (peer-to-peer). SABAM saattoi asian

⁶⁰ 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).

⁶¹ 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).

⁶² 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).

⁶³ Mainittu tuomio on esitetty vuoden 2011 vuosikertomuksessa, s. 37.

kansallisen tuomioistuimen käsiteltäväksi, ja sai ensimmäisessä oikeusasteessa ratkaisun, jolla Scarlet määrättiin lopettamaan tekijänoikeusloukkaukset tekemällä mahdottomaksi kaiken SABAMin kokoelmaan kuuluvan musiikkiteoksen sisältävien tiedostojen lähettämisen ja vastaanottamisen.

Cour d'appel de Bruxelles (Brysselin ylioikeus, Belgia), jonka käsiteltäväksi Scarlet oli saattanut asian, lykkäsi asian käsittelyä ja esitti unionin tuomioistuimelle ennakkoratkaisupyynnön siitä, oliko tällainen määräys unionin oikeuden mukainen.

Unionin tuomioistuin katsoi, että direktiivejä 95/46, 2000/31, 2001/29, 2002/58 ja 2004/48, luettuina yhdessä ja tulkittuina niiden vaatimusten valossa, joita asiaa koskevien perusoikeuksien suojaamisesta aiheutuu, on tulkittava niin, että ne ovat esteenä sille, että Scarlet määrätään ottamaan käyttöön suodatusjärjestelmä, joka koskee kaikkia sen palveluiden kautta kulkevia sähköisiä viestejä ja erityisesti vertaisverkko-ohjelmistojen kautta kulkevia viestejä ja jota sovelletaan erotuksetta koko sen asiakaskuntaan, ennakolta, ja joka toteutetaan täysin internetyhteyden tarjoajan omalla kustannuksella ja jolle ei ole asetettu ajallista rajoitusta ja joka pystyy tunnistamaan internetyhteyden tarjoajan verkosta sellaisten sähköisten tiedostojen liikenteen, jotka sisältävät musiikkiteoksen, elokuvateoksen tai audiovisuaalisen teoksen, jota koskevien immateriaalioikeuksien haltija määräystä vaatinut väittää olevansa, sellaisten tiedostojen siirron estämiseksi, joiden vaihtaminen loukkaa tekijänoikeutta (54 kohta ja tuomiolauselma).

Unionin tuomioistuimen mukaan nimittäin tällainen määräys ei ole sen direktiivin 2003/31 15 artiklan 1 kohdassa asetetun kiellon mukainen, jonka mukaan internetyhteyden tarjoajalle ei saa asettaa yleistä valvontavelvollisuutta, eikä se täytä myöskään vaatimusta, jonka mukaan on varmistettava asianmukainen tasapaino yhtäältä immateriaalioikeuden suojan ja toisaalta elinkeinovapauden, oikeuden henkilötietojen suojaan ja vapauden vastaanottaa ja levittää tietoja välillä (40 ja 49 kohta).

Unionin tuomioistuin totesi tässä yhteydessä yhtäältä, että on selvää, että määräys riidanalaisen suodatusjärjestelmän käyttöönotosta merkitsisi kaiken sisällön järjestelmällistä analysointia sekä niiden käyttäjien IP-osoitteiden keräämistä ja yksilöimistä, joilta verkkoon on alun perin lähetetty laitonta sisältöä, ja että kyseiset osoitteet ovat suojattuja henkilötietoja, koska niiden avulla mainitut käyttäjät on mahdollista tunnistaa täsmällisesti (51 kohta). Toisaalta mainittu määräys saattaisi myös vaarantaa tiedonvälityksen vapauden, koska kyseinen järjestelmä ei välttämättä riittävästi erottelisi laitonta ja laillista sisältöä, joten sen käyttö saattaisi johtaa sellaisten viestien estämiseen, joiden sisältö on laillinen. Ei nimittäin ole kiistetty, että vastaus kysymykseen siirron laillisuudesta riippuu myös tekijänoikeudesta tehtyjen sellaisten laillisten poikkeusten soveltamisesta, jotka vaihtelevat jäsenvaltiosta toiseen. Lisäksi tietyt teokset saattavat olla tietyissä jäsenvaltioissa vapaasti käytettävissä tai kyseessä olevat tekijät ovat saattaneet laittaa ne verkkoon ilmaiseksi (52 kohta).

