Oikeustapauskokoelma

JULKISASIAMIEHEN RATKAISUEHDOTUS
HENRIK SAUGMANDSGAARD ØE
19 päivänä joulukuuta 2019[1]

Asia C-311/18

Data Protection Commissioner
vastaan
Facebook Ireland Limited ja
Maximillian Schrems,
Amerikan yhdysvaltojen,
Electronic Privacy Information Centren,
BSA Business Software Alliance, Inc:n ja
Digitaleuropen
osallistuessa asian käsittelyyn

(Ennakkoratkaisupyyntö – High Court (ylempi piirituomioistuin, Irlanti))

Ennakkoratkaisupyyntö – Luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä – Asetus (EU) 2016/679 – 2 artiklan 2 kohta – Soveltamisala – Henkilötietojen siirto kaupallisessa tarkoituksessa Amerikan yhdysvaltoihin – Amerikan yhdysvaltojen viranomaisten toteuttama siirrettyjen tietojen käsittely kansallista turvallisuutta varten – 45 artikla – Kolmannen maan tietosuojan riittävyyden arviointi – 46 artikla – Rekisterinpitäjän toteuttamat asianmukaiset suojatoimet – Tietosuojaa koskevat vakiolausekkeet – 58 artiklan 2 kohta – Valvontaviranomaisten toimivaltuudet – Päätös 2010/87/EU – Pätevyys – Täytäntöönpanopäätös (EU) 2016/1250 – EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely – Pätevyys – Euroopan unionin perusoikeuskirjan 7, 8 ja 47 artikla

Sisällys

I Johdanto 3

II Asiaa koskevat oikeussäännöt 4

A Direktiivi 95/46/EY 4

B Tietosuoja-asetus 6

C Päätös 2010/87 10

D Privacy Shield -päätös 14

1 Alkuperäinen kieli: ranska.

III Pääasia, ennakkoratkaisukysymykset ja asian käsittely unionin tuomioistuimessa 15

IV Asian tarkastelu 24

A Alustavat toteamukset 24

B Ennakkoratkaisupyynnön tutkittavaksi ottaminen 25

1. Direktiivin 95/46 ajallinen sovellettavuus 25

2. DPC:n ilmaisemien epäilyjen alustavuus 26

3. Asian tosiseikkojen määrittämiseen liittyvät epävarmuustekijät 27

C Unionin oikeuden sovellettavuus siirrettäessä henkilötietoja kaupallisessa tarkoituksessa kolmanteen valtioon, joka saattaa käsitellä niitä kansallista turvallisuutta varten (ensimmäinen kysymys) 28

D Edellytetty suojan taso mallisopimuslausekkeisiin perustuvan siirron yhteydessä (kuudennen kysymyksen ensimmäinen osa) 29

E Päätöksen 2010/87 pätevyys perusoikeuskirjan 7, 8 ja 47 artiklan kannalta (seitsemäs, kahdeksas ja yhdestoista kysymys) 31

1. Rekisterinpitäjien velvollisuudet 32

2. Valvontaviranomaisten velvollisuudet 34

F Se, ettei asiassa ole tarpeen vastata muihin ennakkoratkaisukysymyksiin eikä tutkia Privacy Shield -päätöksen pätevyyttä 37

1. Se, etteivät unionin tuomioistuimen vastaukset ole tarpeen pääasian kohteen kannalta 38

2. Syyt, jotka puoltavat sitä, ettei unionin tuomioistuin tutki asiaa DPC:n vireillä olevan menettelyn kohteen kannalta 40

G Toissijaiset toteamukset Privacy Shield -päätöksen vaikutuksista ja pätevyydestä 42

1. Privacy Shield -päätöksen vaikutus siihen, miten valvontaviranomainen käsittelee sopimukseen perustuviin suojatoimiin perustuvan siirron laillisuudesta tehtyä kantelua 42

2. Privacy Shield -päätöksen pätevyys 43

a) Tietosuojan riittävyyttä koskevan päätöksen pätevyyttä koskevan tarkastelun sisältöä koskevat täsmennykset 44

1) Vertailuperusteet, joiden nojalla voidaan arvioida, onko tietosuojan taso ”pääosiltaan vastaava” 44

2) Tarve varmistaa riittävä suojan taso tietojen siirtämisvaiheessa 49

3) Komission ja ennakkoratkaisua pyytäneen tuomioistuimen Yhdysvaltojen oikeudesta esittämien tosiseikkoja koskevien toteamusten huomioon ottaminen 51

4) Pääosiltaan vastaavaa koskevan vaatimuksen ulottuvuus 52

b) Privacy Shield -päätöksen pätevyys yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevien oikeuksien kannalta 53

1) Puuttumisen olemassaolo 53

2) Puuttumisesta säätäminen lailla 55

3) Perusoikeuksien keskeisen sisällön loukkaamatta jättäminen 57

4) Oikeutetun tavoitteen toteuttaminen 60

5) Puuttumisen tarpeellisuus ja oikeasuhteisuus 61

c) Privacy Shield -päätöksen pätevyys tehokasta oikeussuojaa koskevan oikeuden kannalta .. 64

1) Yhdysvaltojen oikeudessa säädettyjen oikeussuojakeinojen tehokkuus 65

2) Oikeusasiamiesmekanismin vaikutus tehokasta oikeussuojakeinoa koskevan oikeuden suojan tasoon 69

V Ratkaisuehdotus 70

I Johdanto

1. Koska maailmassa ei ole henkilötietojen suojaa koskevia yhteisiä takeita, tällaisten tietojen rajatylittäviin siirtoihin liittyy vaara keskeytyksistä Euroopan unionissa varmistetun tietosuojan tasossa. Unionin lainsäätäjä on pyrkinyt helpottamaan näiden tietojen liikkuvuutta ja samalla rajoittamaan tätä vaaraa ottamalla käyttöön kolme mekanismia, joiden perusteella henkilötietoja voidaan siirtää unionista kolmanteen valtioon.

2. Tällainen siirto voidaan ensinnäkin toteuttaa päätöksellä, jolla Euroopan komissio toteaa, että kyseinen kolmas valtio varmistaa siihen siirrettyjen tietojen ”riittävän tietosuojan tason”.[2] Jollei tällaista päätöstä ei ole tehty, toiseksi siirto on sallittu, jos siihen liittyy ”asianmukaisia suojatoimia”.[3] Nämä suojatoimet voidaan toteuttaa tietojen viejän ja tietojen tuojan välisellä sopimuksella, johon sisällytetään komission antamia tietosuojaa koskevia vakiolausekkeita. Kolmanneksi tietosuoja-asetuksessa säädetään eräistä poikkeuksista, jotka perustuvat muun muassa rekisteröidyn suostumukseen, jonka perusteella siirto kolmanteen maahan on mahdollinen jopa ilman tietosuojan riittävyyttä koskevaa päätöstä tai asianmukaisia suojatoimia.[4]

3. High Courtin (ylempi piirituomioistuin, Irlanti) esittämä ennakkoratkaisupyyntö koskee toista näistä mekanismeista. Siinä on erityisesti kyse päätöksen 2010/87/EU[5], jolla komissio on laatinut mallisopimuslausekkeita tietyille siirtojen ryhmille, pätevyydestä Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 7, 8 ja 47 artiklan kannalta.

2 Ks. luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) (EUVL 2016, L 119, s. 1; jäljempänä tietosuoja-asetus) 45 artikla.

3 Ks. tietosuoja-asetuksen 46 artikla.

4 Ks. tietosuoja-asetuksen 49 artikla.

5 Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen siirtoa varten kolmansiin maihin sijoittautuneille henkilötietojen käsittelijöille 5.2.2010 annettu komissio päätös (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) (jäljempänä päätös 2010/87).

4. Tämä kysymys on esitetty asiassa, jossa asianosaisina ovat Data Protection Commissioner (tietosuojavaltuutettu, Irlanti; jäljempänä DPC) sekä Facebook Ireland Ltd ja Maximillian Schrems. Viimeksi mainittu teki DPC:lle kantelun siitä, että Facebook Ireland oli siirtänyt hänen henkilötietojaan Amerikan yhdysvaltoihin (jäljempänä Yhdysvallat) sijoittautuneelle emoyhtiölleen Facebook Inc:lle. DPC katsoo, että tämän kantelun käsittely riippuu siitä, onko päätös 2010/87 pätevä. Tässä yhteydessä se on saattanut asian ennakkoratkaisua pyytäneen tuomioistuimen käsiteltäväksi ja pyytänyt sitä esittämään unionin tuomioistuimelle tästä kysymyksiä.

5. Totean heti alkuun, että ennakkoratkaisukysymysten tarkastelussa ei mielestäni ole tullut esiin seikkoja, jotka voisivat vaikuttaa päätöksen 2010/87 pätevyyteen.

6. Ennakkoratkaisua pyytänyt tuomioistuin on tuonut esille tiettyjä epäilyjä, jotka koskevat lähinnä Yhdysvalloissa varmistetun tietosuojan riittävyyttä siihen nähden, että Yhdysvaltojen tiedusteluviranomaiset puuttuvat toiminnallaan henkilöiden, joiden tietoja siirretään tähän kolmanteen maahan, perusoikeuksien käyttöön. Nämä epäilyt saattavat komission täytäntöönpanopäätöksessä (EU) 2016/1250[6] tältä osin esittämät arvioinnit välillisesti kyseenalaisiksi. Vaikka pääasian ratkaisu ei edellytä unionin tuomioistuimen käsittelevän tätä kysymystä ja vaikka ehdotan sen näin ollen pidättyvän sen käsittelystä, esitän toissijaisesti syyt, joiden vuoksi olen päätynyt pohtimaan kyseisen päätöksen pätevyyttä.

7. Tätä tarkasteluani ohjaa kauttaaltaan pyrkimys saattaa tasapainoon yhtäältä se, että tarvitaan ”kohtuullista pragmaattisuutta vuorovaikutuksen mahdollistamiseksi muun maailman kanssa”,[7] ja toisaalta se, että unionin ja sen jäsenvaltioiden oikeusjärjestyksissä, erityisesti perusoikeuskirjassa, tunnustettuja perusarvoja on tarpeen lujittaa.

II Asiaa koskevat oikeussäännöt

A Direktiivi 95/46/EY

8. Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annetun direktiivin 95/46/EY[8] 3 artiklan 2 kohdassa säädettiin seuraavaa:

”Tätä direktiiviä ei sovelleta henkilötietojen käsittelyyn,

– joka suoritetaan sellaisessa toiminnassa, joka ei kuulu yhteisön oikeuden soveltamisalaan, kuten toiminta, josta on määrätty Euroopan unionista tehdyn sopimuksen V ja VI osastossa, ja kaikissa tapauksissa käsittely, joka koskee yleistä turvallisuutta, puolustusta, valtion turvallisuutta (myös valtion taloudellista hyvinvointia, kun käsittelyoperaatio on sidoksissa valtion turvallisuutta koskeviin kysymyksiin) ja rikosoikeuden alalla tapahtuvaa valtion toimintaa,

– –”

6 [Direktiivin 95/46] nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä 12.7.2016 annettu komission päätös (EUVL 2016, L 207, s. 1; jäljempänä Privacy Shield -päätös).

7 Ks. entisen Euroopan tietosuojavaltuutetun P. Hustinxin puhe ”Le droit de l’Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données”, s. 49, saatavilla osoitteessa https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf.

8 24.10.1995 annettu Euroopan parlamentin ja neuvoston direktiivi (EYVL 1995, L 281, s. 31), sellaisena kuin se on muutettuna 29.9.2003 annetulla Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 1882/2003 (EUVL 2003, L 284, s. 1) (jäljempänä direktiivi 95/46).

9. Tämän direktiivin 13 artiklan 1 kohdan sanamuoto oli seuraava:

”Jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla pyritään rajoittamaan 6 artiklan 1 kohdassa, 10 artiklassa, 11 artiklan 1 kohdassa sekä 12 ja 21 artiklassa säädettyjen oikeuksien ja velvoitteiden alaa, jos tällaiset rajoitukset ovat välttämättömiä, jotta varmistettaisiin

a) valtion turvallisuus,

b) puolustus,

c) yleinen turvallisuus,

d) rikosten tai, säännellyn ammattitoiminnan osalta, ammattietiikan rikkomusten torjunta, tutkinta, selvittäminen ja syyteharkinta,

e) jäsenvaltiolle tai [unionille] tärkeä taloudellinen tai rahoituksellinen etu, myös rahaa, talousarviota ja verotusta koskevissa asioissa,

f) valvonta-, tarkastus- tai sääntelytehtävä, joka satunnaisestikin liittyy julkisen vallan käyttämiseen c, d ja e alakohdassa tarkoitetuissa tapauksissa,

g) rekisteröidyn suojelu tai muiden oikeudet ja vapaudet.”

10. Kyseisen direktiivin 25 artiklassa säädettiin seuraavaa:

”1. Jäsenvaltioiden on säädettävä siitä, että käsiteltävien tai siirron jälkeen käsiteltäviksi tarkoitettujen henkilötietojen siirto kolmanteen maahan voidaan suorittaa ainoastaan, jos kyseisessä kolmannessa maassa taataan tietosuojan riittävä taso, jollei tämän direktiivin muiden säännösten mukaisesti säädetyistä kansallisista säännöksistä muuta johdu.

2. Kolmannessa maassa taattavan tietosuojan tason riittävyyttä on arvioitava kaikkien tiettyyn siirtoon tai siirtojen ryhmään liittyvien olosuhteiden osalta; erityisesti on otettava huomioon tietojen luonne, suunnitellun käsittelyn tai suunniteltujen käsittelyjen tarkoitus ja kestoaika, alkuperämaa ja lopullinen kohde, kyseisessä kolmannessa maassa voimassa olevat yleiset tai alakohtaiset oikeussäännöt sekä ammattisäännöt ja tässä maassa noudatettavat turvatoimet.

– –

6. Komissio voi 31 artiklan 2 kohdassa vahvistetun menettelyn mukaisesti todeta, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso tämän artiklan 2 kohdan tarkoittamassa merkityksessä, mikä johtuu kyseisen maan sisäisestä lainsäädännöstä tai kansainvälisistä sitoumuksista, jotka on tehty erityisesti 5 kohdassa tarkoitettujen neuvottelujen yhteydessä henkilöiden yksityiselämän ja perusoikeuksien ja -vapauksien turvaamiseksi.

Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet noudattaakseen komission päätöstä.”

11. Saman direktiivin 26 artiklan 2 ja 4 kohdassa säädettiin seuraavaa:

”2. Jäsenvaltio voi hyväksyä henkilötietojen siirron tai siirtojen sarjan sellaiseen kolmanteen maahan, jossa ei taata 25 artiklan 2 kohdassa tarkoitettua tietosuojan riittävää tasoa, jos rekisterinpitäjä antaa riittävät takeet henkilöiden yksityisyyden suojasta ja perusoikeuksien ja -vapauksien suojasta sekä vastaavien oikeuksien soveltamisesta, sanotun kuitenkaan rajoittamatta 1 kohdan soveltamista; nämä takeet voivat erityisesti johtua soveltuvista sopimuslausekkeista.

– –

4. Jos komissio päättää – –, että tietyillä mallisopimuslausekkeilla annetaan riittävät tämän artiklan 2 kohdassa tarkoitetut takeet, jäsenvaltioiden on toteutettava tarvittavat toimenpiteet noudattaakseen komission päätöstä.”

12. Direktiivin 95/46 28 artiklan 3 kohdan sanamuoto oli seuraava:

”Kullakin valvontaviranomaisella on erityisesti oltava:

– –

– tehokkaat toimintavaltuudet, kuten esimerkiksi valtuudet 20 artiklan mukaisesti antaa lausuntoja ennen käsittelyn toteuttamista ja varmistaa näiden lausuntojen asianmukainen julkistaminen taikka valtuudet määrätä tietojen suojaamisesta, poistamisesta tai tuhoamisesta tai kieltää käsittely väliaikaisesti tai lopullisesti taikka valtuudet antaa rekisterinpitäjälle huomautus tai varoitus taikka valtuudet saattaa asioita käsiteltäväksi kansalliselle parlamentille tai muille poliittisille elimille,

– –”

B Tietosuoja-asetus

13. Direktiivi 95/64 kumottiin tietosuoja-asetuksen 94 artiklan 1 kohdan nojalla 25 päivästä toukokuuta 2018, jolloin tätä asetusta alettiin soveltaa sen 99 artiklan 2 kohdan mukaisesti.

14. Kyseisen asetuksen 2 artiklan 2 kohdassa säädetään seuraavaa:

”Tätä asetusta ei sovelleta henkilötietojen käsittelyyn,

a) jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan;

b) jota suorittavat jäsenvaltiot toteuttaessaan SEU V osaston 2 luvun soveltamisalaan kuuluvaa toimintaa;

– –

d) jota toimivaltaiset viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelua ja tällaisten uhkien ehkäisyä varten.”

15. Saman asetuksen 4 artiklan 2 alakohdan mukaan ”käsittelyllä” tarkoitetaan ”toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista”.

16. Tietosuoja-asetuksen 23 artiklassa säädetään seuraavaa:

”1. Rekisterinpitäjään tai henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan lainsäädäntötoimenpiteellä rajoittaa 12–22 artiklassa ja 34 artiklassa sekä 5 artiklassa, siltä osin kuin sen säännökset vastaavat 12–22 artiklassa säädettyjä oikeuksia ja velvollisuuksia, säädettyjen velvollisuuksien ja oikeuksien soveltamisalaa, jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide, jotta voidaan taata

a) kansallinen turvallisuus;

b) puolustus;

c) yleinen turvallisuus;

d) rikosten ennalta estäminen, tutkinta, paljastaminen tai rikoksiin liittyvät syytetoimet taikka rikosoikeudellisten seuraamusten täytäntöönpano, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu tai tällaisten uhkien ehkäisy;

e) muut unionin tai jäsenvaltion yleiseen julkiseen etuun liittyvät tärkeät tavoitteet, erityisesti unionille tai jäsenvaltiolle tärkeä taloudellinen tai rahoituksellinen etu – –;

– –

2. Edellä 1 kohdassa tarkoitettujen lainsäädäntötoimenpiteiden on sisällettävä tarpeen mukaan erityisiä säännöksiä, jotka koskevat ainakin

a) käsittelytarkoitusta tai käsittelyn ryhmiä;

b) henkilötietoryhmiä;

c) käyttöön otettujen rajoitusten soveltamisalaa;

d) suojatoimia, joilla estetään väärinkäyttö tai lainvastainen pääsy tietoihin tai niiden siirtäminen;

e) rekisterinpitäjän tai rekisterinpitäjien ryhmien määrittämistä;

f) tietojen säilytysaikoja ja sovellettavia suojatoimia ottaen huomioon käsittelyn tai käsittelyryhmien luonne, laajuus ja tarkoitukset;

g) rekisteröidyn oikeuksiin ja vapauksiin kohdistuvia riskejä; ja

h) rekisteröityjen oikeutta saada tietoa rajoituksesta, paitsi jos tämä voisi vaarantaa rajoituksen tarkoituksen.”

17. Tämän asetuksen 44 artiklassa, jonka otsikkona on ”Siirtoja koskeva yleinen periaate”, säädetään seuraavaa:

”Sellaisten henkilötietojen siirto, joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen, toteutetaan vain jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat tässä luvussa vahvistettuja edellytyksiä ja ellei tämän asetuksen muista säännöksistä muuta johdu; tämä koskee myös henkilötietojen siirtämistä edelleen kyseisestä kolmannesta maasta tai kansainvälisestä järjestöstä toiseen kolmanteen maahan tai toiselle kansainväliselle järjestölle. Kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tällä asetuksella taattua luonnollisten henkilöiden henkilötietojen suojan tasoa ei vaaranneta.”

18. Kyseisen asetuksen 45 artiklassa, jonka otsikkona on ”Siirto tietosuojan riittävyyttä koskevan päätöksen perusteella”, säädetään seuraavaa:

”1. Henkilötietojen siirto johonkin kolmanteen maahan tai kansainväliselle järjestölle voidaan toteuttaa, jos komissio on päättänyt, että kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö varmistaa riittävän tietosuojan tason. Tällaiselle siirrolle ei tarvita erityistä lupaa.

2. Arvioidessaan tietosuojan riittävyyttä komissio ottaa huomioon etenkin seuraavat seikat:

a) oikeusvaltioperiaate, ihmisoikeuksien ja perusvapauksien kunnioitus, sekä yleinen että alakohtainen asiaankuuluva lainsäädäntö, joka koskee muun muassa yleistä turvallisuutta, puolustusta, kansallista turvallisuutta ja rikosoikeutta sekä viranomaisten pääsyä henkilötietoihin, sekä tällaisen lainsäädännön täytäntöönpano, tietosuojaa koskevat säännöt, ammatilliset säännöt ja turvatoimet, mukaan lukien asianomaisessa kolmannessa maassa tai kansainvälisessä järjestössä noudatettavat säännöt henkilötietojen siirtämisestä edelleen muuhun kolmanteen maahan tai muulle kansainväliselle järjestölle, oikeuskäytäntö sekä rekisteröidyille kuuluvat vaikuttavat ja täytäntöönpanokelpoiset oikeudet ja tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot niitä rekisteröityjä varten, joiden henkilötietoja siirretään;

b) se, onko kyseisessä kolmannessa maassa tai siinä kolmannessa maassa, jonka alaisuuteen kansainvälinen järjestö kuuluu, vähintään yksi tehokkaasti toimiva riippumaton valvontaviranomainen, joka vastaa tietosuojasääntöjen noudattamisen varmistamisesta ja täytäntöönpanosta, kuten riittävistä valvontavaltuuksista, oikeuksien käyttämistä koskevan avun ja neuvojen tarjoamisesta rekisteröidyille sekä yhteistyön tekemisestä jäsenvaltioiden valvontaviranomaisten kanssa;

c) asianosaisen kolmannen maan tai kansainvälisen järjestön tekemät kansainväliset sitoumukset tai muut oikeudellisesti sitovista yleissopimuksista tai säädöksistä taikka monenvälisiin tai alueellisiin järjestelmiin osallistumisesta johtuvat velvoitteet, jotka koskevat erityisesti henkilötietojen suojaamista.

3. Komissio voi suojan riittävyyttä arvioituaan päättää, että kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö tarjoaa tämän artiklan 2 kohdassa tarkoitetun riittävän tietosuojan tason. Täytäntöönpanosäädöksessä on säädettävä vähintään joka neljäs vuosi tehtävästä määräaikaistarkastelusta, jossa on otettava huomioon kaikki asiaan liittyvä kehitys kyseisessä kolmannessa maassa tai kansainvälisessä järjestössä. – –

4. Komissio seuraa jatkuvasti kolmansissa maissa ja kansainvälisissä järjestöissä tapahtuvaa kehitystä, joka saattaa vaikuttaa tämän artiklan 3 kohdan mukaisesti hyväksyttyjen päätösten ja direktiivin [95/46] 25 artiklan 6 kohdan perusteella hyväksyttyjen päätösten toimivuuteen.

5. Jos saatavilla olevista tiedoista käy ilmi varsinkin tämän artiklan 3 kohdassa tarkoitetun tarkastelun jälkeen, että kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö ei tarjoa enää tämän artiklan 2 kohdassa tarkoitettua riittävää tietosuojan tasoa, komissio tekee tästä päätöksen ja tarvittaessa kumoaa tämän artiklan 3 kohdassa tarkoitetun päätöksen, muuttaa sitä tai lykkää sen voimaantuloa täytäntöönpanosäädöksellä ilman takautuvaa vaikutusta. – –

6. Komissio aloittaa neuvottelut kolmannen maan tai kansainvälisen järjestön kanssa korjatakseen tilanteen, jonka johdosta 5 kohdan mukainen päätös annettiin.

– –

9. Komission direktiivin [95/46] 25 artiklan 6 kohdan nojalla antamat päätökset pysyvät voimassa, kunnes niitä muutetaan, ne korvataan tai kumotaan tämän artiklan 3 tai 5 kohdan mukaisesti annetulla komission päätöksellä.”

19. Saman asetuksen 46 artikla, jonka otsikkona on ”Siirto asianmukaisia suojatoimia soveltaen”, on muotoiltu seuraavasti:

”1. Jollei 45 artiklan 3 kohdan mukaista päätöstä ole tehty, rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja.

2. Edellä 1 kohdassa tarkoitettuja asianmukaisia suojatoimia voivat olla seuraavat, ilman että edellytetään erityistä valvontaviranomaisen antamaa lupaa:

– –

c) komission 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen antamat tietosuojaa koskevat vakiolausekkeet;

– –

5. Hyväksynnät, jotka jäsenvaltio tai valvontaviranomainen on antanut direktiivin [95/46] 26 artiklan 2 kohdan nojalla, pysyvät voimassa, kunnes kyseinen valvontaviranomainen tarpeen vaatiessa muuttaa niitä tai korvaa tai kumoaa ne. Päätökset, jotka komissio on antanut direktiivin [95/46] 26 artiklan 4 kohdan nojalla, pysyvät voimassa, kunnes niitä tarpeen vaatiessa muutetaan, ne korvataan tai kumotaan tämän artiklan 2 kohdan mukaisesti annetulla komission päätöksellä.”

20. Tietosuoja-asetuksen 58 artiklan 2, 4 ja 5 kohdassa säädetään seuraavaa:

”2. Jokaisella valvontaviranomaisella on kaikki seuraavat korjaavat toimivaltuudet:

a) varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää siitä, että aiotut käsittelytoimet ovat todennäköisesti tämän asetuksen säännösten vastaisia;

b) antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos käsittelytoimet ovat olleet tämän asetuksen säännösten vastaisia;

c) määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat tähän asetukseen perustuvien rekisteröidyn oikeuksien käyttöä;

d) määrätä rekisterinpitäjä tai henkilötietojen käsittelijä saattamaan käsittelytoimet tämän asetuksen säännösten mukaisiksi, tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa;

e) määrätä rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle;

f) asettaa väliaikainen tai pysyvä rajoitus käsittelylle, mukaan lukien käsittelykielto;

– –

i) määrätä 83 artiklan nojalla hallinnollinen sakko tässä kohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden asemesta kunkin yksittäisen tapauksen olosuhteista riippuen;

j) määrätä tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle.

– –

4. Valvontaviranomaiselle tämän artiklan nojalla annettujen valtuuksien käyttöön sovelletaan asianmukaisia suojatoimia, muun muassa tehokkaita oikeussuojakeinoja ja oikeudenmukaista menettelyä, joista säädetään unionin oikeudessa ja jäsenvaltion lainsäädännössä perusoikeuskirjan mukaisesti.

5. 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 tämän asetuksen säännösten täytäntöönpanemiseksi.”

C Päätös 2010/87

21. Komissio antoi direktiivin 95/46 26 artiklan 4 kohdan nojalla kolme päätöstä, joissa se totesi, että niissä vahvistetuilla mallisopimuslausekkeilla annetaan riittävät takeet yksityisyyden ja yksilöiden perusoikeuksien ja -vapauksien suojaamiseksi ja vastaavien oikeuksien toteutumiseksi (jäljempänä mallisopimuslausekkeita koskevat päätökset). [9]

22. Yksi näistä päätöksistä on päätös 2010/87, jonka 1 artiklan mukaan ”liitteessä olevien mallisopimuslausekkeiden katsotaan antavan riittävät takeet yksityisyyden ja yksilöiden perusoikeuksien ja -vapauksien suojaamiseksi ja vastaavien oikeuksien toteutumiseksi direktiivin [95/46] 26 artiklan 2 kohdassa edellytetyllä tavalla”.

23. Tämän päätöksen 3 artiklassa säädetään seuraavaa:

”Tässä päätöksessä käytetään seuraavia määritelmiä:

– –

c) ’tietojen viejällä’ tarkoitetaan rekisterinpitäjää, joka siirtää henkilötietoja;

d) ’tietojen tuojalla’ tarkoitetaan kolmanteen maahan sijoittautunutta henkilötietojen käsittelijää, joka hyväksyy vastaanottavansa tietojen viejältä henkilötietoja, jotka on siirron jälkeen tarkoitus käsitellä tietojen viejän puolesta tämän antamien ohjeiden mukaisesti ja tämän päätöksen mukaisia edellytyksiä noudattaen, ja jota ei koske direktiivin [95/46] 25 artiklan 1 kohdassa tarkoitettu riittävän tietosuojan takaava kolmannen maan järjestelmä;

9 Direktiivin [95/46] mukaisista mallisopimuslausekkeista henkilötietojen kolmansiin maihin siirtoa varten 15.6.2001 tehty komission päätös 2001/497/EY (EYVL 2001, L 181, s. 19); päätöksen [2001/497] muuttamisesta vaihtoehtoisten mallisopimuslausekkeiden ottamiseksi käyttöön henkilötietojen kolmansiin maihin siirtoa varten 27.12.2004 tehty komission päätös 2004/915/EY (EUVL 2004, L 385, s. 74) ja päätös 2010/87.

– –

f) ’sovellettavalla tietosuojalainsäädännöllä’ tarkoitetaan lainsäädäntöä, jolla suojataan yksilöiden perusoikeudet ja -vapaudet ja erityisesti näiden yksilöiden oikeus yksityisyyteen henkilötietojen käsittelyssä ja jota sovelletaan rekisterinpitäjään siinä jäsenvaltioissa, johon tietojen viejä on sijoittautunut;

– –”

24. Kyseisen päätöksen 4 artiklan alkuperäisen version 1 kohdassa säädettiin seuraavaa:

”Jäsenvaltioiden toimivaltaiset viranomaiset voivat käyttää nykyisiä toimivaltuuksiaan kolmansiin maihin suuntautuvien tiedonsiirtojen kieltämiseksi tai lykkäämiseksi suojatakseen yksilöitä näiden henkilötietojen käsittelyssä, sanotun kuitenkaan rajoittamatta kyseisten viranomaisten toimivaltuuksia toteuttaa toimenpiteitä direktiivin [95/46] II, III, V ja VI luvun nojalla annettujen kansallisten säännösten noudattamisen varmistamiseksi, jos

a) todetaan, että tietojen tuojaan tai alihankkijana toimivaan käsittelijään sovellettavaan lainsäädäntöön sisältyy sellaisia vaatimuksia poiketa sovellettavasta tietosuojalainsäädännöstä, joiden rajoitukset menevät pitemmälle kuin on tarpeen demokraattisessa yhteiskunnassa direktiivin [95/46] 13 artiklan mukaan, kun kyseisillä vaatimuksilla on todennäköisesti merkittävä haitallinen vaikutus mallisopimuslausekkeilla annettaviin takeisiin;

b) toimivaltainen viranomainen on todennut, ettei tietojen tuoja tai alihankkijana toimiva käsittelijä ole noudattanut liitteessä olevia mallisopimuslausekkeita; tai

c) on hyvin todennäköistä, että liitteessä olevia mallisopimuslausekkeita ei noudateta tai ei tulla noudattamaan, ja siirron jatkaminen merkitsisi välitöntä vaaraa vakavan haitan aiheutumisesta rekisteröidyille.”

25. Nykyisessä versiossaan, sellaisena kuin se perustuu päätöksen 2010/87 muuttamiseen täytäntöönpanopäätöksellä (EU) 2016/2297[10], päätöksen 2010/87 4 artiklassa säädetään, että ”kun jäsenvaltioiden toimivaltaiset viranomaiset käyttävät direktiivin [95/46] 28 artiklan 3 kohdan mukaisia toimivaltuuksiaan ja tästä seuraa se, että tiedonsiirrot kolmansiin maihin keskeytetään väliaikaisesti tai kielletään kokonaan yksilöiden suojelemiseksi heidän henkilötietojensa käsittelyssä, asianomaisen jäsenvaltion on viipymättä ilmoitettava asiasta komissiolle, joka välittää tiedon edelleen muille jäsenvaltioille”.

26. Päätöksen 2010/87 liitteeseen sisältyy useita mallisopimuslausekkeita. Erityisesti tässä liitteessä olevan lausekkeen 3, jonka otsikkona on ”Kolmatta osapuolta suojaava edunsaajalauseke”, sanamuoto on seuraava:

”1. Rekisteröity voi panna täytäntöön tämän lausekkeen, lausekkeen 4 kohdan b–i, lausekkeen 5 kohdan a–e sekä kohdan g–j, lausekkeen 6 kohdan 1 ja 2, lausekkeen 7, lausekkeen 8 kohdan 2 ja lausekkeen 9–12 tietojen viejää vastaan edunsaajana olevan kolmannen osapuolen ominaisuudessa.

10 [Direktiivin 95/46] mukaisista, henkilötietojen siirtoa kolmansiin maihin ja tällaisten tietojen siirtoa kyseisiin maihin sijoittautuneille henkilötietojen käsittelijöille koskevista mallisopimuslausekkeista annettujen päätösten [2001/497] ja [2010/87] muuttamisesta 16.12.2016 annettu komission päätös (EUVL 2016, L 344, s. 100).

2. Rekisteröity voi panna täytäntöön tämän lausekkeen, lausekkeen 5 kohdan a–e ja g, lausekkeen 6 ja 7, lausekkeen 8 kohdan 2 ja lausekkeen 9–12 tietojen tuojaa vastaan tapauksissa, joissa tietojen viejä on tosiasiallisesti lakkautettu tai lakannut oikeudellisesti olemasta, ellei mahdollinen seuraaja ole ottanut hoitaakseen tietojen viejän kaikkia oikeudellisia velvoitteita sopimuksella tai lain perusteella, minkä tuloksena se ottaa vastaan tietojen viejän oikeudet ja velvoitteet, jolloin rekisteröity voi panna lausekkeet täytäntöön tällaista seuraajaa vastaan.

– –”

27. Kyseisessä liitteessä olevassa lausekkeessa 4, jonka otsikkona on ”Tietojen viejän velvollisuudet”, todetaan seuraavaa:

”Tietojen viejä hyväksyy ja takaa, että

a) henkilötietojen käsittely, mukaan luettuna itse siirto, on suoritettu ja suoritetaan edelleen sovellettavan tietosuojalainsäädännön asiaankuuluvien säännösten mukaisesti (ja siitä on tarvittaessa ilmoitettu sen jäsenvaltion toimivaltaisille viranomaisille, johon tietojen viejä on sijoittautunut), ja ettei siirrolla rikota kyseisen valtion asiaankuuluvia säännöksiä,

b) tietojen viejä on antanut ohjeet ja antaa koko henkilötietojen käsittelypalvelun kestoajan ohjeita tietojen tuojalle siitä, että tämä käsittelee siirrettyjä henkilötietoja ainoastaan tietojen viejän puolesta ja sovellettavan tietosuojalainsäädännön ja lausekkeiden mukaisesti,

c) tietojen tuoja antaa riittävät takeet tämän sopimuksen lisäyksen 2 mukaisista teknisistä ja organisatorisista turvatoimista,

d) sen jälkeen kun sovellettavan tietosuojalainsäädännön mukaiset vaatimukset on arvioitu, kyseisten turvatoimien avulla henkilötiedot voidaan asianmukaisesti suojata tahattomalta tai laittomalta tuhoamiselta, tahattomalta häviämiseltä, muuttamiselta, luvattomalta luovuttamiselta tai tietoihin pääsyltä erityisesti kun tietoja siirretään verkossa käsittelyn yhteydessä, ja muulta henkilötietojen laittomalta käsittelytavalta, ja että nämä toimet takaavat käsittelyyn liittyviä riskejä ja suojattavien tietojen luonnetta vastaavan turvallisuuden tason, kun otetaan huomioon nykyinen tekninen taso ja toimenpiteiden toteuttamisen kustannukset,

e) tietojen viejä varmistaa kyseisten turvatoimien noudattamisen,

f) jos siirto koskee erityisiä tietoryhmiä, rekisteröidyille on ilmoitettu tai ilmoitetaan ennen siirtoa tai mahdollisimman pian sen jälkeen, että niiden tietoja voidaan siirtää kolmanteen maahan, jossa ei taata direktiivissä [95/46] tarkoitettua tietosuojan riittävää tasoa,

g) tietojen viejä toimittaa tietojen tuojalta tai alihankkijana toimivalta käsittelijältä lausekkeen 5 kohdan b ja lausekkeen 8 kohdan 3 mukaisesti saadun tiedon tietosuojaviranomaisille, kun se päättää jatkaa siirtoa tai lopettaa lykkäyksen,

h) tietojen viejä saattaa rekisteröityjen saataville pyynnöstä jäljennöksen lausekkeista, paitsi lisäyksestä 2, ja yleisen kuvauksen turvatoimista, sekä jäljennöksen mahdollisesta alihankintana suoritettavia käsittelypalveluita koskevasta sopimuksesta, joka on tehtävä lausekkeiden mukaisesti, elleivät lausekkeet tai sopimus sisällä kaupallisia tietoja, jolloin tietojen viejä voi poistaa tällaiset kaupalliset tiedot,

i) jos käsittely suoritetaan alihankintana, alihankkijana toimiva käsittelijä suorittaa käsittelytoiminnan lausekkeen 11 mukaisesti ja suojaa rekisteröidyn henkilötiedot ja oikeudet vähintään yhtä hyvin kuin tietojen tuoja näiden lausekkeiden mukaisesti, ja

j) tietojen viejä varmistaa lausekkeen 4 kohdan a–i noudattamisen.”

28. Samaan liitteeseen sisältyvässä lausekkeessa 5, jonka otsikkona on ”Tietojen tuojan velvollisuudet ([1])”, todetaan seuraavaa:

”Tietojen tuoja hyväksyy ja takaa, että

a) tietojen tuoja käsittelee henkilötietoja ainoastaan tietojen viejän puolesta tämän antamien ohjeiden ja lausekkeiden mukaisesti, ja jos se ei voi noudattaa näitä ohjeita ja sääntöjä mistä tahansa syystä, se ilmoittaa tästä viipymättä tietojen viejälle, jolloin tietojen viejällä on oikeus lykätä tietojen siirtoa ja/tai irtisanoa sopimus,

b) tietojen tuojalla ei ole mitään syytä olettaa, että siihen sovellettava lainsäädäntö estäisi tietojen viejältä saatujen ohjeiden noudattamisen ja tietojen tuojalle sopimuksen mukaan kuuluvien velvoitteiden täyttämisen, ja jos kyseistä lainsäädäntöä muutetaan ja muutoksella on todennäköisesti merkittävä haitallinen vaikutus lausekkeilla annettaviin takeisiin ja lausekkeiden mukaisiin velvoitteisiin, tietojen tuoja antaa muutoksen tiedoksi tietojen viejälle viipymättä saatuaan itse tiedon siitä, jolloin tietojen viejällä on oikeus lykätä tietojen siirtoa ja/tai irtisanoa sopimus,

c) tietojen tuoja on pannut täytäntöön lisäyksessä 2 määritellyt tekniset ja organisatoriset turvatoimet ennen siirrettyjen henkilötietojen käsittelyä,

d) tietojen tuoja ilmoittaa viipymättä tietojen viejälle seuraavista seikoista:

   i) säännösten täytäntöönpanosta vastaavan viranomaisen oikeudellisesti sitovasta pyynnöstä luovuttaa henkilötietoja, ellei sitä muutoin kielletä esimerkiksi rikoslainsäädännön mukaisella kiellolla lainvalvontaan liittyvien tutkimusten luottamuksellisuuden säilyttämiseksi,

   ii) kaikista tahattomista tai luvattomista pääsyistä tietoihin, ja

   iii) rekisteröidyiltä suoraan saaduista tiedusteluista niihin vastaamatta, ellei siihen muutoin anneta lupaa,

e) tietojen tuoja hoitaa tietojen viejältä saadut siirrettävien henkilötietojen käsittelyyn liittyvät tiedustelut viipymättä ja asianmukaisesti ja noudattaa siirrettyjen tietojen käsittelyssä valvontaviranomaisen neuvoja,

f) tietojen tuoja antaa tietojen viejän vaatimuksesta tietojenkäsittelyjärjestelmänsä tarkastettavaksi lausekkeiden piiriin kuuluvien käsittelytoimien osalta. Tarkastuksen suorittaa tietojen viejä tai vaaditun ammattipätevyyden omaavien ja salassapitovelvollisuuden alaisten riippumattomien jäsenten muodostama tarkastuselin, jonka tietojen viejä valitsee mahdollisesti valvontaviranomaisen kanssa,

_ _”

29. Alaviitteessä 1, johon päätöksen 2010/87 liitteessä olevassa lausekkeessa 5 viitataan, todetaan seuraavaa:

”Tietojen tuojaan sovellettavat kansallisen lainsäädännön sisältämät pakolliset vaatimukset, jotka eivät mene pitemmälle kuin on tarpeen demokraattisessa yhteiskunnassa direktiivin [95/46] 13 artiklan 1 kohdassa lueteltujen etujen perusteella, toisin sanoen vaatimukset, jotka ovat välttämättömiä, jotta varmistettaisiin valtion turvallisuus, puolustus, yleinen turvallisuus, rikosten tai, säännellyn ammattitoiminnan osalta, ammattietiikan rikkomusten torjunta, tutkinta, selvittäminen ja

syyteharkinta, valtion tärkeä taloudellinen tai rahoituksellinen etu tai rekisteröidyn suojelu tai muiden oikeudet ja vapaudet, ja jotka eivät ole ristiriidassa mallisopimuslausekkeiden kanssa. Esimerkkejä tällaisista pakollisista vaatimuksista, jotka eivät mene pitemmälle kuin on tarpeen demokraattisessa yhteiskunnassa, ovat kansainvälisesti tunnustetut pakotteet, raportointivaatimukset verotusta varten ja raportointivaatimukset rahanpesun torjumiseksi."

30. Tähän liitteeseen sisältyvän lausekkeen 6, jonka otsikkona on "Vastuu", sanamuoto on seuraava:

"1. Sopimuspuolet sopivat, että rekisteröidyllä, jolle on koitunut vahinkoa jonkin sopimuspuolen tai alihankkijana toimivan käsittelijän rikottua lausekkeessa 3 tai lausekkeessa 11 tarkoitettuja velvoitteita, on oikeus saada tietojen viejältä korvaus aiheutuneista vahingoista.

2. Jos rekisteröity ei voi nostaa kohdan 1 mukaista vahingonkorvauskannetta tietojen viejää vastaan, kun tietojen tuoja tai sen alihankkijana toimiva käsittelijä ei ole täyttänyt lausekkeessa 3 tai 11 tarkoitettuja velvoitteitaan, sen vuoksi, että tietojen viejä on tosiasiallisesti lakkautettu, lakannut oikeudellisesti olemasta tai todettu maksukyvyttömäksi, tietojen tuoja hyväksyy, että rekisteröity voi nostaa kanteen tietojen tuojaa vastaan samaan tapaan kuin tietojen viejää vastaan, ellei mahdollinen seuraaja ole ottanut hoitaakseen tietojen viejän kaikkia oikeudellisia velvoitteita sopimuksella tai lain perusteella, jolloin rekisteröity voi panna oikeutensa täytäntöön tällaista seuraajaa vastaan.

