Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
YVESA BOTA
od 23. rujna 2015.[1]

Predmet C-362/14

Maximillian Schrems
protiv
Data Protection Commissioner

(zahtjev za prethodnu odluku koji je uputio Visoki sud (High Court, Irska))

„Zahtjev za prethodnu odluku – Osobni podaci – Zaštita fizičkih osoba u pogledu obrade tih podataka – Povelja Europske unije o temeljnim pravima – Članci 7., 8. i 47. – Direktiva 95/46/EZ – Članak 25. – Odluka 2000/520/EZ – Prijenos osobnih podataka u SAD – Procjena odgovarajuće ili neodgovarajuće razine zaštite – Pritužba fizičke osobe čiji su podaci preneseni iz Europske unije trećoj zemlji – Nacionalno nadzorno tijelo – Ovlasti“

I – **Uvod**

1. Kako je Europska komisija zaključila u svojoj Komunikaciji od 27. studenoga 2013.[2], „[p]rijenosi osobnih podataka važan su i nužan element transatlantskih odnosa. Oni čine sastavni dio trgovinskih razmjena preko Atlantika, uključujući nove i rastuće poslovne subjekte koji se bave digitalnom tehnologijom, poput društvenih medija i računalstva u oblaku, pri čemu velike količine podataka odlaze iz EU-a u SAD“[3].

2. Trgovinske razmjene predmet su Odluke Komisije 2000/520/EZ od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a[4]. Ta odluka predstavlja pravnu osnovu za prijenos osobnih podataka iz Unije poduzećima s poslovnim nastanom u SAD-u koja poštuju načela privatnosti „sigurne luke“.

3. Navedena odluka danas je postavljena pred izazov jer mora omogućavati protok podataka između Unije i SAD-a, jamčeći visoku razinu zaštite tih podataka kako to zahtijeva pravo Unije.

4. Naime, nedavno je u više navrata otkriveno da postoje američki programi masovnog prikupljanja informacija. Ta su otkrića pobudila nesigurnost u pogledu poštovanja pravnih normi Unije pri prijenosu osobnih podataka poduzećima s poslovnim nastanom u SAD-u i slabosti sustava „sigurne luke“.

1 — Izvorni jezik: francuski

2 — Komunikacija Komisije Europskom parlamentu i Vijeću o „Ponovnoj uspostavi povjerenja u protoku podataka između EU-a i SAD-a“ [COM(2013) 846 *final*].

3 — Stranica 2.

4 — (SL L 215, str. 7.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 16., svezak 3., str. 9.) i ispravak SL 2001., L 115, str.14.

5. U ovom se zahtjevu za prethodnu odluku od Suda traži pojašnjenje kakav bi pristup trebali zauzeti nacionalna nadzorna tijela i Komisija kada budu suočeni s nepravilnostima pri primjeni Odluke 2000/520.

6. Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka [5] predviđa u svojem Poglavlju IV. pravila o prijenosu osobnih podataka trećim zemljama.

7. U tom poglavlju, načelo uspostavljeno u članku 25. stavku 1. te direktive određuje da se prijenos osobnih podataka koji se obrađuju ili koje je potrebno obraditi nakon prijenosa trećoj zemlji može izvršiti jedino ako te treće zemlje osiguraju odgovarajuću razinu zaštite takvih podataka.

8. S druge strane, kako to zakonodavac Unije određuje u uvodnoj izjavi 57. navedene direktive, prijenos osobnih podataka trećoj zemlji koja ne pruža odgovarajuću razinu zaštite mora se zabraniti.

9. U skladu s člankom 25. stavkom 2. Direktive 95/46 „[o]dgovarajuća razina zaštite koju osiguravaju treće zemlje procjenjuje se ovisno o svim okolnostima u vezi s prijenosom podataka ili skupom postupaka prijenosa podataka; posebno se razmatra priroda podataka, svrha i trajanje predloženog postupka ili postupka obrade, država podrijetla i država konačnog odredišta, važeća pravna pravila, kako ona opća, tako i posebna, u toj trećoj zemlji te profesionalna pravila i mjere sigurnosti koje se primjenjuju u toj državi“.

10. Na temelju članka 25. stavka 6. te direktive, Komisija može utvrditi da treća zemlja svojim domaćim zakonodavstvom ili međunarodnim obvezama koje je preuzela osigurava odgovarajuću razinu zaštite osobnih podataka. Kada Komisija donese odluku u tom smislu, može se izvršiti prijenos osobnih podataka trećoj zemlji.

11. Primjenjujući tu odredbu Komisija je donijela Odluku 2000/520. Iz članka 1. stavka 1. te odluke proizlazi da se smatra da „načela privatnosti ‚sigurne luke'“ provedena u skladu sa smjernicama iz „često postavljanih pitanja“ [6] osiguravaju primjerenu razinu zaštite osobnih podataka prenesenih iz Unije poduzećima s poslovnim nastanom u SAD-u.

12. Posljedično, Odluka 2000/520 dopušta prijenos osobnih podataka iz država članica poduzećima s poslovnim nastanom u SAD-u koja su se obvezala da će poštovati načela “sigurne luke“.

13. U Prilogu I. Odluci 2000/520 navedeno je niz načela kojih se poduzeća mogu dobrovoljno pridržavati, zajedno s ograničenjima te poseban sustav nadzora. U 2013. broj poduzeća koja su se pridržavala nečeg što se može kvalificirati kao „kodeks ponašanja“ prelazio je 3200.

14. Sustav „sigurne luke“ temelji se na rješenju koje kombinira vlastito potvrđivanje i samoocjenjivanje privatnih poduzeća te intervenciju javne vlasti.

15. Načela „sigurne luke“ su „izrađena u dogovoru s gospodarstvenicima i javnošću kako bi se olakšali trgovanje i trgovin[a] između Sjedinjenih Američkih Država i Unije […]. Načela su namijenjena isključivo organizacijama SAD-a koje primaju osobne podatke iz […] Unije radi kvalificiranja za „sigurnu luku” i iz nje proizašlog preduvjeta „primjerenosti” zaštite podataka“ [7].

5 — (SL L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.), Direktiva kako je izmijenjena Uredbom (EZ) br. 1882/2003 Europskog parlamenta i Vijeća od 29. rujna 2003. (SL L 284, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 1., svezak 16., str. 96., u daljnjem tekstu: Direktiva 95/46).

6 — Frequently asked questions, u daljnjem tekstu: često postavljana pitanja.

7 — Drugi stavak Priloga I. Odluci 2000/520.

16. Načela "sigurne luke" koja se nalaze u Prilogu I. Odluci 2000/520 predviđaju među ostalim:

— obvezu obavještavanja prema kojoj „[o]rganizacija mora obavijestiti pojedince o namjeni prikupljanja i uporabi njihovih osobnih podataka, kako mogu kontaktirati organizaciju radi upita ili pritužbi, o kategorijama trećih strana kojima otkriva te podatke te mogućnostima i sredstvima koje organizacija nudi pojedincima za ograničivanje njihove uporabe i otkrivanja. Ova obavijest […] mora biti sastavljena […] kada se od pojedinaca prvi put zatraži da daju osobne podatke organizaciji ili čim prije nakon toga, ali u svakom slučaju prije nego organizacija koristi takve informacije u neku drugu svrhu osim one za koju ih je prvotno prikupila ili obradila organizacija koja je izvršila prijenos ili prije nego što ih po prvi put otkrije trećoj osobi“ [8];

— obvezu da organizacija pojedincima ponudi mogućnost da odaberu hoće li se njihovi podaci moći otkriti trećoj osobi ili koristiti u svrhu koja nije sukladna sa svrhom (svrhama) za koju su izvorno prikupljeni ili za koju je pojedinac naknadno dao odobrenje. Kod osjetljivih informacija „mora im biti ponuđena potvrdna ili izričita mogućnost odabira (pristanak) ako će se te informacije otkriti trećoj osobi ili koristiti u neku drugu svrhu osim one za koju su prvotno prikupljene ili za koju je pojedinac naknadno dao odobrenje koristeći mogućnost odabira“ [9];

— pravila o daljnjem prijenosu podataka. Tako „[p]ri otkrivanju podataka trećoj osobi, organizacije moraju primjenjivati načela obavijesti i mogućnosti izbora“ [10];

— što se tiče sigurnosti podataka, obvezu za „[o]rganizacije koje stvaraju, održavaju, koriste ili prenose osobne podatke [da] poduzmu odgovarajuće mjere da bi ih zaštitile od gubitka, zlouporabe i neovlaštenog pristupa, otkrivanja, izmjene i uništenja“ [11];

— što se tiče nepovredivosti podataka, obvezu da organizacije „[…] trebaju poduzeti odgovarajuće korake da podaci budu pouzdani za namjeravano korištenje, točni, potpuni i ažurirani“ [12];

— da pojedinci čije podatke čuva organizacija moraju u načelu „imati pristup osobnim podacima koje organizacija čuva, te ih moći ispraviti, promijeniti ili obrisati ako su netočni“ [13];

— obvezu da predvidi „mehanizme kojima se osigurava poštovanje načela ‚sigurne luke', pravna zaštita pojedinaca na koje se odnose podaci na koje nepridržavanja načela utječe, te posljedice za organizaciju kad ne poštuje načela“ [14].

17. Američka organizacija koja želi pristupiti načelima „sigurne luke“ mora se u svojoj politici zaštite privatnosti obvezati da će objaviti da je pristupila tim načelima i da ih stvarno poštuje te sama mora potvrditi poštovanje načela tako da pri Department of Commerce izjavi da poštuje navedena načela [15].

8 — Vidjeti Prilog I. pod naslovom „Obavijest“.

9 — Vidjeti Prilog I. pod naslovom „Mogućnost izbora“.

10 — Vidjeti Prilog I. pod naslovom „Daljnji prijenos“.

11 — Vidjeti Prilog I. pod naslovom „Sigurnost“.

12 — Vidjeti Prilog I. pod naslovom „Nepovredivost podataka“.

13 — Vidjeti Prilog I. pod naslovom „Pristup“.

14 — Vidjeti Prilog I. pod naslovom „Provedba“.

15 — Članak 1. stavci 2. i 3. Odluke 2000/520. Vidjeti također Prilog II., često postavljano pitanje 6.

18. Organizacijama na raspolaganju stoji više načina za usklađivanje s načelima „sigurne luke“. Tako se one mogu na primjer „uključi[ti] u samoregulativni program privatnosti koji se pridržava načela [ili] ispuniti uvjete tako da stvore vlastite samoregulativne politike zaštite privatnosti ako su one u skladu s načelima. […] Osim toga, organizacije koje podliježu zakonskim, regulatornim, upravnim ili drugim propisima (ili pravilima) i učinkovito štiti osobnu privatnost, mogu se također kvalificirati za prednosti koje pruža ‚sigurna luka’“ [16].

19. Za provjeru poštuju li se načela ‚sigurne luke’ postoji više mehanizama koji kombiniraju privatnu arbitražu i nadzor javnih vlasti. Nadzor se također može osigurati posredstvom sustava izvansudskog rješavanja sporova koji vrši neovisna treća osoba. Osim toga, poduzeća se mogu obvezati da surađuju s Unijinim odborom za zaštitu podataka. Naposljetku, Savezna trgovinska komisija (Federal Trade Commision, u daljnjem tekstu: FTC) na osnovi ovlasti koje su joj dodijeljene na temelju odjeljka 5. Zakona o Saveznoj trgovinskoj komisiji (Federal Trade Commission Act) i Ministarstvo prometa (Department of Transportation) na osnovi ovlasti koje su mu dodijeljene na temelju članka 49. odjeljka 41712. Zakonika SAD-a (United States Code) nadležni su za rješavanje pritužbi.

20. Na temelju četvrtog stavka Priloga I. Odluci 2000/520, pridržavanje načela ‚sigurne luke’ može biti ograničeno, među ostalim „u onoj mjeri koja je potrebna da se ispune uvjeti nacionalne sigurnosti, javnog interesa, ili uvjeti za provedbu zakona“ i zakonom, vladinom uredbom ili sudskom praksom koji proizvode proturječne obveze ili izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezino nepošt[o]vanje načela ograničeno u mjeri potrebnoj da se ostvare pretežući zakoniti interesi koje podupire takvo dopuštenje“ [17].

21. Osim toga, da bi nadležna tijela država članica mogla prekinuti protok podataka mora biti ispunjeno više uvjeta predviđenih u članku 3. stavku 1. Odluke 2000/520.

