Oikeustapauskokoelma

JULKISASIAMIEHEN RATKAISUEHDOTUS
YVES BOT
23 päivänä syyskuuta 2015 [1]

Asia C-362/14

Maximillian Schrems
vastaan
Data Protection Commissioner

(Ennakkoratkaisupyyntö – High Court (Irlanti))

Ennakkoratkaisupyyntö — Henkilötiedot — Yksilöiden suojelu näiden tietojen käsittelyssä — Euroopan unionin perusoikeuskirja — 7, 8 ja 47 artikla — Direktiivi 95/46/EY — 25 artikla — Päätös 2000/520/EY — Henkilötietojen siirtäminen Yhdysvaltoihin — Tietosuojan tason riittävyyden tai riittämättömyyden arviointi — Sellaisen luonnollisen henkilön tekemä kantelu, jonka tiedot on siirretty kolmanteen maahan — Kansallinen valvontaviranomainen — Valtuudet

I **Johdanto**

1. Kuten Euroopan komissio on todennut 27.11.2013 päivätyssä tiedonannossaan, [2] ”henkilötietojen siirto on tärkeä ja välttämätön osa transatlanttisia suhteita. Se on olennainen osa Atlantin yli käytävää kauppaa, jonka yhteydessä siirretään suuria tietomääriä EU:sta Yhdysvaltoihin. Tämä koskee myös muun muassa sosiaalisen median tai pilvipalvelujen alalla toimivia uusia kasvavia digitaaliyrityksiä”. [3]

2. Kyseisestä kaupankäynnistä tehtiin 26.7.2000 komission päätös 2000/520/EY Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä. [4] Tämä päätös on oikeudellisena perustana henkilötietojen siirrolle unionista Yhdysvaltoihin sijoittautuneille yrityksille, jotka noudattavat safe harbor -periaatteita.

3. Kyseisen päätöksen kohtalo on tällä hetkellä vaakalaudalla, kun tietovirta unionin ja Yhdysvaltojen välillä sallitaan samalla kun pitäisi taata näiden tietojen suojan korkea taso, kuten unionin oikeudessa edellytetään.

4. Viime aikoina on näet tehty tiettyjä paljastuksia Yhdysvaltojen laajamittaisista tiedonkeruuohjelmista. Nämä paljastukset ovat herättäneet huolta siitä, noudatetaanko unionin oikeussääntöjä siirrettäessä henkilötietoja Yhdysvaltoihin sijoittautuneille yrityksille, ja safe harbor -järjestelmän heikkouksista.

1 — Alkuperäinen kieli: ranska.

2 — Komission tiedonanto Euroopan parlamentille ja neuvostolle ”Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon” (COM(2013) 846 final).

3 — S. 2.

4 — EYVL L 215, s. 7, ja oikaisu EYVL 2001, L 115, s. 14.

5. Nyt käsiteltävässä ennakkoratkaisupyynnössä pyydetään unionin tuomioistuinta täsmentämään, miten kansallisten valvontaviranomaisten ja komission pitäisi suhtautua häiriöihin, joita tapahtuu päätöksen 2000/520 soveltamisessa.

6. Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY [5] IV luvussa vahvistetaan säännöt, joita sovelletaan henkilötietojen siirtoon kolmansiin maihin.

7. Tämän direktiivin kyseisen luvun 25 artiklan 1 kohdassa vahvistetaan periaate, jonka mukaan käsiteltävien tai siirron jälkeen käsiteltäviksi tarkoitettujen henkilötietojen siirto kolmanteen maahan voidaan suorittaa ainoastaan, jos kyseisessä kolmannessa maassa taataan tietosuojan riittävä taso.

8. Toisaalta on niin, kuten unionin lainsäätäjä toteaa kyseisen direktiivin johdanto-osan 57 perustelukappaleessa, että jos tietosuojan taso kolmannessa maassa ei ole riittävä, henkilötietojen siirto kyseiseen maahan on kiellettävä.

9. Direktiivin 95/46 25 artiklan 2 kohdan mukaan ”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”.

10. Kyseisen direktiivin 25 artiklan 6 kohdan nojalla komissio voi todeta, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso, mikä johtuu kyseisen maan sisäisestä lainsäädännöstä tai kansainvälisistä sitoumuksista. Kun komissio on tehnyt tällaisen päätöksen, henkilötiedot voidaan siirtää asianomaiseen kolmanteen maahan.

11. Komissio teki kyseisen säännöksen täytäntöön panemiseksi päätöksen 2000/520. Tämän päätöksen 1 artiklan 1 kohdasta ilmenee, että ”yksityisyyden suojaa koskevien – – safe harbor -periaatteiden”, joita sovelletaan ”tavallisimpien kysymysten” [6] tarjoaman ohjauksen mukaisesti, katsotaan varmistavan unionista Yhdysvaltoihin sijoittautuneille yrityksille siirrettyjen henkilötietojen riittävän suojelun tason.

12. Näin ollen päätöksessä 2000/520 sallitaan henkilötietojen siirto jäsenvaltioista Yhdysvaltoihin sijoittautuneille yrityksille, jotka ovat sitoutuneet noudattamaan safe harbor -periaatteita.

13. Päätöksen 2000/520 liitteessä I vahvistetaan tiettyjä periaatteita, joihin yritykset voivat sitoutua vapaaehtoisesti ja joihin liittyy rajoituksia ja erityinen valvontajärjestelmä. Niiden yritysten lukumäärä, jotka ovat sitoutuneet näihin ”käytännesääntöihin”, ylitti 3 200 vuonna 2013.

14. Safe harbor -järjestelmä perustuu ratkaisuun, jossa yhdistetään yksityisten yritysten oma varmennus ja itsearviointi sekä julkisen vallan toimenpiteet.

15. Safe harbor -periaatteet on laadittu ”yhdessä elinkeinoelämän ja kuluttajien edustajien kanssa Yhdysvaltojen ja Euroopan unionin välisen kaupankäynnin helpottamiseksi. Ne on tarkoitettu käytettäviksi yksinomaan yhdysvaltalaisissa yrityksissä, jotka saavat henkilötietoja Euroopan unionista ja jotka käyttävät periaatteiden noudattamista keinona safe harbor -järjestelmään osallistumiselle asetettujen kelpoisuusvaatimusten täyttämiseksi ja sen luoman tietosuojan riittävyyden olettamuksen saavuttamiseksi”. [7]

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

6 — Frequently asked questions, jäljempänä FAQ.

7 — Päätöksen 2000/520 liitteessä I oleva toinen kohta.

16. Päätöksen 2000/520 liitteessä I olevissa safe harbor -periaatteissa säädetään muun muassa

— ilmoitusvelvollisuudesta, jonka mukaan ”organisaation on ilmoitettava yksityishenkilöille, mihin tarkoitukseen se kerää ja käyttää heitä koskevia tietoja, miten organisaatioon saa yhteyden lisätietoja ja valituksia varten, minkälaisille kolmansille osapuolille se antaa tietoja sekä minkälaisia valintoja ja keinoja organisaatio tarjoaa henkilöille tietojen käytön ja luovuttamisen rajoittamiseksi. Ilmoitus on tehtävä – – samassa yhteydessä, kun henkilöitä ensimmäisen kerran pyydetään antamaan henkilötietoja organisaatiolle tai niin pian tämän jälkeen kuin mahdollista. Ilmoitus on joka tapauksessa tehtävä ennen kuin organisaatio käyttää tällaisia tietoja muuhun tarkoitukseen kuin siihen, mitä varten tiedot on alun perin kerätty tai mitä varten tiedot siirtävä organisaatio on ne käsitellyt tai luovuttaa ne ensimmäisen kerran kolmannelle osapuolelle” [8]

— organisaatioille asetetusta velvollisuudesta tarjota asianomaisille henkilöille mahdollisuus valita, voidaanko heidän tietojaan antaa kolmannelle osapuolelle tai käyttää tarkoitukseen, joka ei vastaa tietojen keruun alkuperäistä tarkoitusta tai tarkoitusta, johon rekisteröity on myöhemmin antanut luvan. Arkaluonteisten tietojen osalta ”kyseisten henkilöiden on tehtävä myönteinen tai selkeästi ilmaistu (opt in) valinta, jos tietoja aiotaan antaa kolmannelle osapuolelle tai käyttää muuhun kuin alkuperäiseen tarkoitukseen kuin mihin henkilö on aiemmin antanut selkeän suostumuksensa tehdessään valinnan (opt in)” [9]

— tiedon siirtämistä edelleen koskevista säännöistä. Organisaatio voi siten antaa tietoja kolmannelle osapuolelle ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti [10]

— tietoturvan osalta velvollisuudesta organisaatioille, ”jotka luovat, säilyttävät, käyttävät tai toimittavat edelleen henkilötietoja, [toteuttaa] riittävät varotoimet tietojen katoamisen, väärinkäytösten ja vääriin käsiin joutumisen, paljastumisen, muuttamisen ja hävittämisen ehkäisemiseksi” [11]

— tietojen koskemattomuuden osalta organisaatioiden velvollisuudesta toteuttaa ”tarvittavat toimet sen varmistamiseksi, että tiedot ovat käyttötarkoitukseensa nähden luotettavia ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia” [12]

— siitä, että ”henkilöiden on saatava itseään koskevat tiedot organisaatiolta ja voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä” [13]

— velvollisuudesta ottaa käyttöön ”menettelyt, joilla varmistetaan tietosuojaperiaatteiden noudattaminen ja organisaatiolle koituvat seuraamukset niiden noudattamatta jättämisestä. Siihen on myös sisällyttävä valitusmenettely, johon henkilö voi vedota silloin, kun häntä koskeviin tietoihin ei ole sovellettu periaatteita”. [14]

17. Amerikkalaisen organisaation, joka haluaa sitoutua safe harbor -periaatteisiin, on vahvistettava yksityisyyden suojaa koskevassa ohjelmassaan sitoutuvansa näihin periaatteisiin ja tosiasiallisesti noudattavansa niitä sekä suoritettava oma varmennuksensa ilmoittamalla Yhdysvaltojen kauppaministeriölle, että se noudattaa näitä periaatteita. [15]

8 — Ks. liite I, otsikko ”Ilmoitus”.

9 — Ks. liite I, otsikko ”Valinta”.

10 — Ks. liite I, otsikko ”Tiedon siirtäminen edelleen”.

11 — Ks. liite I, otsikko ”Turvallisuus”.

12 — Ks. liite I, otsikko ”Tietojen koskemattomuus”.

13 — Ks. liite I, otsikko ”Tiedonsaanti”.

14 — Ks. liite I, otsikko ”Täytäntöönpano”.

15 — Päätöksen 2000/520 1 artiklan 2 ja 3 kohta. Ks. myös liite II, FAQ 6.

18. Organisaatioilla on lukuisia tapoja noudattaa safe harbor -periaatteita. Ne voivat esimerkiksi liittyä ”yksityissektorilla kehitettyyn, kyseisten periaatteiden mukaiseen tietosuojaohjelmaan [tai kehittää] omat tietosuojaa koskevat toimintalinjansa, mikäli ne ovat safe harbor -periaatteiden mukaiset. – – Lisäksi organisaatiot, joihin sovelletaan yleistä, sääntelevää, hallinnollista tai muuta lainsäädäntöä taikka säännöstöä, joka takaa tehokkaan henkilötietosuojan, voivat liittyä safe harbor -järjestelmään”. [16]

19. Useita mekanismeja, joissa yhdistetään yksityinen välitysmenettely ja viranomaisten harjoittama valvonta, on käytössä sen varmistamiseksi, että safe harbor -periaatteita noudatetaan. Valvontaa voi siten harjoittaa riippumaton kolmas osapuoli tuomioistuinten ulkopuolisen riitojenratkaisujärjestelmän välityksellä. Lisäksi yritykset voivat sitoutua yhteistyöhön unionin tietosuojapaneelin kanssa. Toimivaltaisia käsittelemään kanteluja ovat liittovaltion kauppakomissio (Federal Trade Commission, jäljempänä FTC) niiden valtuuksien perusteella, jotka sille annetaan liittovaltion kauppakomissiosta annetun lain (Federal Trade Commission Act) 5 §:n nojalla, ja Yhdysvaltojen liikenneministeriö (Department of Transportation) niiden valtuuksien nojalla, jotka sille annetaan Yhdysvaltojen lakikokoelman (United States Code) 49 osaston 41712 §:n nojalla.

20. Päätöksen 2000/520 liitteessä I olevan neljännen kohdan mukaan safe harbor -periaatteiden noudattamista voidaan rajoittaa erityisesti ”siinä määrin, kuin se on tarpeen kansallisen turvallisuuden, yleisen edun ja [Yhdysvaltojen] lainsäädännön vaatimusten vuoksi”, ja ”lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä, joilla syntyy ristiriitaisia velvoitteita tai joilla selkeästi annetaan lupa tiettyyn toimintaan, sillä edellytyksellä, että aina tällaista lupaa käyttäessään organisaatio voi osoittaa, että periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi”. [17]

21. Lisäksi jäsenvaltioiden toimivaltaisten viranomaisten mahdollisuudelle keskeyttää tiedonsiirto asetetaan useita edellytyksiä, joista säädetään päätöksen 2000/520 3 artiklan 1 kohdassa.

22. Nyt käsiteltävän ennakkoratkaisupyynnön vuoksi on tarkasteltava päätöksen 2000/520 ulottuvuutta Euroopan unionin perusoikeuskirjan (jäljempänä perusoikeuskirja) 7, 8 ja 47 artiklan sekä direktiivin 95/46 25 artiklan 6 kohdan ja 28 artiklan kannalta. Tämä pyyntö on esitetty riidassa, jossa ovat vastakkain Schrems ja Data Protection Commissioner (tietosuojavaltuutettu) ja joka koskee sitä, että viimeksi mainittu on kieltäytynyt tutkimasta kantelua, jonka Schrems oli tehnyt sen vuoksi, että Facebook Ireland Ltd. (jäljempänä Facebook Ireland) säilyttää käyttäjiensä henkilötietoja Yhdysvalloissa sijaitsevilla palvelimilla.

23. Schrems on Itävallan kansalainen, joka asuu Itävallassa. Hän on ollut Facebookin sosiaalisen verkoston jäsen vuodesta 2008 lähtien.

24. Kaikkia Facebookin käyttäjiä, jotka asuvat unionin alueella, pyydetään tekemään sopimus Facebook Irelandin kanssa; tämä on Yhdysvalloissa sijaitsevan emoyhtiön Facebook Inc:n (jäljempänä Facebook USA) tytäryhtiö. Unionin alueella asuvien Facebook Irelandin käyttäjien tiedot siirretään kokonaan tai osittain Facebook USA:n palvelimille, jotka sijaitsevat Yhdysvaltojen alueella, ja säilytetään siellä.

25. Schrems teki 25.6.2013 tietosuojavaltuutetulle kantelun, jossa hän vetosi lähinnä siihen, että Yhdysvaltojen oikeus ja käytännöt eivät tarjonneet mitään tosiasiallista suojaa valtion harjoittamaa tarkkailua vastaan tiedoille, joita säilytettiin Yhdysvaltojen alueella. Tämä ilmeni hänen mukaansa paljastuksista, joita Edward Snowden oli tehnyt toukokuusta 2013 lähtien Yhdysvaltojen tiedustelupalvelujen, erityisesti kansallisen turvallisuusviranomaisen (National Security Agency, jäljempänä NSA) toiminnasta.

16 — Liitteessä I oleva kolmas kohta.

17 — Ks. myös liitteessä IV oleva B kohta.

26. Näistä paljastuksista ilmenee muun muassa, että NSA oli ottanut käyttöön ns. ”PRISM”-ohjelman, jonka yhteydessä tämä virasto oli saanut vapaan pääsyn massatietoihin, joita oli tallennettu Yhdysvalloissa sijaitseville palvelimille, jotka olivat useiden internet- ja teknologia-alalla toimivien yhtiöiden, kuten Facebook USA:n omistuksessa tai valvonnassa.

27. Tietosuojavaltuutettu arvioi, ettei se ollut velvollinen tutkimaan kantelua, koska sillä ei ollut oikeudellista perustaa. Se katsoi, ettei ollut näyttöä siitä, että NSA olisi päässyt Schremsin tietoihin. Sen mielestä kantelu piti hylätä myös päätöksen 2000/520 vuoksi, koska komissio oli todennut siinä, että Yhdysvalloissa taataan siirrettyjen henkilötietojen tietosuojan riittävä taso. Kaikki kysymykset, jotka liittyvät näiden tietojen suojan riittävyyteen Yhdysvalloissa, pitäisi ratkaista tämän päätöksen mukaisesti, mikä estää sen mukaan kantelussa esiin tuodun ongelman tutkimisen.

28. Kansallinen lainsäädäntö, jonka perusteella tietosuojavaltuutettu hylkäsi kantelun, on seuraava.

29. Vuoden 1988 tietosuojalain (Data Protection Act), sellaisena kuin se on muutettuna vuoden 2003 tietosuojalailla (Data Protection (Amendment) Act 2003, jäljempänä tietosuojalaki), 10 §:n 1 momentissa annetaan tietosuojavaltuutetulle toimivalta tutkia kantelut ja säädetään seuraavaa:

”a) Tietosuojavaltuutettu voi tutkia tai tutkituttaa, onko tämän lain säännöksiä rikottu tai saatetaanko niitä rikkoa tietyn henkilön osalta, joko sillä perusteella, että tämä henkilö kantelee hänelle minkä tahansa näiden säännösten rikkomisesta, tai sillä perusteella, että tietosuojavaltuutettu arvioi, että kilpailusääntöjä on saatettu rikkoa tällä tavoin.

b) Jos henkilö tekee tietosuojavaltuutetulle kantelun tämän momentin a kohdan perusteella, tietosuojavaltuutettu:

i) tutkii tai tutkituttaa kantelun, ellei hän katso, että kantelu on turha tai se on tehty haitantekona, ja,

ii) mikäli hän ei voi saada kohtuullisessa ajassa asianomaisia osapuolia sopimaan vapaaehtoisesti kantelun kohteesta, hän antaa kantelijalle kantelusta tekemänsä päätöksen tiedoksi kirjallisesti ja ilmoittaa, että jos tämä päätös on kantelijalle vastainen, tämä voi hakea siihen muutosta tuomioistuimessa tämän lain 26 §:n nojalla 21 päivän kuluessa tiedoksiannon vastaanottamisesta.”