_ _"

31. Kyseisessä liitteessä olevassa lausekkeessa 7, jonka otsikkona on "Sovittelu ja toimivaltainen tuomioistuin", todetaan seuraavaa:

"1. Jos rekisteröity vetoaa kolmannen osapuolen etua suojaavaan oikeuteen ja/tai vaatii vahingonkorvausta lausekkeiden nojalla, tietojen tuoja hyväksyy rekisteröidyn päätöksen

a) saattaa riita käsiteltäväksi sovittelumenettelyssä, jossa on mukana riippumaton henkilö tai tarvittaessa valvontaviranomainen,

b) saattaa riita sen jäsenvaltion tuomioistuinten ratkaistavaksi, johon tietojen viejä on sijoittautunut.

2. Sopimuspuolet sopivat, että rekisteröidyn tekemä valinta ei vaikuta rekisteröidyn oikeuteen hakea tilanteeseen korjausta asiasisällön tai menettelyn osalta kansallisen tai kansainvälisen yksityisoikeuden muiden säännösten mukaisesti."

32. Samaan liitteeseen sisältyvässä lausekkeessa 9, jonka otsikkona on "Sovellettava laki", todetaan, että lausekkeisiin sovelletaan sen jäsenvaltion lakia, johon tietojen viejä on sijoittautunut.

D Privacy Shield -päätös

33. Komissio antoi direktiivin 95/46 25 artiklan 6 kohdan perusteella kaksi peräkkäistä päätöstä, joissa se totesi, että Yhdysvallat takaa riittävän suojan tason henkilötiedoille, jotka siirretään Yhdysvaltoihin sijoittautuneille yrityksille, jotka ovat ilmoittaneet noudattavansa oma varmennus -menetelmän perusteella näiden päätösten mukaisia periaatteita.

34. Komissio teki ensin päätöksen 2000/520/EY yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä.[11] Unionin tuomioistuin totesi 6.10.2015 antamallaan tuomiolla Schrems[12] tämän päätöksen pätemättömäksi.

35. Tämän tuomion seurauksena komissio antoi seuraavaksi Privacy Shield -päätöksen.

36. Tämän päätöksen 1 artiklassa säädetään seuraavaa:

”1. Komissio katsoo direktiivin [95/46] 25 artiklan 2 kohdan soveltamiseksi, että Yhdysvallat takaa riittävän suojan henkilötiedoille, jotka siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa unionista Yhdysvalloissa oleville organisaatioille.

2. EU:n ja Yhdysvaltojen välinen Privacy Shield -järjestely muodostuu Yhdysvaltojen kauppaministeriön 7 päivänä heinäkuuta 2016 antamista järjestelyn periaatteista, jotka on esitetty liitteessä II, ja virallisista lausumista ja sitoumuksista, jotka sisältyvät liitteissä I ja III–VII lueteltuihin asiakirjoihin.

3. Edellä olevan 1 kohdan soveltamiseksi henkilötietoja siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa silloin, kun ne siirretään unionista sellaisille Yhdysvalloissa oleville organisaatioille, jotka on sisällytetty Yhdysvaltojen kauppaministeriön liitteessä II esitettyjen järjestelyn periaatteiden I ja III jakson mukaisesti ylläpitämään ja julkisesti saataville asettamaan Privacy Shield -luetteloon.”

37. Tämän päätöksen liite III A, jonka otsikkona on ”EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn signaalitiedustelua koskeva oikeusasiamiesmekanismi” ja joka on liitetty silloisen Secretary of Staten (ulkoministeri, Yhdysvallat) John Kerryn 7.7.2016 päivättyyn kirjeeseen, sisältää muistion, jossa kuvataan uutta oikeusasiamiesmekanismia, jota ulkoministerin nimeämä ”tietotekniikkaan liittyvän kansainvälisen diplomatian johtava koordinaattori” (jäljempänä oikeusasiamies) soveltaa.

38. Tämän muistion mukaan kyseisen mekanismin ”avulla helpotetaan sellaisten kysymysten ja niihin annettavien vastausten käsittelyä, jotka liittyvät [unionista] Yhdysvaltoihin toimitettuihin tietoihin ja jotka koskevat kansallisen turvallisuuden perusteella tietoihin myönnettävää pääsyä. Tietojen toimittaminen perustuu Privacy Shield -järjestelyyn, vakiosopimuslausekkeisiin, yrityksiä koskeviin sitoviin sääntöihin, poikkeuksiin tai mahdollisiin tuleviin poikkeuksiin, ja tiedot toimitetaan vakiintuneita reittejä pitkin Yhdysvaltojen lainsäädännön ja toimintaperiaatteiden nojalla”.

III Pääasia, ennakkoratkaisukysymykset ja asian käsittely unionin tuomioistuimessa

39. Maximillian Schrems, joka on Itävallan kansalainen ja asuu Itävallassa, on Facebook-verkkoyhteisöpalvelun käyttäjä. Kukin unionin alueella asuva tämän verkkoyhteisöpalvelun käyttäjä joutuu siihen liittyessään tekemään sopimuksen Facebook Irelandin kanssa; tämä on Facebook Inc:n, jonka kotipaikka on Yhdysvalloissa, tytäryhtiö. Näiden käyttäjien henkilötiedot siirretään kokonaan tai osittain käsiteltäviksi Facebook Inc:lle kuuluville palvelimille, jotka sijaitsevat Yhdysvaltojen alueella.

11 Direktiivin [95/46] mukaisesti 26.7.2000 tehty päätös (EYVL 2000, L 215, s. 7; jäljempänä safe harbor -päätös).

12 C-362/14 (EU:C:2015:650; jäljempänä tuomio Schrems).

40. Schrems teki 25.6.2013 DPC:lle kantelun, jossa hän pääasiallisesti vaati tätä kieltämään Facebook Irelandia siirtämästä hänen henkilötietojaan Yhdysvaltoihin. Hänen mielestään tässä kolmannessa maassa voimassa olevat oikeussäännöt ja käytännöt eivät takaa sen alueella säilytetyille henkilötiedoille riittävää suojaa viranomaisten siellä harjoittamaan tarkkailutoimintaan perustuvalta tunkeutumiselta. Schrems viittaa tässä yhteydessä paljastuksiin, jotka Edward Snowden on tehnyt Yhdysvaltojen tiedustelupalvelujen, erityisesti National Security Agencyn (NSA) (kansallinen turvallisuusvirasto, Yhdysvallat), toiminnasta.

41. Tämä kantelu hylättiin muun muassa sillä perusteella, että kaikki kysymykset suojan riittävyydestä Yhdysvalloissa on ratkaistava safe harbor -päätöksen mukaisesti. Tässä päätöksessä komissio on todennut, että Yhdysvalloissa taataan riittävä suoja henkilötiedoille, jotka siirretään sen alueelle sijoittautuneille yrityksille, jotka ovat ilmoittaneet noudattavansa kyseisen päätöksen mukaisia periaatteita.

42. Schrems nosti kantelunsa hylkäämisestä tehdystä päätöksestä kanteen High Courtissa. Kyseinen tuomioistuin totesi, että vaikkei Schrems ollut muodollisesti riitauttanut safe harbor -päätöksen pätevyyttä, hän riitautti kantelussaan itse asiassa tällä päätöksellä käyttöön otetun järjestelmän laillisuuden. Tässä tilanteessa kyseinen tuomioistuin esitti unionin tuomioistuimelle kysymyksiä selvittääkseen, onko jäsenvaltion tietosuojaviranomaisten (jäljempänä valvontaviranomaiset), jotka käsittelevät niille tehtyä kantelua henkilön oikeuksien ja vapauksien suojasta kyseisen henkilön kolmanteen maahan siirrettyjen henkilötietojen käsittelyssä, noudatettava toteamuksia, jotka komissio on tehnyt direktiivin 96/46 25 artiklan 6 kohdan nojalla tämän kolmannen valtion tarjoaman tietosuojan riittävyydestä, vaikka kantelija kiistää nämä toteamukset.

43. Todettuaan tuomion Schrems 51 ja 52 kohdassa, että tietosuojan riittävyyttä koskeva päätös sitoo valvontaviranomaisia niin kauan kuin sitä ei ole todettu pätemättömäksi, unionin tuomioistuin totesi tämän tuomion 63 ja 65 kohdassa seuraavaa:

”63. – – kun henkilö, jonka henkilötiedot on siirretty tai voitaisiin siirtää direktiivin 95/46 25 artiklan 6 kohtaan perustuvan komission päätöksen kohteena olevaan kolmanteen maahan, saattaa kansallisen valvontaviranomaisen käsiteltäväksi vaatimuksen oikeuksiensa ja vapauksiensa suojelusta näiden tietojen käsittelyssä ja riitauttaa tällaisen vaatimuksen yhteydessä – – kyseisen päätöksen yhteensoveltuvuuden henkilöiden yksityiselämän sekä perusvapauksien ja -oikeuksien suojan kanssa, mainitun viranomaisen asiana on tutkia kyseinen vaatimus kaikkea asianmukaista huolellisuutta noudattaen.

– –

65. – – tapauksessa, jossa kyseinen viranomainen pitää [tämän henkilön] esittämiä perusteita perusteltuina, on niin, että saman viranomaisen on direktiivin 95/46 28 artiklan 3 kohdan ensimmäisen alakohdan kolmannen luetelmakohdan, luettuna erityisesti perusoikeuskirjan 8 artiklan 3 kohdan valossa, mukaisesti voitava olla asianosaisena oikeudenkäynnissä. Tässä yhteydessä kansallisen lainsäätäjän asiana on säätää oikeussuojakeinoista, joiden avulla asianomainen kansallinen valvontaviranomainen voi esittää perusteltuina pitämänsä perusteet kansallisissa tuomioistuimissa, jotta nämä voisivat, mikäli ne kyseisen viranomaisen tavoin epäilevät komission päätöksen pätevyyttä, pyytää ennakkoratkaisua päätöksen pätevyyden tutkimiseksi.”

44. Unionin tuomioistuin tarkasteli kyseisessä tuomiossa myös safe harbor -päätöksen pätevyyttä direktiivistä 95/46, luettuna perusoikeuskirjan valossa, johtuvien vaatimusten kannalta. Tämän tarkastelunsa päätteeksi se totesi kyseisen päätöksen pätemättömäksi. [13]

13 Ks. tuomio Schrems (106 kohta).

45. Ennakkoratkaisua pyytänyt tuomioistuin kumosi tuomion Schrems seurauksena päätöksen, jolla DPC oli hylännyt Schremsin kantelun, ja palautti sen DPC:n käsiteltäväksi. DPC aloitti tutkinnan ja kehotti Schremsiä muotoilemaan uudelleen kantelunsa safe harbor -päätöksen pätemättömyyden huomioon ottaen.

46. Tässä tarkoituksessa Schrems pyysi Facebook Irelandia ilmoittamaan, mihin oikeusperustoihin Facebook-verkkoyhteisöpalvelun käyttäjien henkilötietojen siirrot unionista Yhdysvaltoihin perustuvat. Ilmoittamatta kaikkia oikeusperustoja, joihin se tukeutuu, Facebook Ireland viittasi Facebook Inc:n kanssa tekemäänsä tietojen siirtoa ja käsittelyä koskevaan sopimukseen (data transfer processing agreement), jota on sovellettu 20.11.2015 alkaen, ja vetosi päätökseen 2010/87.

47. Uudelleen muotoillussa kantelussaan Schrems väittää, että tähän sopimukseen sisältyvät lausekkeet eivät ole päätöksen 2010/87 liitteessä olevien mallisopimuslausekkeiden mukaisia. Schrems katsoo joka tapauksessa, että hänen henkilötietojensa siirtoa Yhdysvaltoihin ei voida perustaa näihin mallisopimuslausekkeisiin. Tämä johtuu siitä, että Yhdysvaltojen oikeudessa Facebook Inc. velvoitetaan saattamaan käyttäjien henkilötiedot Yhdysvaltojen viranomaisten, kuten NSA:n ja Federal Bureau of Investigationin (FBI) (liittovaltion poliisi, Yhdysvallat), saataville tarkkailuohjelmissa, jotka rajoittavat perusoikeuskirjan 7, 8 ja 47 artiklassa taattujen oikeuksien käyttämistä. Schrems väittää, että rekisteröidyt eivät voi millään oikeussuojakeinolla vedota yksityisyyden ja henkilötietojen suojaa koskeviin oikeuksiinsa. Tässä tilanteessa Schrems vaatii DPC:tä keskeyttämään tämän siirron päätöksen 2010/87 4 artiklan perusteella.

48. Facebook Ireland myönsi DPC:n tutkinnan yhteydessä jatkavansa unionin alueella asuvien Facebook-verkkoyhteisöpalvelun käyttäjien henkilötietojen siirtämistä Yhdysvaltoihin ja tukeutuvansa tätä varten suurelta osin päätöksen 2010/87 liitteessä oleviin mallisopimuslausekkeisiin.

49. DPC:n tutkinnalla oli tarkoitus selvittää, taataanko Yhdysvalloissa unionin kansalaisten henkilötietojen riittävä suoja, ja jos ei, annetaanko mallisopimuslausekkeita koskevilla päätöksillä riittävät takeet näiden henkilöiden perusoikeuksien ja -vapauksien suojasta.

50. Tältä osin DPC katsoi päätösluonnoksessa (draft decision) alustavasti, että Yhdysvaltojen oikeudessa ei anneta perusoikeuskirjan 47 artiklassa tarkoitettuja tehokkaita oikeussuojakeinoja unionin kansalaisille, joiden tietoja siirretään Yhdysvaltoihin, jossa on vaarana, että Yhdysvaltojen virastot käsittelevät näitä tietoja kansallista turvallisuutta varten perusoikeuskirjan 7 ja 8 artiklan kanssa yhteensopimattomalla tavalla. Mallisopimuslausekkeita koskevien päätösten liitteenä olevilla lausekkeilla annetut takeet eivät korjaa tätä puutetta, koska ne eivät sido Yhdysvaltojen viranomaisia tai virastoja ja koska niillä annetaan rekisteröidyille vain sopimukseen perustuvia oikeuksia tietojen viejää ja/tai tuojaa vastaan.

51. Tässä tilanteessa DPC katsoi, ettei Schremsin kantelua voida ratkaista ilman, että unionin tuomioistuin tutkii mallisopimuslausekkeita koskevien päätösten pätevyyden. Tuomion Schrems 65 kohdassa todetun mukaisesti DPC saattoi ennakkoratkaisua pyytäneessä tuomioistuimessa vireille menettelyn, jotta tämä siinä tapauksessa, että se yhtyy DPC:n epäilyksiin, esittäisi unionin tuomioistuimelle ennakkoratkaisupyynnön näiden päätösten pätevyydestä.

52. Yhdysvaltojen hallitus, Electronic Privacy Information Centre (EPIC), Business Software Alliance (BSA) ja Digitaleurope hyväksyttiin osallistumaan asian käsittelyyn ennakkoratkaisua pyytäneessä tuomioistuimessa.

53. Selvittääkseen, onko DPC:n epäilyksiin mallisopimuslausekkeita koskevien päätösten pätevyydestä syytä yhtyä, High Court vastaanotti todisteita riidan asianosaisilta ja kuuli näiden asianosaisten sekä muiden osapuolten esittämät perustelut. Asiantuntijat esittivät näyttöä erityisesti Yhdysvaltojen oikeuden säännöksistä. Irlannin oikeudessa ulkomaan oikeutta pidetään tosiseikkana, jonka toteen näyttämiseksi on esitettävä todisteita samalla tavoin kuin kaikista muista tosiseikoista.

Ennakkoratkaisua pyytänyt tuomioistuin arvioi näiden todisteiden perusteella Yhdysvaltojen oikeuden säännöksiä, joissa sallitaan valtion viranomaisten ja virastojen toteuttama tarkkailu, kahden julkisesti tunnustetun tarkkailuohjelman (PRISM ja Upstream) toimintaa, yksityisille, joiden oikeuksia on loukattu tarkkailutoimilla, annettuja eri oikeussuojakeinoja sekä systeemisiä takeita ja valvontamekanismeja. Kyseinen tuomioistuin sisällytti tämän arvioinnin tulokset 3.10.2017 annettuun tuomioon, joka on liitetty sen ennakkoratkaisupyyntöön (jäljempänä High Courtin 3.10.2017 antama tuomio).

54. Tässä tuomiossa ennakkoratkaisua pyytänyt tuomioistuin viittasi oikeusperustoina, joiden nojalla Yhdysvaltojen tiedustelupalveluille annetaan oikeus ulkomaisen viestinnän kaappaukseen, ulkomaantiedustelun valvonnasta annetun lain (Foreign Intelligence Surveillance Act (FISA)) 702 §:ään ja presidentin asetukseen 12333 (Executive Order 12333, jäljempänä EO 12333).

55. Kyseisessä tuomiossa esitettyjen toteamusten mukaan FISA:n 702 §:n mukaan Attorney General (oikeusministeri, Yhdysvallat) ja Director of National Intelligence (DNI) (kansallisen tiedusteluviraston johtaja, Yhdysvallat) voivat yhdessä antaa ulkomaantiedustelutietojen hankkimiseksi yhden vuoden ajaksi luvan tarkkailla henkilöitä, jotka eivät ole Yhdysvaltojen kansalaisia ja jotka eivät asu vakituisesti Yhdysvalloissa (ns. ei-yhdysvaltaiset henkilöt), jos heidän voidaan kohtuudella olettaa olevan Yhdysvaltojen ulkopuolella.[14] FISA:n mukaan ”ulkomaantiedustelu” kohdistuu tietoihin, jotka koskevat valtion kykyä varautua ulkomaisiin hyökkäyksiin, terrorismia, joukkotuhoaseiden levittämistä sekä Yhdysvaltojen ulkosuhteiden hoitamista.[15]

56. Foreign Intelligence Surveillance Courtin (FISC) (ulkomaantiedustelun valvonnasta vastaava tuomioistuin, Yhdysvallat) on hyväksyttävä nämä vuosittaiset luvat sekä menettelyt, jotka koskevat tarkkailun kohteena olevien henkilöiden kohdentamista ja kerättyjen tietojen käsittelyä (ns. minimointi).[16] Kun FISA:n muihin säännöksiin perustuva ”perinteinen” tarkkailu edellyttää ”todennäköistä syytä” epäillä, että tarkkailun kohteena olevat henkilöt kuuluvat ulkovaltaan tai ovat ulkovallan edustajia, FISA:n 702 §:n nojalla toteutettu tarkkailutoiminta ei edellytä tällaista ”todennäköistä syytä” tai FISC:n antamaa hyväksyntää tiettyjen henkilöiden kohdentamiselle. Ennakkoratkaisua pyytäneen tuomioistuimen esittämistä toteamuksista ilmenee lisäksi, että minimointimenettelyjä ei sovelleta Yhdysvaltojen ulkopuolella oleviin ei-yhdysvaltalaisiin henkilöihin.

57. Käytännössä FISC:n annettua luvan NSA lähettää Yhdysvaltoihin sijoittautuneille sähköisten viestintäpalvelujen tarjoajille määräyksiä, jotka sisältävät hakukriteerejä, niin kutsuttuja valintakriteerejä, jotka liittyvät kohdennettuihin henkilöihin (kuten puhelinnumeroita tai sähköpostiosoitteita). Näillä palveluntarjoajilla on velvollisuus toimittaa valintakriteerejä vastaavat tiedot NSA:lle ja pitää niille osoitetut määräykset salassa. Ne voivat nostaa FISC:ssä kanteen ja vaatia NSA:n määräyksen muuttamista tai hylkäämistä. FISC:n ratkaisuun voi hakea muutosta Foreign Intelligence Surveillance Court of Review’ltä (FISCR) (ulkomaantiedustelun valvonnasta vastaava muutoksenhakutuomioistuin, Yhdysvallat).

58. High Court totesi, että FISA:n 702 § on oikeusperustana PRISM- ja Upstream-ohjelmille.

14 50 U.S.C. 1881 (a).

15 50 U.S.C. 1881 (e).

16 Ennakkoratkaisua pyytäneen tuomioistuimen mukaan kohdentamismenettelyt koskevat tapaa, jolla toimeenpanovalta päättää, että on kohtuullista olettaa tietty henkilö ei-yhdysvaltalaiseksi henkilöksi, joka oleskelee Yhdysvaltojen ulkopuolella, ja että tämän henkilön kohdentaminen voi johtaa ulkomaantiedustelutietojen hankkimiseen. Minimointimenettelyt kattavat kaikki yhdysvaltalaisista henkilöistä FISA:n 702 §:n nojalla hankittujen ei-julkisten tietojen hankkimisen, säilyttämisen, käytön ja levittämisen.

59. PRISM-ohjelmassa sähköisten viestintäpalvelujen tarjoajien on toimitettava NSA:lle kaikki sen ilmoittaman valintakriteerin ”lähtevä” tai ”saapuva” viestintä. Osa tästä viestinnästä toimitetaan FBI:lle ja Central Intelligence Agencylle (CIA) (keskustiedustelupalvelu, Yhdysvallat). Vuonna 2015 tarkkailtiin 94 386 henkilöä, ja vuonna 2011 Yhdysvaltojen hallitus hankki yli 250 miljoonaa viestiä tämän ohjelman perusteella.

60. Upstream-ohjelma perustuu siihen, että yritykset, jotka ylläpitävät runkoverkkoa – eli kaapeliverkkoja, verkkokytkimiä ja verkkoreitittimiä –, jonka kautta puhelinviestintä ja internetviestintä siirtyvät, ovat velvollisia antamaan apuaan. Näiden yritysten on pakko antaa NSA:n kopioida ja suodattaa internetliikennettä tämän viraston määräyksessä mainitun valintakriteerin ”lähtevän”, ”saapuvan” tai sitä ”koskevan” viestinnän hankkimiseksi. Valintakriteeriä ”koskevalla” viestinnällä tarkoitetaan viestintää, jossa viitataan tähän valintakriteeriin ilman, että kyseiseen valintakriteeriin yhdistetty ei-yhdysvaltalainen henkilö välttämättä osallistuu siihen. Vaikka FISC:n 26.4.2017 antamasta lausunnosta ilmenee, että kyseisestä päivästä lukien Yhdysvaltojen hallitus ei enää kerää ja hanki tiettyä valintakriteeriä ”koskevaa” viestintää, tässä lausunnossa ei todeta, että NSA olisi lakannut kopioimasta ja suodattamasta tarkkailujärjestelmänsä kautta kulkevaa viestintävirtaa. Upstream-ohjelma merkitsee siis sitä, että NSA:lla on pääsy sekä metatietoihin että viestinnän sisältöön. Vuodesta 2011 NSA on hankkinut noin 26,5 miljoonaa viestiä vuodessa Upstream-ohjelman perusteella, mikä vastaa kuitenkin vain pientä osaa tämän ohjelman nojalla toteutettuun suodatinmenettelyyn saatetusta viestinnästä.

61. High Courtin toteamusten mukaan EO 12333:ssa hyväksytään sähköisen viestinnän tarkkailu Yhdysvaltojen alueen ulkopuolella antamalla pääsy ulkomaantiedustelua varten joko tälle alueelle ”siirrettäviin” tietoihin tai tietoihin, jotka ”siirretään” tämän alueen ”kautta” ilman, että niitä olisi tarkoitus käsitellä siellä, sekä näiden tietojen kerääminen ja säilyttäminen. EO 12333:n mukaan ulkomaantiedustelutiedolla tarkoitetaan tietoja, jotka koskevat ulkomaisten hallitusten, ulkomaisten organisaatioiden tai ulkomaalaisten henkilöiden valmiuksia, aikomuksia tai toimintaa. [17]

62. EO 12333:ssa annetaan NSA:lle pääsy merenalaisiin kaapeleihin, jotka sijaitsevat Atlantin valtameren pohjassa ja joita pitkin tiedot siirretään unionista Yhdysvaltoihin ennen kuin nämä tiedot saapuvat Yhdysvaltoihin ja ovat tämän johdosta FISA:n säännösten alaisia. Ei kuitenkaan ole näyttöä siitä, että tämän presidentin asetuksen nojalla olisi pantu yhtään ohjelmaa täytäntöön.

63. Vaikka EO 12333:ssa säädetään rajoituksista tietojen keräämiselle, säilyttämiselle ja levittämiselle, näitä rajoituksia ei sovelleta ei-yhdysvaltalaisiin henkilöihin. Näillä viimeksi mainituilla henkilöillä on ainoastaan presidentin määräyksessä nro 28 (Presidential Policy Directive 28, jäljempänä PPD 28), jota sovelletaan kaikkeen ulkomaantiedustelun signaalitiedustelutietojen keräämiseen ja käyttöön, annetut takeet. PPD 28:ssä säädetään, että yksityisyyden suoja on erottamaton osa tämän toiminnan suunnittelussa huomioon otettavia näkökohtia, että tietojen keruun ainoana tarkoituksena on oltava ulkomaantiedustelu- ja vastatiedustelutietojen hankkiminen ja että tämän toiminnan on oltava ”mahdollisimman räätälöityä”.

64. Ennakkoratkaisua pyytäneen tuomioistuimen mukaan NSA:n toiminnasta, joka perustuu EO 12333:een, jonka Yhdysvaltojen presidentti voi milloin tahansa muuttaa tai kumota, ei säädetä lailla, se ei ole tuomioistuinvalvonnan kohteena eikä sen osalta ole käytettävissä oikeussuojakeinoja.

65. Näiden toteamusten perusteella kyseinen tuomioistuin katsoo, että Yhdysvallat harjoittaa laajamittaista ja erottelematonta henkilötietojen käsittelyä, joka voi saattaa rekisteröidyt vaaraan siitä, että heidän perusoikeuskirjan 7 ja 8 artiklaan perustuvia oikeuksiaan loukataan.

17 EO 12333, 3.5 kohdan e alakohta.

66. Lisäksi kyseinen tuomioistuin toteaa, että unionin kansalaisilla ei ole käytettävissään samoja oikeussuojakeinoja kuin Yhdysvaltojen kansalaisilla Yhdysvaltojen viranomaisten käsitellessä heidän henkilötietojaan lainvastaisesti. Yhdysvaltojen perustuslain neljäs lisäys, joka muodostaa tärkeimmän suojan lainvastaista valvontaa vastaan, ei ole sovellettavissa unionin kansalaisiin, joilla ei ole merkittävää omaehtoista yhteyttä Yhdysvaltoihin. Vaikka viimeksi mainituilla on käytettävissään kuitenkin joitakin muita oikeussuojakeinoja, niiden käytölle on huomattavia esteitä.

67. Erityisesti Yhdysvaltojen perustuslain III §:n mukaan kaikki kanteet liittovaltion tuomioistuimissa edellyttävät kyseessä olevan henkilön asiavaltuuden (standing) osoittamista. Asiavaltuus edellyttää, että tämä henkilö osoittaa, että hänelle on aiheutunut todellista vahinkoa, joka on yhtäältä konkreettinen ja erottuva ja toisaalta tosiasiallinen tai välittömästi uhkaava. Ennakkoratkaisua pyytänyt tuomioistuin viittaa muun muassa Supreme Court of the United Statesin (Yhdysvaltojen ylin tuomioistuin) antamaan tuomioon Clapper v. Amnesty International US [18] ja katsoo, että tätä edellytystä on käytännössä kohtuuttoman vaikea täyttää, kun otetaan huomioon, ettei rekisteröidyille tarvitse ilmoittaa heitä kohtaan toteutetuista tarkkailutoimenpiteistä. [19] Osa unionin kansalaisten käytettävissä olevista oikeussuojakeinoista edellyttää lisäksi muiden rajoittavien edellytysten noudattamista, kuten taloudellisen vahingon toteen näyttämistä. Tiedusteluelimille tunnustettu täysivaltainen koskemattomuus ja tietojen turvallisuusluokitus ovat niin ikään esteenä tiettyjen oikeussuojakeinojen käyttämiselle. [20]

68. High Court viittaa lisäksi tiedusteluelinten toimintaa koskeviin eri valvonta- ja vastuumekanismeihin.

69. Näihin mekanismeihin kuuluvat yhtäältä sertifiointimekanismi, jolla FISC vahvistaa vuosittain FISA:n 702 §:ään perustuvat ohjelmat ja jonka yhteydessä FISC ei kuitenkaan hyväksy yksittäisiä valintakriteerejä. Ulkomaantiedustelutietojen keräämiseen EO 12333:n nojalla ei myöskään kohdistu minkäänlaista tuomioistuimen etukäteisvalvontaa.

70. Ennakkoratkaisua pyytänyt tuomioistuin viittaa myös useisiin tiedustelutoimintaa koskeviin tuomioistuimen ulkopuolisiin vastuumekanismeihin. Se mainitsee erityisesti Inspectors Generalin (valvontaviranomaiset, Yhdysvallat), joiden tehtävänä on tarkastaa tarkkailutoimintaa kussakin tiedusteluelimessä. Lisäksi Privacy and Civil Liberties Oversight Board (PCLOB) (yksityisyyden ja kansalaisvapauksien valvontalautakunta, Yhdysvallat), joka on toimeenpanovaltaan kuuluva itsenäinen elin, saa raportteja kussakin elimessä kansalaisvapauksiin tai yksityisyyden suojaan liittyviä tehtäviä hoitavaksi virkamieheksi (civil liberties or privacy officers) nimetyiltä henkilöiltä. PCLOB laatii säännönmukaisesti raportteja parlamentin valiokunnille ja presidentille. Kyseisten elinten on saatettava ulkomaantiedustelutietojen keräämistä sääntelevien sääntöjen ja menettelyjen noudattamatta jättämistä koskevat tapaukset muun muassa DNI:n tietoon. Näistä tapauksista raportoidaan myös FISC:lle. Myös Yhdysvaltojen kongressilla on edustajainhuoneen ja senaatin tiedusteluvaliokuntien välityksellä ulkomaantiedustelutoimintaan liittyvää valvontavastuuta.

71. High Court korostaa kuitenkin perustavanlaatuista eroa yhtäältä niiden sääntöjen, joilla on tarkoitus varmistaa, että tiedot on saatu laillisesti ja että niiden saamisen jälkeen niitä ei käytetä väärin, ja toisaalta näiden sääntöjen rikkomistapauksessa käytettävissä olevien oikeussuojakeinojen välillä. Rekisteröityjen perusoikeuksien suoja varmistetaan vain, jos he voivat tehokkaiden oikeussuojakeinojen avulla vedota oikeuksiinsa tapauksessa, jossa kyseisiä sääntöjä ei noudateta.

18 133 S.Ct. 1138 (2013).

19 Ennakkoratkaisua pyytänyt tuomioistuin toteaa kuitenkin, että periaatteesta, jonka mukaan ilmoitusta tarkkailutoimenpiteen kohteena olevalle henkilölle ei edellytetä, voidaan poiketa silloin, jos Yhdysvaltojen hallituksella on tarkoitus käyttää tätä henkilöä vastaan FISA:n 702 §:n nojalla kerättyjä tietoja rikosoikeudellisessa tai hallinnollisessa menettelyssä.

20 Ennakkoratkaisua pyytänyt tuomioistuin tuo erityisesti esille, että vaikka oikeussuojaa koskevalla lailla (Judicial Redress Act (JRA)) yksityisyyden suojaa koskevan lain (Privacy Act), jossa annetaan luonnollisille henkilöille oikeus saada tietyillä viranomaisilla olevat heitä itseään koskevat tiedot tiettyjen kolmansien maiden osalta, säännökset on ulotettu koskemaan unionin kansalaisia, NSA ei lukeudu JRA:ssa tarkoitettuihin viranomaisiin.

72. Tässä tilanteessa ennakkoratkaisua pyytänyt tuomioistuin pitää perusteltuina DPC:n väitteitä, joiden mukaan Yhdysvaltojen oikeudessa asetetut rajoitukset niiden henkilöiden oikeussuojakeinoille, joiden tietoja siirretään unionista, eivät ole perusoikeuskirjan 47 artiklassa taatun oikeuden keskeisen sisällön mukaisia ja joka tapauksessa merkitsevät suhteetonta puuttumista tämän oikeuden käyttämiseen.

73. High Courtin mukaan se, että Yhdysvaltojen hallitus on ottanut käyttöön Privacy Shield -päätöksessä kuvatun oikeusasiamiesmekanismin, ei kyseenalaista tätä arviointia. Korostettuaan, että tämä mekanismi on niiden unionin kansalaisten käytettävissä, joilla on kohtuullinen peruste katsoa, että heidän tietojaan on siirretty mallisopimuslausekkeita koskevien päätösten mukaisesti,[21] kyseinen tuomioistuin huomauttaa, että oikeusasiamies ei ole perusoikeuskirjan 47 artiklan vaatimukset täyttävä tuomioistuin eikä etenkään riippumaton toimeenpanovallasta.[22] Kyseinen tuomioistuin epäilee myös sitä, että oikeusasiamiehen, jonka päätöksistä ei voi valittaa tuomioistuimeen, toiminta merkitsisi tehokasta oikeussuojakeinoa. Oikeusasiamiehen toiminnan perusteella henkilöt, joiden henkilötietoja on kerätty, käsitelty tai jaettu lainvastaisesti, eivät voi saada korvausta tai määräystä lopettaa lainvastaiset toimet, koska oikeusasiamies ei vahvista tai kiistä sitä, että henkilö on ollut sähköisen tarkkailun kohteena.

74. Tuotuaan näin esille huolensa siitä, vastaavatko Yhdysvaltojen oikeudessa annetut takeet ja perusoikeuskirjan 7, 8 ja 47 artiklasta seuraavat vaatimukset pääosin toisiaan, ennakkoratkaisua pyytänyt tuomioistuin on esittänyt kysymyksiä siitä, voidaanko mallisopimuslausekkeita koskeviin päätöksiin sisältyvillä mallisopimuslausekkeilla – jotka eivät luonteensa vuoksi sido Yhdysvaltojen viranomaisia – kuitenkin varmistaa rekisteröityjen perusoikeuksien suoja. Kyseinen tuomioistuin on todennut yhtyvänsä DPC:n epäilyihin, jotka kohdistuvat näiden päätösten pätevyyteen.

75. Tältä osin ennakkoratkaisua pyytänyt tuomioistuin katsoo erityisesti, että direktiivin 95/46 28 artiklan 3 kohta, johon päätöksen 2010/87 4 artiklassa viitataan, siltä osin kuin siinä annetaan valvontaviranomaisille valta keskeyttää tai kieltää tähän päätökseen sisältyviin mallisopimuslausekkeisiin perustuvat siirrot, ei riitä poistamaan näitä epäilyjä. Ennakkoratkaisua pyytäneen tuomioistuimen mukaan tämä valta on luonteeltaan vain harkintavaltaa, minkä lisäksi se pohtii päätöksen 2010/87 johdanto-osan 11 perustelukappaleen valossa mahdollisuutta käyttää tätä valtaa, kun todetut laiminlyönnit eivät koske yksittäistä poikkeustapausta vaan ovat luonteeltaan yleisiä ja systeemisiä.[23] Se katsoo myös, että vaara eri jäsenvaltioissa annettavista erilaisista ratkaisuista voisi olla esteenä sille, että tällaisten laiminlyöntien toteaminen annetaan valvontaviranomaisten tehtäväksi.

76. Tässä tilanteessa High Court päätti 4.5.2018 tekemällään päätöksellä[24], joka on saapunut unionin tuomioistuimeen 9.5.2018, lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

”1) Olosuhteissa, joissa yksityinen yritys siirtää henkilötietoja [unionin] jäsenvaltiosta yksityiselle yritykselle kolmanteen maahan kaupallisessa tarkoituksessa [päätöksen 2010/87] nojalla ja näitä tietoja voivat edelleen käsitellä kolmannessa maassa sen viranomaiset kansallista turvallisuutta

21 Ennakkoratkaisua pyytänyt tuomioistuin viittaa tässä tarkoituksessa Privacy Shield -päätöksen liitteeseen III A (ks. tämän ratkaisuehdotuksen 37 ja 38 kohta).

22 Ennakkoratkaisua pyytänyt tuomioistuin viittaa 27.1.2005 annettuun tuomioon Denuit ja Cordenier (C-125/04, EU:C:2005:69, 12 kohta).

23 Päätöksen 2010/87 johdanto-osan 11 perustelukappaleessa todetaan seuraavaa: ”Tässä sopimusmenettelyssä jäsenvaltioiden valvontaviranomaisilla on keskeinen tehtävä sen varmistamisessa, että henkilötietoja suojataan riittävästi niiden siirron jälkeen. Poikkeustapauksissa, joissa tietojen viejä kieltäytyy antamasta tietojen tuojalle ohjeita tai ei kykene antamaan niitä asianmukaisesti, ja on olemassa välitön vaara vakavasta haitasta rekisteröidyille, mallisopimuslausekkeiden olisi mahdollistettava se, että valvontaviranomaiset voivat tarkastaa tietojen tuojien ja alihankkijoina toimivien käsittelijöiden toimintaa ja tarvittaessa tehdä tietojen tuojia ja alihankkijana toimivia käsittelijöitä velvoittavia päätöksiä. Valvontaviranomaisilla olisi oltava oikeus kieltää tai lykätä mallisopimuslausekkeisiin perustuva tietojen siirto tai siirtojen sarja tietyin edellytyksin niissä poikkeustapauksissa, joissa sopimusperusteisella siirrolla todennäköisesti on merkittävä haitallinen vaikutus takeisiin ja velvoitteisiin, joilla rekisteröidylle annetaan riittävä tietosuoja.”

24 Facebook Ireland valitti ennakkoratkaisupyynnön esittämistä koskevasta päätöksestä Supreme Courtiin (ylin tuomioistuin, Irlanti). Valitus hylättiin 31.5.2019 annetulla tuomiolla The Data Protection Commissioner v. Facebook Ireland Limited ja Maximillian Schrems, valitus nro 2018/68 (jäljempänä Supreme Courtin 31.5.2019 antama tuomio).

varten mutta myös lainvalvontaa ja kolmannen maan ulkosuhteiden hoitamista varten, sovelletaanko unionin oikeutta (mukaan lukien perusoikeuskirja) tietojensiirtoon huolimatta SEU 4 artiklan 2 kohdan kansallista turvallisuutta koskevista määräyksistä ja [direktiivin 95/46] 3 artiklan 2 kohdan ensimmäisen luetelmakohdan yleistä turvallisuutta, puolustusta ja valtion turvallisuutta koskevista säännöksistä?

2) a) Määritettäessä, onko kyseessä henkilön oikeuksien loukkaus, kun tietoja siirretään [päätöksen 2010/87] nojalla unionista kolmanteen maahan, jossa niitä voidaan edelleen käsitellä kansallista turvallisuutta varten, onko vertailuperusteena direktiivin [95/46] mukaisesti

   i) perusoikeuskirja, SEU, SEUT, direktiivi [95/46], [Roomassa 4.11.1950 allekirjoitettu ihmisoikeuksien ja perusvapauksien suojaamiseksi tehty yleissopimus, jäljempänä Euroopan ihmisoikeussopimus] (tai jokin muu unionin oikeussääntö) vai

   ii) yhden tai useamman jäsenvaltion lainsäädäntö?

   b) Jos vertailuperuste on ii), onko kansalliseen turvallisuuteen liittyvät käytännöt yhdessä tai useammassa jäsenvaltiossa myös sisällytettävä vertailuperusteeseen?

3) Arvioitaessa, takaako kolmas maa sinne lähetetyille henkilötiedoille unionin lainsäädännössä edellytetyn suojan tason direktiivin [95/46] 26 artiklan mukaisesti, onko suojan tasoa kolmannessa maassa arvioitava käyttäen perusteena

   a) kolmannessa maassa sovellettavia sääntöjä, jotka seuraavat sen omasta lainsäädännöstä tai kansainvälisistä sitoumuksista, ja näiden sääntöjen noudattamisen varmistamiseksi laadittua käytäntöä, mukaan lukien ammatilliset säännöt ja turvatoimenpiteet, joita noudatetaan kolmannessa maassa

   vai

   b) edellä a kohdassa mainittuja sääntöjä yhdessä sellaisten hallinnollisten käytäntöjen, sääntelykäytäntöjen ja valvontakäytäntöjen, toimintaperiaatteisiin liittyvien suojakeinojen, menettelyiden, protokollien, seurantajärjestelmien ja tuomioistuimen ulkopuolisten oikeussuojakeinojen kanssa, jotka kolmannessa maassa ovat käytössä?

4) Kun otetaan huomioon High Courtin Yhdysvaltojen lainsäädännöstä tekemät tosiseikkoja koskevat toteamukset, loukkaako henkilötietojen siirto unionista Yhdysvaltoihin [päätöksen 2010/87] nojalla perusoikeuskirjan 7 ja/tai 8 artiklassa tarkoitettuja yksilöiden oikeuksia?

5) Kun otetaan huomioon High Courtin Yhdysvaltojen lainsäädännöstä tekemät tosiseikkoja koskevat toteamukset siirrettäessä henkilötietoja unionista Yhdysvaltoihin [päätöksen 2010/87] nojalla,

   a) kunnioittaako Yhdysvaltojen tarjoama suojan taso yksilölle perusoikeuskirjan 47 artiklassa taatun oikeussuojakeinoa koskevan oikeuden keskeistä sisältöä siinä tapauksessa, että yksilön tietosuojaoikeuksia loukataan?

Jos edellä a kohtaan vastataan myöntävästi,

   b) ovatko rajoitukset, joita Yhdysvaltojen lainsäädännössä asetetaan yksilön oikeussuojakeinoa koskevalle oikeudelle Yhdysvaltojen kansallisen turvallisuuden yhteydessä, suhteellisuusperiaatteen mukaisia perusoikeuskirjan 52 artiklassa tarkoitetulla tavalla ja sellaisia, että ne eivät mene yli sen, mikä on tarpeen demokraattisessa yhteiskunnassa kansallisen turvallisuuden perusteella?

6) a) Minkä tasoista suojaa edellytetään annettavan henkilötiedoille, jotka on siirretty kolmanteen maahan mallisopimuslausekkeiden mukaisesti, jotka on annettu [direktiivin 95/46] 26 artiklan 4 kohdan nojalla annetun komission päätöksen mukaisesti, [tämän] direktiivin säännösten valossa ja erityisesti [sen] 25 ja 26 artiklan valossa, kun ne luetaan perusoikeuskirjan valossa?

b) Mitä seikkoja on otettava huomioon arvioitaessa, täyttääkö [päätöksen 2010/87] nojalla kolmanteen maahan siirretyille tiedoille annettu suojan taso direktiivissä [95/46] ja perusoikeuskirjassa asetetut vaatimukset?

