Kohtulahendite kogumik

KOHTUJURISTI ETTEPANEK
YVES BOT
esitatud 23. septembril 2015 [1]

Kohtuasi C-362/14

Maximillian Schrems
versus
Data Protection Commissioner

(eelotsusetaotlus, mille on esitanud High Court, Iirimaa)

Eelotsusetaotlus — Isikuandmed — Füüsiliste isikute kaitse seoses nende andmete töötlemisega — Euroopa Liidu põhiõiguste harta — Artiklid 7, 8 ja 47 — Direktiiv 95/46/EÜ — Artikkel 25 — Otsus 2000/520/EÜ — Isikuandmete edastamine Ameerika Ühendriikidesse — Kaitsetaseme piisavuse või ebapiisavuse hindamine — Kaebus, mille esitas füüsiline isik, kelle andmed on edastatud kolmandale riigile — Liikmesriigi järelevalveasutus — Volitused

I. **Sissejuhatus**

1. Euroopa Komisjon on oma 27. novembri 2013. aasta teatises [2] märkinud, et „[i]sikuandmete edastamine on atlandiüleste suhete oluline ja vajalik aspekt. See moodustab atlandiüleste kaubandussuhete lahutamatu osa muu hulgas uute kasvavate digitaalettevõtete jaoks, kes tegutsevad näiteks sotsiaalmeedia või pilvandmetöötluse vallas ja edastavad EList Ameerika Ühendriikidesse suuri andmehulki” [3].

2. Kaubandussuhteid käsitleb komisjoni 26. juuli 2000. aasta otsus 2000/520/EÜ vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium [4]. See otsus annab õigusliku aluse liidust isikuandmete edastamiseks Ameerika Ühendriikides asuvatele ettevõtjatele, kes järgivad Safe Harbor’ põhimõtteid.

3. Nimetatud otsuse ees seisab täna proovikivi: kuidas võimaldada andmete liikumist liidu ja Ameerika Ühendriikide vahel, tagades samal ajal nende andmete kõrgetasemelise kaitse, nagu liidu õigus nõuab.

4. Nimelt on teatavad paljastused viimasel ajal toonud päevavalgele Ameerika Ühendriikide laiaulatuslike teabekogumise programmide olemasolu. Need paljastused on tekitanud kahtlusi seoses sellega, kas Ameerika Ühendriikides asuvatele ettevõtjatele isikuandmete edastamisel järgitakse liidu õigusnorme, ja seoses Safe Harbor’ süsteemi puudustega.

1 — Algkeel: prantsuse.

2 — Komisjoni teatis Euroopa Parlamendile ja nõukogule „Usalduse taastamine ELi ja Ameerika Ühendriikide vaheliste andmevoogude vastu” (COM(2013) 846 final).

3 — Lk 2.

4 — ELT L 215, lk 7, parandus ELT 2001, L 115, lk 14.

5. Käesolevas eelotsusetaotluses palutakse Euroopa Kohtul täpsustada, kuidas peavad toimima liikesriigi järelevalveasutused ja komisjon, kui nad seisavad silmitsi häiretega otsuse 2000/520 kohaldamisel.

6. Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta [5] näeb IV peatükis ette reeglid isikuandmete edastamiseks kolmandatesse riikidesse.

7. Selles peatükis sisaldub direktiivi artikli 25 lõikes 1 kehtestatud põhimõte, et töödeldavate või pärast edastamist töötlemiseks kavandatud isikuandmete edastamine kolmandatesse riikidesse võib toimuda ainult juhul, kui kõnealune kolmas riik tagab andmekaitse piisava taseme.

8. Seevastu, nagu märkis ka liidu seadusandja nimetatud direktiivi põhjenduses 57, tuleb keelata isikuandmete edastamine kolmandatesse riikidesse, kus nende kaitse tase ei ole piisav.

9. Direktiivi 95/46 artikli 25 lõikes 2 on sätestatud, et „[a]ndmekaitse taset kolmandates riikides hinnatakse, pidades silmas kõiki andmete edastamise toimingute või andmete edastamise toimingute kogumi asjaolusid; tähelepanu pööratakse eelkõige andmete laadile, kavandatud töötlemistoimingu või töötlemistoimingute eesmärgile ja kestusele, päritoluriigile ja lõppsihtriigile, kõnealuses kolmandas riigis kehtivatele nii üldistele kui ka konkreetse sektori õigusnormidele ja kõnealuses riigis järgitavatele ametieeskirjadele ja turvameetmetele".

10. Kõnesoleva direktiivi artikli 25 lõike 6 kohaselt võib komisjon leida, et kolmas riik tagab isikuandmete kaitse piisava taseme oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega. Isikuandmeid võib asjaomasesse kolmandasse riiki edastada siis, kui komisjon on teinud vastavasisulise otsuse.

11. Selle sätte rakendamisel võttis komisjon vastu otsuse 2000/520. Nimetatud otsuse artikli 1 lõikest 1 tuleneb, et „„Safe Harbor' põhimõtte[i]d" eraelu puutumatuse kohta", rakendatuna kooskõlas „korduma kippuvate küsimustega" [6], leitakse tagavat kaitse piisava taseme liidust Ameerika Ühendriikides asuvatele ettevõtjatele edastatavatele isikuandmetele.

12. Seetõttu lubab otsus 2000/520 edastada isikuandmeid liikmesriikidest nendele Ameerika Ühendriikides asuvatele ettevõtjatele, kes on võtnud kohustuse järgida Safe Harbor' põhimõtteid.

13. Otsuse 2000/520 I lisas sätestatakse teatavad põhimõtted, millele ettevõtjad võivad vabatahtlikult alla kirjutada ja millega kaasnevad piirangud ning konkreetne järelevalvemehhanism. 2013. aastal ületas sellele „käitumiskoodeksile" alla kirjutanud ettevõtjate arv 3200 ettevõtja piiri.

14. Programm Safe Harbor toetub lahendusele, mis ühendab eraõiguslike ettevõtjate poolset enesesertifitseerimist ja -hindamist ning avaliku võimu sekkumist.

15. Safe Harbor' põhimõtted töötati välja „koostöös tootjate ja üldsusega äri- ja kaubandustegevuse lihtsustamiseks Ameerika Ühendriikide ja [liidu] vahel. Nad on mõeldud kasutamiseks ainult isikuandmeid [liidust] vastu võtvate Ameerika Ühendriikide organisatsioonide poolt, et saavutada vastavus programmi Safe Harbor põhimõtetega ja seeläbi saavutada eeldatav „piisav" andmekaitse [7].

5 — EÜT L 281, lk 31; ELT eriväljaanne 13/15, lk 355. Direktiiv sellisel kujul, nagu seda muudeti Euroopa Parlamendi ja nõukogu 29. septembri 2003. aasta määrusega (EÜ) nr 1882/2003 (ELT L 284, lk 1; ELT eriväljaanne 01/04, lk 447) (edaspidi „direktiiv 95/46").

6 — Korduma kippuvad küsimused, edaspidi „KKK".

7 — Otsuse 2000/520 I lisa teine lõik.

16. Otsuse 2000/520 I lisas loetletud Safe Harbor' põhimõtted sisaldavad muu hulgas järgmist:

— teavitamiskohustus, mille kohaselt „organisatsioon peab üksikisikutele teatama, millistel eesmärkidel ta kogub ja kasutab nende kohta käivaid andmeid, kuidas võtta organisatsiooniga ühendust päringute või kaebuste korral, missugust liiki kolmandatele osapooltele ta andmeid avaldab ning valikutest ja vahenditest, mida organisatsioon üksikisikutele andmete kasutamise ja avaldamise piiramiseks pakub. Selline teade tuleb esitada selges ja arusaadavas keeles, kui üksikisikutel palutakse esmakordselt esitada isikuandmeid organisatsioonile, või pärast seda niipea, kui see on teostatav, kuid igal juhul enne, kui organisatsioon seda teavet kasutab muul eesmärgil kui see, milleks need algselt koguti või milleks andmeid edastav organisatsioon neid töötles või avaldab need esmakordselt kolmandale osapoolele" [8];

— organisatsiooni kohustus pakkuda üksikisikutele võimalust valida, kas nende isikuandmeid avaldatakse kolmandale osapoolele või kasutatakse muul eesmärgil kui see, milleks neid algselt koguti või milleks üksikisik seejärel loa andis. Üksikisikutele tuleb võimaldada selge ja arusaadav, käepärane ja taskukohane mehhanism valiku teostamiseks. Tundliku teabe osas „tuleb võimaldada kinnitav või selge valik, kui teave avalikustatakse kolmandale osapoolele või seda kasutatakse muul eesmärgil kui see, milleks seda algselt koguti või milleks üksikisik loa andis nõustuva valikuga [9];

— andmete edasise edastamise eeskirjad. „Teabe avalikustamisel kolmandale osapoolele peavad organisatsioonid kohaldama teate ja valikuvõimaluse põhimõtteid" [10];

— andmete turvalisuse osas nende „organisatsioonid[e], mis tekitavad, säilitavad, kasutavad või levitavad isikuandmeid, [kohustus] rakenda[d]a põhjendatud ettevaatusabinõusid nende kaitsmiseks kadumise, väärkasutuse ja volitamatu juurdepääsu, avalikustamise, muutmise ja hävitamise eest" [11];

— andmeterviklikkuse osas on organisatsioon kohustatud „[…] võtma mõistlikke meetmeid, tagamaks et andmed on kavatsetud kasutuseks usaldusväärsed, täpsed, täielikud ja aktuaalsed" [12];

— üksikisikutel peab põhimõtteliselt olema „juurdepääs organisatsiooni käes olevatele neid puudutavatele isikuandmetele ning võimalus neid parandada, muuta või kustutada, kui need on ebatäpsed" [13];

— kohustus näha ette „mehhanisme [Safe Harbor'] põhimõtetele vastavuse tagamiseks, kaebuste käsitlemise võimalust üksikisikutele, keda puudutavaid andmeid põhimõtete eiramine on mõjutanud, ning tagajärgi organisatsiooni[de]le, […] kes on deklareerinud oma vastavust neile [14].

17. Ameerika Ühendriikide organisatsioon, kes soovib Safe Harbor' põhimõtete järgimist kinnitada, peab tema järgitavas eraelu puutumatuse kaitse poliitikas avalikult deklareerima, et ta vastab nendele põhimõtetele ja tegelikult neid ka järgib, ning teostama enesesertifitseerimise, teavitades Ameerika Ühendriikide kaubandusministeeriumit, et ta vastab nendele põhimõtetele [15].

8 — Vt I lisa, punkt „Teade".

9 — Vt I lisa, punkt „Valikuvõimalus".

10 — Vt I lisa, punkt „Edasine edastamine".

11 — Vt I lisa, punkt „Turvalisus".

12 — Vt I lisa, punkt „Andmeterviklikkus".

13 — Vt I lisa, punkt „Juurdepääs".

14 — Vt I lisa, punkt „Täitmise tagamine".

15 — Otsuse 2000/520 artikli lõiked 2 ja 3. Vt ka II lisa, KKK 6.

18. Organisatsioon võib Safe Harbor' põhimõtteid järgida mitmel moel. Näiteks võib ta „liitu[da] põhimõtteid järgiva [erasektori hallatava] eraelu puutumatuse kaitse programmiga [või] saavuta[da] vastavuse [Safe Harbor' põhimõtetele] siis, kui ta töötab välja isereguleeruvad eraelu puutumatuse normid, tingimusel et need vastavad põhimõtetele. […] Lisaks võib programmi Safe Harbor soodustustele õigus olla organisatsioonidel, mis alluvad normatiiv-, regulatiiv-, administratiiv- või muude seaduste (või õigusnormide) kogumile, mis eraelu puutumatust tõhusalt kaitseb". [16]

19. Safe Harbor' põhimõtete järgimise kontrollimiseks on kasutusel mitu mehhanismi, mis ühendavad endas eraõiguslikku vahekohut ja avaliku võimu järelevalvet. Kolmas sõltumatu osapool saab seega tagada kontrolli vaidluste kohtuvälise lahendamise teel. Lisaks võivad ettevõtjad teha koostööd liidu andmekaitseteemalise paneeliga. Lõpetuseks on Federal Trade Commission (föderaalne kaubanduskomisjon, edaspidi „FTC") pädev kaebusi läbi vaatama nende volituste alusel, mis talle on antud Federal Trade Commission Act'i (föderaalse kaubanduskomisjoni seadus) puntis 5, ning Department of Transportation (transpordiministeerium) on pädev kaebusi läbi vaatama nende volituste alusel, mis talle on antud United States Code'i (Ameerika Ühendriikide seadustik) 49. jaotises asuvas punktis 41712.

20. Otsuse 2000/520 I lisa neljandas lõigus on sätestatud, et Safe Harbor' põhimõtete järgimist võib piirata muu hulgas „[Ameerika Ühendriikide] riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks" ja „statuudi, valitsuse määruse või pretsedendiõigusega, mis loovad vasturääkivaid kohustusi või annavad otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon demonstreerida, et põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks" [17].

21. Lisaks on liikmesriikide pädevate ametiasutuste võimalused andmevoogu peatada allutatud mitmele tingimusele, mis on ette nähtud otsuse 2000/520 artikli 3 lõikes 1.

22. Käesolev eelotsusetaotlus käsitleb küsimust, milline on otsuse 2000/520 ulatus, võttes arvesse Euroopa Liidu põhiõiguste harta (edaspidi „harta") artikleid 7, 8 ja 47 ning direktiivi 95/46 artikli 25 lõiget 6 ja artiklit 28. Eelotsusetaotlus esitati M. Schrems'i ja Data Protection Commissioner'i (edaspidi „andmekaitsevolinik") vahelises vaidluses, mis puudutas viimase otsust keelduda menetlemast kaebust, mille M. Schrems esitas seetõttu, et Facebook Ireland Ltd. (edaspidi „Facebook Ireland") säilitab oma kasutajate isikuandmeid Ameerika Ühendriikides asuvas serveris.

23. M. Schrems on Austria kodanik, kes elab Austrias. Ta on sotsiaalvõrgustiku Facebook kasutaja alates 2008. aastast.

24. Kõik liidu territooriumil elavad Facebooki kasutajad peavad sõlmima lepingu Facebook Ireland'iga, kes on Ameerika Ühendriikides asuva emaettevõtja Facebook Inc. (edaspidi „Facebook USA") tütarettevõtja. Liidu territooriumil elavate Facebook Ireland'i kasutajate andmed edastatakse kas tervikuna või osaliselt Facebook USA serveritesse, mis asuvad Ameerika Ühendriikide territooriumil, ja neid säilitatakse seal.

25. M. Schrems esitas 25. juunil 2013 andmekaitsevolinikule kaebuse, väites sisuliselt, et Ameerika Ühendriikide kehtiv õigus ja valitsev praktika ei taga Ameerika Ühendriikide territooriumil säilitatavate andmete puhul mitte mingisugust tegelikku kaitset riigipoolse jälgimise eest. Kaebuse ajendiks olid alates 2013. aasta maikuust Edward Snowdeni poolt Ameerika Ühendriikide luureteenistuste ja täpsemalt National Security Agency (riiklik julgeolekuagentuur, edaspidi „NSA") tegevuse kohta tehtud paljastused.

16 — I lisa kolmas lõik.

17 — Vt ka IV lisa jaotis B.

26. Nendest paljastustest ilmneb muu hulgas, et NSA oli loonud PRISM-nimelise programmi, mille raames sai see agentuur õiguse vabalt tutvuda andmekogumitega, mis on salvestatud Ameerika Ühendriikides asuvates serverites, mida omavad või juhivad rida äriühinguid, kes on tegevad interneti ja tehnoloogia valdkonnas, näiteks Facebook USA.

27. Andmekaitsevolinik leidis, et ei ole kohustatud kaebust menetlema, kuna sellel puudus õiguslik alus. Tema arvates ei olnud tõendeid selle kohta, et NSA oleks tutvunud M. Schremsi andmetega. Lisaks tuli kaebus andmekaitsevoliniku hinnangul tagasi lükata otsuse 2000/520 tõttu, milles komisjon sedastas, et programmi Safe Harbor raames tagavad Ameerika Ühendriigid edastatud isikuandmete kaitse piisava taseme. Kõik Ameerika Ühendriikides nende andmete kaitse piisavat taset puudutavad küsimused tuli lahendada kooskõlas selle otsusega, mis takistas tal kaebuses tõstatatud probleemi käsitlemast.