22. Ovaj zahtjev za prethodnu odluku odnosi se na doseg Odluke 2000/520 s obzirom na članke 7., 8. i 47. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja) kao i na članak 25. stavak 6. i članak 28. Direktive 95/46. Ovaj zahtjev upućen je u okviru spora između M. Schremsa i Data Protection Commissionera (povjerenik za zaštitu podataka, u daljnjem tekstu: povjerenik) u vezi s odbijanjem povjerenika da ispita pritužbu M. Schremsa o činjenici da Facebook Ireland Ltd (u daljnjem tekstu: Facebook Irska) zadržava osobne podatke svojih korisnika na poslužiteljima smještenima u SAD-u.

23. M. Schrems austrijski je državljanin s boravištem u Austriji. Od 2008. korisnik je društvene mreže Facebook.

24. Svaki korisnik Facebooka s boravištem na državnom području Unije dužan je prilikom registriranja sklopiti ugovor s Facebookom Irska, društvom kćeri Facebooka Inc. (u daljnjem tekstu: Facebook SAD) koje ima sjedište u SAD-u. Osobni podaci korisnika Facebooka Irska koji borave na državnom području Unije prenose se u cijelosti ili djelomično na poslužitelje Facebooka SAD, koji su smješteni na državnom području SAD-a, gdje se zadržavaju.

25. M. Schrems uputio je 25. lipnja 2013. pritužbu povjereniku tvrdeći, u biti, da pravo i prakse SAD-a ne daju nikakvu stvarnu zaštitu podataka koji su zadržani na području SAD-a protiv nadzora države. To je proizašlo iz otkrića koja je objavljivao Edward Snowden o aktivnostima američkih obavještajnih službi, posebice National Security Agencyja (u daljnjem tekstu: NSA) od svibnja 2013.

16 — Prilog II. treći stavak.

17 — Vidjeti također Prilog IV., B.

26. Iz tih otkrića među ostalim proizlazi da je NSA uspostavila program nazvan „PRISM“ u okviru kojeg je ta agencija stekla slobodan pristup masovnim podacima koji su pohranjeni na poslužiteljima smještenima u SAD-u, koje posjeduju ili su pod nadzorom niza društava koja djeluju u području interneta i tehnologije kao što je Facebook SAD.

27. Povjerenik je zaključio da nije dužan ispitati pritužbu jer je pravno neosnovana. Smatrao je da nije bilo dokaza o tome da je NSA pristupila podacima M. Schremsa. Osim toga, pritužba je prema njegovu mišljenju trebala biti odbijena na temelju Odluke 2000/520 u kojoj je Komisija zaključila da SAD u okviru sustava sigurne luke osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka. O svakom pitanju o odgovarajućoj zaštiti tih podataka u SAD-u trebalo bi odlučiti u skladu s tom odlukom koja ga je sprečavala da ispita pitanja navedena u pritužbi.

28. Povjerenik je odbio pritužbu na temelju niže navedenog nacionalnog zakonodavstva.

29. Članak 10. stavak 1. Zakona o zaštiti podataka iz 1988. (Data Protection Act 1988) kako je izmijenjen Zakonom o zaštiti podataka iz 2003. [Data Protection (Amendment) Act 2003, u daljnjem tekstu: Zakon o zaštiti podataka] daje mu ovlast ispitivanja pritužbi i glasi:

„(a) Povjerenik može ispitati ili naložiti ispitivanje jesu li odredbe ovog zakona bile, jesu li ili bi mogle biti povrijeđene u vezi s određenom osobom ako ta osoba njemu podnese pritužbu zbog povrede neke od tih odredaba ili ako povjerenik smatra da takva povreda postoji.

(b) Kada osoba podnese pritužbu pred povjerenikom na temelju točke (a) ovog stavka, povjerenik:

(i) istražuje ili nalaže istragu pritužbe, osim ako je zaključio da je zlonamjerna ili da je podnesena iz obijesti i,

(ii) ako povjerenik ili povjerenica ne mogu u razumnom roku mirno riješiti spor dotičnih stranaka o predmetu pritužbe, pisano obavještavaju podnositelja pritužbe o odluci koju je donio ili donijela o pritužbi, upućujući ga da, ako ta odluka utječe negativno na njegov položaj, može protiv te odluke izjaviti pravni lijek na temelju članka 26. ovog zakona u roku od 21 dana od primitka obavijesti.“

30. Povjerenik je u ovom slučaju odlučio da je pritužba M. Schremsa bila „zlonamjerna ili podnesena iz obijesti“ u smislu da je bila osuđena na propast jer je bila lišena pravnog temelja. Zbog tog razloga je odbio tu pritužbu.

31. Članak 11. Zakona o zaštiti podataka uređuje prijenos osobnih podataka izvan nacionalnog područja. Članak 11. stavak 2. točka (a) tog zakona predviđa:

„Kada se u bilo kojem postupku koji uređuje ovaj zakon pojavi pitanje:

(i) utvrđivanja je li u državi ili na području izvan Europskog gospodarskog prostora [(EGP)] u koje će biti preneseni osobni podaci osigurana odgovarajuća razina zaštite precizirana u prvom stavku ovog članka, i

(ii) ako je Unija donijela utvrđenje koje se odnosi na vrstu prijenosa o kojem je riječ,

o pitanju će se odlučiti u skladu s tim utvrđenjem“.

32. Članak 11. stavak 2. točka (b) Zakona o zaštiti podataka određuje pojam utvrđenja Unije kako slijedi:

„U točki (a) ovog stavka ‚utvrđenje Unije' znači utvrđenje koje je Komisija […] donijela u skladu sa stavkom 4. ili 6. članka 25. Direktive [95/46], u okviru postupka predviđenog u članku 31. stavku 2. te direktive da bi utvrdila je li u državi ili području izvan [EGP] osigurana odgovarajuća razina zaštite precizirana u stavku 1. ovog članka]."

33. Povjerenik je zaključio da je Odluka 2000/520 bila „utvrđenje Unije" u smislu članka 11. stavka 2. točke (a) Zakona o zaštiti podataka, na način da se na temelju tog zakona o pitanju o odgovarajućoj zaštiti podataka u trećim državama u koje su oni preneseni treba odlučiti u skladu s tim utvrđenjem. Budući da se radilo o bitnom dijelu pritužbe M. Schremsa, to jest o tome da su osobni podaci preneseni trećoj zemlji koja u praksi ne osigurava odgovarajuću razinu zaštite, povjerenik je smatrao da ga je narav i samo postojanje Odluke 2000/520 spriječilo da ispita to pitanje.

34. M. Schrems podnio je tužbu pred Visokim sudom protiv povjerenikove odluke da odbije njegovu pritužbu. Nakon ispitivanja dokaza koji su podneseni u glavnom postupku, taj je sud utvrdio da elektronički nadzor i presretanje prenesenih osobnih podataka ispunjavaju nužne i neophodne svrhe u javnom interesu, to jest održavanje nacionalne sigurnosti i sprečavanje teških kaznenih djela. High Court u tom pogledu navodi da nadzor i presretanje osobnih podataka koji su preneseni iz Unije u SAD služe legitimnim protuterorističkim ciljevima.

35. Prema mišljenju istog suda, otkrića E. Snowdena su ipak pokazala da su NSA i druga slična tijela izvršili značajna prekoračenja. Iako Foreign Intelligence Surveillance Court (u daljnjem tekstu: FISC) provodi nadzor na temelju Zakona o nadzoru inozemnih obavještajnih službi iz 1978. (Foreign Intelligence Surveillance Act of 1978) [18], postupak pred njim je tajan i nekontradiktoran. Štoviše, osim činjenice da su odluke o pristupu osobnim podacima donesene na temelju američkog prava, građani Unije ne raspolažu nikakvim pravom na saslušanje u vezi s pitanjem nadzora i presretanja njihovih podataka.

36. Iz opsežnih dokumenata koji su bili priloženi izjavama pod prisegom danima u glavnom postupku jasno je proizlazilo da točnost brojnih Snowdenovih otkrića nije dovedena u pitanje. Visoki sud je stoga zaključio da jednom kada su osobni podaci preneseni u SAD, NSA i druge američke sigurnosne agencije kao što je Federal Bureau of Investigation (FBI) njima mogu pristupiti u okviru provedbe nadzora i masovnog neselektivnog presretanja.

37. Visoki sud je zaključio da u irskom pravu važnost ustavnih prava na privatnost i nepovredivost doma zahtijeva da svako miješanje u ta prava bude proporcionalno i usklađeno sa zahtjevima predviđenima zakonom. Masovni i neselektivni pristup osobnim podacima nikako nije u skladu sa zahtjevom proporcionalnosti i stoga bi se trebalo smatrati da je protivan irskom ustavu [19].

38. Visoki sud navodi da, kako bi se presretanja elektroničke komunikacije mogla smatrati ustavnima, treba dokazati da su utvrđena presretanja komunikacije i nadzora određenih osoba ili određenih skupina osoba objektivno opravdani u interesu nacionalne sigurnosti i suzbijanja kriminaliteta i da postoje odgovarajuća i provjerljiva jamstva.

18 — Vidjeti odjeljak 702. tog zakona kako je izmijenjen Zakonom iz 2008. (Foreign Intelligence Surveillance Act of 2008). Na temelju tog odjeljka NSA drži bazu podataka poznatu pod nazivom „PRISM" (vidjeti report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection od 27. studenoga 2013.).

19 — Visoki sud osobito upućuje na poštovanje ljudskog dostojanstva i slobode pojedinca (preambula), osobne autonomije (članak 40. stavak 3. točke 1. i 2.), nepovredivosti doma (članak 40. stavak 5.) i zaštitu obiteljskog života (članak 41.).

39. Slijedom toga, Visoki sud upućuje da bi se, ako bi se ovaj predmet rješavao samo na temelju irskog prava, pojavio veliki problem o tome da li SAD „osigurava odgovarajuću razinu zaštite privatnosti kao i temeljnih prava i sloboda“ u smislu članka 11. stavka 1. Zakona o zaštiti podataka. Iz toga proizlazi da, na temelju irskog prava i osobito ustavnih zahtjeva, povjerenik nije smio odbiti pritužbu M. Schremsa, već je morao ispitati to pitanje.

40. Međutim, Visoki sud utvrđuje da se predmet o kojem odlučuje odnosi na provedbu prava Unije u smislu članka 51. stavka 1. Povelje na način da se zakonitost povjerenikove odluke treba ocjenjivati s obzirom na pravo Unije.

41. Visoki sud je na sljedeći način objasnio problem koji se našao pred povjerenikom. Na temelju članka 11. stavka 2. točke (a) Zakona o zaštiti podataka, povjerenik je dužan odlučiti o odgovarajućoj zaštiti u trećoj zemlji „u skladu“ s utvrđenjem Unije koje je Komisija donijela u skladu s člankom 25. stavkom 6. Direktive 95/46. Iz toga proizlazi da povjerenik nije mogao odstupiti od tog utvrđenja. Budući da je Komisija u svojoj Odluci 2000/520 zaključila da SAD jamči odgovarajuću razinu zaštite što se tiče obrade podataka društava koja poštuju načela privatnosti „sigurne luke“, povjerenik bi pritužbu u kojoj se tvrdi da takva zaštita nije odgovarajuća nužno morao odbiti.

42. Smatrajući da je povjerenik tako dokazao detaljno poštovanje Direktive 95/46 i Odluke 2000/520, Visoki sud navodi da M. Schrems zapravo više prigovara uvjetima sustava „sigurne luke“ nego načinu na koji ga je primijenio povjerenik, pri čemu je naglasio da nije neposredno osporavao valjanost Direktive 95/46 ni Odluke 2000/520.

43. Prema mišljenju Visokog suda, temeljno pitanje bi stoga bilo je li, s obzirom na pravo Unije i vodeći računa osobito o naknadnom stupanju na snagu članaka 7. i 8. Povelje, povjerenik potpuno vezan utvrđenjem Komisije navedenim u Odluci 2000/520 o odgovarajućoj zaštiti prava i praksi u području zaštite osobnih podataka u SAD-u.

44. Visoki sud osim toga precizira da u tužbi o kojoj odlučuje nijedan prigovor nije istaknut u pogledu aktivnosti Facebooka Irska i Facebooka SAD kao takvih. Članak 3. stavak 1. točka (b) Odluke 2000/520 koji omogućava nadležnim nacionalnim tijelima da nalože poduzeću da suspendira protok podataka trećoj zemlji, prema mišljenju tog suda primjenjuje se samo u okolnostima kada je pritužba usmjerena protiv ponašanja poduzeća u pitanju, što ovdje nije slučaj.