7) Onko se, että mallisopimuslausekkeita sovelletaan tietojen viejän ja tietojen tuojan välillä ja ne eivät sido kansallisia viranomaisia kolmannessa maassa, joka voi pyytää tietojen tuojaa asettamaan turvallisuuspalvelujensa saataville edelleen käsittelyä varten [päätöksen 2010/87] lausekkeiden mukaisesti siirretyt henkilötiedot, esteenä sille, että lausekkeet voisivat tarjota direktiivin [95/46] 26 artiklan 2 kohdassa tarkoitetut riittävät takeet?

8) Jos kolmannen maan tietojen tuojaan sovelletaan tarkkailulainsäädäntöä, joka [valvontaviranomaisen] näkökulmasta on ristiriidassa [mallisopimuslausekkeiden] tai direktiivin [95/46] 25 ja 26 artiklan ja/tai perusoikeuskirjan kanssa, onko [valvontaviranomaisen] käytettävä direktiivin [95/46] 28 artiklan 3 kohdan mukaisia lainvalvontavaltuuksiaan keskeyttääkseen tietojensiirrot, vai onko näiden valtuuksien käyttö rajattu vain poikkeuksellisiin tapauksiin [päätöksen 2010/87] johdanto-osan 11 perustelukappaleen valossa, vai voiko [valvontaviranomainen] käyttää harkintavaltaansa ja olla keskeyttämättä tietojensiirtoa?

9) a) Onko [Privacy Shield -päätös] direktiivin [95/46] 25 artiklan 6 kohdassa tarkoitettu yleisesti sovellettava toteamus, joka sitoo jäsenvaltioiden [valvontaviranomaisia] ja tuomioistuimia ja jonka mukaan Yhdysvallat varmistaa direktiivin [95/46] 25 artiklan 2 kohdassa tarkoitetun riittävän suojan tason kansallisessa lainsäädännössään tai kansainvälisissä sitoumuksissaan?

b) Jos näin ei ole, mitä merkitystä Privacy Shield -päätöksellä on arvioitaessa niiden takeiden riittävyyttä, jotka [päätöksen 2010/87] mukaisesti annetaan Yhdysvaltoihin siirretyille tiedoille?

10) Kun otetaan huomioon High Courtin tekemät toteamukset Yhdysvaltojen lainsäädännöstä, varmistaako Privacy Shield -päätöksen [liitteeseen III A] sisältyvä Privacy Shield -oikeusasiamiesjärjestelmä, kun sitä tarkastellaan yhdessä Yhdysvaltojen olemassa olevan järjestelmän kanssa, että Yhdysvallat tarjoaa rekisteröidyille, joiden henkilötietoja on siirretty Yhdysvaltoihin [päätöksen 2010/87] perusteella, oikeussuojakeinon, joka on yhteensopiva perusoikeuskirjan 47 artiklan kanssa?

11) Loukataanko [päätöksellä 2010/87] perusoikeuskirjan 7, 8 ja/tai 47 artiklaa?”

77. DPC, Facebook Ireland, Schrems, Yhdysvaltojen hallitus, EPIC, BSA, Digitaleurope, Irlanti, Belgian, Tšekin, Saksan, Alankomaiden, Itävallan, Puolan, Portugalin ja Yhdistyneen kuningaskunnan hallitukset, Euroopan parlamentti ja komissio toimittivat kirjalliset huomautuksensa unionin tuomioistuimelle. DPC, Facebook Ireland, Schrems, Yhdysvaltojen hallitus, EPIC, BSA, Digitaleurope, Irlanti, Saksan, Ranskan, Alankomaiden, Itävallan ja Yhdistyneen kuningaskunnan hallitukset, parlamentti, komissio ja Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB) olivat edustettuina 9.7.2019 pidetyssä istunnossa.

IV Asian tarkastelu

A Alustavat toteamukset

78. Unionin tuomioistuimen todettua tuomiossa Schrems safe harbor -päätöksen pätemättömäksi henkilötietojen siirto Yhdysvaltoihin on jatkunut muiden oikeusperustojen nojalla. Erityisesti tietojen viejäyhtiöt ovat voineet turvautua tietojen tuojien kanssa tehtäviin sopimuksiin, jotka sisältävät komission laatimia mallilausekkeita. Näitä lausekkeita voidaan käyttää myös oikeusperustana siirroille useisiin muihin kolmansiin maihin, joiden osalta komissio ei ole tehnyt tietosuojan riittävyyttä koskevaa päätöstä.[25] Privacy Shield -päätöksen perusteella yritykset, jotka ovat antaneet oman varmennuksen siinä mainittujen periaatteiden noudattamisesta, voivat vastedes siirtää henkilötietoja Yhdysvaltoihin ilman muita muodollisuuksia.

79. Kuten ennakkoratkaisupyynnössä nimenomaisesti todetaan ja kuten BSA, Digitaleurope, Irlanti, Itävallan ja Ranskan hallitukset, parlamentti ja komissio korostavat, High Courtissa vireillä olevan pääasian ainoana tarkoituksena on sen ratkaiseminen, onko päätös, jolla komissio on ottanut käyttöön mallisopimuslausekkeet, joihin on vedottu Schremsin kantelussa tarkoitettujen siirtojen tueksi, eli päätös 2010/87[26] pätevä.

80. Tämän oikeusriidan taustalla on hakemus, jossa DPC pyysi ennakkoratkaisua pyytänyttä tuomioistuinta esittämään unionin tuomioistuimelle ennakkoratkaisukysymyksen päätöksen 2010/87 pätevyydestä. Kyseisen tuomioistuimen mukaan pääasia koskee siten sen oikeussuojakeinon käyttöä, josta unionin tuomioistuin on tuomion Schrems 65 kohdassa velvoittanut jäsenvaltiot säätämään.

81. Unionin tuomioistuinhan totesi kyseisen tuomion 63 kohdassa, että kun henkilö, jonka henkilötiedot on siirretty tai voitaisiin siirtää tietosuojan riittävyyttä koskevan päätöksen kohteena olevaan kolmanteen maahan, saattaa valvontaviranomaisen käsiteltäväksi kantelun ja riitauttaa tämän päätöksen yhteensoveltuvuuden perusoikeuskirjassa vahvistettujen perusoikeuksien kanssa, valvontaviranomaisen on tutkittava kyseinen kantelu kaikkea asianmukaista huolellisuutta noudattaen. Kyseisen tuomion 65 kohdan mukaan tapauksessa, jossa tämä viranomainen pitää tässä kantelussa esitettyjä perusteita perusteltuina, sen on direktiivin 95/46 28 artiklan 3 kohdan ensimmäisen alakohdan kolmannen luetelmakohdan (jota tietosuoja-asetuksen 58 artiklan 5 kohta vastaa), luettuna perusoikeuskirjan 8 artiklan 3 kohdan valossa, mukaisesti voitava olla asianosaisena oikeudenkäynnissä. Tässä yhteydessä kansallisen lainsäätäjän on säädettävä oikeussuojakeinoista, joiden avulla kyseinen viranomainen voi esittää perusteltuina pitämänsä perusteet kansallisissa tuomioistuimissa, jotta nämä voisivat, mikäli ne yhtyvät kyseisen viranomaisen epäilyihin, pyytää ennakkoratkaisua kyseisen päätöksen pätevyydestä.

82. Katson ennakkoratkaisua pyytäneen tuomioistuimen tavoin, että nämä johtopäätökset pätevät analogisesti, kun valvontaviranomainen epäilee sille esitetyn kantelun käsittelyn yhteydessä tietosuojan riittävyyttä koskevan päätöksen sijaan päätöksen 2010/87 kaltaisen päätöksen, jolla vahvistetaan mallisopimuslausekkeet henkilötietojen siirrolle kolmansiin maihin, pätevyyttä. Toisin kuin Saksan hallitus väittää, on merkityksetöntä, vastaavatko nämä epäilyt kantelijan valvontaviranomaiselle esittämiä perusteita tai kyseenalaistaako tämä viranomainen kyseisen päätöksen pätevyyden omasta aloitteestaan. Tietosuoja-asetuksen 58 artiklan 5 kohdasta ja perusoikeuskirjan 8 artiklan 3 kohdasta

25 BSA:n mukaan 70 prosenttia tästä tehtyyn kyselyyn vastanneista sen jäsenyrityksistä ilmoitti turvautuneensa mallisopimuslausekkeisiin henkilötietojen kolmansiin maihin siirtämisen pääasiallisena perustana. Digitaleurope katsoo myös, että mallisopimuslausekkeet ovat pääasiallinen oikeudellinen väline, johon näiden siirtojen tueksi on vedottu.

26 Vaikka ennakkoratkaisua pyytänyt tuomioistuin toteaa ennakkoratkaisupyyntönsä koskevan kolmen mallisopimuslausekkeita koskevan päätöksen pätevyyttä, sillä ne on tutkittu DPC:n päätösluonnoksessa ja 3.10.2017 annetussa tuomiossa, ennakkoratkaisukysymyksissä viitataan yksinomaan päätökseen 2010/87. Tämä johtuu siitä, että Facebook Ireland on kyseisessä tuomioistuimessa ilmoittanut tämän päätöksen oikeusperustaksi Facebook-verkkoyhteisöpalvelun käyttäjien tietojen siirrolle Yhdysvaltoihin. Tarkasteluni koskee siksi yksinomaan kyseistä päätöstä.

seuraavia vaatimuksia, joihin unionin tuomioistuimen perustelut perustuvat, sovelletaan riippumatta valvontaviranomaiselle tehdyssä kantelussa tarkoitetun siirron oikeusperustasta ja syistä, jotka ovat saaneet tämän viranomaisen epäilemään kyseisen päätöksen pätevyyttä tämän kantelun käsittelyn yhteydessä.

83. Tämän tultua todetuksi on kuitenkin niin, että DPC on halunnut ennakkoratkaisua pyytäneen tuomioistuimen kysyvän unionin tuomioistuimelta päätöksen 2010/87 pätevyydestä nimenomaan sen vuoksi, että hän on pitänyt unionin tuomioistuimen tästä asiasta esittämää selvennystä tarpeellisena voidakseen käsitellä kantelun, jolla Schrems pyytää häntä käyttämään direktiivin 95/46 28 artiklan 3 kohdan toisessa luetelmakohdassa hänelle annettua toimivaltuutta – joka on sittemmin annettu tietosuoja-asetuksen 58 artiklan 2 kohdan f alakohdassa – keskeyttää Facebook Irelandin toteuttama Schremsin henkilötietojen siirto Facebook Inc:lle.

84. Kun pääasia koskee yksinomaan päätöksen 2010/87 pätevyyttä *abstraktilla tasolla*, sen taustalla oleva DPC:n vireillä oleva menettely koskee viimeksi mainitun korjaavien toimivaltuuksien käyttöä *erityisessä tapauksessa*. Ehdotan, että unionin tuomioistuin pitäytyy tarkastelemaan esitettyjä kysymyksiä siltä osin kuin se on tarpeellista päätöksen 2010/87 pätevyyden selvittämiseksi, koska ennakkoratkaisua pyytäneellä tuomioistuimella on tällaisen tarkastelun perusteella riittävät edellytykset ratkaista siinä vireillä oleva asia. [27]

85. Ennen tämän päätöksen pätevyyden arvioimista on hylättävä tietyt väitteet, joiden mukaan ennakkoratkaisupyyntö pitäisi jättää tutkimatta.

B Ennakkoratkaisupyynnön tutkittavaksi ottaminen

86. Ennakkoratkaisupyynnön tutkittavaksi ottamista on vastustettu useilla perusteilla, jotka liittyvät lähinnä ennakkoratkaisukysymyksissä tarkoitetun direktiivin 95/46 ajalliseen soveltumattomuuteen (osa 1), siihen, että DPC:n menettely ei ole saavuttanut riittävän edistynyttä vaihetta, jotta ennakkoratkaisupyyntöä olisi perusteltua pitää hyödyllisenä (osa 2), ja siihen, että ennakkoratkaisua pyytäneen tuomioistuimen kuvaamiin asian tosiseikkoihin liittyy edelleen epävarmuustekijöitä (osa 3).

87. Vastaan näihin oikeudenkäyntiväitteisiin pitäen mielessä, että unionin tuomioistuimelle SEUT 267 artiklan nojalla esitetyillä kysymyksillä oletetaan olevan merkitystä asian ratkaisemisen kannalta. Vakiintuneen oikeuskäytännön mukaan unionin tuomioistuin voi kieltäytyä ratkaisemasta ennakkoratkaisupyynnön ainoastaan silloin, kun on ilmeistä, että pyydetyllä unionin oikeuden tulkitsemisella ei ole mitään yhteyttä kansallisessa tuomioistuimessa käsiteltävän asian tosiseikkoihin tai kohteeseen, jos kyseinen ongelma on luonteeltaan hypoteettinen taikka jos unionin tuomioistuimella ei ole tiedossaan niitä tosiseikkoja ja oikeudellisia seikkoja, jotka ovat tarpeen, jotta se voisi antaa hyödyllisen vastauksen sille esitettyihin kysymyksiin. [28]

1. Direktiivin 95/46 ajallinen sovellettavuus

88. Facebook Ireland vetoaa ennakkoratkaisukysymysten tutkittavaksi ottamisen edellytysten puuttumiseen sillä perusteella, että niissä viitataan direktiiviin 95/46, vaikka tämä direktiivi on kumottu ja korvattu tietosuoja-asetuksella 25.5.2018 alkaen. [29]

89. Yhdyn kantaan, jonka mukaan päätöksen 2010/87 pätevyyttä on tarkasteltava tietosuoja-asetuksen säännösten valossa.

27 Ks. tämän ratkaisuehdotuksen 167–186 kohta.

28 Ks. mm. tuomio 10.12.2018, Wightman ym. (C-621/18, EU:C:2018:999, 27 kohta) ja tuomio 19.11.2019, A. K. ym. (Ylimmän tuomioistuimen kurinpitojaoston riippumattomuus) (C-585/18, C-624/18 ja C-625/18, EU:C:2019:982, 98 kohta).

29 Ks. tietosuoja-asetuksen 94 artiklan 1 kohta ja 99 artiklan 1 kohta.

90. Tämän asetuksen 94 artiklan 2 kohdan mukaan ”viittauksia kumottuun direktiivin pidetään viitauksina [kyseiseen asetukseen]”. Nähdäkseni tästä seuraa, että siltä osin kuin päätöksessä 2010/87 mainitaan oikeusperustaksi direktiivin 95/46 26 artiklan 4 kohta, siinä on ymmärrettävä viitattavan tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohtaan, jossa toistetaan olennaisilta osin sen sisältö.[30] Näin ollen komission direktiivin 95/46 26 artiklan 4 kohdan nojalla ennen tietosuoja-asetuksen voimaantuloa antamia täytäntöönpanopäätöksiä on tulkittava tämän asetuksen valossa. Myös niiden pätevyyttä on tarvittaessa arvioitava kyseisen asetuksen kannalta.

91. Tätä johtopäätöstä ei kyseenalaisteta oikeuskäytännössä, jonka mukaan unionin toimen laillisuutta on arvioitava toimen antamishetkellä vallinneiden tosiseikkojen ja oikeudellisten seikkojen kannalta. Tämä oikeuskäytäntö koskee unionin toimen pätevyyden tarkastelua toimen antamisajankohtana merkityksellisten tosiasiallisten olosuhteiden kannalta[31] tai sellaisten menettelysääntöjen kannalta, joilla säännellään sen antamista.[32] Unionin tuomioistuin on sitä vastoin toistuvasti tutkinut johdetun oikeuden toimien pätevyyttä näiden toimien antamisen jälkeen voimaan tulleiden ylemmäntasoisten aineellisoikeudellisten normien kannalta.[33]

92. Vaikka ennakkoratkaisukysymyksissä oleva viittaus toimeen, joka ei enää ole ajallisesti sovellettavissa, oikeuttaa näiden kysymysten muotoilemisen uudelleen, se ei kuitenkaan voi johtaa niiden tutkimatta jättämiseen.[34] Kuten DPC ja Schrems väittävät, ennakkoratkaisukysymyksissä olevat viittaukset direktiiviin 95/46 voivat selittyä myös esillä olevan asian käsittelyaikataululla, sillä nämä kysymykset on esitetty unionin tuomioistuimelle ennen tietosuoja-asetuksen voimaantuloa.

93. Tietosuoja-asetuksen säännöksissä, joita käsitellään ennakkoratkaisukysymysten arvioimiseksi, erityisesti sen 45, 46 ja 58 artiklassa, joka tapauksessa toistetaan hienoisia eroavaisuuksia lukuun ottamatta direktiivin 95/46 25, 26 ja 28 artiklan pääasiallinen sisältö ja samalla kehitetään sitä. Siltä osin kuin ne ovat merkityksellisiä päätöksen 2010/87 pätevyyden arvioimiseksi, en näe mitään syytä antaa näille tietosuoja-asetuksen säännöksille eri merkitystä kuin direktiivin 95/46 vastaaville säännöksille.[35]

2. DPC:n ilmaisemien epäilyjen alustavuus

94. Saksan hallituksen mukaan ennakkoratkaisupyyntö on jätettävä tutkimatta, koska tuomion Schrems 65 kohdassa tarkoitettu muutoksenhakumenettely edellyttää, että valvontaviranomainen on muodostanut lopullisen kannan kantajan kyseessä olevan päätöksen pätevyyttä vastaan esittämistä perusteista. Näin ei ole tässä tapauksessa, koska DPC on ilmaissut epäilevänsä päätöksen 2010/87 pätevyyttä – jota Schrems ei ole riitauttanut – päätösluonnoksessa, joka on annettu alustavasti sen kuitenkaan rajoittamatta Facebook Irelandin ja Schremsin oikeutta esittää mahdollisia täydentäviä huomautuksia.

30 Korostettakoon, että tietosuoja-asetuksen 46 artiklan 5 kohdan mukaan päätökset, jotka komissio on antanut direktiivin 95/46 26 artiklan 4 kohdan nojalla, pysyvät voimassa, kunnes niitä muutetaan, ne korvataan tai kumotaan.

31 Ks. mm. tuomio 7.2.1979, Ranska v. komissio (15/76 ja 16/76, EU:C:1979:29, 7 kohta); tuomio 17.5.2001, IECC v. komissio (C-449/98 P, EU:C:2001:275, 87 kohta) ja tuomio 17.10.2013, Schaible (C-101/12, EU:C:2013:661, 50 kohta).

32 Ks. mm. tuomio 16.4.2015, parlamentti v. neuvosto (C-540/13, EU:C:2015:224, 35 kohta); tuomio 16.4.2015, parlamentti v. neuvosto (C-317/13 ja C-679/13, EU:C:2015:223, 45 kohta) ja tuomio 22.9.2016, parlamentti v. neuvosto (C-14/15 ja C-116/15, EU:C:2016:715, 48 kohta).

33 Erityisesti tuomiossa Schrems unionin tuomioistuin arvioi safe harbor -päätöksen pätevyyttä perusoikeuskirjan – joka on annettu kyseisen päätöksen tekemisen jälkeen – määräysten kannalta. Ks. myös tuomio 17.3.2011, AJD Tuna (C-221/09, EU:C:2011:153, 48 kohta) ja tuomio 11.6.2015, Pfeifer & Langen (C-51/14, EU:C:2015:380, 42 kohta).

34 Ks. mm. tuomio 15.7.2010, Pannon Gép Centrum (C-368/09, EU:C:2010:441, 30–35 kohta); tuomio 10.2.2011, Andersson (C-30/10, EU:C:2011:66, 20 ja 21 kohta) ja tuomio 25.10.2018, Roche Lietuva (C-413/17, EU:C:2018:865, 17–20 kohta).

35 Ks. tältä osin julkisasiamies Bobekin ratkaisuehdotus Fashion ID (C-40/17, EU:C:2018:1039, 87 kohta).

95. Mielestäni se, että DPC:n ilmaisemat epäilyt ovat alustavia, ei vaikuta ennakkoratkaisupyynnön tutkittavaksi ottamiseen. Ennakkoratkaisukysymyksen tutkittavaksi ottamisen kriteerejä on arvioitava suhteessa asian kohteeseen, sellaisena kuin ennakkoratkaisua pyytänyt tuomioistuin on sen määritellyt.[36] On selvää, että asian kohteena on päätöksen 2010/87 pätevyys. Ennakkoratkaisupyynnön ja siihen liitetyn tuomion mukaan kyseinen tuomioistuin katsoo, että DPC:n ilmaisemat epäilyt – olipa ne ilmaistu alustavasti tai lopullisesti – ovat perusteltuja, ja pyytää tämän vuoksi unionin tuomioistuinta ottamaan kantaa tämän päätöksen pätevyyteen. Tässä tilanteessa unionin tuomioistuimen tältä osin esittämällä selvennyksellä on epäilyksettä merkitystä, jotta ennakkoratkaisua pyytänyt tuomioistuin voi ratkaista käsiteltäväkseen saatetun asian.

3. Asian tosiseikkojen määrittämiseen liittyvät epävarmuustekijät

96. Yhdistyneen kuningaskunnan hallitus väittää, että ennakkoratkaisua pyytäneen tuomioistuimen kuvaus asian tosiseikoista paljastaa useita puutteita, jotka saattavat ennakkoratkaisukysymysten tutkittavaksi ottamisen kyseenalaiseksi. Kyseinen tuomioistuin ei ole sen mukaan tehnyt selväksi, onko Schremsin henkilötiedot tosiasiallisesti siirretty Yhdysvaltoihin, ja jos on, ovatko Yhdysvaltojen viranomaiset keränneet ne. Näiden mahdollisten siirtojen oikeusperustaa ei myöskään ole todettu varmuudella, sillä ennakkoratkaisupyynnössä ainoastaan mainitaan, että
Facebook-verkkoyhteisöpalvelun eurooppalaisten käyttäjien tiedot siirretään ”suurelta osin” päätökseen 2010/87 sisältyvien mallisopimuslausekkeiden perusteella. Asiassa on joka tapauksessa jäänyt näyttämättä, että Facebook Irelandin ja Facebook Inc:n välisessä sopimuksessa, johon vedotaan riidanalaisten siirtojen tueksi, toistettaisiin nämä lausekkeet tarkasti. Saksan hallituksen mukaan ennakkoratkaisupyyntö on lisäksi jätettävä tutkimatta sen vuoksi, että ennakkoratkaisua pyytänyt tuomioistuin ei ole tutkinut, onko Schrems varmasti antanut suostumuksensa kyseisiin siirtoihin, jolloin ne perustuisivat pätevästi direktiivin 95/46 26 artiklan 1 kohtaan (jonka sisältö toistetaan olennaisilta osin tietosuoja-asetuksen 49 artiklan 1 kohdan a alakohdassa).

97. Näillä väitteillä ei mitenkään kyseenalaisteta ennakkoratkaisupyynnön merkitystä pääasian kohteen kannalta. Koska kyseisen asian taustalla on se, että DPC käyttää tuomion Schrems 65 kohdassa tarkoitettua oikeussuojakeinoa, sen nimenomaisena kohteena on saada kansallinen tuomioistuin esittämään ennakkoratkaisupyyntö päätöksen 2010/87 pätevyydestä. Saksan ja Yhdistyneen kuningaskunnan hallitukset eivät tosiasiassa kiistä ennakkoratkaisukysymysten tarpeellisuutta sen selvittämiseksi, onko tämä päätös pätevä, vaan niiden tarpeellisuuden, siltä kannalta, että DPC voi konkreettisesti ottaa kantaa Schremsin kanteluun.

98. Katson joka tapauksessa, että päätöksen 2010/87 pätevyyttä koskevat ennakkoratkaisukysymykset eivät ole merkityksettömiä edes tämän pääasian taustalla olevan menettelyn kannalta. Ennakkoratkaisua pyytänyt tuomioistuin toteaa, että Facebook Ireland on jatkanut käyttäjiensä tietojen siirtoa Yhdysvaltoihin safe harbor -päätöksen pätemättömäksi toteamisen jälkeen ja että nämä siirrot perustuvat ainakin osittain päätökseen 2010/87. Lisäksi katson, että vaikka voi olla hyödyllistä, että kaikki asian kannalta merkitykselliset tosiseikat on näytetty toteen ennen kuin tuomioistuin käyttää SEUT 267 artiklan mukaista toimivaltaansa, on yksin ennakkoratkaisua pyytäneen tuomioistuimen asiana arvioida, missä menettelyn vaiheessa se tarvitsee ennakkoratkaisua unionin tuomioistuimelta.[37]

99. Kaiken edellä esitetyn perusteella ennakkoratkaisupyyntö on mielestäni otettava tutkittavaksi.

36 Ks. tämän ratkaisuehdotuksen 87 kohta.

37 Ks. vastaavasti tuomio 1.4.1982, Holdijk ym. (141/81–143/81, EU:C:1982:122, 5 kohta) ja tuomio 9.12.2003, Gasser (C-116/02, EU:C:2003:657, 27 kohta).

C Unionin oikeuden sovellettavuus siirrettäessä henkilötietoja kaupallisessa tarkoituksessa kolmanteen valtioon, joka saattaa käsitellä niitä kansallista turvallisuutta varten (ensimmäinen kysymys)

100. Ensimmäisellä kysymyksellään ennakkoratkaisua pyytänyt tuomioistuin haluaa tietää, sovelletaanko unionin oikeutta tilanteessa, jossa jäsenvaltiossa sijaitseva yritys siirtää henkilötietoja kolmanteen maahan sijoittautuneelle yritykselle kaupallisessa tarkoituksessa, kun siirron aloittamisen jälkeen tämän kolmannen maan viranomaiset voivat käsitellä tietoja tarkoituksiin, jotka käsittävät kansallisen turvallisuuden suojelemisen.

101. Tämän kysymyksen merkitys pääasian ratkaisun kannalta on siinä, että jos tällainen siirto jäisi unionin oikeuden soveltamisalan ulkopuolelle, kaikki tässä asiassa päätöksen 2010/87 pätevyyttä vastaan tässä asiassa esitetyt väitteet olisivat perusteettomia.

102. Kuten ennakkoratkaisua pyytänyt tuomioistuin huomauttaa, henkilötietojen siirto kansallista turvallisuutta varten oli jätetty direktiivin 95/46 soveltamisalan ulkopuolelle tämän direktiivin 3 artiklan 2 kohdan nojalla. Tietosuoja-asetuksen 2 artiklan 2 kohdassa täsmennetään nyt, että tätä asetusta ei sovelleta muun muassa henkilötietojen käsittelyyn, jota suoritetaan sellaisen toiminnan yhteydessä, joka ei kuulu unionin lainsäädännön soveltamisalaan, tai jota toimivaltaiset viranomaiset suorittavat yleisen turvallisuuden suojelua varten. Nämä säännökset heijastavat SEU 4 artiklan 2 kohdassa jäsenvaltioille kansallisen turvallisuuden suojelun alalla varattua toimivaltaa.

103. DPC, Schrems, Irlanti, Saksan, Itävallan, Belgian, Tšekin, Alankomaiden, Puolan ja Portugalin hallitukset sekä parlamentti ja komissio väittävät, että näitä säännöksiä ei sovelleta Schremsin kantelussa tarkoitettujen siirtojen kaltaisiin siirtoihin ja että ne kuuluvat siten unionin oikeuden soveltamisalaan. Facebook Ireland puoltaa vastakkaista kantaa. Kannatan ensin mainittujen näkemystä.

104. Tältä osin on korostettava, että henkilötietojen siirto jäsenvaltiosta kolmanteen maahan on sellaisenaan tietosuoja-asetuksen 4 artiklan 2 alakohdassa tarkoitettua käsittelyä jäsenvaltion alueella.[38] Ensimmäisellä ennakkoratkaisukysymyksellä on tarkoitus nimenomaan selvittää, sovelletaanko unionin oikeutta *käsittelyyn, jota siirto itsessään on*. Tämä kysymys ei koske unionin oikeuden sovellettavuutta tilanteessa, jossa Yhdysvaltojen viranomaiset mahdollisesti myöhemmin käsittelevät Yhdysvaltoihin siirrettyjä henkilötietoja kansallista turvallisuutta varten, sillä nämä käsittelyt eivät kuulu tietosuoja-asetuksen alueelliseen soveltamisalaan.[39]

105. Tässä mielessä ratkaistaessa, sovelletaanko unionin oikeutta kyseessä olevaan tietojensiirtoon, on otettava huomioon ainoastaan toiminta, johon siirto kuuluu, eikä kohdemaana olevan kolmannen maan viranomaisten suorittaman siirrettyjen tietojen mahdollisen myöhemmän käsittelyn tarkoituksella ole merkitystä.[40]

106. Ennakkoratkaisupyynnöstä ilmenee, että Schremsin kantelussa tarkoitettu siirto liittyy kaupalliseen toimintaan. Siirtoa ei myöskään toteuteta siinä tarkoituksessa, että Yhdysvaltojen viranomaiset voisivat myöhemmin käsitellä kyseisiä tietoja kansallista turvallisuutta varten.

38 Ks. vastaavasti tuomio 30.5.2006, parlamentti v. neuvosto ja komissio (C-317/04 ja C-318/04, EU:C:2006:346; jäljempänä tuomio PNR, 56 kohta) ja tuomio Schrems (45 kohta). Tietosuoja-asetuksen 4 artiklan 2 alakohdassa toistetaan olennaisilta osin direktiivin 95/46 2 artiklan b alakohtaan sisältynyt käsittelyn määritelmä.

39 Tietosuoja-asetuksen 3 artiklan 1 kohdan mukaan tätä asetusta sovelletaan käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei. Kysymys siitä, onko unionin oikeus sovellettavissa kolmannen maan tiedustelupalvelujen suorittamaan käsittelyyn unionin ulkopuolella, on pidettävä erillään kysymyksestä, joka koskee tähän käsittelyyn kyseisessä kolmannessa maassa sovellettavien sääntöjen ja käytäntöjen merkitystä sen selvittämiseksi, varmistetaanko siellä riittävä tietosuoja. Tämä viimeksi mainittu kysymyksenasettelu on toisen ennakkoratkaisukysymyksen kohteena, ja sitä käsitellään jäljempänä tämän ratkaisuehdotuksen 201–229 kohdassa.

40 Ratkaisuehdotuksessani Ministerio Fiscal (C-207/16, EU:C:2018:300, 47 kohta) korostin erottelua henkilötietojen suoraan käsittelyyn valtion julkisen vallan tehtävien yhteydessä ja kaupalliseen käsittelyyn, jonka jälkeen viranomaiset käyttävät henkilötietoja.

107. Facebook Irelandin ehdottama lähestymistapa veisi myös tehokkaan vaikutuksen siirtoa kolmansiin maihin koskevilta tietosuoja-asetuksen säännöksiltä, koska ei voida koskaan pitää poissuljettuna, että kaupallisen toiminnan yhteydessä siirrettyjä tietoja käsitellään kansallista turvallisuutta varten siirron jälkeen.

108. Tietosuoja-asetuksen 45 artiklan 2 kohdan a alakohdan sanamuoto tukee puoltamaani tulkintaa. Tämän säännöksen mukaan tietosuojan riittävyyttä koskevan päätöksen antaessaan komissio ottaa huomioon muun muassa päätöksen kohteena olevan kolmannen maan lainsäädännön *kansallisen turvallisuuden alalla*. Tästä voidaan päätellä, että mahdollisuus, että kohdemaana olevan kolmannen maan viranomaiset käsittelevät tietoja kansallisen turvallisuuden suojelemiseksi, ei merkitse sitä, että unionin oikeutta ei voitaisi soveltaa käsittelyyn, jota tietojensiirto tähän kolmanteen maahan on.

109. Unionin tuomioistuimen päättely ja johtopäätös tuomiossa Schrems perustuvat myös tähän olettamaan. Unionin tuomioistuin tutki siinä erityisesti safe harbor -päätöksen pätevyyttä siltä osin kuin se koski henkilötietojen siirtoa Yhdysvaltoihin, jossa ne voitiin kerätä ja käsitellä kansallisen turvallisuuden suojelemista varten, direktiivin 95/46 25 artiklan 6 kohdan, luettuna perusoikeuskirjan valossa, kannalta. [41]

110. Näillä perusteilla katson, että unionin oikeutta sovelletaan henkilötietojen siirtoon jäsenvaltiosta kolmanteen maahan, kun tämä siirto liittyy kaupalliseen toimintaan, eikä sillä, että tämän kolmannen maan viranomaiset voivat käsitellä siirrettyjä tietoja kansallisen turvallisuuden suojelemiseksi, ole merkitystä.

D Edellytetty suojan taso mallisopimuslausekkeisiin perustuvan siirron yhteydessä (kuudennen kysymyksen ensimmäinen osa)

111. Ennakkoratkaisua pyytänyt tuomioistuin pyrkii kuudennen kysymyksensä ensimmäisen osan mukaan selvittämään, minkä tasoinen perusoikeuksien suoja rekisteröidyille on taattava, jotta henkilötietoja voidaan siirtää kolmanteen maahan päätöksen 2010/87 mukaisten mallisopimuslausekkeiden nojalla.

112. Kyseinen tuomioistuin korostaa, että unionin tuomioistuin tulkitsi tuomiossa Schrems direktiivin 95/46 25 artiklan 6 kohtaa (jonka sisältö on olennaisilta osin toistettu tietosuoja-asetuksen 45 artiklan 3 kohdassa) siten, että sen mukaan komissio voi antaa tietosuojan riittävyyttä koskevan päätöksen vasta varmistuttuaan, että päätöksen kohteena oleva kolmas maa takaa tietosuojan *riittävän* tason, mikä edellyttää komission osoittavan, että tämä maa takaa perusoikeuksien ja -vapauksien suojan sellaisen tason, joka *pääosiltaan vastaa* tasoa, joka taataan unionissa tämän direktiivin, luettuna perusoikeuskirjan valossa, nojalla. [42]

113. Tässä yhteydessä kuudennen ennakkoratkaisukysymyksen ensimmäisessä osassa unionin tuomioistuinta pyydetään ratkaisemaan, onko komission direktiivin 95/46 26 artiklan 4 kohdan mukaisesti antamien ”mallisopimuslausekkeiden” – jotka vastaavat sittemmin tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohdassa mainittuja ”tietosuojaa koskevia vakiolausekkeita” – soveltamisella voitava saavuttaa suojan taso, joka on saman ”pääosiltaan vastaavaa” koskevan vaatimuksen mukainen.

41 Samalla tavoin 26.7.2017 annetussa lausunnossa 1/15 (EU:n ja Kanadan välinen PNR-tietoja koskeva sopimus) (EU:C:2017:592; jäljempänä lausunto 1/15) unionin tuomioistuin tutki, oliko luonnos Kanadan ja unionin väliseksi kansainväliseksi sopimukseksi, joka koski tietoja, jotka oli niiden Kanadaan siirtämisen jälkeen tarkoitettu viranomaisten käsiteltäviksi kansallisen turvallisuuden suojelemista varten, perusoikeuskirjan 7, 8 ja 47 artiklan mukainen.

42 Tuomio Schrems (73 kohta). Unionin tuomioistuin vahvisti tämän johtopäätöksen lausunnossa 1/15 (134 kohta).

114. Tietosuoja-asetuksen 46 artiklan 1 kohdassa säädetään tästä, että jollei tietosuojan riittävyyttä koskevaa päätöstä ole tehty, rekisterinpitäjä voi siirtää henkilötietoja kolmanteen maahan ”vain, jos kyseinen rekisterinpitäjä – – on toteuttanut *asianmukaiset suojatoimet* ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja” (kursivointi tässä).[43] Tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohdan mukaan nämä suojatoimet voivat perustua muun muassa komission laatimiin tietosuojaa koskeviin vakiolausekkeisiin.

115. Katson DPC:n, Schremsin ja Irlannin tavoin, että rekisterinpitäjän toteuttamilla ”asianmukaisilla suojatoimilla”, joihin tietosuoja-asetuksen 46 artiklan 1 kohdassa viitataan, on varmistettava, että niiden henkilöiden oikeudet, joiden tietoja siirretään, saavat – kuten tietosuojan riittävyyttä koskevaan päätökseen perustuvassa siirrossa – pääosiltaan vastaavan suojan tason kuin tietosuoja-asetuksen seurauksena, kun sitä luetaan perusoikeuskirjan valossa.

116. Tämä johtopäätös perustuu kyseisen säännöksen ja säädöksen, jonka osa se on, tarkoitukseen.

117. Tietosuoja-asetuksen 45 ja 46 artiklan tavoitteena on varmistaa tällä asetuksella varmistetun henkilötietojen korkeatasoisen suojan jatkuvuus, kun näitä tietoja siirretään unionin ulkopuolelle. Tietosuoja-asetuksen 44 artiklalla, jonka otsikkona on ”Siirtoja koskeva yleinen periaate”, aloitetaan siirtoja kolmansiin maihin koskeva V luku säätämällä, että kaikkia tämän luvun säännöksiä on sovellettava, jotta varmistetaan, että tietosuoja-asetuksella taattua suojan tasoa ei vaaranneta siirrettäessä tietoja kolmanteen valtioon.[44] Tällä säännöllä pyritään estämään se, että unionin oikeuteen perustuvaa suojan tasoa kierrettäisiin siirtämällä henkilötietoja kolmanteen maahan niiden siellä käsittelyä varten.[45] Tämän tavoitteen kannalta on merkityksetöntä, perustuuko siirto tietosuojan riittävyyttä koskevaan päätökseen vai rekisterinpitäjän erityisesti sopimuslausekkeiden perusteella tarjoamiin takeisiin. Perusoikeuskirjassa taattujen perusoikeuksien suojaa koskevat vaatimukset ovat samoja riippumatta siitä, mihin oikeusperustaan tietty siirto perustuu.[46]

118. Sen sijaan tapa, jolla korkeatasoisen suojan jatkuvuus varmistetaan, eroaa siirron oikeusperustan mukaan.

119. Tietosuojan riittävyyttä koskevan päätöksen tarkoituksena on todeta, että sen kohteena oleva kolmas maa varmistaa itse suojan tason, joka pääosiltaan vastaa tasoa, joka unionissa on saavutettava. Tietosuojan riittävyyttä koskevan päätöksen antaminen edellyttää, että komissio arvioi ennakolta tietyn kolmannen maan oikeudessa taatun suojan tasoa ja tämän kolmannen maan käytäntöjä tietosuoja-asetuksen 45 artiklan 3 kohdassa tarkoitettujen tekijöiden valossa. Tällöin henkilötietoja voidaan siirtää kyseiseen kolmanteen maahan ilman, että rekisterinpitäjän olisi hankittava erityinen lupa.

120. Kuten seuraavassa osassa selostetaan yksityiskohtaisemmin, rekisterinpitäjän toteuttamilla asianmukaisilla suojatoimilla pyritään varmistamaan korkeatasoinen suoja tilanteessa, jossa kohdemaana olevan kolmannen maan suojatoimet ovat puutteelliset. Vaikka tietosuoja-asetuksen 46 artiklan 1 kohdan mukaan henkilötietoja voidaan siirtää kolmanteen valtioon, joka ei takaa riittävää

43 Direktiivin 95/46 26 artiklan 2 kohdassa säädettiin, että jäsenvaltio voi hyväksyä tällaisen siirron, ”jos rekisterinpitäjä antaa *riittävät takeet* henkilöiden yksityisyyden suojasta ja perusoikeuksien ja -vapauksien suojasta sekä vastaavien oikeuksien soveltamisesta (kursivointi tässä). Tässä säännöksessä tarkoitettu riittävien takeiden käsite ja tietosuoja-asetuksen 46 artiklan 1 kohdassa tarkoitettu asianmukaisten suojatoimien käsite ovat mielestäni samansisältöisiä.

44 Tietosuoja-asetuksen johdanto-osan kuudennessa perustelukappaleessa todetaan tältä osin, että tietojen ”korkeatasoinen suoja” on varmistettava sekä unionissa että siirrettäessä tietoja sen ulkopuolelle. Ks. myös tietosuoja-asetuksen johdanto-osan 101 perustelukappale.

45 Ks. tuomio Schrems (73 kohta) ja lausunto 1/15 (214 kohta).

46 Tämä ei kuitenkaan rajoita mahdollisuutta siirtää henkilötietoja silloinkin, jos asianmukaisia suojatoimia ei ole toteutettu, tietosuoja-asetuksen 49 artiklan 1 kohdassa säädetyillä poikkeusperusteilla.

tietosuojan tasoa, tässä säännöksessä sallitaan tällaiset siirrot vain, jos asianmukaiset suojatoimet toteutetaan muilla keinoilla. Komission hyväksymät mallisopimuslausekkeet merkitsevät tältä osin yleistä mekanismia, joka on sovellettavissa siirtoihin kohdemaana olevasta kolmannesta maasta ja siellä varmistetusta tietosuojan tasosta riippumatta.

E Päätöksen 2010/87 pätevyys perusoikeuskirjan 7, 8 ja 47 artiklan kannalta (seitsemäs, kahdeksas ja yhdestoista kysymys)

121. Seitsemännellä kysymyksellään ennakkoratkaisua pyytänyt tuomioistuin kysyy lähinnä, onko päätös 2010/87 pätemätön sen vuoksi, että se ei sido sellaisten kolmansien valtioiden viranomaisia, joihin tietoja siirretään tämän päätöksen liitteeseen sisältyvien mallisopimuslausekkeiden nojalla, ja erityisesti sen vuoksi, että se ei estä niitä vaatimasta, että tietojen tuoja saattaa nämä tiedot niiden saataville. Tällä kysymyksellä saatetaan siten kyseenalaiseksi jo itse mahdollisuus varmistaa tällaisten tietojen riittävä suoja yksinomaan sopimukseen perustuvilla mekanismeilla. Yhdestoista kysymys koskee yleisemmin päätöksen 2010/87 pätevyyttä perusoikeuskirjan 7, 8 ja 47 artiklan kannalta.

122. Kahdeksannella kysymyksellä unionin tuomioistuinta pyydetään ratkaisemaan, onko valvontaviranomaisen käytettävä tietosuoja-asetuksen 58 artiklan 2 kohdan f ja j alakohdassa sille annettuja toimivaltuuksia keskeyttääkseen päätöksen 2010/87 mukaisiin mallisopimuslausekkeisiin perustuvan tietojensiirron kolmanteen maahan, jos se katsoo, että tietojen tuojalle asetetaan siellä velvoitteita, jotka estävät sitä noudattamasta näitä lausekkeita ja joiden seurauksena siirrettyjen tietojen asianmukaista suojaa ei varmisteta. Koska tähän kysymykseen annettavalla vastauksella on nähdäkseni vaikutusta päätöksen 2010/87 pätevyyteen,[47] käsittelen sitä yhdessä seitsemännen ja yhdennentoista kysymyksen kanssa.