28. Liikmesriigi õigusnormid, mille alusel andmekaitsevolinik kaebust tagasilükkava otsuse tegi, on järgmised.

29. 1988. aasta andmekaitseseaduse (Data Protection Act 1988), muudetud 2003. aasta andmekaitseseadusega (Data Protection (Amendment) Act 2003; edaspidi „andmekaitseseadus"), artikli 10 lõikes 1 antakse andmekaitsevolinikule volitus kaebusi läbi vaadata ja sätestatakse järgmist:

„a) andmekaitsevolinik võib kontrollida või lasta kontrollida, kas käesoleva seaduse sätted olid, on või võivad olla konkreetse isiku juhtumil rikutud, kui see isik esitab talle kaebuse mõne selle seaduse säte rikkumise kohta või kui andmekaitsevolinik on seisukohal, et niisugune rikkumine võib esineda;

b) kui andmekaitsevolinikule esitatakse kaebus käesoleva lõigu punkti a alusel, siis andmekaitsevolinik:

i) menetleb kaebust või laseb seda menetleda, välja arvatud juhul, kui ta peab seda põhjendamatuks või pahatahtlikuks, ja

ii) kui ta ei suuda mõistliku aja jooksul saavutada, et pooled sõlmivad kaebuse eseme kohta kompromissi, teavitab ta kaebuse esitajat kaebuse kohta langetatud otsusest kirjalikult, märkides, et kui see otsus kaebuse esitajat kahjustab, siis võib ta selle 21 päeva jooksul alates teatise kättesaamisest kohtusse kaevata vastavalt käesoleva seaduse artiklile 26."

30. Käesoleval juhul järeldas andmekaitsevolinik, et M. Schremsi kaebus oli „põhjendamatu või pahatahtlik", kuna õigusliku aluse puudumise tõttu oli see ebaõnnestumisele määratud. Just sel põhjusel keeldus andmekaitsevolinik kaebust menetlemast.

31. Andmekaitseseaduse artikkel 11 reguleerib isikuandmete edastamist väljapoole liikmesriigi territooriumi. Selle seaduse artikli 11 lõike 2 punkt a näeb ette:

„Kui käesolevas seaduses sätestatud menetluse käigus tõstatakse küsimus, mis puudutab:

i) selle kindlaksmääramist, kas Euroopa Majandusühendusest [(EMÜ)] väljaspool asuv riik või territoorium, kuhu isikuandmed edastatakse, tagab käesolevas artiklis täpsustatud kaitse piisava taseme, ja

ii) kõnealust tüüpi edastamise kohta on olemas liidu järeldus,

lahendatakse see küsimus kooskõlas nimetatud järeldusega."

32. Andmekaitseseaduse artikli 11 lõike 2 punktis b määratletakse mõiste „liidu järeldus" järgmiselt:

„Käesoleva lõigu punktis a tähendab mõiste „liidu järeldus" järeldust, millele Euroopa Komisjon on teinud [direktiivi 95/46] artikli 25 lõike 4 või 6 alusel, [selle direktiivi] artikli 31 lõikes 2 ette nähtud menetluse raames, et määrata kindlaks, kas [EMÜ-st] väljaspool asuv riik või territoorium tagab käesoleva artikli lõikes 1 täpsustatud kaitse piisava taseme."

33. Andmekaitsevolinik märgib, et otsus 2000/520 oli „liidu järeldus" andmekaitseseaduse artikli 11 lõike 2 punkti a tähenduses, mistõttu tuleb selle seaduse kohaselt kõik küsimused, mis puudutavad andmekaitse piisavust kolmandas riigis, kuhu need andmed edastatakse, lahendada kooskõlas selle järeldusega. M. Schremsi kaebuse põhilises osas, nimelt küsimuses, mis puudutab isikuandmete edastamist kolmandasse riiki, mis tegelikkuses ei taga piisaval tasemel kaitset, leiab andmekaitsevolinik, et otsuse 2000/520 laad ja olemasolu ise takistab tal seda küsimust uurimast.

34. M. Schrems pöördus High Courti (ülemkohus), vaidlustades andmekaitsevoliniku otsuse tema kaebus tagasi lükata. Olles põhikohtuasjas esitatud tõendeid uurinud, sedastas kohus, et isikuandmete elektrooniline seire ja infopüük teenib avalikes huvides vajalikke ja möödapääsmatuid eesmärke, nimelt riikliku julgeoleku säilitamist ja raskete kuritegude vältimist. High Court märgib selle kohta, et liidust Ameerika Ühendriikidesse edastatud isikuandmete seire ja infopüük teenib terrorismivastase võitlusega seotud õiguspäraseid eesmärke.

35. Sama kohtu sõnul näitavad E. Snowdeni paljastused siiski seda, et NSA ja teised sarnased asutused on oma volitusi märkimisväärselt ületanud. Kuigi Foreign Intelligence Surveillance Courtil (vastuluure järelevalvekohus, edaspidi „FISC"), mis tegutseb 1978. aasta vastuluureseaduse (Foreign Intelligence Surveillance Act of 1978) [18] alusel, on olemas kontrollipädevus, on selle kohtu menetlus alati salastatud ega ole oma laadilt võistlev. Lisaks, peale selle, et otsuseid selliste andmete kasutamise kohta tehakse Ameerika Ühendriikide seaduste alusel, ei ole EL-i kodanikel oma andmete seire ja infopüügi küsimuses sisuliselt mingit õigust olla ära kuulatud.

36. Põhikohtuasjas esitatud ametlikele kinnitustele lisatud arvukatest tõenditest nähtub selgelt, et suurt osa E. Snowdeni paljastustest ei ole kahtluse alla seatud. High Court järeldas sellest tulenevalt, et kui isikuandmed on kord Ameerika Ühendriikidesse edastatud, võivad NSA ja ka teised Ameerika Ühendriikide julgeolekuasutused, nagu Federal Bureau of Investigation (FBI) (föderaalne juurdlusbüroo), nendega massilise ja valimatu seire ning infopüügi käigus tutvuda.

37. High Court märgib, et Iirimaa õiguses nõuab põhiseaduslike õiguste eraelu ja eluaseme puutumatusele olulisus seda, et igasugune sekkumine neisse õigustesse vastaks seaduses ette nähtud nõuetele ja oleks proportsionaalne. Massiline ja valimatu isikuandmetega tutvumine ei vasta kuidagi proprtsionaalsuse nõudele ning järelikult tuleb seda pidada Iirimaa põhiseadusega vastuolus olevaks [19].

38. High Court märgib, et selleks, et elektroonilise side pealtkuulamist võiks pidada põhiseadusega kooskõlas olevaks, tuleks tõendada, et suhtluse konkreetne pealtkuulamine ja teatavate isikute või isikurühmade jälgimine on riikliku julgeoleku ja kuritegevuse tõkestamise huvides objektiivselt põhjendatud ning et sellega kaasnevad asjakohased ja kontrollitavad kaitsemeetmed.

18 — Vt punkti 702 nimetatud seaduses, mida on muudetud 2008. aasta seadusega (Foreign Intelligence Surveillance Act of 2008). Selle punkti alusel peab NSA andmebaasi, mida tuntakse nime all „PRISM" (vt *Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*, 27.11.2013).

19 — High Court viitab eelkõige inimväärikuse austamisele ja isikuvabadusele (preambul), isiklikule sõltumatusele (artikli 40 lõike 3 punktid 1 ja 2), eluaseme puutumatusele (artikli 40 lõige 5) ja pereelu kaitsele (artikkel 41).

39. Seega märgib High Court, et kui käesolev kohtuasi tuleks lahendada üksnes Iirimaa õiguse alusel, tekiks tõsine probleem seoses küsimusega, kas Ameerika Ühendriigid „tagavad eraelu puutumatuse ning põhiõiguste ja -vabaduste piisava kaitse" andmekaitseseaduse artikli 11 lõike 1 tähenduses. Siit järeldub, et Iirimaa õiguse ja täpsemalt selle põhiseaduslike nõuete kohaselt ei oleks andmekaitsevolinik tohtinud M. Schremsi kaebust tagasi lükata, vaid oleks pidanud seda küsimust käsitlema.

40. Igal juhul märgib High Court, et tema menetluses olev kohtuasi puudutab liidu õiguse kohaldamist harta artikli 51 lõike 1 tähenduses, mistõttu andmekaitsevoliniku otsuse õiguspärasust tuleks hinnata liidu õiguse alusel.

41. Probleemi, millega andmekaitsevolinik silmitsi seisab, kirjeldab High Court järgmiselt. Andmekaitseseaduse artikli 11 lõike 2 punkti a kohaselt peab andmekaitsevolinik lahendama kolmandates riikides kehtiva kaitse piisavuse küsimuse „kooskõlas" liidu seisukohaga, mille komisjon võttis vastavalt direktiivi 95/46 artikli 25 lõikele 6. Sellest järeldub, et andmekaitsevolinik ei saa niisugusest seisukohast kõrvale kalduda. Kuna komisjon on oma otsuses 2000/520 märkinud, et Ameerika Ühendriigid tagavad Safe Harbor' põhimõtteid järgivate äriühingute poolt andmete töötlemisel piisaval tasemel kaitse, siis peab andmekaitsevolinik niisuguse kaitse ebapiisavuse kohta esitatud kaebuse igal juhul tagasi lükkama.

42. Tehes küll järelduse selle kohta, et andmekaitsevolinik oli seega vankumatult ja täht-tähelt järginud direktiivi 95/46 ja otsust 2000/520, märgib High Court, et M. Schremsi vastuseis on tegelikult suunatud pigem Safe Harbor' programmi enda tingimuste vastu, mitte selle vastu, kuidas andmekaitsevolinik on seda kohaldanud, rõhutades siiski, et ei direktiivi 95/46 ega otsuse 2000/520 kehtivust ei ole otseselt vaidlustatud.

43. High Courti sõnul on põhiküsimus selles, kas liidu õiguse kohaselt ning võttes eelkõige arvesse harta artiklite 7 ja 8 hilisemat jõustumist, on andmekaitsevolinik absoluutselt kohustatud järgima järeldust, mille komisjon esitas otsuses 2000/520 Ameerika Ühendriikide kehtiva õiguse ja valitseva praktikaga tagatud isikuandmete kaitse piisavuse kohta.

44. High Court täpsustab lisaks, et tema menetluses olevas hagis ei tõstatatud kordagi küsimust Facebook Irelandi ja Facebook USA tegevuse enda kohta. Otsuse 2000/520 artikli 3 lõike 1 punkt b, mille alusel võivad liikmesriigi pädevad asutused anda ettevõtjale korralduse peatada andmete edastamine kolmandasse riiki, on selle kohtu arvates kohaldatav üksnes olukorras, kus kaebus on suunatud asjaomase ettevõtja tegevuse vastu, millega käesoleval juhul tegu ei ole.

45. High Court rõhutab seega, et tegelik etteheide ei puuduta mitte Facebook USA kui sellise tegevust, vaid pigem asjaolu, et komisjon asus seisukohale, et Ameerika Ühendriikide andmekaitseseadused ja -tavad tagavad piisava kaitse, samas kui E. Snowdeni paljastuste põhjal on selge, et Ameerika Ühendriikide ametiasutused võivad massiliselt ja valimatult tutvuda EL-i territooriumil elavate isikute isikuandmetega [20].

46. Selles osas leiab High Court, et raske on aru saada, kuidas otsus 2000/520 saab praktikas olla kooskõlas harta artiklite 7 ja 8 nõuetega, *a fortiori* arvestades Euroopa Kohtu poolt kohtuasjas Digital Rights Ireland jt [21] sedastatud põhimõtteid. Nimelt oleks harta artiklis 7 sätestatud ja liikmesriikide traditsioonide ühistest väärtustest lähtuv tagatis täielikult rikutud, kui riigiasutused saaksid elektroonilise sidega suvaliselt ja üldiselt tutvuda, ilma et neil oleks selleks vaja objektiivset põhjust, mis põhineks riikliku julgeoleku kaalutlustel või konkreetse asjaomase isiku või isikutega seotud

20 — High Court märgib selles osas, et peamine väide, mille M. Schrems selles kohtus esitas, seisnes kinnituses, et võttes arvesse E. Snowdeni hiljutisi paljastusi ning asjaolu, et isikuandmed olid tehtud Ameerika Ühendriikide luureteenistustele laiaulatuslikult kättesaadavaks, siis ei saa andmekaitsevolinik põhjendatult väita, et selles kolmandas riigis on need andmed piisavalt kaitstud.

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

kuritegevuse ennetamise vajadusel, ning millega kaasneksid asjakohased ja kontrollitavad kaitsemeetmed. Kuna M. Schremsi kaebuses väidetakse, et otsus 2000/520 võib *in abstracto* olla kokkusobimatu harta artiklitega 7 ja 8, siis võib Euroopa Kohus leida, et direktiivi 95/46, eelkõige selle artikli 25 lõiget 6 ning otsust 2000/520 võib tõlgendada viisil, mis lubab liikmesriigi asutustel viia ise läbi uurimisi, et teha kindlaks, kas isikuandmete edastamine kolmandasse riiki vastab harta artiklite 7 ja 8 nõuetele.

47. Neil tingimustel otsustas High Court menetluse peatada ja esitada Euroopa Kohtule järgmised eelotsuse küsimused:

„Kas harta artikleid 7, 8 ja 47 arvesse võttes ja ilma, et see piiraks direktiivi 95/46 artikli 25 lõike 6 kohaldamist, on andmekaitsevolinik, kes menetleb kaebust seoses isikuandmete edastamisega kolmandasse riiki (käesoleval juhul Ameerika Ühendriikidesse), milles kehtiv õigus ja valitsev praktika ei taga kaebuse esitaja väitel asjaomasele isikule piisavat kaitset, absoluutselt kohustatud järgima liidu vastupidist järeldust, mis sisaldub otsuses 2000/520?

Kas vastupidisel juhul võib või peab andmekaitsevolinik oma uurimises võtma arvesse pärast otsuse 2000/520 esmakordset avaldamist toimunud faktilist arengut?"

II. **Kohtujuristi analüüs**

48. Nende kahe High Courti sõnastatud küsimusega palutakse Euroopa Kohtul täpsustada liikmesriigi järelevalveasutuse volitusi, kui need lahendavad kaebust seoses isikuandmete edastamisega kolmandas riigis asuvale ettevõtjale, ja kaebuses väidetakse, et see kolmas riik ei taga edastatavatele andmetele piisaval tasemel kaitset, samas kui komisjon on direktiivi 95/46 artikli 25 lõike 6 alusel võtnud vastu otsuse, milles tunnistatakse nimetatud kolmanda riigi poolt tagatud kaitse tase piisavaks.

49. Olgu märgitud, et M. Schremsi esitatud kaebus andmekaitsevolinikule hõlmab kahte aspekti. Sellega vaidlustatakse Facebook Irelandi poolt isikuandmete edastamine Facebook USA-le. M. Schrems palub, et edastamine lõpetataks, kuna tema sõnul ei taga Ameerika Ühendriigid piisaval tasemel kaitset isikuandmetele, mida programmi Safe Harbor raames edastatakse. Täpsemalt heidab ta sellele kolmandale riigile ette programmi PRISM loomist, mis võimaldab NSA-l vabalt tutvuda andmekogumiga, mida säilitatakse Ameerika Ühendriikides asuvates serverites. Seega puudutab kaebus konkreetselt isikuandmete edastamist Facebook Irelandist Facebook Ameerika Ühendriikidesse, seades üldisemalt kahtluse alla ka programmi Safe Harbor raames niisugustele andmetele tagatud kaitse taseme.

50. Andmekaitsevoliniku sõnul takistas teda kaebust läbi vaatamast just see asjaolu, et on olemas komisjoni otsus, milles tunnistatakse, et Ameerika Ühendriigid tagavad programmi Safe Harbor raames kaitse piisava taseme.

51. Seega tuleb uurida koos neid kahte küsimust, milles palutakse sisuliselt selgitada, kas direktiivi 95/46 artiklit 28, koostoimes harta artiklitega 7 ja 8, tuleb tõlgendada nii, et asjaolu, et eksisteerib otsus, mille komisjoni tegi sama direktiivi artikli 25 lõike 6 alusel, takistab liikmesriigi järelevalveasutust uurimast kaebust, milles väidetakse, et kolmas riik ei taga edastatavate isikuandmete kaitset piisaval tasemel, ja nende andmete vaidlustatud edastamist vajaduse korral peatamast.

52. Harta artikkel 7 tagab õiguse eraelu austamisele, samas kui harta artikkel 8 sätestab sõnaselgelt õiguse isikuandmete kaitsele. Viimati nimetatud artikli lõiked 2 ja 3 täpsustavad, et selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ette nähtud õiguslikul alusel; et igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist, ning et nende sätete täitmist kontrollib sõltumatu asutus.