45. Visoki sud stoga ističe da stvarni prigovor nije usmjeren na ponašanje Facebook SAD-a kao takvog, već više na činjenicu da je Komisija ustvrdila da pravo i prakse u području zaštite podataka u SAD-u jamče odgovarajuću zaštitu, dok otkrića E. Snowdena jasno ukazuju na to da američka tijela mogu masovno i neselektivno pristupiti osobnim podacima stanovništva koje živi na području Unije [20].

46. U tom pogledu Visoki sud smatra da je teško predvidjeti kako bi Odluka 2000/520 u praksi mogla zadovoljiti zahtjeve članaka 7. i 8. Povelje, *a fortiori* ako uzmemo u obzir načela koja je uobličio Sud u svojoj presudi Digital Rights Ireland i dr. [21]. Osobito bi bilo ugroženo jamstvo predviđeno u članku 7. Povelje i temeljnim vrijednostima koje su zajedničke tradicijama država članica ako bi javnim vlastima bilo dopušteno nasumično i općenito pristupati elektroničkim komunikacijama a da ne postoji nikakvo objektivno opravdanje utemeljeno na razlozima nacionalne sigurnosti ili sprečavanja kriminaliteta koji su posebno povezani s dotičnim pojedincima i bez ikakvog odgovarajućeg i provjerljivog jamstva. Kako se sugerira u tužbi M. Schremsa, Odluka 2000/520 bi mogla *in abstracto* biti neusklađena s člancima 7.

20 — Visoki sud u tom pogledu navodi da je glavni tužbeni razlog koji pred njim ističe M. Schrems taj da, uzevši u obzir nedavna otkrića E. Snowdena i činjenicu da su osobni podaci masovno stavljeni na raspolaganje obavještajnim službama, povjerenik nije mogao valjano zaključiti da u toj trećoj zemlji postoji odgovarajuća razina zaštite tih podataka.

21 — C-293/12 i C-594/12, EU:C:2014:238, t. 65. do 69.

i 8. Povelje, pa bi Sud mogao smatrati da je Direktivu 95/46 i osobito njezin članak 25. stavak 6. kao i Odluku 2000/520 moguće tumačiti na način koji nacionalnim tijelima omogućava da provode vlastite istrage kako bi utvrdili zadovoljava li prijenos osobnih podataka trećoj zemlji zahtjeve koji proizlaze iz članaka 7. i 8. Povelje.

47. U tim je okolnostima Visoki sud odlučio prekinuti postupak i uputiti Sudu sljedeća prethodna pitanja:

„S obzirom na članke 7., 8. i 47. Povelje i ne dovodeći u pitanje odredbe članka 25. stavka 6. Direktive 95/46, je li prilikom odlučivanja o pritužbi u vezi s prenošenjem osobnih podataka u treću zemlju (u ovom slučaju SAD), u kojoj podnositelj pritužbe tvrdi da pravo i praksa ne pružaju odgovarajuću zaštitu osobi čiji se podaci obrađuju, povjerenik apsolutno vezan suprotnim stajalištem Unije koje je sadržano u Odluci 2000/520?

Ako nije, može li ili mora li provesti vlastitu istragu vodeći se činjeničnim razvojem događaja od kad je Odluka 2000/520 bila prvi puta objavljena?“

II – **Moja analiza**

48. Sud na temelju pitanja koje je postavio Visoki sud mora precizirati ovlasti nacionalnih nadzornih tijela kada odlučuju o pritužbi u vezi s prijenosom osobnih podataka u poduzeće koje ima sjedište u trećoj zemlji i za koju se tvrdi, u potporu toj pritužbi, da ne jamči odgovarajuću razinu zaštite prenesenih podataka, čak i kada je Komisija, na temelju članka 25. stavka 6. Direktive 95/46 donijela odluku koja priznaje odgovarajuću razinu zaštite koju osigurava navedena treća zemlja.

49. Moram primijetiti da pritužba koju je M. Schrems podnio povjereniku ima dvije dimenzije. Ona ima za cilj pobijati prijenos osobnih podataka iz Facebooka Irska u Facebook SAD. M. Schrems traži da se prekine taj prijenos jer SAD prema njegovu mišljenju ne osigurava odgovarajuću zaštitu osobnih podataka koji su preneseni u okviru sustava „sigurne luke“. Konkretno, on prigovara SAD-u da je uspostavio program PRISM koji je omogućio NSA-i slobodno pristupanje masovnim podacima pohranjenima na poslužiteljima smještenima u SAD-u. Pritužba se tako posebno odnosi na prijenos osobnih podataka iz Facebooka Irska u Facebook SAD, pri čemu ona na općenitiji način dovodi u pitanje razinu zaštite koja je osigurana tim podacima u okviru sustava „sigurne luke“.

50. Povjerenik smatra da ga samo postojanje Odluke Komisije koja priznaje da SAD osigurava, u okviru sustava „sigurne luke“, odgovarajuću razinu zaštite, sprečava u ispitivanju pritužbe.

51. Stoga treba zajedno ispitati ta dva pitanja, koja su u bitnome usmjerena na to treba li članak 28. Direktive 95/46 u vezi s člancima 7. i 8. Povelje tumačiti na način da postojanje odluke koju je donijela Komisija na temelju članka 25. stavka 6. te direktive ima takav učinak da onemogućava nacionalno nadzorno tijelo da ispita pritužbu u kojoj se navodi da treća zemlja ne osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka i da po potrebi suspendira prijenos tih podataka.

52. Članak 7. Povelje jamči pravo na poštovanje privatnog života, dok članak 8. iste izričito proglašava pravo na zaštitu osobnih podataka. Članak 8. stavci 2. i 3. preciziraju da se takvi podaci moraju obrađivati pošteno, u utvrđene svrhe i na temelju pristanka osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom, da svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje te da poštovanje tih pravila podliježe nadzoru neovisnog tijela.

A – *Ovlasti nacionalnih nadzornih tijela u slučaju Odluke Komisije o primjerenosti*

53. Kao što je u svojim očitovanjima naveo M. Schrems za potrebe pritužbe o kojoj je riječ u glavnom postupku, središnje pitanje je pitanje prijenosa osobnih podataka iz Facebooka Irska u Facebook SAD u svjetlu općenitog pristupa NSA-e i drugih američkih sigurnosnih agencija podacima pohranjenima kod Facebooka SAD na temelju ovlasti koje im povjerava američko zakonodavstvo.

54. Nacionalno nadzorno tijelo, kojem je podnesena pritužba radi pobijanja tvrdnje da treća zemlja osigurava odgovarajuću razinu zaštite prenesenih podataka, je prema mišljenju M. Schremsa ovlašteno da, ako raspolaže s dovoljno elemenata za osnovanost tvrdnji sadržanih u toj pritužbi, naloži suspenziju prijenosa podataka koji vrši poduzeće na koje se upućuje u navedenoj pritužbi.

55. S obzirom na obveze povjerenika da štiti temeljna prava M. Schremsa, M. Schrems tvrdi da povjerenik ima obvezu ne samo istražiti već također, ako je pritužba usvojena, iskoristiti svoje ovlasti da suspendira protok podataka između Facebooka Irska i Facebooka SAD.

56. Međutim, povjerenik je odbio pritužbu na osnovi odredaba Zakona o zaštiti podataka u kojem su nabrojane njegove ovlasti. Taj zaključak je utemeljen na stajalištu povjerenika da je vezan Odlukom 2000/520.

57. Iz toga proizlazi da je središnji problem u ovom predmetu pitanje veže li ocjena Komisije koja se odnosi na odgovarajuću razinu zaštite sadržana u Odluci 2000/520 apsolutno nacionalno tijelo za zaštitu podataka i sprečava li ga da ispita tvrdnje koje osporavaju to utvrđenje. Prethodna se pitanja odnose stoga na doseg istražnih ovlasti nacionalnih tijela za zaštitu podataka kada postoji Odluka Komisije o primjerenosti.

58. Prema mišljenju Komisije treba uzeti u obzir odnos među ovlasti Komisije i ovlasti nacionalnih tijela za zaštitu podataka. Nadležnosti potonjih koncentrirane su na primjenu relevantnog zakonodavstva na pojedinačne slučajeve, dok općenito preispitivanje Odluke 2000/520, uključujući svaku odluku o njezinoj odgodi ili ukidanju, potpada pod nadležnost Komisije.

59. Komisija tvrdi da M. Schrems nije naveo posebne argumente koji bi dokazali da je postojala trenutačna opasnost da mu se ozbiljno našteti zbog prijenosa podataka između Facebooka Irska i Facebooka SAD. Upravo suprotno, zbog njihove apstraktne i općenite naravi, zabrinutost koju je izrazio M. Schrems u pogledu programa nadzora koje provode američke sigurnosne agencije jednaka je onoj koja je navela Komisiju da pokrene preispitivanje Odluke 2000/520.

60. Prema mišljenju Komisije, nacionalna nadzorna tijela bi posegnula za njezinim nadležnostima za ponovno pregovaranje o uvjetima te odluke sa SAD-om ili, po potrebi, za njezinu suspenziju, ako bi poduzimala mjere na osnovi pritužbi koje sadržavaju samo strukturalne i apstraktne zabrinutosti.

61. Ne slažem se s mišljenjem Komisije. Smatram da postojanje odluke koju je donijela Komisija na temelju članka 25. stavka 6. Direktive 95/46 ne smije ni ukinuti ni smanjiti ovlasti kojima raspolažu nacionalna nadzorna tijela na temelju članka 28. te direktive. Protivno tvrdnjama Komisije, smatram da ako je pred nacionalnim nadzornim tijelima podnesena pojedinačna pritužba, to ih ne sprečava da na temelju njihovih istražnih ovlasti i njihove neovisnosti stvore vlastito mišljenje o općenitoj razini zaštite koju osigurava treća zemlja i da iz toga izvuku zaključke kada odlučuju o pojedinačnim slučajevima.

62. Iz ustaljene sudske prakse Suda proizlazi da, pri tumačenju odredbe prava Unije, u obzir treba uzeti ne samo njezin tekst, nego i kontekst u kojemu se nalazi te ciljeve propisa kojeg je dio [22].

22 — Vidjeti osobito presudu Koushkaki (C-84/12, EU:C:2013:862, t. 34. i navedena sudska praksa).

63. Iz uvodne izjave 62. Direktive 95/46 proizlazi da „osnivanje potpuno neovisnih nadzornih tijela u državama članicama osnovni [je] dio zaštite pojedinaca u vezi obrade osobnih podataka“.

64. Sukladno članku 28. stavku 1. prvom podstavku te direktive „[s]vaka država članica osigurava da je jedno ili više javnih tijela na njenom području odgovorno za nadzor primjene odredbi koje su donijele države članice u skladu s ovom direktivom“. Članak 28. stavak 1. drugi podstavak navedene direktive određuje da „[t]a tijela u provedbi funkcija koje su im povjerene djeluju potpuno neovisno“.

65. Članak 28. stavak 3. Direktive 95/46 nabraja ovlasti koje ima svako nacionalno nadzorno tijelo, to jest istražne ovlasti, učinkovite ovlasti za posredovanje koje mu omogućavaju da nametne privremenu ili konačnu zabranu obrade kao i ovlast za sudjelovanje u sudskim postupcima ako su prekršene nacionalne odredbe donesene u skladu s ovom direktivom ili za upoznavanje sudskih tijela s tim kršenjima.

66. Osim toga, na temelju članka 28. stavka 4. prvog podstavka Direktive 95/46 „[s]vako nadzorno tijelo razmatra zahtjeve koje podnese bilo koja osoba […] u vezi zaštite njezinih prava i sloboda u odnosu na obradu osobnih podataka“. Članak 28. stavak 4. drugi podstavak te direktive precizira da „[s]vako nadzorno tijelo posebno razmatra zahtjev za provjeru zakonitosti obrade podataka koji preda bilo koja osoba kada se primjenjuju nacionalne odredbe donesene u skladu s člankom 13. [navedene] direktive. Pojašnjavam da potonja odredba državama članicama omogućava da poduzmu zakonodavne mjere za ograničavanje dosega nekoliko obveza i prava predviđenih u Direktivi 95/46 kada je takvo ograničenje mjera potrebno za očuvanje, među ostalim, državne sigurnosti, obrane, javne sigurnosti te prevencije, istrage, utvrđivanja i progona kaznenih djela.