Näin ollen unionin tuomioistuin totesi, että kun kyseinen kansallinen tuomioistuin on antanut määräyksen, jolla se on velvoittanut Scarletin ottamaan käyttöön riidanalaisen suodatusjärjestelmän, se ei ole noudattanut vaatimusta asianmukaisen tasapainon varmistamisesta yhtäältä immateriaalioikeuden suojan ja toisaalta elinkeinovapauden, oikeuden henkilötietojen suojaan ja vapauden vastaanottaa ja levittää tietoja välillä (53 kohta).

[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 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 (55 ja 56 kohta).

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 pyydetty 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 (58 kohta).

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 (61 kohta ja tuomiolauselma).

[Tuomio 17.6.2021, M.I.C.M. \(C-597/19, EU:C:2021:492\)](#)

Mircom International Content Management & Consulting (M.I.C.M.) Limited -niminen yritys (jäljempänä Mircom) on esittänyt Ondernemingsrechtbank Antwerpenille (Antwerpenin yritystuomioistuin, Belgia; jäljempänä ennakkoratkaisua pyytänyt tuomioistuin) tietopyynnön, joka kohdistuu Telenet BVBA -nimiseen internetyhteyden tarjoajaan. Kyseisellä pyynnöllä pyritään saamaan päätös, jolla Telenet veloitetaan esittämään asiakkaidensa tunnistustiedot erikoistuneen yhtiön Mircomin lukuun keräämien IP-osoitteiden perusteella. Telenetin asiakkaiden internetyhteyksiä on käytetty Mircomin tuotevalikoimaan kuuluvien elokuvien jakamiseen vertaisverkossa (peer-to-peer) BitTorrent-protokollan avulla. Telenet vastustaa Mircomin pyyntöä.

Ennakkoratkaisua pyytänyt tuomioistuin on tässä tilanteessa ensinnäkin tiedustellut unionin tuomioistuimelta, onko suojatun teoksen sisältävän mediatiedoston osien jakaminen mainitussa verkossa yleisölle välittämistä unionin oikeuden nojalla. Se pyrkii tämän jälkeen selvittämään, voiko Mircomin kaltainen immateriaalioikeuksien haltija, joka ei käytä näitä oikeuksia vaan vaatii vahingonkorvausta oletetuilta loukkaajilta, hyötyä unionin oikeudessa säädetyistä toimenpiteistä, menettelyistä ja oikeussuojakeinoista kyseisten oikeuksien noudattamisen varmistamiseksi esimerkiksi tietoja pyytämällä. Ennakkoratkaisua pyytänyt tuomioistuin pyytää lopuksi unionin tuomioistuinta selvittämään kysymystä yhtäältä sen tavan laillisuudesta, jolla Mircom on kerännyt asiakkaiden IP-osoitteet, ja toisaalta sen laillisuudesta, että Telenet toimittaa Mircomin pyytämät tiedot.

Unionin tuomioistuin toteaa, että unionin oikeus⁶⁴ ei lähtökohtaisesti ole esteenä sille, että immateriaalioikeuksien haltija tai kolmas osapuoli sen lukuun tallentavat järjestelmällisesti sellaisten vertaisverkon käyttäjien IP-osoitteet, joiden internetyhteyksiä väitetään käytetyn loukkaavassa toiminnassa (alkuvaiheen käsittely), eikä sille, että käyttäjien nimet ja postiosoitteet toimitetaan kyseiselle oikeudenhaltijalle tai kolmannelle osapuolelle vahingonkorvauskannetta varten (myöhemmän vaiheen käsittely). Tätä koskevien aloitteiden ja pyyntöjen on kuitenkin oltava perusteltuja ja oikeasuhteisia eivätkä ne saa merkitä väärinkäyttöä, ja niistä on säädettävä kansallisessa lainsäädännöllisessä toimenpiteessä, jolla rajoitetaan unionin oikeuden alaan kuuluvien oikeuksien ja velvollisuuksien ulottuvuutta. Unionin tuomioistuin täsmentää, että unionin oikeudessa ei säädetä Telenetin kaltaiselle yhtiölle velvollisuudesta toimittaa yksityishenkilöille henkilötietoja, jotta siviilituomioistuimissa voidaan panna vireille menettely tekijänoikeuksien loukkauksien vuoksi. Unionin oikeuden mukaan jäsenvaltiot voivat kuitenkin asettaa tällaisen velvollisuuden (97 ja 125–127 kohta ja tuomiolauselman 3 kohta).