123. Tietosuoja-asetuksen 46 artiklan 1 kohdan sanamuodossa, siltä osin kuin siinä säädetään, että ” *jollei 45 artiklan 3 kohdan mukaista päätöstä ole tehty*, rekisterinpitäjä tai henkilötietojen käsittelijä voi siirtää henkilötietoja kolmanteen maahan – – vain, jos kyseinen rekisterinpitäjä tai henkilötietojen käsittelijä *on toteuttanut* asianmukaiset suojatoimet – –” (kursivointi tässä), tuodaan esille päätöksessä 2010/87 säädetyn kaltaisten sopimusmekanismien taustalla oleva logiikka. Kuten tietosuoja-asetuksen johdanto-osan 108 ja 114 perustelukappaleessa korostetaan, näiden mekanismien tarkoituksena on mahdollistaa siirrot kolmansiin maihin, joiden osalta komissio ei ole antanut tietosuojan riittävyyttä koskevaa päätöstä, jolloin mahdolliset puutteet kyseisen kolmannen maan oikeusjärjestyksessä varmistetussa tietosuojassa *kompensoidaan* suojatoimilla, joita tietojen viejä ja tietojen tuoja sitoutuvat sopimusteitse noudattamaan.

124. Koska sopimukseen perustuvien suojatoimien tarkoituksena itsessään on juuri korjata mahdolliset puutteellisuudet kohdemaana olevien kolmansien maiden – olivatpa ne mitä maita tahansa – tarjoamassa suojassa, päätöksen, jolla komissio toteaa tiettyjen mallisopimuslausekkeiden korjaavan asianmukaisesti nämä puutteellisuudet, pätevyys ei voi riippua suojan tasosta kussakin nimenomaisessa kolmannessa maassa, johon tietoja voitaisiin siirtää. Tällaisen päätöksen pätevyys riippuu yksinomaan näissä lausekkeissa kohdemaana olevan kolmannen maan mahdollisen puutteellisen suojan kompensoimiseksi määrättyjen suojatoimien vakaudesta. Näiden suojatoimien tehokkuutta arvioitaessa on otettava huomioon myös tietosuoja-asetuksen 58 artiklan 2 kohtaan perustuvat valvontaviranomaisten valtuuksien muodostamat takeet.

47 Ks. tämän ratkaisuehdotuksen 128 kohta.

125. Kuten DPC, Schrems, BSA, Irlanti, Itävallan, Ranskan, Puolan ja Portugalin hallitukset ja komissio ovat tuoneet esille, mallisopimuslausekkeiden sisältämiä suojatoimia voidaan heikentää tai ne voidaan tehdä jopa merkityksettömiksi, jos kohdemaana olevan kolmannen maan oikeudessa tietojen tuojalle asetetaan näissä lausekkeissa edellytetyn vastaisia velvoitteita. Kohdemaana olevan kolmannen maan asiaa koskevat oikeussäännöt voivat siirron konkreettisista olosuhteista riippuen [48] tehdä näiden lausekkeiden mukaisten velvoitteiden täyttämisestä mahdotonta.

126. Tässä tilanteessa, kuten Schrems ja komissio korostavat, tietosuoja-asetuksen 46 artiklan 2 kohdan c alakohdassa säädetty sopimusmekanismi perustuu tietojen viejän ja toissijaisesti valvontaviranomaisten vastuuseen saattamiseen. Rekisterinpitäjän tai tämän jättäessä toimimatta valvontaviranomaisen on kunkin nimenomaisen siirron osalta *tapauskohtaisesti* tutkittava, onko kohdemaana olevan kolmannen maan oikeus esteenä mallisopimuslausekkeiden täytäntöönpanolle ja siten siirrettyjen tietojen asianmukaiselle suojalle, jolloin siirrot on kiellettävä tai keskeytettävä.

127. Nämä toteamukset huomioon ottaen katson, että se, että päätös 2010/87 ja siihen sisältyvät mallisopimuslausekkeet eivät sido kohdemaana olevan kolmannen maan viranomaisia, ei yksinään tee tästä päätöksestä pätemätöntä. Päätöksen 2010/87 yhteensopivuus perusoikeuskirjan 7, 8 ja 47 artiklan kanssa riippuu mielestäni siitä, onko käytettävissä riittävän vakaita mekanismeja, joilla voidaan varmistaa, että mallisopimuslausekkeisiin perustuvat siirrot keskeytetään tai kielletään, jos näitä lausekkeita rikotaan tai niiden noudattaminen on mahdotonta.

128. Tältä osin tietosuoja-asetuksen 46 artiklan 1 kohdassa säädetään, että asianmukaisiin suojatoimenpiteisiin perustuva siirto voi toteutua vain, ”jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja”. On tarkistettava, voidaanko päätöksen 2010/87 liitteeseen sisältyvillä suojatoimilla, joita valvontaviranomaisten valtuudet täydentävät, varmistaa tämän edellytyksen noudattaminen. Mielestäni näin on ainoastaan sillä edellytyksellä, että on asetettu *velvollisuus* – joka kohdistuu rekisterinpitäjiin (osa 1), ja jos nämä jättävät toimimatta, valvontaviranomaisiin (osa 2) – keskeyttää tai kieltää siirto, jos mallisopimuslausekkeista seuraavien velvoitteiden ja kohdemaana olevan kolmannen maan oikeudessa asetettujen velvollisuuksien välisen ristiriidan vuoksi näitä lausekkeita ei voida noudattaa.

1. Rekisterinpitäjien velvollisuudet

129. Päätöksen 2010/87 liitteeseen sisältyvät mallisopimuslausekkeet edellyttävät, että tilanteessa, jossa niissä määrätyt velvoitteet ovat ristiriidassa kohdemaana olevan kolmannen maan oikeuteen perustuvien määräysten kanssa, näihin lausekkeisiin ei vedota tähän kolmanteen maahan suuntautuvan siirron tueksi, tai jos siirto on jo aloitettu näiden lausekkeiden perusteella, tietojen viejälle ilmoitetaan tästä ristiriidasta, jolloin se voi keskeyttää siirron.

130. Lausekkeen 5 kohdan a mukaan tietojen tuoja sitoutuu käsittelemään siirrettyjä henkilötietoja ainoastaan tietojen viejän puolesta tämän antamien ohjeiden ja mallisopimuslausekkeiden mukaisesti. Jos tietojen tuoja ei voi noudattaa näitä lausekkeita, se ilmoittaa tästä viipymättä tietojen viejälle, jolloin tietojen viejällä on oikeus lykätä tietojen siirtoa ja/tai irtisanoa sopimus. [49]

48 Kuvitellaan esimerkiksi, että kolmannessa maassa televiestintäpalvelujen tarjoajat velvoitetaan antamaan viranomaisille pääsy siirrettyihin tietoihin ilman minkäänlaisia rajoituksia tai suojatoimia. Vaikka tällaiset palveluntarjoajat eivät kykenisi noudattamaan mallisopimuslausekkeita, yrityksiä, joille ei ole asetettu tällaista velvoitetta, ei estettäisi noudattamasta niitä.

49 Huomattakoon myös, että lausekkeen 5 kohdan d alakohdassa i tietojen tuoja vapautetaan velvollisuudestaan ilmoittaa tietojen viejälle kolmannen maan säännösten täytäntöönpanosta vastaavan viranomaisen oikeudellisesti sitovasta pyynnöstä luovuttaa tietoja, kun tämän kolmannen maan oikeus on esteenä tällaiselle ilmoitukselle. Tällaisessa tilanteessa tietojen viejällä ei ole mahdollisuutta keskeyttää siirtoa, jos tällä tietojen luovutuksella, josta se ei ole tietoinen, rikotaan mallisopimuslausekkeita. Tietojen tuoja on kuitenkin lausekkeen 5 kohdan a nojalla velvollinen tarvittaessa ilmoittamaan tietojen viejälle siitä, että se katsoo tämän kolmannen maan lainsäädännön estävän sitä täyttämästä sovittujen sopimuslausekkeiden mukaisia velvoitteitaan.

131. Lausekkeeseen 5 liittyvässä alaviitteessä 2 täsmennetään, että mallisopimuslausekkeita ei rikota, jos tietojen tuoja noudattaa kolmannessa maassa sovellettavia kansallisen lainsäädännön sisältämiä pakollisia vaatimuksia, kunhan nämä vaatimukset eivät mene pitemmälle kuin on tarpeen demokraattisessa yhteiskunnassa direktiivin 95/46 13 artiklan 1 kohdassa (jonka sisältö on olennaisilta osin toistettu tietosuoja-asetuksen 23 artiklan 1 kohdassa) lueteltujen etujen, kuten yleisen turvallisuuden ja valtion turvallisuuden, suojaamiseksi. Kääntäen näiden lausekkeiden noudattamatta jättämistä kohdemaana olevan kolmannen maan oikeuteen perustuvan sellaisen ristiriitaisen velvollisuuden noudattamiseksi, jolla ylitetään se, mikä on oikeasuhteista unionissa tunnustetun oikeutetun edun turvaamiseksi, pidetään kyseisten lausekkeiden rikkomisena.

132. Mielestäni – ja kuten Schrems ja komissio väittävät – lausekkeen 5 kohdan a ei voida tulkita tarkoittavan sitä, että siirron keskeyttäminen tai sopimuksen irtisanominen on vain valinnaista, jos tietojen tuoja ei kykene noudattamaan mallisopimuslausekkeita. Vaikka tässä lausekkeessa viitataan vain tällaiseen tietojen viejän oikeuteen, tämä sanamuoto on ymmärrettävä sen sopimuksen yhteydessä, johon se liittyy. Se, että tietojen viejällä on *kahdenvälisissä suhteissaan tietojen tuojan kanssa* oikeus keskeyttää siirto tai irtisanoa sopimus, jos viimeksi mainittu ei kykene noudattamaan sopimuslausekkeita, ei rajoita tietojen viejän velvollisuutta toimia tällä tavoin *tietosuoja-asetukseen perustuvien rekisteröityjen oikeuksien suojaamista koskevien vaatimusten perusteella*. Mikä tahansa muu tulkinta johtaisi päätöksen 2010/87 pätemättömyyteen, koska siihen sisältyvien mallisopimuslausekkeiden perusteella siirtoon ei voitaisi liittää ”asianmukaisia suojatoimia” tietosuoja-asetuksen 46 artiklan 1 kohdassa, luettuna perusoikeuskirjan määräysten valossa, vaaditulla tavalla. [50]

133. Lisäksi lausekkeen 5 kohdan b mukaan tietojen tuoja vakuuttaa, että sillä ei ole mitään syytä olettaa, että siihen sovellettava lainsäädäntö estäisi tietojen viejältä saatujen ohjeiden noudattamisen ja tietojen tuojalle sopimuksen mukaan kuuluvien velvoitteiden täyttämisen. Jos tätä lainsäädäntöä muutetaan ja muutoksella on todennäköisesti merkittävä haitallinen vaikutus mallisopimuslausekkeilla annettaviin takeisiin ja lausekkeiden mukaisiin velvoitteisiin, tietojen tuoja antaa muutoksen tiedoksi tietojen viejälle viipymättä, jolloin tietojen viejällä on oikeus lykätä tietojen siirtoa ja/tai irtisanoa sopimus. Lausekkeen 4 kohdan g mukaan tietojen viejän on toimitettava tietojen tuojalta saatu tieto toimivaltaisille valvontaviranomaisille, kun se päättää jatkaa siirtoa.

134. Pidän tarpeellisena esittää tässä joitakin täsmennyksiä siitä, millainen tutkimus sopimuspuolten on suoritettava selvittääkseen lausekkeeseen 5 liittyvän alaviitteen kannalta, merkitsevätkö kolmannen valtion oikeudessa tietojen tuojalle asetetut velvollisuudet mallisopimuslausekkeiden rikkomista, jolloin ne estävät siirtoon liittyvät asianmukaiset suojatoimet. Tämä kysymyksenasettelu on tuotu pääosin esille kuudennen ennakkoratkaisukysymyksen toisessa osassa.

135. Tällainen tutkimus edellyttää mielestäni sitä, että huomioon otetaan kaikki kuhunkin siirtoon liittyvät olosuhteet, joita voivat olla tietojen luonne ja niiden mahdollinen arkaluonteisuus, tietojen viejän ja/tai tuojan käyttöön ottamat mekanismit niiden turvallisuuden takaamiseksi, [51] kolmannen maan viranomaisten tietoihin kohdistaman käsittelyn luonne ja tarkoitukset, tämän käsittelyn toteuttamista koskevat yksityiskohdat sekä kyseisessä kolmannessa maassa asetetut rajoitukset ja toteutetut suojatoimet. Kyseisen kolmannen maan viranomaisten suorittamalle käsittelytoiminnalle ominaiset seikat ja sen oikeusjärjestyksessä sovellettavat suojatoimet voivat mielestäni olla tietosuoja-asetuksen 45 artiklan 2 kohdassa mainittujen seikkojen kanssa päällekkäisiä.

50 Oikeuskäytännöstä ilmenee, että täytäntöönpanopäätöksen säännöksiä on tulkittava perustoimen, jolla lainsäätäjä on hyväksynyt sen antamisen, säännösten mukaisesti (ks. vastaavasti mm. tuomio 26.7.2017, Tšekki v. komissio (C-696/15 P, EU:C:2017:595, 51 kohta); tuomio 17.5.2018, Evonik Degussa (C-229/17, EU:C:2018:323, 29 kohta) ja tuomio 20.6.2019, ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518, 112 kohta)). Lisäksi unionin tointa on tulkittava niin pitkälle kuin mahdollista tavalla, joka ei aseta sen pätevyyttä kyseenalaiseksi, ja kaiken primaarioikeuden sekä erityisesti perusoikeuskirjan määräysten mukaisesti (ks. mm. tuomio 14.5.2019, M ym. (Pakolaisaseman peruuttaminen) (C-391/16, C-77/17 ja C-78/17, EU:C:2019:403, 77 kohta oikeuskäytäntöviittauksineen)).

51 Tietosuoja-asetuksen johdanto-osan 109 perustelukappaleessa kannustetaan tietojen viejää ja tietojen tuojaa tarjoamaan lisäsuojaa tietosuojaa koskeviin vakiolausekkeisiin erityisesti sopimusteitse.

136. Päätöksen 2010/87 liitteeseen sisältyvillä mallisopimuslausekkeilla annetaan rekisteröidyille täytäntöönpanokelpoisia oikeuksia ja oikeussuojakeinoja tietojen viejää ja toissijaisesti tietojen tuojaa vastaan.

137. Lausekkeen 3, jonka otsikkona on ”Kolmatta osapuolta suojaava edunsaajalauseke”, kohdassa 1 annetaan rekisteröidylle oikeus nostaa tietojen viejää vastaan kanne muun muassa lausekkeen 5 kohdan a tai b rikkomisen tapauksessa. Lausekkeen 3 kohdan 2 mukaan silloin, jos tietojen viejä on tosiasiallisesti lakkautettu tai lakannut oikeudellisesti olemasta, rekisteröity voi panna lausekkeet täytäntöön tietojen tuojaa vastaan.

138. Lausekkeen 6 kohdassa 1 annetaan rekisteröidylle, jolle on koitunut vahinkoa lausekkeessa 3 tarkoitettujen velvoitteiden rikkomisesta, oikeus saada tietojen viejältä korvaus aiheutuneista vahingoista. Lausekkeen 7 kohdan 1 mukaan silloin, jos rekisteröity vetoaa kolmannen osapuolen etua suojaavaan oikeuteen ja/tai vaatii vahingonkorvausta, tietojen tuoja hyväksyy rekisteröidyn päätöksen joko saattaa riita käsiteltäväksi sovittelumenettelyssä, jossa on mukana riippumaton henkilö tai tarvittaessa valvontaviranomainen, tai saattaa riita sen jäsenvaltion tuomioistuinten ratkaistavaksi, johon tietojen viejä on sijoittautunut.

139. Päätöksen 2010/87 liitteeseen sisältyviin mallisopimuslausekkeisiin perustuvien oikeussuojakeinojen lisäksi rekisteröidyt, jotka katsovat näitä lausekkeita rikotun, voivat vaatia valvontaviranomaisia toteuttamaan korjaavia toimenpiteitä tietosuoja-asetuksen 58 artiklan 2 kohdan, johon päätöksen 2010/87 4 artiklassa viitataan,[52] nojalla.

2. Valvontaviranomaisten velvollisuudet

140. Seuraavista syistä katson Schremsin, Irlannin sekä Saksan, Itävallan, Belgian, Alankomaiden ja Portugalin hallitusten ja Euroopan tietosuojaneuvoston tavoin, että tietosuoja-asetuksen 58 artiklan 2 kohdassa velvoitetaan valvontaviranomaiset, jos ne katsovat asiaa huolellisesti tutkittuaan, että kolmanteen maahan siirretyt tiedot eivät saa asianmukaista suojaa sovittujen sopimuslausekkeiden noudattamatta jättämisen vuoksi, toteuttamaan riittävät toimenpiteet tämän lainvastaisuuden korjaamiseksi ja tarvittaessa määräämään siirron keskeyttämisestä.

141. Toisin kuin DPC väittää, on huomattava, ettei päätöksen 2010/87 yhdessäkään säännöksessä rajata poikkeustapauksiin tietosuoja-asetuksen 58 artiklan 2 kohdan f ja j alakohdan nojalla valvontaviranomaisille annettuja valtuuksia ”asettaa väliaikainen tai pysyvä rajoitus käsittelylle, mukaan lukien käsittelykielto” ja ”määrätä tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle”.

142. Päätöksen 2010/87 4 artiklan alkuperäisen version 1 kohdassa tosin rajattiin valvontaviranomaisten toimivaltuudet keskeyttää tai kieltää tietojen rajatylittävät siirrot tiettyihin tilanteisiin, joissa oli todettu, että sopimusehtoihin perustuvalla siirrolla oli todennäköisesti merkittävä haitallinen vaikutus rekisteröidyn suojaamiseksi tarkoitettuihin takeisiin. Tämän päätöksen, sellaisena kuin komissio sitä muutti vuonna 2016 noudattaakseen tuomiota Schrems,[53] 4 artiklassa kuitenkin vastedes ainoastaan viitataan näihin toimivaltuuksiin niitä mitenkään rajoittamatta. Joka tapauksessa on katsottava, että komission täytäntöönpanopäätöksellä, kuten päätöksellä 2010/87, ei voida pätevästi rajoittaa itse tietosuoja-asetuksella valvontaviranomaisille annettuja valtuuksia.[54]

52 Vaikka päätöksen 2010/87 4 artiklan 1 kohdassa viitataan direktiivin 95/46 28 artiklan 3 kohtaan, muistutan, että tietosuoja-asetuksen 94 artiklan 2 kohdan nojalla viittauksia tähän direktiiviin pidetään viittauksina tietosuoja-asetuksen vastaaviin säännöksiin.

53 Ks. päätöksen 2016/2297 johdanto-osan kuudes ja seitsemäs perustelukappale. Tuomion Schrems 101–104 kohdassa unionin tuomioistuin totesi pätemättömäksi safe harbor -päätöksen säännöksen, jolla direktiivin 95/46 28 artiklassa valvontaviranomaisille annetut valtuudet rajattiin ”poikkeustapauksiin”, koska komissiolla ei ollut toimivaltaa rajoittaa näitä valtuuksia.

54 Ks. tuomio Schrems (103 kohta).

143. Tätä johtopäätöstä ei voida kyseenalaistaa päätöksen 2010/87 johdanto-osan 11 perustelukappaleella, jossa todetaan, että valvontaviranomaiset voivat käyttää valtuuksiaan keskeyttää ja kieltää siirrot vain ”poikkeustapauksissa”. Tämä perustelukappale, joka oli jo tämän päätöksen alkuperäisessä versiossa, liittyi kyseisen päätöksen entisen 4 artiklan 1 kohtaan, jossa rajoitettiin valvontaviranomaisten valtuuksia. Kun päätöstä 2010/87 tarkistettiin päätöksellä 2016/2297, komissio ei poistanut tai muuttanut kyseistä perustelukappaletta mukauttaakseen sen uuden 4 artiklan sisältöön. Päätöksen 2016/2297 johdanto-osan viidennellä perustelukappaleella kuitenkin vahvistettiin valvontaviranomaisten valtuudet keskeyttää tai kieltää siirrot, joita ne pitävät unionin oikeuden vastaisina muun muassa sen vuoksi, että tietojen tuoja ei ole noudattanut mallisopimuslausekkeita. Siltä osin kuin päätöksen 2010/87 johdanto-osan 11 perustelukappale on nyt ristiriidassa päätöksen oikeudellisesti sitovan säännöksen sekä sanamuodon että tarkoituksen kanssa, sen on katsottava tulleen tarpeettomaksi. [55]

144. Toisin kuin DPC niin ikään väittää, tietosuoja-asetuksen 58 artiklan 2 kohdan f ja j alakohdassa säädettyjen keskeyttämistä ja kieltämistä koskevien valtuuksien käyttö ei ole pelkkä valvontaviranomaisten harkintavaltaan jätetty mahdollisuus. Tämä johtopäätös perustuu mielestäni tietosuoja-asetuksen 58 artiklan 2 kohdan tulkintaan tämän asetuksen muiden säännösten ja perusoikeuskirjan valossa sekä päätöksen 2010/87 systematiikkaan ja tavoitteisiin.

145. Erityisesti tietosuoja-asetuksen 58 artiklan 2 kohtaa on luettava perusoikeuskirjan 8 artiklan 3 kohdan ja SEUT 16 artiklan 2 kohdan valossa. Näiden määräysten mukaan riippumattomien viranomaisten on valvottava henkilötietojen suojaa koskevaan perusoikeuteen liittyvien vaatimusten noudattamista. Tämä myös tietosuoja-asetuksen 57 artiklan 1 kohdan a alakohdassa mainittu tehtävä valvoa henkilötietojen suojaa koskevien vaatimusten noudattamista merkitsee sitä, että valvontaviranomaisilla on velvollisuus toimia tavalla, jolla varmistetaan tämän asetuksen asianmukainen soveltaminen.

146. Valvontaviranomaisen on siten tutkittava kaikkea asianmukaista huolellisuutta noudattaen sellaisen henkilön tekemä kantelu, joka väittää henkilötietojaan siirretyn kolmanteen valtioon siirtoon sovellettavien mallisopimuslausekkeiden vastaisesti. [56] Tietosuoja-asetuksen 58 artiklan 1 kohdassa valvontaviranomaisille annetaan tässä tarkoituksessa merkittävät tutkintavaltuudet. [57]

147. Toimivaltaisen valvontaviranomaisen on myös reagoitava asianmukaisesti mahdollisiin rekisteröidyn oikeuksien loukkauksiin, jotka se toteaa tutkimuksensa perusteella. Tältä osin kullakin valvontaviranomaisella on tietosuoja-asetuksen 58 artiklan 2 kohdan nojalla laaja valikoima keinoja – tässä säännöksessä luetellut eri korjaavat toimivaltuudet – sille annetun tehtävän täyttämiseksi. [58]

148. Vaikka tehokkaimman keinon valinta kuuluu toimivaltaisen valvontaviranomaisen harkintavaltaan kyseessä olevan siirron kaikki olosuhteet huomioon ottaen, sen on suoritettava täysimääräisesti sille annettu valvontatehtävä. Tämän viranomaisen on tarvittaessa keskeytettävä siirto, jos se katsoo, että mallisopimuslausekkeita ei noudateta ja että siirrettyjen tietojen asianmukaista suojaa ei voida taata muilla keinoilla, jollei tietojen viejä ole itse lopettanut siirtoa.

55 Unionin säädöksen johdanto-osalla ei ole oikeudellisesti sitovaa merkitystä, eikä siihen voida vedota tämän säädöksen varsinaisista säännöksistä poikkeamiseksi. Ks. tuomio 19.11.1998, Nilsson ym. (C-162/97, EU:C:1998:554, 54 kohta); tuomio 12.5.2005, Meta Fackler (C-444/03, EU:C:2005:288, 25 kohta) ja tuomio 10.1.2006, IATA ja ELFAA (C-344/04, EU:C:2006:10, 76 kohta).

56 Ks. analogisesti tuomio Schrems (63 kohta).

57 Lisättäköön vielä, että päätöksen 2010/87 liitteessä olevan lausekkeen 8 kohdan 2 mukaan sopimuspuolet sopivat, että valvontaviranomaisella on oikeus tehdä tietojen tuojaan kohdistuvia tarkastuksia samoin edellytyksin kuin se voisi tehdä tietojen viejään kohdistuvia tarkastuksia sovellettavan lainsäädännön nojalla.

58 Ks. vastaavasti tuomio Schrems (43 kohta).

149. Tätä tulkintaa tukee tietosuoja-asetuksen 58 artiklan 4 kohta, jossa säädetään, että valvontaviranomaisille tämän artiklan nojalla annettujen valtuuksien käyttöön sovelletaan asianmukaisia suojatoimia, muun muassa tehokkaita oikeussuojakeinoja perusoikeuskirjan 47 artiklan mukaisesti. Tietosuoja-asetuksen 78 artiklan 1 ja 2 kohdassa tunnustetaan jokaisella henkilöllä oleva oikeus tehokkaisiin oikeussuojakeinoihin itseään koskevaa valvontaviranomaisen oikeudellisesti sitovaa päätöstä vastaan tai jos tämä viranomainen ei ole käsitellyt hänen valitustaan. [59]

150. Nämä säännökset merkitsevät, kuten Schrems, BSA, Irlanti, Puolan ja Yhdistyneen kuningaskunnan hallitukset ja komissio väittävät, ennen kaikkea, että päätös, jolla valvontaviranomainen pidättyy kieltämästä tai keskeyttämästä siirtoa kolmanteen maahan sellaisen henkilön pyynnöstä, joka vetoaa vaaraan siitä, että hänen tietojaan käsitellään siellä hänen perusoikeuksiensa vastaisesti, voi olla oikeussuojakeinon kohteena. Tällaisen oikeussuojakeinoa koskevan oikeuden tunnustaminen edellyttää, että valvontaviranomaisten toimivalta on sidottua eikä puhtaasti harkintavaltaa. Lisäksi Schrems ja komissio korostavat perustellusti, että tehokkaan tuomioistuinvalvonnan harjoittaminen edellyttää, että riitautetun toimen antanut viranomainen on perustellut toimen asianmukaisesti. [60] Tämä perusteluvelvollisuus ulottuu mielestäni valvontaviranomaisten päätökseen käyttää jotakin tietosuoja-asetuksen 58 artiklan 2 kohdassa niille annetuista valtuuksista.

151. On vielä kuitenkin vastattava DPC:n väitteisiin siitä, että vaikka valvontaviranomaisten olisi keskeytettävä tai kiellettävä siirto, kun rekisteröidyn oikeudet sitä edellyttävät, tällä ei kuitenkaan varmistettaisi päätöksen 2010/87 pätevyyttä.

152. DPC katsoo ensinnäkin, että tällainen velvollisuus ei korjaisi systeemisiä ongelmia, jotka koskevat asianmukaisten suojatoimien puuttumista Yhdysvaltojen kaltaisessa kolmannessa maassa. Valvontaviranomaisten valtuuksia voidaan käyttää vain tapauskohtaisesti, kun taas Yhdysvaltojen oikeudelle ominaiset puutteellisuudet ovat luonteeltaan yleisiä ja rakenteellisia. Tämän vuoksi on vaarana, että eri valvontaviranomaiset antavat toisistaan poikkeavia päätöksiä toisiinsa rinnastettavista siirroista.

153. Tältä osin en voi sivuuttaa käytännön vaikeuksia, jotka liittyvät lainsäädännölliseen ratkaisuun antaa valvontaviranomaisten vastuulle rekisteröityjen perusoikeuksien noudattamisen valvomisen erityisten siirtojen tai tietylle vastaajanottajalle suuntautuvien tiedonsiirtojen yhteydessä. Nämä vaikeudet eivät nähdäkseni kuitenkaan aiheuta päätöksen 2010/87 pätemättömyyttä.

154. Unionin oikeudessa ei mielestäni edellytetä kokonaisvaltaista ja ennalta ehkäisevää ratkaisua kaikille tiettyyn kolmanteen maahan suuntautuville siirroille, jotka voivat käsittää samat vaarat perusoikeuksien loukkaamisesta.

155. Lisäksi vaara eri valvontaviranomaisten noudattamien lähestymistapojen hajanaisuudesta liittyy lainsäätäjän haluamaan hajautettuun valvontarakenteeseen. [61] Kuten Saksan hallitus korostaa, tietosuoja-asetuksen VII luvussa, jonka otsikkona on ”Yhteistyö ja yhdenmukaisuus”, otetaan käyttöön mekanismit tämän vaaran välttämiseksi. Tämän asetuksen 60 artiklassa säädetään tietojen rajatylittävän käsittelyn tapauksessa osallistuvien valvontaviranomaisten ja rekisterinpitäjän toimipaikan

59 Tietosuoja-asetuksen johdanto-osan 141 perustelukappaleen mukaan jokaisella henkilöllä on oltava oikeus soveltaa tehokkaita oikeussuojakeinoja perusoikeuskirjan 47 artiklan mukaisesti, jos valvontaviranomainen ”ei ryhdy toimiin, jotka ovat tarpeen [tämän henkilön] oikeuksien suojaamiseksi”. Ks. myös tietosuoja-asetuksen johdanto-osan 129 ja 143 perustelukappale.

60 Ks. mm. tuomio 28.7.2011, Samba Diouf (C-69/10, EU:C:2011:524, 57 kohta) ja tuomio 17.11.2011, Gaydarov (C-430/10, EU:C:2011:749, 41 kohta).

61 Ks. tästä tuomio 5.6.2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, 69–73 kohta).

valvontaviranomaisen eli niin kutsutun johtavan valvontaviranomaisen [62] välisestä yhteistyömenettelystä. Eriävien näkemysten tapauksessa erimielisyydet ratkaistaan Euroopan tietosuojaneuvostossa. [63] Viimeksi mainitulla on myös toimivalta antaa valvontaviranomaisen pyynnöstä lausuntoja kysymyksistä, joilla on merkitystä useammassa kuin yhdessä jäsenvaltiossa. [64]

156. Toiseksi DPC vetoaa päätöksen 2010/87 pätemättömyyteen perusoikeuskirjan 47 artiklan kannalta sillä perusteella, että valvontaviranomaiset voivat suojata rekisteröityjen oikeuksia vain tulevaisuutta varten, eivätkä ne voi tarjota ratkaisua niille, joiden tiedot on jo siirretty. DPC tuo erityisesti esille, että tietosuoja-asetuksen 58 artiklan 2 kohdassa ei säädetä oikeudesta saada pääsy kolmannen maan viranomaisten keräämiin tietoihin tai oikeudesta näiden tietojen oikaisemiseen ja poistamiseen eikä myöskään mahdollisuudesta saada korvausta rekisteröidyille aiheutuneesta vahingosta.

157. Tarkasteltaessa väitettä, jonka mukaan oikeutta saada pääsy kerättyihin tietoihin ja oikeutta niiden oikaisemiseen ja poistamiseen ei ole, on todettava, että kun kohdemaana olevassa kolmannessa maassa ei ole tehokkaita oikeussuojakeinoja, unionissa säädetyillä oikeussuojakeinoilla rekisterinpitäjää vastaan ei voida saada tämän kolmannen maan viranomaisilta pääsyä näihin tietoihin tai saada niitä oikaisemaan tai poistamaan nämä tiedot.

158. Mielestäni tällä väitteellä ei kuitenkaan voida perustella päätöksen 2010/87 yhteensopimattomuutta perusoikeuskirjan 47 artiklan kanssa. Tämän päätöksen pätevyys ei nimittäin riipu suojan tasosta kussakin kolmannessa maassa, johon tietoja voitaisiin siirtää siihen sisältyvien mallisopimuslausekkeiden perusteella. Jos kohdemaana olevan kolmannen valtion lainsäädäntö estää tietojen tuojaa noudattamasta näitä lausekkeita siten, että tätä edellytetään antamaan viranomaisille tietoihin pääsyn, johon ei liity asianmukaisia oikeussuojakeinoja, valvontaviranomaisten on toteutettava korjaavia toimenpiteitä, jollei tietojen viejä ole keskeyttänyt siirtoa päätöksen 2010/87 liitteessä olevan lausekkeen 5 kohdan a tai b nojalla.

159. Kuten Schrems korostaa, henkilöillä, joiden oikeuksia on loukattu, on nyt tietosuoja-asetuksen 82 artiklan nojalla oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus tämän asetuksen rikkomisesta aiheutuneesta aineellisesta tai aineettomasta vahingosta. [65]

160. Kuten kaikista näistä perusteluista ilmenee, tarkastelussani ei ole tullut esiin seikkoja, jotka vaikuttaisivat päätöksen 2010/87 pätevyyteen perusoikeuskirjan 7, 8 ja 47 artiklan kannalta.

F Asiassa ei ole tarpeen vastata muihin ennakkoratkaisukysymyksiin eikä tutkia Privacy Shield -päätöksen pätevyyttä

161. Tässä osassa esitän syyt, jotka liittyvät pääasiallisesti siihen, että pääasian kohde on rajattu päätöksen 2010/87 pätevyyteen, ja joiden vuoksi katson, ettei asiassa ole syytä vastata toiseen, kolmanteen, neljänteen, viidenteen, yhdeksänteen ja kymmenenteen ennakkoratkaisukysymykseen eikä ottaa kantaa Privacy Shield -päätöksen pätevyyteen.

62 Ks. tietosuoja-asetuksen 56 artiklan 1 kohta. Tämän asetuksen 61 artiklan mukaan valvontaviranomaisten on annettava toisilleen keskinäistä apua. Kyseisen asetuksen 62 artiklassa niille annetaan oikeus toteuttaa yhteisiä operaatioita.

63 Ks. tietosuoja-asetuksen 65 artikla.

64 Ks. tietosuoja-asetuksen 64 artiklan 2 kohta.

65 Tietosuoja-asetuksen 83 artiklan 5 kohdan c alakohdassa säädetään myös rekisterinpitäjän maksettavaksi tulevista hallinnollisista sakoista tapauksissa, joissa tämän asetuksen 44–49 kohtaa rikotaan.

162. Toinen ennakkoratkaisukysymys koskee niiden suojan tasoa koskevien vaatimusten määrittämistä, joita kolmannen maan on noudatettava, jotta sinne voidaan siirtää laillisesti tietoja mallisopimuslausekkeiden perusteella, kun tämän kolmannen maan viranomaiset voivat käsitellä näitä tietoja niiden siirtämisen jälkeen kansallista turvallisuutta varten. Unionin tuomioistuimelle esitetyn kolmannen kysymyksen tarkoituksena on määrittää kohdemaana olevassa kolmannessa valtiossa sovellettavalle suojajärjestelmälle ominaiset seikat, jotka on otettava huomioon sen selvittämiseksi, noudattaako se näitä vaatimuksia.

163. Neljännellä, viidennellä ja kymmenennellä kysymyksellään ennakkoratkaisua pyytänyt tuomioistuin pyrkii lähinnä selvittämään, kun otetaan huomioon sen toteamat Yhdysvaltojen oikeutta koskevat tosiseikat, onko siinä säädetty asianmukaisista suojatoimista sitä vastaan, että Yhdysvaltojen tiedusteluviranomaiset puuttuvat yksityisyyden suojaa, henkilötietojen suojaa ja tehokasta oikeussuojaa koskevien perusoikeuksien käyttöön.

164. Yhdeksäs ennakkoratkaisukysymys koskee – sen tutkimuksen yhteydessä, jolla valvontaviranomainen tarkistaa, liittyykö päätökseen 2010/87 sisältyviin mallisopimuslausekkeisiin perustuvaan siirtoon Yhdysvaltoihin asianmukaisia suojatoimia – sen seikan vaikutusta, että komissio on Privacy Shield -päätöksessä todennut, että Yhdysvallat varmistaa rekisteröityjen perusoikeuksien riittävän suojan tällaista puuttumista vastaan.

165. Ennakkoratkaisua pyytänyt tuomioistuin ei puolestaan ole nimenomaisesti esittänyt kysymystä Privacy Shield -päätöksen pätevyydestä, vaikka, kuten jäljempänä selitetään,[66] neljännessä, viidennessä ja kymmenennessä ennakkoratkaisukysymyksessä saatetaan välillisesti kyseenalaiseksi tietosuojan riittävyyttä koskeva toteamus, jonka komissio on tässä päätöksessä tehnyt.

166. Edellä esitystä tarkastelusta ilmenevien seikkojen vuoksi mielestäni unionin tuomioistuimen näihin kysymyksiin antama selvennys ei vaikuttaisi sen johtopäätökseen siitä, onko päätös 2010/87 abstraktilla tasolla pätevä, eikä siten vaikuttaisi pääasian ratkaisuun (osa 1). Vaikka unionin tuomioistuimen vastauksilla voisi myöhemmässä vaiheessa olla hyötyä DPC:lle, jotta se voi selvittää tämän riidan taustalla olevassa menettelyssä, onko kyseessä olevat siirrot konkreettisesti keskeytettävä asianmukaisten suojatoimien väitetyn puuttumisen vuoksi, nähdäkseni olisi ennenaikaista käsitellä niitä tämän asian yhteydessä (osa 2).

1. Unionin tuomioistuimen vastaukset eivät ole tarpeen pääasian kohteen kannalta

167. On syytä palauttaa mieleen, että pääasia on tullut vireille DPC:n käytettyä oikeussuojakeinoa, joka kuvataan tuomion Schrems 65 kohdassa, jonka mukaan kunkin jäsenvaltion on annettava valvontaviranomaiselle oikeus pyytää, jos se pitää sitä tarpeellisena käsiteltäväkseen saatetun kantelun käsittelemiseksi, kansallista tuomioistuinta esittämään unionin tuomioistuimelle ennakkoratkaisukysymys, joka koskee tietosuojan riittävyyttä koskevan päätöksen tai analogisesti mallisopimuslausekkeita koskevan päätöksen pätevyyttä.

168. Tältä osin High Court on korostanut, että DPC:n saatettua asian sen käsiteltäväksi sen ainoina vaihtoehtoina oli joko esittää DPC:n pyytämä ennakkoratkaisupyyntö päätöksen 2010/87 pätevyydestä siinä tapauksessa, että se DPC:n tavoin epäilisi tämän päätöksen pätevyyttä, tai päinvastaisessa tapauksessa kieltäytyä tämän pyynnön esittämisestä. Kyseinen tuomioistuin katsoo, että jos se olisi päätynyt tähän jälkimmäiseen vaihtoehtoon, sen olisi pitänyt lopettaa asian käsittely, koska DPC:n hakemuksella ei ollut muuta kohdetta.[67]

66 Ks. tämän ratkaisuehdotuksen 175 kohta.

67 High Courtin 3.10.2017 antama tuomio (337 kohta).

169. Samansuuntaisesti Supreme Court, johon Facebook Ireland valitti ennakkoratkaisupyynnön esittämistä koskevasta päätöksestä, kuvasi pääasiaa vahvistamismenettelyksi, jolla DPC vaati ennakkoratkaisua pyytänyttä tuomioistuinta esittämään unionin tuomioistuimelle ennakkoratkaisukysymyksen päätöksen 2010/87 pätevyydestä. Irlannin ylimmän tuomioistuimen mukaan ainoa aineellinen kysymys, joka on tuotu esille ennakkoratkaisua pyytäneessä tuomioistuimessa ja unionin tuomioistuimessa, koskee siten tämän päätöksen pätevyyttä. [68]

170. Kun otetaan huomioon näin rajattu pääasian kohde, ennakkoratkaisua pyytänyt tuomioistuin on esittänyt unionin tuomioistuimelle kymmenen ensimmäistä ennakkoratkaisukysymystään siltä osin kuin se katsoo niiden tarkastelun liittyvän kokonaisarviointiin, joka on tarpeen, jotta unionin tuomioistuin voi vastauksena 11. kysymykseen ottaa kantaa päätöksen 2010/87 pätevyyteen perusoikeuskirjan 7, 8 ja 47 artiklan kannalta. Tämä kysymys on ennakkoratkaisupyynnön mukaan looginen seuraus sitä edeltävistä kysymyksistä.

171. Tämän vuoksi toisen, kolmannen, neljännen, viidennen, yhdeksännen ja kymmenennen kysymyksen taustalla näyttää olevan olettama, jonka mukaan päätöksen 2010/87 pätevyys riippuisi perusoikeuksien suojan tasosta kussakin kolmannessa maassa, johon tietoja voidaan siirtää siihen sisältyvien mallisopimuslausekkeiden perusteella. Kuten seitsemättä kysymystä koskevasta tarkastelustani ilmenee, [69] tämä olettama on mielestäni virheellinen. Kohdemaana olevan kolmannen maan oikeutta on tutkittava vain, jos komissio antaa tietosuojan riittävyyttä koskevan päätöksen tai jos rekisterinpitäjä – tai sen jättäessä toimimatta toimivaltainen valvontaviranomainen – tarkistaa, että tietosuoja-asetuksen 46 artiklan 1 kohdassa tarkoitettuihin asianmukaisiin suojatoimiin perustuvan siirron yhteydessä tämän kolmannen maan oikeudessa tietojen tuojalle asetetut velvollisuudet eivät vaaranna näillä suojatoimilla varmistetun suojan tehokkuutta.

172. Unionin tuomioistuimen vastaukset edellä mainittuihin kysymyksiin eivät näin ollen voi vaikuttaa sen johtopäätökseen 11. kysymyksestä. [70] Niihin ei siten ole syytä vastata pääasian kohteen kannalta.

173. Ehdotan, että unionin tuomioistuin rajoittaa esillä olevan asian käsittelyn tämän riidan kohteeseen. Unionin tuomioistuimen ei mielestäni pitäisi mennä pidemmälle kuin kyseisen riidan ratkaisu edellyttää ja käsitellä ennakkoratkaisukysymyksiä taustalla olevan DPC:n vireillä olevan menettelyn kannalta. Kuten jäljempänä selitetään, tämä kehotus pidättyvyyteen johtuu tarpeesta varmistaa, ettei asiassa tehdä tyhjäksi sen menettelyn normaalia kulkua, jota DPC:n on määrä jatkaa unionin tuomioistuimen otettua kantaa päätöksen 2010/87 pätevyyteen. Toisaalta asian tosiseikkojen perusteella unionin tuomioistuimen olisi nähdäkseni hieman ennenaikaista, myös tämän menettelyn tarkoituksen kannalta, tutkia kysymyksenasetteluja, jotka on tuotu esille toisessa, kolmannessa, neljännessä, viidennessä, yhdeksännessä ja kymmenennessä kysymyksessä.

68 Supreme Courtin 31.5.2019 antaman tuomion (2.7 kohta) mukaan ”[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]”. Kyseisen tuomion 2.9 kohdassa todetaan tämän jälkeen seuraavaa: ”Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*” (kursivointi tässä).