67. Kao što je Sud već naveo, zahtjev da neovisno tijelo nadzire poštovanje pravila Unije o zaštiti fizičkih osoba u vezi s obradom osobnih podataka također proizlazi iz primarnog prava Unije, osobito iz članka 8. stavka 3. Povelje i članka 16. stavka 2. UFEU-a [23]. Sud je također naveo da „ [u]spostava neovisnih nadzornih nacionalnih tijela u državama članicama stoga čini bitan dio poštovanja zaštite fizičkih osoba u vezi s obradom osobnih podataka“ [24].

68. Sud je također presudio da „članak 28. stavak 1. drugi podstavak Direktive 95/46 treba tumačiti na način da nacionalna nadzorna tijela nadležna za nadzor nad obradom osobnih podataka trebaju biti neovisna, što im omogućuje ispunjavanje njihovih zadataka bez izvanjskog utjecaja. Ta neovisnost, među ostalim, isključuje svaki nalog te bilo kakav drugi izvanjski utjecaj u bilo kojem obliku, bilo izravan ili neizravan, koji bi mogao utjecati na njihove odluke i koji bi također mogao dovesti u pitanje izvršavanje zadatka nacionalnih tijela koji se sastoji u uspostavi pravilne ravnoteže između prava na privatni život i slobodnog kretanja osobnih podataka“ [25].

69. Sud je također precizirao da „[j]amstvo neovisnosti nacionalnih nadzornih tijela nastoji osigurati učinkovitost i pouzdanost nadzora poštovanja odredaba u području zaštite fizičkih osoba u pogledu obrade osobnih podataka“ [26]. To jamstvo neovisnosti je uspostavljeno „kako bi ojačalo zaštitu osoba i tijela na koja se odnose odluke tih [nacionalnih nadzornih tijela]“ [27].

23 — Vidjeti presude Komisija/Austrija (C-614/10, EU:C:2012:631, t. 36.) i Komisija/Mađarska (C-288/12, EU:C:2014:237, t. 47.).

24 — Vidjeti osobito presudu Komisija/Mađarska (C-288/12, EU:C:2014:237, t. 48. i navedena sudska praksa). U tom smislu vidjeti također presudu Digital Rights Ireland i dr. (C-293/12 i C-594/12, EU:C:2014:238, t. 68. kao i navedena sudska praksa).

25 — Vidjeti osobito presudu Komisija/Mađarska (C-288/12, EU:C:2014:237, t. 51. i navedena sudska praksa).

26 — Presuda Komisija/Njemačka (C-518/07, EU:C:2010:125, t. 25.).

27 — *Idem.*

70. Kako to proizlazi, među ostalim, iz uvodne izjave 10. i članka 1. Direktive 95/46, svrha te direktive je unutar Unije jamčiti „visoku razinu zaštite sloboda i temeljnih prava u pogledu obrade osobnih podataka“ [28]. Prema mišljenju Suda „nadzorna tijela predviđena u članku 28. Direktive 95/46 su stoga zaštitnici navedenih temeljnih prava i sloboda“ [29].

71. Uzevši u obzir važnost uloge koju zauzimaju nacionalna nadzorna tijela u području zaštite fizičkih osoba u pogledu obrade osobnih podataka, njihove ovlasti za intervenciju moraju ostati nedirnute čak i kada Komisija donese odluku na temelju članka 25. stavka 6. Direktive 95/46.

72. U tom pogledu smatram da ništa ne upućuje na to da su sustavi prijenosa osobnih podataka u treću zemlju isključeni iz materijalnog područja primjene članka 8. stavka 3. Povelje koji postavlja na najvišu razinu hijerarhije normi prava Unije važnost nadzora koji vrši neovisno tijelo u pogledu poštovanja pravila o zaštiti osobnih podataka.

73. Ako bi nacionalna nadzorna tijela bila apsolutno vezana odlukama koje donosi Komisija, to bi nužno ograničavalo njihovu potpunu neovisnost. Sukladno njihovoj ulozi zaštitnika temeljnih prava, nacionalna nadzorna tijela moraju potpuno neovisno moći provoditi istrage, na zahtjeve koji su im upućeni, u prevladavajućem interesu zaštite pojedinaca u pogledu obrade osobnih podataka.

74. Osim toga, kao što su to na raspravi ispravno naveli belgijska vlada i Europski parlament, ne postoji nikakva hijerarhijska veza između Poglavlja IV. Direktive 95/46 o prijenosu osobnih podataka trećim zemljama i Poglavlja VI. te direktive koja uređuje, među ostalim, ulogu nacionalnih nadzornih tijela. Ništa u Poglavlju VI. ne upućuje na to da su odredbe o nacionalnim nadležnim tijelima podređene na bilo koji način posebnim odredbama o prijenosu navedenim u Poglavlju IV. Direktive 95/46.

75. S druge strane, iz članka 25. stavka 1. u Poglavlju IV. te direktive proizlazi da dozvola da se osobni podaci prenose trećoj zemlji koja osigurava odgovarajuću zaštitu vrijedi jedino ako se ne dovode u pitanje nacionalne odredbe donesene u skladu s drugim odredbama navedene direktive.

76. U tom pogledu treba podsjetiti da na temelju te odredbe, države članice moraju u svojim zakonodavstvima osigurati da odobrenje prijenosa osobnih podataka trećoj zemlji koja osigurava odgovarajuću razinu zaštite vrijedi jedino ako je, ne dovodeći u pitanje nacionalne odredbe, dano u skladu s drugim odredbama navedene direktive.

77. U skladu s člankom 28. stavkom 1. te direktive nacionalna nadzorna tijela na području svake države članice odgovorna su za nadzor primjene odredaba koje su donijele države članice u skladu s navedenom direktivom.

78. Usporedba te dvije odredbe omogućava da se zaključi da je pravilo iz članka 25. stavka 1. Direktive 95/46 prema kojem se osobni podaci mogu prenositi trećoj zemlji ako im treća zemlja primateljica osigurava odgovarajuću razinu zaštite, pripada pravilima čiju primjenu moraju nadzirati nacionalna nadzorna tijela.

79. U skladu s člankom 8. stavkom 3. Povelje, ovlasti nacionalnih nadzornih tijela da neovisno istražuju pritužbe pojedinaca koje su im podnesene na temelju članka 28. Direktive 95/46 treba široko tumačiti. Te ovlasti se stoga ne mogu ograničiti ovlastima koje je zakonodavac Unije povjerio Komisiji, na temelju članka 25. stavka 6. te direktive, kako bi se utvrdila odgovarajuća razina zaštite koju pruža treća zemlja.

28 — *Ibidem* (t. 22. i navedena sudska praksa).

29 — *Ibidem* (t. 23.). Vidjeti također u tom smislu Komisija/Austrija (C-614/10, EU:C:2012:631, t. 52.) i Komisija/Mađarska (C-288/12, EU:C:2014:237, t. 53.).

80. S obzirom na njihovu bitnu ulogu u području zaštite osobnih podataka, nacionalna nadzorna tijela moraju moći provesti istragu kada im je podnesena pritužba u kojoj se nalaze elementi koji bi mogli dovesti u pitanje razinu zaštite koju osigurava treća zemlja, uključujući i kada je Komisija, u odluci donesenoj na temelju članka 25. stavka 6. Direktive 95/46 zaključila da treća zemlja o kojoj je riječ osigurava odgovarajuću razinu zaštite.

81. Ako na kraju istraga koje je provelo nacionalno nadzorno tijelo, ono procijeni da osporavani prijenos podataka ugrožava zaštitu koju moraju uživati građani Unije u pogledu obrade njihovih podataka, ona ima ovlast suspendirati prijenos podataka u pitanju, bez obzira na opću procjenu Komisije u njezinoj odluci.

82. U skladu s člankom 25. stavkom 2. Direktive 95/46 nesporno je da se odgovarajuća razina zaštite koju pruža treća zemlja ocjenjuje prema svim činjeničnim i pravnim okolnostima. Ako se neka okolnost promijeni i čini se da dovodi u pitanje odgovarajuću razinu zaštite koju osigurava treća zemlja, nacionalno nadzorno tijelo pred kojim je podnesena pritužba mora iz toga moći izvući zaključke u odnosu na sporni prijenos.

83. Točno je, kako je navela Irska, da su povjerenik ali i ostala državna tijela vezani Odlukom 2000/520. Iz članka 288. četvrtog stavka UFEU-a naime proizlazi da je odluka koju je donijela institucija Unije u cijelosti obvezujuća. Posljedično, Odluka 2000/520 obvezuje države članice kojima je upućena.

84. U tom pogledu ističem da sama Odluka 2000/520 u svom članku 5. određuje da „[d]ržave članice poduzimaju sve mjere potrebne za usklađivanje s [njom] najkasnije u 90 dana od dana njezine objave u državama članicama“. Osim toga, članak 6. te odluke određuje da je „[ona] upućena državama članicama“.

85. Međutim, smatram da u pogledu gore navedenih odredaba iz Direktive 95/46 i Povelje, obvezujući učinak Odluke 2000/520 nije takav da isključuje svako povjerenikovo ispitivanje pritužbi u kojima se tvrdi da prijenos osobnih podataka izvršen prema SAD-u u okviru te odluke nije zadovoljavao potrebna jamstva zaštite koja zahtijeva pravo Unije. Drugim riječima, takav ograničavajući učinak nije takve naravi da nameće da se svaku pritužbu te vrste odbije po kratkom postupku, to jest odmah i bez ispitivanja njezine osnovanosti.

86. Dodajem da iz strukture članka 25. Direktive 95/46 osim toga proizlazi da utvrđenje poštuje li treća zemlja odgovarajuću razinu zaštite, donose ili države članice ili Komisija. Radi se stoga o podijeljenoj nadležnosti.

87. Iz članka 25. stavka 6. te direktive proizlazi da, kada Komisija utvrdi da treća zemlja osigurava odgovarajuću razinu zaštite u smislu članka 25. stavka 2. navedene direktive, države članice moraju poduzeti mjere potrebne za usklađivanje s odlukom Komisije.

88. Kako je učinak takve odluke dozvoliti prijenos osobnih podataka trećoj zemlji za koju Komisija smatra da osigurava odgovarajuću zaštitu, države članice moraju u načelu dozvoliti vršenje prijenosa poduzećima sa sjedištem na njihovom području.

89. Međutim, članak 25. Direktive ne dodjeljuje Komisiji isključivu nadležnost u području utvrđenja postoji li ili ne odgovarajuća razine zaštite prenesenih osobnih podataka. Iz strukture tog članka vidljivo je da države članice također imaju važnu ulogu u tom području. Točno je da Komisija ima važnu ulogu u ujednačavanju uvjeta prijenosa koji su valjani unutar država članica. Međutim, to ujednačavanje može trajati samo dok se to utvrđenje ne dovede u pitanje.

90. Argument da je nužno ujednačavanje uvjeta prijenosa osobnih podataka trećoj zemlji, po mom je mišljenju ograničen u situaciji kao što je ova u glavnom postupku, gdje ne samo da je Komisija obaviještena o tome da se njeno utvrđenje kritizira već i ona sama upućuje takve kritike i vodi pregovore da se situacija popravi.

91. Ocjena je li razina zaštite koju osigurava treća zemlja odgovarajuća ili ne može također dovesti i do suradnje između država članica i Komisije. Članak 25. stavak 3. Direktive u tom pogledu predviđa da se „[d]ržave članice i Komisija međusobno […] obavješćuju o slučajevima za koje smatraju da treća zemlja ne osigurava odgovarajuću razinu zaštite u smislu stavka 2. ovog članka“. Kao što to navodi Parlament, to jasno pokazuje da države članice i Komisija imaju jednakovrijednu ulogu pri otkrivanju koja treća zemlja ne osigurava odgovarajuću razinu zaštite.

92. Odluka o primjerenosti ima za cilj dozvoliti prijenos osobnih podataka dotičnoj trećoj zemlji. To ne znači da građani Unije više ne mogu pred nacionalnim nadzornim tijelima podnijeti pritužbu čija je svrha zaštititi njihove osobne podatke. U tom pogledu navodim da članak 28. stavak 4. prvi podstavak Direktive 95/46 prema kojem „[s]vako nadzorno tijelo razmatra zahtjeve koje podnese bilo koja osoba […] u vezi zaštite njezinih prava i sloboda u odnosu na obradu osobnih podataka“, ne predviđa iznimku od tog načela u slučaju da postoji odluka Komisije u skladu s člankom 25. stavkom 6. te direktive.