3. Henkilötietojen poistaminen hakutulosten luettelosta

⁶⁴ Yleisen tietosuojasetuksen 6 artiklan 1 kohdan f alakohta ja direktiivin 2002/58 15 artiklan 1 kohta.

[Tuomio 24.9.2019 \(suuri jaosto\), GC ym. \(Arkaluonteisten tietojen poistaminen hakutulosten luettelosta\) \(C-136/17, EU:C:2019:773\)⁶⁵](#)

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 pyynnöt 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 kiellettyä⁶⁶ tietyin poikkeuksin. Rikoksiin, tuomioihin tai turvaamistoimiin liittyvää tietojenkäsittelyä voidaan lähtökohtaisesti suorittaa ainoastaan julkisen viranomaisen valvonnassa tai jos kansallisessa lainsäädännössä säädetään erityisistä tarpeellisista suojatoimista⁶⁷ (39 ja 40 kohta).

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 (42–44 kohta).

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 (46 ja 47 kohta).

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

⁶⁵ Mainittu tuomio on esitetty vuoden 2019 vuosikertomuksessa, s. 117 ja 118.

⁶⁶ Direktiivin 95/46 8 artiklan 1 kohta ja asetuksen 2016/679 9 artiklan 1 kohta.

⁶⁷ Direktiivin 95/46 8 artiklan 5 kohta ja asetuksen 2016/679 10 artikla.

luettelosta poistamista koskevan pyynnön, jos se toteaa, että kyseessä olevat linkit johtavat sisältöihin, joissa on henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi,⁶⁸ 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 vuoksi⁶⁹ (65 ja 69 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 suoritetun haun johdosta näkyvään luetteloon tarpeen sitä tiedonvälityksen vapautta koskevan oikeuden käyttämiseen, joka on internetin käyttäjillä, jotka ovat mahdollisesti kiinnostuneita saamaan kyseisen internetsivun tällaisella haululla 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 (66 ja 68 kohta).

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 suoritetun 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 luettelo 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 (77 ja 78 kohta).

[Tuomio 24.9.2019 \(suuri jaosto\), Google \(Hakutulosten luettelosta poistamista koskevan oikeuden alueellinen ulottuvuus\) \(C-507/17, EU:C:2019:772\)](#)⁷⁰

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

⁶⁸ Direktiivin 95/46 8 artiklan 2 kohdan e alakohta ja asetuksen 2016/679 9 artiklan 2 kohdan e alakohta.

⁶⁹ Direktiivin 95/46 14 artiklan ensimmäisen kohdan a alakohta ja asetuksen 2016/679 21 artiklan 1 kohta.

⁷⁰ Mainittu tuomio on esitetty vuoden 2019 vuosikertomuksessa, s. 118 ja 119.

nimellään suoritetun 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.⁷¹

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 suojelu kaikkialla unionissa, unionin oikeudesta⁷² 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 suojaa 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 (62 ja 73 kohta).

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 (70 kohta).

⁷¹ Direktiivin 95/46 4 artiklan 1 kohdan a alakohta ja asetuksen 2016/679 3 artiklan 1 kohta.

⁷² 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 kiellä. 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 (65 ja 72 kohta).

4. Internetsivun käyttäjän suostumus tietojen tallentamiseen tai tietojen käyttämiseen evästeiden avulla

[Tuomio 1.10.2019 \(suuri jaosto\), Planet49 \(C-673/17, EU:C:2019:801\)](#)⁷³

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.

Ennakkoratkaisupyynnö koski lähinnä direktiivissä 2002/58,⁷⁴ luettuna yhdessä direktiivin 95/46⁷⁵ sekä yleisen tietosuojasetuksen⁷⁶ 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 tietosuojasetuksessa säädetään siten vastedes nimenomaisesti aktiivisesta suostumuksesta,⁷⁷ 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” (49, 52, 56 ja 62 kohta).

⁷³ Mainittu tuomio on esitetty vuoden 2019 vuosikertomuksessa, s. 120 ja 121.

⁷⁴ 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.

⁷⁵ Direktiivin 95/46 2 artiklan h alakohta.

⁷⁶ Asetuksen 2016/679 6 artiklan 1 kohdan a alakohta.

⁷⁷ IDEM.

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 evätäkseen 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 (63 kohta).

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 (69 ja 71 kohta).

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 (73–75 ja 81 kohta).