69 Ks. tämän ratkaisuehdotuksen 124 kohta.

70 Samasta syystä Supreme Court katsoi 31.5.2019 antamassaan tuomiossa (8.1–8.5 kohta), että sillä ei ole toimivaltaa kyseenalaistaa ennakkoratkaisua pyytäneen tuomioistuimen päätöstä ennakkoratkaisukysymysten esittämisestä unionin tuomioistuimelle ja muuttaa niiden sanamuotoa, ja samalla ilmaisi epäilevänsä, olivatko tietyt näistä kysymyksistä tarpeellisia. Erityisesti kyseisen tuomion 8.5 kohdassa todetaan seuraavaa: ”The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures – –.”

2. Syyt, jotka puoltavat sitä, ettei unionin tuomioistuin tutki asiaa DPC:n vireillä olevan menettelyn kohteen kannalta

174. DPC:lle tekemässään kantelussa Schrems vaatii tätä valvontaviranomaista käyttämään tietosuoja-asetuksen 58 artiklan 2 kohdan f alakohdan mukaisia toimivaltuuksiaan ja määräämään, että Facebook Ireland keskeyttää hänen henkilötietojensa siirtämisen mallisopimuslausekkeiden perusteella Yhdysvaltoihin. Schrems vetoaa tämän vaatimuksensa tueksi lähinnä siihen, että nämä sopimukseen perustuvat suojatoimet eivät ole asianmukaisia siihen nähden, miten Yhdysvaltojen tiedustelupalvelujen toiminnalla puututaan hänen perusoikeuksiensa käyttämiseen.

175. Schremsin esittämillä perusteluilla kyseenalaistetaan komission Privacy Shield -päätöksessä esittämä toteamus, jonka mukaan Yhdysvallat takaa tietosuojan riittävän tason tiedoille, jotka siirretään tämän päätöksen nojalla, kun otetaan huomioon Yhdysvaltojen tiedusteluviranomaisten näihin tietoihin pääsylle ja niiden käytölle asetetut rajoitukset ja rekisteröityjen oikeussuoja.[71] Myös huolenaiheet, jotka alustavasti DPC[72] sekä ennakkoratkaisua pyytänyt tuomioistuin neljännessä, viidennessä ja kymmenennessä kysymyksessään ovat tuoneet esille, herättävät välillisesti epäilyjä tämän toteamuksen perusteltavuudesta.

176. On selvää, että Privacy Shield -päätöksessä rajoitutaan toteamaan niiden henkilötietojen suojan riittävyys, jotka on siirretty siinä todettujen periaatteiden mukaisesti Yhdysvaltoihin sijoittautuneelle yritykselle, joka on antanut oman varmennuksen näiden periaatteiden noudattamisesta.[73] Tässä päätöksessä esitetyt perustelut ylittävät kuitenkin päätöksen soveltamisalaan kuuluvien siirtojen asiayhteyden, koska ne koskevat tässä kolmannessa maassa voimassa olevaa oikeutta ja käytäntöjä, jotka liittyvät siirrettyjen tietojen käsittelyyn kansallista turvallisuutta varten. Kuten Facebook Ireland, Schrems, Yhdysvaltojen hallitus ja komissio ovat huomauttaneet, Yhdysvaltojen tiedusteluviranomaisten harjoittamaa tarkkailua toteutetaan ja takeita siihen liittyvän väärinkäytön vaaroja vastaan ja mekanismeja näiden takeiden noudattamisen valvomiseksi sovelletaan riippumatta siitä, mihin oikeusperustaan siirron tueksi vedotaan unionin oikeuden kannalta.

177. Tässä mielessä kysymys siitä, sitovatko Privacy Shield -päätöksessä tältä osin esitetyt toteamukset valvontaviranomaisia, kun ne tutkivat mallisopimuslausekkeiden perusteella toteutetun siirron laillisuutta, voisi olla merkityksellinen DPC:n käsitellessä Schremsin kantelua. Jos tähän kysymykseen vastattaisiin myöntävästi, olisi vielä pohdittava, onko tämä päätös pätevä.

178. Mielestäni unionin tuomioistuimen ei kuitenkaan pidä ottaa kantaa näihin kysymyksiin pelkästään siinä tarkoituksessa, että se auttaisi DPC:tä tämän kantelun käsittelyssä, sillä niihin ei ole vastattava, jotta ennakkoratkaisua pyytänyt tuomioistuin voisi ratkaista pääasian. Koska SEUT 267 artiklassa määrätyssä menettelyssä on kyse tuomioistuinten välisestä vuoropuhelusta, unionin tuomioistuimen ei ole esitettävä asiaan selvennystä ainoastaan siinä tarkoituksessa, että autetaan hallintoviranomaista tämän riidan taustalla olevassa menettelyssä.

71 Ks. Privacy Shield -päätöksen johdanto-osan 64–141 perustelukappale. On syytä muistaa, että kuten tämän päätöksen 1 artiklan 2 kohdasta ilmenee, Privacy Shield -järjestely muodostuu paitsi periaatteista, joita yritysten, jotka haluavat siirtää tietoja tämän päätöksen perusteella, on noudatettava, myös virallisista lausumista ja sitoumuksista, jotka on saatu Yhdysvaltojen hallitukselta ja jotka sisältyvät päätökseen liitettyihin asiakirjoihin.

72 DPC:n päätösluonnos on tehty ennen Privacy Shield -päätöksen antamista. Kuten DPC täsmentää tässä luonnoksessa, vaikka alustavan toteamuksen mukaan Yhdysvaltojen oikeudessa annetuilla takeilla ei voitu ainakaan varmistaa tähän kolmanteen maahan suuntautuvien siirtojen yhdenmukaisuutta perusoikeuskirjan 47 artiklan kanssa, *hän ei tässä vaiheessa tutkinut tai ottanut huomioon Privacy Shield -päätöksen luonnoksessa suunniteltuja uusia järjestelyjä, koska sitä ei ollut vielä annettu*. High Court totesi kuitenkin 3.10.2017 antamansa tuomion 307 kohdassa seuraavaa: ”It is fair to conclude – – that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U.S.], conflicts with the case made by the DPC to this court.”

73 Ks. Privacy Shield -päätöksen 1 artiklan 1 ja 3 kohta ja johdanto-osan 14–16 perustelukappale.

179. Tämä varaus on mielestäni esitettävä sitäkin suuremmalla syyllä, että unionin tuomioistuimelle ei ole nimenomaisesti esitetty kysymystä Privacy Shield -päätöksen pätevyydestä; tästä päätöksestä on sitä paitsi jo nostettu kumoamiskanne unionin yleisessä tuomioistuimessa vireillä olevassa asiassa.[74]

180. Lisäksi jos unionin tuomioistuin ottaisi kantaa edellä kuvattuihin kysymyksiin, se mielestäni häiritsisi sen menettelyn normaalia kulkua, jonka on määrä jatkua sen annettua tuomionsa esillä olevassa asiassa. Tässä menettelyssä DPC:n on käsiteltävä Schremsin kantelu, jolloin huomioon on otettava unionin tuomioistuimen 11. kysymykseen antama vastaus. Jos unionin tuomioistuin toteaa, kuten ehdotan ja toisin kuin DPC on unionin tuomioistuimessa väittänyt, että päätös 2010/87 ei ole pätemätön perusoikeuskirjan 7, 8 ja 47 artiklan kannalta, DPC:n pitäisi nähdäkseni hyväksyä mahdollisuus käsitellä uudelleen DPC:ssä vireillä olevan menettelyn asiakirjat. Jos DPC katsoisi, ettei hänellä ole edellytyksiä käsitellä Schremsin kantelua ilman unionin tuomioistuimen ensin antamaa ratkaisua siitä, onko Privacy Shield -päätös esteenä hänen kyseisen siirron keskeyttämistä koskevien valtuuksiensa käyttämiselle, ja vahvistaisi epäilynsä tämän päätöksen pätevyydestä, hän voisi saattaa asian uudelleen kansallisten tuomioistuinten käsiteltäväksi, jotta nämä esittäisivät tästä unionin tuomioistuimelle kysymyksiä.[75]

181. Tällöin alkaisi menettely, jossa kaikki Euroopan unionin tuomioistuimen perussäännön 23 artiklan toisessa kohdassa tarkoitetut asianosaiset ja osapuolet voisivat esittää unionin tuomioistuimessa huomautuksia erityisesti Privacy Shield -päätöksen pätevyydestä ja tarvittaessa ilmoittaa, mitkä erityiset arvioinnit ne riitauttavat, ja syyt, joiden vuoksi ne katsovat komission tällä päätöksellä ylittäneen rajoitetun harkintavaltansa.[76] Tällaisen menettelyn yhteydessä komissiolla olisi mahdollisuus vastata nimenomaisesti ja yksityiskohtaisesti kuhunkin kyseistä päätöstä vastaan esitettyyn mahdolliseen kritiikkiin. Vaikka nyt esillä olevassa asiassa asianosaisilla ja osapuolilla, jotka ovat esittäneet huomautuksia unionin tuomioistuimessa, on ollut tilaisuus käsitellä joitakin merkityksellisiä näkökohtia arvioitaessa Privacy Shield -päätöksen yhdenmukaisuutta perusoikeuskirjan 7, 8 ja 47 artiklan kanssa, tämä kysymys ansaitsee merkityksensä vuoksi tulla käsitellyksi kattavasti ja perusteellisesti.

182. Mielestäni varovaisuus edellyttää, että nämä menettelyvaiheet on käyty läpi ennen kuin unionin tuomioistuin tarkastelee Privacy Shield -päätöksen vaikutusta siihen, miten valvontaviranomainen käsittelee tietosuoja-asetuksen 46 artiklan 1 kohtaan perustuvan Yhdysvaltoihin suuntautuvan siirron keskeyttämistä koskevan vaatimuksen, ja ottaa kantaa tämän päätöksen pätevyyteen.

183. Näin on sitä suuremmalla syyllä sen vuoksi, että unionin tuomioistuimen käsiteltäväksi saatetun asiakirja-aineiston perusteella ei voida katsoa, että se, miten DPC käsittelee Schremsin kantelua, riippuu välttämättä siitä, onko Privacy Shield -päätös esteenä sille, että valvontaviranomaiset käyttävät valtuuttaan keskeyttää mallisopimuslausekkeisiin perustuva siirto.

184. Tältä osin ei ole poissuljettua, että DPC päätyy keskeyttämään siirron muilla perusteilla kuin niillä, joiden mukaan Yhdysvallat ei väitetysti takaa riittävää suojaa Yhdysvaltojen tiedustelupalvelujen toimintaan perustuvilta rekisteröityjen perusoikeuksien loukkauksilta. Ennakkoratkaisua pyytänyt tuomioistuin täsmentää erityisesti, että Schrems väittää DPC:lle tekemässään kantelussa, että sopimuslausekkeet, joihin Facebook Ireland vetoaa tämän siirron tueksi, eivät vastaa täysin päätöksen 2010/87 liitteessä olevia sopimuslausekkeita. Schrems väittää lisäksi, että kyseinen siirto ei kuulu tämän päätöksen vaan pikemminkin muiden mallisopimuslausekkeita koskevien päätösten soveltamisalaan.[77]

74 Vireillä oleva asia T-738/16, La Quadrature du Net ym. v. komissio (EUVL 2017, C 6, s. 39).

75 Huomattakoon, että kirjallisissa huomautuksissaan DPC ei ole ottanut kantaa siihen, miten Privacy Shield -päätös vaikuttaa hänelle tehdyn kantelun käsittelyyn.

76 Ks. tältä osin tuomio Schrems (78 kohta).

77 Schrems väittää tämän kantansa tueksi, että Facebook Inc. on katsottava paitsi henkilötietojen käsittelijäksi, myös tietosuoja-asetuksen 4 artiklan 7 alakohdassa tarkoitetuksi ”rekisterinpitäjäksi” siltä osin kuin kyse on Facebook-verkkoyhteisöpalvelun käyttäjien henkilötietojen käsittelystä. Ks. tältä osin tuomio 5.6.2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, 30 kohta).

185. DPC ja ennakkoratkaisua pyytänyt tuomioistuin korostavat myös, että Facebook Ireland ei ole Schremsin kantelussa tarkoitetun siirron tueksi vedonnut Privacy Shield -päätökseen,[78] minkä tämä yhtiö vahvisti istunnossa. Vaikka Facebook Inc. on antanut oman varmennuksen Privacy Shield -periaatteiden noudattamisesta 30.9.2016 lähtien,[79] Facebook Ireland väittää, että tämä periaatteiden noudattaminen koskee vain joidenkin tietoryhmien eli Facebook Inc:n kauppakumppaneita koskevien tietojen siirtoa. Mielestäni unionin tuomioistuimen ei olisi asianmukaista ennakoida kysymyksiä, jotka voisivat tulla tältä osin esille, ja oletettaessa, että Facebook Ireland ei voisi vedota päätökseen 2010/87 kyseisen siirron tueksi, tutkia, kuuluisiko tämä siirto kuitenkin Privacy Shield -päätöksen soveltamisalaan, vaikka viimeksi mainittu yhtiö ei ole esittänyt tällaista väitettä ennakkoratkaisua pyytäneessä tuomioistuimessa tai DPC:lle.

186. Päättelen tästä, että asiassa ei ole syytä vastata toiseen, kolmanteen, neljänteen, viidenteen, yhdeksänteen ja kymmenenteen ennakkoratkaisukysymykseen eikä tutkia Privacy Shield -päätöksen pätevyyttä.

G Toissijaiset toteamukset Privacy Shield -päätöksen vaikutuksista ja pätevyydestä

187. Vaikka edellä esitetyn tarkastelun perusteella ehdotan, että unionin tuomioistuin ensisijaisesti pidättyy ottamasta kantaa Privacy Shield -päätöksen vaikutukseen Schremsin DPC:lle tekemän kantelun kaltaisen kantelun käsittelyyn ja tämän päätöksen pätevyyteen, pidän hyödyllisenä esittää toissijaisesti ja tietyin varauksin tältä osin joitakin toteamuksia, jotka eivät ole tyhjentäviä.

1. Privacy Shield -päätöksen vaikutus siihen, miten valvontaviranomainen käsittelee sopimukseen perustuviin suojatoimiin perustuvan siirron laillisuudesta tehtyä kantelua

188. Yhdeksännellä ennakkoratkaisukysymyksellä halutaan selvittää, onko Privacy Shield -päätöksessä esitetty toteamus Yhdysvaltojen varmistaman tietosuojan riittävyydestä, kun otetaan huomioon siirrettyihin tietoihin pääsylle ja niiden käytölle kansallista turvallisuutta varten Yhdysvaltojen viranomaisille asetetut rajoitukset sekä rekisteröityjen oikeussuojan rajoitukset, esteenä sille, että valvontaviranomainen keskeyttää mallisopimuslausekkeiden nojalla toteutetun siirron tämän kolmanteen maahan.

189. Tämä kysymyksenasettelu on nähdäkseni ymmärrettävä suhteessa tuomion Schrems 51 ja 52 kohtaan, joista ilmenee, että tietosuojan riittävyyttä koskeva päätös velvoittaa valvontaviranomaisia niin kauan kuin sitä ei ole todettu pätemättömäksi. Valvontaviranomainen, joka on saanut käsiteltäväkseen kantelun henkilöltä, jonka tietoja siirretään tietosuojan riittävyyttä koskevan päätöksen kohteena olevaan kolmanteen maahan, ei voi näin ollen keskeyttää siirtoa sillä perusteella, että tietosuojan taso on siellä riittämätön, ilman että unionin tuomioistuin on sitä ennen todennut tämän päätöksen pätemättömäksi.[80]

190. Ennakkoratkaisua pyytänyt tuomioistuin haluaa ennen kaikkea tietää, onko siltä osin kuin kyse on tietosuojan riittävyyttä koskevasta päätöksestä – kuten Privacy Shield -päätöksestä tai sitä ennen safe harbor -päätöksestä –, joka perustuu yritysten vapaaehtoiseen ilmoitukseen siinä todettujen periaatteiden noudattamisesta, tämä johtopäätös voimassa ainoastaan, jos siirto kyseiseen kolmanteen maahan kuuluu tämän päätöksen soveltamisalaan, vai myös silloin, jos se perustuu erilliseen oikeusperustaan.

78 Ks. High Courtin 3.10.2017 antama tuomio (66 kohta).

79 Ks. Privacy Shield -järjestelyn verkkosivu (https://www.privacyshield.gov/participant_search).

80 Ks. vastaavasti tuomio Schrems (59 kohta).

191. Schremsin, Saksan, Alankomaiden, Puolan ja Portugalin hallitusten ja komission mukaan Privacy Shield -päätöksessä esitetty tietosuojan riittävyyttä koskeva toteamus ei vie valvontaviranomaisilta toimivaltuutta keskeyttää tai kieltää mallisopimuslausekkeiden nojalla toteutettu siirto Yhdysvaltoihin. Kun siirto Yhdysvaltoihin ei perustu Privacy Shield -päätökseen, tämä päätös ei muodollisesti sido valvontaviranomaisia niiden käyttäessä tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisia toimivaltuuksiaan. Nämä viranomaiset voisivat toisin sanoen poiketa komission toteamuksista, jotka koskevat sitä, onko suoja Yhdysvaltojen viranomaisten puuttumiselta rekisteröityjen perusoikeuksien käyttöön riittävä. Alankomaiden hallitus ja komissio täsmentävät, että valvontaviranomaisten on kuitenkin otettava ne huomioon näitä toimivaltuuksia käyttäessään. Saksan hallituksen mukaan nämä viranomaiset voisivat tehdä vastakkaisia arviointeja vasta suoritettuaan komission esittämistä toteamuksista aineellisen tutkimuksen, joka käsittää asian kannalta merkitykselliset selvitykset.

192. Facebook Ireland ja Yhdysvaltojen hallitus väittävät sitä vastoin, että tietosuojan riittävyyttä koskevan päätöksen sitovuus merkitsee oikeusvarmuuden ja unionin oikeuden yhdenmukaista soveltamista koskevien vaatimusten valossa sitä, että valvontaviranomaisilla ei ole oikeutta kyseenalaistaa kyseiseen päätökseen sisältyviä toteamuksia edes käsitellessään kantelua, jolla pyritään saamaan muulla kuin tämän päätöksen perusteella toteutetut siirrot kyseessä olevaan kolmanteen maahan keskeytetyiksi.

193. Kannatan näistä kahdesta lähestymistavasta ensin mainittua. Koska Privacy Shield -päätöksen soveltamisala on rajattu siirtoihin tämän päätöksen nojalla oman varmennuksen antaneelle yritykselle, kyseinen päätös ei voi muodollisesti sitoa valvontaviranomaisia siltä osin kuin kyse on siirroista, jotka eivät kuulu tähän soveltamisalaan. Vastaavasti Privacy Shield -päätöksen tarkoituksena on oikeusvarmuuden takaaminen vain niille tietojen viejille, jotka siirtävät tietoja siinä vahvistetuissa puitteissa. Tietosuoja-asetuksen 52 artiklassa valvontaviranomaisille tunnustetulla riippumattomuudella pyritään nähdäkseni myös estämään se, että ne olisivat sidottuja komission tietosuojan riittävyyttä koskevassa päätöksessä esittämiin toteamuksiin sen soveltamisalan ulkopuolella.

194. On selvää, että Privacy Shield -päätöksessä esitetyt toteamukset, jotka koskevat Yhdysvaltojen tiedustelupalvelujensa toimintaan liittyvää puuttumista vastaan takaaman tietosuojan riittävyyttä, muodostavat lähtökohdan tarkastelulle, jossa valvontaviranomainen arvioi tapauskohtaisesti, onko mallisopimuslausekkeisiin perustuva siirto keskeytettävä tällaisen puuttumisen vuoksi. Jos valvontaviranomainen katsoo asiaa perusteellisesti tutkittuaan, ettei se voi yhtyä näihin toteamuksiin käsiteltäväkseen saatetun siirron osalta, sillä on mielestäni edelleen mahdollisuus käyttää tietosuoja-asetuksen 58 artiklan 2 kohdan f ja j alakohdan mukaisia toimivaltuuksiaan.

195. Tilanteessa, jossa unionin tuomioistuin päättäisi vastata nyt tarkasteltuun kysymykseen toisin kuin esitän, olisi kuitenkin tutkittava, pitäisikö nämä toimivaltuudet kuitenkin palauttaa Privacy Shield -päätöksen pätemättömyyden vuoksi.

2. Privacy Shield -päätöksen pätevyys

196. Seuraavassa esitettävät huomautukset herättävät tiettyjä kysymyksiä Privacy Shield -päätöksessä esitettyjen arviointien perusteltavuudesta siltä osin kuin kyse on Yhdysvaltojen varmistamasta, tietosuoja-asetuksen 45 artiklan 1 kohdassa tarkoitetusta tietosuojan tason riittävyydestä Yhdysvaltojen tiedusteluviranomaisten harjoittaman sähköisen viestinnän tarkkailutoiminnan osalta. Näillä huomautuksilla ei ole tarkoitus esittää lopullista tai tyhjentävää kantaa tämän päätöksen pätevyydestä. Niissä esitetään vain joitakin ajatuksia, joista voi olla hyötyä unionin tuomioistuimelle, jos se vastoin suositustani ottaa tältä osin kantaa.

197. Privacy Shield -päätöksen johdanto-osan 64 perustelukappaleesta ja liitteessä II olevasta I.5 kohdasta ilmenee, että yritysten tässä päätöksessä tarkoitettujen periaatteiden noudattamista voidaan rajoittaa muun muassa siinä määrin kuin on tarpeellista kansallisen turvallisuuden, yleisen edun ja lainvalvonnan vaatimusten vuoksi tai Yhdysvaltojen oikeuteen perustuvien ristiriitaisten velvoitteiden vuoksi.

198. Komissio on arvioinut Yhdysvaltojen lainsäädännön mukaiset suojatoimet siltä osin kuin on kyse Yhdysvaltojen viranomaisten pääsystä siirrettyihin tietoihin ja niiden käytöstä erityisesti kansallisen turvallisuuden nimissä.[81] Se on saanut Yhdysvaltojen hallitukselta tiettyjä sitoumuksia, jotka koskevat rajoituksia Yhdysvaltojen viranomaisten pääsylle siirrettyihin tietoihin ja niiden käyttämiselle sekä rekisteröidyille annettua oikeussuojaa.[82]

199. Schrems vetoaa unionin tuomioistuimessa Privacy Shield -päätöksen pätemättömyyteen sillä perusteella, että näin kuvatut suojatoimet eivät riitä varmistamaan riittävää perusoikeuksien suojaa henkilöille, joiden tietoja siirretään Yhdysvaltoihin. Kyseenalaistamatta suoraan tämän päätöksen pätevyyttä DPC, EPIC sekä Itävallan, Puolan ja Portugalin hallitukset riitauttavat komission siinä esittämät arvioinnit tietosuojan riittävyydestä Yhdysvaltojen tiedustelupalvelujen toimintaan perustuvaa puuttumista vastaan. Nämä epäilyt heijastavat parlamentin[83], Euroopan tietosuojaneuvoston[84] ja Euroopan tietosuojavaltuutetun[85] ilmaisemia huolenaiheita.

200. Ennen kuin tarkastellaan Privacy Shield -päätöksessä tietosuojan riittävyydestä tehdyn toteamuksen perusteltavuutta on syytä täsmentää, mitä menetelmää tässä tarkastelussa on noudatettava.

a) Tietosuojan riittävyyttä koskevan päätöksen pätevyyttä koskevan tarkastelun sisältöä koskevat täsmennykset

1) Vertailuperusteet, joiden nojalla voidaan arvioida, onko tietosuojan taso ”pääosiltaan vastaava”

201. Tietosuoja-asetuksen 45 artiklan 3 kohdan ja unionin tuomioistuimen oikeuskäytännön[86] mukaan komissio voi todeta kolmannen maan tarjoavan riittävän tietosuojan tason vain, jos se on asianmukaisin perusteluin päätellyt, että rekisteröityjen perusoikeuksien suojan taso ”pääosiltaan vastaa” siellä tasoa, jota edellytetään unionissa tämän asetuksen, luettuna perusoikeuskirjan valossa, nojalla.

81 Ks. Privacy Shield -päätöksen johdanto-osan 65 perustelukappale.

82 Ks. Privacy Shield -päätöksen liitteet III–VII.

83 Parlamentin 6.4.2017 antama päätöslauselma EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn tarjoaman suojan riittävyydestä, P8_TA(2017)0131 ja 5.7.2018 antama päätöslauselma EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn tarjoaman suojan riittävyydestä, P8_TA(2018)0315.

84 Ks. 29 artiklan mukainen tietosuojatyöryhmä (jäljempänä tietosuojatyöryhmä), Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 13.4.2016, WP 238; tietosuojatyöryhmä, EU-US Privacy Shield – First Annual Joint Review, 28.11.2017, WP 255, ja Euroopan tietosuojaneuvosto, EU-US Privacy Shield – Second Annual Joint Review, 22.1.2019. Tietosuojatyöryhmä perustettiin direktiivin 95/46 29 artiklan 1 kohdan nojalla, jonka mukaan se oli luonteeltaan neuvoa-antava ja toiminnassaan itsenäinen. Tämän artiklan 2 kohdan mukaan kyseinen työryhmä koostui kunkin kansallisen valvontaviranomaisen edustajasta, yhteisön toimielimiä ja elimiä varten perustettujen viranomaisten edustajasta sekä komission edustajasta. Tietosuoja-asetuksen voimaantulosta lähtien tietosuojatyöryhmä on korvattu Euroopan tietosuojaneuvostolla (ks. tämän asetuksen 94 artiklan 2 kohta).

85 Ks. Euroopan tietosuojavaltuutettu, lausunto 4/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskevasta päätösluonnoksesta, 30.5.2016. Euroopan tietosuojavaltuutettu perustettiin yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 18.12.2000 annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 (EYVL 2001, L 8, s. 1) 1 artiklan 2 kohdalla. Euroopan tietosuojavaltuutettu valvoo tämän asetuksen säännösten soveltamista.

86 Ks. tämän ratkaisuehdotuksen 112 kohta.

202. Kolmannessa maassa taatun tietosuojan riittävyyden tarkistaminen edellyttää siten välttämättä tässä kolmannessa maassa vallitsevien sääntöjen ja käytäntöjen vertailua unionissa voimassa oleviin suojan tasoa koskeviin vaatimuksiin. Toisella kysymyksellään ennakkoratkaisua pyytänyt tuomioistuin pyytää unionin tuomioistuinta täsmentämään tämän vertailun perusteita.[87]

203. Tarkemmin ottaen kyseinen tuomioistuin pyrkii selvittämään, merkitseekö SEU 4 artiklan 2 kohdassa ja tietosuoja-asetuksen 2 artiklan 2 kohdassa jäsenvaltioille kansallisen turvallisuuden suojelun alalla varattu toimivalta sitä, että unionin oikeusjärjestyksessä ei ole suojan tasoa koskevia vaatimuksia, joihin kolmannessa maassa, jossa viranomaiset käsittelevät sinne siirrettyjä tietoja kansallista turvallisuutta varten, toteutettuja suojatoimia pitäisi verrata niiden riittävyyden arvioimiseksi. Jos tähän vastataan myöntävästi, kyseinen tuomioistuin haluaa tietää, miten asian kannalta merkityksellinen viitekehys on määritettävä.

204. Tältä osin on pidettävä mielessä, että kun unionin oikeudessa edellytetään rekisteröityjen oikeuksien suojan tason jatkuvuutta, siinä henkilötietojen kansainvälisille siirroille asetettujen rajoitusten tarkoituksena on pyrkiä välttämään vaara unionissa sovellettavien vaatimusten kiertämisestä.[88] Kuten Facebook Ireland väittää, tämän tarkoituksen kannalta ei olisi mitenkään perusteltua odottaa, että kolmas maa noudattaa vaatimuksia, jotka eivät vastaa jäsenvaltioille asetettuja velvoitteita.

205. Perusoikeuskirjan 51 artiklan 1 kohdan mukaan perusoikeuskirjan määräykset koskevat jäsenvaltioita ainoastaan silloin, kun ne soveltavat unionin oikeutta. Tämän vuoksi tietosuojan riittävyyttä koskevan päätöksen pätevyys rekisteröityjen perusoikeuksien käytölle kohdemaana olevan kolmannen maan lainsäädännössä asetettuihin rajoituksiin nähden riippuu näiden rajoitusten vertailusta rajoituksiin, jotka jäsenvaltiot voisivat asettaa perusoikeuskirjan määräysten perusteella *ainoastaan siltä osin kuin jäsenvaltion samankaltainen säännöstö kuuluisi unionin oikeuden soveltamisalaan*.

206. Kohdemaana olevassa kolmannessa valtiossa varmistetun tietosuojan riittävyyttä ei kuitenkaan voida arvioida sivuuttamalla mahdollinen puuttuminen rekisteröityjen perusoikeuksien käyttöön erityisesti kansallisen turvallisuuden alalla toteutetuilla valtion toimenpiteillä, jotka jäisivät unionin oikeuden soveltamisalan ulkopuolelle, jos ne olisivat jäsenvaltion toteuttamia. Tätä arviointia varten tietosuoja-asetuksen 45 artiklan 2 kohdan a alakohdassa edellytetään, että huomioon otetaan ilman minkäänlaisia rajoituksia kyseisessä kolmannessa maassa voimassa oleva kansallista turvallisuutta koskeva lainsäädäntö.

207. Tietosuojan riittävyyden arviointi tällaisten valtion toimenpiteiden osalta edellyttää mielestäni niihin liittyvien suojatoimien vertailua unionissa jäsenvaltioiden oikeuden nojalla edellytettyyn suojan tasoon, mukaan lukien niiden sitoumukset Euroopan ihmisoikeussopimuksen perusteella. Koska jäsenvaltioiden liittyminen Euroopan ihmisoikeussopimukseen velvoittaa ne saattamaan kansalliset oikeusjärjestyksensä yhteensopiviksi tämän sopimuksen määräysten kanssa ja koska se on, kuten Facebook Ireland, Saksan ja Tšekin hallitukset ja komissio ovat korostaneet, jäsenvaltioiden yhteinen nimittäjä, pidän näitä määräyksiä merkityksellisenä vertailuperusteena tässä arvioinnissa.

87 On syytä muistaa, että sitä, vastaako kolmannen maan tarjoaman tietosuojan taso pääosiltaan unionissa edellytettyä tasoa, on arvioitava myös, kun päätökseen 2010/87 sisältyviin mallisopimuslausekkeisiin perustuvan erityisen siirron yhteydessä rekisterinpitäjä tai tämän jättäessä toimimatta toimivaltainen valvontaviranomainen tarkistaa, asettavatko kohdemaana olevan kolmannen maan viranomaiset tietojen tuojalle vaatimuksia, jotka menevät pidemmälle kuin on tarpeen demokraattisessa yhteiskunnassa (ks. päätöksen 2010/87 liitteessä oleva lauseke 5 ja siihen liittyvä alaviite). Ks. tämän ratkaisuehdotuksen 115, 134 ja 135 kohta.

88 Ks. tämän ratkaisuehdotuksen 117 kohta.

208. Tässä tapauksessa, kuten edellä on tuotu esille,[89] Yhdysvaltojen kansallista turvallisuutta koskevat vaatimukset saavat etusijan Privacy Shield -päätöksen nojalla oman varmennuksen antaneiden yritysten velvoitteisiin nähden. Tämän päätöksen pätevyys riippuu myös siitä, liittyykö näihin vaatimuksiin suojatoimia, joilla tarjotaan suojan taso, joka pääosiltaan vastaa unionissa varmistettavan suojan tasoa.

209. Tähän kysymykseen annettava vastaus edellyttää, että ensin määritetään vaatimukset – perusoikeuskirjaan tai Euroopan ihmisoikeussopimukseen perustuvat vaatimukset – jotka komission Privacy Shield -päätöksessä tutkimien kaltaisten sähköisen viestinnän tarkkailusäännöstöjen olisi täytettävä unionissa. Sovellettavien vaatimusten määrittäminen riippuu siitä, kuuluisivatko FISA:n 702 §:n ja EO 12333:n kaltaiset säännöstöt, jos ne olisivat jonkin jäsenvaltion säännöstöjä, tietosuoja-asetuksen 2 artiklan 2 kohdan, luettuna SEU 4 artiklan 2 kohdan valossa, nojalla tämän asetuksen soveltamisalaan kohdistuvan rajoituksen piiriin vai eivät.

210. Tältä osin SEU 4 artiklan 2 kohdan sanamuodosta ja vakiintuneesta oikeuskäytännöstä ilmenee, että unionin oikeutta ja muun muassa henkilötietojen suojaa koskevia johdetun oikeuden säädöksiä ei sovelleta toimintoihin kansallisen turvallisuuden suojelun alalla siltä osin kuin ne ovat valtiolle tai valtion viranomaisille tyypillisiä toimintoja, jotka eivät liity yksityisten henkilöiden toiminta-aloihin.[90]

211. Tämä periaate merkitsee *yhtäältä* sitä, että kansallisen turvallisuuden suojelun alalla annettu lainsäädäntö ei kuulu unionin oikeuden soveltamisalaan, kun siinä säännellään yksinomaan valtion toimintaa eikä rajoiteta mitenkään yksityisten henkilöiden harjoittamaa toimintaa. Tämän vuoksi tätä oikeutta ei nähdäkseni sovelleta henkilötietojen keräämistä ja käyttöä koskeviin kansallisiin toimenpiteisiin, jotka valtio on pannut suoraan täytäntöön kansallisen turvallisuuden suojelemiseksi asettamatta erityisiä velvoitteita yksityisille toimijoille. Kuten komissio väitti istunnossa, erityisesti jäsenvaltion toteuttama toimenpide, jolla EO 12333:n tavoin annettaisiin sen turvallisuuspalveluille suora pääsy siirrettäviin tietoihin, jäisi unionin oikeuden soveltamisalan ulkopuolelle.[91]

212. Toisella tapaa monimutkaisempi on kysymys siitä, jäisivätkö *toisaalta* unionin oikeuden soveltamisalan ulkopuolelle myös kansalliset säännökset, joissa FISA:n 702 §:n tavoin sähköisten viestintäpalvelujen tarjoajat velvoitetaan tarjoamaan kansallisen turvallisuuden alalla toimivaltaisille viranomaisille tukea, jotta nämä saisivat pääsyn tiettyihin henkilötietoihin.

213. Vaikka tuomio PNR puoltaa myöntävän vastauksen antamista tähän kysymykseen, tuomiossa Tele2 Sverige ja tuomiossa Ministerio Fiscal esitetyn päättelyn vuoksi siihen voisi olla perusteltua vastata kieltävästi.

214. Tuomiolla PNR kumottiin päätös, jolla komissio oli todennut tulli- ja rajavartioasioissa toimivaltaiselle Yhdysvaltojen viranomaiselle toimitettujen lentomatkustajia koskevaan matkustajarekisteriin (Passenger Name Records, PNR) sisältyvien henkilötietojen suojan riittävyyden.[92] Tuomiossa katsottiin, että tämän päätöksen kohteena ollut käsittely – lentoyhtiöiden suorittama PNR-tietojen siirto kyseessä olevalle viranomaiselle – kuului *sen tarkoitus huomioon ottaen* direktiivin 95/46 3 artiklan 2 kohdassa sen soveltamisalasta säädetyn poikkeuksen piiriin. Kyseisen tuomion

89 Ks. tämän ratkaisuehdotuksen 197 kohta.

90 Ks. mm. tuomio 6.11.2003, Lindqvist (C-101/01, EU:C:2003:596, 43 ja 44 kohta); tuomio PNR (58 kohta); tuomio 16.12.2008, Satakunnan Markkinapörssi ja Satamedia (C-73/07, EU:C:2008:727, 41 kohta); tuomio 21.12.2016, Tele2 Sverige ja Watson ym. (C-203/15 ja C-698/15, EU:C:2016:970; jäljempänä tuomio Tele2 Sverige; 69 kohta) ja tuomio 2.10.2018, Ministerio Fiscal (C-207/16, EU:C:2018:788; jäljempänä tuomio Ministerio Fiscal; 32 kohta).

91 Epäselvyyksien välttämiseksi tässä suhteessa korostan, että komissio ei kyennyt Privacy Shield -päätöksessä määrittämään, kaappaako Yhdysvallat todella transatlanttisia kaapeleita pitkin siirrettävää viestintää, koska Yhdysvaltojen viranomaiset eivät ole vahvistaneet tai kumonneet tätä väitettä (ks. tämän päätöksen johdanto-osan 75 perustelukappale ja sen liitteessä VI olevaan I kohdan a alakohtaan sisältyvä Robert Littin 22.2.2016 päivätty kirje). Koska Yhdysvaltojen hallitus ei kuitenkaan ole kiistänyt keräävänsä siirrettäviä tietoja EO 12333:n perusteella, komission oli mielestäni ennen tietosuojan riittävyyden toteamista saatava kyseiseltä hallitukselta vakuutus siitä, että jos tällaista tietojen keräämistä tapahtuu, siihen liittyvät riittävät suojatoimet väärinkäytön vaaroja vastaan. Tässä tarkoituksessa komissio on kyseisen päätöksen johdanto-osan 68–77 perustelukappaleessa tutkinut tällaisessa tilanteessa PPD 28:n nojalla sovellettavat rajoitukset ja suojatoimet.

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

mukaan tämä käsittely ei ollut tarpeen palvelujen tarjoamiseksi, vaan se oli tarpeellinen yleisen turvallisuuden suojelemiseksi ja lainvalvontatarkoituksia varten. Koska kyseinen siirto tapahtui julkishallinnon asettamissa puitteissa, jotka liittyvät yleiseen turvallisuuteen, se jäi tämän direktiivin soveltamisalan ulkopuolelle huolimatta siitä, että alun perin yksityiset toimijat keräsivät PNR-tiedot sen soveltamisalaan kuuluvan kaupallisen toiminnan yhteydessä ja järjestivät tämän siirron.[93]

215. Tämän jälkeen annetussa tuomiossa Tele2 Sverige[94] unionin tuomioistuin totesi, että direktiivin 2002/58/EY[95] 15 artiklan 1 kohtaan perustuvat kansalliset säännökset, jotka koskevat sekä sähköisten viestintäpalvelujen tarjoajien toteuttamaa liikenne- ja paikkatietojen säilyttämistä että viranomaisten oikeutta saada säilytettyjä tietoja tässä säännöksessä mainittuihin tarkoituksiin, jotka käsittävät rikosten torjunnan ja kansallisen turvallisuuden suojelun, kuuluvat tämän direktiivin ja siten perusoikeuskirjan soveltamisalaan. Unionin tuomioistuimen mukaan tämän direktiivin soveltamisalasta säädettyä poikkeusta sen 1 artiklan 3 kohdassa, jossa viitataan muun muassa valtion toimiin rikosoikeuden ja kansallisen turvallisuuden suojelun alalla, ei sovelleta tietojen säilyttämistä koskeviin säännöksiin eikä myöskään säilytettyjen tietojen saantia koskeviin säännöksiin.[96] Unionin tuomioistuin vahvisti tämän oikeuskäytännön tuomiossa Ministerio Fiscal.[97]

216. FISA:n 702 § eroaa kuitenkin tällaisesta säännöstöstä siltä osin, että tässä säännöksessä ei aseteta sähköisten viestintäpalvelujen tarjoajille minkäänlaista tietojen säilyttämisvelvollisuutta tai muuta velvollisuutta käsitellä tietoja ilman tiedusteluviranomaisten esittämää pyyntöä tietojen saamisesta.

217. Näin ollen on pohdittava, kuuluvatko kansalliset toimenpiteet, joissa näille palveluntarjoajille asetetaan velvollisuus saattaa tietoja viranomaisten saataville kansallista turvallisuutta varten *säilyttämisvelvollisuudesta riippumatta*, tietosuoja-asetuksen ja siten perusoikeuskirjan soveltamisalaan.[98]

218. *Ensimmäinen lähestymistapa* voisi olla sovittaa mahdollisimman pitkälle yhteen edellä mainitut kaksi oikeuskäytännön linjaa tulkitsemalla unionin tuomioistuimen tuomiossa Tele2 Sverige ja tuomiossa Ministerio Fiscal tekemän johtopäätöksen unionin oikeuden sovellettavuudesta toimenpiteisiin, jotka koskevat kansallisten viranomaisten pääsyä tietoihin muun muassa kansallisen turvallisuuden suojelemiseksi,[99] rajoittuvan tilanteisiin, joissa nämä tiedot on säilytetty direktiivin

93 Tuomio PNR (56–58 kohta). Yhteisöjen tuomioistuin totesi 10.2.2009 antamassaan tuomiossa Irlanti v. parlamentti ja neuvosto (C-301/06, EU:C:2009:68, 90 ja 91 kohta), että tuomiossa PNR esitetyt näkökohdat eivät olleet sovellettavissa yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta 15.3.2006 annetussa Euroopan parlamentin ja neuvoston direktiivissä 2006/24/EY (EUVL 2006, L 105, s. 54) tarkoitettuun käsittelyyn. Yhteisöjen tuomioistuin perusteli tätä johtopäätöstä sillä, että toisin kuin tuomiossa PNR kyseessä ollut päätös, direktiivi 2006/24 koskee ainoastaan palvelujen tarjoajien toimintaa sisämarkkinoilla, eikä sillä säännellä mitenkään viranomaisten lainvalvontatoimintaa. Tällä päättelyllään yhteisöjen tuomioistuin näyttää todenneen, että vastakkaispäätelmänä tuomiossa PNR tehty johtopäätös olisi ollut sovellettavissa säännöksiin, jotka koskevat näiden viranomaisten pääsyä säilytettyihin tietoihin tai näiden tietojen käyttöä.

94 Tuomio Tele2 Sverige (67–81 kohta).

95 Henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12.7.2002 annettu Euroopan parlamentin ja neuvoston direktiivi (sähköisen viestinnän tietosuojadirektiivi) (EYVL 2002, L 201, s. 37).

96 Koska direktiivissä 2002/58 konkretisoidaan direktiivin 95/46, joka on sittemmin kumottu sen sisällön pitkälti toistavalla tietosuoja-asetuksella, vaatimukset, mielestäni direktiivin 2002/58 1 artiklan 3 kohdan tulkintaa koskeva oikeuskäytäntö soveltuu analogisesti tietosuoja-asetuksen 2 artiklan 2 kohdan tulkintaan. Ks. vastaavasti tuomio Tele2 Sverige (69 kohta) ja tuomio Ministerio Fiscal (32 kohta).