30. Tässä tapauksessa tietosuojavaltuutettu päätteli, että Schremsin kantelu oli ”turha tai haitantekoa” siten, että sillä ei ollut menestymisen mahdollisuuksia, koska sillä ei ollut oikeudellista perustaa. Se kieltäytyi tällä perusteella tutkimasta kyseistä kantelua.

31. Tietosuojalain 11 §:ssä säännellään henkilötietojen siirrosta kansallisen alueen ulkopuolelle. Sen 11 §:n 2 momentin a kohdassa säädetään seuraavaa:

”Kun tällä lailla säännellyssä menettelyssä tulee esiin kysymys, joka koskee

i) sen määrittämistä, taataanko Euroopan talousalueen [(ETA)] ulkopuolisessa maassa tai ulkopuolisella alueella, jonne henkilötietoja siirretään, tämän pykälän 1 momentissa täsmennetty suojan riittävä taso, ja

ii) tällaisista siirroista on tehty unionin toteamus,

kysymys ratkaistaan tämän toteamuksen mukaisesti.”

32. Tietosuojalain 11 §:n 2 momentin b kohdassa määritellään unionin toteamuksen käsite seuraavasti:

”Tämän momentin a kohdassa ’unionin toteamuksella’ tarkoitetaan toteamusta, jonka – – komissio on tehnyt direktiivin [95/46] 25 artiklan 4 tai 6 kohdan soveltamiseksi sen 31 artiklan 2 kohdassa säädetyn menettelyn mukaisesti siitä, taataanko [ETA:n] ulkopuolisessa maassa tai ulkopuolisella alueella tämän artiklan 1 kohdassa täsmennetyn suojan riittävä taso.”

33. Tietosuojavaltuutettu huomautti, että päätös 2000/520 oli tietosuojalain 11 §:n 2 momentin a kohdassa tarkoitettu ”unionin toteamus”, joten tämän lain nojalla kaikki kysymykset, jotka liittyvät tietosuojan riittävyyteen kolmannessa maassa, jonne tiedot siirretään, pitäisi ratkaista tämän toteamuksen mukaisesti. Tietosuojavaltuutettu arvioi Schremsin kantelun pääsisällöstä eli siitä, että henkilötietoja siirrettiin kolmanteen maahan, jossa ei käytännössä taattu tietosuojan riittävää tasoa, että jo päätöksen 2000/520 luonne ja olemassaolo estivät häntä tutkimasta tätä kysymystä.

34. Schrems nosti High Courtissa kanteen tästä tietosuojavaltuutetun päätöksestä hylätä hänen kantelunsa. Tutkittuaan pääasian oikeudenkäynnissä esitetyt todisteet tämä tuomioistuin totesi, että henkilötietojen sähköinen tarkkailu ja sieppaaminen vastaavat yleisen edun mukaisia tarpeellisia ja välttämättömiä tavoitteita eli kansallisen turvallisuuden säilyttämistä ja vakavien rikosten estämistä. High Court esittää tässä yhteydessä, että unionista Yhdysvaltoihin siirrettyjen henkilötietojen tarkkailu ja sieppaaminen palvelevat terrorismin torjuntaan liittyviä hyväksyttäviä tavoitteita.

35. Tämän saman tuomioistuimen mukaan Snowdenin paljastukset ovat kuitenkin osoittaneet, että NSA ja muut vastaavat elimet olivat ylittäneet hyväksyttävyyden rajat merkittävällä tavalla. Vaikka Foreign Intelligence Surveillance Court (jäljempänä FISC), joka toimii ulkomaisten tiedustelupalvelujen tarkkailusta vuonna 1978 annetun lain (Foreign Intelligence Surveillance Act) nojalla,[18] harjoittaa valvontaa, siinä käytävä menettely on kuitenkin salainen eikä se ole kontradiktorinen menettely. Sen lisäksi, että henkilötietoihin tutustumista koskevaan oikeuteen liittyvät päätökset tehdään Yhdysvaltojen oikeuden perusteella, unionin kansalaisilla ei ole myöskään mitään tosiasiallista oikeutta tulla kuulluiksi heidän tietojensa tarkkailua ja sieppaamista koskevasta kysymyksestä.

36. Pääasian käsittelyn yhteydessä annettujen juhlallisten lausumien liitteenä olevasta runsaasta asiakirja-aineistosta ilmenee selvästi, että Snowdenin paljastusten paikkansapitävyyttä ei ole suureksi osaksi kyseenalaistettu. High Court on näin ollen katsonut, että kun henkilötietoja siirretään Yhdysvaltoihin, NSA sekä muut Yhdysvaltojen turvallisuusvirastot, kuten Federal Bureau of Investigation (FBI), voivat tutustua niihin tarkkaillessaan ja siepatessaan erottelemattomia massatietoja.

37. High Court toteaa, että Irlannin oikeudessa perusoikeuksien merkitys yksityiselämälle ja kotirauhalle edellyttää, että kaikki puuttuminen näihin oikeuksiin on laissa säädettyjen vaatimusten mukaista ja oikeasuhtaista. Massiivinen ja erottelematon pääsy henkilötietoihin ei missään tapauksessa vastaa oikeasuhteisuuden vaatimusta, joten sen pitäisi katsoa olevan Irlannin perustuslain vastaista.[19]

38. High Court korostaa, että jotta sähköisen viestinnän sieppaamista voitaisiin pitää perustuslain mukaisena, olisi osoitettava, että määrätyt viestien sieppaamiset ja tiettyjen henkilöiden tai tiettyjen henkilöryhmien tarkkailu ovat objektiivisesti perusteltavissa kansallisen turvallisuuden ja rikollisuuden torjunnan nimissä ja että on olemassa riittävät ja todennettavissa olevat takeet.

18 — Ks. tämän lain, sellaisena kuin se on muutettuna vuoden 2008 lailla (Foreign Intelligence Surveillance Act of 2008), 702 §. Tämän pykälän perusteella NSA ylläpitää tietokantaa, jota kutsutaan nimellä ”PRISM” (ks. raportti Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27.11.2013).

19 — High Court viittaa erityisesti ihmisarvon ja henkilön vapauden kunnioittamiseen (johdanto-osa), henkilökohtaiseen autonomiaan (40 §:n 3 momentin 1 ja 2 kohta), kotirauhan rikkomattomuuteen (40 §:n 5 momentti) ja perhe-elämän suojeluun (41 §).

39. Näin ollen High Court toteaa, että jos nyt käsiteltävää asiaa pitäisi käsitellä yksinomaan Irlannin oikeuden perusteella, tulisi esiin huomattava ongelma, joka koskisi sitä, taataanko Yhdysvalloissa ”riittävä yksityisyyden suojan taso sekä perusvapaudet ja -oikeudet” tietosuojalain 11 §:n 1 momentin mukaisesti. Tästä seuraa, että Irlannin oikeuden ja erityisesti sen perustuslaillisten vaatimusten perusteella tietosuojavaltuutettu ei olisi saanut hylätä Schremsin kantelua, vaan sen olisi pitänyt tutkia tämä kysymys.

40. High Court toteaa kuitenkin, että sen käsiteltävänä oleva asia koskee unionin oikeuden soveltamista perusoikeuskirjan 51 artiklan 1 kohdassa tarkoitetulla tavalla, joten tietosuojavaltuutetun päätöksen laillisuutta pitäisi arvioida unionin oikeuden kannalta.

41. High Court selittää tietosuojavaltuutetun kohtaamaa ongelmaa seuraavalla tavalla. Tietosuojalain 11 §:n 2 momentin a kohdassa säädetään, että tietosuojavaltuutetun on määritettävä tietyn kolmannen maan tietosuojan tason riittävyys komission direktiivin 95/46 25 artiklan 6 kohdan nojalla tekemän unionin toteamuksen ”mukaisesti”. Tästä seuraa, että tietosuojavaltuutettu ei voi poiketa tällaisesta toteamuksesta. Koska komissio on päätöksessään 2000/520 todennut, että Yhdysvalloissa taataan tietosuojan riittävä taso safe harbor -periaatteisiin sitoutuneiden yhtiöiden harjoittaman tietojen käsittelyn osalta, tietosuojavaltuutetun pitäisi väistämättä hylätä kantelu, jossa viitataan tällaisen suojan riittämättömyyteen.

42. Samalla kun High Court toteaa, että tietosuojavaltuutettu on noudattanut tunnollisen tarkasti direktiivin 95/46 ja päätöksen 2000/520 sanamuotoa, se katsoo, että Schrems vastustaa tosiasiallisesti enemmän itse safe harbor -järjestelmän ehtoja kuin tapaa, jolla tietosuojavaltuutettu on sitä soveltanut, ja korostaa samaan aikaan, että Schrems ei ole riitauttanut suoraan direktiivin 95/46 eikä päätöksen 2000/520 pätevyyttä.

43. High Courtin mukaan olennainen kysymys koskee siis sitä, sitooko komission päätöksessä 2000/520 vahvistama toteamus, joka liittyy henkilötietojen suojelua koskevan oikeuden ja käytäntöjen riittävyyteen Yhdysvalloissa, ehdottomasti tietosuojavaltuutettua unionin oikeuden perusteella, kun otetaan huomioon erityisesti myöhemmin voimaan tulleen perusoikeuskirjan 7 ja 8 artikla.

44. High Court täsmentää lisäksi, että sen käsiteltävänä olevassa kanteessa ei ole esitetty mitään moitteita Facebook Irelandin ja Facebook USA:n toiminnasta sellaisenaan. Päätöksen 2000/520 3 artiklan 1 kohdan b alakohtaa, jossa sallitaan se, että toimivaltaiset kansalliset viranomaiset määräävät yrityksen keskeyttämään tietovirran kolmanteen maahan, sovelletaan tämän tuomioistuimen mukaan vain niissä olosuhteissa, joissa kantelu kohdistetaan kyseisen yrityksen käyttäytymiseen, mikä ei ole tilanne tässä tapauksessa.

45. High Court korostaa näin ollen, että varsinaista vastalausetta ei kohdisteta Facebook USA:n käyttäytymistä sellaisenaan vaan pikemminkin sitä vastaan, että komissio on arvioinut, että tietosuojaa koskevalla oikeudella ja sitä koskevilla käytännöillä taataan tietosuojan riittävä taso Yhdysvalloissa, vaikka Snowdenin paljastuksista ilmenee selvästi, että Yhdysvaltojen viranomaiset voivat tutustua massiivisesti ja erottelematta unionin alueella asuvan väestön henkilötietoihin. [20]

46. High Court arvioi tässä yhteydessä, että on vaikeaa nähdä, miten päätös 2000/520 voisi käytännössä täyttää perusoikeuskirjan 7 ja 8 artiklan vaatimukset varsinkin, kun otetaan huomioon unionin tuomioistuimen tuomiossaan Digital Rights Ireland ym. esittämät periaatteet. [21] Erityisesti perusoikeuskirjan 7 artiklaan ja jäsenvaltioiden perinteille yhteisiin olennaisiin arvoihin perustuvat takeet vaarannettaisiin, jos viranomaisille sallittaisiin sattumanvaraisesti ja yleisesti pääsy sähköiseen

20 — High Court esittää tässä yhteydessä, että Schremsin siinä esittämä pääasiallinen väite koski sitä, että Snowdenin viimeaikaisten paljastusten perusteella ja sillä perusteella, että henkilötietoja annettiin laajasti Yhdysvaltojen tiedustelupalvelun käyttöön, tietosuojavaltuutettu ei olisi saanut pätevästi päätellä, että kyseisessä kolmannessa maassa on henkilötietojen tietosuojan riittävä taso.

21 — C-293/12 ja C-594/12, EU:C:2014:238, 65–69 kohta.

viestintään ilman velvoitetta perustella tätä objektiivisesti kansalliseen turvallisuuteen tai rikollisuuden ehkäisemiseen liittyvillä syillä, jotka liittyvät nimenomaisesti kyseisiin yksilöihin, ja ilman että annettaisiin mitään riittäviä ja todennettavissa olevia takeita. Koska Schremsin kanteessa viitattiin siihen, että päätös 2000/520 saattaisi kaiken kaikkiaan olla ristiriidassa perusoikeuskirjan 7 ja 8 artiklan kanssa, unionin tuomioistuin saattaisi arvioida, että on mahdollista tulkita direktiiviä 95/46 ja erityisesti sen 25 artiklan 6 kohtaa sekä päätöstä 2000/520 siten, että siinä sallitaan kansallisten viranomaisten tekevän omia tutkimuksiaan selvittääkseen, täyttääkö henkilötietojen siirto kolmanteen maahan perusoikeuskirjan 7 ja 8 artiklasta johtuvat vaatimukset.

47. Tässä tilanteessa High Court on päättänyt lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavat ennakkoratkaisukysymykset:

”Kun itsenäinen tietosuojavaltuutettu, jonka lakisääteisenä tehtävänä on soveltaa tietosuojalainsäädäntöä ja valvoa sen noudattamista, käsittelee sille tehtyä kantelua henkilötietojen siirrosta kolmanteen maahan (tässä tapauksessa Yhdysvaltoihin), jonka lainsäädäntö ja käytäntö eivät kantelijan mukaan sisällä riittävää suojaa rekisteröidylle, onko tietosuojavaltuutetun ehdottomasti noudatettava yhteisön päätöksessä 2000/520 tekemää päinvastaista toteamusta, kun perusoikeuskirjan 7, 8 ja 47 artikla otetaan huomioon eikä sanottu rajoita direktiivin 95/46 25 artiklan 6 kohdan säännösten soveltamista?

Jos näin ei ole, onko tietosuojavaltuutetulla päinvastoin mahdollisuus ja/tai velvollisuus tehdä asiasta oma tutkimuksensa sen valossa, miten tosiseikat ovat kehittyneet komission päätöksen julkaisemisen jälkeen?”

II **Arviointi asiasta**

48. High Courtin esittämissä kahdessa kysymyksessä pyydetään unionin tuomioistuinta täsmentämään kansallisten valvontaviranomaisten valtuuksia, kun niiden käsiteltävänä on kantelu, joka koskee henkilötietojen siirtoa tiettyyn kolmanteen maahan sijoittautuneelle yritykselle, ja kun tämän kantelun tueksi väitetään, että tässä kolmannessa maassa ei taata siirrettävien henkilötietojen tietosuojan riittävää tasoa, vaikka komissio on tehnyt direktiivin 95/46 25 artiklan 6 kohdan nojalla päätöksen, jossa tunnustetaan kyseisessä kolmannessa maassa taattavan suojan tason riittävyys.

49. Huomautettakoon, että Schremsin tietosuojavaltuutetulle tekemä kantelu on kaksitahoinen. Siinä pyritään riitauttamaan henkilötietojen siirto Facebook Irelandilta Facebook USA:lle. Schrems vaatii tämän siirron lopettamista, koska hänen mukaansa Yhdysvalloissa ei taata tietosuojan riittävää tasoa niiden henkilötietojen osalta, joita siirretään safe harbor -järjestelmän yhteydessä. Hän arvostelee tarkemmin sanoen tätä kolmatta maata siitä, että se on ottanut käyttöön PRISM-ohjelman, joka antaa NSA:lle mahdollisuuden tutustua vapaasti massatietoihin, jotka on tallennettu Yhdysvalloissa sijaitseville palvelimille. Kantelu koskee siten nimenomaisesti henkilötietojen siirtämistä Facebook Irelandilta Facebook USA:lle samalla kun siinä riitautetaan yleisemmin suojan taso, joka tällaisille tiedoille taataan safe harbor -järjestelmän yhteydessä.

50. Tietosuojavaltuutettu on arvioinut, että jo se, että on olemassa komission päätös, jossa tunnustetaan, että Yhdysvalloissa taataan safe harbor -järjestelmän yhteydessä tietosuojan riittävä taso, estäisi kantelun tutkimisen.

51. On siis tutkittava yhdessä nämä kaksi kysymystä, joissa tiedustellaan ennen kaikkea, onko direktiivin 95/46 28 artiklaa, luettuna yhdessä perusoikeuskirjan 7 ja 8 artiklan valossa, tulkittava siten, että sellaisen päätöksen olemassaolo, jonka komissio on tehnyt tämän direktiivin 25 artiklan 6 kohdan nojalla, estää kansallista valvontaviranomaista tutkimasta kantelua, jossa väitetään, että tietyssä kolmannessa maassa ei taata siirrettävien henkilötietojen tietosuojan riittävää tasoa, ja keskeyttämästä tarvittaessa näiden tietojen siirtoa.

52. Perusoikeuskirjan 7 artiklassa taataan oikeus yksityiselämän kunnioittamiseen, kun taas sen 8 artiklassa vahvistetaan nimenomaisesti oikeus henkilötietojen suojaan. Viimeksi mainitun artiklan 2 ja 3 kohdassa täsmennetään, että näiden tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla, että jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi ja että itsenäinen viranomainen valvoo näiden sääntöjen noudattamista.

A *Kansallisten valvontaviranomaisten valtuudet silloin, jos komissio on tehnyt päätöksen suojan riittävyydestä*

53. Kuten Schrems esittää huomautuksissaan, pääasian kohteena olevan kantelun kannalta keskeinen kysymys koskee henkilötietojen siirtoa Facebook Irelandilta Facebook USA:lle siinä valossa, että NSA:lla ja muilla Yhdysvaltojen turvallisuuspalveluilla on yleisesti pääsy tietoihin, joita on tallennettu Facebook USA:n haltuun niille Yhdysvaltojen lainsäädännössä annettujen valtuuksien perusteella.

54. Kansallisella valvontaviranomaisella, jonka käsiteltävänä on kantelu, jolla pyritään kyseenalaistamaan toteamus, jonka mukaan tietyssä kolmannessa maassa taataan siirrettyjen tietojen tietosuojan riittävä taso, on Schremsin mukaan valtuudet määrätä kyseisessä kantelussa kuvatun yrityksen suorittaman tiedonsiirron keskeyttämisestä, jos sillä on tietoja, joiden mukaan tähän kanteluun sisältyvät väitteet ovat paikkansapitäviä.