A. *Liikmesriigi järelevalveasutuse volitused seoses komisjoni piisavusotsusega*

53. Nagu M. Schrems oma seisukohtades märkis, on põhikohtuasja kaebuse puhul keskne küsimus isikuandmete edastamine Facebook Irelandist Facebook USAle, selles valguses, et tulenevalt volitustest, mida Ameerika Ühendriikide õigusnormid NSAle ja teistele Ameerika Ühendriikide julgeolekuasutustele annavad, on viimastel üldine õigus tutvuda Facebook USA juures säilitatavate andmetega.

54. Lahendades kaebust, milles seatakse kahtluse alla järeldus, et kolmas riik tagab edastatavate andmete kaitse piisaval tasemel, on liikmesriigi järelevalveasutus – kui tal on tõendeid, et kaebuses esitatud väited on põhjendatud – M. Schremsi sõnul pädev andma korraldust nimetatud kaebuses märgitud ettevõtjapoolse andmete edastamise peatamiseks.

55. Võttes arvesse andmekaitsevoliniku kohustust kaitsta M. Schremsi põhiõigusi, väidab viimane, et andmekaitsevolinikul ei ole mitte üksnes kohustus kaebust menetleda, vaid juhul, kui kaebus rahuldatakse, ka kohustus kasutada oma pädevust Facebook Irelandi ja Facebook USA vahelise andmevoo peatamiseks.

56. Andmekaitsevolinik lükkas kaebuse tagasi andmekaitseseaduse nende sätete alusel, kus on loetletud tema volitused. Järeldus tugines andmekaitsevoliniku seisukohal, et ta on seotud otsusega 2000/520.

57. Siit järeldub, et käesoleva kohtuasja keskne küsimus on see, kas komisjoni hinnang kaitse taseme piisavuse kohta, mis sisaldub otsuses 2000/520, on liikmesriigi andmekaitseasutusele absoluutselt siduv ja takistab tal menetlemast väiteid, millega see järeldus kahtluse alla seatakse. Eelotsuse küsimused käsitlevad seega liikmesriigi andmekaitseasutuste uurimisvolituste ulatust, kui eksisteerib komisjoni piisavusotsus.

58. Komisjoni sõnul tuleb arvesse võtta seost tema volituste ja liikmesriigi andmekaitseasutuse volituste vahel. Viimase volitused keskenduvad selle valdkonna õigusnormide kohaldamisele üksikjuhtumitel, samas kui otsuse 2000/520 kohaldamise üldine läbivaatamine, sealhulgas kõik selle otsuse peatamist või tühistamist puudutavad otsused, kuulub komisjoni pädevusse.

59. Komisjon märgib, et M. Schrems ei ole esitanud konkreetseid aegumente, mis viitaksid sellele, et Facebook Irelandi ja Facebook USA vahelise andmete edastamise tõttu tekib tal otsene tõsise kahju tekkimise oht. Vastupidi, oma abstraktse ja üldise olemuse tõttu on M. Schremsi väljendatud kahtlused seoses Ameerika Ühendriikide julgeolekuasutuste seireprogrammide rakendamisega identsed nendega, millest lähtuvalt algatas komisjon otsuse 2000/520 uuesti läbivaatamise.

60. Komisjon leiab, et kui liikmesriigi järelevalveasutused võtaksid meetmeid üksnes struktuurset ja abstraktset muret väljendavate kaebuste alusel, sekkuksid nad komisjoni pädevusse rääkida otsuse tingimused Ameerika Ühendriikidega uuesti läbi või vajaduse korral selle otsuse täitmine peatada.

61. Ma ei ole komisjoni seisukohaga nõus. Minu arvates ei saa asjaolu, et eksisteerib otsus, mille komisjon tegi direktiivi 95/46 artikli 25 lõike 6 alusel, välistada ega ka vähendada liikmesriigi järelevalveasutuse volitusi, mis tulenevad selle direktiivi artiklist 28. Vastupidi komisjoni väidetule ei takista see liikmesriigi järelevalveasutusi individuaalsete kaebuste lahendamisel minu arvates neil oma uurimisvolitustest ja sõltumatusest tulenevalt kujundada omaenda hinnagut selle kohta, milline on kolmanda riigi tagatava kaitse üldine tase, ning tegema sellest vastavaid järeldusi üksikjuhtumite lahendamisel.

62. Euroopa Kohtu väljakujunenud praktika kohaselt ei tule liidu õigusnormi tõlgendamisel arvestada mitte üksnes normi sõnastust, vaid ka konteksti ning selle õigusaktiga taotletavaid eesmärke, mille osa norm on [22].

63. Direktiivi 95/46 põhjendusest 62 ilmneb, et „liikmesriikides täiesti sõltumatult oma tööülesandeid täitvate järelevalveasutuste loomine on oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega".

64. Selle direktiivi artikli 28 lõike 1 esimeses lõigus on kirjas, et „[i]ga liikmesriik näeb ette ühe või mitu riigiasutust, et teostada järelevalvet tema territooriumil käesoleva direktiivi kohaselt vastuvõetud sätete kohaldamise üle". Nimetatud direktiivi artikli 28 lõike 1 teine lõik sätestab, et „[k]õnealused asutused tegutsevad neile usaldatud ülesannete täitmisel täiesti sõltumatult".

65. Direktiivi 95/46 artikli 28 lõikes 3 on loetletud iga järelevalveasutuse volitused, nimelt uurimisvolitused, tõhusad sekkumisvolitused, mis võimaldavad tal keelata töötlemine ajutiselt või alaliselt, ning volitused osaleda kohtumenetlustes, kui selle direktiivi kohaselt vastu võetud siseriiklikke sätteid on rikutud, või juhtida kõnealustele rikkumistele õigusasutuste tähelepanu.

66. Lisaks on direktiivi 95/46 artikli 28 lõike 4 esimeses lõigus kirjas, et „[i]ga järelevalveasutus vaatab läbi kõigi isikute […] esitatud avaldused nende õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega". Selle direktiivi artikli 28 lõike 4 teises lõigus on täpsustatud, et „[i]ga järelevalveasutus vaatab läbi eelkõige kõigi isikute avaldused kontrollida andmete töötlemise seaduslikkust, kui kohaldatakse [nimetatud] direktiivi artikli 13 kohaselt vastuvõetud siseriiklikke sätteid". Täpsustaksin, et viimane säte annab liikmesriikidele õiguse võtta seadusandlikke meetmeid, et piirata mitmete direktiivis 95/46 ette nähtud kohustuste ja õiguste ulatust, kui niisugune piirang osutub vajalikuks meetmeks, et tagada muu hulgas riigi julgeolek, riigikaitse, avalik kord ning kuritegude ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine.

67. Nagu Euroopa Kohus on juba märkinud, tuleneb nõue, et sõltumatu asutus kontrollib liidu nende eeskirjade täitmist, mis reguleerivad üksikisikute kaitset seoses isikuandmete töötlemisega, ka liidu esmasest õigusest, eelkõige Euroopa Liidu põhiõiguste harta artikli 8 lõikest 3 ja ELTL artikli 16 lõikest 2 [23]. Samuti tuletas ta meelde, et „[s]õltumatute järelevalveasutuste loomine liikmesriikides on seega oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega" [24].

68. Euroopa Kohus on veel otsustanud, et „direktiivi 95/46 artikli 28 lõike 1 teist lõiku tuleb tõlgendada nii, et järelevalveasutused, kes on pädevad teostama järelevalvet isikuandmete töötlemise üle, peavad olema sõltumatud, mis võimaldab neil täita oma ülesandeid välisele mõjule allumata. See sõltumatus välistab eelkõige igasugused ettekirjutused ja muu mis tahes vormis välise mõju, mis võib olla otsene või kaudne ning mis võib suunata nende otsuseid ja seada kahtluse alla nimetatud asutuste poolt oma ülesande täitmise, milleks on õiglase tasakaalu saavutamine eraelu puutumatuse kaitse ja isikuandmete vaba liikumise vahel". [25]

69. Euroopa Kohus on ka täpsustanud, et „[l]iikmesriikide järelevalveasutuste sõltumatuse tagatise eesmärk on tagada isikuandmete töötlemisel üksikisikute kaitset käsitlevate sätete järgimise üle teostatava kontrolli tõhusus ja usaldusväärsus". [26] See tagatis kehtestati „eesmärgiga tugevdada nende isikute ja asutuste kaitset, keda [liikmesriigi] järelevalveasutuste otsused puudutavad". [27]

22 — Vt eelkõige kohtuotsus Koushkaki (C-84/12, EU:C:2013:862, punkt 34 ja seal viidatud kohtupraktika).

23 — Vt kohtuotsused komisjon *vs*. Austria (C-614/10, EU:C:2012:631, punkt 36) ja komisjon *vs*. Ungari (C-288/12, EU:C:2014:237, punkt 47).

24 — Vt eelkõige kohtuotsus komisjon *vs*. Ungari (C-288/12, EU:C:2014:237, punkt 48 ja seal viidatud kohtupraktika). Vt selle kohta ka kohtuotsus Digital Rights Ireland jt (C-293/12 ja C-594/12, EU:C:2014:238, punkt 68 ja seal viidatud kohtupraktika).

25 — Vt eelkõige kohtuotsus komisjon *vs*. Ungari (C-288/12, EU:C:2014:237, punkt 51 ja seal viidatud kohtupraktika).

26 — Kohtuotsus komisjon *vs*. Saksamaa (C-518/07, EU:C:2010:125, punkt 25).

27 — *Idem.*

70. Nagu ilmneb muu hulgas direktiivi 95/46 põhjendusest 10 ja artiklist 1, on selle direktiivi eesmärk tagada liidus „põhiõiguste ja -vabaduste kaitse kõrge tase seoses isikuandmete töötlemisega”. [28] Euroopa Kohtu sõnul „[d]irektiivi 95/46 artiklis 28 ette nähtud järelevalveasutused on seega nimetatud õiguste ja põhivabaduste kaitsjad”. [29]

71. Võttes arvesse seda, kui tähtsat rolli mängivad liikmesriigi järelevalveasutused üksikisikute kaitsel seoses isikuandmete töötlemisega, peavad nende sekkumisvolitused jääma puutumatuks isegi siis, kui komisjon on võtnud direktiivi 95/46 artikli 25 lõike 6 alusel vastu otsuse.

72. Selles osas märgin, et miski ei viita sellele, et kolmandatesse riikidesse isikuandmete edastamise programmid oleksid välja jäetud harta artikli 8 lõike 3 esemelisest kohaldamisalast, mis liidu õigusnormide kõige kõrgemal hierarhilisel tasemel sätestab, kui tähtis on sõltumatu ametiasutuse läbiviidav isikuandmete kaitsega seotud normide täitmise kontroll.

73. Kui liikmesriigi järelevalveasutused oleksid absoluutselt seotud komisjoni tehtud otsustega, piiraks see vältimatult nende täit sõltumatust. Vastavalt nende rollile põhiõiguste kaitsjatena peavad liikmesriigi järelevalveasutused saama täiesti sõltumatult menetleda neile esitatud kaebusi, lähtudes ülekaalukast huvist kaitsta üksikisikuid seoses isikuandmete töötlemisega.

74. Lisaks, nagu Belgia valitsus ja Euroopa Parlament on kohtuistungil õigesti märkinud, puudub igasugune hierarhiline seos direktiivi 95/46 IV peatüki, mis käsitleb isikuandmete edastamist kolmandatesse riikidesse, ning VI peatüki vahel, mis käsitleb muu hulgas liikmesriikide järelevalveasutuste rolli. Miski VI peatükis ei viita sellele, et liikmesriikide järelevalveasutusi puudutavad sätted oleks mingil moel allutatud direktiivi 95/46 IV peatükis kehtestatud konktreetsetele isikuandmete edastamist käsitlevatele sätetele.

75. Vastupidi, direktiivi IV peatükis asuva artikli 25 lõikest 1 ilmneb sõnaselgelt, et isikuandmete edastamist kolmandasse riiki, kes tagab andmekaitse piisava taseme, võib lubada ainult juhul, kui nimetatud direktiivi muude sätete kohaselt vastu võetud siseriiklikest sätetest ei tulene teisiti.

76. Tuletan selle kohta meelde, et kõnesoleva sätte kohaselt peavad liikmesriigid nägema oma siseriiklikes õigusnormides ette, et töödeldavate või pärast edastamist töötlemiseks kavandatud isikuandmete edastamine kolmandatesse riikidesse võib toimuda ainult juhul, kui kõnealune kolmas riik tagab andmekaitse piisava taseme, kui direktiivi 95/46 muude sätete kohaselt vastu võetud siseriiklikest sätetest ei tulene teisiti.

77. Vastavalt kõnealuse direktiivi artikli 28 lõikele 1 on liikmesriigi järelevalveasutused kohustatud teostama järelevalvet iga liikmesriigi territooriumil liikmesriigi poolt nimetatud direktiivi kohaselt vastu võetud sätete kohaldamise üle.

78. Nende kahe sätte lähedusest võib järeldada, et direktiivi 95/46 artikli 25 lõikes 1 sätestatud eeskiri, mille kohaselt võib isikuandmete edastamine toimuda ainult juhul, kui kolmas riik, kellele andmed edastatakse, tagab andmekaitse piisava taseme, kuulub nende reeglite hulka, mille kohaldamise üle tuleb liikmesriigi järelevalveasutusel järelevalvet teostada.

79. Vastavalt harta artikli 8 lõikele 3 tuleb liikmesriigi järelevalveasutuse volitusi uurida täiesti sõltumatult talle direktiivi 95/46 artikli 28 alusel esitatud kaebusi tõlgendada laialt. Neid volitusi ei saa järelikult piirata liidu seadusandja poolt komisjonile selle direktiivi artikli 25 lõike 6 alusel antud volitused tuvastada kolmanda riigi pakutud kaitse piisav tase.

28 — *Ibidem* (punkt 22 ja seal viidatud kohtupraktika).

29 — *Ibidem* (punkt 23). Vt selle kohta ka kohtuotsused komisjon *vs.* Austria (C-614/10, EU:C:2012:631, punkt 52) ja komisjon *vs.* Ungari (C-288/12, EU:C:2014:237, punkt 53).

80. Võttes arvesse liikmesriigi järelevalveastutuste olulist rolli isikuandmete kaitsel, peavad need asutused saama uurimist läbi viia, kui neile esitatakse kaebus, milles viidatakse tõenditele, mis võiksid kahtluse alla seada kolmanda riigi tagatud kaitse taseme, sealhulgas juhul, kui komisjon on direktiivi 95/46 artikli 25 lõike 6 alusel võetud otsuses tunnistanud, et asjaomane kolmas riik tagab piisaval tasemel kaitse.

81. Kui liikmesriigi järelevalveasutus pärast uurimise läbiviimist leiab, et vaidlustatud andmete edastamine kahjustab kaitset, mis peab olema liidu kodanikele tagatud seoses oma andmete töötlemisega, on tal voli kõnealuste andmete edastamine peatada, ja seda olenemata sellest, millise üldhinnangu andis oma otsuses komisjon.

82. Nimelt on direktiivi 95/46 artikli 25 lõike 2 kohaselt selge, et kolmanda riigi pakutud kaitse taseme piisavust hinnatakse kõiki asjaolusid, nii faktilisi kui ka õiguslikke asjaolusid arvesse võttes. Kui mõni neist asjaoludest muutub ja näib seadvat kahtluse alla kolmanda riigi pakutava kaitse taseme piisavuse, peab kaebust käsitlev liikmesriigi järelevalveasutus olema võimeline tegema sellest järeldusi vaidlustatud edastamise kohta.

83. Tõepoolest, nagu Iirimaa märgib, on andmekaitsevolinik nagu iga teinegi riigiasutus seotud otsusega 2000/520. ELTL artikli 288 neljandast lõigust ilmneb nimelt, et liidu institutsiooni otsused on tervikuna siduvad. Järelikult on otsus 2000/520 kehtiv nende liikmesriikide suhtes, kellele see on adresseeritud.

84. Selles osas märgin, et otsuse 2000/520 enda artiklis 5 on sätestatud, et „[l]iikmesriigid võtavad kõik [selle] otsuse järgimiseks vajalikud meetmed hiljemalt 90 päeva möödumisel selle teatavaks tegemisest liikmesriikidele". Lisaks kinnitatakse selle otsuse artiklis 6, et „[see] otsus on adresseeritud liikmesriikidele".