VI. Kansalliset valvontaviranomaiset

1. Riippumattomuusvaatimuksen ulottuvuus

[*Tuomio 9.3.2010 \(suuri jaosto\), komissio v. Saksa \(C-518/07, EU:C:2010:125\)*](#)⁷⁸

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

⁷⁸ Mainittu tuomio on esitetty vuoden 2010 vuosikertomuksessa, s. 34.

kanssa samaan hallintokoneistoon kuuluvat viranomaiset, joiden on ensin mainittujen tavoin täytettävä direktiivin 95/46 tavoitteet.

Unionin tuomioistuin katsoi, että direktiivissä 95/46 tarkoitettulla 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 (25 kohta).

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 ennakkoiden 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 suojaa valvovaksi viranomaiseksi perustetun Datenschutzkommissionin (tietosuojalautakunta) osalta.

Unionin tuomioistuin totesi, että Itävallan tasavalta ei ollut noudattanut jäsenyysvelvoitteitaan, 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 (66 kohta ja tuomiolauselma).

Unionin tuomioistuin muistutti ensimmäiseksi, että direktiivin 95/46 28 artiklan 1 kohdan toisen alakohdan ilmaisua "itsenäisesti" on tulkittava siten, että valvovilla viranomaisilla on oltava sellainen itsenäisyys, että ne voivat hoitaa tehtäviään ilman ulkopuolista vaikuttamista. Se, että tällainen viranomaisen 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 (41–43 ja 52 kohta).

Unionin tuomioistuin täsmensi, että jotta henkilötietojen suojaaja 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" (58 kohta).

[Tuomio 8.4.2014 \(suuri jaosto\), komissio v. Unkari \(C-288/12, EU:C:2014:237\)⁷⁹](#)

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

Unionin tuomioistuin katsoi, että jäsenvaltio, joka päättää henkilötietojen suojaaja valvovan viranomaisen toimikauden ennenaikaisesti, ei noudata direktiivin 95/46 mukaisia velvoitteitaan (62 kohta ja tuomiolauselman 1 kohta).

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 (51 kohta).

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

⁷⁹ Mainittu tuomio on esitetty vuoden 2014 vuosikertomuksessa, s. 62.

ilmassa kaiken aikaa tämän viranomaisen hoitaessa tehtävänsä, 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 (52–55 kohta).

2. Sovellettavan oikeuden ja toimivaltaisen valvontaviranomaisen määrittäminen

[*Tuomio 1.10.2015, Weltimmo \(C-230/14, EU:C:2015:639\)*](#)⁸⁰

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 pyynnöstään 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 (41 kohta ja tuomiolauselman 1 kohta).

⁸⁰ Mainittu tuomio on esitetty vuoden 2015 vuosikertomuksessa, s. 55.

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 (54 kohta). 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 (57 ja 60 kohta sekä tuomiolauselman 2 kohta).

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 (43 kohta).

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 (44 kohta).

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 suojaa 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 (45 ja 47 kohta).

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

Tässä tuomiossa (ks. myös otsikko II.5 ”Käsite ’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) (64 kohta ja tuomiolauselman 2 kohta).

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 toimivaltuuksia 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 toimivaltuuksiaan alueelleen sijoittautuneen elimen suhteen pyytämättä ensin kyseisen toisen jäsenvaltion valvontaviranomaista toimimaan (74 kohta ja tuomiolauselman 3 kohta).

[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, yhteisöliitännäisten⁸¹ 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.

⁸¹ Esimerkiksi painikkeet ”tykkää” tai ”jaa”.

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

Ennakkoratkaisua pyytäneellä tuomioistuimella on epäilyjä yleisessä tietosuojasetuksessa⁸² 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 tietosuojasetuksessa säädetyn ”yhden luukun” periaatteen nojalla vaikuttaa näet siltä, että ainoastaan Irlannin tietosuojavaltuutettu olisi toimivaltainen nostamaan kieltokanteen Irlannin tuomioistuinten valvonnassa (36 ja 37 kohta).

Unionin tuomioistuimen suuri jaosto täsmentää tuomiossaan kansallisten valvontaviranomaisten valtuudet yleisen tietosuojasetuksen puitteissa. Se katsoo erityisesti, että tässä asetuksessa sallitaan tietyin edellytyksin se, että jäsenvaltion valvontaviranomainen käyttää valtuuksiaan saattaa kaikki yleisen tietosuojasetuksen väitetyt rikkomiset tämän valtion tuomioistuimen tietoon ja tarvittaessa panna vireille tai käynnistää muulla tavoin oikeustoimet siltä osin kuin kyse on rajatylittävästä tietojenkäsittelystä,⁸³ vaikka se ei ole johtava valvontaviranomainen tämän käsittelyn osalta (tuomiolauselman 1 kohta).