93. Tako, iako odluka Komisije u skladu s izvršnim ovlastima koje im povjerava potonja odredba ima učinak dozvoliti prijenos osobnih podataka trećoj zemlji, takva odluka s druge strane ne smije imati učinak da državama članicama oduzme sve ovlasti a osobito njihovim nacionalnim nadzornim tijelima, čak niti da samo ograniči njihove ovlasti kada su suočeni s navodima o povredi temeljnih prava.

94. Nacionalno nadzorno tijelo mora biti u stanju izvršavati svoje ovlasti predviđene u članku 28. stavku 3. Direktive 95/46, kao što je ovlast privremene ili konačne zabrane obrade osobnih podataka. Iako nabrojane ovlasti iz te odredbe ne predviđaju izričito ovlasti u vezi s prijenosom iz države članice trećoj zemlji, takav prijenos po mojem mišljenju treba smatrati obradom podataka [30]. Kao što to proizlazi iz teksta navedene odredbe, nabrajanje nije iscrpno. U svakom slučaju, s obzirom na bitnu ulogu koju nacionalna nadzorna tijela imaju u sustavu uspostavljenom Direktive 95/46, ona moraju imati ovlast suspenzije prijenosa podataka u slučaju dokazane povrede ili rizika povrede temeljnih prava.

95. Dodajem da bi lišenje nacionalnog nadzornog tijela njegovih istražnih ovlasti u okolnostima poput onih o kojima je riječ u ovom postupku, bilo protivno ne samo načelu neovisnosti već i cilju Direktive 95/46 kao što to proizlazi iz njezina članka 1. stavka 1.

96. Kako je naveo Sud „[i]z uvodnih izjava 3., 8. i 10. Direktive 95/46 proizlazi da je zakonodavac Unije htio olakšati slobodni protok osobnih podataka približavanjem zakonodavstava država članica uz zaštitu temeljnih prava osoba, osobito pravo na privatni život, i uz jamstvo visokog stupnja zaštite u Uniji. Članak 1. te direktive tako predviđa da države članice moraju osigurati zaštitu sloboda i temeljnih prava fizičkih osoba, osobito njihovog privatnog života, u pogledu obrade osobnih podataka“ [31].

97. Odredbe Direktive 95/46 stoga se moraju tumačiti u skladu s ciljem te direktive koji želi osigurati visoku razinu zaštite sloboda i temeljnih prava fizičkih osoba, osobito njihovog privatnog života u pogledu obrade osobnih podataka unutar Unije.

30 — Vidjeti mišljenje nezavisnog odvjetnika Légera u predmetu Parlament/Vijeće i Komisija (C-317/04, EU:C:2005:710, t. 92. do 95.). Vidjeti također presudu Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346, t. 56.).

31 — Vidjeti osobito presudu IPI (C-473/12, EU:C:2013:715, t. 28. i navedena sudska praksa).

98. Važnost tog cilja i uloge koje države članice moraju imati da bi se on ostvario znači da, kada posebne okolnosti dovedu do ozbiljne sumnje o poštovanju temeljnih prava koje jamči Povelja u slučaju prijenosa osobnih podataka trećoj zemlji, države članice i stoga unutar njih nacionalna nadzorna tijela ne mogu biti apsolutno vezani Komisijinom odlukom o primjerenosti.

99. Sud je već presudio da „se odredbe Direktive 95/46, koje uređujući obradu osobnih podataka mogu povrijediti temeljne slobode i posebno pravo na privatnost, nužno moraju tumačiti u svjetlu temeljnih prava koja prema ustaljenoj sudskoj praksi čine sastavni dio općih načela prava čije poštovanje Sud osigurava i koja su upisana u Povelju“ [32].

100. Osim toga upućujem na sudsku praksu prema kojoj „na državama članicama je ne samo da tumače svoje nacionalno pravo u skladu s pravom Unije nego i da skrbe da se ne temelje na tumačenju teksta sekundarnog prava koje bi bilo u sukobu s temeljnim pravima ili s drugim općim načelima prava Unije“ [33].

101. Sud je tako već presudio u presudi N. S. i dr. [34] da „primjena Uredbe [(EZ)] br. 343/2003 [35] na temelju neoborive pretpostavke da će država članica koja je inače nadležna za rješavanje zahtjeva za azil, poštovati temeljna prava, nije sukladna obvezi država članica da tumače i primjenjuju Uredbu br. 343/2030 u skladu s temeljnim pravima“ [36].

102. U tom pogledu, Sud je priznao da se, u kontekstu statusa države članice kao sigurne države podrijetla u odnosu na druge, za pravna pitanja i prakse u vezi s pravom azila, treba pretpostavljati da je obrada zahtjeva tražitelja azila u svakoj državi članici u skladu sa zahtjevima Povelje, Konvencije o statusu izbjeglica koja je potpisana u Ženevi 28. srpnja 1951. [37], kao i Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda, koja je potpisana u Rimu 4. studenoga 1950. [38]. Međutim, Sud je presudio da „[s]e ne može […] isključiti da će taj sustav u praksi imati velike poteškoće pri funkcioniranju u određenoj državi članici, tako da postoji ozbiljna opasnost da će se pri prebacivanju tražitelja azila u tu državu članicu prema njima postupati na način koji nije u skladu s njihovim temeljnim pravima“ [39].

103. Posljedično, Sud je presudio da „države članice, uključujući nacionalne sudove ne smiju prebaciti tražitelja azila u ‚odgovornu državu članicu' u smislu Uredbe br. 343/2003 kada ne mogu ignorirati da sustavne nepravilnosti u postupku azila i uvjeti prihvata tražitelja azila u toj državi članici predstavljaju ozbiljne i utvrđene razloge za vjerovanje da će tražitelj biti izložen stvarnoj opasnosti od podvrgavanja neljudskom i ponižavajućem postupanju u smislu članka 4. Povelje“ [40].

104. Čini mi se da se doprinos presude N. S. i dr. [41] može proširiti na situaciju poput one o kojoj je riječ u glavnom postupku. Za tumačenje sekundarnog prava Unije koje se temelji na neoborivoj pretpostavki da će država članica, Komisija ili treća država poštovati temeljna prava, mora se smatrati da je neusklađena s obvezom država članica da sekundarno pravo Unije tumače i primjenjuju na način koji je sukladan temeljnim pravima. Članak 25. stavak 6. Direktive 95/46 ne nalaže takvu neoborivu pretpostavku poštovanja temeljnih prava u pogledu Komisijine ocjene odgovarajuće razine zaštite koju

32 — Vidjeti osobito presudu Google Španjolska (C-131/12, EU:C:2014:317, t. 68. i navedena sudska praksa).

33 — Vidjeti osobito presudu N. S. i dr. (C-411/10 i C-493/10, EU:C:2011:865, t. 77. kao i navedena sudska praksa).

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

35 — Uredba Vijeća (EZ) br. 343/2003 od 18. veljače 2003. o utvrđivanju kriterija i mehanizama za određivanje države članice odgovorne za razmatranje zahtjeva za azil koji je u jednoj od država članica podnio državljanin treće zemlje (SL L 50, str. 1) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 19., svezak 12., str. 37.).

36 — Točka 99. te presude.

37 — *Zbornik ugovora Ujedinjenih naroda, sv. 189., str. 150., br. 2545 (1954).*

38 — Vidjeti presudu N. S. i dr. (C-411/10 i C-493/10, EU:C:2011:865, t. 80.).

39 — *Ibidem* (t. 81.).

40 — *Ibidem* (t. 94.).

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

osigurava treća zemlja. Upravo suprotno, pretpostavka koja je u osnovi te odredbe da prijenos podataka trećoj zemlji poštuje temeljna prava, treba se smatrati oborivom [42]. Posljedično, ta se odredba ne smije tumačiti na način da dovodi u pitanje jamstva koja su određena, među ostalim, u članku 28. stavku 3. Direktive 95/46 i u članku 8. stavku 3. Povelje, koja imaju za cilj zaštitu i poštovanje osobnih podataka.

105. Iz navedene presude stoga zaključujem da u slučaju sustavnih nepravilnosti u trećim zemljama kamo su preneseni osobni podaci, države članice moraju moći poduzeti nužne mjere za zaštitu temeljnih prava iz članaka 7. i 8. Povelje.

106. Osim toga, kao što je navela talijanska vlada u svojim očitovanjima, Komisijino donošenje odluke o primjerenosti ne može imati takav učinak da smanji zaštitu građana Unije u pogledu obrade njihovih podataka kada se prenose u treće zemlje u odnosu na razinu zaštite koje bi te osobe uživale da se njihovi podaci obrađuju unutar Unije. Nacionalna nadzorna tijela posljedično moraju moći intervenirati i vršiti svoje ovlasti u pogledu prijenosa podataka u treće zemlje koje su predmet odluke o primjerenosti. U suprotnom slučaju bi građani Unije bili slabije zaštićeni nego u slučaju obrade njihovih podataka unutar Unije.

107. Tako Komisijino donošenje odluke o primjerenosti u skladu s člankom 25. stavkom 6. Direktive 95/46 ima učinak da samo uklanja opću zabranu izvoza osobnih podataka trećim zemljama koje imaju sličnu razinu zaštite kao što je utvrđeno tom direktivom. Drugim riječima, ne radi se o tome da se stvori poseban sustav izuzeća koji bi građanima Unije pružao manju zaštitu u odnosu na opći sustav koji predviđa navedena direktiva o obradi podataka unutar Unije.

108. Točno je da je Sud u točki 63. presude Lindqvist uputio [43] da „[p]oglavlje IV. Direktive 95/46 u kojem se nalazi članak 25. uspostavlja poseban sustav“. Međutim, to prema mom mišljenju ne znači da takav sustav mora pružati manju zaštitu. Naprotiv, kako bi se postigao cilj zaštite podataka utvrđen u članku 1. stavku 1. Direktive 95/46, članak 25. te direktive utvrđuje niz obveza za države članice i Komisiju [44] i postavlja načelo prema kojem, kada treće zemlje ne pružaju odgovarajuću razinu zaštite, prijenos osobnih podataka trećim zemljama mora biti zabranjen [45].

109. Što se, konkretno, tiče sustava „sigurne luke“ Komisija smatra da nacionalna nadzorna tijela mogu intervenirati i suspendirati protok podataka samo u okviru utvrđenom u članku 3. stavku 1. točki (b) Odluke 2000/520.

110. Prema uvodnoj izjavi 8. te odluke „[u] interesu transparentnosti i radi zaštite sposobnosti nadležnih tijela u državama članicama da osiguraju zaštitu pojedinaca s obzirom na obradu njihovih osobnih podataka, potrebno je u ovoj odluci navesti iznimne okolnosti u kojima suspenzija određenih protoka podataka može biti opravdana, neovisno o pronalaženju primjerene zaštite“.

111. U okviru ovog predmeta osobito se raspravljalo o primjeni članka 3. stavka 1. točke (b) navedene odluke. Tako na temelju te odredbe nacionalna nadzorna tijela mogu odlučiti o suspenziji protoka podataka u slučajevima „da postoji stvarna vjerojatnost da se krše načela; ako postoje opravdani razlozi da se vjeruje da dotični mehanizam provedbe ne poduzima ili neće poduzeti primjerene i pravovremene korake da razriješi dotični slučaj; ako bi nastavak prijenosa stvorio trenutačnu opasnost da ozbiljno našteti osobama čiji se podaci obrađuju, te ako su nadležna tijela država članica poduzela odgovarajuće napore da u tim okolnostima obavijeste organizaciju i dala joj mogućnost da se očituje“.

42 — Točka 104. te presude.

43 — C-101/01, EU:C:2003:596.

44 — Točka 65.

45 — Točka 64.

112. Navedena odredba postavlja više uvjeta koje su stranke u ovom postupku različito tumačile [46]. Bez ulaženja u detalje tih tumačenja, iz njih proizlazi da ti uvjeti strogo propisuju ovlast nacionalnih nadzornih tijela da suspendiraju protok podataka.

113. Međutim, suprotno tvrdnjama Komisije, članak 3. stavak 1. točka (b) Odluke 2000/520 mora se tumačiti u skladu s ciljem zaštite osobnih podataka koji se nastoji postići Direktivom 95/46 kao i u vezi s člankom 8. Povelje. Nužnost tumačenja u skladu s temeljnim pravima podupire široko tumačenje te odredbe.