85. Leian sellegipoolest, et võttes arvesse direktiivi 95/46 eespool viidatud sätteid ja harta sätteid, ei ole otsuse 2000/520 kohustuslik mõju selline, et see välistaks igasuguse andmekaitsevolinikupoolse uurimise kaebuste puhul, milles väidetakse, et selle otsuse raames Ameerika Ühendriikidesse isikuandmete edastamine ei paku vajalikke kaitsetagatisi, mida nõuab liidu õigus. Teisisõnu ei ole niisugune siduv mõju oma olemuselt selline, et see nõuaks, et iga seda tüüpi kaebus tuleks lihtsalt, see tähendab viivitamata ja põhjendatust uurimata tagasi lükata.

86. Tuleb lisada, et ka direktiivi 95/46 artikli 25 ülesehitusest ilmneb, et kolmanda riigi poolt pakutava kaitse piisava taseme võib tuvastada nii liikmesriik kui ka komisjon. Seega on tegemist jagatud pädevusega.

87. Selle direktiivi artikli 25 lõikest 6 tuleneb, et kui komisjon teeb järelduse, et kolmas riik tagab piisaval tasemel kaitse nimetatud direktiivi artikli 25 lõike 2 tähenduses, peavad liikmesriigid võtma vajalikud meetmed komisjoni otsuse täitmiseks.

88. Kuna niisuguse otsuse toimel lubatakse isikuandmete edastamisi kolmandasse riiki, mille kaitsetaset hindab komisjon piisavaks, peavad liikmesriigid seega põhimõtteliselt lubama, et nende territooriumil asuvad ettevõtjad niisuguseid edastamisi teostavad.

89. Direktiivi 95/46 artikkel 25 ei anna siiski komisjonile selles valdkonnas ainuõigust järeldada, kas edastatud isikuandmete kaitse on piisav või mitte. Nimetatud artikli ülesehitus annab tunnistust sellest, et ka liikmesriikidel on selles valdkonnas oma roll. Komisjoni otsusel on kindlasti oluline roll liikmesriikides kehtivate edastamistingimuste ühtlustamisel. Sellegipoolest saab see ühtlustamine kesta üksnes seni, kuni seda järeldust ei ole kahtluse alla seatud.

90. Kolmandasse riiki isikuandmete edastamise tingimuste ühtlustamise vajadust puudutaval argumendil on minu arvates omad piirid niisuguses olukorras nagu põhikohtuasjas käsitlusel, kus komisjon mitte ainult ei ole informeeritud sellest, et tema järeldust kritiseeritakse, vaid on ka ise kriitiline ning peab läbirääkimisi selle olukorra parandamiseks.

91. Kolmanda riigi pakutud kaitse taseme piisavuse või ebapiisavuse hindamine võib toimuda ka liikmesriikide ja komisjoni koostöös. Direktiivi 95/46 artikli 25 lõige 3 näeb selle kohta ette, et „[l]iikmesriigid ja komisjon teatavad üksteisele juhtudest, mille puhul nad leiavad, et kolmas riik ei taga kaitse piisavat taset lõike 2 tähenduses". Nagu märgib ka parlament, näitab see selgelt, et liikmesriikidel ja komisjonil on võrdne roll nende juhtumite tuvastamisel, kus kolmas riik ei taga kaitse piisavat taset.

92. Piisavusotsuse eesmärk on lubada isikuandmete edastamist asjaomasesse kolmandasse riiki. See ei tähenda, et liidu kodanikud ei tohi oma isikuandmete kaitse küsimuses enam kaebustega järelevalveasutuste poole pöörduda. Selles osas tuleb märkida, et direktiivi 95/46 artikli 28 lõike 4 esimene lõik, mille kohaselt „[i]ga järelevalveasutus vaatab läbi kõigi isikute […] avaldused nende õiguste ja vabaduste kaitse kohta seoses isikuandmete töötlemisega", ei näe ette erandit sellest põhimõttest juhuks, kui komisjon on selle direktiivi artikli 25 lõike 6 alusel juba otsuse teinud.

93. Seega, kuigi komisjoni poolt viimati nimetatud sättest tulenevate rakendusvolituste alusel tehtud otsusega lubatakse isikuandmete edastamist kolmandasse riiki, ei saa niisuguse otsuse mõju aga olla selline, et see võtab liikmesriigilt, eriti selle järelevalveasutustelt kogu pädevuse, või mis isegi lihtsalt piirab nende pädevust olukorras, kus nad uurivad väidetavat põhiõiguste rikkumist.

94. Liikmesriigi järelevalveasutus peab olema võimeline täitma direktiivi 95/46 artikli 28 lõikes 3 sätestatud volitusi, sealhulgas keelama isikuandmete töötlemise ajutiselt või alaliselt. Kuigi selles sättes välja toodud volituste loetelu ei viita sõnaselgelt volitustele seoses edastamisega liikmesriigist kolmandasse riiki, tuleb niisugust edastamist minu arvates käsitada andmetöötlusena.[30] Nagu ilmneb ka nimetatud sätte sõnastusest, ei ole see loetelu ammendav. Igal juhul, võttes arvesse liikmesriikide järelevalveasutuste olulist rolli direktiiviga 95/46 loodud süsteemis, peab neid olema õigus andmete edastamine peatada, kui põhiõiguste rikkumine on tõendatud või esineb nende rikkumise oht.

95. Lisaksin, et kui võtta niisugustel asjaludel nagu käesolevas kohtuasjas käsitlusel liikmesriigi järelevalveasutuselt uurimispädevus, läheks see vastuollu mitte ainult sõltumatuse põhimõttega, vaid ka direktiivi 95/46 eesmärgiga, mis ilmneb selle artikli 1 lõikest 1.

96. Nagu Euroopa Kohus on märkinud, „tuleneb direktiivi 95/46 põhjendustest 3, 8 ja 10, et liidu seadusandja soovis lihtsustada isikuandmete vaba liikumist, ühtlustades liikmesriikide õigusnorme, tagades samas isikute põhiõiguste, eelkõige õiguse eraelu puutumatusele kaitse ja liidus kaitstuse kõrgema taseme. Selle direktiivi artikkel 1 kohustab liikmesriike kaitsma isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusele".[31]

97. Direktiivi 95/46 sätteid tuleb seega tõlgendada vastavalt selle direktiivi eesmärgile, mis on tagada füüsliste isikute põhiõiguste, eelkõige õiguse eraelu puutumatusele kaitse kõrge tase seoses isikuandmete töötlemisega liidus.

98. Selle eesmärgi olulisus ja liikmesriikide roll selle saavutamisel tähendab, et kui konkreetsed asjaolud kolmandasse riiki isikuandmete edastamisel annavad alust hartaga tagatud põhiõiguste järgimises kahelda, ei saa liikmesriigid ja järelikult ka nende järelevalveasutused olla absoluutselt seotud komisjoni piisavusotsusega.

30 — Vt kohtujuristi ettepanek, Léger, kohtuasi parlament *vs.* nõukogu ja komisjon (C-317/04, EU:C:2005:710, punktid 92–95). Vt ka kohtuotsus parlament *vs.* nõukogu ja komisjon (C-317/04 ja C-318/04, EU:C:2006:346, punkt 56).

31 — Vt eelkõige kohtuotsus IPI (C-473/12, EU:C:2013:715, punkt 28 ja seal viidatud kohtupraktika).

99. Euroopa Kohus on juba otsustanud, et „kuivõrd direktiivi 95/46 sätted reguleerivad isikuandmete töötlemist, mis võib riivata põhivabadusi ja eriti õigust eraelu puutumatusele, tuleb nende tõlgendamisel tingimata lähtuda põhiõigustest, mis moodustavad väljakujunenud kohtupraktika kohaselt õiguse üldpõhimõtete lahutamatu osa ning mille järgimise tagab Euroopa Kohus ja mis on praegu sätestatud hartas”. [32]

100. Lisaks viitaksin kohtupraktikale, mille kohaselt „liikmesriigid mitte üksnes ei pea tõlgendama siseriiklikku õigust kooskõlas liidu õigusega, vaid nad peavad ka jälgima, et nad ei tugineks teisese õiguse tõlgendusele, mis on vastuolus liidu õiguskorras kaitstavate põhiõigustega või muude liidu õiguse üldpõhimõtetega”. [33]

101. Euroopa Kohus on sedastanud kohtuotsuses N. S. jt.[34], et „määruse [(EÜ)] nr 343/2003[35] kohaldamine, mis tugineb ümberlükkamatule eeldusele, et varjupaigataotleja taotluse läbivaatamise eest esmajärjekorras vastutavas liikmesriigis kaitstakse varjupaigataotleja põhiõigusi, ei ole vastavuses liikmesriikide kohustusega tõlgendada ja kohaldada määrust nr 343/2003 kooskõlas põhiõigustega”. [36]

102. Selle kohta on Euroopa Kohus tunnistanud, et olukorras, kus liikmesriikidel on üksteise jaoks varjupaigaõiguse õiguslike ja praktiliste küsimuste lahendamise kontekstis päritoluriigi staatus, tuleb eeldada, et igas liikmesriigis toimub varjupaigataotluste menetlemine kooskõlas harta, Genfis 28. juulil 1951 alla kirjutatud pagulasseisundi konventsiooni[37] ja Roomas 4. novembril 1950 alla kirjutatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni[38] nõuetega. Siiski on Euroopa Kohus sedastanud, et „[e]i saa aga välistada, et praktikas esineb selle süsteemi funktsioneerimisel teatud liikmesriigis suuri probleeme, mistõttu on olemas tõsine oht, et varjupaigataotlejaid koheldakse sellesse liikmesriiki saatmisel viisil, mis ei ole kooskõlas nende isikute põhiõigustega”. [39]

103. Sellest tulenevalt on Euroopa Kohus otsustanud, et „liikmesriigid, sealhulgas liikmesriikide kohtud, ei või anda varjupaigataotlejat üle „vastutavale liikmesriigile” määruse nr 343/2003 tähenduses, kui neile ei saa olla teadmata, et selles liikmesriigis varjupaigamenetluses ja varjupaigataotlejate vastuvõtutingimustes esinevad süsteemsed puudused annavad tõsist alust arvata, et varjupaigataotlejal tekib reaalne oht saada koheldud ebainimlikult ja alandavalt harta artikli 4 tähenduses”. [40]

104. Kohuotsuses N. S. jt[41] tehtud järeldusi saab minu arvates laiendada ka niisugusele olukorrale, nagu on kõne all põhikohtuasjas. Liidu teisese õiguse tõlgendamist lähtuvalt ümberlükkamatust eeldusest, et kas siis liikmesriik, komisjon või kolmas riik järgib põhiõigusi, tuleb seega käsitada nii, et see on vastuolus liikmesriikide kohustusega tõlgendada ja kohaldada liidu teisest õigust kooskõlas põhiõigustega. Direktiivi 95/46 artikli 25 lõikest 6 ei tulene seega niisugust ümberlükkamatut eeldust, et kui tegemist on komisjoni hinnanguga kolmanda riigi pakutud kaitse piisava taseme kohta, siis on põhiõigusi järgitud. Vastupidi, selles sättes nimetatud eeldust, et andmete edastamine kolmandasse riiki järgib põhiõigusi, tuleb pidada ümberlükatavaks.[42] Järelikult ei või nimetatud sätet tõlgendada nii, et sellega seatakse kahtluse alla eelkõige direktiivi 95/46 artikli 28 lõikes 3 ja harta artikli 8 lõikes 3 kehtestatud tagatised, mille eesmärk on tagada isikuandmete kaitse õiguse kaitse ja järgimine.

32 — Vt eelkõige kohtuotsus Google Spain ja Google (C-131/12, EU:C:2014:317, punkt 68 ja seal viidatud kohtupraktika).

33 — Vt eelkõige kohtuotsus N. S. jt (C-411/10 ja C-493/10, EU:C:2011:865, punkt 77 ja seal viidatud kohtupraktika).

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

35 — Nõukogu 18. veebruari 2003. aasta määrus (EÜ) nr 343/2003, millega kehtestatakse kriteeriumid ja mehhanismid selle liikmesriigi määramiseks, kes vastutab mõnes liikmesriigis kolmanda riigi kodaniku esitatud varjupaigataotluse läbivaatamise eest (ELT L 50, lk 1; ELT eriväljaanne 19/06, lk 109).

36 — Selle kohtuotsuse punkt 99.

37 — *United Nations Treaty Series*, köide 189, lk 150, nr 2545 (1954).

38 — Vt kohtuotsus N. S. jt. (C-411/10 ja C-493/10, EU:C:2011:865, punkt 80).

39 — *Ibidem* (punkt 81).

40 — *Ibidem* (punkt 94).

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

42 — Selle kohtuotsuse punkt 104.

105. Järeldan seega nimetatud kohtuotsusest, et kui on tuvastatud süsteemsete puuduste esinemine kolmanda riigi puhul, kuhu isikuandmed edastatakse, peavad liikmesriigid saama võtta vajalikke meetmeid harta artiklites 7 ja 8 tagatud õiguste kaitseks.

106. Lisaks, nagu Itaalia valitsus on oma seisukohtades märkinud, ei saa komisjoni poolt piisavusotsuse vastuvõtmisel olla niisugust mõju, mis vähendaks liidu kodanike kaitset seoses nende andmete töötlemisega kolmandasse riiki edastamisel, võrreldes nende isikute kaitse tasemega siis, kui nende andmeid töödeldakse liidus. Liikmesriigi järelevalveasutused peavad seetõttu olema võimelised sekkuma ja täitma oma volitusi seoses andmete edastamisega kolmandatesse riikidesse, mille kohta on tehtud piisavusotsus. Vastupidisel juhul oleksid liidu kodanikud kaitstud halvemini kui siis, kui nende andmeid töödeldakse liidus.

107. Asjaolu, et komisjon võttis direktiivi 95/46 artikli 25 lõike 6 alusel vastu otsuse, toob kaasa üksnes selle, et kaob üldine keeld eksportida isikuandmeid kolmandatesse riikidesse, mis tagavad direktiiviga võrreldaval tasemel kaitse. Teisisõnu ei ole küsimust selles, et luuakse erandlik erikord, mis pakub liidu kodanikele vähem kaitset võrreldes nimetatud direktiiviga liidus toimuva andmetöötluse suhtes kehtestatud üldise korraga.

108. Euroopa Kohus on kohtuotsuse Lindqvist [43] punktis 63 küll märkinud, et „[d]irektiivi 95/46 IV peatükk, kuhu kuulub artikkel 25, kehtestab erikorra". Minu arvates ei tähenda see siiski seda, et niisugune kord pakuks vähem kaitset. Vastupidi, direktiivi 95/46 artikli 1 lõikes 1 kindlaks määratud andmekaitse-eesmärgi saavutamiseks näeb selle direktiivi artikkel 25 liikmesriikidele ja komisjonile ette rea kohustusi [44] ning artikkel 25 kehtestab põhimõtte, et kui kaitse tase kolmandas riigis ei ole piisav, tuleb keelata isikuandmete edastamine sellesse riiki. [45]

109. Mis täpsemalt puudutab programmi Safe Harbor, siis näeb komisjon liikmesriikide järelevalveasutuste sekkumise ja nende poolt andmevoo peatamise ette üksnes otsuse 2000/520 artikli 3 lõike 1 punktis b piiritletud olukorras.

110. Selle otsuse põhjenduses 8 on kirjas, et „[s]elguse ja arusaadavuse huvides ning võimaldamaks liikmesriikide pädevatel ametiasutustel tagada üksikisikute kaitset neid puudutavate isikuandmete töötlemisel, tuleb käesolevas otsuses kindlaks määrata need erandlikud asjaolud, mille korral konkreetsete andmevoogude peatamine oleks põhjendatud olenemata sellest, et andmete kaitsetase on tunnistatud piisavaks".

111. Käesoleva kohtuasja raames arutati pigem selle otsuse artikli 3 lõike 1 punkti b kohaldatavuse küsimust. Selles sätte kohaselt võivad need liikmesriigi järelevalveasutused kasutada oma volitusi andmete edastamise peatamiseks, kui „on väga tõenäoline, et põhimõtteid rikutakse; on põhjust arvata, et asjakohane täitmise tagamise mehhanism ei rakenda piisavaid ja õigeaegseid meetmeid kõnealuse olukorra lahendamiseks; edastamise jätkamisel tekiks raske kahju otsene oht andmesubjektidele; ning liikmesriigi pädevad asutused on teinud selles olukorras mõistlikke pingutusi organisatsiooni teavitamiseks ja andnud võimaluse vastata".