55. Koska tietosuojavaltuutettu on velvollinen suojelemaan Schremsin perusoikeuksia, hän väittää, että tietosuojavaltuutettu on velvollinen paitsi tutkimaan kantelun, myös käyttämään valtuuksiaan keskeyttää tietojen siirto Facebook Irelandin ja Facebook USA:n välillä, jos kantelu hyväksytään.

56. Tietosuojavaltuutettu hylkäsi kantelun niiden tietosuojalain säännösten perusteella, joissa luetellaan sen valtuudet. Tämä päätelmä perustui tietosuojavaltuutetun näkemykseen, jonka mukaan päätös 2000/520 sitoi sitä.

57. Tästä seuraa, että keskeinen ongelma nyt käsiteltävässä asiassa koskee sitä, sitooko päätökseen 2000/520 sisältyvä komission arviointi suojan tason riittävyydestä ehdottomasti kansallista tietosuojaviranomaista ja estääkö se sitä tutkimasta väitteitä, joilla pyritään kyseenalaistamaan tämä toteamus. Ennakkoratkaisukysymykset koskevat siten sitä, miten laajat valtuudet kansallisilla tietosuojaviranomaisilla on tutkia tietosuojaa suojan riittävyydestä tehdyn komission päätöksen yhteydessä.

58. Komission mukaan on tärkeää ottaa huomioon sen ja kansallisten tietosuojaviranomaisten valtuuksien välinen rakenne. Kansallisten tietosuojaviranomaisten valtuudet keskittyvät tätä alaa koskevan lainsäädännön soveltamiseen yksittäistapauksissa, kun taas päätöksen 2000/520 soveltamisen yleinen uudelleentutkiminen, mukaan luettuna kaikki päätökset, jotka sisältävät sen soveltamisen keskeyttämisen tai kumoamisen, kuuluvat komission toimivaltaan.

59. Komissio väittää, että Schrems ei ole esittänyt erityisiä perusteluja, joiden mukaan voitaisiin ajatella, että olisi olemassa välitön vaara siitä, että hänelle aiheutuisi vakavia vahinkoja tietojen siirrosta Facebook Irelandin ja Facebook USA:n välillä. Schremsin Yhdysvaltojen turvallisuuspalvelujen toteuttamista tarkkailuohjelmista esittämät huolet ovat abstrakteja ja yleisiä ja siten samanlaisia kuin ne huolet, joiden perusteella komissio aloitti päätöksen 2000/520 uudelleentutkimisen.

60. Komission mukaan kansalliset valvontaviranomaiset loukkaisivat komission toimivaltaa neuvotella uudelleen tämän päätöksen edellytyksistä Yhdysvaltojen kanssa tai tarvittaessa keskeyttää sen soveltaminen, jos ne toteuttaisivat toimenpiteitä sellaisten kantelujen perusteella, joissa viitataan vain rakenteellisiin ja abstrakteihin huoliin.

61. En yhdy komission näkemykseen. Mielestäni se, että on olemassa direktiivin 95/46 25 artiklan 6 kohdan nojalla tehty komission päätös, ei voi mitätöidä tai edes heikentää valtuuksia, joita kansallisilla valvontaviranomaisilla on tämän direktiivin 28 artiklan nojalla. Toisin kuin komissio esittää, jos kansallisten valvontaviranomaisten käsiteltävänä on yksittäisiä kanteluja, tämä ei mielestäni estä niitä ilmaisemasta omien tutkintavaltuuksiensa ja itsenäisyytensä perusteella omaa näkemystään sen suojan yleisestä tasosta, joka taataan kolmannessa maassa, ja tekemästä siitä päätelmiä, kun ne ratkaisevat yksittäistapauksia.

62. Unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin oikeuden säännöksiä tulkittaessa on otettava huomioon paitsi niiden sanamuoto myös niiden asiayhteys ja sillä lainsäädännöllä tavoitellut päämäärät, jonka osa säännös on. [22]

63. Direktiivin 95/46 johdanto-osan 62 perustelukappaleesta ilmenee, että ”jäsenvaltioissa itsenäisesti toimivien valvontaviranomaisten perustaminen on keskeinen tekijä yksilöiden suojelussa henkilötietojen käsittelyssä”.

64. Tämän direktiivin 28 artiklan 1 kohdan ensimmäisen alakohdan mukaan ”kunkin jäsenvaltion on säädettävä siitä, että jäsenvaltioiden tämän direktiivin mukaisesti toteuttamien toimenpiteiden soveltamista sen alueella valvoo yksi tai useampi julkinen viranomainen”. Kyseisen direktiivin 28 artiklan 1 kohdan toisessa alakohdassa säädetään, että ”näiden viranomaisten on hoidettava tehtäviään itsenäisesti”.

65. Direktiivin 95/46 28 artiklan 3 kohdassa luetellaan kunkin valvontaviranomaisen valtuudet eli tutkintavaltuudet, tehokkaat toimintavaltuudet, joihin kuuluvat muun muassa valtuudet kieltää käsittely väliaikaisesti tai lopullisesti sekä valtuudet olla asianosaisena oikeudenkäynnissä, jos tämän direktiivin mukaisesti toteutettuja kansallisia toimenpiteitä rikotaan, tai valtuudet saattaa nämä rikkomukset lainkäyttöviranomaisten tietoon.

66. Lisäksi direktiivin 95/46 28 artiklan 4 kohdan ensimmäisessä alakohdassa säädetään, että ”kuka tahansa henkilö – – voi esittää valvontaviranomaiselle oikeuksiensa ja vapauksiensa suojelua henkilötietojen käsittelyn osalta koskevan vaateen”. Tämän direktiivin 28 artiklan 4 kohdan toisessa alakohdassa täsmennetään, että ”kuka tahansa henkilö voi erityisesti esittää valvontaviranomaiselle vaateen käsittelyn laillisuuden tarkastamisesta sovellettaessa [kyseisen] direktiivin 13 artiklan mukaisesti toteutettuja kansallisia toimenpiteitä”. Täsmennettäköön, että viimeksi mainitun säännöksen mukaan jäsenvaltiot saavat lainsäädännöllään rajoittaa direktiivin 95/46 tiettyjen vaatimusten soveltamisalaa, jos se on välttämätöntä valtion turvallisuuden, puolustuksen, yleisen turvallisuuden taikka rikosten torjunnan, tutkinnan, selvittämisen tai syyteharkinnan kannalta.

67. Kuten unionin tuomioistuin on jo korostanut, vaatimus siitä, että riippumaton viranomainen valvoo yksilöiden suojelua henkilötietojen käsittelyssä koskevien unionin säännösten noudattamista, perustuu myös unionin primaarioikeuteen, erityisesti Euroopan unionin perusoikeuskirjan 8 artiklan 3 kohtaan ja SEUT 16 artiklan 2 kohtaan. [23] Se on myös muistuttanut, että ”itsenäisten valvontaviranomaisten perustaminen jäsenvaltioissa on siis keskeinen tekijä yksilöiden suojelussa henkilötietojen käsittelyssä”. [24]

68. Unionin tuomioistuin on myös todennut, että ”direktiivin 95/46 28 artiklan 1 kohdan toista alakohtaa on tulkittava siten, että valvontaviranomaisten, jotka ovat toimivaltaisia valvomaan henkilötietojen käsittelyä, on oltava itsenäisiä siten, että ne voivat suorittaa tehtävänsä vapaina ulkoisesta vaikuttamisesta. Tämä itsenäisyys sulkee pois kaikki sellaiset määräykset ja kaiken muun

22 — Ks. esim. tuomio Koushkaki (C-84/12, EU:C:2013:862, 34 kohta oikeuskäytäntöviittauksineen).

23 — Ks. tuomio komissio v. Itävalta (C-614/10, EU:C:2012:631, 36 kohta) ja tuomio komissio v. Unkari (C-288/12, EU:C:2014:237, 47 kohta).

24 — Ks. mm. tuomio komissio v. Unkari (C-288/12, EU:C:2014:237, 48 kohta oikeuskäytäntöviittauksineen). Ks. vastaavasti myös tuomio Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238, 68 kohta oikeuskäytäntöviittauksineen).

missä muodossa tahansa tapahtuvan ulkoisen vaikuttamisen, olipa se sitten suoraa tai välillistä, jotka saattaisivat ohjata niiden päätöksiä ja voisivat näin asettaa kyseenalaiseksi sen, että nämä viranomaiset täyttävät tehtävänsä, joka on oikean tasapainon saavuttaminen yksityisyyden suojan ja henkilötietojen vapaan liikkuvuuden välillä”. [25]

69. Unionin tuomioistuin on lisäksi täsmentänyt, että ”kansallisten valvontaviranomaisten itsenäisyyden takaamisella pyritään varmistamaan yksilöiden suojelua henkilötietojen käsittelyssä koskevien säännösten ja määräysten noudattamisen valvonnan tehokkuus ja luotettavuus”. [26] Nämä itsenäisyyden takeet on otettu käyttöön ”sen vuoksi, että niille henkilöille ja elimille, joita niiden päätökset koskevat, annettavaa suojaa vahvistettaisiin”. [27]

70. Kuten erityisesti direktiivin 95/46 johdanto-osan 10 perustelukappaleesta ja 1 artiklasta ilmenee, sillä pyritään takaamaan unionissa ”perusvapauksien ja -oikeuksien suojan korkea taso henkilötietojen käsittelyssä”. [28] Unionin tuomioistuimen mukaan ”direktiivin 95/46 28 artiklassa tarkoitetut valvontaviranomaiset ovat siis näiden perusoikeuksien ja -vapauksien vartijoita”. [29]

71. Kun otetaan huomioon sen tehtävän merkitys, joka kansallisilla valvontaviranomaisilla on yksilöiden suojelussa henkilötietojen käsittelyn yhteydessä, niiden toimintavaltuuksien on pysyttävä täysimääräisinä silloinkin, kun komissio tekee päätöksen direktiivin 95/46 25 artiklan 6 kohdan nojalla.

72. Tässä yhteydessä on huomattava, että mikään ei viittaa siihen, että henkilötietojen siirtoa kolmansiin maihin koskevat järjestelmät jäisivät perusoikeuskirjan 8 artiklan 3 kohdan aineellisen soveltamisalan ulkopuolelle, kun siinä vahvistetaan unionin oikeuden normihierarkian korkeimmalla tasolla itsenäisen viranomaisen harjoittaman valvonnan merkitys henkilötietojen suojaan liittyvien sääntöjen noudattamisen kannalta.

73. Jos komission tekemät päätökset sitoisivat ehdottomalla tavalla kansallisia valvontaviranomaisia, tällä rajoitettaisiin väistämättä niiden täydellistä itsenäisyyttä. Koska kansallisten valvontaviranomaisten tehtävänä on suojella perusoikeuksia, niiden on voitava tutkia täysin itsenäisesti niille tehdyt kantelut yksilöiden suojelemiseen henkilötietojen käsittelyn yhteydessä liittyvän korkeammantasoisen intressin nimissä.

74. Kuten Belgian hallitus ja Euroopan parlamentti ovat lisäksi perustellusti korostaneet istunnossa, direktiivin 95/46 IV luku, joka koskee henkilötietojen siirtoa kolmansiin maihin, ja sen VI luku, jossa vahvistetaan muun muassa kansallisten valvontaviranomaisten asema, eivät ole hierarkkisessa suhteessa toisiinsa. Mikään tässä VI luvussa ei viittaa siihen, että kansallisia valvontaviranomaisia koskevat säännökset olisivat millään tavoin alisteisia direktiivin 95/46 IV luvussa vahvistetuille tietojen siirtoa koskeville eri säännöksille.

75. Tämän direktiivin IV lukuun sisältyvästä 25 artiklan 1 kohdasta ilmenee päinvastoin nimenomaisesti, että henkilötietojen siirtoa kolmanteen maahan, jossa taataan tietosuojan riittävä taso, koskeva lupa on voimassa vain sillä varauksella, että noudatetaan kansallisia säännöksiä, jotka on annettu kyseisen direktiivin muiden säännösten nojalla.

25 — Ks. mm. tuomio komissio v. Unkari (C-288/12, EU:C:2014:237, 51 kohta oikeuskäytäntöviittauksineen).

26 — Tuomio komissio v. Saksa (C-518/07, EU:C:2010:125, 25 kohta).

27 — Idem.

28 — Ibidem (tuomion 22 kohta oikeuskäytäntöviittauksineen).

29 — Ibidem (tuomion 23 kohta). Ks. vastaavasti myös tuomio komissio v. Itävalta (C-614/10, EU:C:2012:631, 52 kohta) ja tuomio komissio v. Unkari (C-288/12, EU:C:2014:237, 53 kohta).

76. Muistutettakoon tässä yhteydessä, että jäsenvaltioiden on kyseisen säännöksen nojalla säädettävä kansallisessa lainsäädännössään siitä, että käsiteltävien tai siirron jälkeen käsiteltäviksi tarkoitettujen henkilötietojen siirto kolmanteen maahan voidaan suorittaa ainoastaan, jos kyseisessä kolmannessa maassa taataan tietosuojan riittävä taso, jollei direktiivin 95/46 muiden säännösten mukaisesti säädetyistä kansallisista säännöksistä muuta johdu.

77. Kyseisen direktiivin 28 artiklan 1 kohdan mukaisesti kansallisten valvontaviranomaisten on valvottava jäsenvaltioiden kyseisen direktiivin mukaisesti toteuttamien toimenpiteiden soveltamista kunkin jäsenvaltion alueella.

78. Kun otetaan huomioon nämä molemmat säännökset yhdessä, voidaan katsoa, että direktiivin 95/46 25 artiklan 1 kohdassa vahvistettu sääntö, jonka mukaan henkilötietoja voidaan siirtää vain, jos vastaanottajana olevassa kolmannessa maassa taataan tietosuojan riittävä taso, kuuluu sääntöihin, joiden soveltamista kansallisten valvontaviranomaisten on valvottava.

79. Perusoikeuskirjan 8 artiklan 3 kohdan mukaisesti on tulkittava laajasti kansallisten valvontaviranomaisten valtuuksia tutkia täysin itsenäisesti kanteluita, joita saatetaan niiden käsiteltäväksi direktiivin 95/46 28 artiklan perusteella. Näitä valtuuksia ei siis voida rajoittaa valtuuksilla, joita unionin lainsäätäjä on antanut komissiolle tämän direktiivin 25 artiklan 6 kohdan nojalla, jotta voitaisiin todeta kolmannen maan tarjoaman suojan tason riittävyys.

80. Kun otetaan huomioon kansallisten valvontaviranomaisten olennainen tehtävä henkilötietojen suojan osalta, niiden on voitava suorittaa tutkinta, kun niiden käsiteltävänä on kantelu, jossa viitataan seikkoihin, jotka saattaisivat kyseenalaistaa tietyssä kolmannessa maassa taattavan suojan tason, myös silloin, kun komissio on todennut direktiivin 95/46 25 artiklan 6 kohdan nojalla tehdyssä päätöksessä, että kyseisessä kolmannessa maassa taataan tietosuojan riittävä taso.

81. Jos kansallinen valvontaviranomainen arvioi tutkimustensa perusteella, että riidanalaisella tietojen siirrolla loukataan suojaa, joka on annettava unionin kansalaisten tietojen käsittelylle, sillä on toimivalta keskeyttää riidanalaisten tietojen siirto riippumatta komission päätöksessään tekemästä yleisestä arvioinnista.

82. Direktiivin 95/46 25 artiklan 2 kohdan sanamuodon perusteella on näet kiistatonta, että kolmannessa maassa taattavan tietosuojan tason riittävyyttä on arvioitava sekä kaikkien tosiseikkojen että oikeudellisten seikkojen perusteella. Jos jokin näistä seikoista muuttuu ja on ilmeistä, että tällä kyseenalaistetaan kolmannen maan tarjoaman suojan tason riittävyys, kantelua käsittelevän kansallisen valvontaviranomaisen on voitava ryhtyä toimenpiteisiin riidanalaisen siirron osalta.

83. On tosin totta, kuten Irlanti on korostanut, että päätös 2000/520 sitoo tietosuojavaltuutettua, kuten muitakin valtion viranomaisia. SEUT 288 artiklan neljännestä kohdasta näet ilmenee, että unionin toimielimen päätös on kaikilta osiltaan velvoittava. Näin ollen päätös 2000/520 velvoittaa jäsenvaltioita, joille se on osoitettu.

84. Korostettakoon tässä yhteydessä, että päätöksen 2000/520 5 artiklassakin säädetään, että ”jäsenvaltioiden on toteutettava kaikki [sen] noudattamisen edellyttämät toimenpiteet yhdeksänkymmenen päivän kuluessa siitä päivästä, jona se annettiin tiedoksi jäsenvaltioille”. Lisäksi tämän päätöksen 6 artiklassa vahvistetaan, että ”[se] on osoitettu kaikille jäsenvaltioille”.

85. Katson kuitenkin, että kun otetaan huomioon direktiivin 95/46 ja perusoikeuskirjan edellä mainitut säännökset ja määräykset, päätöksen 2000/520 velvoittavuus ei tarkoita sitä, että tietosuojavaltuutettu ei voisi lainkaan tutkia kanteluja, joissa väitetään, että tämän päätöksen perusteella suoritetuissa henkilötietojen siirroissa Yhdysvaltoihin ei anneta tarvittavia unionin oikeudessa edellytettyjä suojan takeita. Tällainen velvoittava vaikutus ei toisin sanoen edellytä sitä, että kaikki tällaiset kantelut hylättäisiin summittaisesti eli välittömästi ja ilman minkäänlaista paikkansapitävyyden tutkimista.

86. Lisättäköön, että myös direktiivin 95/46 25 artiklan rakenteesta ilmenee, että toteamuksen siitä, täyttyykö tietosuojan riittävä taso, voivat tehdä joko jäsenvaltiot tai komissio. Kyseessä on siis jaettu toimivalta.

87. Kyseisen direktiivin 25 artiklan 6 kohdasta ilmenee, että kun komissio toteaa, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso 25 artiklan 2 kohdan tarkoittamalla tavalla, jäsenvaltioiden on toteutettava tarvittavat toimenpiteet noudattaakseen komission päätöstä.