Unionin tuomioistuin täsmentää ensiksi edellytykset, joita noudattaen kansallisen valvontaviranomaisen, joka ei ole johtava valvontaviranomainen rajatylittävän tietojenkäsittelyn osalta, on käytettävä valtuuksiaan saattaa kaikki yleisen tietosuojasetuksen väitetyt rikkomiset jäsenvaltion tuomioistuimen tietoon ja tarvittaessa panna vireille tai käynnistää muulla tavoin oikeustoimet tämän asetuksen soveltamisen varmistamiseksi. Niinpä yhtäältä yleisessä tietosuojasetuksessa 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 noudattaen⁸⁴ (75 kohta ja tuomiolauselman 1 kohta).

Yleisessä tietosuojasetuksessa säädetään nimittäin ”yhden luukun” järjestelmästä,⁸⁵ 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 tietosuojasetuksessa annetaan johtavalle valvontaviranomaiselle lähtökohtainen toimivalta tehdä päätös, jossa todetaan, että rajatylittävällä käsittelyllä rikotaan

⁸² Yleisen tietosuojasetuksen 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 kuitenkaan rajoittamatta 55 artiklan soveltamista.”

⁸³ Yleisen tietosuojasetuksen 4 artiklan 23 kohta.

⁸⁴ Yleisen tietosuojasetuksen 56 ja 60 artikla.

⁸⁵ Yleisen tietosuojasetuksen 56 artiklan 1 kohta.

tässä asetuksessa vahvistettuja sääntöjä,⁸⁶ kun taas poikkeuksena on muiden osallistuvien valvontaviranomaisten toimivalta tehdä tällainen päätös, edes väliaikainen.⁸⁷ 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 (50–53, 56–59 ja 63–65 kohta).

Unionin tuomioistuin 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,⁸⁸ on yhteensopivaa Euroopan unionin perusoikeuskirjan 7, 8 ja 47 artiklan kanssa, joissa taataan rekisteröidylle oikeus henkilötietojensa suojaan ja oikeus tehokkaisiin oikeussuojakeinoihin (67 kohta).

Unionin tuomioistuin katsoo toiseksi, että rajatylittävän tietojenkäsittelyn tilanteessa jäsenvaltion valvontaviranomaisen, joka ei ole johtava valvontaviranomainen, oikeudellisen menettelyn vireille panemista koskevien valtuuksien käyttäminen⁸⁹ 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,⁹⁰ mikä edellyttää, että rajatylittävää käsittelyä suorittavalla rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka unionin alueella (80, 83 ja 84 kohta sekä tuomiolauselman 2 kohta).

Unionin tuomioistuin 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 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.

⁸⁶ Yleisen tietosuoja-asetuksen 60 artiklan 7 kohta.

⁸⁷ Yleisen tietosuoja-asetuksen 56 artiklan 2 kohdassa ja 66 artiklassa säädetään johtavan valvontaviranomaisen päätöksentekotoimivallan periaatteesta tehtävistä poikkeuksista.

⁸⁸ Yleisen tietosuoja-asetuksen 55 ja 56 artikla, luettuina yhdessä asetuksen 60 artiklan kanssa.

⁸⁹ Yleisen tietosuoja-asetuksen 58 artiklan 5 kohdan nojalla.

⁹⁰ 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”.

Unionin tuomioistuin täsmentää, että näiden valtuuksien käyttäminen edellyttää kuitenkin, että yleinen tietosuojasetus 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 tietosuojasetuksen soveltamisalaan (94–96 kohta ja tuomiolauselman 3 kohta).

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 tietosuojasetus 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 tietosuojasetuksen 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 (105 kohta ja tuomiolauselman 4 kohta).

Unionin tuomioistuin toteaa viidenneksi ja viimeiseksi, että yleisen tietosuojasetuksen 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 (113 kohta ja tuomiolauselman 5 kohta).

VII. Unionin lainsäädännön alueellinen soveltamisala

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

Tässä tuomiossa (ks. myös otsikko II.3 "Henkilötietojen käsittelyn käsite" ja otsikko V.1 "Oikeus vastustaa henkilötietojen käsittelyä ("oikeus tulla unohdetuksi")" unionin tuomioistuin lausui myös direktiivin 95/46 alueellisesta soveltamisalasta.