112. Nimetatud säte kehtestab mitmed tingimused, mida pooled on käesoleva menetluse käigus erinevalt tõlgendanud. [46] Laskumata nende tõlgenduste detailidesse, on nende alusel ilmne, et need tingimused piiritlevad rangelt liikmesriikide järelevalveasutuste volitusi andmevoogu peatada.

43 — C-101/01, EU:C:2003:596.

44 — Punkt 65.

45 — Punkt 64.

46 — M. Schremsi sõnul ei ole täidetud esimene tingimus, nimelt see, et „on väga tõenäoline, et põhimõtteid rikutakse". Keegi ei väida, et Facebook USA kui enesesertifitseeritud organisatsioon, kellele andmeid edastatakse, oleks ise rikkunud Safe Harbor' põhimõtteid, kuna Ameerika Ühendriikide ametiasutused saavad massiliselt ja valimatult tutvuda nende käsutuses olevate andmetega. Nimelt on Safe Harbor' põhimõtted sõnaselgelt piiratud Ameerika Ühendriikide seadustega, mida otsuse 2000/520 I lisa neljas lõik määratleb õigus- ja haldusnormidele ning kohtupraktikale viidates.

113. Sellegipoolest, vastupidi komisjoni väidetele, tuleb otsuse 2000/520 artikli 3 lõike 1 punkti b tõlgendada vastavalt direktiivis 95/46 taotletud isikuandmete kaitse eesmärgile ning võttes arvesse harta artiklit 8. Nõue, et tõlgendus oleks kooskõlas põhiõigustega, toetab selle sätte laia tõlgendust.

114. Siit järeldub, et otsuse 2000/520 artikli 3 lõike 1 punktis b ette nähtud tingimused ei saa minu arvates takistada liikmesriigi järelevalveasutust täiesti sõltumatult täitmast volitusi, mille ta on saanud direktiivi 95/46 artikli 28 lõike 3 alusel.

115. Nagu Belgia ja Austria valitsus kohtuistungil sisuliselt märkisid, on otsuse 2000/520 artikli 3 lõike 1 punktis b sätestatud nn varuväljapääs niivõrd kitsas, et seda on raske praktikas kasutada. See eeldab kattuvaid kriteeriume ning asetab lati liiga kõrgele. Harta artikli 8 lõiget 3 arvesse võttes on võimatu, et liikmesriikide järelevalveasutuste tegutsemisruum direktiivi 95/46 artikli 28 lõikest 3 tulenevate eelduste puhul oleks piiratud sellisel moel, et nad neid enam kasutada ei saaks.

116. Selles osas on parlament põhjendatult märkinud, et see oli liidu seadusandja, kes otsustas, millised volitused tuleks liikmesriigi järelevalveasutustele anda. Liidu seadusandja poolt direktiivi 95/46 artikli 25 lõikes 6 komisjonile antud rakenduspädevus ei mõjuta sama seadusandja poolt selle direktiivi artikli 28 lõikes 3 liikmesriigi järelevalveasutusele antud volitusi. Teisisõnu puudub komisjonil pädevus piirata liikmesriigi järelevalveasutuste volitusi.

117. Järelikult, selleks et tagada füüsiliste isikute põhiõiguste asjakohane kaitse seoses isikuandmete töötlemisega, peab liikmesriigi järelevalveasutustel olema juhul, kus väidetavalt on neid õigusi rikutud, võimalik uurimist läbi viia. Kui niisuguste uurimiste järel peaksid need asutused leidma, et piisavusotsusega hõlmatud komandas riigis on tõsiseid märke liidu kodanike isikuandmete kaitse õiguse rikkumisest, peab neil olema õigus selles kolmandas riigis asuvale adressaadile andmete edastamine peatada.

118. Teisisõnu peab liikmesriigi järelevalveasutustel olema õigus viia läbi uurimisi ja vajaduse korral peatada andmete edastamine, sõltumata otsuse 2000/520 artikli 3 lõike 1 punktis b kehtestatud piiravatest tingimustest.

119. Lisaks, tulenevalt direktiivi 95/46 artikli 28 lõikes 3 ette nähtud õigusest osaleda kohtumenetluses, kui selle direktiivi alusel võetud riiklikke õigusnorme on rikutud, või õigusest juhtida õigusasutuste tähelepanu neile rikkumistele, peab liikmesriigi järelevalveasutustel – kui nad saavad teada asjaoludest, mis tõendavad, et kolmas riik ei taga kaitse piisavat taset – olema õigus pöörduda liikmesriigi kohtusse, kes omalt poolt saab vajaduse korral otsustada, kas esitada komisjoni piisavusotsuse kehtivuse hindamiseks Euroopa Kohule eelotsusetaotlus.

120. Kõigest eeltoodust järeldub, et direktiivi 95/46 artiklit 28, koostoimes harta artiklitega 7 ja 8, tuleb tõlgendada nii, et selle direktiivi artikli 25 lõike 6 alusel komisjoni poolt vastu võetud otsuse olemasolu ei saa takistada liikmesriigi järelevalveasutust menetlemast kaebust, milles väidetakse, et kolmas riik ei taga edastatud isikuandmete kaitse piisavat taset, ja vajaduse korral nende andmete edastamist peatamast.

121. Kuigi Hight Court rõhutab, et M. Schrems ei ole põhikohtuasja kaebuses ametlikult vaidlustanud ei direktiivi 95/46 ega otsuse 2000/520 kehtivust, tuleneb eelotsusetaotlusest, et M. Schremsi sõnastatud põhiline kriitika on suunatud sellele, et seada kahtluse alla järeldust, mille kohaselt programmi Safe Harbor raames tagavad Ameerika Ühendriigid edastatud andmete kaitse piisava taseme.

122. Samuti ilmneb andmekaitsevoliniku seisukohtadest, et M. Schremsi kaebus seab otsuse 2000/520 otseselt kahtluse alla. Oma kaebust esitades soovis viimane vaidlustada programmi Safe Harbor kui sellise tingimusi ja toimimist põhjusel, et Ameerika Ühendriikidesse edastatud andmete massiline seire näitab, et nende isikuandmete tegelikku kaitset ei ole selles kolmandas riigis kehtiva õiguse ja valitseva praktika alusel olemas.

123. Lisaks märgib eelotsusetaotluse esitanud kohus ise, et harta artiklis 7 sätestatud ja liikmesriikide traditsioonide ühistest väärtustest lähtuv tagatis oleks täielikult rikutud, kui riigiasutused saaksid elektroonilise sidega suvaliselt ja üldiselt tutvuda, ilma et neil oleks selleks vaja objektiivset põhjust, mis põhineks riikliku julgeoleku kaalutlustel või konkreetse asjaomase isiku või isikutega seotud kuritegevuse ennetamise vajadusel ning millega kaasneksid asjakohased ja kontrollitavad kaitsemeetmed.[47] Eelotsusetaotluse esitanud kohus väljendab seega kaudselt kahtlusi otsuse 2000/520 kehtivuses.

124. Hinnates küsimust, kas Ameerika Ühendriigid tagavad programmi Safe Harbor raames edastatud isikuandmete kaitse piisaval tasemel, kerkib vältimatult üles ka kõnealuse otsuse kehtivuse teema.

125. Selles osas tuleb märkida, et ELTL artiklis 267 kehtestatud Euroopa Kohtu ja liikmesriilkide vahelise koostöö instrumendi raames võib Euroopa Kohus – isegi kui talle esitatud eelotsusetaotlus puudutab ainult liidu õiguse tõlgendamise küsimust – teatavatel asjaoludel pidada vajalikuks käsitleda teisese õiguse sätete kehtivust.

126. Seetõttu on Euroopa Kohus mitmel korral omal algatusel kuulutanud kehtetuks akti, mida tal paluti üksnes tõlgendada.[48] Euroopa Kohus on ka sedastanud, et „kui näib, et siseriikliku kohtu esitatud küsimuste tõeline eesmärk viitab pigem [liidu] aktide kehtivuse hindamisele kui tõlgendamisele, siis on Euroopa Kohtu ülesanne nimetatud kohut oma arvamusest teavitada, sundimata teda aeganõudvateks formaalsusteks, mis oleks vastuolus [ELTL artiklis 267] kehtestatud mehhanismide olemusega".[49] Euroopa Kohus on lisaks juba sedastanud, et eelotsusetaotluse esitanud kohtu väljendatud kahtlusi teisese õiguse akti kokkusobivusest põhiõiguste kaitse normidega tuleb mõista nii, et nendega seatakse kahtluse alla selle akti kehtivus liidu õiguse suhtes.[50]

127. Tuletaksin veel meelde, et Euroopa Kohtu praktikast tuleneb, et liidu institutsioonide, organite ja asutuste aktide õiguspärasust eeldatakse, mis tähendab, et need loovad õiguslikke tagajärgi seni, kuni neid ei ole tagasi võetud, kui neid ei ole tühistamishagi menetlemise tulemusena tühistatud või eelotsusemenetluses või õigusvastasuse tõttu kehtetuks tunnistatud. Euroopa Kohus on ainsana pädev tuvastama liidu õigusakti kehtetust – pädevus, mille eesmärk on tagada õiguskindlus seeläbi, et tagatakse liidu õiguse ühetaoline kohaldamine. Kui komisjon ei ole otsust kehtetuks tunnistanud, seda muutnud või tühistanud, muutub see kogu ulatuses siduvaks ja kõikides liikmesriikides vahetult kohaldatavaks.[51]

128. Eelotsusetaotluse esitanud kohtule tervikliku vastuse andmiseks ja kõrvaldamaks käesoleva menetluse käigus väljendatud kahtlusi otsuse 2000/520 kehtivuse suhtes, olen arvamusel, et Euroopa Kohus peaks selle otsuse kehtivust hindama.

47 — Eelotsusetaotluse punkt 24.

48 — Vt eelkõige kohtuotsused Strehl (62/76, EU:C:1977:18, punktid 10–17); Roquette Frères (145/79, EU:C:1980:234, punkt 6) ning Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, punktid 32–39).

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

50 — Vt kohtuotsus Hauer (44/79, EU:C:1979:290, punkt 16).

51 — Vt eelkõige kohtuotsus CIVAD (C-533/10, EU:C:2012:347, punktid 39–41 ja seal viidatud kohtupraktika).

129. Seetõttu on oluline ka täpsustada, et selle hindamine, kas otsus 2000/520 on kehtiv või mitte, peab piirduma käesoleva menetluse raames toimunud vaidluse esemeks olevate väidetega. Nimelt ei ole kõiki Safe Harbor' programmi toimimise aspekte selle raames arutatud, mistõttu ma ei pea siinkohal võimalikuks ammendavalt süveneda selle programmi puudustesse.

130. Seevastu küsimus, kas see, et Ameerika Ühendriikide luureteenistused saavad edastatud andmetega üldiselt ja suvaliselt tutvuda, võib mõjutada otsuse 2000/520 õiguspärasust, oli käesoleva menetluse raames Euroopa Kohtus arutlusel. Selle otsuse kehtivust võib järelikult selle nurga alt hinnata.

B. *Otsuse 2000/520 kehtivus*

1. Tegurid, mida otsuse 2000/520 kehtivuse hindamisel tuleb arvese võtta

131. Tasub meeles pidada kohtupraktikat, mille kohaselt „tühistamishagi raames tuleb õigusakti seaduslikkust hinnata õigusakti vastuvõtmise ajal esinenud faktilisi ja õiguslikke asjaolusid silmas pidades, kuna komisjoni hinnangut saab kritiseerida vaid siis, kui näib, et ta on ilmselgelt eksinud nende asjaolude suhtes, mis tal kõnealuse õigusnormi vastuvõtmise ajal teada olid". [52]

132. Kohtuotsuses Gaz de France – Berliner Investissement [53] tuletas Euroopa Kohus meelde põhimõtet, et „Euroopa Kohtu poolt eelotsusetaotluse menetluses õigusakti kehtivusele hinnangu andmisel tuleb tavaliselt lähtuda selle akti vastuvõtmise ajal valitsenud olukorrast". [54] Sellegipoolest näib ta tunnistavat, et „õigusakti kehtivust võib teatud juhtudel hinnata uusi, pärast selle vastuvõtmist saabunud asjaolusid arvestades". [55]

133. Niisugune Euroopa Kohtu poolt rõhutatud avatud lähenemine näib mulle käesolevas asjas eriti asjakohasena.

134. Nimelt on komisjoni poolt direktiivi 95/46 artikli 25 lõike 6 alusel vastu võetud otsused erilised. Need on tehtud selleks, et hinnata, kas kolmanda riigi pakutud isikuandmete kaitse tase on piisav või mitte. Tegemist on hinnanguga, mis kindlasti varieerub vastavalt kolmandas riigis valitsevale faktilisele ja õiguslikule kontekstile.

135. Võttes arvesse asjaolu, et piisavusotsuse puhul on tegemist eriliigilise otsusega, tuleb käesolevas asjas täpsustada reeglit, mille kohaselt selle otsuse kehtivust saab hinnata üksnes selle otsuse vastuvõtmise ajal esinenud asjaolusid arvestades. Muidu võib niisugune reegel kaasa tuua olukorra, kus Euroopa Kohus ei saa aastaid pärast piisavusotsuse vastuvõtmist selle kehtivust hinnates võtta arvesse hiljem toimunud sündmusi, kuigi kehtivuse hindamiseks eelotsusetaotluse esitamine ei ole ajaliselt kuidagi piiratud ja selle algatamine võib eelkõige lähtuda hilisematest asjaoludest, mis viitavad kõnealuse akti ebapiisavusele.

52 — Vt eelkõige kohtuotsus BVGD *vs.* komisjon (T-104/07 ja T-339/08, EU:T:2013:366, punkt 291), mis viitab kohtuotsusele IECC *vs.* komisjon (C-449/98 P, EU:C:2001:275, punkt 87).

53 — C-247/08, EU:C:2009:600.

54 — Punkt 49 ja seal viidatud kohtupraktika.

55 — Punkt 50 ja seal viidatud kohtupraktika. Vt selle kohta Lenaerts, K., Maselis, I., ja Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, kus selgitatakse, et „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" (punkt 10.16, lk 471).

136. Käesoleval juhul annab asjaolu, et otsus 2000/520 on olnud jätkuvalt jõus ligi 15 aastat, tunnistust sellest, et komisjon oma 2000. aastal antud hinnangut vaikimisi kinnitab. Juhul kui eelotsusetaotluse raames palutakse Euroopa Kohtul hinnata komisjoni ajas muutumatuna püsinud hinnangu kehtivust, on seetõttu mitte ainult võimalik, vaid ka asjakohane, et ta saaks vastandada nimetatud hinnangut uutele asjaoludele, mis on piisavusotsuse vastuvõtmisest alates esile kerkinud.

137. Piisavusotsuse eripära arvesse võttes peab komisjon selle regulaarselt üle vaatama. Kui komisjon vahepeal esile kerkinud asjaolude järel oma otsust ei muuda, kinnitab ta seega vaikimisi, kuid kindlalt oma esialgset hinnangut. Komisjon kinnitab seega oma järeldust, mille kohaselt asjaomane kolmas riik tagab edastatud isikuandmete kaitse piisava taseme. Euroopa Kohtu ülesanne on uurida, kas see järeldus on jätkuvalt kehtiv, vaatamata hiljem esile kerkinud asjaoludele.

138. Selleks et tagada seda tüüpi otsuse tõhus kohtulik kontroll, tuleb minu arvates selle kehtivuse hindamisel pidada silmas praegust faktilist ja õiguslikku konteksti.

2. Mõiste „kaitse piisav tase”

139. Direktiivi 95/46 artikkel 25 tugineb tervikuna põhimõttel, mille kohaselt isikuandmete edastamine kolmandasse riiki võib toimuda ainult juhul, kui kõnealune kolmas riik tagab nende andmete kaitse piisava taseme. Selle artikli eesmärk on niisiis tagada selle direktiiviga kehtestatud järjepidev kaitse, kui isikuandmeid edastatakse kolmandasse riiki. Selles osas tuleb meeles pidada, et nimetatud direktiiv pakub liidu kodanikele kõrgetasemelist kaitset seoses nende isikuandmete töötlemisega.

140. Võttes arvesse, kui oluline roll on isikuandmete kaitsel seoses eraelu austamise põhiõigusega, peab niisugune kõrgetasemeline kaitse olema tagatud ka juhul, kui isikuandmed edastatakse kolmandasse riiki.