114. Iz toga slijedi da uvjeti koji su predviđeni u članku 3. stavku 1. točki (b) Odluke 2000/520 po mojem mišljenju ne mogu spriječiti nacionalno nadležno tijelo da neovisno vrši ovlasti koje su mu dodijeljene u članku 28. stavku 3. Direktive 95/46.

115. Kao što su u bitnome na raspravi navele belgijska i austrijska vlada, izlaz za slučaj nužde koji predstavlja članak 3. stavak 1. točke (b) Odluke 2000/520 je toliko uzak da ga je teško provesti u praksu. On određuje kumulativne kriterije i postavlja ljestvicu previsoko. U vezi s člankom 8. stavkom 3. Povelje, manevarski prostor nacionalnih nadzornih tijela koji se odnosi na ovlasti koje proizlaze iz članka 28. stavka 3. Direktive 95/46, ne smije biti tako ograničen da se te ovlasti više ne mogu koristiti.

116. U tom pogledu, Parlament je ispravno primijetio da je zakonodavac Unije taj koji je odlučio koje ovlasti trebaju imati nacionalna nadzorna tijela. Izvršne ovlasti koje je zakonodavac Unije dodijelio Komisiji u članku 25. stavku 6. Direktive 95/46 ne utječu na ovlasti koje je taj isti zakonodavac dodijelio nacionalnim nadzornim tijelima u članku 28. stavku 3. te direktive. Drugim riječima, Komisija nije nadležna za ograničavanje ovlasti nacionalnim nadzornim tijelima.

117. Posljedično, kako bi se osigurala odgovarajuća zaštita temeljnih prava fizičkih osoba u pogledu obrade osobnih podataka, nacionalna nadležna tijela moraju biti ovlaštena provoditi istrage kada postoje tvrdnje o povredama tih prava. Ako nakon provođenja istrage ta tijela smatraju da u trećoj zemlji obuhvaćenom odlukom o primjerenosti postoje ozbiljni indiciji o povredi prava građana Unije na zaštitu njihovih privatnih podataka, ona moraju suspendirati prijenos podataka adresatu koji ima sjedište u toj trećoj zemlji.

118. Drugim riječima, nacionalna nadzorna tijela moraju moći provoditi svoje istrage i po potrebi suspendirati prijenos podataka, bez obzira na restriktivne uvjete utvrđene u članku 3. stavku 1. točki (b) Odluke 2000/520.

119. Nacionalna nadzorna tijela moraju osim toga moći, na temelju ovlasti za sudjelovanje u sudskim postupcima, ako su prekršene nacionalne odredbe donesene u skladu s Direktivom 95/46 ili za upoznavanje sudskih tijela s tim povredama, kada saznaju za činjenice koje dokazuju da treća zemlja ne osigurava odgovarajuću razinu zaštite, pokrenuti postupak pred nacionalnim sudom koji po potrebi može odlučiti uputiti Sudu zahtjev za prethodnu odluku kako bi ocijenio valjanost Komisijine odluke o primjerenosti.

120. Iz tih svih elemenata proizlazi da se članak 28. Direktive 95/46 u vezi s člancima 7. i 8. Povelje mora tumačiti u smislu da postojanje odluke koju je donijela Komisija na temelju članka 25. stavka 6. te direktive nema učinak spriječiti nacionalno nadzorno tijelo da ispita pritužbu u kojoj se tvrdi da treća zemlja ne osigurava odgovarajuću razinu zaštite prenesenim osobnim podacima i, po potrebi, suspendirati prijenos tih podataka.

46 — Prema mišljenju M. Schremsa, prvi uvjet prema kojem je „postoji stvarna vjerojatnost da se krše načela“ nije ispunjen. Nije navedeno da Facebook SAD kao tijelo koje je provelo vlastito potvrđivanje i kojem su preneseni podaci, sâmo povrijedilo načela „sigurne luke“ time što su američke vlasti masovno i neselektivno pristupile podacima koje on ima. Naime, načela „sigurne luke“ izričito su ograničena američkim pravom, a definirana su u Prilogu I. četvrtom stavku Odluke 2000/520 upućivanjem na zakonske tekstove, upravne propise i sudske odluke.

121. Iako Visoki sud u odluci kojom se upućuje prethodno pitanje naglašava da M. Schrems u tužbi u glavnom postupku nije formalno pobijao ni valjanost Direktive 95/46 ni valjanost Odluke 2000/520, iz te odluke kojom se upućuje prethodno pitanje proizlazi da glavna kritika koju je izrazio M. Schrems ima za cilj dovesti u pitanje utvrđenje prema kojem SAD u okviru sustava „sigurne luke“ osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka.

122. Iz očitovanja povjerenika također proizlazi da pritužba M. Schremsa ima za cilj dovesti u pitanje neposredno Odluku 2000/520. Podnoseći pritužbu, M. Schrems je želio pobiti izričaje i funkcioniranje sustava „sigurna luke“ kao takvog jer masovno nadziranje osobnih podataka prenesenih u SAD pokazuje da ne postoji prava zaštita tih podataka u pravu i u praksi koji su na snazi u toj trećoj zemlji.

123. Štoviše, sam sud koji je uputio zahtjev navodi da bi jamstvo koje je pruženo u članku 7. Povelje i u temeljnim vrijednostima koje su zajedničke tradicijama država članica bilo ugroženo ako bi javnim vlastima bilo dopušteno nasumično i općenito pristupati elektroničkim komunikacijama a da nisu dužna dati nikakvo objektivno opravdanje utemeljeno na razlozima nacionalne sigurnosti ili sprečavanja kriminaliteta koji su posebno povezani s dotičnim pojedincima i da te prakse nisu popraćene odgovarajućim i provjerljivim jamstvima [47]. Sud koji je uputio zahtjev je tako posredno izrazio sumnje o valjanosti Odluke 2000/520.

124. Ocjena pitanja jamči li SAD u okviru sustava „sigurne luke“ odgovarajuću razinu zaštite osobnih podataka nužno dovodi do razmatranja valjanosti te odluke.

125. U tom pogledu treba navesti da, u okviru instrumenta suradnje između Suda i nacionalnih sudova koji je uspostavljan u članku 267. UFEU-a, čak i u slučaju kada je pokrenut postupak isključivo zbog prethodnog pitanja o tumačenju prava Unije, Sud u određenim posebnim okolnostima može zaključiti da je potrebno ispitati valjanost odredaba sekundarnog prava.

126. Stoga je Sud u nekoliko navrata po službenoj dužnosti poništio akt za koji se od njega tražilo samo tumačenje [48]. Sud je također presudio da „budući da se čini da se pravi predmet pitanja koja je postavio nacionalni sud odnosi više na ispitivanje valjanosti nego na tumačenje akata [Unije], dužnost je Suda da to odmah pojasni navedenom sudu ne zahtijevajući od njega ispunjavanje formalnosti koja samo odugovlači postupak i koja je nespojiva sa samom naravi mehanizama uspostavljenih člankom [267. UFEU-a]” [49]. Osim toga, Sud je već odlučio da se sumnje suda koji je uputio zahtjev o usklađenosti akta sekundarnog prava s pravilima zaštite temeljnih prava moraju shvatiti tako da dovode u pitanje valjanost tog akta u svjetlu prava Unije [50].

127. Podsjećam također da iz sudske prakse Suda proizlazi da akti institucija, tijela i ureda uživaju pretpostavku valjanosti što znači da oni proizvode pravne učinke sve dok ih se ne povuče, poništi u okviru tužbe za poništenje ili proglasi nevaljanim povodom zahtjeva za prethodnu odluku ili prigovora nezakonitosti. Jedino je Sud nadležan za utvrđivanje nevaljanosti akta Unije, a cilj te nadležnosti je jamčiti pravnu sigurnost osiguranjem ujednačene primjene prava Unije. Ako Komisija nije proglasila akt nevaljanim, nije ga izmijenila niti ukinula, odluka ostaje obvezujuća u cijelosti i neposredno se primjenjuje u svim državama članicama [51].

128. Kako bi se dao potpun odgovor sudu koji je uputio zahtjev i kako bi se riješile sumnje o valjanosti Odluke 2000/520 koje su izražene tijekom ovog postupka, smatram da bi Sud trebao ocijeniti valjanost te odluke.

47 — Točka 24. zahtjeva za prethodnu odluku.

48 — Vidjeti osobito presude Strehl (62/76, EU:C:1977:18, t. 10. do 17.); Roquette Frères (145/79, EU:C:1980:234, t. 6.), kao i Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, t. 32. do 39.).

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

50 — Vidjeti presudu Hauer (44/79, EU:C:1979:290, t. 16.).

51 — Vidjeti osobito presudu CIVAD (C-533/10, EU:C:2012:347, t. 39. do 41. i navedena sudska praksa).

129. S obzirom na navedeno, također treba pojasniti da se ispitivanje pitanja valjanosti ili nevaljanosti Odluke 2000/520 treba ograničiti na prigovore o kojima se raspravljalo u okviru ovog postupka. Naime, u ovom okviru nije se raspravljalo o svim aspektima koji se odnose na funkcioniranje sustava „sigurne luke“ i zato mi se ne čini da se ovdje mogu iscrpno ispitivati nedostatnosti tog sustava.

130. S druge strane, pred Sudom se u okviru ovog postupka raspravljalo o pitanju može li opći i neciljani pristup američkih obavještajnih službi prenesenim podacima utjecati na zakonitost Odluke 2000/520. Valjanost te odluke može se stoga ocjenjivati s tog gledišta.

B – *O valjanosti Odluke 2000/520*

1. Elementi koji se trebaju uzeti u obzir pri ocjeni valjanosti Odluke 2000/520

131. Treba podsjetiti na sudsku praksu prema kojoj „u okviru tužbe za poništenje, zakonitost akta se treba ocjenjivati s obzirom na činjenične i pravne elemente koji su postojali kada je akt donesen, ocjena Komisije podložna je kritici samo ako se pokaže očito pogrešnom s obzirom na elemente kojima je ona raspolagala u vrijeme donošenja predmetnog akta“ [52].

132. U svojoj presudi Gaz de France – Berliner Investissement [53], Sud je podsjetio na načelo prema kojem „ocjena valjanosti akta koju Sud provodi u okviru zahtjeva za prethodnu odluku, treba u pravilu biti utemeljena na okolnostima koje su postojale u trenutku donošenja akta“ [54]. Međutim, čini se da je Sud dopustio da se „u određenim slučajevima valjanost akta može ocjenjivati s obzirom na nove elemente koji su nastali nakon donošenja akta“ [55].

133. To otvaranje koje je Sud naznačio čini mi se posebno važnim u okviru ovog postupka.

134. Naime, odluke koje je donijela Komisija na temelju članka 25. stavka 6. Direktive 95/46 imaju posebne značajke. One su namijenjene ocjeni je li razina zaštite osobnih podataka koju osigurava treća zemlja odgovarajuća. Radi se o ocjeni koja će se mijenjati s obzirom na činjenični i pravni kontekst koji prevladava u trećoj zemlji.

135. S obzirom na činjenicu da odluka o primjerenosti predstavlja posebnu vrstu odluke, pravilo prema kojem se ocjena njezine valjanosti može izvršavati samo s obzirom na elemente koji postoje u trenutku njenog donošenja u ovom se slučaju mora prilagoditi. U protivnom bi takvo pravilo dovelo do toga da više godina nakon donošenja odluke o primjerenosti, ocjena valjanosti koju Sud mora izvršiti ne može uzeti u obzir događaje koji su nastupili kasnije i to čak i kada zahtjev za prethodnu odluku radi ocjene valjanosti nije vremenski ograničen i moguće ga je podnijeti zbog naknadnih činjenica koje upućuju na nedostatke akta o kojem je riječ.

136. U ovom slučaju, činjenica da je Odluka 2000/520 ostala na snazi otprilike 15 godina svjedoči o tome da je Komisija implicitno potvrdila svoju ocjenu iz 2000. Kada se u okviru zahtjeva za prethodnu odluku od Suda traži da ocijeni valjanost ocjene Komisije koja se održala duže vrijeme, ne samo da je moguće već je i primjereno da Sud usporedi tu ocjenu s novim okolnostima koje su nastupile od donošenja odluke o primjerenosti.

52 — Vidjeti osobito presudu BVGD/Komisija (T-104/07 i T-339/08, EU:T:2013:366, t. 291.), koja upućuje na presudu IECC/Komisija (C-449/98 P, EU:C:2001:275, t. 87.).

53 — C-247/08, EU:C:2009:600.

54 — Točka 49. i navedena sudska praksa.