Sen mukaan henkilötietojen käsittely suoritetaan jäsenvaltion alueella sijaitsevassa rekisterinpitäjän toimipaikassa tapahtuvan toiminnan yhteydessä kyseisessä direktiivissä tarkoitetulla tavalla silloin, kun hakukoneen ylläpitäjä – huolimatta siitä, että sen kotipaikka on kolmannessa valtiossa – perustaa jäsenvaltioon sivuliikkeen tai tytäryhtiön, jonka tehtävänä on markkinoida ja myydä hakukoneen tarjoamia mainospaikkoja ja jonka toiminta kohdistuu kyseisen jäsenvaltion asukkaisiin (55 ja 60 kohta sekä tuomiolauselman 2 kohta).

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 (56 kohta).

VIII. Yleisön oikeus tutustua Euroopan unionin toimielinten asiakirjoihin ja henkilötietojen suoja

[*Tuomio 29.6.2010 \(suuri jaosto\), komissio v. Bavarian Lager \(C-28/08 P, EU:C:2010:378\)*](#)

Bavarian Lager on yhtiö, jonka tarkoituksena on tuoda saksalaista olutta Yhdistyneessä kuningaskunnassa oleviin anniskelupaikkoihin. Se ei kuitenkaan voinut myydä tuotettaan, koska suuri joukko anniskelupaikkojen pitäjistä Yhdistyneessä kuningaskunnassa oli sidottu yksinostosopimuksiin, jotka velvoittivat ne hankkimaan oluen tietyiltä panimoilta.

Oluen toimittamista koskevan Yhdistyneen kuningaskunnan määräyksen (jäljempänä GBP) mukaan brittiläisten panimoiden on myönnettävä pubien pitäjille mahdollisuus ostaa toisesta panimosta tulevaa olutta edellyttäen, että se on tynnyrissä kypsytettävää olutta. Suurinta osaa Yhdistyneen kuningaskunnan ulkopuolella tuotetuista oluista ei voida pitää GBP:ssä tarkoitettuna tynnyrissä kypsytettävänä oluena, eivätkä ne siten kuulu GBP:n soveltamisalaan. Bavarian Lager katsoi, että mainittu säännöstö oli tuonnin määrällistä rajoitusta vaikutukseltaan vastaava toimenpide ja teki komissiolle kantelun.

Komissio pani Yhdistynyttä kuningaskuntaa vastaan vireille jäsenyysvelvoitteiden noudattamatta jättämistä koskevan menettelyn, jonka aikana yhteisön ja Yhdistyneen kuningaskunnan viranomaisten sekä yhteismarkkinoiden panimoliiton (jäljempänä CBMC) edustajat osallistuivat 11.10.1996 pidettyyn kokoukseen. Saatuaan Yhdistyneen kuningaskunnan viranomaisilta tietää kyseessä olevan säännösten muutosesityksestä, jonka mukaan pullossa kypsytettävää olutta voitaisiin jälleenmyydä vierasoluena samoin kuin tynnyrissä kypsytettävää oluttakin, komissio ilmoitti Bavarian Lagerille jäsenyysvelvoitteiden noudattamatta jättämistä koskevan menettelyn lykkäämisestä.

Bavarian Lager esitti pyynnön saada lokakuussa 1996 pidetyn kokouksen täydellinen pöytäkirja, joka sisältää kaikkien osanottajien nimet. Komissio epäsi tämän pyynnön 18.3.2004 tekemällään päätöksellä vedoten muun muassa kyseisten henkilöiden yksityiselämän suojaan, sellaisena kuin se taataan asetuksessa N:o 45/2001.

Tämän jälkeen Bavarian Lager nosti kanteen unionin yleisessä tuomioistuimessa ja vaati komission mainitun päätöksen kumoamista. Unionin yleinen tuomioistuin kumosi komission päätöksen 8.11.2007 antamallaan tuomiolla ja katsoi, että pelkästään se, että asianomaisen henkilön nimi esiintyy jonkin kokouksen osanottajien luettelossa sillä perusteella, että hän edustaa tiettyä yhteisöä, ei merkitse minkäänlaista loukkausta saati vahingoita asianomaisten henkilöiden yksityiselämän suojaa. Komissio, jota Yhdistynyt kuningaskunta ja neuvosto tukivat, valitti kyseisestä tuomiosta unionin tuomioistuimeen.