141. Seetõttu leian, et komisjon võib direktiivi 95/46 artikli 26 lõike 6 alusel teha järelduse, et kolmas riik tagab kaitse piisava taseme, üksnes siis, kui pärast kõnealuse kolmanda riigi kehtiva õiguse ja valitseva praktika kogumina hindamist on komisjon võimeline kinnitama, et see kolmas riik pakub kaitset, mis on sisuliselt samal tasemel kui selles direktiivis pakutu, isegi kui selle kaitse üksikasjad võivad erineda sellest, mis on liidus tavapäraselt kasutusel.

142. Kuigi ingliskeelset mõistet „adequate” võib lingvistilisest vaatenurgast käsitada kui viidet kaitsetasemele, mis on lihtsalt rahuldav või piisav, ning millel seega on prantsuskeelsest mõistest „adéquat” erinev semantiline ulatus, tuleb märkida, et ainus kriteerium, millest tuleb selle mõiste tõlgendamisel juhinduda, on eesmärk saavutada põhiõiguste kõrgetasemeline kaitse, nagu nõuab direktiiv 95/46.

143. Kolmanda riigi pakutud kaitse taseme hindamine peab keskenduma kahele põhielemendile, nimelt kohaldatavate eeskirjade sisule ja nende eeskirjade täitmise tagamise vahenditele.[56]

144. Olen seisukohal, et saavutamaks kaitsetaset, mis sisuliselt võrduks sellega, mis kehtib liidus, peaks programmiga Safe Harbor, mis suures osas tugineb selles programmis vabatahtlikult osalevate ettevõtjate enesesertifitseerimisel ja -hindamisel, kaasnema piisavad tagatised ja piisav järelevalvemehhanism. Seega ei tohiks isikuandmete edastamine kolmandasse riiki saada nõrgema kaitse osaliseks kui liidusiseselt toimuvad edastused.

56 — Vt komisjoni töödokument WP 12, pealkirjaga „Isikuandmete edastamine kolmandatesse riikidesse: andmekaitsedirektiivi artiklid 25 ja 26”, mille töörühm üksikisikute kaitseks seoses isikuandmete töötlemisega võttis vastu 24. juulil 1998, punkt 5.

145. Selles osas märgiksin alustuseks, et liidus valitseb arusaam, et sõltumatu asutuse kujul toimiv väliskontrolli mehhanism on kogu süsteemi jaoks vajalik element, mis peab tagama isikuandmete kaitse reeglite järgimise.

146. Lisaks, tagamaks direktiivi 95/46 artikli 25 lõigete 1–3 kasulik mõju, tuleb arvesse võtta asjaolu, et kolmanda riigi pakutud kaitse taseme piisavus on arenev olukord, mis võib mitmetest teguritest sõltuvalt aja jooksul muutuda. Liikmesriigid ja komisjon peavad seega olema pidevalt valvsad asjaolude muutumise suhtes, mis võib tingida vajaduse kolmanda riigi pakutud kaitse taseme piisavus üle vaadata. Selle kaitse taseme piisavuse hindamist ei saa mingil juhul kinnitada kindla ajahetke seisuga ja igavesti selle juurde jääda, olenemata asjaolude mis tahes muutumisest, millest ilmneb, et tegelikkuses see pakutud kaitse tase ei ole enam piisav.

147. Kolmanda riigi kohustus tagada kaitse piisav tase on seega kestev kohustus. Kuigi hindamine viiakse läbi konkreetsel ajahetkel, eeldab piisavusotsuse jõusse jätmine seda, et ükski sellest ajast alates esile kerkinud asjaolu ei oleks selline, mis võiks komisjoni esialgse hinnangu kahtluse alla seada.

148. Nimelt ei tohi unustada, et direktiivi 95/46 artikli 25 eesmärk on alati vältida seda, et isikuandmed edastatakse kolmandasse riiki, mis ei taga kaitse piisavat taset, rikkudes harta artiklis 8 tagatud põhiõigust isikuandmete kaitsele.

149. Oluline on rõhutada, et liidu seadusandja poolt komisjonile direktiivi 95/46 artikli 25 lõikes 6 antud volitus tuvastada, et kolmas riik tagab kaitse piisava taseme, sõltub sõnaselgelt nõudest, et see kolmas riik tagab kaitse piisava taseme selle artikli lõike 2 tähenduses. Kui uued asjaolud seavad komisjoni esialgse hinnangu kahtluse alla, peab viimane oma otsuse vastavalt ajakohastama.

3. Kohtujuristi hinnang

150. Tuletan meelde, et direktiivi 95/46 artikli 25 lõige 6 sätestab, et „[k]omisjon võib leida artikli 31 lõikes 2 sätestatud korras, et kolmas riik tagab kaitse piisava taseme käesoleva artikli lõike 2 tähenduses oma siseriikliku õigusega või endale võetud rahvusvaheliste kohustustega, mis tulenevad eelkõige lõikes 5 osutatud läbirääkimistest, et kaitsta eraelu puutumatust ja üksikisikute põhivabadusi ja -õigusi". Koostoimes selle direktiivi artikli 25 lõikega 2 tähendab selle direktiivi artikli 25 lõige 6 seda, et tuvastamaks, et kolmas riik tagab kaitse piisava taseme, peab komisjon kogumis hindama kõiki selles riigis kehtivaid õigusnorme ning nende kohaldamist.

151. Oleme näinud, et komisjoni poolt otsuse 2000/520 jõusse jätmist, vaatamata uute faktiliste ja õguslike tegurite ilmnemisele, tuleb vaadelda tema soovina kinnitada oma esialgset hinnangut.

152. Euroopa Kohtu ülesanne ei ole eelotsusetaotluse raames hinnata selle vaidluse asjaolusid, mis viisid liikmesriigi kohtu selle taotluse esitamiseni.[57]

153. Seetõttu tuginen eelotsusetaotluse esitanud kohtu poolt eelotsusetaotluses nimetatud asjaoludele, mille tõendatust komisjon on ise suures osas tunnistanud.[58]

154. Üksikasju, mis Euroopa Kohtule esitati, vaidlustamaks komisjoni hinnagut, mille kohaselt programm Safe Harbor tagab liidust Ameerika Ühendriikidesse edastatud isikuandmete kaitse piisava taseme, võib kirjeldada nii.

57 — Vt eelkõige kohtuotsus Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, punkt 22 ja seal viidatud kohtupraktika).

58 — Vt komisjoni teatist, millele viidatakse joonealuses märkuses nr 2, ja komisjoni teatis Euroopa Parlamendile ja nõukogule, mis käsitleb programmi Safe Harbor toimimist ELi kodanike ja ELis asutatud äriühingute seisukohast (COM(2013) 847 final).

155. Oma eelotsusetaotluses lähtub selle esitanud kohus järgnevast kahest faktilisest järeldusest. Esiteks, niisuguse ettevõtja nagu Facebook Ireland poolt oma Ameerika Ühendriikides asuvale emaettevõtjale edastatud isikuandmetega võivad NSA ja teised Ameerika Ühendriikide julgeolekuasutused seejärel massilise ja suvalise seire ja infopüügi käigus tutvuda. Nimelt pärast E. Snowdeni paljastusi ei olegi olemasolevate tõendite põhjal võimalik teha mingisugust muud järeldust. [59] Teiseks ei ole ELi kodanikel NSA ja teiste Ameerika Ühendriikide julgeolekuasutuste poolt oma andmete seire ja infopüügi küsimuses sisuliselt mingit õigust olla ära kuulatud. [60]

156. High Courti faktilisi järeldusi toetavad komisjoni enda avaldused.

157. Oma eespool viidatud teatises, mis käsitleb programmi Safe Harbor toimimist liidu kodanike ja liidu territooriumil asutatud äriühingute seisukohast, lähtub komisjon järeldusest, et Ameerika Ühendriikide seireprogrammide ulatust ja suurust käsitlev teave on 2013. aasta jooksul tekitanud küsimusi seoses programmi Safe Harbor raames Ameerika Ühendriikidesse seaduslikult edastatud isikuandmete kaitse järjepidevusega. Komisjon märkis, et kõik programmis PRISM osalevad äriühingud, kes annavad Ameerika Ühendriikide ametiasutustele juurdepääsu salvestatud ja töödeldud andmetele, tunduvad olevat programmi Safe Harbor raames sertifitseeritud. Komisjoni sõnul on see teinud programmist Safe Harbor ühe kanali, mille kaudu on Ameerika Ühendriikide luureasutustel juurdepääs algselt ELis töödeldud isikuandmete kogumisele. [61]

158. Nendest asjaoludest nähtub, et Ameerika Ühendriikide kehtiv õigus ja valitsev praktika võimaldavad laiaulatuslikult koguda programmi Safe Harbor raames edastatud liidu kodanike isikuandmeid, ilma et viimastel oleks võimalus kasutada tõhusat õiguskaitsevahendit.

159. Need faktilised järeldused näitavad minu arvates seda, et otsus 2000/520 ei sisalda piisavalt tagatisi. Nende tagatiste puudumise tõttu rakendati seda otsust viisil, mis ei vasta harta ja ka direktiivi 95/46 nõuetele.

160. Komisjoni poolt direktiivi 95/46 artikli 25 lõike 6 alusel vastu võetud otsuse eesmärk on tuvastada, et kolmas riik „tagab" kaitse piisava taseme. Sõna „tagab", mida pööratakse olevikus, tähendab seda, et kehtivuse säilitamiseks peab niisugune otsus puudutama riiki, mis pärast nimetatud otsuse vastuvõtmist jätkuvalt tagab kaitse piisava taseme.

161. Avaldused NSA tegevuse kohta, kes kasutab programmi Safe Harbor raames edastatud andmeid, heidavad valgust otsuse 2000/520 kui õigusliku aluse puudustele.

162. Käesoleva menetluse käigus esile toodud puudused esinevad eelkõige selle otsuse I lisa neljandas lõigus.

163. Tuletaksin meelde, et selle sätte kohaselt „[programmi Safe Harbor] põhimõtete järgimist võib piirata: a) riikliku julgeoleku, avaliku huvi või õiguskaitseliste vajaduste täitmiseks vajalikus ulatuses; b) statuudi, valitsuse määruse või pretsedendiõigusega, mis loovad vasturääkivaid kohustusi või annavad otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon demonstreerida, et põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks".

164. Põhiliselt tekib probleem sellest, et Ameerika Ühendriikide ametiasutused kasutavad selles sättes ette nähtud erandeid. Liiga üldise sõnastuse tõttu ei piirdu Ameerika Ühendriikide ametiasutused nende erandite rakendamisel rangelt vajalikuga.

59 — Eelotsusetaotluse punkti 7 alapunkt c.

60 — Eelotsusetaotluse punkti 7 alapunkt b.

61 — Komisjoni teatise lk 19.

165. Sellele liiga üldisele sõnastusele lisandub asjaolu, et liidu kodanikel puuduvad asjakohased õiguskaitsevahendid oma isikuandmete töötlemise vaidlustamiseks, kui see toimub muudel eesmärkidel kui need, milleks neid algselt koguti ja seejärel Ameerika Ühendriikidesse edastati.

166. Otsuses 2000/520 ette nähtud eranditega programmi Safe Harbor põhimõtete kohaldamisest, eelkõige riikliku julgeoleku kaalutlustel, oleks pidanud kaasnema ka sõltumatu järelevalvemehhanismi loomine, mis oleks tuvastatud eraelu austamise õiguse rikkumiste kõrvaldamiseks sobiv.

167. Seega, paljastused, mis puudutavad Ameerika Ühendriikide luureasutuste tegevust seoses programmi Safe Harbor raames edastatud andmete üldise seirega, heidavad valgust teatavatele otsuse 2000/520 puudustele.

168. Käesoleva menetluse raames tehtud väited ei vii järelduseni, et Facebook rikub programmi Safe Harbor põhimõtteid. Kui niisugune sertifitseeritud ettevõtja nagu Facebook USA võimaldab Ameerika Ühendriikide ametiasutustel tutvuda andmetega, mis on talle edastatud mõnest liikmesriigist, siis võib seda käsitada nii, et ta teeb seda Ameerika Ühendriikide õigusnormide täitmiseks. Võttes arvesse asjaolu, et niisugune olukord on otsuses 2000/520 sõnaselgelt lubatud seal sisalduvate erandite laia sõnastuse tõttu, on käesoleva kohtuasja raames tegelikult tõstatatud küsimus, kas niisugused erandid on kooskõlas liidu esmase õigusega.

169. Selles osas tuleb rõhutada, et Euroopa Kohtu väljakujunenud praktikast ilmneb, et inimõiguste austamine on üks liidu õigusaktide seaduslikkuse tingimustest ja et liidus ei ole lubatud meetmed, mis oleks inimõiguste austamisega vastuolus.[62]

170. Lisaks tuleneb Euroopa Kohtu praktikast, et kogutud isikuandmete edastamine kolmandale isikule – kas avalik- või eraõiguslikule – riivab asjassepuutuvate isikute õigust eraelu puutumatusele „hoolimata sellest, milleks edastatud teavet edaspidi kasutatakse".[63] Lisaks on Euroopa Kohus kohtuotsuses Digital Rights Ireland jt[64] kinnitanud, et pädevate siseriiklike asutuste juurdepääs andmetele kujutab endast täiendavat põhiõiguse riivet.[65] Lisaks on igasugune isikuandmete töötlemine hõlmatud harta artikliga 8 ning riivab õigust niisuguste andmete kaitsele.[66] Ameerika Ühendriikide luureteenistuste võimalus edastatud andmetega tutvuda riivab seega samuti põhiõigust isikuandmete kaitsele, mis on tagatud harta artikliga 8, kuna niisugune andmetega tutvumine kujutab endast nende andmete töötlemist.

171. Nagu Euroopa Kohus on nimetatud otsuses nentinud, on niisugune riive laiaulatuslik ning seetõttu tuleb seda käsitada eriti raske riivena, võttes arvesse asjassepuutuvate kasutajate suurt arvu ja edastatud andmete hulka. Need tegurid, millele lisandub salastatus seoses Ameerika Ühendriikide ametiasutuste tegevusega Ameerika Ühendriikides asuvatele ettevõtjatele edastatud isikuandmetega tutvumisel, muudavad riive eriti tõsiseks.

172. Siia lisandub veel asjaolu, et liidu kodanikud, kes kasutavad Facebooki, ei ole teadlikud asjaolust, et Ameerika Ühendriikide julgeolekuasutused võivad nende isikuandmetega üldisel viisil tutvuda.

62 — Vt eelkõige kohtuotsus Kadi ja Al Barakaat International Foundation *vs.* nõukogu ja komisjon (C-402/05 P ja C-415/05 P, EU:C:2008:461, punkt 284 ja seal viidatud kohtupraktika).

63 — Kohtuotsus Österreichischer Rundfunk jt (C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, punkt 74).

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

65 — Punkt 35.

66 — Punkt 36.

173. Samuti tuleb toonitada asjaolu, et eelotsusetaotluse esitanud kohus tuvastas, et Ameerika Ühendriikides ei ole liidu kodanikel mingit tegelikku õigust olla ära kuulatud oma andmete seire ja infopüügi küsimuses. FISC teostab järelevalvet, kuid tema menetlused on salastatud ega ole oma laadilt võistlevad.[67] Leian, et siin on tegemist riivega, mis puudutab liidu kodanike õigust tõhusale õiguskaitsevahendile, mis on kaitstud harta artikliga 47.

174. Harta artiklitega 7, 8 ja 47 kaitstud põhiõiguste riive, mida võimaldavad otsuse 2000/520 I lisa neljandas lõigus sätestatud erandid programmi Safe Harbor põhimõtetest, on seega tuvastatud.

175. Nüüd on vaja uurida, kas see riive on õigustatud või mitte.

176. Vastavalt harta artikli 52 lõikele 1 peavad kõik hartaga tunnustatud õiguste ja vabaduste teostamise piirangud olema ette nähtud seaduses ning arvestama nimetatud õiguste ja vabaduste olemust. Proportsionaalsuse põhimõtet austades tohib nimetatud õigustele ja vabadustele piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.