55 — Točka 50. i navedena sudska praksa. Vidjeti u tom smislu Lenaerts, K., Maselis, I., i Gutman, K., *EU Procedural Law*, Oxford University Press, 2014 koji navode da „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” (t. 10.16, str. 471.).

137. Vodeći računa o posebnoj naravi odluke o primjerenosti, Komisija ju mora redovito preispitivati. Ako uslijed novih elemenata koji su nastupili u međuvremenu Komisija ne promijeni svoju odluku, to znači da ona implicitno ali nužno potvrđuje početnu ocjenu. Ona tako ponavlja svoje utvrđenje da treća zemlja o kojoj je riječ osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka. Na Sudu je da ispita je li to utvrđenje i dalje valjano unatoč okolnostima koje su naknadno uslijedile.

138. Kako bi se osigurao učinkovit sudski nadzor te vrste odluka, smatram da se ocjena njezine valjanosti treba izvršiti tako da se uzima u obzir trenutačni činjenični i pravni kontekst.

2. Pojam odgovarajuća razina zaštite

139. Članak 25. Direktive 95/46 u potpunosti počiva na načelu prema kojem se prijenos osobnih podataka trećoj zemlji može izvršiti jedino ako ta treća zemlja jamči odgovarajuću razinu zaštite tih podataka. Svrha tog članka je tako osigurati kontinuitet zaštite koju daje ta direktiva u slučaju prijenosa osobnih podataka trećoj zemlji. U tom pogledu treba podsjetiti da navedena direktiva građanima Unije pruža visoku razinu zaštite u pogledu obrade njihovih osobnih podataka.

140. Uzevši u obzir važnu ulogu zaštite privatnih podataka u vezi s temeljnim pravom zaštite privatnog života, takva visoka razina zaštite stoga treba biti zajamčena, uključujući i slučaj prijenosa osobnih podataka trećoj zemlji.

141. Zato smatram da Komisija na temelju članka 25. stavka 6. Direktive 95/46 može utvrditi da treća zemlja osigurava odgovarajuću razinu zaštite samo kada nakon ocjene cjelokupnog prava i prakse u trećoj zemlji o kojoj je riječ, Komisija može utvrditi da ta treća zemlja pruža razinu zaštite koja je bitno ekvivalentna razini koju pruža ta direktiva, iako načini te zaštite mogu biti drugačiji od onih koji se obično koriste unutar Unije.

142. Iako se engleski izričaj *adequate* može s lingvističkog gledišta razumjeti tako da označava razinu zaštite koja je zadovoljavajuća ili dovoljna i tako bi imao drugačije semantičko polje od francuskog izričaja *adéquat*, valja istaknuti da je jedini kriterij koji treba voditi tumačenje tog izričaja cilj da se dostigne visoka razina zaštite temeljnih prava, kao što to zahtjeva Direktiva 95/46.

143. Ispitivanje razine zaštite koju pruža treća zemlja treba se usmjeriti na dva temeljna elementa, to jest na sadržaj pravila koja se primjenjuju i sredstva za osiguranje poštovanja tih pravila [56].

144. Smatram da bi, kako bi se dostigla razina zaštite koja je bitno ekvivalentna razini koja je na snazi unutar Unije, sustav „sigurne luke“ koji u velikoj mjeri počiva na vlastitom potvrđivanju i samoocjenjivanju poduzeća koja dobrovoljno sudjeluju u tom sustavu, trebao uključivati odgovarajuća jamstva i mehanizam dostatnog nadzora. Tako prijenosi osobnih podataka trećim zemljama ne bi smjeli imati nižu razinu zaštite od prijenosa koji su izvršeni unutar Unije.

145. U tom pogledu uvodno ističem da unutar Unije prevladava shvaćanje da vanjski nadzorni mehanizam u obliku neovisnog tijela predstavlja nužan element cijelog sustava koji ima za cilj osigurati poštovanje pravila o zaštiti osobnih podataka.

56 — Vidjeti str. 5. Komisijinog radnog dokumenta WP 12 naslovljenog „Prijenos osobnih podataka u treće zemlje: Primjena članaka 25. i 26. Direktive o zaštiti podataka“ koji je 24. srpnja 1998. donijela radna skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka.

146. Osim toga, kako bi se osigurao koristan učinak članka 25. stavaka 1. do 3. Direktive 95/46 valja uzeti u obzir činjenicu da je odgovarajuća razina zaštite koju pruža treća zemlja situacija koja se razvija i koja se vremenom s obzirom na niz faktora može promijeniti. Države članice i Komisija stoga moraju stalno paziti na svaku promjenu okolnosti koje mogu dovesti do potrebe za ponovnom ocjenom odgovarajuće razine zaštite koju pruža treća zemlja. Ocjena te odgovarajuće razine zaštite ne može se ograničiti na određeni trenutak i onda biti beskonačno održavana, neovisno o svim promjenama okolnosti koje zapravo pokazuju da pružena razina zaštite više nije odgovarajuća.

147. Obveza treće zemlje da osigura odgovarajuću razinu zaštite tako predstavlja trajnu obvezu. Iako je ocjena izvršena u određenom trenutku, održavanje odluke o primjerenosti pretpostavlja da nikakva okolnost koja je od tada uslijedila nije takve naravi da dovede u pitanje početnu ocjenu Komisije.

148. Naime, ne treba izgubiti iz vida da je cilj članka 25. Direktive 95/46 izbjeći da se osobni podaci prenose trećoj zemlji koja ne osigurava odgovarajuću razinu zaštite, čime se krši temeljno pravo na zaštitu osobnih podataka koje se jamči u članku 8. Povelje.

149. Treba istaknuti da je ovlast koju je zakonodavac Unije povjerio Komisiji u članku 25. stavku 6. Direktive 95/46 da utvrđuje osigurava li treća zemlja odgovarajuću razinu zaštite, izričito uvjetovana zahtjevom da ta treća zemlja osigura takvu razinu u smislu stavka 2. tog članka. Ako su nove okolnosti takve da dovode u pitanje Komisijinu početnu ocjenu, ona bi posljedično trebala prilagoditi svoju odluku.

3. Moja ocjena

150. Podsjećam da na temelju članka 25. stavka 6. Direktive 95/46 „Komisija može u skladu s postupkom iz članka 31. stavka 2. ove Direktive, utvrditi da treća zemlja temeljem domaćeg zakonodavstva ili međunarodnih obveza koje je preuzela, osigurava odgovarajuću razinu zaštite u smislu stavka 2. ovog članka, posebno nakon završetka pregovora iz stavka 5. ovog članka, za zaštitu privatnog života i osnovnih sloboda i prava pojedinaca“. Članak 25. stavak 6. te direktive u vezi s člankom 25. stavkom 2. te direktive znači da za utvrđivanje da li treća zemlja osigurava odgovarajuću razinu zaštite, Komisija mora provesti cjelovitu ocjenu pravnih pravila koja su na snazi u toj zemlji kao i njihove primjene.

151. Vidjeli smo da se činjenica da je Komisija zadržala svoju Odluku 2000/520 unatoč pojavljivanju novih činjeničnih i pravnih novosti, mora razumjeti kao njezina želja da potvrdi svoju početnu ocjenu.

152. Nije na Sudu da u okviru zahtjeva za prethodnu odluku ocjenjuje činjenice zbog kojih je nastao spor i koje su navele nacionalni sud da uputi taj zahtjev za prethodnu odluku [57].

153. Stoga se oslanjam na činjenice koje je sud koji je uputio zahtjev naveo u svojem zahtjevu za prethodnu odluku, činjenice koje je sâma Komisija uostalom priznala kao dokazane [58].

154. Elementi koji su istaknuti pred Sudom da bi se osporila ocjena Komisije prema kojoj sustav „sigurne luke“ osigurava odgovarajuću razinu zaštite osobnih podataka prenesenih iz Unije u SAD mogu se opisati na sljedeći način.

57 — Vidjeti osobito presudu Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, t. 22. i navedena sudska praksa).

58 — Vidjeti Komunikaciju Komisije navedenu u bilješci 2. i Komunikaciju Komisije Europskom parlamentu i Vijeću o funkcioniranju „sigurne luke“ iz perspektive građana EU-a i poduzeća s poslovnim nastanom u Europskoj uniji [COM(2013) 847 *final*].

155. U svom zahtjevu za prethodnu odluku sud koji je uputio zahtjev polazi od dva činjenična utvrđenja. S jedne strane, osobne podatke koje su poduzeća kao što je Facebook Irska prenijela društvu majci sa sjedištem u SAD-u, mogu potom pregledati NSA kao i druge američke sigurnosne agencije tijekom nadzornih aktivnosti i neciljanih masovnih presretanja. Naime, uslijed otkrića E. Snowdena niti jedan drugi vjerojatni zaključak se trenutačno ne bi mogao izvući iz dostupnih dokaza [59]. S druge strane, građani Unije ne raspolažu nikakvim djelotvornim pravom na saslušanje o pitanju nadzora i presretanja njihovih podataka od strane NSA i drugih američkih sigurnosnih agencija [60].

156. Činjenice koje je tako utvrdio Visoki sud poduprte su utvrđenjima koje je izvršila sama Komisija.

157. Tako je Komisija u gore navedenoj Komunikaciji o funkcioniranju „sigurne luke“ iz perspektive građana EU-a i poduzeća s poslovnim nastanom na njezinom području, zaključila da su tijekom 2013. podaci o opsegu i dosegu američkih programa nadzora izazvali zabrinutost što se tiče kontinuiteta zaštite osobnih podataka koji su zakonito preneseni u SAD u okviru sustava „sigurne“ luke. Komisija je navela da su sva poduzeća uključena u program PRISM koja nadležnim tijelima SAD-a omogućavaju pristup pohranjenim i obrađenim podacima u SAD-u, članovi „sigurne luke“. Prema mišljenju Komisije „sigurna luka“ je postala jedan od kanala kojim je obavještajnim agencijama SAD-a omogućen pristup prikupljanju podataka koji su prvotno obrađeni u Uniji [61].

158. Iz tih elemenata proizlazi da pravo i praksa SAD-a omogućavaju opsežno prikupljanje osobnih podataka građana Unije koji su preneseni u okviru sustava „sigurne luke“ a da ti građani nemaju osiguranu učinkovitu pravnu zaštitu.

159. Smatram da ta činjenična utvrđenja pokazuju da Odluka 2000/520 ne sadržava dovoljno jamstava. Zbog toga manjka jamstava ta odluka se provodi na način koji ne odgovara zahtjevima Povelje niti Direktive 95/46.

160. Cilj odluke koju je na temelju članka 25. stavka 6. Direktive 95/46 donijela Komisija je utvrditi da treća zemlja „osigurava“ odgovarajuću razinu zaštite. Izričaj „osigurava“ konjugiran u prezentu znači da se takva odluka, kako bi se mogla zadržati, treba odnositi na treću zemlju koja nakon donošenja te odluke nastavlja jamčiti odgovarajuću razinu zaštite.

161. Zapravo, otkrića koja se odnose na aktivnosti NSA koja koristi podatke prenesene u okviru sustava „sigurne luke“ rasvijetlila su slabosti pravne osnove koja čini Odluku 2000/520.

162. Nedostaci koji su istaknuti tijekom ovog postupka osobito se nalaze u Prilogu I. četvrtom stavku te odluke.

163. Podsjećam da u skladu s navedenom odredbom „[p]ridržavanje […] načela [sigurne luke] može biti ograničeno: (a) u onoj mjeri koja je potrebna da se ispune uvjeti nacionalne sigurnosti, javnog interesa, ili uvjeti za provedbu zakona; (b) zakonom, vladinom uredbom ili sudskom praksom koji proizvode proturječne obveze ili izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezino nepošt[o]vanje načela ograničeno u mjeri potrebnoj da se ostvare pretežući zakoniti interesi koje podupire takvo dopuštenje“.

164. Problem proizlazi prvenstveno iz toga kako američka tijela koriste odstupanja predviđena u navedenoj odredbi. Zbog njihovih preopćenitih formulacija, tijela provode ta odstupanja na način koji nije ograničen na ono što je nužno potrebno.

59 — Točka 7., podtočka (c) zahtjeva za prethodnu odluku.

60 — Point 7, podtočka (b) zahtjeva za prethodnu odluku.

61 — Stranica 19. njezine Komunikacije.

165. Uz preopćenitu formulaciju dodaje se okolnost da građani Unije ne raspolažu primjerenim pravnim lijekom protiv obrade njihovih osobnih podataka radi ciljeva koji nisu oni zbog kojih su početno prikupljani, a zatim preneseni u SAD.