97 Tuomio Ministerio Fiscal (34, 35 ja 37 kohta).

98 Tämä sama kysymys on esitetty unionin tuomioistuimessa vireillä olevan kolmen muun ennakkoratkaisupyynnön yhteydessä. Ks. asia C-623/17, Privacy International (EUVL 2018, C 22, s. 29) sekä yhdistetyt asiat C-511/18 ja C-512/18, La Quadrature du Net ym. ja French Data Network ym. (EUVL 2018, C 392, s. 7).

99 Vaikka tuomiossa Tele2 Sverige unionin tuomioistuin keskittyi tarkastelemaan kyseessä olleisiin säilyttämis- ja tietojensaantitoimenpiteisiin perustuvan puuttumisen oikeuttamista rikosten torjumista koskevaan tavoitteeseen nähden, sen tekemä johtopäätös pätee soveltuvin osin myös silloin, kun tällaisilla toimenpiteillä on kansallisen turvallisuuden suojelemista koskeva tavoite. Direktiivin 2002/58 15 artiklan 1 kohdassa mainitaan tavoitteina, joilla tällaiset toimenpiteet voidaan oikeuttaa, sekä rikosten torjuminen että kansallisen turvallisuuden suojelu. Direktiivin 2002/58 1 artiklan 3 kohdassa ja tietosuoja-asetuksen 2 artiklan 2 kohdassa jätetään näiden säädösten soveltamisalan ulkopuolelle valtion toiminta sekä kansallisen turvallisuuden että rikosoikeuden alalla. Tuomion Tele2 Sverige taustalla olleessa asiassa kyseessä olleilla toimenpiteillä oli myös kansalliseen turvallisuuteen liittyvä tarkoitus. Tämän tuomion 119 kohdassa unionin tuomioistuin käsitteli nimenomaisesti liikenne- ja paikkatietojen säilyttämistä ja saantia koskevien toimenpiteiden oikeuttamista kansallisen turvallisuuden suojelua koskevalla tavoitteella siltä osin kuin se pitää sisällään terrorismin torjumisen.

2002/58 15 artiklan 1 kohdan mukaisen *lakisääteisen velvollisuuden nojalla*. Tämä johtopäätös ei sen sijaan soveltuisi tosiseikkoihin, jotka eroavat tuomiosta PNR, joka koski lentoyhtiöiden kaupallisessa tarkoituksessa omasta aloitteestaan säilyttämien tietojen siirtoa sisäisen turvallisuuden alalla toimivaltaiselle yhdysvaltalaiselle viranomaiselle.

219. *Toisessa lähestymistavassa*, jota komissio suosii ja jota pidän vakuuttavampana, tuomiossa Tele2 Sverige ja tuomiossa Ministerio Fiscal esitetyn päättelyn vuoksi olisi perusteltua soveltaa unionin oikeutta kansallisiin sääntöihin, joissa sähköisten viestintäpalvelujen tarjoajat velvoitetaan antamaan apuaan kansallisesta turvallisuudesta vastaaville viranomaisille, jotta nämä saisivat pääsyn tiettyihin tietoihin, *liittyipä näihin sääntöihin ennalta asetettu tietojen säilyttämisvelvollisuus tai ei*.

220. Tämän päättelyn keskeinen sisältö ei perustu kyseisten säännösten tarkoitukseen, kuten tuomiossa PNR, vaan pikemminkin siihen, että nämä säännökset koskivat palveluntarjoajien toimintaa, kun ne velvoitettiin ryhtymään tietojen käsittelyyn. Tämä toiminta ei ollut valtion toimintaa direktiivin 2002/58 1 artiklan 3 kohdassa ja direktiivin 95/46 3 artiklan 2 kohdassa, joiden olennainen sisältö toistetaan tietosuoja-asetuksen 2 artiklan 2 kohdassa, tarkoitetuilla aloilla.

221. Unionin tuomioistuin totesi tuomiossa Tele2 Sverige, että ”oikeus saada – – palveluntarjoajien säilyttämiä tietoja, koskee *viimeksi mainittujen* suorittamaa henkilötietojen käsittelyä, joka kuuluu kyseisen direktiivin soveltamisalaan”.[100] Vastaavasti se totesi tuomiossa Ministerio Fiscal, että lainsäädännöllinen toimenpide, jossa velvoitetaan palveluntarjoajat antamaan toimivaltaisille viranomaisille oikeus saada säilytettyjä tietoja, ”merkitsee väistämättä sitä, että *nämä palveluntarjoajat* käsittelevät [näitä] tietoja”.[101]

222. Se, että rekisterinpitäjä saattaa tietoja viranomaisen saataville, vastaa tietosuoja-asetuksen 4 artiklan 2 alakohdassa säädettyä käsittelyn määritelmää.[102] Sama pätee siihen, että tietoja suodatetaan ennalta hakukriteerien avulla viranomaisten pyytämien tietojen erottamiseksi.[103]

223. Päättelen tästä, että unionin tuomioistuimen tuomiossa Tele2 Sverige ja tuomiossa Ministerio Fiscal esittämän päättelyn mukaisesti tietosuoja-asetusta ja siten perusoikeuskirjaa sovelletaan kansalliseen lainsäädäntöön, jossa sähköisten viestintäpalvelujen tarjoaja velvoitetaan tarjoamaan apuaan kansallisesta turvallisuudesta vastaaville viranomaisille saattamalla niiden saataville tietoja, tarvittaessa suodatettuaan ne, riippumatta siitä, onko näiden tietojen säilyttämiseen lakisääteinen velvollisuus.

224. Tämä tulkinta näyttää lisäksi perustuvan ainakin välillisesti tuomioon Schrems. Kuten DPC, Itävallan ja Puolan hallitukset sekä komissio korostavat, unionin tuomioistuin totesi siinä safe harbor -päätöksen pätevyyttä tutkiessaan, että tietosuojan riittävyyttä koskevan päätöksen kohteena olevan kolmannen maan oikeudessa on säädettävä sitä vastaan, että sen viranomaiset puuttuvat kansallista turvallisuutta varten rekisteröityjen perusoikeuksiin, takeista, jotka pääosiltaan vastaavat erityisesti perusoikeuskirjan 7, 8 ja 47 artiklaan perustuvia takeita.[104]

100 Tuomio Tele2 Sverige (78 kohta, kursivointi tässä). Kuten ilmaisun ”lisäksi” käyttäminen osoittaa, unionin tuomioistuin korosti tämän tuomion 79 kohdassa tässä asiassa kyseessä olleen tietojen säilyttämisvelvollisuuden erottamatonta yhteyttä niihin säännöksiin, jotka koskevat kansallisten viranomaisten oikeutta saada säilytetty tietoja, ainoastaan vahvistaakseen johtopäätöksensä direktiivin 2002/58 sovellettavuudesta.

101 Tuomio Ministerio Fiscal (37 kohta, kursivointi tässä).

102 Ks. vastaavasti tuomio Ministerio Fiscal (38 kohta).

103 Ks. vastaavasti tuomio 13.5.2014, Google Spain ja Google (C-131/12, EU:C:2014:317, 28 kohta).

104 Tuomio Schrems (91–96 kohta). Komissio viittaa myös Privacy Shield -päätöksen johdanto-osan 90, 124 ja 141 perustelukappaleessa perusoikeuskirjan määräyksiin ja hyväksyy siten periaatteen, jonka mukaan perusoikeuksiin kohdistuvien rajoitusten, joilla on kansallisen turvallisuuden suojelua koskeva tavoite, on oltava perusoikeuskirjan mukaisia.

225. Tästä seuraa tarkemmin sanottuna, että kansallinen toimenpide, jolla sähköisten viestintäpalvelujen tarjoajat velvoitetaan vastaamaan toimivaltaisten kansallisten turvallisuusviranomaisten pyyntöön saada näiden palveluntarjoajien kaupallisen toimintansa yhteydessä ilman minkäänlaista lakisääteistä velvollisuutta säilyttämiä tiettyjä tietoja yksilöimällä ennakolta pyydetyt tiedot valintakriteerejä soveltamalla (kuten PRISM-ohjelmassa), ei kuuluisi tietosuoja-asetuksen 2 artiklan 2 kohdan soveltamisalaan. Sama pätisi kansalliseen toimenpiteeseen, jolla televiestinnän runkoverkkoa ylläpitävät yritykset velvoitetaan antamaan kansallisesta turvallisuudesta vastaaville viranomaisille pääsy tietoihin, jotka siirretään niiden ylläpitämän infrastruktuurin kautta (kuten Upstream-ohjelmassa).

226. Sen sijaan sen jälkeen, kun kyseiset tiedot ovat valtion viranomaisten käsissä, tapaukset, joissa nämä viranomaiset myöhemmin säilyttävät ja käyttävät niitä kansallista turvallisuutta varten, kuuluvat – samoista syistä kuin edellä tämän ratkaisuehdotuksen 211 kohdassa on esitetty – tietosuoja-asetuksen 2 artiklan 2 kohdassa säädetyn poikkeuksen piiriin, joten ne eivät kuulu tämän asetuksen eivätkä siten perusoikeuskirjan soveltamisalaan.

227. Kaiken edellä esitetyn perusteella katson, että Privacy Shield -päätöksen pätevyyden valvonta, kun otetaan huomioon Yhdysvaltojen tiedusteluviranomaisten toiminnasta mahdollisesti seuraavat rajoitukset siinä ilmaistuille periaatteille, edellyttää kahden seikan tarkistamista.

228. On *ensinnäkin* tutkittava, takaako Yhdysvallat suojan, joka pääosiltaan vastaa tasoltaan tietosuoja-asetuksen säännöksiin ja perusoikeuskirjan määräyksiin perustuvaa suojaa, FISA:n 702 §:n soveltamisesta seuraavilta rajoituksilta siltä osin kuin tämän säännöksen perusteella NSA voi velvoittaa palveluntarjoajat saattamaan henkilötietoja sen saataville.

229. *Toiseksi* Euroopan ihmisoikeussopimuksen määräykset muodostavat asian kannalta merkityksellisen viitekehyksen arvioitaessa, kyseenalaistavatko rajoitukset, joita EO 12333:n soveltamisesta voisi seurata siltä osin kuin siinä annetaan tiedusteluviranomaisille oikeus kerätä itse ilman yksityisten toimijoiden myötävaikutusta henkilötietoja, Yhdysvalloissa varmistetun tietosuojan riittävyyden. Nämä määräykset ovat myös vertailuperusteita, joiden perusteella voidaan arvioida tämän suojan tason riittävyyttä siihen nähden, että nämä viranomaiset säilyttävät ja käyttävät hankittuja tietoja kansallista turvallisuutta varten.

230. Asiassa on kuitenkin vielä ratkaistava, edellyttääkö tietosuojan riittävyyttä koskeva toteamus, että tietojen keräämiseen EO 12333:n nojalla liittyy suojan taso, joka pääosiltaan vastaa tasoa, joka unionissa on varmistettava, *myös siltä osin kuin tämä kerääminen tapahtuu Yhdysvaltojen alueen ulkopuolella* vaiheessa, jossa tietoja siirretään unionista tähän kolmanteen maahan.

2) Tarve varmistaa riittävä suojan taso tietojen siirtämisvaiheessa

231. Unionin tuomioistuimelle on esitetty kolme erilaista kantaa siitä, onko komission tarpeen ottaa huomioon kolmannessa maassa taatun suojan riittävyyden arvioimiseksi kansalliset toimenpiteet, jotka koskevat tämän kolmannen maan viranomaisten pääsyä tietoihin sen alueen ulkopuolella vaiheessa, jossa tietoja siirretään unionista tälle alueelle.

232. Ensinnäkin Facebook Ireland sekä Yhdysvaltojen ja Yhdistyneen kuningaskunnan hallitukset väittävät, että tällaisilla toimenpiteillä ei ole vaikutusta tietosuojan riittävyyttä koskevaan toteamukseen. Ne vetoavat tämän kantansa tueksi siihen, että kolmannen valtion on mahdotonta valvoa kaikkia viestintäkanavia, jotka sijaitsevat sen alueen ulkopuolella ja joiden kautta unionista lähtevät tiedot siirretään, joten lähtökohtaisesti ei voida koskaan taata, että jokin toinen kolmas valtio ei kerää salaa tietoja niiden siirtämisen aikana.

233. Toiseksi DPC, Schrems, EPIC, Itävallan ja Alankomaiden hallitukset, parlamentti ja Euroopan tietosuojaneuvosto väittävät, että tietosuoja-asetuksen 44 artiklassa asetettu vaatimus suojan tason jatkuvuudesta edellyttää, että tämä taso on riittävä koko siirron ajan, myös silloin, kun tiedot siirretään merenalaisia kaapeleita pitkin ennen niiden saapumista kohdemaana olevaan kolmanteen maahan.

234. Kolmanneksi komissio, joka samalla tunnustaa tämän periaatteen, väittää, että tietosuojan riittävyyttä koskevan toteamuksen tarkoitus rajoittuu päätöksen kohteena olevan kolmannen maan varmistamaan suojaan *sen rajojen sisäpuolella*, joten se, että riittävää suojan tasoa ei ole taattu *siirrettäessä* tietoja tähän kolmanteen maahan, ei kyseenalaista tietosuojan riittävyyttä koskevan päätöksen pätevyyttä. Rekisterinpitäjän on kuitenkin tietosuoja-asetuksen 32 artiklan mukaisesti huolehdittava siirron turvallisuudesta suojaamalla mahdollisimman pitkälle henkilötietoja niiden kyseiseen kolmanteen maahan siirtämisen vaiheessa.

235. Huomautan tältä osin, että tietosuoja-asetuksen 44 artiklassa asetetaan tietojen kolmanteen maahan siirron edellytykseksi tämän asetuksen V luvun säännöksissä asetettujen edellytysten noudattaminen siltä osin kuin tietoja voidaan käsitellä ”siirtämisen jälkeen”. Tämän ilmaisun voitaisiin ymmärtää tarkoittavan, kuten Yhdysvaltojen hallitus väitti kirjallisessa vastauksessaan unionin tuomioistuimen kysymyksiin, että näitä edellytyksiä on noudatettava *tietojen saavuttua kohteeseensa* tai että ne velvoittavat *sen jälkeen, kun siirto on aloitettu* (myös siirtämisvaiheen aikana).

236. Koska tietosuoja-asetuksen 44 artiklan sanamuoto ei ole ratkaiseva, kannatan teleologisen tulkinnan perusteella toista näistä tulkinnoista ja pidän näin ollen edellä mainituista lähestymistavoista toiseksi mainittua parhaana. Jos nimittäin katsottaisiin, että tässä säännöksessä asetettu vaatimus suojan tason jatkuvuudesta kattaisi ainoastaan kohdemaana olevan kolmannen maan alueen sisällä toteutetut tarkkailutoimenpiteet, sitä voitaisiin kiertää, kun tämä kolmas maa toteuttaa tällaisia toimenpiteitä alueensa ulkopuolella tietojen siirtämisvaiheessa. Tämän riskin välttämiseksi kolmannen maan takaaman tietosuojan riittävyyden arvioinnin on koskettava tämän kolmannen maan oikeusjärjestyksen kaikkia, muun muassa kansallista turvallisuutta koskevia, säännöksiä,[105] joihin kuuluvat yhtä lailla sen alueella toteutettua tarkkailua koskevat säännökset kuin säännökset, joiden perusteella tälle alueelle siirrettäviä tietoja voidaan tarkkailla.[106]

237. Kukaan ei kuitenkaan kiistä sitä, että kuten Euroopan tietosuojaneuvosto korostaa, tietosuojan riittävyyden arviointi koskee tietosuoja-asetuksen 45 artiklan 1 kohdasta ilmenevällä tavalla pelkästään *tietojen kohdemaana olevan kolmannen maan* oikeusjärjestyksen säännöksiä. Tähän arviointiin ei vaikuta Facebook Irelandin sekä Yhdysvaltojen ja Yhdistyneen kuningaskunnan hallitusten esille tuoma mahdottomuus taata, ettei jokin toinen kolmas valtio salaa keräisi näitä tietoja niiden siirtämisen aikana. Tällaista riskiä ei sitä paitsi voida sulkea pois edes sen jälkeen, kun tiedot ovat saapuneet kohdemaana olevan kolmannen valtion alueelle.

238. On myös totta, että komissio voisi arvioidessaan kolmannen maan takaaman tietosuojan riittävyyttä mahdollisesti joutua tilanteeseen, jossa tämä kolmas maa ei paljasta sille tiettyjen salaisten tarkkailuohjelmien olemassaoloa. Tästä ei kuitenkaan seuraa, että *jos tällaiset ohjelmat saatetaan sen tietoon*, komissio voisi olla ottamatta niitä huomioon tietosuojan riittävyyttä tutkiessaan. Jos tietosuojan riittävyyttä koskevan päätöksen antamisen jälkeen komissiolle paljastetaan päätöksen kohteena olevan kolmannen maan alueellaan tai tietojen sinne siirtämisen aikana toteuttamien tiettyjen salaisten tarkkailuohjelmien olemassaolo, komission on tarkasteltava uudelleen toteamustaan tämän kolmannen maan takaaman tietosuojan riittävyydestä, jos tällainen paljastus herättää tältä osin epäilyjä.[107]

105 Ks. vastaavasti tuomio Schrems (74 ja 75 kohta).

106 Ks. vastaavasti Euroopan tietosuojaneuvosto, EU-US Privacy Shield – Second Annual Joint Review, 22.1.2019 (s. 17, 86 kohta).

107 Ks. tietosuoja-asetuksen 45 artiklan 5 kohta. Ks. myös tuomio Schrems (76 kohta).

3) Komission ja ennakkoratkaisua pyytäneen tuomioistuimen Yhdysvaltojen oikeudesta esittämien tosiseikkoja koskevien toteamusten huomioon ottaminen

239. Vaikka on selvää, ettei unionin tuomioistuimella ole toimivaltaa esittää kolmannen maan oikeudesta tulkintaa, joka velvoittaisi kyseisen maan oikeusjärjestyksessä, Privacy Shield -päätöksen pätevyys riippuu siitä, ovatko komission arvioinnit Yhdysvaltojen oikeudessa ja käytännöissä taatusta henkilöiden, joiden tietoja siirretään tähän kolmanteen maahan, perusoikeuksien suojan tasosta perusteltuja. Komission oli perusteltava toteamuksensa tietosuojan riittävyydestä erityisesti kyseisen kolmannen maan oikeuden sisältöä koskevien, tietosuoja-asetuksen 45 artiklan 2 kohdassa mainittujen seikkojen osalta.[108]

240. High Court esitti 3.10.2017 antamassaan tuomiossa yksityiskohtaisia toteamuksia, joissa kuvattiin Yhdysvaltojen oikeuden asian kannalta merkityksellisiä piirteitä, arvioituaan ensin riidan asianosaisten esittämät todisteet.[109] Tämä selostus on pitkälti päällekkäinen niiden komission Privacy Shield -päätöksessä esittämien toteamusten kanssa, jotka koskevat Yhdysvaltojen tiedusteluviranomaisten toteuttamaa siirrettyjen tietojen keräämistä ja niiden pääsyä näihin tietoihin sekä tähän toimintaan liittyviä oikeussuojakeinoja ja valvontamekanismeja koskevien sääntöjen sisältöä.

241. Ennakkoratkaisua pyytänyt tuomioistuin sekä useat unionin tuomioistuimessa huomautuksia esittäneistä asianosaisista ja osapuolista kyseenalaistavat sekä komission näistä toteamuksista tekemät oikeudelliset johtopäätökset – eli päätelmän, jonka mukaan Yhdysvallat takaa riittävän perusoikeuksien suojan henkilöille, joiden tietoja siirretään tämän päätöksen nojalla –, että komission esittämän kuvauksen Yhdysvaltojen oikeuden sisällöstä.

242. Tässä tilanteessa arvioin Privacy Shield -päätöksen pätevyyttä ennen kaikkea komission itsensä esittämien toteamusten valossa siltä osin kuin kyse on Yhdysvaltojen oikeuden sisällöstä ja tutkin, oikeuttavatko nämä toteamukset tietosuojan riittävyyttä koskevan päätöksen antamisen.

243. Tässä suhteessa en yhdy DPC:n ja Schremsin puolustamaan kantaan, jonka mukaan High Courtin toteamukset Yhdysvaltojen oikeudesta sitoisivat unionin tuomioistuinta sen tutkiessa Privacy Shield -päätöksen pätevyyttä. Viimeksi mainitut väittävät, että koska Irlannin prosessioikeuden mukaan ulkomaan oikeus on tosiseikkoja koskeva kysymys, ennakkoratkaisua pyytäneellä tuomioistuimella on yksin toimivalta vahvistaa sen sisältö.

244. Vakiintuneen oikeuskäytännön mukaan kansallisella tuomioistuimella on toki yksinomainen toimivalta todeta asian kannalta merkitykselliset tosiseikat sekä tulkita ja soveltaa jäsenvaltion oikeutta siinä vireillä olevassa oikeusriidassa.[110] Tämä oikeuskäytäntö ilmentää unionin tuomioistuimen ja ennakkoratkaisua pyytäneen tuomioistuimen välistä tehtävänjakoa SEUT 267 artiklalla käyttöön otetussa menettelyssä. Vaikka ainoastaan unionin tuomioistuimella on toimivalta tulkita unionin oikeutta ja ottaa kantaa johdetun oikeuden pätevyyteen, kansallisen tuomioistuimen, jonka ratkaistavana on sen käsiteltäväksi saatettu konkreettinen oikeusriita, on vahvistettava asiaa koskevat tosiseikat ja oikeussäännöt, jotta unionin tuomioistuin voi antaa sille hyödyllisen vastauksen.

108 Safe harbor -päätös todettiin pätemättömäksi, koska komissio ei ollut todennut tässä päätöksessä, että Yhdysvallat tosiasiallisesti takaa tietosuojan riittävän tason sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta (tuomio Schrems, 97 kohta). Erityisesti komissio ei ollut todennut valtiollisia sääntöjä, joilla olisi tarkoitus rajoittaa mahdollista puuttumista rekisteröityjen perusoikeuksiin (tuomio Schrems, 88 kohta), tai tällaista puuttumista vastaan olemassa olevaa tehokasta oikeussuojaa (tuomio Schrems, 89 kohta).

109 Tämän ratkaisuehdotuksen 54–73 kohdassa esitetään yhteenveto näistä toteamuksista.

110 Ks. mm. tuomio 4.5.1999, Sürül (C-262/96, EU:C:1999:228, 95 kohta); tuomio 11.9.2008, Eckelkamp ym. (C-11/07, EU:C:2008:489, 32 kohta) ja tuomio 26.10.2016, Senior Home (C-195/15, EU:C:2016:804, 20 kohta).

245. Tämän ennakkoratkaisua pyytäneen tuomioistuimen yksinomaisen toimivallan tarkoitusta ei mielestäni voida ulottaa koskemaan tilannetta, jossa kolmannen maan oikeus vahvistetaan seikaksi, joka voi vaikuttaa unionin tuomioistuimen johtopäätökseen johdetun oikeuden toimen pätevyydestä.[111] Koska tällaisen toimen pätemättömyyden toteaminen vaikuttaa erga omnes unionin oikeusjärjestyksessä,[112] unionin tuomioistuimen johtopäätös ei voi riippua ennakkoratkaisupyynnön alkuperästä. Kuten Facebook Ireland ja Yhdysvaltojen hallitus korostavat, kyseinen johtopäätös riippuisi tästä alkuperästä, jos unionin tuomioistuin olisi sidottu ennakkoratkaisua pyytäneen tuomioistuimen kolmannen valtion oikeudesta esittämiin toteamuksiin, sillä ne voivat vaihdella niitä esittävän kansallisen tuomioistuimen mukaan.

246. Katson näillä perusteilla, että kun vastaus unionin toimen pätevyydestä esitettyyn ennakkoratkaisukysymykseen edellyttää kolmannen valtion oikeuden sisällön arvioimista, unionin tuomioistuin ei ole sidottu ennakkoratkaisua pyytäneen tuomioistuimen esittämiin toteamuksiin tämän kolmannen valtion oikeudesta, vaikka se voikin ottaa ne huomioon. Unionin tuomioistuin voi tarvittaessa poiketa niistä tai täydentää niitä ottamalla huomioon kontradiktorista periaatetta noudattaen muita lähteitä kyseessä olevan toimen pätevyyden arvioimisen kannalta tarpeellisten seikkojen toteamiseksi.[113]

4) ”Pääosiltaan vastaavaa” tasoa koskevan vaatimuksen ulottuvuus

247. Muistutettakoon, että Privacy Shield -päätöksen pätevyys riippuu siitä, taataanko Yhdysvaltojen oikeusjärjestyksessä henkilöille, joiden tietoja siirretään unionista tähän kolmanteen maahan, ”pääosiltaan vastaava” suojan taso kuin jäsenvaltioissa taataan tietosuoja-asetuksen ja perusoikeuskirjan nojalla sekä unionin oikeuden soveltamisalan ulkopuolelle jäävillä aloilla niiden Euroopan ihmisoikeussopimukseen perustuvien sitoumusten nojalla.

248. Kuten unionin tuomioistuin korostaa tuomiossa Schrems,[114] tämä vaatimus ei merkitse sitä, että suojan tason olisi oltava ”täysin sama” kuin unionissa edellytetty taso. Vaikka keinot, joita kolmas maa käyttää rekisteröityjen oikeuksien suojaamiseksi, voivat poiketa niistä, joista tietosuoja-asetuksessa, luettuna perusoikeuskirjan valossa, säädetään, näiden ”keinojen on käytännössä osoittauduttava tehokkaiksi takaamaan suoja, joka pääosiltaan vastaa unionissa taattua suojaa”.

249. Mielestäni tästä seuraa niin ikään, että kohdemaana olevan kolmannen valtion oikeus voi heijastaa sen omaa arvoasteikkoa, jonka mukaan kyseessä olevien eri etujen painoarvo voi poiketa unionin oikeusjärjestyksessä niille annetusta painoarvosta. Unionissa annettu henkilötietojen suoja vastaa erityisen korkeaa vaatimusta verrattuna muualla maailmassa voimassa olevaan suojan tasoon. Siksi ”pääosiltaan vastaavaa” koskevaa kriteeriä pitäisi mielestäni soveltaa siten, että tietty joustavuus säilyy erilaisten oikeudellisten ja kulttuuristen perinteiden huomioon ottamiseksi. Jotta tämän kriteerin sisältöä ei tehtäisi tyhjäksi, se edellyttää kuitenkin, että tietyillä perusoikeuskirjasta ja Euroopan ihmisoikeussopimuksesta seuraavilla perusoikeuksien suojaamista koskevilla vähimmäistakeilla ja yleisillä vaatimuksilla on vastineensa kohdemaana olevan kolmannen maan oikeusjärjestyksessä.[115]

111 Ks. tältä osin Supreme Courtin tuomio 31.5.2019 (6.18 kohta).

112 Ks. tuomio 13.5.1981, International Chemical Corporation (66/80, EU:C:1981:102, 12 ja 13 kohta).

113 Ks. tältä osin tuomio 22.3.2012, GLS (C-338/10, EU:C:2012:158, 15, 33 ja 34 kohta), jossa arvioidessaan polkumyyntitullin käyttöön ottamisesta annetun asetuksen pätevyyttä unionin tuomioistuin otti huomioon Eurostatin tilastot, jotka komissio oli toimittanut unionin tuomioistuimen pyynnöstä. Ks. myös tuomio 22.10.1991, Nölle (C-16/90, EU:C:1991:402, 17, 23 ja 24 kohta). Myös tuomiossa Schrems (90 kohta) unionin tuomioistuin otti huomioon safe harbor -päätöksen pätevyyttä arvioidessaan tietyt komission tiedonannot.

114 Tuomio Schrems (73 ja 74 kohta).

115 Ks. vastaavasti tietosuojatyöryhmä, ”Adequacy Referential (updated)”, 28.11.2017, WP 254 (s. 3, 4 ja 9).

250. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa vahvistettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen, ja suhteellisuusperiaatteen mukaisesti näiden rajoitusten on oltava välttämättömiä ja vastattava tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Nämä vaatimukset vastaavat olennaisesti Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleessa asetettuja vaatimuksia. [116]

251. Siltä osin kuin perusoikeuskirjan 7, 8 ja 47 artiklassa taatut oikeudet vastaavat Euroopan ihmisoikeussopimuksen 8 ja 13 artiklassa vahvistettuja oikeuksia, niillä on perusoikeuskirjan 52 artiklan 3 kohdan mukaisesti sama merkitys ja ulottuvuus, mutta unionin oikeudessa voidaan kuitenkin myöntää tätä laajempi suoja. Kuten jäljempänä esittämästäni selostuksesta ilmenee, tältä kannalta perusoikeuskirjan 7, 8 ja 47 artiklasta seuraavat vaatimukset, sellaisina kuin unionin tuomioistuin on niitä tulkinnut, ovat tietyiltä osin ankarampia kuin Euroopan ihmisoikeussopimuksen 8 artiklasta seuraavat vaatimukset Euroopan ihmisoikeustuomioistuimen sille antaman tulkinnan mukaan.

252. Huomattakoon myös, että kummallakin näistä tuomioistuimista on niissä vireillä olevien asioiden johdosta tilaisuus harkita uudelleen joitakin oikeuskäytäntönsä näkökohtia. Euroopan ihmisoikeustuomioistuimen kaksi viimeaikaista tuomiota, jotka koskevat sähköisen viestinnän valvontaa – tuomio Centrum för Rättvisa v. Ruotsi [117] ja tuomio Big Brother Watch v. Yhdistynyt kuningaskunta [118] – on palautettu uudelleen käsittelyä varten suureen jaostoon. Toisaalta kolme kansallista tuomioistuinta on esittänyt unionin tuomioistuimelle ennakkoratkaisupyynnöt, joilla aloitetaan näkemystenvaihto siitä, onko sen tuomioon Tele2 Sverige perustuvaa oikeuskäytäntöä tarpeen muuttaa vai ei. [119]

253. Näiden täsmennysten jälkeen tarkastelen seuraavaksi Privacy Shield -päätöksen pätevyyttä tietosuoja-asetuksen 45 artiklan 1 kohdan kannalta, luettuna perusoikeuskirjan ja Euroopan ihmisoikeussopimuksen valossa siltä osin kuin niissä taataan oikeus yksityiselämän kunnioittamiseen ja henkilötietojen suojaan (osa b) sekä oikeus tehokkaaseen oikeussuojaan (osa c).

b) Privacy Shield -päätöksen pätevyys yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevien oikeuksien kannalta

254. Neljännellä kysymyksellään ennakkoratkaisua pyytänyt tuomioistuin kyseenalaistaa ennen kaikkea sen, että Yhdysvalloissa taattu suojan taso vastaisi pääosiltaan sen suojan tasoa, jonka rekisteröidyt saavat unionissa yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeville perusoikeuksilleen.

1) Puuttumisen olemassaolo

255. Privacy Shield -päätöksen johdanto-osan 67–124 perustelukappaleessa komissio viittaa mahdollisuuteen, että Yhdysvaltojen viranomaiset saavat pääsyn unionista siirrettäviin tietoihin ja käyttävät niitä kansallista turvallisuutta varten erityisesti FISA:n 702 §:ään tai EO 12333:een perustuvien ohjelmien yhteydessä.

116 Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleessa ei kuitenkaan viitata yksityiselämän kunnioitusta koskevan oikeuden ”keskeiseen sisältöön”. Ks. tästä tämän ratkaisuehdotuksen alaviite 161.

117 Euroopan ihmisoikeustuomioistuimen tuomio 19.6.2018 (CE:ECHR:2018:0619JUD003525208; jäljempänä tuomio Centrum för Rättvisa).

118 Euroopan ihmisoikeustuomioistuimen tuomio 13.9.2018 (CE:ECHR:2018:0913JUD005817013; jäljempänä tuomio Big Brother Watch).

119 Ks. tämän ratkaisuehdotuksen alaviitteessä 98 mainitut asiat ja asia C-520/18, Ordre des barreaux francophones et germanophones ym. (EUVL 2018, C 408, s. 39).

256. Näiden ohjelmien täytäntöönpano merkitsee Yhdysvaltojen viranomaisten harjoittamaa tunkeutumista, jota pidettäisiin puuttumisena perusoikeuskirjan 7 artiklassa ja Euroopan ihmisoikeussopimuksen 8 artiklassa taattuun yksityiselämän kunnioittamista koskevaan oikeuteen, jos se olisi jäsenvaltion viranomaisten toteuttamaa. Se myös altistaa rekisteröidyt riskille, että heidän henkilötietojaan käsitellään tavalla, joka ei täytä perusoikeuskirjan 8 artiklassa asetettuja vaatimuksia. [120]

257. Täsmennän heti alkuun, että oikeus yksityiselämän kunnioittamiseen ja oikeus henkilötietojen suojaan käsittävät paitsi viestinnän sisällön suojan myös liikennetietojen [121] ja paikkatietojen (joihin viitataan yhdessä käsitteellä metatiedot) suojan. Sekä unionin tuomioistuin että Euroopan ihmisoikeustuomioistuin ovat katsoneet, että metatiedot voivat sisältöä koskevien tietojen tavoin paljastaa hyvin tarkkoja tietoja henkilön yksityiselämästä. [122]

258. Unionin tuomioistuimen oikeuskäytännön mukaan perusoikeuskirjan 7 artiklassa taatun oikeuden käyttämiseen puuttumisen osoittamisessa merkitystä ei ole sillä, ovatko kyseiset tiedot arkaluonteisia vai eivät ja onko asianomaisille henkilöille mahdollisesti aiheutunut haittaa kyseisestä tarkkailutoimenpiteestä. [123]

259. FISA:n 702 §:ään perustuvat tarkkailuohjelmat merkitsevät ensisijaisesti puuttumista henkilöiden perusoikeuksien käyttöön, kun heidän viestintänsä vastaa NSA:n määrittämiä valintakriteerejä ja sähköisten viestintäpalvelujen tarjoajat toimittavat sen näin ollen NSA:lle. [124] Koska palveluntarjoajille asetetulla velvollisuudella *saattaa* tiedot NSA:n *saataville* poiketaan viestinnän luottamuksellisuuden periaatteesta, [125] se merkitsee itsessään perusoikeuksiin puuttumista, vaikka tiedusteluviranomaiset eivät myöhemmin tutustuisi näihin tietoihin ja käyttäisi niitä. [126] Yhtä lailla se, että nämä viranomaiset *säilyttävät* saatavilleen saatetut metatiedot ja viestinnän sisällön ja niillä on tosiasiallinen *pääsy* niihin, samoin kuin se, että ne *käyttävät* näitä tietoja, merkitsevät myös perusoikeuksiin puuttumista. [127]

260. Lisäksi ennakkoratkaisua pyytäneen tuomioistuimen esittämien toteamusten [128] ja muiden lähteiden, kuten Yhdysvaltojen hallituksen unionin tuomioistuimelle toimittaman, FISA:n 702 §:n nojalla toteutettuja ohjelmia koskevan PCLOB:n raportin, [129] mukaan NSA:lla on jo Upstream-ohjelman perusteella tietojen *suodatusta varten pääsy* laajoihin tietoaineistoihin (ns. tietopaketteihin), jotka ovat osa televiestinnän runkoverkon kautta kulkevaa viestintävirtaa ja käsittävät viestintää, johon ei sisälly NSA:n yksilöimiä valintakriteerejä. NSA voi tutkia nämä tietoaineistot vain nopeasti selvittääkseen automatisoidulla tavalla, sisältävätkö ne näitä

120 Vaikka käsittely voi olla samalla perusoikeuskirjan 7 ja 8 artiklan vastaista, 8 artiklan soveltamisen kannalta merkityksellinen tarkastelutapa poikkeaa rakenteellisesti 7 artiklaan liittyvästä tarkastelutavasta. Oikeus henkilötietojen suojaan merkitsee perusoikeuskirjan 8 artiklan 2 kohdan mukaan sitä, että ”tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla” ja että ”jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi”. Tämän oikeuden loukkaaminen edellyttää, että henkilötietoja käsitellään näiden vaatimusten vastaisesti. Näin on etenkin silloin, jos käsittely ei perustu asianomaisen henkilön suostumukseen *tai muuhun laissa säädettyyn oikeuttavaan perusteeseen*. Tällaisessa tilanteessa, vaikka kysymys puuttumisen olemassaolosta ja kysymys sen oikeuttamisesta poikkeavat 7 artiklan yhteydessä käsitteellisesti toisistaan, perusoikeuskirjan 8 artiklan tapauksessa ne ovat päällekkäisiä.

121 Direktiivin 2002/58 2 artiklan toisen kohdan b alakohdan mukaan ”liikennetiedoilla” tarkoitetaan ”tietoja, joita käsitellään sähköisessä viestintäverkossa välitettävää viestintää tai sen laskutusta varten”.

122 Ks. tuomio 8.4.2014, Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238; jäljempänä tuomio Digital Rights Ireland; 27 kohta) ja tuomio Tele2 Sverige (99 kohta). Ks. myös Euroopan ihmisoikeustuomioistuimen tuomio 2.8.1984, Malone v. Yhdistynyt kuningaskunta (CE:ECHR:1984:0802JUD000869179, 84 kohta) ja Euroopan ihmisoikeustuomioistuimen tuomio 8.2.2018, Ben Faiza v. Ranska (CE:ECHR:2018:0208JUD00344612, 66 kohta).

123 Ks. tuomio Digital Rights Ireland (33 kohta); lausunto 1/15 (124 kohta) ja tuomio Ministerio Fiscal (51 kohta).

124 Ks. Privacy Shield -päätöksen johdanto-osan 78–81 perustelukappale ja liitteessä VI oleva II kohta.

125 Ks. tältä osin tuomio Digital Rights Ireland (32 kohta).

126 Ks. vastaavasti lausunto 1/15 (124 ja 125 kohta), josta ilmenee, että tietojen välittäminen kolmannelle merkitsee puuttumista asianomaisten henkilöiden perusoikeuksien käyttöön tietojen myöhemmästä käytöstä riippumatta.

127 Ks. vastaavasti tuomio Digital Rights Ireland (35 kohta); tuomio Schrems (87 kohta) ja lausunto 1/15 (123–126 kohta).

128 Ks. tämän ratkaisuehdotuksen 60 kohta.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2.7.2014 (jäljempänä PCLOB:n raportti, s. 84 ja 111). Ks. myös tietosuojatyöryhmä, EU-U.S. Privacy Shield – First Annual Joint Review, 28.11.2017, WP 255 (B.1.1 kohta, s. 15).

valintakriteerejä. Tällöin ainoastaan näin suodatettu viestintä tallennetaan NSA:n tietokantoihin. Mielestäni myös tämä tietoihin pääsy niiden suodatusta varten merkitsee puuttumista rekisteröityjen yksityiselämän kunnioittamista koskevan oikeuden käyttöön säilytettyjen tietojen myöhemmästä käytöstä riippumatta.[130]

261. Kyseessä olevien tietojen saataville saattaminen ja suodattaminen,[131] tiedusteluviranomaisten pääsy näihin tietoihin sekä kyseisten tietojen mahdollinen säilyttäminen, analysoiminen ja käyttö kuuluvat tietosuoja-asetuksen 4 artiklan 2 alakohdassa ja perusoikeuskirjan 8 artiklan 2 kohdassa tarkoitetun käsittelyn käsitteen alaan. Näiden käsittelyjen on näin ollen täytettävä tässä viimeksi mainitussa määräyksessä asetetut vaatimukset.[132]

262. EO 12333:een perustuva tarkkailu voisi puolestaan edellyttää tiedusteluviranomaisten suoraa pääsyä siirrettäviin tietoihin, mikä merkitsisi puuttumista Euroopan ihmisoikeussopimuksen 8 artiklassa taatun oikeuden käyttöön. Tämän puuttumisen lisäksi myös näiden tietojen mahdollinen myöhempi käyttö merkitsisi tällaista puuttumista.

2) Puuttumisesta säätäminen lailla

263. Unionin tuomioistuimen oikeuskäytännön[133] ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön[134] mukaan vaatimus, jonka mukaan perusoikeuksien käyttämiseen voidaan puuttua ainoastaan lailla perusoikeuskirjan 52 artiklan 1 kohdassa ja Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleessa tarkoitetulla tavalla, merkitsee paitsi sitä, että tämän puuttumisen mahdollistavalla toimenpiteellä on oltava oikeusperusta kansallisessa oikeudessa, myös sitä, että tähän oikeusperustaan on voitava liittää tiettyjä saatavuuden ja ennakoitavuuden omaisuuksia, jotta riski mielivallasta vältetään.

264. Tältä osin asianosaiset ja osapuolet, jotka ovat esittäneet huomautuksia unionin tuomioistuimessa, ovat eri mieltä lähinnä siitä, täyttävätkö FISA:n 702 § ja EO 12333 lain ennakoitavuutta koskevan edellytyksen.

265. Tämä edellytys, sellaisena kuin unionin tuomioistuin[135] ja Euroopan ihmisoikeustuomioistuin[136] ovat sitä tulkinneet, edellyttää, että säännöstö, joka merkitsee puuttumista yksityiselämän kunnioittamista koskevan oikeuden käyttöön, sisältää selvät ja täsmälliset kyseessä olevan toimenpiteen laajuutta ja soveltamista koskevat säännöt, joissa asetetaan vähimmäisvaatimukset, jotta asianomaiset henkilöt saavat riittävät takeet tietojensa suojaamiseksi väärinkäytön vaaroilta sekä kaikenlaiselta

130 Ks. tämän ratkaisuehdotuksen alaviite 126.

131 Ks. tästä tämän ratkaisuehdotuksen 222 kohta.

132 Ks. lausunto 1/15 (123 kohta oikeuskäytäntöviittauksineen).

133 Ks. mm. lausunto 1/15 (146 kohta).

134 Ks. mm. Euroopan ihmisoikeustuomioistuimen tuomio 2.8.1984, Malone v. Yhdistynyt kuningaskunta (CE:ECHR:1984:0802JUD000869179, 66 kohta); Euroopan ihmisoikeustuomioistuimen päätös 29.6.2006, Weber ja Saravia v. Saksa (CE:ECHR:2006:0629DEC005493400; jäljempänä päätös Weber ja Saravia; 84 kohta oikeuskäytäntöviittauksineen) ja Euroopan ihmisoikeustuomioistuimen tuomio 4.12.2015, Zakharov v. Venäjä (CE:ECHR:2015:1204JUD004714306; jäljempänä tuomio Zakharov; 228 kohta).

135 Ks. mm. tuomio Digital Rights Ireland (54 ja 65 kohta); tuomio Schrems (91 kohta); tuomio Tele2 Sverige (109 kohta) ja lausunto 1/15 (141 kohta).