177. Arvestades selliselt kehtestatud tingimusi, mis hartaga kaitstud õiguste ja vabaduste teostamisele piirangute seadmiseks tuleb täita, on minu arvates sügavalt kaheldav, et käsolevas kohtuasjas käsitletavad piirangud võiksid olla vastavuses harta artiklite 7 ja 8 põhisisuga. Nimelt näib Ameerika Ühendriikide luureteenistuste õigus edastatud andmetega tutvuda laienevat ka elektroonilise side sisule, mis kahjustab eraelu austamise põhiõiguse ja muude harta artikliga 7 tagatud õiguste olemust. Lisaks, kuivõrd otsuse 2000/520 I lisa neljandas lõigus ette nähtud erandite lai sõnastus võimaldab potentsiaalselt jätta kohaldamata kõik programmi Safe Harbor põhimõtted, siis võib järeldada, et need piirangud kahjustavad isikuandmete kaitse põhiõiguse olemust.[68]

178. Mis puudutab küsimust, kas tuvastatud riive vastab üldist huvi pakkuvatele eesmärkidele, siis tuletaksin esmalt meelde, et otsuse 2000/520 I lisa neljanda lõigu punkti b kohaselt võib programmi Safe Harbor põhimõtete järgimist piirata „statuudi, valitsuse määruse või pretsedendiõigusega, mis loovad vasturääkivaid kohustusi või annavad otseseid volitusi, tingimusel et selliste volituste kasutamisel suudab organisatsioon tõendada, et põhimõtete mittejärgimine tema poolt piirdub ulatusega, mis on vajalik selliste volitustega seotud ülekaaluka õigustatud huvi järgimiseks".

179. Oluline on märkida, et „õigustatud huvi", millele selles sättes viidatakse, ei ole täpsustatud. See tekitab ebakindlust kõnealuse erandi – potentsiaalselt väga laia – kohaldamisala osas, kui seda kohaldatakse programmi Safe Harbor põhimõtetele nende ettevõtjate poolt, kes on nende põhimõtete järgimist kinnitanud.

180. Seda muljet kinnitab ka otsuse 2000/520 IV lisa jaotises B „Otsesed õiguslikud volitused" sisalduvate selgituste sõnastus, eriti kinnitus, mille kohaselt „[s]elge on, et kui Ameerika Ühendriikide seadustes sätestatakse vastandlik kohustus, peavad Ameerika Ühendriikide organisatsioonid, sõltumata sellest, kas nad osalevad programmis Safe Harbor või mitte, seadust täitma". Lisaks, mis puutub otsestesse volitustesse, „siis kui programmi Safe Harbor põhimõtete eesmärgiks on ületada erinevusi Ameerika Ühendriikide ja Euroopa eraelu puutumatuse kaitse viiside vahel, peame meie austama meie valitud seadusandjate seadusandlikke prerogatiive".

181. Minu arvates järeldub sellest, et see erand on vastuolus harta artiklitega 7, 8 ja artikli 52 lõikega 1, kuna see ei vasta üldist huvi pakkuvatele eesmärkidele, mis on piisavalt selgelt määratletud.

67 — Eelotsusetaotluse punkti 7 alapunkt b.

68 — Vt selle kohta kohtuotsus Digital Rights Ireland jt (C-293/12 ja C-594/12, EU:C:2014:238, punktid 39 ja 40).

182. Igal juhul ei sobi pinnapealsus ja üldsõnalisus, millega otsus 2000/520 näeb ise oma I lisa neljanda lõigu punktis b ja IV lisa jaotises B ette, et programmi Safe Harbor põhimõtted võib jätta kohaldamata Ameerika Ühendriikide õigusnormide puhul, kokku tingimusega, et erandid isikuandmete kaitse eeskirjadest peavad piirduma rangelt vajalikuga. Tõepoolest on mainitud vajalikkuse tingimust, kuid peale selle, et selle tingimuse täitmise tõendamine on pandud asjaomase ettevõtja kohustuseks, ei mõista ma, kuidas niisugune ettevõtja võiks hoiduda kohustusest eirata programmi Safe Harbor põhimõtteid, mis tuleneb selle õiguse normidest, mida ta peab kohaldama.

183. Seetõttu olen arvamusel, et otsus 2000/520 tuleb tunnistada kehtetuks, kuna niisuguse erandi olemasolu, mis sedavõrd üldises ja ebatäpses sõnastuses võimaldab eirata programmi Safe Harbor põhimõtteid, ei lase iseenesest teha järeldust, et see programm tagab liidust Ameerika Ühendriikidesse edastatud isikuandmete kaitse piisava taseme.

184. Mis nüüd puudutab otsuse 2000/520 I lisa neljanda lõigu punktis a ette nähtud esimese kategooria piiranguid riikliku julgeoleku, avaliku huvi või Ameerika Ühendriikide õiguskaitseliste vajaduste täitmiseks, siis näib mulle, et üksnes esimene eesmärk on piisavalt täpne, et seda saaks käsitada liidu poolt tunnustatud üldist huvi pakkuva eesmärgina harta artikli 52 lõike 1 tähenduses.

185. Nüüd tuleb hinnata tuvastatud riive proportsionaalsust.

186. Seoses sellega on sobilik meenutada, et vastavalt Euroopa Kohtu väljakujunenud praktikale „nõuab proportsionaalsuse põhimõte, et liidu institutsioonide aktid oleksid vastava õigusaktiga taotletavate õiguspäraste eesmärkide saavutamiseks sobivad ega läheks kaugemale sellest, mis on nende eesmärkide saavutamiseks sobiv ja vajalik”.[69]

187. Nende tingimuste täitmise kohtuliku kontrolli kohta olgu märgitud, et „kui tegemist on põhiõiguste riivega, siis võib liidu seadusandja kaalutlusõigus olla piiratud sõltuvalt reast teguritest, mille hulka kuuluvad asjassepuutuv valdkond, hartaga tagatud õiguse olemus, riive laad ja raskus ning riive eesmärk”.[70]

188. Olen arvamusel, et otsused, mille komisjon võtab vastu direktiivi 95/46 artikli 25 lõike 6 alusel, alluvad täielikult Euroopa Kohtu kontrollile, kui tuleb tuvastada, kas kõnealune institutsioon on proportsionaalselt hinnanud seda, kas teatavas kolmandas riigis pakutava kaitse tase on piisav, tulenevalt „oma siseriiklikust õigusest või endale võetud rahvusvahelistest kohustustest”.

189. Sellega seoses tuleb märkida, et kohtuotsuses Digital Rights Ireland jt[71] on Euroopa Kohus sedastanud, et „võttes arvesse ühelt poolt seda, kui oluline roll on isikuandmete kaitsel seoses põhiõigusega eraelu puutumatusele, ja teiselt poolt seda, kui ulatuslikult ja raskelt [kõnealune] direktiiv seda õigust riivab, on liidu seadusandja kaalutlusõigust vähendatud, mistõttu peab kontroll olema range”.[72]

190. Niisugune riive peab olema sobiv vahend kõnealuse liidu aktiga taotletud eesmärgi saavutamiseks ja selle eesmärgi saavutamiseks vajalik.

191. Sellega seoses, „mis puudutab õigust eraelu puutumatusele, siis Euroopa Kohtu väljakujunenud praktika kohaselt nõuab selle põhiõiguse kaitse, et isikuandmete kaitse erandite ja piirangute puhul tuleb piirduda rangelt vajalikuga”.[73]

69 — Kohtuotsus Digital Rights Ireland jt. (C-293/12 ja C-594/12, EU:C:2014:238, punkt 46 ja seal viidatud kohtupraktika).

70 — *Ibidem* (punkt 47 ja seal viidatud kohtupraktika).

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

72 — Punkt 48.

73 — Kohtuotsus Digital Rights Ireland jt (C-293/12, EU:C:2014:238, punkt 52 ja seal viidatud kohtupraktika).

192. Oma kontrolli teostades võtab Euroopa Kohus arvesse ka asjaolu, et „isikuandmete kaitse, milleks harta artikli 8 lõige 1 sõnaselgelt kohustab, on harta artiklis 7 ette nähtud eraelu puutumatuse õiguse jaoks eriti tähtis”.[74]

193. Euroopa Kohtu sõnul, kes selles osas tugineb Euroopa Inimõiguste Kohtu praktikale, „peab kõnesolev liidu õigusakt sätestama selged ja täpsed reeglid meetme ulatuse ja kohaldamise kohta ning kehtestama miinimumnõuded, nii et isikutel, kelle andmeid säilitatakse, oleksid piisavad garantiid, mis võimaldavad tõhusalt kaitsta nende isikuandmeid kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest”[75]. Euroopa Kohus märgib, et „niisuguste garantiide olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt […] ja kui esineb suur oht, et nende andmetega võidakse tutvuda ebaseaduslikult”.[76]

194. Minu arvates esineb otsuse 2000/520 I lisa neljanda lõigu punkti a ja direktiivi 95/46 artikli 13 lõike 1 vahel analoogia. Esimeses sättes on märgitud, et programmi Safe Harbor põhimõtete järgimist võib piirata „riikliku julgeoleku, avaliku huvi või Ameerika Ühendriikide õiguskaitseliste vajaduste täitmiseks”. Teises sättes on nähtud ette, et liikmesriigid võivad artikli 6 lõikes 1, artiklis 10, artikli 11 lõikes 1 ja artiklites 12 ja 21 sätestatud kohustuste ja õiguste ulatuse piiramiseks võtta vastu õigusakte, kui sellised piirangud on vajalikud, et kindlustada muu hulgas riigi julgeolek, riigikaitse, avalik kord ning kuritegude ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine.

195. Nagu Euroopa Kohus on märkinud oma kohtuotsuses IPI[77], tuleneb direktiivi 95/46 artikli 13 lõike 1 sõnastusest, et liikmesriigid võivad selles sättes viidatud meetmeid ette näha vaid siis, kui need on vajalikud. Meetmete „vajalikkuse” tingimus on liikmesriikidele selles sättes antud õiguse eeltingimus.[78] Liidus isikuandmete töötlemise puhul tuleb selle direktiivi artiklis 13 ette nähtud piiranguid käsitada nii, et need keskenduvad taotletud eesmärgi saavutamiseks rangelt vajalikule. Minu arvates tuleb sama kohaldada ka piirangutele programmi Safe Harbor põhimõtetest, mis on ette nähtud otsuse 2000/520 I lisa neljandas lõigus.

196. Tuleb märkida, et kõik keeleversioonid ei nimeta otsuse 2000/520 I lisa neljanda lõigu punkti a sõnastuses vajalikkuse kriteeriumi. Muu hulgas kehtib see prantsuskeelse versiooni kohta, mis sätestab, et „[l]'adhésion aux principes peut être limitée par [...] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois aux États-Unis”, samas kui näiteks hispaania-, saksa- ja ingliskeelses versioonis on märgitud, et kehtestatud piirangud peavad olema eespool nimetatud eesmärkide saavutamiseks vajalikud.

197. Olgu kuidas on, aga eelotsusetaotluse esitanud kohtu ja komisjoni poolt eespool viidatud kirjavahetuses esitatud faktilised asjaolud näitavad selgelt, et tegelikkuses ei keskenduta nende piirangute kohaldamisel üksnes viidatud eesmärgi saavutamiseks rangelt vajalikule.

198. Sellega seoses märgiksin, et Ameerika Ühendriikide luureteenistuste õigus edastatud isikuandmetega tutvuda hõlmab üldistatult kõiki isikuid ning kõiki elektroonilise side vahendeid ja edastatud andmekogumit, sealhulgas teabevahetuse sisu, ilma et taotletavat üldist huvi teenivat eesmärki arvestades oleks ette nähtud mingit eristamist, piirangut või erandit.[79]

74 — *Ibidem* (punkt 53).

75 — *Ibidem* (punkt 54 ja seal viidatud kohtupraktika).

76 — *Ibidem* (punkt 55 ja seal viidatud kohtupraktika).

77 — C-473/12, EU:C:2013:715.

78 — Punkt 32.

79 — Vt analoogia korras kohtuotsus Digital Rights Ireland jt (C-293/12 ja C-594/12, EU:C:2014:238, punkt 57 ja seal viidatud kohtupraktika).

199. Nimelt puudutab Ameerika Ühendriikide luureteenistuste õigus edastatud andmetega tutvuda üleüldiselt kõiki isikuid, kes kasutavad elektroonilisi sideteenuseid, ilma et nõutaks, et asjaomasted isikud kujutaksid ohtu avalikule julgeolekule.[80]

200. Niisugune massiline ja suvaline seire on oma olemuselt ebaproportsionaalne ja kujutab endast harta artiklitega 7 ja 8 tagatud õiguste põhjendamatut riivet.

201. Nagu parlament oma seisukohtades põhjendatult märkis, kuna liidu seadusandjal või liikmesriikidel on välistatud võtta vastu õigusnorme, mis hartat rikkudes näevad ette massilise ja suvalise seire, siis järeldub siit vältimatult, et *a fortiori* ei saa kolmandaid riike mingil juhul pidada liidu kodanike isikuandmete piisavat kaitsetaset tagavaks, kui nende õigusnormid võimaldavad tegelikkuses niisuguste andmete massilist ja suvalist seiret ja infopüüki.

202. Lisaks tuleb rõhutada, et programm Safe Harbor, nagu see on määratletud otsuses 2000/520, ei sisalda tagatisi, mis suudaksid välistada massilise ja üldise tutvumise edastatud andmetega.

203. Selles osas märgin, et Euroopa Kohus on oma kohtuotsuses Digital Rights Ireland jt[81] rõhutanud, kui oluline on näha ette „selged ja täpsed reeglid, mis reguleeriksid harta artiklites 7 ja 8 ette nähtud põhiõiguste riive ulatust".[82] Niisugune riive peab Euroopa Kohtu sõnul olema „täpselt piiritletud sätetega, mis võimaldaks tagada, et riive piirdub tõepoolest vaid vältimatult vajalikuga".[83] Euroopa Kohus on selles kohtuotsuses rõhutanud ka vajadust näha ette „piisavaid garantiisid – nagu nõuab harta artikkel 8 –, mis võimaldaksid tagada säilitatavate [isiku]andmete tõhusa kaitsmise kuritarvituste ohu eest ning ebaseadusliku juurdepääsu ja kasutamise eest".[84]

204. Tuleb märkida, et eraõigusliku vahekohtu mehhanismid ja FTC, tulenevalt oma piiratud rollist kaubanduslikes vaidlustes, ei kujuta endast vahendeid, mis võiksid vaidlustada Ameerika Ühendriikide luureteenistuste õiguse tutvuda liidust edastatud isikuandmetega.

205. FTC pädevus hõlmab ebaausat tegevust ja pettust kaubanduse valdkonnas ega laiene seega isikuandmete kogumisele ja kasutamisele mittekaubanduslikel eesmärkidel.[85] FTC piiratud pädevusvaldkond piirab üksikisikute õigust oma isikuandmete kaitsele. FTC loodi mitte selleks, et tagada üksikisiku eraelu austamise õiguse kaitse, nagu see on järelevalveasutuste puhul liidus, vaid selleks, et tagada õiglane ja tarbijate jaoks usaldusväärne kaubandus, mis *de facto* piirab tema võimalusi sekkuda isikuandmete kaitset puudutavasse valdkonda. FTC-l puudub seega liikmesriigi järelevalveasutustega võrreldav roll, mis on ette nähtud direktiivi 95/46 artiklis 28.

206. Liidu kodanikud, kelle andmed on edastatud, võivad pöörduda Ameerika Ühendriikides asutatud spetsialiseerunud vahekohtutesse nagu TRUSTe ja BBBOnline, et nõuda selgitusi selle kohta, kas ettevõtja, kelle valduses on nende isikuandmed, rikub enesesertifitseerimise korra tingimusi. Niisuguste asutuste nagu TRUSTe poolt tagatud eraõiguslik vahekohtumenetlus ei saa tegeleda isikuandmete kaitse õiguse rikkumistega, mille on toime pannud muud kui enesesertifitseeritud asutused või organid. Neil vahekohtuasutustel puuduvad igasugused volitused lahendada Ameerika Ühendriikide julgeolekuasutuste tegevuse õiguspärasuse küsimusi.

80 — *Ibidem* (punktid 58 ja 59).

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

82 — Punkt 65.

83 — *Idem.*

84 — *Ibidem* (punkt 66).

85 — Vt selle kohta otsuse 2000/520 II lisa, KKK 11, punkt „FTC meetmed", ja selle otsuse III, V ja VII lisa.

207. Ei FTC ega eraõiguslikud vahekohtuorganid ei ole volitatud kontrollima isikuandmete kaitse põhimõtete võimalikke rikkumisi, mille on toime pannud niisugused avaliku võimu esindajad nagu Ameerika Ühendriikide julgeolekuasutused. Niisugune pädevus oleks siiski oluline, et täielikult tagada õigus nende andmete tegelikule kaitsele. Komisjon ei saa seega otsust 2000/520 vastu võttes ja seda jõusse jättes tunnistada, et kõigile Ameerika Ühendriikidesse edastatud isikuandmete puhul on harta artikli 8 l'õikega 3 antud õigus piisavalt kaitstud, see tähendab et sõltumatu asutus teostab tegelikku kontrolli nende andmete kaitse- ja ohutusnõuete täitmise üle.