Unionin tuomioistuin totesi ensinnäkin, että silloin, kun asiakirjojen saamisesta yleisön tutustuttavaksi annetussa asetuksessa N:o 1049/2001⁹¹ perustuvalla hakemuksella pyydetään oikeutta tutustua henkilötietoja sisältävään asiakirjaan, asetuksen N:o 45/2001 säännökset tulevat kaikilta osin sovellettaviksi, myös säännös, jonka mukaan henkilötietojen siirron vastaanottaja veloitetaan osoittamaan tietojen ilmaisemisen olevan tarpeen, ja säännös, jonka mukaan rekisteröidyllä on oikeus milloin tahansa vastustaa itseään koskevien tietojen käsittelyä tilanteeseensa liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi (63 kohta).

Unionin tuomioistuin totesi myös, että jäsenyysveloitteiden noudattamatta jättämistä koskevan menettelyn yhteydessä pidetyn kokouksen osanottajien luettelo sisältää asetuksen N:o 45/2001 2 artiklan a alakohdassa tarkoitettuja henkilötietoja, koska henkilöt, jotka ovat voineet osallistua tähän kokoukseen, ovat siitä tunnistettavissa (70 kohta).

Se katsoi lisäksi, että vaatiessaan Bavarian Lageria osoittamaan niiden henkilöiden, jotka eivät olleet antaneet nimenomaista suostumustaan, henkilötietojen siirron olleen tarpeen komissio on toiminut asetuksen N:o 45/2001 8 artiklan b alakohdan säännösten mukaisesti (77 kohta).

Koska asetuksen N:o 1049/2001 mukaisen asiakirjoihin tutustumista koskevan pyynnön yhteydessä ei ollut esitetty mitään nimenomaista ja laillista tarkoitusta eikä minkäänlaisia vakuuttavia argumentteja, joilla osoitettaisiin tarve näiden henkilötietojen siirtoon, komissio ei voi vertailla asianosaisten eri intressejä. Se ei voi myöskään selvittää, oliko syytä ajatella, että rekisteröityjen oikeudet edut voisivat siirron vuoksi vaarantua, kuten asetuksen N:o 45/2001 8 artiklan b alakohdassa edellytetään (78 kohta).⁹²

[Tuomio 16.7.2015, ClientEarth ja PAN Europe v. EFSA \(C-615/13 P, EU:C:2015:489\)](#)

Euroopan elintarviketurvallisuusviranomainen (jäljempänä EFSA) oli perustanut työryhmän laatiakseen ohjeet asetuksen (EY) N:o 1107/2009⁹³ 8 artiklan 5 kohdan täytäntöönpanemisesta. Mainitun säännöksen mukaan kasvinsuojeluaineen markkinoille saattamista koskevan luvan hakijan on oheistettava asiakirja-aineistoon EFSan määrittämä vertaisarvioitu vapaasti käytettävissä oleva sellainen tieteellinen aineisto, jossa käsitellään tehoaineen ja sen aineenvaihduntatuotteiden haitallisia sivuvaikutuksia terveyteen, ympäristöön ja muihin kuin torjuttaviin lajeihin.

Ohjeiden luonnoksesta järjestettiin julkinen kuuleminen, jonka yhteydessä ClientEarth ja Pesticide Action Network Europe (PAN Europe) esittivät huomautuksia luonnoksesta. Ne esittivät tässä yhteydessä yhdessä EFSAlle pyynnön saada tutustua useisiin asiakirjoihin, jotka koskivat ohjelunonoksen valmisteluun liittyviä asiakirjoja, myös ulkopuolisten asiantuntijoiden esittämiä huomautuksia.

⁹¹ Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi 30.5.2001 annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001 (EYVL 2001, L 145, s. 43).

⁹² Mainittu tuomio on esitetty vuoden 2010 vuosikertomuksessa, s. 14.

⁹³ Kasvinsuojeluaineiden markkinoille saattamisesta sekä neuvoston direktiivien 79/117/ETY ja 91/414/ETY kumoamisesta 21.10.2009 annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 1107/2009 (EUVL 2009, L 309, s. 1).

EFSA myönsi ClientEarthille ja PAN Europelle oikeuden tutustua muun muassa ulkopuolisten asiantuntijoiden ohjelunoksesta esittämiin huomautuksiin. Se totesi kuitenkin, että se oli poistanut kyseisten asiantuntijoiden nimet asetuksen N:o 1049/2001 4 artiklan 1 kohdan b alakohdan sekä henkilötietojen suojaa koskevan unionin lainsäädännön ja erityisesti asetuksen N:o 45/2001 mukaisesti. Se väitti, että näiden asiantuntijoiden nimien paljastamista oli pidettävä asetuksen N:o 45/2001 8 artiklassa tarkoitettuna henkilötietojen siirtämisenä, eivätkä kyseisessä artiklassa asetetut tietojen siirtoa koskevat edellytykset käsiteltävässä asiassa täyttyneet.