88. Koska tällaisen päätöksen vaikutuksesta sallitaan henkilötietojen siirto kolmanteen maahan, jossa komissio katsoo suojan tason olevan riittävä, jäsenvaltioiden on siten lähtökohtaisesti sallittava se, että niiden alueelle sijoittautuneet yritykset siirtävät tällaisia tietoja.

89. Direktiivin 95/46 25 artiklassa ei anneta kuitenkaan komissiolle yksinoikeutta todeta siirrettävien henkilötietojen suojan tason riittävyyttä tai riittämättömyyttä. Tämän artiklan rakenne osoittaa, että myös jäsenvaltioilla on tässä oma asemansa. Komission päätöksellä on kyllä merkittävä asema siinä, että yhdenmukaistetaan voimassa olevat siirron edellytykset jäsenvaltioiden välillä. Tämä yhdenmukaistaminen voi kuitenkin olla voimassa vain niin kauan kuin tätä toteamusta ei kyseenalaisteta.

90. Perustelua, jonka mukaan on tarpeen yhdenmukaistaa henkilötietojen siirtoa kolmanteen maahan koskevat edellytykset, on mielestäni rajattava pääasian kohteena olevan kaltaisessa tilanteessa, jossa paitsi ilmoitetaan komissiolle siitä, että sen toteamusta arvostellaan, se myös itse esittää tällaista arvostelua ja johtaa neuvotteluja tilanteen korjaamiseksi.

91. Kolmannen maan tarjoaman suojan tason riittävyyden tai riittämättömyyden arviointi voi edellyttää myös jäsenvaltioiden ja komission välistä yhteistyötä. Direktiivin 95/46 25 artiklan 3 kohdassa säädetään tästä, että ”jäsenvaltioiden ja komission on informoitava toisiaan, jos ne arvioivat, että tietyssä kolmannessa maassa ei taata tietosuojan riittävää tasoa 2 kohdan tarkoittamassa merkityksessä”. Kuten parlamentti huomauttaa, tämä osoittaa hyvin, että jäsenvaltioilla ja komissiolla on samankaltainen tehtävä tuoda esiin tapauksia, joissa tietyssä kolmannessa maassa ei taata tietosuojan riittävää tasoa.

92. Suojan riittävyyttä koskevan päätöksen tarkoituksena on sallia henkilötietojen siirto asianomaiseen kolmanteen maahan. Tämä ei merkitse sitä, että unionin kansalaiset eivät voisi enää esittää valvontaviranomaisille vaateita henkilötietojensa suojaamisesta. Todettakoon tästä, että direktiivin 95/46 28 artiklan 4 kohdan ensimmäisessä alakohdassa, jonka mukaan ”kuka tahansa henkilö – – voi esittää valvontaviranomaiselle oikeuksiensa ja vapauksiensa suojelua henkilötietojen käsittelyn osalta koskevan vaateen”, ei säädetä poikkeuksesta, joka tehtäisiin tästä periaatteesta siinä tapauksessa, että komissio olisi tehnyt päätöksen tämän direktiivin 25 artiklan 6 kohdan nojalla.

93. Vaikka siis päätöksestä, jonka komissio on tehnyt sille tällä viimeksi mainitulla säännöksellä annetun toimeenpanovallan nojalla, seuraa, että henkilötietojen siirto tiettyyn kolmanteen maahan sallitaan, tästä päätöksestä ei sitä vastoin voi seurata, että jäsenvaltioilta ja erityisesti niiden valvontaviranomaisilta vietäisiin kaikki valtuudet tai että niiden tehtäviä edes rajoitettaisiin, jos niille on esitetty perusoikeuksien loukkauksia koskevia väitteitä.

94. Kansallisen valvontaviranomaisen on kyettävä käyttämään direktiivin 95/46 28 artiklan 3 kohdassa säädettyjä valtuuksia, joihin kuuluvat valtuudet kieltää henkilötietojen käsittely väliaikaisesti tai lopullisesti. Vaikka tähän säännökseen sisältyvässä valtuuksien luettelossa ei säädetä nimenomaisesti valtuuksista, jotka liittyisivät tietojen siirtoon jäsenvaltiosta kolmanteen maahan, tällaisen siirron on mielestäni katsottava tarkoittavan tietojen käsittelyä.[30] Kuten tämän säännöksen sanamuodosta

30 — Ks. julkisasiamies Léger’n ratkaisuehdotus asiassa parlamentti v. neuvosto ja komissio (C-317/04, EU:C:2005:710, 92–95 kohta). Ks. myös tuomio parlamentti v. neuvosto ja komissio (C-317/04 ja C-318/04, EU:C:2006:346, 56 kohta).

ilmenee, luettelo ei ole myöskään tyhjentävä. Kun otetaan huomioon kansallisten valvontaviranomaisten olennainen tehtävä direktiivillä 95/46 käyttöön otetussa järjestelmässä, niillä on joka tapauksessa oltava valtuudet keskeyttää tietojen siirto siinä tapauksessa, että perusoikeuksia osoitetaan loukattavan tai tällainen vaara on olemassa.

95. Lisättäköön, että jos kansalliselta valvontaviranomaiselta evättäisiin tutkintavaltuudet nyt käsiteltävän asian kohteena olevien kaltaisissa olosuhteissa, tämä olisi ristiriidassa paitsi itsenäisyyden periaatteen, myös direktiivin 95/46 tavoitteen, sellaisena kuin se ilmenee direktiivin 1 artiklan 1 kohdasta, kanssa.

96. Kuten unionin tuomioistuin on korostanut, ”direktiivin 95/46 johdanto-osan 3, 8 ja 10 perustelukappaleesta ilmenee, että unionin lainsäätäjä on tarkoittanut helpottaa henkilötietojen vapaata liikkuvuutta lähentämällä jäsenvaltioiden lainsäädäntöjä yksilöiden perusoikeuksia, erityisesti yksityisyyden suojaa koskevaa oikeutta, kunnioittaen ja varmistamalla suojan korkean tason unionissa. Mainitun direktiivin 1 artiklassa säädetään siis, että jäsenvaltioiden on henkilötietojen käsittelyssä turvattava yksilöille heidän perusoikeutensa ja -vapautensa ja erityisesti heidän oikeutensa yksityisyyteen”. [31]

97. Direktiivin 95/46 säännöksiä on siten tulkittava sen tavoitteen mukaisesti, ja sen tavoitteena on taata yksilöiden perusoikeuksien ja erityisesti heidän yksityisyytensä suojan korkea taso, kun unionissa käsitellään henkilötietoja.

98. Tämän tavoitteen tärkeys ja asema, joka jäsenvaltioilla on oltava sen saavuttamisessa, merkitsevät sitä, että kun erityisten olosuhteiden vuoksi on perusteita epäillä vakavasti, kunnioitetaanko perusoikeuskirjassa taattuja perusoikeuksia siirrettäessä henkilötietoja tiettyyn kolmanteen maahan, komission päätös suojan riittävyydestä ei voi sitoa ehdottomalla tavalla jäsenvaltioita eikä siten myöskään niiden kansallisia valvontaviranomaisia.

99. Unionin tuomioistuin on jo todennut, että ”niitä direktiivin 95/46 säännöksiä, joilla säännellään sellaisten henkilötietojen käsittelyä, jotka saattavat loukata perusvapauksia ja varsinkin oikeutta yksityisyyteen, on välttämättä tulkittava perusoikeuksien valossa, sillä nämä perusoikeudet ovat vakiintuneen oikeuskäytännön mukaan erottamaton osa yleisiä oikeusperiaatteita, joiden noudattamista unionin tuomioistuin valvoo ja jotka sisältyvät nykyään perusoikeuskirjaan”. [32]

100. Viittaan lisäksi oikeuskäytäntöön, jonka mukaan ”jäsenvaltioiden tehtävänä on paitsi tulkita kansallista oikeuttaan unionin oikeuden mukaisesti myös varoa tukeutumasta sellaiseen johdetun oikeuden tekstin tulkintaan, joka johtaisi ristiriitaan unionin oikeusjärjestyksessä suojattujen perusoikeuksien kanssa tai muiden unionin oikeuden yleisten periaatteiden kanssa”. [33]

101. Unionin tuomioistuin on siten todennut tuomiossaan N. S. ym., [34] että ”asetuksen N:o 343/2003[[35]] soveltaminen sen kumoamattoman olettaman perusteella, että turvapaikanhakijan perusoikeuksia noudatetaan jäsenvaltiossa, joka on tavallisesti toimivaltainen käsittelemään hänen hakemuksensa, ei ole yhteensopiva sen jäsenvaltioiden velvoitteen kanssa, että asetusta N:o 343/2003 on tulkittava ja sovellettava noudattaen perusoikeuksia”. [36]

31 — Ks. esim. tuomio IPI (C-473/12, EU:C:2013:715, 28 kohta oikeuskäytäntöviittauksineen).

32 — Ks. esim. tuomio Google Spain ja Google (C-131/12, EU:C:2014:317, 68 kohta oikeuskäytäntöviittauksineen).

33 — Ks. esim. tuomio N. S. ym. (C-411/10 ja C-493/10, EU:C:2011:865, 77 kohta oikeuskäytäntöviittauksineen).

34 — C-411/10 ja C-493/10, EU:C:2011:865.

35 — Niiden perusteiden ja menettelyjen vahvistamisesta, joiden mukaisesti määritetään kolmannen maan kansalaisen johonkin jäsenvaltioon jättämän turvapaikkahakemuksen käsittelystä vastuussa oleva jäsenvaltio, 18.2.2003 annettu neuvoston asetus (EUVL L 50, s. 1).

36 — Kyseisen tuomion 99 kohta.

102. Unionin tuomioistuin on myöntänyt tässä yhteydessä tilanteessa, jossa jäsenvaltioilla on asema turvallisina alkuperämaina toisiinsa nähden kaikissa turvapaikkaan liittyvissä oikeudellisissa ja käytännöllisissä seikoissa, että on oletettava, että turvapaikanhakijoiden kohtelu kussakin jäsenvaltiossa vastaa perusoikeuskirjan, Genevessä 28.7.1951 allekirjoitetun pakolaisten oikeusasemaa koskevan yleissopimuksen [37] ja Roomassa 4.11.1950 allekirjoitetun, ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen vaatimuksia. [38] Unionin tuomioistuin totesi kuitenkin, että ”ei ole kuitenkaan mahdotonta, että tällä järjestelmällä on käytännössä suuria toimintavaikeuksia jossakin jäsenvaltiossa siten, että on olemassa vakava vaara siitä, että turvapaikanhakijoita, jotka siirretään tähän jäsenvaltioon, kohdellaan heidän perusoikeuksiensa vastaisesti”. [39]

103. Näin ollen unionin tuomioistuin on todennut, että ”jäsenvaltioiden – myöskään kansallisten tuomioistuinten – ei pidä siirtää turvapaikanhakijaa asetuksessa N:o 343/2003 tarkoitettuun ’hakemuksen käsittelystä vastuussa olevaan jäsenvaltioon’, jos ne eivät voi olla tietämättömiä siitä, että kyseisen jäsenvaltion turvapaikkamenettelyyn ja turvapaikanhakijoiden vastaanotto-olosuhteisiin liittyvät systeemiset puutteet ovat uskottavia perusteita uskoa, että turvapaikanhakija altistuisi todelliselle vaaralle joutua perusoikeuskirjan 4 artiklassa tarkoitetun epäinhimillisen tai halventavan kohtelun kohteeksi”. [40]

104. Tuomio N. S. ym. [41] voidaan mielestäni ulottaa koskemaan pääasian kohteena olevan kaltaista tilannetta. Unionin johdetun oikeuden tulkinnan, joka perustuisi perusoikeuksien kunnioittamista koskevaan olettamaan, joka ei olisi kumottavissa – olipa kyseessä jäsenvaltio, komissio tai tietty kolmas valtio – olisi katsottava olevan yhteensopimaton sen kanssa, että jäsenvaltiot ovat velvollisia tulkitsemaan ja soveltamaan unionin johdettua oikeutta perusoikeuksien mukaisella tavalla. Direktiivin 95/46 25 artiklan 6 kohdassa ei siis edellytetä tällaista perusoikeuksien kunnioittamista koskevaa olettamaa, joka ei olisi kumottavissa, kun kyseessä on komission arviointi jonkin kolmannen maan tarjoaman suojan tason riittävyydestä. Tämän säännöksen taustalla olevaa olettamaa siitä, että tietojen siirto kolmanteen maahan on perusoikeuksien mukaista, on päinvastoin katsottava olevan kumottavissa. [42] Tätä säännöstä ei näin ollen pitäisi tulkita siten, että siinä kyseenalaistetaan muun muassa direktiivin 95/46 28 artiklan 3 kohtaan ja perusoikeuskirjan 8 artiklan 3 kohtaan sisältyvät takeet, joilla pyritään suojelemaan ja kunnioittamaan henkilötietojen suojaa koskevaa oikeutta.

105. Päättelen siis kyseisestä tuomiosta, että kun kyseessä ovat systeemiset puutteet, joita on todettu kolmannessa maassa, johon henkilötietoja siirretään, jäsenvaltioiden on voitava toteuttaa toimenpiteitä, jotka ovat tarpeen perusoikeuskirjan 7 ja 8 artiklassa suojeltujen perusoikeuksien turvaamiseksi.

106. Kuten Italian hallitus on korostanut huomautuksissaan, siitä, että komissio on tehnyt päätöksen suojan riittävyydestä, ei voi myöskään seurata unionin kansalaisten suojan heikentyminen heidän tietojensa käsittelyn osalta, kun niitä siirretään kolmanteen maahan, verrattuna siihen suojan tasoon, joka näille henkilöille kuuluisi, jos heidän tietojaan käsiteltäisiin unionin sisällä. Kansallisten valvontaviranomaisten on näin ollen kyettävä puuttumaan asiaan ja käyttämään valtuuksiaan, kun tietoja siirretään kolmansiin maihin, joita päätös suojan riittävyydestä koskee. Päinvastaisessa tapauksessa unionin kansalaisia suojattaisiin heikommin kuin siinä tapauksessa, että heidän tietojaan käsiteltäisiin unionissa.

37 — *Yhdistyneiden Kansakuntien sopimuskokoelma*, osa 189, s. 150, nro 2245 (1954).

38 — Ks. tuomio N. S. ym. (C-411/10 ja C-493/10, EU:C:2011:865, 80 kohta).

39 — Ibidem (tuomion 81 kohta).

40 — Ibidem (tuomion 94 kohta).

41 — C-411/10 ja C-493/10, EU:C:2011:865.

42 — Kyseisen tuomion 107 kohta.

107. Siitä, että komissio tekee päätöksen direktiivin 95/46 25 artiklan 6 kohdan nojalla, seuraa siis ainoastaan, että poistetaan henkilötietojen siirtoa koskeva yleinen kielto niiden kolmansien maiden osalta, joissa taataan tässä direktiivissä tarjottavaan suojaan verrattava suojan taso. Toisin sanoen sillä ei luoda erityistä poikkeusjärjestelyä, joka suojaisi unionin kansalaisia heikommin kuin kyseisessä direktiivissä säädetty yleinen järjestelmä sellaisen tietojen käsittelyn osalta, jota tehdään unionin sisällä.

108. Unionin tuomioistuin on tosin todennut tuomionsa Lindqvist [43] 63 kohdassa, että ”direktiivin 95/46/EY IV luvussa, jossa sen 25 artikla on, perustetaan erityinen järjestelmä”. Tämä ei kuitenkaan mielestäni merkitse sitä, että tällainen järjestelmä olisi vähemmän suojaava. Direktiivin 95/46 1 artiklan 1 kohdassa vahvistetun tietojen suojaamisen tavoitteen saavuttamiseksi sen 25 artiklassa asetetaan päinvastoin jäsenvaltioille ja komissiolle velvoitteita, [44] ja kyseisessä 25 artiklassa vahvistetaan periaate siitä, että jos tietosuojan taso kolmannessa maassa ei ole riittävä, henkilötietojen siirto kyseiseen maahan on kiellettävä. [45]

109. Kun kyseessä on nimenomaan safe harbor -järjestelmä, komissio katsoo, että kansallisten valvontaviranomaisten toimenpiteet ja tietovirran keskeyttäminen niiden toimesta ovat mahdollisia vain päätöksen 2000/520 3 artiklan 1 kohdan b alakohdassa säädetyissä tapauksissa.

110. Kyseisen päätöksen johdanto-osan kahdeksannen perustelukappaleen mukaan ”avoimuuden saavuttamiseksi ja sen varmistamiseksi, että jäsenvaltioiden toimivaltaiset viranomaiset kykenevät turvaamaan yksityishenkilöiden suojan henkilötietoja käsiteltäessä, tässä päätöksessä on tarpeen määritellä poikkeukselliset olot, joissa tiettyjen tiedonsiirtojen keskeyttäminen olisi oikeutettua siitä huolimatta, että tietosuojan taso on todettu riittäväksi”.

111. Nyt käsiteltävän asian yhteydessä on keskusteltu erityisesti kyseisen päätöksen 3 artiklan 1 kohdan b alakohdan soveltamisesta. Kyseisen säännöksen nojalla kansalliset valvontaviranomaiset voivat päättää keskeyttää tietovirrat siinä tapauksessa, että ”on huomattavan todennäköistä, että periaatteita loukataan; on kohtuullinen syy uskoa, että asianomainen täytäntöönpano-organisaatio ei ole ryhtynyt tai ryhdy riittäviin ja ajankohtaisiin toimenpiteisiin kyseessä olevan tapauksen ratkaisemiseksi; tietojen siirron jatkaminen aiheuttaisi välittömän vakavan haitan vaaran rekisteröidyille; ja jäsenvaltion toimivaltaiset viranomaiset ovat olosuhteisiin nähden kohtuullisessa määrin pyrkineet antamaan organisaatiolle ilmoituksen ja tilaisuuden vastata siihen”.

112. Kyseisessä säännöksessä asetetaan useita edellytyksiä, joita asianosaiset ovat tulkinneet eri tavoin tässä oikeudenkäynnissä. [46] Tutkimatta näitä tulkintoja yksityiskohtaisesti niistä ilmenee, että näillä edellytyksillä rajataan tarkasti kansallisten valvontaviranomaisten valtuuksia keskeyttää tietovirrat.