136 Ks. mm. päätös Weber ja Saravia (94 ja 95 kohta); tuomio Zakharov (236 kohta) ja Euroopan ihmisoikeustuomioistuimen tuomio 12.1.2016, Szabó ja Vissy v. Unkari (CE:ECHR:2016:0112JUD003713814; jäljempänä tuomio Szabó ja Vissy; 59 kohta).

näiden tietojen laittomalta saannilta tai käytöltä. Näissä säännöissä on erityisesti ilmoitettava, missä olosuhteissa ja millä edellytyksillä viranomaiset voivat säilyttää henkilötietoja, päästä niihin ja käyttää niitä.[137] Itse siinä oikeusperustassa, joka mahdollistaa puuttumisen, on määritettävä yksityiselämän kunnioittamista koskevan oikeuden käyttämiselle asettavien rajoitusten laajuus.[138]

266. Minulla on Schremsin ja EPIC:n tavoin epäilyksiä sen suhteen, ovatko EO 12333 sekä PPD 28, jossa vahvistetaan kaikkeen signaalitiedustelutoimintaan liittyvät suojatoimet,[139] riittävän ennakoitavissa, jotta niitä voitaisiin pitää lakeina.

267. Näissä oikeudellisissa välineissä todetaan nimenomaisesti, että niillä ei anneta asianomaisille henkilöille oikeudellisesti täytäntöönpanokelpoisia oikeuksia.[140] Nämä henkilöt eivät siis voi vedota PPD 28:ssa tarkoitettuihin suojatoimiin tuomioistuimissa.[141] Komissio toteaa Privacy Shield -päätöksessä lisäksi, että vaikka tässä presidentin määräyksessä tarkoitetut suojatoimet sitovat tiedustelupalveluja,[142] niitä ”ei ole ilmaistu oikeudellisin termein”.[143] EO 12333 ja PPD 28 muistuttavat ennen kaikkea sisäisiä hallinnollisia ohjeita, jotka Yhdysvaltojen presidentti voi kumota tai muuttaa. Euroopan ihmisoikeustuomioistuin on jo todennut, että sisäiset hallinnolliset määräykset eivät ole ”lakeja”.[144]

268. Siltä osin kuin kyse on FISA:n 702 §:stä Schrems on kyseenalaistanut tämän säännöksen ennakoitavuuden sillä perusteella, että siinä ei liitetä tietojen suodattamiseksi käytettyjen valintakriteerien määrittämiseen riittäviä suojatoimia väärinkäytön vaaroja vastaan. Koska tämä kysymyksenasettelu liittyy myös siihen, onko FISA:n 702 §:ssä tarkoitettu puuttuminen täysin välttämätöntä, tarkastelen sitä jäljempänä tässä esityksessäni.[145]

269. Kolmas ennakkoratkaisukysymys leikkaa aihepiiriä, joka liittyy ”lakia” koskevan edellytyksen noudattamiseen. Tällä kysymyksellä ennakkoratkaisua pyytänyt tuomioistuin pyrkii ennen kaikkea selvittämään, onko kolmannessa maassa varmistetun tietosuojan riittävyyttä tutkittava pelkästään tässä kolmannessa maassa voimassa olevien oikeudellisesti sitovien sääntöjen ja niiden noudattamisen varmistamiseksi tarkoitettujen käytäntöjen kannalta vai myös erilaisten muiden kuin sitovien välineiden ja niihin sovellettujen tuomioistuimen ulkopuolisten valvontamekanismien kannalta.

137 Ks. tuomio Tele2 Sverige (117 kohta) ja lausunto 1/15 (190 kohta). Ks. myös mm. Euroopan ihmisoikeustuomioistuimen tuomio 2.8.1984, Malone v. Yhdistynyt kuningaskunta (CE:ECHR:1984:0802JUD000869179, 67 kohta); tuomio Zakharov (229 kohta) ja tuomio Szabó ja Vissy (62 kohta). Euroopan ihmisoikeustuomioistuin täsmentää niissä, että ennakoitavuuden vaatimuksella ei ole samaa sisältöä viestinnän kaappauksen yhteydessä kuin muilla aloilla. Salaisen tarkkailun yhteydessä ”ennakoitavuuden vaatimus ei voi tarkoittaa sitä, että jonkin tahon olisi saatava ennakoida, onko – ja milloin – sen viestintä vaarassa joutua viranomaisten kaappaamaksi, jotta se voisi säännellä toimintaansa sen mukaisesti”.

138 Lausunto 1/15 (139 kohta). Ks. vastaavasti myös Euroopan ihmisoikeustuomioistuimen tuomio 25.3.1983, Silver ym. v. Yhdistynyt kuningaskunta (CE:ECHR:1983:0325JUD000594772, 88 ja 89 kohta).

139 Privacy Shield -päätöksen johdanto-osan 69–77 perustelukappaleessa ja liitteessä VI olevassa I kohdassa on selostus PPD 28:sta. Siinä täsmennetään, että tätä presidentin määräystä sovelletaan sekä FISA:n 702 §:ään perustuvaan tiedustelutoimintaan että Yhdysvaltojen alueen ulkopuolella tapahtuvaan tiedustelutoimintaan.

140 EO 12333:n 3.7 kohdan c alakohdassa todetaan seuraavaa: ”[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person”. Lisäksi PPD 28:n 6 §:n d alakohdassa säädetään seuraavaa: ”This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person”.

141 Ks. vastaavasti Euroopan tietosuojaneuvosto, EU-U.S. Privacy Shield – Second Annual Joint Review, 22.1.2019 (99 kohta).

142 Ks. Privacy Shield -päätöksen johdanto-osan 69 ja 77 perustelukappale.

143 Privacy Shield -päätöksen johdanto-osan 76 perustelukappale.

144 Ks. Euroopan ihmisoikeustuomioistuimen tuomio 25.3.1983, Silver ym. v. Yhdistynyt kuningaskunta (CE:ECHR:1983:0325JUD000594772, 26 ja 86 kohta).

145 Ks. tämän ratkaisuehdotuksen 295–301 kohta. Tuomiossa Tele2 Sverige (116 ja 117 kohta) ja lausunnossa 1/15 (140 ja 141 kohta) lain ennakoitavuuden vaatimuksen on esitetty liittyvän erottamattomasti puuttumisen välttämättömyyttä ja oikeasuhteisuutta koskevaan edellytykseen. Vastaavasti Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan tehokkaat takeet väärinkäytön vaaroja vastaan liittyvät edellytyksiin sekä puuttumisen ”ennakoitavuudesta” että sen ”välttämättömyydestä demokraattisessa yhteiskunnassa”, minkä vuoksi kummankin edellytyksen noudattamista on tutkittava yhdessä. Ks. mm. Euroopan ihmisoikeustuomioistuimen tuomio 18.5.2010, Kennedy v. Yhdistynyt kuningaskunta (CE:ECHR:2010:0518JUD002683905, 155 kohta); tuomio Zakharov (236 kohta); tuomio Centrum för Rättvisa (107 kohta) ja tuomio Big Brother Watch (322 kohta).

270. Tietosuoja-asetuksen 45 artiklan 2 kohdan a alakohdassa on tältä osin luettelo, joka ei ole tyhjentävä, seikoista, jotka komission on otettava huomioon arvioidessaan kolmannen maan tarjoaman tietosuojan tason riittävyyttä. Näihin seikkoihin kuuluvat sovellettava lainsäädäntö ja tapa, jolla se on pantu täytäntöön. Tässä säännöksessä mainitaan myös muunkaltaisten normien, kuten ammatillisten sääntöjen ja turvatoimien, vaikutus. Lisäksi siinä vaaditaan ottamaan huomioon ”vaikuttavat ja täytäntöönpanokelpoiset oikeudet” ja ”tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot niitä rekisteröityjä varten, joiden henkilötietoja siirretään”. [146]

271. Kun kyseinen säännös luetaan kokonaisuutena ja otetaan huomioon, ettei sen sisältämä luettelo ole tyhjentävä, nähdäkseni se tarkoittaa sitä, että käytännöt tai välineet, jotka eivät perustu saatavilla ja ennakoitavissa olevaan oikeusperustaan, voidaan ottaa huomioon kyseessä olevan kolmannen maan takaaman suojan tason kokonaisarvioinnissa siten, että tuetaan suojatoimia, joilla itsellään on saatavilla ja ennakoitavissa oleva oikeusperusta. Kuten DPC, Schrems, Itävallan hallitus ja Euroopan tietosuojaneuvosto väittävät, tällaiset välineet tai käytännöt eivät sen sijaan voi korvata tällaisia suojatoimia eikä niillä itsellään voida näin ollen varmistaa vaadittua suojan tasoa.

3) Perusoikeuksien keskeistä sisältöä ei ole loukattu

272. Perusoikeuskirjan 52 artiklan 1 kohdassa asetettu vaatimus, jonka mukaan perusoikeuskirjassa taattuja oikeuksia tai vapauksia voidaan rajoittaa ainoastaan kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen, merkitsee sitä, että kun niihin puututaan, sitä ei voida perustella millään oikeutetulla tavoitteella. Puuttuminen katsotaan silloin perusoikeuskirjan vastaiseksi ilman, että olisi tutkittava, voidaanko sillä toteuttaa tavoiteltu päämäärä ja onko se tarpeellinen sen toteuttamiseksi.

273. Unionin tuomioistuin on tältä osin todennut, että kansallisella säännöstöllä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän *sisältöön*, loukataan perusoikeuskirjan 7 artiklassa taatun yksityiselämän kunnioittamista koskevan oikeuden keskeistä sisältöä. [147] Sen sijaan unionin tuomioistuin on korostaessaan *liikenne- ja paikkatietoihin* pääsyyn ja niiden analysointiin liittyviä riskejä [148] katsonut, että tämän oikeuden keskeistä sisältöä ei loukata, kun kansallisessa säännöstössä annetaan viranomaisille yleinen pääsy näihin tietoihin. [149]

274. Nyt esillä olevassa asiassa FISA:n 702 §:ssä ei mielestäni voida katsoa annettavan Yhdysvaltojen tiedusteluviranomaisille yleistä pääsyä sähköisen viestinnän sisältöön.

275. Yhtäältä tiedusteluviranomaisten pääsy tietoihin FISA:n 702 §:n nojalla niiden mahdollista *analysointia ja käyttöä varten* on rajattu tietoihin, jotka vastaavat yksittäisiin kohteisiin liittyviä valintakriteerejä.

146 Ks. myös tietosuoja-asetuksen johdanto-osan 104 perustelukappale.

147 Ks. tuomio Schrems (94 kohta) Ks. myös tuomio Digital Rights Ireland (39 kohta) ja tuomio Tele2 Sverige (101 kohta). Kun otetaan huomioon yksityiselämän kunnioittamista koskevan oikeuden läheinen yhteys henkilötietojen suojaa koskevaan oikeuteen, kansallisella toimenpiteellä, jolla viranomaisille annetaan yleinen pääsy viestinnän sisältöön, loukattaisiin nähdäkseni myös perusoikeuskirjan 8 artiklassa vahvistetun oikeuden keskeistä sisältöä.

148 Ks. tämän ratkaisuehdotuksen 257 kohta. Tuomiossa Tele2 Sverige (99 kohta) unionin tuomioistuin korosti, että metatietojen perusteella voidaan erityisesti laatia asianomaisten henkilöiden profiili. Tietosuojatyöryhmä totesi 10.4.2014 antamassaan lausunnossa 04/2014 sähköisen viestinnän valvonnasta tiedustelua ja kansallista turvallisuutta varten, WP 215 (s. 5), että metatietojen vertailu ja analysointi on niiden järjestyneisyyden vuoksi helpompaa kuin sisältöä koskevien tietojen vertailu ja analysointi.

149 Ks. tuomio Tele2 Sverige (99 kohta). Jotkut kommentoijat ovat pohtineet, onko perusteltua erotella yleinen pääsy viestinnän sisältöön ja yleinen pääsy metatietoihin, kun otetaan huomioon teknologian ja viestintätapojen kehitys. Ks. Falot, N. ja Hijmans, H., ”Tele2: de afweging tussen privacy en veiligheid nader omlijnd”, *Nederlands Tijdschrift voor Europees Recht*, nro 3, 2017 (s. 48) ja Ojanen, T., ”Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter” (tuomion Schrems kommentti), *European Constitutional Law Review*, 2016 (s. 5).

276. Toisaalta Upstream-ohjelma voisi tosin merkitä yleistä pääsyä sähköisen viestinnän sisältöön *automatisoitua suodatusta varten* tilanteessa, jossa valintakriteerejä sovellettaisiin paitsi ”lähtevään” ja ”saapuvaan” viestintään, myös viestintävirran kaikkeen sisältöön (jolloin haku ”koskee” valintakriteeriä).[150] Kuten komissio väittää ja toisin kuin Schrems ja EPIC esittävät, tiedusteluviranomaisten tilapäistä pääsyä kaikkeen sähköisen viestinnän sisältöön pelkästään sen suodattamiseksi valintakriteerejä soveltamalla ei kuitenkaan voida rinnastaa yleiseen pääsyyn tähän sisältöön.[151] Mielestäni puuttuminen, joka seuraa tästä ajallisesti rajoitetusta pääsystä automatisoitua suodatusta varten, ei ole yhtä vakavaa kuin puuttuminen, joka seuraa viranomaisten yleisestä pääsystä tähän sisältöön sen analysointia ja mahdollista käyttöä varten.[152] Tilapäinen pääsy suodatusta varten ei anna näille viranomaisille oikeutta säilyttää valintakriteerejä vastaamattoman viestinnän metatietoja tai sisältöä eikä etenkään, kuten Yhdysvaltojen hallitus huomauttaa, laatia profiileja henkilöistä, joihin näitä kriteerejä ei ole kohdennettu.

277. Kysymys siitä, rajoittaako kohdentaminen valintakriteereillä FISA:n 702 §:ään perustuvien ohjelmien yhteydessä tehokkaasti tiedusteluviranomaisten toimivaltuuksia, riippuu kuitenkin valintakriteerien määrittämisen rajaamisesta.[153] Schrems väittää tältä osin, että koska tässä tarkoituksessa ei ole riittävää valvontaa, Yhdysvaltojen oikeudessa ei ole säädetty suojatoimista sitä vastaan, että viestinnän sisältöön on yleinen pääsy jo suodatusvaiheessa, minkä vuoksi sillä loukataan rekisteröityjen yksityiselämän kunnioittamista koskevan oikeuden keskeistä sisältöä.

278. Kuten selostan yksityiskohtaisemmin jäljempänä,[154] olen taipuvainen yhtymään näihin epäilyihin sen suhteen, onko valintakriteerien määrittämistä rajattu riittävästi, jotta puuttumisen ennakoitavuuden ja oikeasuhteisuuden edellytykset täyttyisivät. Tällainen epätäydellinenkin rajaaminen on kuitenkin esteenä johtopäätökselle, jonka mukaan FISA:n 702 §:ssä annetaan viranomaisille yleinen pääsy sähköisen viestinnän sisältöön ja että se siten merkitsisi perusoikeuskirjan 7 artiklassa vahvistetun oikeuden keskeisen sisällön loukkaamista.

279. Korostan myös, että unionin tuomioistuin totesi lausunnossa 1/15, että perusoikeuskirjan 8 artiklassa taatun henkilötietojen suojaa koskevan oikeuden keskeinen sisältö säilytetään, kun käsittelyn tarkoitukset on rajattu ja kun käsittelyyn liittyy sääntöjä, joilla on tarkoitus varmistaa muun muassa tietoturva ja näiden tietojen luottamuksellisuus ja eheys ja suojata niitä siltä, että niihin pääsisiin ja niitä käsiteltäisiin laittomasti.[155]

150 Ks. Privacy Shield -päätöksen alaviite 87. EPIC:n huomautusten ja Yhdysvaltojen hallituksen unionin tuomioistuimen esittämiin kysymyksiin antaman kirjallisen vastauksen mukaan FISC on kuitenkin vuonna 2017 vaatinut keskeyttämään valintakriteeriä ”koskevat” haut tämänkaltaisiin hakuihin liittyvien sääntöjenvastaisuuksien vuoksi. Kongressi on kuitenkin säätänyt vuonna 2018 antamassaan FISA:n uudelleen hyväksymistä koskevassa toimessa mahdollisuudesta ottaa uudelleen käyttöön tämänkaltaiset haut FISC:n ja kongressin suostumuksella. Ks. myös Euroopan tietosuojaneuvosto, EU-U.S. Privacy Shield – Second Annual Joint Review, 22.1.2019 (s. 27, 55 kohta).

151 Tässä tarkoituksessa ennakkoratkaisua pyytänyt tuomioistuin erottelee 3.10.2017 antamansa tuomion 188 ja 189 kohdassa toisistaan valikoimattoman haun ja valikoimattoman hankinnan, keruun tai säilyttämisen. Kyseinen tuomioistuin katsoo ennen kaikkea, että vaikka Upstream-ohjelma merkitsee valikoimatonta hakua kaikesta televiestinnän runkoverkon kautta kulkevasta tietovirrasta, hankinta, keruu ja säilyttäminen ovat kohdennettuja siltä osin kuin ne koskevat ainoastaan kyseessä olevat valintakriteerit sisältäviä tietoja.

152 Ks. vastaavasti Supreme Courtin tuomio 31.5.2019 (11.2 ja 11.3 kohta). Kyseinen tuomioistuin toteaa siinä seuraavaa: ”[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term “processing” covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis.”

153 Ks. lausunto 1/15 (122 kohta). Ks. myös Euroopan komission Demokratiaa oikeusteitse -komission (Venetsian komissio) 15.12.2015 laatima raportti signaalitiedustelusta vastaavien elinten demokraattisesta valvonnasta, tutkimus nro 719/2013 (CDL-AD(2015)011), s. 11): ”Käytännössä pyrittäessä selvittämään, rajoitetaanko tällä menettelyllä sopivasti viattomaan henkilökohtaiseen viestintään kohdistuvaa tarpeetonta tunkeutumista, on määritettävä, onko valintakriteeri riittävän merkityksellinen ja tarkka ja onko valittujen parametrien puitteissa merkityksellisten tietojen yksilöimiseen käytetty ohjelmistoalgoritmi laadultaan tyydyttävä – –”.

154 Ks. tämän ratkaisuehdotuksen 297–301 kohta.

155 Lausunto 1/15 (150 kohta).

280. Komissio toteaa Privacy Shield -päätöksessä, että sekä FISA:n 702 §:ssä että PPD 28:ssa rajoitetaan käyttötarkoituksia, joihin tietoja voidaan kerätä FISA:n 702 §:n nojalla täytäntöön pantujen ohjelmien puitteissa.[156] Komissio toteaa siinä myös, että PPD 28:ssa vahvistetaan sääntöjä, jotka rajoittavat tietoihin pääsyä ja niiden säilyttämistä ja levittämistä tietoturvan varmistamiseksi ja luvattomalta pääsyltä suojaamiseksi.[157] Kuten jäljempänä tästä esityksestäni käy ilmi,[158] pidän kyseenalaisena erityisesti sitä, onko kyseessä olevien käsittelyjen tarkoitukset määritelty niin selvästi ja tarkasti, että voidaan varmistaa suojan taso, joka pääosiltaan vastaa unionin oikeusjärjestyksessä vallitsevaa suojan tasoa. Nämä mahdolliset puutteellisuudet eivät kuitenkaan mielestäni riittäisi perusteeksi toteamukselle, jonka mukaan tällaiset ohjelmat loukkaisivat, jos ne toteutettaisiin unionissa, henkilötietojen suojaa koskevan oikeuden keskeistä sisältöä.

281. On syytä muistaa, että EO 12333:een perustuvan tarkkailutoiminnan yhteydessä varmistetun tietosuojan riittävyyttä on arvioitava Euroopan ihmisoikeussopimuksen määräysten kannalta. Tältä osin Privacy Shield -päätöksestä ilmenee, että ainoat rajoitukset, jotka koskevat EO 12333:een perustuvien toimenpiteiden täytäntöönpanoa ei-yhdysvaltalaisia henkilöitä koskevien tietojen keräämiseksi, on asetettu PPD 28:ssa.[159] Tämän presidentin määräyksen mukaan ulkomaantiedustelutiedon käytön on oltava ”mahdollisimman räätälöityä”. Siinä mainitaan kuitenkin nimenomaisesti mahdollisuus kerätä tietoja ”valikoimattomasti” Yhdysvaltojen alueen ulkopuolella tiettyjen kansallista turvallisuutta koskevien erityisten tavoitteiden saavuttamiseksi.[160] Schremsin mukaan PPD 28:n, jolla ei sitä paitsi luoda oikeuksia yksityisille, säännökset eivät suojaa rekisteröityjä vaaralta, että heidän sähköisen viestintänsä sisältöön on yleinen pääsy.

282. Totean tältä osin ainoastaan, että Euroopan ihmisoikeustuomioistuin ei ole Euroopan ihmisoikeussopimuksen 8 artiklaa koskevassa oikeuskäytännössään turvautunut yksityiselämän kunnioitusta koskevan oikeuden keskeisen sisällön tai itse ytimen loukkaamista koskevaan käsitteeseen.[161] Kyseinen tuomioistuin ei ole tähän mennessä katsonut, että järjestelmät, joissa sallitaan jopa laajamittainen sähköisen viestinnän kaappaus, *ylittäisivät sellaisinaan jäsenvaltioiden harkintavallan*. Euroopan ihmisoikeustuomioistuin katsoo, että tällaiset järjestelmät ovat yhteensopivia

156 Ks. Privacy Shield -päätöksen johdanto-osan 70, 103 ja 109 perustelukappale.

157 Ks. Privacy Shield -päätöksen johdanto-osan 83–87 perustelukappale ja liitteessä VI olevan I kohdan c alakohta. Huomattakoon, että PCLOB:n raportin (s. 51–66) mukaan NSA:n minimointiin liittyvät menettelyt FISA:n 702 §:n nojalla kohdistuvat useimmissa tapauksissa vain yhdysvaltalaisiin henkilöihin. PPD 28:lla oli tarkoitus ulottaa sovellettavat suojatoimet ei-yhdysvaltalaisiin henkilöihin. Ks. PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, saatavilla osoitteessa https://www.pclob.gov/reports/report-PPD28/ (s. 2). Sen jälkeen, kun viranomaiset ovat hankkineet nämä tiedot, niiden säilyttäminen ja käyttäminen kansallista turvallisuutta varten eivät mielestäni kuulu unionin oikeuden soveltamisalaan (ks. tämän ratkaisuehdotuksen 226 kohta). Tämän toiminnan yhteydessä varmistetun tietosuojan riittävyyttä on siis arvioitava ainoastaan Euroopan ihmisoikeussopimuksen 8 artiklan kannalta.

158 Ks. tämän ratkaisuehdotuksen 283–289 kohta.

159 Erityisesti komissio toteaa Privacy Shield -päätöksen johdanto-osan 127 perustelukappaleessa, että Yhdysvaltojen perustuslain neljättä lisäystä ei sovelleta ei-yhdysvaltalaisiin henkilöihin.

160 Ks. Privacy Shield -päätöksen johdanto-osan 73 ja 74 perustelukappale ja liitteessä VI olevan I kohdan b alakohta. Nämä tavoitteet käsittävät vakoilun torjunnan ja ulkovaltojen Yhdysvaltoihin ja sen etuihin kohdistamien muiden uhkien ja toiminnan torjunnan; terrorismin uhan torjunnan; joukkotuhoaseiden kehittämiseen, hallussapitoon, levittämiseen tai käyttöön perustuvien uhkien torjunnan; kyberturvallisuuteen liittyvien uhkien torjunnan; Yhdysvaltojen tai sen liittolaisten asevoimiin kohdistuvien uhkien torjunnan ja kansainvälisen rikollisuuden uhkien torjunnan. PPD 28:n alaviitteen 5 mukaan valikoimattomasti kerättyjen tietojen käytön oikeuttavien tavoitteiden rajoitusta ei sovelleta, jos tällainen keruu on vain tilapäistä ja tarkoitettu helpottamaan kohdennettua keruuta.

161 Vaikka Euroopan ihmisoikeussopimuksen määräyksissä ei mainita perusoikeuksien ”keskeistä sisältöä”, Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä, joka koskee tiettyjä näistä määräyksistä, on käytetty perusoikeuden keskeistä sisältöä vastaavaa käsitettä. Ks. Euroopan ihmisoikeussopimuksen 6 artiklassa taatun oikeudenmukaista oikeudenkäyntiä koskevan oikeuden keskeisestä sisällöstä mm. Euroopan ihmisoikeustuomioistuimen tuomio 25.5.1985, Ashingdane v. Yhdistynyt kuningaskunta (CE:ECHR:1985:0528JUD000822578, 57 ja 59 kohta); Euroopan ihmisoikeustuomioistuimen tuomio 21.12.2000, Heaney ja McGuinness v. Irlanti (CE:ECHR:2000:1221JUD003472097, 55 ja 58 kohta) ja Euroopan ihmisoikeustuomioistuimen tuomio 23.6.2016, Baka v. Unkari (CE:ECHR:2016:0623JUD002026112, 121 kohta). Ks. Euroopan ihmisoikeussopimuksen 12 artiklassa vahvistetun avioliittoa koskevan oikeuden keskeisestä sisällöstä Euroopan ihmisoikeustuomioistuimen tuomio 11.7.2002, Christine Goodwin v. Yhdistynyt kuningaskunta (CE:ECHR:2002:0711JUD002895795, 99 ja 101 kohta). Ks. Euroopan ihmisoikeussopimuksen ensimmäisen lisäpöytäkirjan 2 artiklassa taatun koulutusta koskevan oikeuden keskeisestä sisällöstä Euroopan ihmisoikeustuomioistuimen tuomio 23.7.1968, Belgian opetuksen kielijärjestelyyn liittyviä tiettyjä näkökohtia koskeva asia (CE:ECHR:1968:0723JUD000147462, 5 kohta).

Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleen kanssa, jos niihin on liitetty tietty määrä vähimmäissuojatoimia.[162] Tässä tilanteessa mielestäni ei ole asianmukaista katsoa, että EO 12333:ssa käyttöön otetun kaltaisella tarkkailujärjestelmällä ylitettäisiin jäsenvaltioiden harkintavalta, tutkimatta lainkaan siihen liitettyjä mahdollisia suojatoimia.

4) Oikeutetun tavoitteen toteuttaminen

283. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa vahvistettuja oikeuksia koskevien rajoitusten on vastattava tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita. Lisäksi perusoikeuskirjan 8 artiklan 2 kohdassa määrätään, että henkilötietojen käsittelyn, joka ei perustu asianomaisen henkilön suostumukseen, on tapahduttava ”laissa säädetyn oikeuttavan perusteen” nojalla. Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleessa taas luetellaan päämäärät, joilla voidaan oikeuttaa puuttuminen yksityiselämän kunnioitusta koskevan oikeuden käyttämiseen.

284. Privacy Shield -päätöksen mukaan siinä tarkoitettujen periaatteiden noudattamista voidaan rajoittaa kansallista turvallisuutta, yleistä etua ja lainvalvontaa koskevien velvollisuuksien täyttämiseksi.[163] Tämän päätöksen johdanto-osan 67–124 perustelukappaleessa tarkastellaan tarkemmin rajoituksia, jotka seuraavat siitä, että Yhdysvaltojen viranomaisilla on pääsy tietoihin ja että ne käyttävät niitä kansallista turvallisuutta varten.

285. On selvää, että kansallisen turvallisuuden suojelu on oikeutettu tavoite, jonka vuoksi voi olla perusteltua poiketa tietosuoja-asetukseen perustuvista vaatimuksista[164] ja perusoikeuskirjan 7 ja 8 artiklassa[165] sekä Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleessa vahvistetuista perusoikeuksista. Schrems, Itävallan hallitus ja EPIC huomauttavat kuitenkin, että FISA:n 702 §:ään ja EO 12333:een perustuvien tarkkailuohjelmien puitteissa toteutetut tavoitteet menevät kansallista turvallisuutta pidemmälle. Näiden välineiden tarkoituksena on ”ulkomaantiedustelutiedon” hankkiminen, ja tämä käsite kattaa eri tyyppisiä tietoja, jotka sisältävät kansallista turvallisuutta koskevat tiedot mutta eivät kuitenkaan välttämättä rajoitu niihin.[166] FISA:n 702 §:ssä tarkoitettuun ulkomaantiedustelutiedon käsitteeseen kuuluvat siten tiedot, jotka koskevat ulkosuhteiden hoitamista.[167] EO 12333:n mukaan tällä käsitteellä taas tarkoitetaan tietoja, jotka koskevat ulkomaisten hallitusten, ulkomaisten organisaatioiden ja ulkomaalaisten henkilöiden valmiuksia, aikomuksia tai toimintaa.[168] Schrems kyseenalaistaa tämän tavoitteen oikeutettavuuden siltä osin kuin se ylittää kansallisen turvallisuuden.

162 Ks. erityisesti tuomio Centrum för Rättvisa (112–114 kohta oikeuskäytäntöviittauksineen) ja tuomio Big Brother Watch (337 kohta).

163 Ks. tämän ratkaisuehdotuksen 197 kohta.

164 Ks. tietosuoja-asetuksen 23 artiklan 1 kohdan a alakohta.

165 Ks. tuomio Schrems (88 kohta). Unionin tuomioistuin on pitänyt EUT-sopimuksen määräyksissä tarkoitettua lähikäsitettä ”yleinen turvallisuus”, joka oikeuttaa poikkeamisen siinä taatuista perusvapauksista, unionin oikeuden itsenäisenä käsitteenä, johon kuuluvat sekä jäsenvaltioiden sisäinen turvallisuus että niiden ulkoinen turvallisuus (ks. mm. tuomio 26.10.1999, Sirdar (C-273/97, EU:C:1999:523, 17 kohta) ja tuomio 13.9.2016, CS (C-304/14, EU:C:2016:674, 39 kohta oikeuskäytäntöviittauksineen). Kun sisäiseen turvallisuuteen voi vaikuttaa mm. suora uhka asianomaisen jäsenvaltion väestön rauhalle ja fyysiselle turvallisuudelle, ulkoiseen turvallisuuteen puolestaan voivat vaikuttaa muun muassa ulkosuhteiden tai kansojen rauhanomaisen rinnakkaiselon vakavan häiriintymisen vaara. Jäsenvaltiot eivät voi yksinään määritellä näiden käsitteiden ulottuvuutta, mutta niillä on tietty harkintavalta keskeisten turvallisuusetujensa määrittämisessä. Ks. erityisesti tuomio 2.5.2018, K. ja H. F. (Oleskeluoikeus ja väitetyt sotarikokset) (C-331/16 ja C-366/16, EU:C:2018:296, 40–42 kohta oikeuskäytäntöviittauksineen). Näitä perusteluja voidaan mielestäni soveltaa tulkittaessa kansallisen turvallisuuden käsitettä etuna, jonka suojelu voi oikeuttaa rajoitukset tietosuoja-asetuksen säännöksiin ja perusoikeuskirjan 7 ja 8 artiklassa taattuihin oikeuksiin.

166 Ks. tältä osin Privacy Shield -päätöksen johdanto-osan 89 perustelukappale ja alaviite 97.

167 Ks. tämän ratkaisuehdotuksen 55 kohta.

168 Ks. tämän ratkaisuehdotuksen 61 kohta.

286. Nähdäkseni kansallisen turvallisuuden alue voi käsittää tietyssä määrin ulkosuhteiden hoitamiseen liittyvien etujen suojelun.[169] Ei ole ajateltavissa, että jotkin muut FISA:n 702 §:ssä ja EO 12333:ssa määritellyn ulkomaantiedustelun käsitteen kattamista tavoitteista kuin kansallisen turvallisuuden suojelu vastaisivat merkittäviä yleisen edun mukaisia tavoitteita, joilla voitaisiin oikeuttaa puuttuminen yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin. Nämä tavoitteet olisivat joka tapauksessa vähemmän painavia kuin kansallisen turvallisuuden varmistaminen punnittaessa rekisteröityjen perusoikeuksia suhteessa puuttumisella tavoiteltuun päämäärään.[170]

287. Perusoikeuskirjan 52 artiklan 1 kohdan mukaisesti edellytetään vielä, että kyseessä olevaa puuttumista koskevilla toimenpiteillä pyritään tosiasiallisesti toteuttamaan kansallista turvallisuutta koskeva tavoite tai jokin muu oikeutettu tavoite.[171] Lisäksi puuttumisen päämäärät on määriteltävä siten, että ne täyttävät selvyyden ja täsmällisyyden vaatimukset.[172]

288. Schremsin mukaan FISA:n 702 §:ssä ja EO 12333:ssa tarkoitettujen tarkkailutoimenpiteiden tavoitetta ei ole ilmoitettu riittävän selvästi, jotta niissä noudatettaisiin ennakoitavuutta ja oikeasuhteisuutta koskevia suojatoimia. Näin on erityisesti sen vuoksi, että näissä välineissä määritellään ulkomaantiedustelu poikkeuksellisen laajasti. Lisäksi komissio on todennut Privacy Shield -päätöksen johdanto-osan 109 perustelukappaleessa, että FISA:n 702 §:n mukaan ulkomaantiedustelutietojen hankkiminen on keruun ”huomattava tarkoitus”, eikä tämä sanamuoto sulje pois ensi arviolta, kuten EPIC on tuonut esille, muihin määrittelemättömiin tavoitteisiin pyrkimistä.

289. Näistä syistä – ilman että olisi poissuljettua, että FISA:n 702 §:n tai EO 12333:n mukaiset tarkkailutoimenpiteet ovat oikeutettujen tavoitteiden mukaisia – voidaan pohtia, onko ne määritelty riittävän selvästi ja täsmällisesti väärinkäytön vaarojen välttämiseksi ja puuttumisen oikeasuhteisuuden valvonnan mahdollistamiseksi.[173]

5) Puuttumisen tarpeellisuus ja oikeasuhteisuus

290. Unionin tuomioistuin on toistuvasti korostanut, että perusoikeuskirjan 7 ja 8 artiklassa vahvistetut oikeudet eivät ole ehdottomia, vaan niitä on tarkasteleva suhteessa niiden tehtävään yhteiskunnassa ja niiden on suhteellisuusperiaatteen mukaisesti oltava oikeassa suhteessa muihin perusoikeuksiin.[174] Kuten Facebook Ireland korostaa, näihin muihin oikeuksiin kuuluu perusoikeuskirjan 6 artiklassa taattu oikeus turvallisuuteen.

291. Yhtä vakiintuneen oikeuskäytännön mukaan perusoikeuskirjan 7 ja 8 artiklassa taattujen oikeuksien käyttöön puuttumisen oikeasuhteisuutta on valvottava tarkasti.[175]

169 Tuomiossa Centrum för Rättvisa (111 kohta) Euroopan ihmisoikeustuomioistuin totesi, että tarkkailutoiminnalla, jolla pyrittiin tukemaan Ruotsin ulkopolitiikkaa, puolustuspolitiikkaa ja turvallisuuspolitiikkaa sekä selvittämään Ruotsissa järjestetyt ulkoiset uhat, oli kansallista turvallisuutta koskevat oikeutetut tavoitteet.

170 Ks. tästä tuomio Tele2 Sverige (115 kohta) ja tuomio Ministerio Fiscal (55 kohta). Unionin tuomioistuin korosti niissä puuttumisen vakavuuden yhteyttä siihen etuun, johon puuttumisen oikeuttamiseksi vedotaan.

171 Tietosuojatyöryhmä painotti sähköisen viestinnän tarkkailusta tiedustelua ja kansallista turvallisuutta varten 5.12.2014 laatimassaan työskentelyasiakirjassa, WP 228 (s. 27), että on tärkeää arvioida kriittisesti, toteutetaanko tarkkailu tosiasiallisesti kansallista turvallisuutta varten.

172 Ks. lausunto 1/15 (181 kohta), jossa unionin tuomioistuin totesi, että puuttumista sääntelevien säännösten sanamuoto ei täyttänyt selvyyden ja täsmällisyyden vaatimuksia, minkä vuoksi tämä puuttuminen ei rajoittunut siihen, mikä on täysin välttämätöntä. Vastaavasti julkisasiamies Bot katsoi ratkaisuehdotuksessaan Schrems (C-362/14, EU:C:2015:627, 181–184 kohta), että tarkkailutoimenpiteiden tavoitteet oli muotoiltu liian yleisiksi, jotta niitä voitaisiin pitää yleisen edun mukaisina tavoitteina, paitsi siltä osin kuin kyse on kansallisesta turvallisuudesta.

173 Euroopan tietosuojavaltuutettu on esittänyt samankaltaisia epäilyjä 30.5.2016 antamassaan lausunnossa 4/2016 EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyyttä koskevasta päätösluonnoksesta (s. 8).

174 Ks. tuomio 9.11.2010, Volker und Markus Schecke ja Eifert (C-92/09 ja C-93/09, EU:C:2010:662, 48 kohta); lausunto 1/15 (136 kohta) ja tuomio 24.9.2019, Google (Hakutulosten luettelosta poistamisen alueellinen ulottuvuus) (C-507/17, EU:C:2019:772, 60 kohta).

175 Ks. mm. tuomio 16.12.2008, Satakunnan Markkinapörssi ja Satamedia (C-73/07, EU:C:2008:727, 56 kohta); tuomio Digital Rights Ireland (48 ja 52 kohta); tuomio Schrems (78 ja 92 kohta) ja lausunto 1/15 (139 ja 140 kohta). Ks. myös Privacy Shield -päätöksen johdanto-osan 140 perustelukappale.

292. Tuomiosta Schrems ilmenee erityisesti, että ”siihen, mikä on ehdottomasti tarpeen, ei – – rajoitu säännöstö, jossa sallitaan yleisesti – – 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”. [176]

293. Unionin tuomioistuin on myös todennut, että tietoihin pääsy edellyttää asianmukaisesti perusteltuja kiireellisiä tapauksia lukuun ottamatta joko tuomioistuimen tai riippumattoman hallintoelimen etukäteisvalvontaa ja niiden päätöksessä tietoihin pääsy ja niiden käyttö on rajoitettava siihen, mikä on täysin välttämätöntä tavoitellun päämäärän saavuttamiseksi. [177]

294. Tietosuoja-asetuksen 23 artiklan 2 kohdassa vahvistetaan nyt useita suojatoimia, joista jäsenvaltion on säädettävä, jos se poikkeaa tämän asetuksen säännöksistä. Säännöstön, jossa sallitaan tällainen poikkeus, on sisällettävä säännöksiä, jotka koskevat muun muassa käsittelytarkoitusta, poikkeuksen soveltamisalaa, suojatoimia, joilla estetään väärinkäyttö, tietojen säilytysaikoja ja rekisteröityjen oikeutta saada tietoa poikkeuksesta, paitsi jos tämä voisi vaarantaa sen tarkoituksen.

295. Tässä asiassa Schrems väittää, että FISA:n 702 §:ään ei liity riittäviä suojatoimia väärinkäytön ja lainvastaisen tietoihin pääsyn vaaroja vastaan. Varsinkaan valintakriteerien määrittämistä ei ole rajattu riittävästi, minkä vuoksi tässä säännöksessä ei anneta takeita siitä, ettei viestinnän sisältöön ole yleistä pääsyä.

296. Yhdysvaltojen hallitus ja komissio väittävät sitä vastoin, että FISA:n 702 §:ssä rajoitetaan objektiivisin perustein valintakriteerien määrittämistä, koska tässä säännöksessä sallitaan ainoastaan ei-yhdysvaltaisten henkilöiden, jotka ovat Yhdysvaltojen ulkopuolella, sähköisen viestinnän tietojen keruu ulkomaantiedustelutiedon hankkimiseksi.

297. Mielestäni on kyseenalaista, ovatko nämä perusteet riittävän selviä ja täsmällisiä ja onko väärinkäytön vaarojen välttämiseksi toteutettu riittäviä suojatoimia.

298. Ensinnäkin Privacy Shield -päätöksen johdanto-osan 109 perustelukappaleessa todetaan, että FISC tai mikään muu riippumaton oikeus- tai hallintoelin ei hyväksy yksittäisiä valintakriteerejä ennen niiden soveltamista. Komissio toteaa siinä, että ”[FISC] ei – – anna lupaa yksittäisille valvontatoimenpiteille. Sen sijaan se hyväksyy valvontaohjelmia – – vuotuisten sertifiointihakemusten perusteella”, minkä Yhdysvaltojen hallitus on vahvistanut unionin tuomioistuimessa. Tässä perustelukappaleessa täsmennetään, että ”[FISC:n] antamiin sertifiointipäätöksiin ei sisälly tietoa kohteena olevista yksittäisistä ihmisistä, vaan niiden avulla yksilöidään ulkomaantiedustelutietojen luokat”, jotka voidaan kerätä. Komissio toteaa siinä niin ikään, että ”[FISC] ei arvioi todennäköisen syyn perusteella tai muulla tavalla, onko henkilöt kohdennettu asianmukaisesti ulkomaantiedustelutietojen hankkimiseksi”, vaikka se valvoo, että ”hankinnan huomattavana tarkoituksena on hankkia ulkomaantiedustelutietoja”.