ClientEarth ja PAN Europe nostivat unionin yleisessä tuomioistuimessa kanteen, jolla vaadittiin kumottavaksi EFSA:n tekemä päätös. Unionin yleinen tuomioistuin hylkäsi kanteen,⁹⁴ minkä jälkeen ClientEarth ja PAN Europe tekivät valituksen unionin tuomioistuimeen.

Unionin tuomioistuin totesi ensimmäiseksi, että sen johdosta, että tämän tiedon perusteella tietty asiantuntija voitaisiin yhdistää tiettyihin huomautuksiin, se koskee tunnistettua luonnollista henkilöä ja muodostaa näin ollen asetuksen N:o 45/2001 2 artiklan a alakohdassa tarkoitettua henkilötiedon. Koska asetuksen N:o 45/2001 2 artiklan a alakohdassa oleva henkilötietojen käsite ei vastaa yksityiselämää koskevien tietojen käsitettä, unionin tuomioistuin katsoi myös, että ClientEarthin ja PAN Europen väite siitä, että riidanalaiset tiedot eivät koske kyseisten asiantuntijoiden yksityiselämää, on tehoton (29 ja 32 kohta).

Unionin tuomioistuin tutki tämän jälkeen ClientEarthin ja PAN Europen argumentin, joka perustui EFSAan kohdistuvaan luottamuspuolaan, sillä sitä syytettiin usein puolueellisuudesta, koska se käytti asiantuntijoita, joilla oli henkilökohtaisia intressejä, jotka perustuivat heillä teollisuuspiireihin oleviin yhteyksiin, ja tarpeeseen varmistaa kyseisen viranomaisen päätöksentekomenettelyn avoimuus. Tämän argumentin tueksi oli esitetty tutkimus, josta ilmeni, että valtaosalla asiantuntijoista, jotka olivat jäseniä EFSA:n työryhmässä, oli yhteyksiä teollisuuden painostusryhmiin. Unionin tuomioistuin totesi tästä, että asiantuntijoiden nimien saaminen oli tässä yhteydessä tarpeellista, jotta voitiin varmistua konkreettisesti kunkin asiantuntijan puolueettomuudesta hänen tieteellisessä tehtävässään EFSA:n palveluksessa. Täten unionin tuomioistuin kumosi valituksenalaisen tuomion todeten, että unionin yleinen tuomioistuin oli katsonut virheellisesti, että ClientEarthin ja PAN Europen edellä mainittu argumentti ei riittänyt osoittamaan riidanalaisten tietojen siirtämisen tarpeellisuutta (57–59 kohta).

Kolmanneksi arvioidakseen EFSA:n riidanalaisen päätöksen laillisuutta unionin tuomioistuin tutki, oliko syytä olettaa, että kyseisellä siirtämisellä voitiin vaarantaa kyseisten henkilöiden oikeutettuja etuja. Se totesi tästä, että EFSA:n väite siitä, että riidanalaisten tietojen luovuttaminen olisi aiheuttanut vaaran mainittujen asiantuntijoiden yksityiselämän tai koskemattomuuden loukkaamisesta, on yleisluontoinen toteamus, jonka tueksi ei ole esitetty mitään asiaan liittyvää seikkaa. Unionin tuomioistuin katsoi päinvastoin, että tällaisella tietojen luovuttamisella olisi sitä vastoin itsessään voitu häivyttää puheena olevat puolueellisuusepäilyt, tai se olisi antanut mahdollisesti kyseeseen tuleville asiantuntijoille tilaisuuden riitauttaa – tarvittaessa käytettävissä olevin oikeusturvakeinoin – näiden puolueellisuusväitteiden oikeellisuus. Näiden seikkojen perusteella unionin tuomioistuin kumosi EFSA:n päätöksen (69 ja 73 kohta).

⁹⁴ Tuomio 13.9.2013, ClientEarth ja PAN Europe v. EFSA (T-214/11, [EU:T:2013:483](#)).

* * *

Tässä muistiossa esitetyt tuomiot on indeksoitu Oikeuskäytännön hakemiston otsikoihin 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07 ja 4.11.11.01.