113. Toisin kuin komissio esittää, päätöksen 2000/520 3 artiklan 1 kohdan b alakohtaa on kuitenkin tulkittava direktiivin 95/46 tavoitteen eli henkilötietojen suojelun tavoitteen ja perusoikeuskirjan 8 artiklan valossa. Se, että tulkinnan on välttämättä oltava perusoikeuksien mukainen, puoltaa tämän säännöksen laajaa tulkintaa.

114. Tästä seuraa, että edellytykset, joista säädetään päätöksen 2000/520 3 artiklan 1 kohdan b alakohdassa, eivät voi mielestäni estää kansallista valvontaviranomaista käyttämästä täysin itsenäisesti valtuuksia, joita niille on annettu direktiivin 95/46 28 artiklan 3 kohdan nojalla.

43 — C-101/01, EU:C:2003:596.

44 — 65 kohta.

45 — 64 kohta.

46 — Schremsin mukaan ensimmäinen edellytys, jonka mukaan ”on huomattavan todennäköistä, että periaatteita loukataan”, ei täyty. Ei ole väitetty, että Facebook USA, joka on oman varmennuksen suorittanut elin, jolle tiedot sirretään, olisi itse loukannut safe harbor -periaatteita sillä, että Yhdysvaltojen viranomaisilla on pääsy sen hallussa oleviin erottelemattomiin massatietoihin. Yhdysvaltain oikeudessa näet rajoitetaan nimenomaisesti safe harbor -periaatteita, jotka päätöksen 2000/520 liitteessä I olevassa neljännessä kohdassa määritellään viittaamalla säädöksiin, hallinnollisiin säännöksiin ja tuomioistuinten päätöksiin.

115. Kuten lähinnä Belgian ja Itävallan hallitukset ovat esittäneet istunnossa, hätäuloskäynti, jonka päätöksen 2000/520 3 artiklan 1 kohdan b alakohta tarjoaa, on niin kapea, että sitä on vaikea toteuttaa käytännössä. Siinä edellytetään päällekkäisten edellytysten täyttymistä ja asetetaan rima liian korkealle. Perusoikeuskirjan 8 artiklan 3 kohdan valossa on mahdotonta, että kansallisten valvontaviranomaisten harkintavaltaa, joka koskee direktiivin 95/46 28 artiklan 3 kohtaan perustuvia etuoikeuksia, rajoitettaisiin siten, että sitä ei voitaisi enää käyttää.

116. Parlamentti on huomauttanut tässä yhteydessä perustellusti siitä, että unionin lainsäätäjä on päättänyt kansallisille valvontaviranomaisille kuuluvista valtuuksista. Unionin lainsäätäjän komissiolle direktiivin 95/46 25 artiklan 6 kohdassa antama täytäntöönpanovalta ei vaikuta valtuuksiin, joita sama lainsäätäjä on antanut kansallisille valvontaviranomaisille kyseisen direktiivin 28 artiklan 3 kohdassa. Komissiolla ei toisin sanoen ole toimivaltaa rajoittaa kansallisten valvontaviranomaisten valtuuksia.

117. Näin ollen sen varmistamiseksi, että yksilöiden perusoikeuksia suojataan asianmukaisella tavalla henkilötietojen käsittelyn yhteydessä, kansallisilla valvontaviranomaisilla on oltava toimivalta tehdä tutkimuksia, mikäli näitä oikeuksia väitetään loukatun. Mikäli nämä viranomaiset katsovat tällaisten tutkimusten perusteella, että tietyssä kolmannessa maassa, jota suojan riittävyydestä tehty päätös koskee, on vakavia merkkejä siitä, että unionin kansalaisten oikeutta henkilötietojensa suojeluun on loukattu, niiden on voitava keskeyttää tietojen siirto kyseiseen kolmanteen maahan sijoittautuneelle vastaanottajalle.

118. Kansallisten valvontaviranomaisten on toisin sanoen voitava suorittaa tutkimuksiaan ja tarvittaessa keskeyttää tietojen siirto riippumatta päätöksen 2000/520 3 artiklan 1 kohdan b alakohdassa vahvistetuista rajoittavista edellytyksistä.

119. Koska direktiivin 95/46 28 artiklan 3 kohdassa säädetään lisäksi kansallisten valvontaviranomaisten valtuuksista olla asianosaisena oikeudenkäynnissä, jos tämän direktiivin mukaisesti toteutettuja kansallisia toimenpiteitä rikotaan, tai valtuuksista saattaa nämä rikkomukset lainkäyttöviranomaisten tietoon, niiden on voitava saattaa asia kansallisen tuomioistuimen käsiteltäväksi, jos niiden tiedossa on seikkoja, jotka osoittavat, että kolmannessa maassa ei taata tietosuojan riittävää tasoa, ja tämä voi tarvittaessa itse päättää ennakkoratkaisupyynnön esittämisestä unionin tuomioistuimelle suojan riittävyydestä tehdyn komission päätöksen pätevyyden arviointia varten.

120. Kaikista näistä seikoista yhdessä seuraa, että direktiivin 95/46 28 artiklaa, luettuna yhdessä perusoikeuskirjan 7 ja 8 artiklan valossa, on tulkittava siten, ettei se, että on olemassa kyseisen direktiivin 25 artiklan 6 kohdan nojalla tehty komission päätös, estä kansallista valvontaviranomaista tutkimasta kannetta, jossa väitetään, että tietyssä kolmannessa maassa ei taata siirrettävien henkilötietojen tietosuojan riittävää tasoa, ja tarvittaessa keskeyttämästä näiden tietojen siirtoa.

121. Vaikka High Court korostaakin ennakkoratkaisupyynnössään, että Schrems ei ole riitauttanut pääasian kanteessa virallisesti direktiivin 95/46 eikä päätöksen 2000/520 pätevyyttä, tästä ennakkoratkaisupyynnöstä ilmenee, että Schrems pyrkii moitteillaan pääasiassa kyseenalaistamaan toteamuksen, jonka mukaan Yhdysvalloissa taataan safe harbor -järjestelmän yhteydessä tietosuojan riittävä taso siirrettäville henkilötiedoille.

122. Tietosuojavaltuutetun huomautuksista ilmenee niin ikään, että Schremsin kantelussa pyritään kyseenalaistamaan suoraan päätös 2000/520. Tehdessään tämän kantelun Schrems on halunnut riitauttaa safe harbor -järjestelmän ehdot ja toiminnan sellaisenaan sillä perusteella, että Yhdysvaltoihin siirrettävien henkilötietojen massatarkkailu osoittaa, että tässä kolmannessa maassa voimassa olevassa oikeudessa ja käytännöissä ei tosiasiallisesti suojata näitä tietoja.

123. Ennakkoratkaisua pyytävä tuomioistuin huomauttaa lisäksi itse, että perusoikeuskirjan 7 artiklassa ja jäsenvaltioiden valtiosääntöperinteelle yhteisissä keskeisissä arvoissa tarjotut takeet vaarannettaisiin, jos viranomaisille sallittaisiin sattumanvaraisesti ja yleisesti pääsy sähköiseen viestintään ilman että niiden tarvitsisi esittää objektiivisia perusteluja, jotka perustuvat kansalliseen turvallisuuteen tai nimenomaisesti kyseisiin henkilöihin liittyvän rikollisuuden estämiseen, ja ilman asianmukaisia ja todennettavissa olevia takeita.[47] Ennakkoratkaisua pyytävä tuomioistuin epäilee siten epäsuorasti päätöksen 2000/520 pätevyyttä.

124. Sen arvioiminen, taataanko Yhdysvalloissa safe harbor -järjestelmän yhteydessä siirrettäville henkilötiedoille tietosuojan riittävä taso, johtaa siis väistämättä siihen, että on tarkasteltava tämän päätöksen pätevyyttä.

125. Tässä yhteydessä on korostettava, että unionin tuomioistuin saattaa sen ja kansallisten tuomioistuinten välillä SEUT 267 artiklalla käyttöön otetun yhteistyön yhteydessä joutua tietyissä erityisissä olosuhteissa tutkimaan johdetun oikeuden säännösten pätevyyden myös silloin, kun sen käsiteltävänä on yksinomaan unionin oikeuden tulkintaa koskeva ennakkoratkaisukysymys.

126. Näin ollen unionin tuomioistuin on useaan kertaan todennut pätemättömäksi säädöksen, jota sitä pyydettiin vain tulkitsemaan.[48] Se on myös todennut, että ”jos kansallisen tuomioistuimen esittämien kysymysten tosiasiallisena tarkoituksena osoittautuu olevan pikemminkin [unionin] säädösten pätevyyden tutkiminen kuin niiden tulkinta, [unionin] tuomioistuimen asiana on antaa kyseiselle kansalliselle tuomioistuimelle selventävä vastaus heti velvoittamatta tätä aikaa vieviin muodollisuuksiin, jotka ovat ristiriidassa [SEUT 267] artiklassa käyttöön otetun menettelyn perusluonteen kanssa”.[49] Unionin tuomioistuin on lisäksi jo katsonut, että epäilyksiä, joita ennakkoratkaisua pyytävä tuomioistuin oli ilmaissut johdetun oikeuden säädöksen yhteensopivuudesta perusoikeuksien suojaa koskevien sääntöjen kanssa, oli tulkittava siten, että niillä kyseenalaistettiin tämän säädöksen pätevyys unionin oikeuden kannalta.[50]

127. Muistutettakoon lisäksi, että unionin tuomioistuimen oikeuskäytännöstä ilmenee, että unionin toimielinten, elinten ja laitosten toimilla on nimittäin laillisuusolettaman vuoksi oikeusvaikutuksia niin kauan kuin niitä ei ole peruutettu, kumottu kumoamiskanteen johdosta tai todettu pätemättömiksi ennakkoratkaisupyynnön tai lainvastaisuusväitteen vuoksi. Ainoastaan unionin tuomioistuimella on toimivalta todeta unionin toimen pätemättömyys, koska toimivallan tarkoituksena on taata oikeusvarmuus varmistamalla, että unionin oikeutta sovelletaan yhdenmukaisesti. Jos komissio ei ole todennut päätöstä pätemättömäksi eikä muuttanut tai kumonnut sitä, se on edelleen kaikilta osiltaan velvoittava ja välittömästi sovellettavissa kaikissa jäsenvaltioissa.[51]

128. Jotta ennakkoratkaisua pyytävälle tuomioistuimelle voitaisiin antaa täydellinen vastaus ja kyettäisiin poistamaan epäilykset, joita on esitetty tämän oikeudenkäynnin aikana päätöksen 2000/520 pätevyydestä, unionin tuomioistuimen pitäisi siis mielestäni arvioida tämän päätöksen pätevyyttä.

129. Näin ollen on myös tärkeää täsmentää, että tutkittaessa sitä, onko päätös 2000/520 pätevä, on tarkasteltava vain väitteitä, jotka ovat olleet keskustelun kohteena tässä oikeudenkäynnissä. Kaikkia näkökohtia, jotka liittyvät safe harbor -järjestelmän toimintaan, ei näet ole käsitelty tässä yhteydessä, mistä syystä ei ole mielestäni mahdollista tutkia tässä yhteydessä tämän järjestelmän puutteita tyhjentävästi.

47 — Ennakkoratkaisupyynnön 24 kohta.

48 — Ks. esim. tuomio Strehl (62/76, EU:C:1977:18, 10–17 kohta); tuomio Roquette Frères (145/79, EU:C:1980:234, 6 kohta) ja tuomio Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, 32–39 kohta).

49 — Tuomio Schwarze (16/65, EU:C:1965:117, s. 1094).

50 — Ks. tuomio Hauer (44/79, EU:C:1979:290, 16 kohta).

51 — Ks. esim. tuomio CIVAD (C-533/10, EU:C:2012:347, 39–41 kohta oikeuskäytäntöviittauksineen).

130. Sitä vastoin kysymys, joka koskee sitä, onko se, että Yhdysvaltojen tiedustelupalveluilla on yleinen ja kohdentamaton pääsy siirrettyihin tietoihin, omiaan vaikuttamaan päätöksen 2000/520 laillisuuteen, on ollut keskustelun kohteena unionin tuomioistuimessa tässä oikeudenkäynnissä. Tämän päätöksen pätevyyttä voidaan siis arvioida tästä näkökulmasta.

B *Päätöksen 2000/520 pätevyys*

1. Seikat, jotka on otettava huomioon arvioitaessa päätöksen 2000/520 pätevyyttä

131. Oikeuskäytännössä on todettu, että ”säädöksen laillisuutta on arvioitava kumoamiskanteen yhteydessä niiden tosiseikkojen ja oikeudellisten seikkojen perusteella, jotka olivat olemassa sinä päivänä, jona säädös annettiin, ja komission arviointi voidaan kumota vain siinä tapauksessa, että se on ilmeisen virheellinen niiden tietojen perusteella, jotka sillä oli käytettävissään kyseisen säädöksen antamishetkellä”. [52]

132. Unionin tuomioistuin muistutti tuomiossaan Gaz de France – Berliner Investissement [53] periaatteesta, jonka mukaan ”toimen pätevyyden arvioinnin, joka yhteisöjen tuomioistuimen on suoritettava ennakkoratkaisupyynnön yhteydessä, on normaalisti perustuttava toimen toteutushetkellä vallinneeseen tilanteeseen”. [54] Se näytti kuitenkin hyväksyneen sen, että ”toimen pätevyyttä voidaan eräissä tilanteissa arvioida sen toteutuksen jälkeen ilmenneiden uusien seikkojen perusteella”. [55]

133. Unionin tuomioistuimen tällä tavoin kuvaama mahdollisuus vaikuttaa erityisen merkitykselliseltä nyt käsiteltävän asian yhteydessä.

134. Komission direktiivin 95/46 25 artiklan 6 kohdan perusteella tekemiin päätöksiin liittyy näet erityispiirteitä. Niillä on tarkoitus arvioida, onko tietyn kolmannen maan tarjoama henkilötietojen suojan taso riittävä. Kyseessä on arviointi, jonka on tarkoitus muuttua kolmannessa maassa vallitsevan tosiasiallisen ja oikeudellisen tilanteen mukaan.

135. Koska suojan riittävyydestä tehtävä päätös on erityinen päätöksen laji, sääntöä, jonka mukaan sen pätevyyttä voidaan arvioida vain sellaisten seikkojen perusteella, jotka olivat olemassa sen tekohetkellä, on höllennettävä tässä tapauksessa. Muussa tapauksessa tällainen sääntö johtaisi siihen, että unionin tuomioistuimen tekemässä pätevyyden arvioinnissa ei voitaisi useita vuosia suojan riittävyydestä tehdyn päätöksen tekemisen jälkeenkään ottaa huomioon myöhempiä tapahtumia, vaikka pätevyyden arviointia koskevan ennakkoratkaisupyynnön esittämistä ei ole rajoitettu ajallisesti ja sen esittäminen voi nimenomaan olla seurausta myöhemmistä seikoista, jotka osoittavat kyseisen toimen puutteet.

136. Tässä tapauksessa päätöksen 2000/520 pitäminen voimassa noin 15 vuoden ajan osoittaa, että komissio on implisiittisesti vahvistanut vuonna 2000 tekemänsä arvioinnin. Kun unionin tuomioistuimen on ennakkoratkaisupyynnön yhteydessä tarkasteltava sellaisen arvioinnin pätevyyttä, jonka komissio on pitänyt ennallaan ajan kuluessa, ei siis ole ainoastaan mahdollista vaan myös asianmukaista, että se voi verrata tätä arviointia uusiin olosuhteisiin, jotka ovat ilmenneet suojan riittävyydestä tehdyn päätöksen jälkeen.

52 — Ks. m. tuomio BVGD v. komissio (T-104/07 ja T-339/08, EU:T:2013:366, 291 kohta), jossa viitataan tuomioon IECC v. komissio (C-449/98 P, EU:C:2001:275, 87 kohta).

53 — C-247/08, EU:C:2009:600.

54 — 49 kohta oikeuskäytäntöviittauksineen.

55 — 50 kohta oikeuskäytäntöviittauksineen. Ks. vastaavasti Lenaerts, K., Maselis, I., ja Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, jotka toteavat, että ”in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court” (10.16 kohta, s. 471).

137. Kun otetaan huomioon suojan riittävyyttä koskevan päätöksen erityisluonne, komission on tarkasteltava sitä säännöllisesti uudelleen. Jos komissio ei sittemmin tapahtuneiden uusien vaiheiden jälkeen muuta päätöstään, se vahvistaa implisiittisesti mutta väistämättä alun perin tekemänsä arvioinnin. Se toistaa siten toteamuksensa, jonka mukaan asianomaisessa kolmannessa maassa taataan siirretyille henkilötiedoille tietosuojan riittävä taso. On unionin tuomioistuimen tehtävänä tutkia, onko tämä toteamus edelleen pätevä myöhemmin tapahtuneista seikoista huolimatta.

138. Jotta tämän tyyppisen päätöksen osalta voitaisiin taata tehokas oikeussuoja, sen pätevyyttä on siis mielestäni arvioitava siten, että otetaan huomioon tämänhetkinen tosiasiallinen ja oikeudellinen asiayhteys.

2. Tietosuojan riittävän tason käsite

139. Direktiivin 95/46 25 artikla perustuu kaikilta osin periaatteeseen, jonka mukaan henkilötietoja ei voida siirtää kolmanteen maahan, ellei tässä kolmannessa maassa taata tällaisten tietojen osalta tietosuojan riittävää tasoa. Tämän artiklan tavoitteena on siis varmistaa tällä direktiivillä annettavan suojan jatkuvuus siirrettäessä henkilötietoja kolmanteen maahan. Tässä yhteydessä on muistutettava siitä, että kyseisessä direktiivissä annetaan unionin kansalaisille korkea suojan taso heidän henkilötietojensa käsittelyn osalta.

140. Kun otetaan huomioon henkilötietojen suojan tärkeys yksityiselämän kunnioittamista koskevan perusoikeuden kannalta, tällainen korkea suojan taso on näin ollen taattava myös silloin, kun henkilötietoja siirretään johonkin kolmanteen maahan.