176 Tuomio Schrems (93 kohta). Ks. vastaavasti myös tuomio Digital Rights Ireland (60 kohta).

177 Ks. tuomio Tele2 Sverige (120 kohta) ja lausunto 1/15 (202 kohta).

299. Kyseisen perustelukappaleen mukaan FISA:n 702 §:ssä annetaan NSA:lle lupa kerätä tietoja ”vain, jos voidaan kohtuudella olettaa, että tiettyä viestintävälinettä käytetään ulkomaantiedustelutiedon – – välittämiseen”. Privacy Shield -päätöksen johdanto-osan 70 perustelukappaleessa todetaan lisäksi, että valintakriteerien määrittäminen tapahtuu yleisen kansallisia tiedusteluprioriteetteja koskevan kehyksen (National Intelligence Priorities Framework, NIPF) puitteissa. Tässä päätöksessä ei viitata vaatimuksiin perustella tai oikeuttaa tarkemmin valintakriteerien määrittäminen näiden NSA:ta velvoittavien hallinnollisten prioriteettien kannalta. [178]

300. Privacy Shield -päätöksen johdanto-osan 71 perustelukappaleessa viitataan vielä PPD 28:ssa asetettuun vaatimukseen, jonka mukaan tiedusteluaineiston keruun on oltava ”mahdollisimman räätälöityä”. Sen lisäksi, että tässä presidentin määräyksessä ei luoda oikeuksia yksityisille, se, vastaako ”mahdollisimman räätälöidyn” toiminnan kriteeri pääosiltaan ”täysin välttämättömän” kriteeriä, jonka täyttymistä edellytetään perusoikeuskirjan 52 artiklan 1 kohdassa sen 7 ja 8 artiklassa taattujen oikeuksien käyttöön puuttumisen oikeuttamiseksi, on mielestäni kaikkea muuta kuin ilmeistä. [179]

301. Näillä perusteilla ei ole varmaa, että Privacy Shield -päätöksessä esitettyjen seikkojen perusteella FISA:n 702 §:ään perustuviin tarkkailutoimenpiteisiin liittyy suojatoimia, jotka koskevat henkilöiden, jotka voivat olla tarkkailutoimenpiteen kohteena, ja tavoitteiden, joita varten tietoja voidaan kerätä, rajaamista ja jotka pääosiltaan vastaavat tietosuoja-asetuksen, luettuna perusoikeuskirjan 7 ja 8 artiklan valossa, perusteella edellytettyjä suojatoimia. [180]

302. EO 12333:een perustuvaan tarkkailuun liittyvän suojan riittävyyden arvioinnin osalta Euroopan ihmisoikeustuomioistuin katsoo, että jäsenvaltioilla on laaja harkintavalta niiden valitessa keinot kansallisen turvallisuuden suojelemiseksi, mutta tätä harkintavaltaa rajoittaa kuitenkin vaatimus säätää asianmukaisista ja riittävistä suojatoimista väärinkäyttöä vastaan. [181] Euroopan ihmisoikeustuomioistuin tarkistaa salaisia tarkkailutoimenpiteitä koskevassa oikeuskäytännössään, sisältääkö kansallinen oikeus, johon nämä toimenpiteet perustuvat, riittäviä ja tehokkaita suojatoimia ja takeita täyttääkseen vaatimukset ”ennakoitavuudesta” ja ”välttämättömyydestä demokraattisessa yhteiskunnassa”. [182]

303. Euroopan ihmisoikeustuomioistuin 31toteaa tältä osin tietyn määrän vähimmäissuojatoimia. Nämä suojatoimet koskevat selvää ilmoitusta niiden sääntöjenvastaisuuksien luonteesta, jotka voivat antaa valtuudet kaappaukseen, henkilöryhmien, joiden viestintää voidaan kaapata, määrittämistä, toimenpiteen täytäntöönpanon kestolle asetetun rajan vahvistamista, kerättyjen tietojen tutkintaa, käyttöä ja säilyttämistä koskevaa menettelyä, toteutettavia varotoimenpiteitä luovutettaessa tietoja muille osapuolille ja olosuhteita, joissa tallennukset voidaan tai täytyy poistaa tai tuhota. [183]

178 PCLOB:n raportissa (s. 45) täsmennetään seuraavaa: ”With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to “identify” the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification.”

179 Ks. vastaavasti tietosuojatyöryhmä, Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 13.4.2016, WP 238 (3.3.1 kohta, s. 38); parlamentin 6.4.2017 antama päätöslauselma EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn tarjoaman suojan riittävyydestä, P8_TA(2017)0131 (17 kohta) ja parlamentin 20.2.2017 antama kertomus massadatan vaikutuksista perusoikeuksiin: yksityisyys, tietosuoja, syrjimättömyys, turvallisuus ja lainvalvonta, A8-0044/2017 (17 kohta).

180 Ks. vastaavasti tietosuojatyöryhmä, EU-U.S. Privacy Shield – First Annual Joint Review, 28.11.2017, WP 255 (s. 3); Euroopan parlamentin 5.7.2018 antama päätöslauselma EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn tarjoaman suojan riittävyydestä, P8_TA(2018)0315 (22 kohta), ja Euroopan tietosuojaneuvosto, EU-U.S. Privacy Shield – Second Annual Joint Review, 22.1.2019 (81–83 ja 87 kohta).

181 Ks. mm. tuomio Zakharov (232 kohta) ja tuomio Szabó ja Vissy (57 kohta).

182 Ks. mm. tuomio Zakharov (237 kohta); tuomio Centrum för Rättvisa (111 kohta) ja tuomio Big Brother Watch (322 kohta).

183 Ks. mm. päätös Weber ja Saravia (95 kohta); Euroopan ihmisoikeustuomioistuimen tuomio 28.6.2007, Association pour l'intégration européenne et les droits de l'homme ja Ekimdjiev (CE:ECHR:2007:0628JUD006254000, 76 kohta) ja tuomio Zakharov (231 kohta).

304. Puuttumiseen liittyvien suojatoimien riittävyys ja tehokkuus riippuvat kaikista asian olosuhteista, kuten toimenpiteiden luonteesta, laajuudesta ja kestosta, niiden määräämiseen edellytetyistä perusteista, niiden sallimisen, täytäntöönpanon ja valvonnan osalta toimivaltaisista viranomaisista sekä kansallisessa oikeudessa säädetyn oikeussuojakeinon tyypistä. [184]

305. Erityisesti salaisen tarkkailutoimenpiteen perusteltavuutta arvioidessaan Euroopan ihmisoikeustuomioistuin ottaa huomioon kaiken valvonnan toimenpiteestä ”määrättäessä”, sitä ”toteutettaessa” ja sen ”lakattua”. [185] Ensimmäisessä näistä kolmesta vaiheesta Euroopan ihmisoikeustuomioistuin edellyttää, että toimenpide on riippumattoman elimen hyväksymä. Vaikka tuomiovallalla voidaan sen mukaan parhaiten taata riippumattomuus, puolueettomuus ja menettelyn sääntöjenmukaisuus, kyseisen elimen ei välttämättä ole kuuluttava tuomioistuinjärjestelmään. [186] Hyväksymismenettelyn mahdolliset puutteellisuudet voidaan korjata myöhemmässä vaiheessa toteutettavalla perusteellisella tuomioistuinvalvonnalla. [187]

306. Esillä olevassa asiassa Privacy Shield -päätöksestä ilmenee, että ainoat suojatoimet, jotka rajoittavat tietojen keruuta ja käyttöä Yhdysvaltojen alueen ulkopuolella, sisältyvät PPD 28:aan, sillä FISA:n 702 §:ää ei sovelleta tämän alueen ulkopuolella. En ole vakuuttunut siitä, että nämä suojatoimet riittäisivät täyttämään edellytykset ”ennakoitavuudesta” ja ”välttämättömyydestä demokraattisessa yhteiskunnassa”.

307. Olen jo tuonut esille, että tällä presidentin määräyksellä ei luoda oikeuksia yksityisille. Lisäksi epäilen, onko vaatimus ”mahdollisimman räätälöidystä” tarkkailusta muotoiltu riittävän selvästi ja täsmällisesti, jotta rekisteröityjä suojattaisiin asianmukaisesti väärinkäytön vaaroilta. [188] Privacy Shield -päätöksessä ei todeta, että EO 12333:een perustuva tarkkailu edellyttäisi riippumattoman elimen etukäteisvalvontaa tai että se voisi olla tuomioistuimen jälkikäteisvalvonnan kohteena. [189]

308. Tässä tilanteessa pohdin, onko se toteamus perusteltu, jonka mukaan Yhdysvallat varmistaa FISA:n 702 §:n ja EO 12333:n mukaisen tiedustelupalvelujensa toiminnan yhteydessä tietosuoja-asetuksen 45 artiklan 1 kohdassa, luettuna perusoikeuskirjan 7 ja 8 artiklan ja Euroopan ihmisoikeussopimuksen 8 artiklan valossa, tarkoitetun riittävän tietosuojan tason.

c) Privacy Shield -päätöksen pätevyys tehokasta oikeussuojaa koskevan oikeuden kannalta

309. Viidennessä ennakkoratkaisukysymyksessä unionin tuomioistuinta pyydetään määrittämään, saavatko henkilöt, joiden tietoja siirretään Yhdysvaltoihin, siellä oikeussuojaa, joka pääosiltaan vastaa suojaa, joka unionissa on taattava perusoikeuskirjan 47 artiklan nojalla. Kymmenennellä kysymyksellään ennakkoratkaisua pyytänyt tuomioistuin kysyy unionin tuomioistuimelta, onko viidenteen kysymykseen vastattava myöntävästi, kun otetaan huomioon Privacy Shield -päätöksellä käyttöön otettu oikeusasiamiesmekanismi.

310. Totean heti alkuun, että tämän päätöksen johdanto-osan 115 perustelukappaleessa komissio katsoo, että Yhdysvaltojen oikeusjärjestyksessä on yksityisten oikeussuojaa koskevia puutteita.

184 Ks. mm. päätös Weber ja Saravia (106 kohta); tuomio Zakharov (232 kohta) ja tuomio Centrum för Rättvisa (104 kohta).

185 Ks. mm. Euroopan ihmisoikeustuomioistuimen tuomio 6.9.1978, Klass ym. v. Saksa (CE:ECHR:1978:0906JUD000502971, 55 kohta); tuomio Zakharov (233 kohta) ja tuomio Centrum för Rättvisa (105 kohta).

186 Ks. mm. tuomio Klass (56 kohta); Euroopan ihmisoikeustuomioistuimen tuomio 18.5.2010, Kennedy v. Yhdistynyt kuningaskunta (CE:ECHR:2010:0518JUD002683905, 167 kohta) ja tuomio Zakharov (233 ja 258 kohta).

187 Ks. tuomio Szabó ja Vissy (77 kohta) ja tuomio Centrum för Rättvisa (133 kohta).

188 Näin on sitä suuremmalla syyllä tämän ratkaisuehdotuksen 281 kohdassa esitettyjen perustelujen vuoksi.

189 Ks. tämän ratkaisuehdotuksen 330 ja 331 kohta.

311. Tämän perustelukappaleen mukaan mahdollisuus käyttää oikeussuojakeinoja ”ei koske eräitä Yhdysvaltojen tiedusteluviranomaisten käytössä olevia oikeusperustoja (esim. toimeenpanoasetus (E.O.) 12333)”. EO 12333:ssa ja PPD 28:ssa ei nimittäin anneta rekisteröidyille oikeuksia eivätkä nämä voi vedota niihin tuomioistuimissa. Tehokas oikeussuoja edellyttää vähintäänkin, että yksityisillä on oikeuksia, joihin voidaan vedota tuomioistuimessa.

312. Lisäksi kyseisessä perustelukappaleessa todetaan, että ”vaikka periaatteessa ei-yhdysvaltalaisten henkilöiden käytettävissä on oikeussuojakeinoja, esimerkiksi kun on kyse FISAn mukaisesta valvonnasta, käytössä olevat kanneperusteet ovat vähäiset ja – – kanteet jätetään tutkimatta, jos ne eivät pysty osoittamaan kanneoikeuttaan. Tämä rajoittaa pääsyä yleisiin tuomioistuimiin”.

313. Privacy Shield -päätöksen johdanto-osan 116–124 perustelukappaleesta ilmenee, että oikeusasiamiesmekanismin käyttöönotolla pyritään kompensoimaan nämä rajoitukset. Komissio päättelee tämän päätöksen johdanto-osan 139 perustelukappaleessa, että ”*kokonaisuutena tarkasteltuna* Privacy Shield -järjestelyyn kuuluvien *valvonta-* ja *muutoksenhaku*mekanismien avulla voidaan – – tarjota oikeussuojakeinoja rekisteröidylle, jotta tämä voi tutustua itseään koskeviin henkilötietoihin ja saada nämä tiedot oikaistuiksi tai poistetuiksi” (kursivointi tässä).

314. Pitäen mielessä unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä vahvistetut yleiset periaatteet, jotka koskevat oikeussuojakeinoja viestinnän tarkkailutoimenpiteitä vastaan, tutkin, voidaanko Privacy Shield -päätöksessä kuvatun kaltaisilla Yhdysvaltojen oikeudessa säädetyillä oikeussuojakeinoilla varmistaa rekisteröityjen asianmukainen oikeussuoja (osa 1). Tämän jälkeen selvitän, voidaanko tuomioistuimen ulkopuolisen oikeusasiamiesmekanismin käyttöönotolla tarvittaessa korjata mahdolliset puutteet näiden henkilöiden oikeussuojassa (osa 2).

1) Yhdysvaltojen oikeudessa säädettyjen oikeussuojakeinojen tehokkuus

315. Perusoikeuskirjan 47 artiklan ensimmäisessä kohdassa määrätään, että jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa.[190] Tämän artiklan toisen kohdan mukaan jokaisella on oikeus oikeudenkäyntiin riippumattomassa ja puolueettomassa tuomioistuimessa.[191] Oikeus saada asiansa käsitellyksi riippumattomassa tuomioistuimessa on osa perusoikeuskirjan 47 artiklassa taatun oikeuden keskeistä sisältöä.[192]

190 Perusoikeuskirjan selityksissä todetaan tältä osin, että ”[sen 47 artiklassa tarkoitettu] suoja on unionin oikeudessa – – laajempi [kuin Euroopan ihmisoikeussopimuksen 13 artiklassa annettu suoja], sillä siinä turvataan oikeus tehokkaisiin oikeussuojakeinoihin tuomarin edessä”. Ks. myös julkisasiamies Wathelet’n ratkaisuehdotus Berlioz Investment Fund (C-682/15, EU:C:2017:2, 37 kohta).

191 Arvioitaessa perusoikeuskirjan 47 artiklan perusteella ”tuomioistuimen” ominaisuutta on otettava huomioon elimen lakisääteisyys, pysyvyys, sen tuomiovallan pakottavuus, menettelyn kontradiktorisuus, toimiminen oikeussääntöjen soveltajana ja riippumattomuus. Ks. tuomio 27.2.2018, Associação Sindical dos Juízes Portugueses (C-64/16, EU:C:2018:117, 38 kohta oikeuskäytäntöviittauksineen).

192 Ks. mm. tuomio 25.7.2018, Minister for Justice and Equality (Tuomioistuinjärjestelmän puutteet) (C-216/18 PPU, EU:C:2018:586, 59 ja 63 kohta); tuomio 5.11.2019, komissio v. Puola (Yleisten tuomioistuinten riippumattomuus) (C-192/18, EU:C:2019:924, 106 kohta) ja tuomio 19.11.2019, A. K. ym. (Ylimmän tuomioistuimen kurinpitojaoston riippumattomuus) (C-585/18, C-624/18 ja C-625/18, EU:C:2019:982, 120 kohta).

316. Tämän yksityisten oikeussuojaa koskevan oikeuden ohella jäsenvaltioilla on perusoikeuskirjan 7 ja 8 artiklan nojalla velvollisuus asianmukaisesti perusteltuja kiireellisiä tapauksia lukuun ottamatta saattaa kaikki tarkkailutoimenpiteet tuomioistuimen tai riippumattoman hallintoviranomaisen etukäteisvalvontaan. [193]

317. Kuten Saksan ja Ranskan hallitukset väittävät, oikeus tehokkaaseen oikeussuojakeinoon ei ole ehdoton tae, [194] koska tätä oikeutta voidaan rajoittaa kansallista turvallisuutta koskevilla perusteilla. Poikkeukset ovat kuitenkin sallittuja ainoastaan, jos ne eivät loukkaa tämän oikeuden keskeistä sisältöä ja jos ne ovat täysin välttämättömiä tavoitellun päämäärän saavuttamiseksi.

318. Unionin tuomioistuin totesi tältä osin tuomiossa Schrems, että säännöstö, jossa yksityisille ei anneta *mitään mahdollisuutta* käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi, ei ole perusoikeuskirjan 47 artiklassa vahvistetun perusoikeuden keskeisen sisällön mukainen. [195]

319. Korostan, että tämä oikeus saada pääsy tietoihin edellyttää, jollei oikeutetun tavoitteen saavuttamiseksi täysin välttämättömistä poikkeuksista muuta johdu, että henkilöllä on mahdollisuus saada viranomaisilta *vahvistus siitä, että ne käsittelevät tai että ne eivät käsittele häntä koskevia henkilötietoja*. [196] Tämä on mielestäni tietoihin pääsyä koskevan oikeuden käytännön sisältö, kun asianomainen henkilö ei tiedä, ovatko viranomaiset säilyttäneet hänen henkilötietojaan muun muassa sähköisen viestintävirran automatisoidun suodatusmenettelyn jälkeen.

320. Oikeuskäytännöstä ilmenee, että jäsenvaltion viranomaisten on lähtökohtaisesti ilmoitettava oikeudesta saada tietoja *heti, kun ilmoitus ei enää ole omiaan vaarantamaan suoritettavia tutkimuksia*. [197] Tällainen ilmoitus on ennakkoedellytyksenä perusoikeuskirjan 47 artiklan mukaisen oikeussuojakeinon käytölle. [198] Tästä velvollisuudesta on nyt säädetty tietosuoja-asetuksen 23 artiklan 2 kohdan h alakohdassa.

321. Privacy Shield -päätöksen johdanto-osan 111–135 perustelukappaleessa esitetään tiivistetysti henkilöiden, joiden tietoja on siirretty, käytettävissä olevat kaikki oikeussuojakeinot silloin, kun he ovat huolissaan siitä, että Yhdysvaltojen tiedustelupalvelut ovat mahdollisesti käsitelleet heidän henkilötietojaan siirron jälkeen. Nämä oikeussuojakeinot kuvataan myös High Courtin 3.10.2017 antamassa tuomiossa sekä muun muassa Yhdysvaltojen hallituksen huomautuksissa.

193 Ks. tämän ratkaisuehdotuksen 293 kohta. Tietosuoja-asetuksen 45 artiklan 2 kohdan a alakohdassa säädetään, että jäsenvaltion tietosuojan riittävyyttä arvioitaessa on otettava huomioon tehokkaat ”hallinnolliset *ja oikeudelliset* muutoksenhakukeinot” rekisteröityjä varten (kursivointi tässä). Vastaavasti tietosuoja-asetuksen johdanto-osan 104 perustelukappaleen mukaan tietosuojan riittävyyttä koskevan päätöksen antamisen edellytykseksi on asetettava se, että rekisteröidyille taataan päätöksen kohteena olevassa kolmannessa maassa ”tehokkaat hallinnolliset *ja oikeudelliset* muutoksenhakukeinot” (kursivointi tässä). Ks. myös tietosuojatyöryhmä, EU-U.S. Privacy Shield – First Annual Joint Review, 28.11.2017, WP 255 (B.3 kohta); parlamentin 5.7.2018 antama päätöslauselma EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn tarjoaman suojan riittävyydestä, P8_TA(2018)0315 (25 ja 30 kohta) ja Euroopan tietosuojaneuvosto, EU-U.S. Privacy Shield – Second Annual Joint Review, 22.1.2019 (94–97 kohta).

194 Ks. vastaavasti tuomio 28.2.2013, uudelleenkäsittely Arango Jaramillo ym. v. EIP (C-334/12 RX-II, EU:C:2013:134, 43 kohta).

195 Tuomio Schrems (95 kohta).

196 Tietosuoja-asetuksen 15 artiklan, jonka otsikkona on ”Rekisteröidyn oikeus saada pääsy tietoihin”, 1 kohdassa säädetään, että tällä henkilöllä ”on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja jos näitä henkilötietoja käsitellään, oikeus saada pääsy henkilötietoihin”. Privacy Shield -päätöksen liitteessä II olevan II.8 kohdan a alakohdalla on sama merkitys.

197 Tuomio Tele2 Sverige (121 kohta) ja lausunto 1/15 (220 kohta). Kuten Facebook Ireland huomauttaa, ilmoitusta viranomaisten oikeudesta saada pääsy tietoihin ei siis voida edellyttää systemaattisesti. Tältä osin Euroopan ihmisoikeustuomioistuin katsoo, että ”käytännössä ei välttämättä ole mahdollista vaatia ilmoitusta jälkikäteen”, sillä tarkkailutoimenpiteiden kohteena oleva uhka ”voi jatkua vuosien tai jopa vuosikymmenten ajan” näiden toimenpiteiden lakkaamisen jälkeen, joten ilmoitus voi ”vaarantaa pitkäaikaisen tavoitteen, joka oli alun perin tarkkailun perusteena”, ja ”paljastaa tiedustelupalvelujen työskentelymenetelmät, toiminta-alueen ja – – työntekijöiden henkilöllisyyden” (tuomio Zakharov, 287 kohta oikeuskäytäntöviittauksineen). Vaikka tilanteessa, jossa ilmoitusta ei ole tehty, yksittäistapauksissa tarjottavat oikeussuojakeinot eivät siten välttämättä ole käytettävissä lakisääteisten vaatimusten noudattamatta jättämisen vuoksi, muut suojakeinot voivat riittää yksityiselämän kunnioitusta koskevan oikeuden suojaamiseen (ks. myös tuomio Centrum för Rättvisa, 164–167 ja 171–178 kohta). Ks. tämän ratkaisuehdotuksen 330 kohta.

198 Ks. tältä osin tämän ratkaisuehdotuksen alaviite 210.

322. Näiden esitysten sisältöä ei ole tarpeen tuoda yksityiskohtaisesti esille. Ennakkoratkaisua pyytänyt tuomioistuin kyseenalaistaa kyseessä olevien henkilöiden oikeussuojaan liittyvien suojatoimien riittävyyden ennen kaikkea sen vuoksi, että asiavaltuuteen (standing) liittyvät poikkeuksellisen tiukat edellytykset [199] yhdessä sen kanssa, ettei velvollisuutta ilmoittaa tarkkailutoimenpiteen kohteena oleville henkilöille ole *edes silloin, kun ilmoitus ei enää vaarantaisi sen tavoitteita*, tekevät Yhdysvaltojen oikeudessa säädettyjen oikeussuojakeinojen käyttämisestä käytännössä kohtuuttoman vaikeaa. DPC, Schrems, Itävallan, Puolan ja Portugalin hallitukset sekä Euroopan tietosuojaneuvosto yhtyvät näihin epäilyihin. [200]

323. Tyydyn tältä osin tuomaan esille, että asiavaltuutta koskevilla säännöillä ei voida vaarantaa tehokasta oikeussuojaa, [201] ja toteamaan, että Privacy Shield -päätöksessä ei mainita minkäänlaista velvollisuutta ilmoittaa rekisteröidyille siitä, että he ovat olleet tarkkailutoimenpiteen kohteena. [202] Se, ettei tällaisesta toimenpiteestä ilmoittamiseen ole velvollisuutta edes silloin, kun rekisteröidylle ilmoittaminen ei enää vaarantaisi sen tehokkuutta, vaikuttaa tämän ratkaisuehdotuksen 320 kohdassa mainitun oikeuskäytännön kannalta ongelmalliselta, koska se voisi estää oikeussuojakeinojen käyttämisen.

324. Privacy Shield -päätöksen alaviitteessä 169 myönnetään lisäksi, että käytettävissä olevat keinot ”edellyttävät joko vahingon olemassaoloa – – tai sen osoittamista, että hallitus aikoo käyttää tai luovuttaa kyseiseen henkilöön kohdistuvasta sähköisestä valvonnasta hankittuja tai johdettuja tietoja asianomaista henkilöä vastaan”. Kuten ennakkoratkaisua pyytänyt tuomioistuin, DPC ja Schrems korostavat, tämä vaatimus on ristiriidassa sen unionin tuomioistuimen oikeuskäytännön kanssa, jonka mukaan asianomaisen henkilön yksityiselämän kunnioittamista koskevaan oikeuteen puuttumisen osoittamiseksi ei ole välttämätöntä, että asianomaiselle on mahdollisesti aiheutunut haittaa väitetystä puuttumisesta. [203]

325. Facebook Irelandin ja Yhdysvaltojen hallituksen ilmaisema kanta, jonka mukaan puutteellisuudet niiden henkilöiden oikeussuojassa, joiden tietoja siirretään Yhdysvaltoihin, kompensoidaan FISC:n etu- ja jälkikäteisvalvonnalla sekä toimeenpano- ja lainsäädäntövallan piirissä käyttöön otetuilla lukuisilla valvontamekanismeilla, [204] ei mielestäni ole vakuuttava.

326. Edellä on jo todettu, että Privacy Shield -päätöksessä esitettyjen toteamusten mukaan FISC ei valvo yksittäisiä tarkkailutoimenpiteitä ennen niiden toteuttamista. [205] Kuten tämän päätöksen johdanto-osan 109 perustelukappaleessa todetaan ja kuten Yhdysvaltojen hallitus vahvisti kirjallisessa vastauksessaan unionin tuomioistuimen esittämiin kysymyksiin, valintakriteerien soveltamisen jälkikäteisvalvonnalla on tarkoitus varmistaa tilanteessa, jossa tiedusteluelin ilmoittaa FISC:lle

199 Ks. tämän ratkaisuehdotuksen 67 kohta.

200 Ks. Euroopan tietosuojaneuvosto, EU-U.S. Privacy Shield – Second Annual Joint Review, 22.1.2019 (s. 18, 97 kohta).

201 Ks. mm. tuomio 11.7.1991, Verholen ym. (C-87/90–C-89/90, EU:C:1991:314, 24 kohta oikeuskäytäntöviittauksineen) ja tuomio 28.2.2013, uudelleenkäsittely Arango Jaramillo ym. v. EIP (C-334/12 RX-II, EU:C:2013:134, 43 kohta).

202 Yhdysvaltojen hallitus on kuitenkin ennakkoratkaisua pyytäneen tuomioistuimen tavoin täsmentänyt, että FISA:n 702 §:n mukaisesta tarkkailutoimenpiteestä on ilmoitettava kohdennetulle henkilölle, jos kerättyjä tietoja käytetään tätä vastaan tuomioistuimessa käytävässä menettelyssä.

203 Tuomio 20.5.2003, Österreichischer Rundfunk ym. (C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, 75 kohta); tuomio Digital Rights Ireland (33 kohta); tuomio Schrems (87 kohta) ja lausunto 1/15 (124 kohta).

204 Nämä mekanismit kuvataan Privacy Shield -päätöksen johdanto-osan 95–110 perustelukappaleessa. Komissio erottelee ”tehokasta oikeussuojaa” koskevien sääntöjen kategoriassa toisistaan valvontamekanismit (ks. 92–110 perustelukappale) ja oikeussuojakeinot (ks. 111–124 perustelukappale).

205 Ks. tämän ratkaisuehdotuksen 298 kohta.

kohdentamis- ja minimointimenettelyjen mahdollista laiminlyöntiä koskevasta tapauksesta,[206] vuotuisessa varmennuksessa tarkoitettujen valintakriteerien määrittämisedellytysten noudattaminen. Menettely FISC:ssä ei siten näytä tarjoavan yksittäistapauksissa tehokasta oikeussuojakeinoa henkilöille, joiden tietoja siirretään Yhdysvaltoihin.

327. Vaikka Privacy Shield -päätöksen johdanto-osan 95–110 perustelukappaleessa mainituilla tuomioistuimen ulkopuolisilla valvontamenettelyillä voitaisiin tarvittaessa vahvistaa mahdollisia oikeussuojakeinoja, ne eivät nähdäkseni riittäisi varmistamaan tietosuojan riittävää tasoa siltä osin kuin kyse on rekisteröityjen oikeudesta oikeussuojakeinoihin. Varsinkaan kunkin elimen sisäiseen rakenteeseen kuuluvat valvontaviranomaiset eivät mielestäni ole riippumattomia valvontamekanismeja. PCLOB:n ja kongressin tiedusteluvaliokuntien harjoittama valvonta ei puolestaan vastaa yksittäistapauksissa tarjottavan oikeussuojakeinon mekanismia tarkkailutoimenpiteitä vastaan.

328. Näin ollen on tutkittava, korjataanko oikeusasiamiesmekanismilla nämä puutteet siten, että tarjotaan rekisteröidyille tehokas oikeussuojakeino riippumattomassa ja puolueettomassa elimessä.[207]

329. Arvioitaessa, onko Privacy Shield -päätöksessä esitetty toteamus tietosuojan riittävyydestä perusteltu niiden henkilöiden käytettävissä olevien oikeussuojakeinojen kannalta, jotka uskovat olleensa EO 12333:een perustuvan tarkkailun kohteena, asian kannalta merkityksellisen viitekehyksen muodostavat – kuten on muistettava – Euroopan ihmisoikeussopimuksen määräykset.

330. Kuten edellä on selostettu,[208] arvioidessaan, täyttääkö tarkkailutoimenpide edellytykset ”ennakoitavuudesta” ja ”välttämättömyydestä demokraattisessa yhteiskunnassa” Euroopan ihmisoikeussopimuksen 8 artiklan 2 kappaleessa tarkoitetulla tavalla,[209] Euroopan ihmisoikeustuomioistuin tekee kokonaisarvioinnin valvonta- ja tarkkailumekanismeista, jotka on pantu täytäntöön ”ennen” toimenpiteen toteuttamista, sen ”aikana” tai sen ”jälkeen”. Kun oikeussuojakeinoa ei voida yksittäistapauksessa käyttää sen vuoksi, että tarkkailutoimenpiteestä ilmoittaminen ei ole mahdollista sen tehokkuutta vaarantamatta,[210] tämä puute voidaan korjata harjoittamalla riippumatonta valvontaa ennen kyseisen toimenpiteen toteuttamista.[211] Vaikka Euroopan ihmisoikeustuomioistuin pitää tällaista ilmoitusta ”toivottavana”, jos se on mahdollinen tarkkailutoimenpiteen tehokkuutta muuttamatta, se ei ole asettanut sitä vaatimukseksi.[212]

331. Tältä osin Privacy Shield -päätöksestä ei ilmene, että EO 12333:een perustuvista tarkkailutoimenpiteistä ilmoitettaisiin asianomaisille henkilöille tai että niiden mihinkään hyväksymis- tai täytäntöönpanovaiheeseen liittyisi tuomioistuinvalvontaa tai hallinnollista valvontaa koskevia riippumattomia mekanismeja.

206 Privacy Shield -päätöksen johdanto-osan 109 perustelukappaleen mukaan ”oikeusministeri ja [NSA:n] johtaja tarkastavat, että vaatimuksia noudatetaan, ja virastojen on raportoitava kaikista vaatimustenvastaisista tapauksista FISC-tuomioistuimelle – –, joka tällä perusteella voi muuttaa lupaa”.

207 Ks. tämän ratkaisuehdotuksen 333–340 kohta.

208 Ks. tämän ratkaisuehdotuksen 305 kohta.

209 Euroopan ihmisoikeustuomioistuin on televiestinnän tarkkailutoimenpiteitä koskevassa oikeuskäytännössään käsitellyt kysymystä oikeussuojakeinoista tarkastellessaan ”lakia” koskevaa edellytystä ja Euroopan ihmisoikeussopimuksen 8 artiklassa taattuun oikeuteen puuttumisen välttämättömyyttä (ks. mm. tuomio Zakharov (236 kohta) ja tuomio Centrum för Rättvisa (107 kohta). Todettuaan 1.7.2008 antamassaan tuomiossa Liberty ym. v. Yhdistynyt kuningaskunta (CE:ECHR:2008:0701JUD005824300, 73 kohta) ja tuomiossa Zakharov (307 kohta) Euroopan ihmisoikeussopimuksen 8 artiklaa rikotun Euroopan ihmisoikeustuomioistuin ei pitänyt tarpeellisena tutkia erikseen tämän sopimuksen 13 artiklaan perustuvaa väitettä.

210 Euroopan ihmisoikeustuomioistuin katsoo, että vaikka ilmoituksen puuttuminen jossakin vaiheessa ei välttämättä ole esteenä sille, että tarkkailutoimenpide täyttää edellytyksen ”välttämättömyydestä demokraattisessa yhteiskunnassa”, se vaarantaa oikeuden saattaa asia tuomioistuimen käsiteltäväksi ja siten oikeussuojakeinojen tehokkuuden (ks. mm. tuomio 6.9.1978, Klass ym. v. Saksa (CE:ECHR:1978:0906JUD000502971, 57 ja 58 kohta); päätös Weber ja Saravia (135 kohta) ja tuomio Zakharov (302 kohta)).

211 Ks. vastaavasti tuomio Centrum för Rättvisa (105 kohta).

212 Tuomiossa Big Brother Watch (317 kohta) Euroopan ihmisoikeustuomioistuin kieltäytyi lisäämästä vähimmäistakeisiin, joita sovelletaan tarkkailujärjestelmään, jolle on ominaista laajamittainen sähköisen viestinnän kaappaus, vaatimusta tarkkailusta ilmoittamisesta asianomaisille henkilöille. Ks. myös tuomio Centrum för Rättvisa (164 kohta). Näiden tuomioiden Euroopan ihmisoikeustuomioistuimen suureen jaostoon palauttamisen tarkoituksena on erityisesti tämän johtopäätöksen uudelleenkäsittely.

332. Tässä tilanteessa on tutkittava, voidaanko oikeusasiamieheen turvautumalla kuitenkin varmistaa tarkkailutoimenpiteiden riippumaton valvonta myös silloin, kun ne perustuvat EO 12333:een.

2) Oikeusasiamiesmekanismin vaikutus tehokasta oikeussuojakeinoa koskevan oikeuden suojan tasoon

333. Privacy Shield -päätöksen johdanto-osan 116 perustelukappaleen mukaan tämän päätöksen liitteessä III A kuvatulla oikeusasiamiesmekanismilla on tarkoitus tarjota kaikille henkilöille, joiden tietoja siirretään unionista Yhdysvaltoihin, yksi oikeussuojakeino lisää.

334. Kuten Yhdysvaltojen hallitus korostaa, oikeusasiamiehelle tehdyn kantelun tutkittavaksi ottamisen edellytykseksi ei ole asetettu vastaavanlaisten asiavaltuutta koskevien sääntöjen noudattamista kuin oikeudelle saada asiansa Yhdysvaltojen tuomioistuinten käsiteltäväksi. Kyseisen päätöksen johdanto-osan 119 perustelukappaleessa täsmennetään tältä osin, että oikeusasiamieheen turvautuminen ei edellytä henkilön osoittavan, että Yhdysvaltojen hallitus on päässyt hänen henkilötietoihinsa käsiksi.

335. DPC:n, Schremsin, Puolan ja Portugalin hallitusten sekä EPIC:n tavoin epäilen, voidaanko tällä mekanismilla kompensoida henkilöille, joiden tietoja siirretään unionista Yhdysvaltoihin, tarjotun oikeussuojan puutteellisuudet.

336. Heti alkuun on todettava, että vaikka tuomioistuimen ulkopuolinen oikeussuojakeinomekanismi voi olla [perusoikeuskirjan] 47 artiklassa tarkoitettu tehokas oikeussuojakeino, näin on kuitenkin ainoastaan erityisesti, jos kyseinen elin on lakisääteinen ja täyttää riippumattomuuden edellytyksen.[213]

337. Privacy Shield -päätöksestä ilmenee, että oikeusasiamiesmekanismi, jonka perustana on PPD 28,[214] ei perustu lakiin. Ulkoministeri nimeää oikeusasiamiehen, ja tämä kuuluu erottamattomasti Yhdysvaltojen ulkoasiainministeriöön.[215] Tässä päätöksessä ei ole mitään viitettä siitä, että oikeusasiamiehen irtisanomiseen tai nimityksen kumoamiseen liittyisi erityisiä takeita.[216] Vaikka oikeusasiamiehen esitetään olevan ”tiedusteluyhteisöstä riippumaton”, hän raportoi ulkoministerille eikä siten ole riippumaton toimeenpanovallasta.[217]

338. Tuomioistuimen ulkopuolisen oikeussuojakeinon tehokkuus riippuu nähdäkseni myös siitä, voiko kyseinen elin tehdä sitovia ja perusteltuja päätöksiä. Tältä osin Privacy Shield -päätös ei sisällä mitään viitettä siitä, että oikeusasiamies tekisi tällaisia päätöksiä. Siinä ei todeta, että hakijat saisivat oikeusasiamiesmekanismin perusteella pääsyn itseään koskeviin tietoihin ja nämä tiedot oikaistuiksi tai poistetuiksi tai että oikeusasiamies myöntäisi korvauksen tarkkailutoimenpiteen vuoksi vahinkoa kärsineille. Kuten tämän päätöksen liitteessä III A olevan 4 kohdan e alakohdasta ilmenee, ”oikeusasiamies ei vahvista eikä kiistä, onko henkilö ollut tarkkailun kohteena, eikä ilmoita, mitä

213 Riippumattomuuden käsitteen ensimmäinen, ulkoinen osatekijä edellyttää, että asianomainen elin on suojattu sellaisilta ulkoisilta toimenpiteiltä tai painostuksilta, jotka voivat vaarantaa sen jäsenten päätöksenteon riippumattomuuden heidän käsiteltäväkseen saatetuissa asioissa. Tämän käsitteen toinen, sisäinen osatekijä liittyy puolestaan puolueettomuuden käsitteeseen ja merkitsee sitä, että tuomioistuin ylläpitää yhtäläistä etäisyyttä oikeusriidan asianosaisiin ja siihen, mitkä ovat heidän intressinsä oikeusriidan kohteeseen. Ks. mm. tuomio 19.9.2006, Wilson (C-506/04, EU:C:2006:587, 50–52 kohta); tuomio 25.7.2018, Minister for Justice and Equality (Tuomioistuinjärjestelmän puutteet) (C-216/18 PPU, EU:C:2018:586, 63 ja 65 kohta) ja tuomio 19.11.2019, A. K. ym. (Ylimmän tuomioistuimen kurinpitojaoston riippumattomuus) (C-585/18, C-624/18 ja C-625/18, EU:C:2019:982, 121 ja 122 kohta). Vallanjako-opin mukaisesti tuomioistuinten riippumattomuus muun muassa toimeenpanovallasta on taattava. Ks. tuomio 19.11.2019, A. K. ym. (Ylimmän tuomioistuimen kurinpitojaoston riippumattomuus) (C-585/18, C-624/18 ja C-625/18, EU:C:2019:982, 127 kohta oikeuskäytäntöviittauksineen).

214 Privacy Shield -päätöksen liitteessä III A viitataan tältä osin PPD 28:n 4 §:n d momenttiin.

215 Ks. Privacy Shield -päätöksen johdanto-osan 116 perustelukappale.

216 Unionin tuomioistuin korosti 31.5.2005 antamassaan tuomiossa Syfait ym. (C-53/03, EU:C:2005:333, 31 kohta) tällaisten takeiden merkitystä riippumattomuuden edellytyksen täyttämisessä. Ks. tältä osin myös tuomio 24.6.2019, komissio v. Puola (Ylimmän tuomioistuimen riippumattomuus) (C-619/18, EU:C:2019:531, 76 kohta) ja tuomio 5.11.2019, komissio v. Puola (Yleisten tuomioistuinten riippumattomuus) (C-192/18, EU:C:2019:924, 113 kohta).

217 Ks. Privacy Shield -päätöksen johdanto-osan 65 ja 121 perustelukappale sekä liite III A, 1 kohta.

nimenomaista korjaavaa toimenpidettä asiassa on sovellettu”.[218] Vaikka Yhdysvaltojen hallitus on sitoutunut siihen, että tiedustelupalvelujen asianomaisen toimijan on korjattava kaikki oikeusasiamiehen havaitsemat sovellettavien sääntöjen rikkomiset,[219] kyseisessä päätöksessä ei viitata lakisääteisiin suojatoimiin, jotka liittyisivät tähän sitoumukseen ja joihin kyseiset henkilöt voisivat vedota.

339. Oikeusasiamiesmekanismin käyttöönotolla ei siten mielestäni tarjota riippumattomassa elimessä oikeussuojakeinoa antamalla henkilöille, joiden tietoja siirretään, mahdollisuus vedota tietoihin pääsyä koskevaan oikeuteensa tai siihen, että tiedustelupalvelut ovat mahdollisesti rikkoneet sovellettavia sääntöjä.

340. Oikeuskäytännön mukaan perusoikeuskirjan 47 artiklassa taatun oikeuden kunnioittaminen edellyttää, että tämän hallintoviranomaisen, joka ei itse täytä riippumattomuudelle asetettuja edellytyksiä, päätöstä valvoo myöhemmin tuomioistuin, jolla on toimivalta tutkia kaikki merkitykselliset kysymykset.[220] Privacy Shield -päätöksessä esitettyjen tietojen mukaan oikeusasiamiehen päätökset eivät kuitenkaan ole riippumattoman tuomioistuinvalvonnan kohteena.

341. Tässä tilanteessa – samoin kuin DPC, Schrems, EPIC sekä Puolan ja Portugalin hallitukset toteavat – mielestäni on kyseenalaista, vastaako Yhdysvaltojen oikeusjärjestyksessä henkilöille, joiden tietoja siirretään sinne unionista, tarjottu oikeussuoja pääosiltaan tietosuoja-asetukseen, luettuna perusoikeuskirjan 47 artiklan ja Euroopan ihmisoikeussopimuksen 8 artiklan valossa, perustuvaa oikeussuojaa.

342. Kaiken edellä esitetyn perusteella minulla on tiettyjä epäilyjä siitä, onko Privacy Shield -päätös tietosuoja-asetuksen 45 artiklan 1 kohdan, luettuna perusoikeuskirjan 7, 8 ja 47 artiklan ja Euroopan ihmisoikeussopimuksen 8 artiklan valossa, mukainen.

V Ratkaisuehdotus

343. Ehdotan, että unionin tuomioistuin vastaa High Courtin esittämiin ennakkoratkaisukysymyksiin seuraavasti:

Ennakkoratkaisukysymysten tarkastelussa ei ole tullut esiin seikkoja, jotka voisivat vaikuttaa Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen siirtoa varten kolmansiin maihin sijoittautuneille henkilötietojen käsittelijöille 5.2.2010 annetun komission päätöksen 2010/87/EU, sellaisena kuin se on muutettuna 16.12.2016 annetulla komission täytäntöönpanopäätöksellä (EU) 2016/2297, pätevyyteen.

218 Lisäksi Privacy Shield -päätöksen johdanto-osan 121 perustelukappaleessa todetaan, että ”oikeusasiamiehen on ’vahvistettava’, että i) valitus on tutkittu asianmukaisesti ja että ii) sovellettavaa Yhdysvaltojen lainsäädäntöä – erityisesti liitteessä VI esitettyjä rajoituksia ja suojatoimia – on noudatettu, tai jos periaatteita ei noudateta, rikkominen on korjattu”.

219 Komissio toteaa Privacy Shield -järjestelyn kolmannessa vuotuisessa tarkistuksessa, että Yhdysvaltojen hallituksen lausuntojen mukaan tilanteessa, jossa oikeusasiamiehen tutkinnassa paljastuisi, että FISC:n hyväksymiä kohdentamis- ja minimointimenettelyjä ei ole noudatettu, tästä noudattamatta jättämisestä olisi ilmoitettava tälle tuomioistuimelle. FISC suorittaisi tällöin riippumattoman tutkimuksen ja tarvittaessa velvoittaisi asianomaisen tiedusteluelimen korjaamaan kyseisen noudattamatta jättämisen. Ks. Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, 23.10.2019, SWD(2019) 390 final, s. 28. Komissio viittaa siinä asiakirjaan, jonka otsikkona on ”Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure”, saatavilla osoitteessa https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (s. 4 ja 5).

220 Ks. tuomio 16.5.2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, 55 kohta) ja tuomio 13.12.2017, El Hassani (C-403/16, EU:C:2017:960, 39 kohta).