208. Järelikult tuleb tuvastada, et otsusega 2000/520 ette nähtud programmi Safe Harbor puhul puudub sõltumatu asutus, mis saaks kontrollida, et programmi Safe Harbor põhimõtest erandite rakendamine piirdub rangelt vajalikuga. Oleme näinud, et niisugune sõltumatu asutuse kontroll kujutab endast liidu õiguse seisukohast põhitegurit isikute kaitsmisel seoses isikuandmete töötlemisega. [86]

209. Sellega seoses tuleb rõhutada rolli, mis liidu õiguses kehtivas isikuandmete kaitse süsteemis on liikmesriigi järelevalveasutustel, kui nad kontrollivad direktiivi 95/46 artiklis 13 ette nähtud piiranguid. Selle direktiivi artikli 28 lõike 4 teises lõigus on sätestatud, et „[i]ga järelevalveasutus vaatab läbi eelkõige kõigi isikute avaldused kontrollida andmete töötlemise seaduslikkust, kui kohaldatakse käesoleva direktiivi artikli 13 kohaselt vastuvõetud siseriiklikke sätteid". Analoogia korras leian, et otsuse 2000/520 I lisa neljandas lõigus sisalduva viitega programmi Safe Harbor põhimõtete piirangutele oleks pidanud kaasnema järelevalvemehhanismi loomine isikuandmete kaitse valdkonnas spetsialiseerunud sõltumatu ametiasutuse poolt

210. Sõltumatute järelevalveasutuste sekkumine on nimelt Euroopa isikuandmete kaitse süsteemis kesksel kohal. Järelikult on loomulik, et niisuguse ametiasutuse olemasolu peeti esmalt üheks kolmanda riigi pakutud kaitse taseme piisavuse tuvastamiseks vajalikest tingimustest. Siin on tegemist tingimusega, mis peab olema täidetud selleks, et ei keelataks andmevoogu liikmesriikide territooriumilt kolmandatesse riikidesse vastavalt direktiivi 95/46 artiklile 25. [87] Nagu selle direktiivi artikli 29 alusel loodud töögrupi aruteludokumendis on märgitud, valitseb Euroopas üksmeelne seisukoht, et „„välise järelevalve" süsteem sõltumatu järelevalveasutuse näol on kogu andmekaitseeeskirjade järgimise tagamise süsteemi jaoks vajalik tegur". [88]

211. Lisaks märgin, et FISC ei paku tõhusat õiguskaitset liidu kodanikele, kelle isikuandmed on edastatud Ameerika Ühendriikidesse. Nimelt on 1978. aasta vastuluureseaduse punkti 702 raames ette nähtud kaitse riigiteenistustepoolse seire eest kohaldatav üksnes Ameerika Ühendriikide kodanikele ja Ameerika Ühendriikides seaduslikult ja alaliselt elavatele välismaalastele. Nagu komisjon ise on märkinud, võib Ameerika Ühendriikide luureandmete kogumise programmi parendada seeläbi, et FISC rolli tugevdatakse ja kehtestatakse õiguskaitsevahendid üksikisikutele. Need mehhanismid võiksid vähendada liidu kodanikke puudutavate isikuandmete töötlemist, mis ei ole riigi julgeoleku kaisteks asjakohased. [89]

212. Lisaks on komisjon ise märkinud, et liidu kodanikel ei ole mingit võimalust andmetega tutvuda, neid parandada või kustutada, või saada haldus- või õiguskaitset seoses neid puudutavate isikuandmete kogumise ja hilisema töötlemisega Ameerika Ühendriikide seireprogrammide raames. [90]

86 — Vt kohtuotsus Digital Rights Ireland jt (C-293/12 ja C-594/12, EU:C:2014:238, punkt 68 ja seal viidatud kohtrupraktika).

87 — Vt Poullet, Y., *„L'autorité de contrôle: 'vues' de Bruxelles"*, *Revue française d'administration publique*, nr 89, jaanuar–märts 1999, lk. 69, täpsemalt lk 71.

88 — Vt joonealuses märkuses nr 56 viidatud komisjoni töödokument WP 12, lk. 7.

89 — Vt joonealuses märkuses nr 2 viidatud komisjoni teatis, lk 10 ja 11.

90 — Vt joonealuses märkuses nr 56 viidatud komisjoni teatis, punkt 7.2, lk 20.

213. Viimaseks tuleb märkida, et Ameerika Ühendriikide õigusnorme eraelu kaitse kohta saab kohaldada differentseeritult Ameerika Ühendriikide kodanike ja välismaalaste suhtes.[91]

214. Eeltoodust järeldub, et otsuses 2000/520 ei ole ette nähtud selgeid ja täpseid eeskirju harta artiklites 7 ja 8 kehtestatud põhivabaduste riive ulatuse kohta. Seega tuleb nentida, et kõnealune otsus ja selle kohaldamise viis toovad endaga kaasa nende põhiõiguste ulatusliku ja eriti tõsise riive, ilma et õigusnormid niisugust riivet täpsemalt piiritleksid, mis võimaldaks tagada, et see tegelikult piirduks rangelt vajalikuga.

215. Otsust 2000/520 vastu võttes ja seda seejärel jõusse jättes on komisjon seega ületanud piiri, mida proporstionaalsuse põhimõte järgimine nõuab seoses harta artiklitega 7 ja 8 ning artikli 52 lõikega 1. Siia tuleb lisada, et juhuks, kui tuvastatakse, et liidu kodaniku õigusi on õigustamatult riivatud, näeb harta artikkel 47 ette õiguse tõhusale õiguskaitsevahendile.

216. Kõnesolev otsus tuleb järelikult tunnistada kehtetuks, kuna eespool kirjeldatud põhiõiguste rikkumiste tõttu ei saa teha järeldust, et sellega kehtestatud programm Safe Harbor tagab programmi raames liidust Ameerika Ühendriikidesse edastatud isikuandmete kaitse piisava taseme.

217. Arvestades niisugust järeldust liidu kodanike põhiõiguste rikkumiste kohta, leian, et komisjon oleks pidanud otsuse 2000/520 kohaldamise peatama.

218. See otsus on tähtajatu. Käesolev kohtuasi näitab, et kolmanda riigi pakutud kaitse taseme piisavus võib aja jooksul muutuda, tulenevalt nii selle otsuse aluseks olnud faktiliste kui ka õiguslike asjaolude muutumisest.

219. Märgin, et otsus 2000/520 ise sisaldab sätteid, mis näevad komisjonile ette võimaluse seda otsust asjaoludest lähtuvalt kohandada.

220. Niisiis tuleneb selle otsuse põhjendusest 9, et „[v]õib tekkida vajadus põhimõtete ja KKKde alusel loodud programm Safe Harbor läbi vaadata, võttes arvesse kogemusi, eraelu puutumatuse kaitset käsitlevaid arenguid olukorras, kus tehnoloogia pidevalt lihtsustab isikuandmete edastamist ja töötlemist, ning kaasatud täitevasutuste rakendusaruandeid".

221. Samuti on nimetatud otsuse artikli 3 lõikes 4 sätestatud, et „[k]ui lõigete 1, 2 ja 3 alusel kogutud teave annab tunnistust sellest, et Ameerika Ühendriikides kooskõlas KKKdega rakendatud põhimõtete järgimise tagamise eest vastutav asutus ei täida oma rolli tõhusalt, teavitab komisjon Ameerika Ühendriikide kaubandusministeeriumi ja vajaduse korral esitab meetmete eelnõud […] käesoleva otsuse tühistamiseks või peatamiseks või selle reguleerimissala piiramiseks".

222. Lisaks võib otsuse 2000/520 artikli 4 lõike 1 kohaselt seda otsust muuta igal ajal vastavalt selle rakendamise kogemusele ja/või kui Ameerika Ühendriikide õigusaktid jõuavad põhimõtete ja KKK-dega tagatud kaitse taseme tagamiseni. Kolm aastat pärast käesoleva otsuse teatavakstegemist liikmesriikidele hindab komisjon kättesaadava teabe alusel igal juhul selle rakendamist ning esitab direktiivi 95/46[…] artikli 31 alusel moodustatud komiteele aruande kõigi asjakohaste järelduste kohta, sealhulgas tõendid, mis võivad mõjutada järeldust, et käesoleva otsuse artikli 1 sätetega pakutav kaitse on direktiivi 95/46/EÜ artikli 25 tähenduses piisav". Otsuse 2000/520 artikli 4 lõikes 2 on sätestatud, et „komisjon esitab vajaduse korral meetmete eelnõud direktiivi 95/46/EÜ artiklis 31 sätestatud korras".

91 — Vt selle küsimuse kohta Kuner, C., *„Foreign Nationals and Data Protection Law: A Transatlantic Analysis"*, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, lk 213, eriti lk 216 jj.

223. Komisjon märkis oma seisukohtades, et on „väga tõenäoline, et programmi Safe Harbor põhimõtetega võib liituda piiratud määral, mis ei vasta enam riigi julgeoleku valdkonnas ette nähtud erandiga rangelt piiritletud tingimustele”. [92] Komisjon märgib selles osas, et „kõnealused paljastused osutavad suvalisele laiaulatuslikule seirele, mis ei ole kooskõlas selle erandiga ette nähtud vajaduse kriteeriumiga ega üldisemalt ka harta artiklis 8 sätestatud isikuandmete kaitse õigusega”. [93] Pealegi on komisjon ise nentinud, et „jälgimisprogrammide ulatus ja [liidu] kodanike ebavõrdne kohtlemine seavad küsimärgi alla programmi Safe Harbor pakutava kaitse taseme”. [94]

224. Lisaks on komisjon kohtuisungil sõnaselgelt tunnistanud, et otsuse 2000/520 raames, nagu seda tegelikult kohaldatakse, puudub tagatis, et liidu kodanike õigus oma andmete kaitsele oleks tagatud. Tema sõnul see järeldus siiski ei muuda seda otsust kehtetuks. Kuigi komisjon on nõus kinnitusega, et uute asjaolude esinemisel peab ta tegutsema, on ta arvamusel, et ta võttis asjakohaseid ja proportsionaalseid meetmeid, kui alustas Ameerika Ühendriikidega läbirääkimisi proogrammi Safe Harbor reformimiseks.

225. Ma ei jaga seda arvamust. Nimelt oleks vahepeal pidanud liikmesriigi järelevalveasutuse algatusel või talle esitatud kaebuste alusel olema võimalik isikuandmete edastamine Ameerika Ühendriikidesse peatada.

226. Lisaks leian ma, et niisugusi järeldusi arvestades oleks komisjon pidanud otsuse 2000/520 kohaldamise peatama. Nimelt paneb isikuandmete kaitse eesmärk, mida taotlevad nii direktiiv 95/46 kui harta artikkel 8, kohustusi mitte ainult liikmesriikidele, vaid ka liidu institutsioonidele, nagu tuleneb harta artikli 51 lõikest 1.

227. Hinnates kolmanda riigi pakutud kaitse taseme piisavust peab komisjon uurima mitte ainult selle kolmanda riigi siseriiklikke õigusnorme ja rahvusvahelisi kohustusi, vaid ka seda, mil viisil isikuandmete kaitset tegelikult tagatakse. Kui praktika uurimine viitab häiretele, peab komisjon tegutsema ja oma otsuse vajaduse korral peatama ja/või seda viivitamata ajakohastama.

228. Nagu me eespool toodud arutluskäigus nägime, seisneb liikmesriikidele pandud kohustus peamiselt selle tagamises – liikmesriigi järelevalveasutuste tegutsemise kaudu –, et tagataks direktiivis 95/46 ette nähtud eeskirjade järgimine.

229. Kui asjaomase kolmanda riigi poolsed rikkumised on tõendatud, lasub komisjonil kohustus peatada selle direktiivi artikli 25 lõike 6 alusel võetud otsuse kohaldamine ajaks, mil ta peab kolmanda riigiga läbirääkimisi nende rikkumiste lõpetamiseks.

230. Tuletan meelde, et nimetatud sätte alusel komisjoni tehtud otsuse eesmärk on tuvastada, et kolmas riik „tagab” sellesse riiki edastatavate isikuandmete kaitse piisava taseme. Oleviku ajavormis kasutatud mõiste „tagab” viitab sellele, et jõusse jäämiseks peab niisugune otsus puudutama kolmandat riiki, mis pärast selle otsuse vastuvõtmist jätkuvalt tagab niisuguse kaitse piisava taseme.

231. Direktiivi 95/46 põhjenduse 57 kohaselt „tuleb keelata isikuandmete edastamine kolmandatesse riikidesse, kus nende kaitse tase ei ole piisav”.

232. Selle direktiivi artikli 25 lõike 4 kohaselt, „[k]ui komisjon artikli 31 lõikes 2 ettenähtud korras leiab, et kolmas riik ei taga kaitse piisavat taset käesoleva artikli lõike 2 tähenduses, võtavad liikmesriigid vajalikke meetmeid tagamaks, et sama liiki andmeid kõnealusesse kolmandasse riiki ei edastata”. Lisaks näeb nimetatud direktiivi artikli 25 lõige 5 ette, et „[s]obival ajal alustab komisjon läbirääkimisi, et parandada olukorda, mis tekkis lõike 4 kohaselt tehtud avastuse tõttu”.

92 — Punkt 44.

93 — *Idem.*

94 — Vt joonealuses märkuses nr 2 viidatud komisjoni teatis, lk 5.

233. Viimasest sättest tuleneb, et direktiivi 95/46 artikliga 25 kehtestatud süsteemis on kolmanda riigiga peetavate läbirääkimiste eesmärk korvata kaitse piisava taseme tuvastatud puudumise küsimus vastavalt selle direktiivi artikli 31 lõikes 2 ette nähtud menetlusele. Vaatluse all oleval juhul ei ole komisjon selle menetluse kohaselt ametlikult tunnistanud, et programm Safe Harbor ei taga enam kaitse piisavat taset. Seetõttu, kui komisjon otsustas asuda Ameerika Ühendriikidega läbirääkimistesse, on selge, et eelnevalt tegi ta järelduse, et selle kolmanda riigi pakutud kaitse tase ei olnud enam piisav.

234. Seega, kuigi komisjon oli teadlik häiretest selle otsuse kohaldamisel, ei peatanud ega ajakohastanud ta seda otsust, põhjustades seeläbi nende isikute põhiõiguste rikkumise, kelle isikuandmeid programmi Safe Harbor raames edastati ja jätkuvalt edastatakse.

235. Euroopa Kohus on juba sedastanud, ehkki küll teises kontekstis, et komisjon peab hoolitsema õigusnormide kohandamise eest uusi andmeid arvestades. [95]

236. Niisugune tegevusetus komisjoni poolt, mis otseselt kahjustab harta artiklitega 7, 8 ja 47 kaitstud põhiõigusi, on minu arvates täiendav põhjus tunnistada otsus 2000/520 käesoleva eelotsuse raames kehtetuks. [96]

III. **Ettepanek**

237. Eespool toodud arutluskäiku arvesse võttes teen Euroopa Kohtule ettepaneku vastata High Courti esitatud küsimustele järgmiselt:

Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiivi 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta artiklit 28, koostoimes Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8, tuleb tõlgendada nii, et asjaolu, et eksisteerib otsus, mille Euroopa Komisjon tegi direktiivi 95/46 artikli 25 lõike 6 alusel, ei takista liikmesriigi järelevalveasutust menetlemast kaebust, milles väidetakse, et kolmas riik ei taga edastatud isikuandmetele piisaval tasemel kaitset, ja nende isikuandmete vaidlustatud edastamist vajaduse korral peatamast.

Komisjoni 26. juuli 2000. aasta otsus vastavalt Euroopa Parlamendi ja nõukogu direktiivile 95/46/EÜ piisava kaitse kohta, mis on ette nähtud programmi Safe Harbor põhimõtetega ja sellega seotud korduma kippuvate küsimustega, mille on välja andnud Ameerika Ühendriikide kaubandusministeerium, on kehtetu.

95 — Vt selle kohta kohtuotsus Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, punkt 40).

96 — Kuigi Euroopa Kohus on oma kohtuotsuses T. Port (C-68/95, EU:C:1996:452) sedastanud, et „asutamisleping ei näe ette võimalust esitada eelotsusetaotlus, milles liikmesriigi kohus palub Euroopa Kohtul eelotsuse korras tuvastada liikmesriigi tegevusetus" (punkt 53), siis näib, et oma kohtuotsuses Ten Kate Holding Musselkanaal jt (C-511/03, EU:C:2005:625, punkt 29) on ta selle võimaluse suhtes võtnud soodsama hoiaku.