141. Tästä syystä katson, että komissio voi todeta direktiivin 95/46 25 artiklan 6 kohdan nojalla, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso, vain silloin jos se kykenee vahvistamaan kyseisen kolmannen maan lainsäädäntöä ja käytäntöä koskevan kokonaisarvioinnin perusteella, että tässä maassa tarjotaan direktiivissä säädettyä pääosiltaan vastaava suoja taso, vaikka tätä suojaa koskevat yksityiskohtaiset säännöt voivat poiketa niistä, joita yleisesti käytetään unionissa.

142. Vaikka englanninkielinen ilmaisu ”adequate” voidaan kielitieteellisesti ymmärtää siten, että sillä tarkoitetaan juuri ja juuri tyydyttävää tai riittävää tietosuojan tasoa, jolloin sen semanttinen merkitys poikkeaisi ranskankielisen käsitteen ”adéquat” merkityksestä, on huomattava, että tämän ilmaisun tulkinnan ainoana ohjaavana perusteena voi olla perusoikeuksien suojan korkean tason saavuttamisen tavoite, jota edellytetään direktiivissä 95/46.

143. Kolmannen maan tarjoaman suojan tasoa tutkittaessa on tarkasteltava kahta perustavanlaatuista seikkaa, joita ovat sovellettavien sääntöjen sisältö ja keinot, joilla varmistetaan näiden sääntöjen noudattaminen. [56]

144. Jotta saavutettaisiin suojan taso, joka vastaa olennaisilta osin unionissa voimassa olevaa tasoa, safe harbor -järjestelmään, joka perustuu suureksi osaksi tähän järjestelmään vapaaehtoisesti osallistuvien yritysten omaan varmennukseen ja itsearviointiin, pitäisi mielestäni liittyä riittäviä takeita ja riittävä valvontamekanismi. Henkilötietojen siirron kolmansiin maihin ei siten pitäisi saada heikompaa suojaa kuin tietojen käsittelyn unionin sisällä.

145. Korostettakoon tässä yhteydessä heti aluksi, että unionissa on voimassa näkemys, jonka mukaan sellaisen ulkoisen valvonnan mekanismi, jota suorittaa itsenäinen viranomainen, on välttämätön osatekijä jokaisessa järjestelmässä, jolla pyritäään varmistamaan henkilötietojen suojaan liittyvien sääntöjen noudattaminen.

56 — Ks. komission työasiakirjan WP 12, jonka otsikkona on ”Henkilötietojen siirrot kolmansiin maihin: tietosuojadirektiivin 25 ja 26 artiklan soveltaminen” ja jonka henkilöiden suojaamista henkilötietojen käsittelyn yhteydessä käsitellyt ryhmä hyväksyi 24.7.1998, s. 5.

146. Lisäksi direktiivin 95/46 25 artiklan 1–3 kohdan tehokkaan vaikutuksen varmistamiseksi on otettava huomioon, että jonkin kolmannen maan tarjoaman suojan tason riittävyys on vaihteleva tilanne, joka voi muuttua ajan kuluessa erilaisten tekijöiden vaikutuksesta. Jäsenvaltioiden ja komission on siten oltava jatkuvasti valppaina, kun tapahtuu mitä tahansa olosuhteiden muutoksia, jotka voivat tehdä kolmannen maan tarjoaman suojan tason riittävyyden uudelleenarvioinnin tarpeelliseksi. Tämän suojan tason riittävyyden arviointia ei voida missään tapauksessa vahvistaa tiettynä ajankohtana ja pitää tämän jälkeen voimassa rajoittamattoman ajan riippumatta kaikista sellaisista olosuhteiden muutoksista, jotka osoittavat, että tarjottavan suojan taso ei todellisuudessa ole enää riittävä.

147. Kolmannen maan velvollisuus taata riittävä suojan taso on siten jatkuva velvollisuus. Jos arviointi tehdään tiettynä ajankohtana, suojan riittävyyttä koskevan päätöksen voimassaolo edellyttää, että mikään sittemmin tapahtunut seikka ei ole omiaan kyseenalaistamaan komission alun perin tekemää arviointia.

148. Ei pidä näet unohtaa sitä, että direktiivin 95/46 25 artiklan tavoitteena on välttää se, että henkilötietoja siirretään johonkin kolmanteen maahan, jossa ei taata tietosuojan riittävää tasoa, koska tällä loukattaisiin perusoikeuskirjan 8 artiklassa taattua henkilötietojen suojaa koskevaa perusoikeutta.

149. On korostettava, että unionin lainsäätäjän komissiolle direktiivin 95/46 25 artiklan 6 kohdassa antamille valtuuksille todeta, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso, on nimenomaisesti asetettu vaatimukseksi, että tässä kolmannessa maassa taataan tällainen taso tämän artiklan 2 kohdassa tarkoitetulla tavalla. Jos uudet seikat ovat omiaan saattamaan komission alkuperäisen arvioinnin kyseenalaiseksi, sen pitäisi mukauttaa päätöstään vastaavasti.

3. Oikeudellinen arviointi

150. Muistettakoon, että direktiivin 95/46 25 artiklan 6 kohdan nojalla ”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”. Kun direktiivin 25 artiklan 6 kohtaa luetaan yhdessä tämän direktiivin 25 artiklan 2 kohdan kanssa, tämä merkitsee sitä, että jotta komissio voi todeta, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso, sen on arvioitava kaikkia tässä kolmannessa maassa voimassa olevia oikeussääntöjä sekä niiden soveltamista.

151. Olemme todenneet, että se, että komissio on pitänyt päätöksensä 2000/520 voimassa siitä huolimatta, että on tullut esiin uusia tosiseikkoja ja oikeudellisia seikkoja, on tulkittava sen tahdoksi vahvistaa alkuperäinen arviointinsa.

152. Unionin tuomioistuimen tehtävänä ei ole ennakkoratkaisupyynnön yhteydessä arvioida tosiseikkoja, jotka ovat sen riidan taustalla, jonka perusteella kansallinen tuomioistuin on esittänyt ennakkoratkaisupyyntönsä. [57]

153. Nojaudun siis ennakkoratkaisua pyytävän tuomioistuimen ennakkoratkaisupyynnössään esittämiin tosiseikkoihin, jotka komissio on itsekin suureksi osaksi hyväksynyt toteennäytetyiksi. [58]

57 — Ks. mm. tuomio Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, 22 kohta oikeuskäytäntöviittauksineen).

58 — Ks. edellä alaviitteessä 2 mainittu komission tiedonanto ja komission tiedonanto Euroopan parlamentille ja neuvostolle safe harbor -järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta (COM(2013) 847 final).

154. Seikkoja, joita on esitetty unionin tuomioistuimessa sen komission arvioinnin kiistämiseksi, jonka mukaan safe harbor -järjestelmässä taataan unionista Yhdysvaltoihin siirrettyjen henkilötietojen tietosuojan riittävä taso, voidaan siten kuvata seuraavasti.

155. Ennakkoratkaisua pyytävän tuomioistuimen lähtökohtana ennakkoratkaisupyynnössä ovat seuraavat kaksi tosiseikkoja koskevaa toteamusta. Yhtäältä NSA ja muut Yhdysvaltojen turvallisuusvirastot voivat tutustua henkilötietoihin, joita Facebook Irelandin kaltaiset yritykset siirtävät Yhdysvaltoihin sijoittautuneelle emoyhtiölleen, massiivisten kohdentamattomien tarkkailu- ja sieppaustoimien aikana. Käytettävissä olevista todisteista ei näet voida tehdä Snowdenin lausumien perusteella tällä hetkellä mitään muuta uskottavaa päätelmää.[59] Toisaalta unionin kansalaisilla ei ole mitään tosiasiallista oikeutta tulla kuulluiksi siitä, tarkkailevatko ja sieppaavatko NSA ja muut Yhdysvaltojen turvallisuusvirastot heidän tietojaan.[60]

156. Näitä High Courtin tosiseikkoja koskevia toteamuksia tukevat komission omat toteamukset.

157. Komissio piti esimerkiksi edellä mainitussa tiedonannossaan safe harbor -järjestelmän toiminnasta unionin kansalaisten ja unioniin sijoittautuneiden yritysten näkökulmasta lähtökohtana sitä, että Yhdysvaltojen vakoiluohjelmien laajuudesta ja kattavuudesta vuoden 2013 aikana saadut tiedot olivat herättäneet epäilyjä sellaisten henkilötietojen suojelun jatkuvuudesta, jotka on siirretty laillisesti Yhdysvaltoihin safe harbor -järjestelmän mukaisesti. Se korosti, että kaikki yritykset, jotka osallistuvat PRISM-ohjelmaan ja jotka sallivat Yhdysvaltojen viranomaisten pääsyn Yhdysvalloissa tallennettuihin ja käsiteltyihin tietoihin, näyttävät kuuluvan safe harbor -järjestelmään. Näin safe harbor -järjestelmästä on tullut sen mukaan yksi väylistä, joiden kautta Yhdysvaltojen tiedusteluviranomaiset pääsevät keräämään alun perin unionissa käsiteltyjä henkilötietoja.[61]

158. Näistä seikoista seuraa, että Yhdysvaltojen lainsäädännössä ja käytännössä sallitaan se, että kerätään laajamittaisesti unionin kansalaisten henkilötietoja, jotka siirretään safe harbor -järjestelmän yhteydessä, ilman että nämä kansalaiset saisivat tehokasta oikeussuojaa.

159. Nämä tosiseikkoja koskevat toteamukset osoittavat mielestäni, että päätös 2000/520 ei sisällä riittäviä takeita. Koska nämä takeet puuttuvat, tämä päätös on toteutettu tavalla, joka ei vastaa perusoikeuskirjassa ja direktiivissä 95/46 asetettuja vaatimuksia.

160. Komission direktiivin 95/46 25 artiklan 6 kohdan nojalla tekemän päätöksen tarkoituksena on todeta, että tietyssä kolmannessa maassa ”taataan” tietosuojan riittävä taso. Sana ”taataan” preesensissä merkitsee sitä, että jotta tällainen päätös voitaisiin pitää voimassa, sen on koskettava tiettyä kolmatta maata, jossa edelleenkin, kyseisen päätöksen tekemisen jälkeen, taataan tietosuojan riittävä taso.

161. Todellisuudessa paljastukset, joissa viitataan NSA:n toimiin ja joiden mukaan tämä käytti safe harbor -järjestelmän yhteydessä siirrettyjä tietoja, ovat tuoneet esiin päätöksen 2000/520 heikkoudet laillisena perustana.

162. Puutteet, jotka on tuotu esiin tämän oikeudenkäynnin aikana, sisältyvät erityisesti tämän päätöksen liitteessä I olevaan neljänteen kohtaan.

59 — Ennakkoratkaisupyynnön 7 kohdan c alakohta.

60 — Ennakkoratkaisupyynnön 7 kohdan b alakohta.

61 — Sen tiedonannon s. 19.

163. Muistettakoon, että kyseisen säännöksen mukaan ”[safe harbor -] periaatteiden noudattamista voidaan rajoittaa a) siinä määrin, kuin se on tarpeen kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten vuoksi, b) lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä, joilla syntyy ristiriitaisia velvoitteita tai joilla selkeästi annetaan lupa tiettyyn toimintaan, sillä edellytyksellä, että aina tällaista lupaa käyttäessään organisaatio voi osoittaa, että periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi”.

164. Ongelmaksi muodostuu lähinnä se, miten Yhdysvaltojen viranomaiset ovat käyttäneet kyseisessä säännöksessä vahvistettuja poikkeuksia. Koska ne on muotoiltu liian yleisiksi, näiden poikkeusten täytäntöönpanoa näiden viranomaisten toimesta ei ole rajattu vain siihen, mikä on ehdottomasti tarpeen.

165. Tämän liian yleisen sanamuodon lisäksi unionin kansalaisilla ei ole asianmukaista oikeussuojakeinoa vastustaa sitä, että heidän henkilötietojaan on käsitelty muissa tarkoituksissa kuin niissä, joiden perusteella ne alun perin kerättiin ja siirrettiin Yhdysvaltoihin.

166. Päätöksessä 2000/520 säädettyihin poikkeuksiin, jotka koskevat safe harbor -periaatteiden soveltamista erityisesti kansallisen turvallisuuden vaatimusten osalta, olisi pitänyt liittää itsenäinen valvontamekanismi, jolla olisi kyetty välttämään todetut yksityiselämää koskevan oikeuden loukkaukset.

167. Esimerkiksi Yhdysvaltojen tiedustelupalvelujen käytäntöjä koskevat paljastukset, joiden mukaan safe harbor -järjestelmän yhteydessä siirrettyjä tietoja on yleisesti tarkkailtu, ovat tuoneet esiin tiettyjä päätökselle 2000/520 ominaisia puutteita.

168. Väitteet, joihin viitataan nyt käsiteltävän asian yhteydessä, eivät merkitse sitä, että Facebook olisi loukannut safe harbor -periaatteita. Jos luvan saanut yritys, kuten Facebook USA, antaa Yhdysvaltojen viranomaisille pääsyn tietoihin, joita sille on siirretty jostain jäsenvaltiosta, voidaan katsoa, että se menettelee näin noudattaakseen Yhdysvaltojen lainsäädäntöä. Koska tällainen tilanne sallitaan nimenomaisesti päätöksessä 2000/520 sen vuoksi, että siihen sisältyvät poikkeukset on muotoiltu laajasti, nyt käsiteltävän asian yhteydessä tulee todellisuudessa esiin tällaisten poikkeusten yhteensopivuus unionin primaarioikeuden kanssa.

169. Tässä yhteydessä on korostettava, että unionin tuomioistuimen vakiintuneesta oikeuskäytännöstä ilmenee, että ihmisoikeuksien noudattaminen on unionin säädösten laillisuuden edellytys ja että unionissa ei voida hyväksyä sellaisia toimia, jotka ovat ristiriidassa ihmisoikeuksien kunnioituksen kanssa.[62]

170. Unionin tuomioistuimen oikeuskäytännöstä ilmenee myös, että kerättyjen henkilötietojen ilmoittamisella kolmansille julkisille tai yksityisille henkilöille loukataan oikeutta yksityiselämän kunnioittamiseen, ”käytettiinpä näin ilmoitettuja tietoja sittemmin miten tahansa”.[63] Unionin tuomioistuin vahvisti lisäksi tuomiossaan Digital Rights Ireland ym.,[64] että toimivaltaisten kansallisten viranomaisten oikeus saada tällaisia tietoja merkitsee myös puuttumista tähän perusoikeuteen.[65] Lisäksi perusoikeuskirjan 8 artikla koskee kaikenlaista henkilötietojen käsittelyä, ja se merkitsee

62 — Ks. mm. tuomio Kadi ja Al Barakaat International Foundation v. neuvosto ja komissio (C-402/05 P ja C-415/05 P, EU:C:2008:461, 284 kohta oikeuskäytäntöviittauksineen).

63 — Tuomio Österreichischer Rundfunk ym. (C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, 74 kohta).

64 — C-293/12 ja C-594/12, EU:C:2014:238.

65 — 35 kohta.

puuttumista tällaisten tietojen suojaa koskevaan oikeuteen.[66] Yhdysvaltojen tiedustelupalvelujen pääsy siirrettyihin tietoihin merkitsee siis myös puuttumista perusoikeuskirjan 8 artiklassa taattuun henkilötietojen suojaa koskevaan perusoikeuteen, koska tällainen pääsy tietoihin merkitsee näiden tietojen käsittelyä.

171. Kuten unionin tuomioistuin totesi kyseisessä tuomiossa, todettu puuttuminen on laajamittaista, ja sitä on pidettävä erityisen vakavana, kun otetaan huomioon kyseisten käyttäjien suuri määrä ja siirrettyjen tietojen määrät. Nämä seikat yhdessä sen kanssa, että Yhdysvaltojen viranomaiset ovat päässeet salaa tutustumaan henkilötietoihin, joita on siirretty Yhdysvaltoihin sijoittautuneille yrityksille, tekevät puuttumisesta äärimmäisen vakavan.

172. Tähän on lisättävä, että unionin kansalaisille, jotka ovat Facebookin käyttäjiä, ei kerrottu siitä, että heidän henkilötietonsa olisivat yleisesti Yhdysvaltojen turvallisuuspalvelujen käytettävissä.

173. Lisäksi on korostettava, että ennakkoratkaisua pyytävä tuomioistuin on todennut, että Yhdysvalloissa unionin kansalaisilla ei ole mitään tosiasiallista oikeutta tulla kuulluiksi tietojensa tarkkailua ja sieppaamista koskevasta kysymyksestä. FISC harjoittaa valvontaa, mutta siinä käytävä menettely on salainen, eikä käsittely ole kontradiktorista.[67] Kyseessä on mielestäni puuttuminen unionin kansalaisten oikeuteen, joka koskee perusoikeuskirjan 47 artiklassa suojattuja tehokkaita oikeussuojakeinoja.

174. On siis todettava, että päätöksen 2000/520 liitteessä I olevassa neljännessä kohdassa olevilla safe harbor -periaatteita koskevilla poikkeuksilla sallitaan puuttuminen perusoikeuskirjan 7, 8 ja 47 artiklassa suojattuihin perusoikeuksiin.

175. Tässä yhteydessä on syytä selvittää, onko tämä puuttuminen perusteltavissa.

176. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa vahvistettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla, ja näiden oikeuksien ja vapauksien keskeistä sisältöä on kunnioitettava. Rajoituksista näihin oikeuksiin ja vapauksiin voidaan säätää suhteellisuusperiaatetta noudattaen ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

177. Kun otetaan huomioon nämä edellytykset, joiden on täytyttävä, jotta perusoikeuskirjassa suojattujen oikeuksien ja vapauksien rajoitukset voidaan hyväksyä, epäilen vahvasti sitä, että nyt käsiteltävän asian kohteena olevien rajoitusten voitaisiin katsoa olevan perusoikeuskirjan 7 ja 8 artiklan olennaisen sisällön mukaisia. Yhdysvaltojen tiedustelupalvelujen pääsy siirrettyihin tietoihin näyttää ulottuvan sähköisen viestinnän sisältöön, millä loukattaisiin yksityiselämän kunnioittamista koskevan perusoikeuden ja perusoikeuskirjan 7 artiklassa vahvistettujen muiden oikeuksien keskeistä sisältöä. Koska lisäksi päätöksen 2000/520 liitteessä I olevassa neljännessä kohdassa säädettyjen rajoitusten laaja sanamuoto sallii mahdollisesti sen, että hylätään kaikkien safe harbor -periaatteiden soveltaminen, voitaisiin katsoa, että näillä rajoituksilla loukataan henkilötietojen suojaa koskevan perusoikeuden keskeistä sisältöä.[68]

66 — 36 kohta.

67 — Ennakkoratkaisupyynnön 7 kohdan b alakohta.

68 — Ks. tästä tuomio Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238, 39 ja 40 kohta).

178. Muistutettakoon aluksi siitä, vastaako todettu puuttuminen yleisen edun mukaista tavoitetta, että päätöksen 2000/520 liitteessä I olevan neljännen kohdan b alakohdan mukaan safe harbor -periaatteiden noudattamista voidaan rajoittaa ”lainsäädännöllä, hallituksen asetuksilla tai oikeuskäytännöllä, joilla syntyy ristiriitaisia velvoitteita tai joilla selkeästi annetaan lupa tiettyyn toimintaan, sillä edellytyksellä, että aina tällaista lupaa käyttäessään organisaatio voi osoittaa, että periaatteiden noudattamatta jättäminen rajoittuu siihen, mikä on tarpeen tällaisen lupaan liittyvän oikeutetun ja ensisijaisen tavoitteen täyttämiseksi”.

179. On todettava, että ”oikeutettuja tavoitteita”, jotka mainitaan tässä säännöksessä, ei ole täsmennetty. Siitä seuraa epävarmuutta tämän safe harbor -periaatteiden soveltamisesta asianomaisissa yrityksissä tehtävän poikkeuksen soveltamisalasta, joka on mahdollisesti erittäin laaja.

180. Tämän vaikutelman vahvistavat selitykset, jotka sisältyvät päätöksen 2000/520 liitteessä IV olevaan B jaksoon, jonka otsikkona on ”Nimenomainen lakisääteinen lupa”, erityisesti toteamus, jonka mukaan ”on selvää, että jos Yhdysvaltojen lainsäädäntö asettaa yhdysvaltalaiselle organisaatiolle safe harbor -periaatteiden kanssa ristiriitaisen velvoitteen, organisaation on noudatettava lakia riippumatta siitä, kuuluko se safe harbor -järjestelmään vai ei”. Lisäksi todetaan nimenomaisten lupien osalta, että ”vaikka safe harbor -periaatteiden tarkoituksena on tasoittaa yksityisyyden suojassa Yhdysvaltojen ja Euroopan välillä esiintyviä eroja[,] Yhdysvaltojen on kunnioitettava vaaleilla valittujen lainsäätäjien valtaoikeuksia”.

181. Tästä seuraa, että tämä poikkeus on mielestäni perusoikeuskirjan 7 ja 8 artiklan sekä 52 artiklan 1 kohdan vastainen siltä osin kuin siinä ei tavoitella riittävän täsmällisesti määriteltyä yleisen edun mukaista tavoitetta.

182. Joka tapauksessa se, miten helposti ja yleisesti itse päätöksen 2000/520 liitteessä I olevan neljännen kohdan b alakohdassa sekä sen liitteessä IV olevassa B jaksossa säädetään, että safe harbor -periaatteet voidaan hylätä Yhdysvaltojen oikeussääntöjen perusteella, on ristiriidassa sen edellytyksen kanssa, jonka mukaan henkilötietojen suojaamiseen liittyvistä säännöistä tehtävät poikkeukset on rajoitettava siihen, mikä on ehdottomasti tarpeen. Siinä tosin mainitaan tarvetta koskeva edellytys, mutta sen lisäksi, että tämän edellytyksen toteennäyttäminen asetetaan kyseisen yrityksen tehtäväksi, en ymmärrä, miten tällainen yritys voisi välttyä safe harbor -periaatteiden hylkäämistä koskevalta velvoitteelta, joka ilmenee oikeussäännöistä, joita sen on sovellettava.

183. Katson näin ollen, että päätös 2000/520 on todettava pätemättömäksi, koska sellaisen poikkeuksen olemassaolo, joka mahdollistaa näin yleisesti ja epämääräisesti safe harbor -järjestelmän periaatteiden hylkäämisen, estää jo sellaisenaan katsomasta, että tässä järjestelmässä taattaisiin tietosuojan riittävä taso unionista Yhdysvaltoihin siirrettävien henkilötietojen osalta.

184. Kun kyseessä on tässä vaiheessa päätöksen 2000/520 liitteessä I olevan neljännen kohdan a alakohdassa säädettyjen rajoitusten ensimmäinen ryhmä, joka koskee vaatimuksia, jotka liittyvät kansalliseen turvallisuuteen, yleiseen etuun ja lainsäädännön vaatimuksiin, ainoastaan ensimmäinen tavoite on mielestäni riittävän täsmällinen, jotta sitä voidaan pitää unionin perusoikeuskirjan 52 artiklan 1 kohdassa tunnustettuna yleisen edun mukaisena tavoitteena.

185. Tässä vaiheessa on tarpeen selvittää todetun puuttumisen oikeasuhteisuus.

186. Tässä yhteydessä on muistettava, että ”suhteellisuusperiaate edellyttää unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan, että unionin toimielinten säädökset, päätökset ja muut toimet soveltuvat legitiimisti tavoiteltujen päämäärien toteuttamiseen eikä niillä ylitetä niitä rajoja, jotka johtuvat siitä, mikä on tarpeellista niillä tavoiteltujen päämäärien toteuttamiseksi ja tähän

soveltuvaa”. [69]

187. Koska on kyse perusoikeuksiin puuttumisesta, ”näiden edellytysten noudattamista koskevassa tuomioistuinvalvonnassa unionin lainsäätäjän harkintavallan laajuus voi osoittautua rajoitetuksi tiettyjen seikkojen vuoksi, joita ovat muun muassa kyseinen ala, perusoikeuskirjassa taatun oikeuden luonne, puuttumisen luonne ja vakavuus sekä sen päämäärä”. [70]

188. Mielestäni komission direktiivin 95/46 25 artiklan 6 kohdan nojalla tekemät päätökset ovat unionin tuomioistuimen täysimääräisen valvonnan alaisia, kun on todettava, onko kyseinen toimielin arvioinut oikeasuhteisesti sitä, onko tietyssä kolmannessa maassa tarjottavan suojan taso riittävä kyseisen maan ”sisäisestä lainsäädännöstä tai kansainvälisistä sitoumuksista” johtuvista syistä.

189. Tässä yhteydessä on huomattava, että unionin tuomioistuin totesi tuomiossaan Digital Rights Ireland ym., [71] että ”kun otetaan huomioon yhtäältä henkilötietojen suojan tärkeä rooli yksityiselämän kunnioitusta koskevan perusoikeuden kannalta ja toisaalta sen tähän oikeuteen puuttumisen laajuus ja vakavuus, jonka [riidanalainen] direktiivi – – sisältää, unionin lainsäätäjän harkintavalta on käsiteltävässä asiassa pieni, joten valvonnan on oltava tarkkaa”. [72]

190. Tällaisella puuttumisella on voitava saavuttaa riidanalaisella unionin toimella tavoiteltu päämäärä, ja sen on oltava tarpeen tämän päämäärän saavuttamiseksi.

191. Tässä yhteydessä ”unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan yksityiselämän kunnioitusta koskevan perusoikeuden suoja – – edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset on toteutettava täysin välttämättömän rajoissa”. [73]

192. Unionin tuomioistuin ottaa valvontansa yhteydessä huomioon myös sen, että ”henkilötietojen suoja, joka johtuu perusoikeuskirjan 8 artiklan 1 kohdassa määrätystä nimenomaisesta velvollisuudesta, on erityisen tärkeä sen 7 artiklassa vahvistetun yksityiselämän kunnioitusta koskevan oikeuden kannalta”. [74]

193. Unionin tuomioistuin viittaa tässä yhteydessä Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön ja toteaa, että ”kyseisessä unionin lainsäädännössä on säädettävä selvistä ja täsmällisistä kyseisen toimenpiteen laajuutta ja soveltamista koskevista säännöistä, joissa asetetaan vähimmäisvaatimukset, jotta henkilöillä, joiden tietoja on säilytetty, on riittävät takeet, joiden avulla voidaan tehokkaasti suojata heidän henkilötietonsa väärinkäytön vaaroja vastaan sekä kaikenlaista näiden tietojen laitonta saantia ja käyttöä vastaan”. [75] Unionin tuomioistuin toteaa, että ”tarve tällaisista takeista on sitä tärkeämpi, kun – – henkilötietoja käsitellään automaattisesti ja on olemassa huomattava vaara laittomasta pääsystä näihin tietoihin”. [76]

194. Päätöksen 2000/520 liitteessä I olevan neljännen kohdan a alakohta ja direktiivin 95/46 13 artiklan 1 kohta vastaavat mielestäni toisiaan. Ensin mainitussa säännöksessä todetaan, että safe harbor -periaatteiden noudattamista voidaan rajoittaa ”kansallisen turvallisuuden, yleisen edun ja [Yhdysvaltojen] lainsäädännön vaatimusten vuoksi”. Jälkimmäisessä säädetään, että jäsenvaltiot voivat

69 — Tuomio Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238, 46 kohta oikeuskäytäntöviittauksineen).

70 — Ibidem (tuomion 47 kohta oikeuskäytäntöviittauksineen).

71 — C-293/12 ja C-594/12, EU:C:2014:238.

72 — 48 kohta.

73 — Tuomio Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238, 52 kohta oikeuskäytäntöviittauksineen).

74 — Ibidem (tuomion 53 kohta).

75 — Ibidem (tuomion 54 kohta oikeuskäytäntöviittauksineen).

76 — Ibidem (tuomion 55 kohta oikeuskäytäntöviittauksineen).

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 esimerkiksi valtion turvallisuus, puolustus, yleinen turvallisuus sekä rikosten torjunta, tutkinta, selvittäminen ja syyteharkinta.

195. Kuten unionin tuomioistuin totesi tuomiossaan IPI,[77] direktiivin 95/46 13 artiklan 1 kohdan sanamuodosta ilmenee, että jäsenvaltiot voivat säätää kyseisessä säännöksessä tarkoitetuista toimenpiteistä vain silloin, kun ne ovat välttämättömiä. Toimenpiteiden ”välttämättömyys” on siis edellytyksenä kyseisessä säännöksessä jäsenvaltioille annetulle mahdollisuudelle.[78] Kun kyseessä on henkilötietojen käsittely unionin sisällä, kyseisen direktiivin 13 artiklassa säädettyjen rajoitusten on tulkittava ulottuvan vain siihen, mikä on ehdottomasti tarpeen tavoitellun päämäärän saavuttamiseksi. Tilanteen on oltava mielestäni sama, kun kyseessä on safe harbor -periaatteiden rajoittaminen päätöksen 2000/520 liitteessä I olevassa neljännessä kohdassa säädetyllä tavalla.

196. On todettava, että kaikkien päätöksen 2000/520 kieliversioiden liitteessä I olevan neljännen kohdan a alakohdan sanamuodossa ei mainita tarpeellisuutta koskevaa edellytystä. Tämä pätee muun muassa ranskankieliseen versioon, jossa todetaan, että ”l’adhésion aux principes peut être limitée par – – les exigences relatives à la sécurité nationale, l’intérêt public et le respect des lois des États-Unis” (periaatteiden noudattamista voidaan rajoittaa – – kansalliseen turvallisuuteen, yleiseen etuun ja Yhdysvaltojen lainsäädännön noudattamiseen liittyvistä syistä), kun taas esimerkiksi espanjan-, saksan- ja englanninkielisissä versioissa todetaan, että käyttöön otettujen rajoitusten on oltava ehdottomasti tarpeen edellä mainittujen tavoitteiden saavuttamiseksi.

197. Oli miten hyvänsä, ennakkoratkaisua pyytävän tuomioistuimen sekä komission edellä mainituissa tiedonannoissaan esittämät tosiseikat osoittavat selvästi, että käytännössä näiden rajoitusten täytäntöönpanoa ei ole rajoitettu siihen, mikä on ehdottomasti tarpeen edellä mainittujen tavoitteiden saavuttamiseksi.

198. Huomautettakoon tässä yhteydessä, että Yhdysvaltojen tiedustelupalvelun pääsy siirrettyihin henkilötietoihin kattaa yleisesti kaikki henkilöt ja kaikki sähköiset viestintävälineet sekä kaikki siirretyt tiedot viestinnän sisältö mukaan luettuna ilman, että tehtäisiin mitään erottelua, rajoituksia tai poikkeuksia yleisen edun tavoitteen perusteella.[79]

199. Yhdysvaltojen tiedustelupalvelun pääsy siirrettyihin tietoihin koskee näet yleisesti kaikkia henkilöitä, jotka käyttävät sähköisiä viestintäpalveluja, ilman että edellytettäisiin, että kyseiset henkilöt ovat uhkana kansalliselle turvallisuudelle.[80]

200. Tällainen massiivinen ja kohdentamaton tarkkailu on suhteetonta, ja sillä puututaan perusteettomasti perusoikeuskirjan 7 ja 8 artiklassa taattuihin oikeuksiin.

201. Koska on mahdotonta, että unionin lainsäätäjä tai jäsenvaltiot antaisivat säännöksiä, joissa säädettäisiin perusoikeuskirjan vastaisesti massiivisesta ja kohdentamattomasta tarkkailusta, tästä seuraa väistämättä, kuten parlamentti on korostanut perustellusti huomautuksissaan, että etenkään kolmansissa maissa ei voida missään tapauksessa katsoa taattavan unionin kansalaisten henkilötietojen tietosuojan riittävää tasoa, jos niiden lainsäädännössä sallitaan tosiasiallisesti tämäntyyppisten tietojen massiivinen ja kohdentamaton tarkkailu ja sieppaus.

77 — C-473/12, EU:C:2013:715.

78 — 32 kohta.

79 — Ks. vastaavasti tuomio Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238, 57 kohta oikeuskäytäntöviittauksineen).

80 — Ibidem (tuomion 58 ja 59 kohta).

202. On lisäksi tärkeää korostaa, että safe harbor -järjestelmä, sellaisena kuin se on määritelty päätöksessä 2000/520, ei sisällä sellaisia takeita, joilla voitaisiin välttää massiivinen ja yleinen pääsy siirrettyihin tietoihin.

203. Huomautettakoon tässä yhteydessä, että unionin tuomioistuin korosti tuomiossaan Digital Rights Ireland ym.[81] sitä, että on tärkeää säätää ”selvistä ja täsmällisistä säännöistä, joilla säädellään perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin puuttumisen laajuutta”.[82] Tällaisen puuttumisen on unionin tuomioistuimen mielestä oltava ”rajoitettu säännöksillä, joilla voidaan taata, että se todella rajoitetaan täysin välttämättömään”.[83] Unionin tuomioistuin korosti tässä tuomiossa myös tarvetta säätää ”sellaisista perusoikeuskirjan 8 artiklassa edellytetyistä riittävistä takeista, joilla voidaan varmistaa säilytettyjen tietojen tehokas suoja väärinkäytön vaaraa vastaan sekä näiden tietojen kaikenlaista laitonta saantia ja käyttöä vastaan”.[84]

204. On todettava, että yksityisen välitysmenettelyn mekanismit ja FTC, jonka tehtävä koskee vain kaupallisia riitoja, eivät ole keinoja, joilla voidaan riitauttaa Yhdysvaltojen tiedustelupalvelun yksiköiden pääsy unionista siirrettyihin henkilötietoihin.

205. FTC:n toimivalta kattaa sopimattomat ja harhaanjohtavat toimet ja käytännöt kaupan alalla, eikä se siten ulotu henkilötietojen keräämiseen ja käyttöön muissa kuin kaupallisissa tarkoituksissa.[85] FTC:n suppea toimivallan ala rajoittaa yksityisten oikeutta henkilötietojensa suojeluun. FTC:tä ei ole perustettu varmistamaan oikeutta yksityiselämään, kuten unionissa kansalliset valvontaviranomaiset, vaan takaamaan kaupankäynnin rehellisyys ja luotettavuus kuluttajille, mikä rajoittaa tosiasiallisesti sen kykyä puuttua henkilötietojen suojan alaan. FTC:llä ei siis ole vastaavaa asemaa kuin direktiivin 95/46 28 artiklassa säädetyillä kansallisilla valvontaviranomaisilla.

206. Unionin kansalaiset, joiden tietoja on siirretty, voivat kääntyä Yhdysvaltoihin sijoittautuneiden erikoistuneiden välityselinten, kuten TRUSTe:n ja BBBOnlinen, puoleen vaatiakseen täsmennyksiä siihen, rikkooko yritys, jolla on heidän henkilötietonsa hallussaan, omaa varmennusta koskevan järjestelmän ehtoja. TRUSTe:n kaltaisten elinten hoitamassa yksityisessä välitysmenettelyssä ei voida käsitellä henkilötietojen suojaa koskevan oikeuden loukkauksia, joita tekevät muut elimet tai viranomaiset kuin oman varmennuksen antaneet yritykset. Näillä välityselimillä ei ole mitään toimivaltaa antaa ratkaisua Yhdysvaltojen tiedustelupalvelujen toimien laillisuudesta.

207. FTC:llä ja yksityisillä välityselimillä ei siis ole toimivaltaa valvoa mahdollisia henkilötietojen suojaa koskevien periaatteiden loukkauksia, joihin syyllistyvät julkiset toimijat, kuten Yhdysvaltojen tiedustelupalvelut. Tällainen toimivalta olisi kuitenkin olennaisen tärkeä, jotta voitaisiin taata täysimääräisesti oikeus näiden tietojen tehokkaaseen suojaan. Komissio ei siis olisi saanut todeta tehdessään päätöksen 2000/520 ja pitäessään sen voimassa, että kaikkia Yhdysvaltoihin siirrettäviä henkilötietoja koskee riittävä perusoikeuskirjan 8 artiklan 3 kohdassa annetun oikeuden suoja eli että itsenäinen viranomainen valvoi tehokkaasti näiden tietojen suojaa ja turvallisuutta koskevien vaatimusten noudattamista.

208. On näin ollen todettava, että päätöksessä 2000/520 säädetyssä safe harbor -järjestelmässä ei ole itsenäistä viranomaista, joka voisi valvoa, että safe harbor -periaatteista tehtävien poikkeusten täytäntöönpano rajoitetaan siihen, mikä on ehdottomasti tarpeen. Edellä on kuitenkin todettu, että tällainen riippumattoman viranomaisen suorittama valvonta on unionin oikeuden kannalta keskeinen tekijä yksilöiden suojelussa henkilötietojen käsittelyssä.[86]

81 — C-293/12 ja C-594/12, EU:C:2014:238.

82 — 65 kohta.

83 — Ibidem.

84 — Ibidem (66 kohta).

85 — Ks. tästä päätöksen 2000/520 liite II, FAQ 11, jonka otsikkona on ”FTC:n toiminta”, sekä sen liitteet III, V ja VII.

86 — Ks. tuomio Digital Rights Ireland ym. (C-293/12 ja C-594/12, EU:C:2014:238, 68 kohta oikeuskäytäntöviittauksineen).

209. Tässä yhteydessä on korostettava kansallisten valvontaviranomaisten asemaa unionissa voimassa olevassa henkilötietojen suojan järjestelmässä, kun valvotaan direktiivin 95/46 13 artiklassa säädettyjä rajoituksia. Tämän direktiivin 28 artiklan 4 kohdan toisen alakohdan mukaan ”kuka tahansa henkilö voi erityisesti esittää valvontaviranomaiselle vaateen käsittelyn laillisuuden tarkastamisesta sovellettaessa tämän direktiivin 13 artiklan mukaisesti toteutettuja kansallisia toimenpiteitä”. Vastaavasti katson, että päätöksen 2000/520 liitteessä I olevaan neljänteen kohtaan sisältyvään safe harbor -periaatteiden soveltamisen rajoituksia koskevaan mainintaan olisi pitänyt liittää henkilötietojen suojaan erikoistuneen itsenäisen viranomaisen harjoittamaan valvontaan liittyvä mekanismi.

210. Itsenäisten valvontaviranomaisten toimenpiteet kuuluvat näet henkilötietojen suojaa koskevan eurooppalaisen järjestelmän ytimeen. On siis luonnollista, että tällaisen viranomaisen olemassaoloa on pidetty alusta alkaen yhtenä tarpeellisena edellytyksenä, jotta kolmansien maiden tarjoaman suojan tasoa voidaan pitää riittävänä. Kyseessä on yksi edellytys sille, että tietovirtoja jäsenvaltioiden alueelta kolmansien maiden alueelle ei kiellettäisi direktiivin 95/46 25 artiklan nojalla.[87] Kuten tämän direktiivin 29 artiklan nojalla perustetun työryhmän hyväksymässä keskusteluasiakirjassa huomautetaan, Euroopassa on laaja yksimielisyys siitä, että ”’ulkopuolisen valvonnan’ olemassaolo riippumattoman viranomaisen hoidossa on tarvittava osatekijä jokaisessa järjestelmässä, jolla pyritään varmistamaan tietosuojaa koskevien sääntöjen noudattaminen”.[88]

211. Korostettakoon lisäksi, että FISC ei tarjoa tehokasta oikeussuojaa unionin kansalaisille, joiden henkilötietoja siirretään Yhdysvaltoihin. Suojaa hallituksen yksiköiden harjoittamaa tarkkailua vastaan sovelletaan näet ulkomaisten tiedustelupalvelujen tarkkailusta vuonna 1978 annetun lain 702 §:n perusteella yksinomaan Yhdysvaltojen kansalaisiin sekä ulkomaiden kansalaisiin, jotka oleskelevat laillisesti ja pysyvästi Yhdysvalloissa. Kuten komissio on itse korostanut, Yhdysvaltojen tiedustelutietojen keruuohjelmien valvontaa voitaisiin parantaa vahvistamalla FISC:n roolia ja ottamalla käyttöön yksityishenkilöitä koskevia oikeuskeinoja. Näillä järjestelyillä voitaisiin vähentää unionin kansalaisten henkilötietojen käsittelyä tapauksissa, joilla ei ole merkitystä kansallisen turvallisuuden kannalta.[89]

212. Lisäksi komissio on itse todennut, että unionin kansalaisilla ei ole mahdollisuutta saada itseään koskevia tietoja tai saada ne oikaistuksi tai poistetuksi, eivätkä he voi valittaa hallinto- tai oikeusteitse Yhdysvaltojen vakoiluohjelmien puitteissa tapahtuvasta henkilötietojensa keruusta ja edelleenkäsittelystä.[90]

213. Lopuksi on mainittava, että yksityisyyden suojaan liittyviä Yhdysvaltojen oikeussääntöjä voidaan soveltaa eri tavalla Yhdysvaltojen kansalaisiin ja ulkomaiden kansalaisiin.[91]

214. Edellä esitetystä johtuu, ettei päätöksessä 2000/520 vahvisteta selviä ja täsmällisiä sääntöjä, jotka koskisivat perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin puuttumisen laajuutta. Näin ollen on todettava, että tämä päätös ja sen soveltaminen merkitsevät laajaa ja erityisen vakavaa puuttumista näihin perusoikeuksiin ilman, että tällaista puuttumista olisi tarkasti rajattu säännöksillä, joilla voidaan taata, että se todella rajataan siihen, mikä on ehdottomasti tarpeen.

87 — Ks. Poullet, Y., ”L’autorité de contrôle: ‘vues’ de Bruxelles”, *Revue française d’administration publique*, nro 89, tammi-maaliskuu 1999, s. 69, erityisesti s. 71.

88 — Ks. alaviitteessä 56 mainitun komission WP 12 -työasiakirjan s. 7.

89 — Ks. edellä alaviitteessä 2 mainittu komission tiedonanto, s. 10 ja 11.

90 — Ks. edellä alaviitteessä 58 mainittu komission tiedonanto, 7.2 kohta, s. 20.

91 — Ks. tämän kysymyksen osalta Kuner, C., ”Foreign Nationals and Data Protection Law: A Transatlantic Analysis”, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, s. 213, erityisesti s. 216 ja sitä seuraavat sivut.

215. Kun komissio on tehnyt päätöksen 2000/520 ja pitänyt sen myöhemmin voimassa, se on siten ylittänyt rajat, joita suhteellisuusperiaatteen noudattaminen edellyttää perusoikeuskirjan 7 ja 8 artiklan ja 52 artiklan 1 kohdan perusteella. Tähän on lisättävä, että unionin kansalaisilla on perusoikeuskirjan 47 artiklassa suojattu oikeus tehokkaaseen oikeussuojaan, johon on puututtu tavalla, joka ei ole perusteltavissa.

216. Tämä päätös on näin ollen todettava pätemättömäksi, koska edellä kuvattujen perusoikeuksien loukkaamisten vuoksi ei voida katsoa, että siinä käyttöön otetussa safe harbor -järjestelmässä taattaisiin unionista tämän järjestelmän yhteydessä Yhdysvaltoihin siirrettävien henkilötietojen tietosuojan riittävä taso.

217. Komission olisi siis mielestäni pitänyt keskeyttää päätöksen 2000/520 soveltaminen todetessaan unionin kansalaisten perusoikeuksia loukatun tällä tavoin.

218. Tämä päätös on tehty toistaiseksi. Nyt käsiteltävä asia osoittaa, että kolmannen maan tarjoaman suojan tason riittävyys voi vaihdella ajan myötä sitä mukaa kun kyseisen päätöksen taustalla olevat tosiseikat ja oikeudelliset seikat muuttuvat.

219. On korostettava, että päätös 2000/520 itse sisältää säännöksiä, joissa viitataan siihen mahdollisuuteen, että komissio mukauttaa päätöstä olosuhteiden mukaan.

220. Esimerkiksi tämän päätöksen johdanto-osan yhdeksännestä perustelukappaleesta ilmenee, että ”safe harbor -periaatteiden ja FAQ:iden tarkistaminen saattaa olla tarpeen yksityisyyden suojaan liittyvien kokemusten ja kehityksen perusteella, kun teknologia jatkuvasti yksinkertaistaa henkilötietojen siirtoa ja käsittelyä, ja niiden kertomusten perusteella, joita saadaan asiaa käsitteleviltä täytäntöönpanoviranomaisilta”.

221. Samoin kyseisen päätöksen 3 artiklan 4 kohdassa säädetään, että ”jos 1, 2 ja 3 kohdan mukaisesti saadut tiedot osoittavat, että jokin FAQ:iden mukaisesti sovellettavien periaatteiden noudattamisesta Yhdysvalloissa vastuussa oleva elin ei tosiasiallisesti täytä tehtäväänsä, komissio tiedottaa asiasta Yhdysvaltojen kauppaministeriölle ja esittää tarvittaessa – – luonnoksen toimenpiteistä, joiden tarkoituksena on kumota tämä päätös tai lykätä sen soveltamista tai rajoittaa sen soveltamisalaa”.

222. Lisäksi päätöksen 2000/520 4 artiklan 1 kohdan mukaan tätä päätöstä ”voidaan muuttaa milloin tahansa täytäntöönpanosta saatujen kokemusten perusteella ja/tai jos Yhdysvaltojen lainsäädäntö antaa periaatteita ja FAQ:ita paremman suojan. Komissio arvioi tämän päätöksen täytäntöönpanon käytettävissä olevien tietojen perusteella kolme vuotta sen jälkeen, kun se on annettu tiedoksi jäsenvaltioille, ja toimittaa kaikki tärkeät huomiot direktiivin 95/46 – – 31 artiklalla perustetulle komitealle, myös kaiken aineiston, joka voi vaikuttaa tämän päätöksen 1 artiklan säännösten arviointiin direktiivin 95/46 – – 25 artiklassa tarkoitetun riittävän suojan osalta”. Päätöksen 2000/520 4 artiklan 2 kohdan mukaan ”komissio esittää tarvittaessa luonnoksen toimenpiteistä 31 artiklassa säädetyn menettelyn mukaisesti”.

223. Komissio on todennut huomautuksissaan, että on ”erittäin todennäköistä, että sitoutumista safe harbor -periaatteisiin on rajoitettu tavalla, joka ei enää vastaa tarkasti rajattuja edellytyksiä, jotka on asetettu kansallista turvallisuutta koskevan poikkeuksen osalta”. [92] Se huomauttaa tästä, että ”kyseisistä paljastuksista ilmenee, että tarkkailua suoritetaan erottelemattomasti ja laajamittaisesti, mikä ei vastaa

92 — 44 kohta.

tämän poikkeuksen mukaista tarpeellisuuden edellytystä eikä laajemmin perusoikeuskirjan 8 artiklassa vahvistettua oikeutta henkilötietojen suojaan”.[93] Komissio on lisäksi itse todennut, että ”näiden ohjelmien laajuus ja [unionin] kansalaisten eriarvoinen kohtelu niiden yhteydessä herättää epäilyjä siitä, onko safe harbor -järjestelmän tarjoama suojan taso riittävä”.[94]

224. Komissio on lisäksi nimenomaisesti myöntänyt istunnossa, että päätös 2000/520, sellaisena kuin sitä tällä hetkellä sovelletaan, ei sisällä takeita siitä, että unionin kansalaisten oikeus tietojensa suojaan varmistettaisiin. Tämä toteamus ei sen mielestä kuitenkaan tee tästä päätöksestä pätemätöntä. Vaikka komissio on samaa mieltä väitteestä, jonka mukaan sen on ryhdyttävä toimenpiteisiin olosuhteiden muuttuessa, se katsoo toteuttaneensa toimenpiteitä, jotka ovat asianmukaisia ja oikeasuhteisia, aloittaessaan neuvottelut Yhdysvaltojen kanssa safe harbor -järjestelmän muuttamiseksi.

225. En ole samaa mieltä. Tällä välin henkilötietojen siirrot Yhdysvaltoihin on näet voitava keskeyttää kansallisten valvontaviranomaisten aloitteesta tai niille tehtyjen kantelujen perusteella.

226. Katson lisäksi, että komission olisi pitänyt tällaisten toteamusten perusteella keskeyttää päätöksen 2000/520 soveltaminen. Direktiivin 95/46 ja perusoikeuskirjan 8 artiklan tavoittelema henkilötietojen suojan tavoite asettaa näet velvoitteita paitsi jäsenvaltioille, myös unionin toimielimille, kuten perusoikeuskirjan 51 artiklan 1 kohdasta ilmenee.

227. Kun komissio arvioi tietyn kolmannen maan tarjoaman suojan tasoa, sen on tutkittava paitsi tämän kolmannen maan kansallista lainsäädäntöä ja kansainvälisiä sitoumuksia, myös tapaa, jolla henkilötietojen suoja taataan käytännössä. Jos käytännön tutkiminen osoittaa häiriöiden olemassaolon, komission on reagoitava ja tarvittaessa keskeytettävä päätöksensä soveltaminen ja/tai muutettava sitä viipymättä.

228. Kuten edellä on todettu, jäsenvaltiot ovat pääasiallisesti velvollisia takaamaan direktiivin 95/46 sääntöjen noudattamisen kansallisten valvontaviranomaistensa toiminnan avulla.

229. Komission velvollisuutena on keskeyttää tämän direktiivin 25 artiklan 6 kohdan nojalla tekemänsä päätöksen soveltaminen, jos ilmenee, että kyseinen kolmas maa on syyllistynyt laiminlyönteihin, sinä aikana, jona se käy neuvotteluja kyseisen kolmannen maan kanssa kyseisten laiminlyöntien lopettamiseksi.

230. Muistutettakoon siitä, että tämän säännöksen nojalla tehdyn komission päätöksen tarkoituksena on todeta, että tietyssä kolmannessa maassa ”taataan” tähän kolmanteen maahan siirrettävien henkilötietojen tietosuojan riittävä taso. Sana ”taataan” preesensissä merkitsee sitä, että jotta tällainen päätös voidaan pitää voimassa, sen on koskettava tiettyä kolmatta maata, jossa tämän päätöksen jälkeenkin taataan tällaisen suojan riittävä taso.

231. Direktiivin 95/46 johdanto-osan 57 perustelukappaleessa todetaan, että ”jos tietosuojan taso kolmannessa maassa ei ole riittävä, henkilötietojen siirto kyseiseen maahan on kiellettävä”.

232. Tämän direktiivin 25 artiklan 4 kohdassa säädetään, että ”jos komissio 31 artiklan 2 kohdassa vahvistetun menettelyn mukaisesti toteaa, että tietyssä kolmannessa maassa ei taata tietosuojan riittävää tasoa tämän artiklan 2 kohdassa tarkoitetussa merkityksessä, jäsenvaltioiden on toteutettava tarvittavat toimenpiteet kyseiseen kolmanteen maahan kohdistuvien samanluonteisten siirtojen estämiseksi”. Lisäksi kyseisen direktiivin 25 artiklan 5 kohdassa säädetään, että ”komissio aloittaa sopivalla hetkellä neuvottelut 4 kohdan mukaisesti tehdystä toteamuksesta aiheutuneen tilanteen korjaamiseksi”.

93 — Idem.

94 — Ks. edellä alaviitteessä 2 mainittu komission tiedonanto, s. 5.

233. Viimeksi mainitusta säännöksestä seuraa, että direktiivin 95/46 25 artiklalla käyttöön otetussa järjestelmässä kolmannen maan kanssa aloitettujen neuvottelujen tarkoituksena on korjata tämän direktiivin 31 artiklan 2 kohdassa säädetyn menettelyn mukaisesti todetun suojan riittävän tason puuttuminen. Nyt käsiteltävässä asiassa komissio ei ole todennut virallisesti kyseisen menettelyn mukaisella tavalla, että safe harbor -järjestelmä ei enää taannut tietosuojan riittävää tasoa. Jos kuitenkin komissio on päättänyt aloittaa neuvottelut Yhdysvaltojen kanssa, se on varmaankin tätä ennen katsonut, että tässä kolmannessa maassa taattu tietosuojan taso ei ollut enää riittävä.

234. Vaikka komissio tiesi häiriöistä päätöksen 2000/520 soveltamisessa, se ei keskeyttänyt sen soveltamista eikä muuttanut sitä, joten niiden henkilöiden perusoikeuksien loukkaaminen jatkui, joiden henkilötietoja oli siirretty ja edelleen siirrettiin safe harbor -järjestelmän yhteydessä.

235. Yhteisöjen tuomioistuin on jo todennut, joskin eri yhteydessä, että komission tehtävänä on huolehtia siitä, että lainsäädäntöä mukautetaan uusien tietojen mukaisesti. [95]

236. Komission tällainen laiminlyönti, jolla loukataan suoraan perusoikeuskirjan 7, 8 ja 47 artiklassa suojattuja perusoikeuksia, merkitsee mielestäni lisäsyytä todeta päätös 2000/520 pätemättömäksi tämän ennakkoratkaisumenettelyn yhteydessä. [96]

III **Ratkaisuehdotus**

237. Edellä esitetyn perusteella ehdotan, että unionin tuomioistuin ratkaisisi High Courtin esittämät ennakkoratkaisukysymykset seuraavasti:

Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24.10.1995 annetun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY 28 artiklaa, luettuna Euroopan unionin perusoikeuskirjan 7 ja 8 artiklan valossa, on tulkittava siten, että se, että on olemassa direktiivin 95/46 25 artiklan 6 kohdan nojalla tehty Euroopan komission päätös, ei estä kansallista valvontaviranomaista tutkimasta kantelua, jossa väitetään, että tietty kolmas maa ei takaa siirretyille henkilötiedoille tietosuojan riittävää tasoa, ja tarvittaessa keskeyttämästä näiden tietojen siirtoa.

Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä 26.7.2000 tehty komission päätös 2000/520/EY on pätemätön.

95 — Ks. vastaavasti tuomio Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, 40 kohta).

96 — Vaikka yhteisöjen tuomioistuin totesi tuomiossaan T. Port (C-68/95, EU:C:1996:452), että ”perustamissopimuksessa ei ole säädetty sellaisen ennakkoratkaisumenettelyn mahdollisuudesta, jolla kansallinen tuomioistuin voisi vaatia yhteisöjen tuomioistuinta toteamaan ennakkoratkaisussaan toimielimen laiminlyönnin” (53 kohta), vaikuttaa siltä, että se omaksui tälle mahdollisuudelle myönteisemmän näkemyksen tuomiossaan Ten Kate Holding Musselkanaal ym. (C-511/03, EU:C:2005:625, 29 kohta).