166. Uz odstupanja od primjene načela „sigurne luke“ koja su predviđena u Odluci 2000/520, osobito ona zbog zahtjeva nacionale sigurnosti, trebalo je osigurati mehanizam neovisnog nadzora koji bi sprečavao stalna posezanja u pravo na privatni život.

167. Tako su otkrića o praksama američkih obavještajnih službi što se tiče općeg nadzora podataka prenesenih u okviru „sigurne luke“ rasvijetlila određene nedostatke Odluke 2000/520.

168. Tvrdnje o kojima je bilo riječi u ovom predmetu ne odnose se na to da je Facebook povrijedio načela „sigurne luke“. Ako je certificirano poduzeće kao što je Facebook SAD dalo američkim tijelima pristup podacima koja su mu prenesena iz države članice, može se smatrati da ono to čini kako bi uskladilo s američkim zakonodavstvom. S obzirom na činjenicu da je takva situacija izričito priznata Odlukom 2000/520 zbog široke formulacije odstupanja koja sadržava, zapravo se u okviru ovog predmeta postavlja pitanje usklađenosti takvih odstupanja s primarnim pravom Unije.

169. U tom pogledu treba istaknuti da iz ustaljene sudske prakse Suda proizlazi da je poštovanje ljudskih prava uvjet zakonitosti akata Unije i da se u Uniji ne mogu prihvatiti mjere koje s njima nisu spojive [62].

170. Osim toga, iz ustaljene sudske prakse Suda proizlazi da prosljeđivanje osobnih podataka koje su prikupile javne ili privatne treće osobe, predstavlja nepovredivi element u pravu na poštovanje privatnog života „bez obzira na kasnije korištenje tako proslijeđenih podataka“ [63]. Osim toga u svojoj presudi Digital Rights Ireland i dr. [64] Sud je potvrdio da je činjenica da se nacionalna nadležna tijela ovlašćuju na pristup tim podacima predstavlja dodatno miješanje u to temeljno pravo [65]. Osim toga, u članku 8. Povelje pokriven je svaki oblik obrade osobnih podataka i predstavlja miješanje u pravo na zaštitu tih podataka [66]. Pristup osobnim podacima koji imaju američke obavještajne službe predstavlja stoga također miješanje u temeljno pravo na zaštitu osobnih podataka koji se jamči u članku 8. Povelje jer takav pristup predstavlja obradu podataka.

171. Poput onoga što je Sud zaključio u navedenoj presudi, tako utvrđeno miješanje je vrlo opsežno i treba se smatrati posebno ozbiljnim, s obzirom na velik broj korisnika i prenesenih podataka o kojima je riječ. Ti elementi, povezani s tajnosti pristupa američkih tijela osobnim podacima koji su preneseni u poduzeća sa sjedištem u SAD-u, čini miješanje iznimno ozbiljnim.

172. Tome se dodaje okolnost da građani Unije, korisnici Facebooka, nisu obaviješteni o činjenici da će njihovi osobni podaci općenito biti dostupni američkim sigurnosnim agencijama.

173. Također bi trebalo naglasiti činjenicu da je sud koji je uputio zahtjev zaključio da u SAD-u građani Unije nemaju nikakvo djelotvorno pravo na saslušanje o pitanju nadzora i presretanja njihovih podataka. FISC vrši nadzor ali je postupak pred njim tajan i nekontradiktoran [67]. Smatram da se radi o miješanju u pravo na djelotvoran pravni lijek građana Unije koje je zaštićeno u članku 47. Povelje.

62 — Vidjeti osobito presudu Kadi i Al Barakaat International Foundation/Vijeće i Komisija (C-402/05 P i C-415/05 P, EU:C:2008:461, t. 284. kao i navedena sudska praksa).

63 — Presuda Österreichischer Rundfunk i dr. (C-465/00, C-138/01 i C-139/01, EU:C:2003:294, t. 74.).

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

65 — Točka 35.

66 — Točka 36.

67 — Točka 7. podtočka (b) zahtjeva za prethodnu odluku.

174. Miješanje u temeljna prava zaštićena u člancima 7., 8. i 47. Povelje koje je dozvoljeno odstupanjima od „sigurne luke“ iz Priloga I. četvrtog stavka Odluke 2000/520 je stoga utvrđeno.

175. Sada treba provjeriti je li to miješenje opravdano ili ne.

176. U skladu s člankom 52. stavkom 1. Povelje svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Uz poštovanje načela proporcionalnosti, ograničenja navedenih prava i sloboda su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.

177. S obzirom na uvjete koji su tako postavljeni da bi se omogućilo ograničenje pri ostvarivanju prava i sloboda zaštićenih Poveljom, izrazito sumnjam da se može smatrati da ograničenja o kojima je riječ u ovom predmetu poštuju bitan sadržaj članaka 7. i 8. Povelje. Naime, čini se da se pristup američkih obavještajnih službi prenesenim podacima širi na sadržaj elektroničkih komunikacija, što povređuje bitan sadržaj temeljnog prava na zaštitu privatnog života i drugih prava zaštićenih u članku 7. Povelje. Štoviše, budući da široka formulacija ograničenja predviđenih u Prilogu I. četvrtom stavku Odluke 2000/520 potencijalno omogućava isključivanje primjene svih načela „sigurne luke“, može se smatrati da ta ograničenja povređuju bitan sadržaj temeljnog prava na zaštitu osobnih podataka [68].

178. Što se tiče pitanja odgovara li utvrđeno miješanje cilju od javnog interesa, podsjećam kao prvo da u skladu s Prilogom I. četvrtim stavkom točkom (b) Odluke 2000/520, pridržavanje načela „sigurne luke“ može biti ograničeno „zakonom, vladinom uredbom ili sudskom praksom koji proizvode proturječne obveze ili izričita dopuštenja, ako pri korištenju takvog dopuštenja organizacija može dokazati da je njezino nepošt[o]vanje načela ograničeno u mjeri potrebnoj da se ostvare pretežući zakoniti interesi koje podupire takvo dopuštenje“.

179. Treba zaključiti da „zakoniti interesi“ koji se navode u toj odredbi nisu precizni. Iz toga proizlazi nesigurnost što se tiče područja primjene, koje bi moglo biti vrlo široko, tog odstupanja od primjene načela „sigurne luke“ poduzeća koja ih se pridržavaju.

180. Taj dojam se potvrđuje čitanjem objašnjenja u naslovu B. Priloga IV. Odluci 2000/520 naslovljenog „Izričita zakonska ovlaštenja“, osobito tvrdnja da je„[j]asno je da ako pravo SAD-a nameće proturječne obveze, organizacije iz SAD-a bez obzira na to jesu li u ‘sigurnoj luci’ ili nisu moraju poštovati zakon. Osim toga navodi se „[d]ok je namjera načela ‘sigurne luke’ premostiti razlike između američkog i europskog režima zaštite privatnosti, u pogledu izričitih ovlaštenja dužni smo poštovati posebna zakonska prava naših izabranih zakonodavaca“.

181. Smatram da iz tog proizlazi da je to odstupanje protivno člancima 7. i 8. i članku 52. stavku 1. Povelje s obzirom na to da ono ne slijedi cilj javnog interesa koji bi bio dovoljno precizno definiran.

182. U svakom slučaju lakoća i općenitost kojom Odluka 2000/520 u svojim Prilogu I. četvrtom stavku točki (b) i Prilogu IV. B. predviđa da se od načela „sigurne luke“ može odstupiti u skladu s normama američkog prava nije sukladna s uvjetima prema kojima odstupanja od pravila o zaštiti osobnih podataka moraju biti ograničena na ono što je nužno potrebno. Točno je da je naveden uvjet nužnosti, ali osim činjenice da je dotično poduzeće odgovorno za dokazivanje tog uvjeta, ne vidim kako bi takvo poduzeće moglo izbjeći obvezu da ne odstupi od načela „sigurne luke“ koje proizlazi iz pravnih pravila koja mora primjenjivati.

68 — Vidjeti u tom pogledu presudu Digital Rights Ireland i dr. (C-293/12 i C-594/12, EU:C:2014:238, t. 39. i 40.).

183. Stoga smatram da se Odluka 2000/520 mora proglasiti nevaljanom s obzirom na to da postojanje odstupanja koje na tako općenit i neprecizan način omogućava da se odstupi od načela „sigurne luke“ samo po sebi sprečava da se za taj sustav smatra da osigurava odgovarajuću razinu zaštite osobnih podataka koji su preneseni iz Unije u SAD.

184. Što se tiče prve kategorije ograničenja predviđenih u Prilogu I. četvrtom stavku točki (a) Odluke 2000/520 zbog ispunjavanja zahtjeva nacionalne sigurnosti, javnog interesa i poštovanja američkih zakona, samo mi se prvi uvjet čini dovoljno precizan da bi se mogao smatrati ciljem u javnom interesu koji priznaje Unija u smislu članka 52. stavka 1. Povelje.

185. Sada treba provjeriti proporcionalnost utvrđenog miješanja.

186. U tom pogledu valja podsjetiti na to da „prema ustaljenoj sudskoj praksi Suda, načelo proporcionalnosti zahtijeva da su akti institucija Unije sposobni ostvariti legitimne ciljeve koje slijedi zakonodavstvo o kojem je riječ i da ne prelaze granice onoga što je prikladno i nužno za ostvarenje tih ciljeva“ [69].

187. Što se tiče sudskog nadzora poštovanja tih uvjeta „kad je riječ o miješanju u temeljna prava, širina ovlasti ocjene zakonodavca Unije može se pokazati ograničenom s obzirom na određeni broj elemenata, među kojima su posebice područje o kojem je riječ, narav predmetnog prava koje je zajamčeno Poveljom, narav i težina miješanja kao i njegova svrha“ [70].

188. Smatram da su odluke koje Komisija donosi na temelju članka 25. stavka 6. Direktive 95/46 u cijelosti podvrgnute nadzoru Suda što se tiče proporcionalnosti ocjene koju je izvršila ta institucija o odgovarajućoj razini zaštite koju pruža treća zemlja temeljem „svojeg domaćeg zakonodavstva ili međunarodnih obveza“.

189. U tom pogledu treba navesti da je Sud u svojoj presudi Digital Rights Ireland i dr. [71] presudio da „s obzirom na, s jedne strane, važnu ulogu koju ima zaštita osobnih podataka u odnosu na temeljno pravno na poštovanje privatnog života i, s druge strane, širinu i težinu miješanja u to pravo koje sadrži direktiva [o kojoj je riječ], ovlast ocjene zakonodavca Unije smanjena je na način da je potrebno provesti strog nadzor“ [72].

190. Takvo miješanje treba omogućiti postizanje cilja koji slijedi akt Unije o kojem je riječ i treba biti nužno za postizanje tog cilja.

191. U tom pogledu, „kad je riječ o pravu na poštovanje privatnog života, prema ustaljenoj sudskoj praksi Suda zaštita tog temeljnog prava […] zahtijeva da su odstupanja i ograničenja u zaštiti osobnih podataka u granicama onog što je strogo nužno“ [73].

192. U svom nadzoru Sud također uzima u obzir okolnost da „zaštita osobnih podataka koja proizlazi iz izričite obveze predviđene u članku 8. stavku 1. Povelje ima osobitu važnost za pravo na poštovanje privatnog života iz njezinog članka 7.“ [74].

69 — Presuda Digital Rights Ireland i dr.(C-293/12 et C-594/12, EU:C:2014:238, t. 46. kao i navedena sudska praksa).

70 — *Ibidem* (t. 47. i navedena sudska praksa).

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

72 — Točka 48.

73 — Presuda Digital Rights Ireland i dr. (C-293/12 i C-594/12, EU:C:2014:238, t. 52. kao i navedena sudska praksa).

74 — *Ibidem* (t. 53.).

193. Prema mišljenju Suda koji u tom pogledu upućuje na sudsku praksu Europskog suda za ljudska prava „zakonodavstvo Unije o kojem je riječ mora predvidjeti jasna i precizna pravila koja uređuju doseg i primjenu mjere o kojoj je riječ te propisati minimalne uvjete na način da osobe čiji su podaci zadržani raspolažu dostatnim jamstvima koja omogućuju učinkovitu zaštitu njihovih osobnih podataka od rizika zloporabe kao i od svih nezakonitih pristupa i korištenja tih podataka“ [75]. Sud upućuje da „[n]užnost raspolaganja takvim jamstvima još je i značajnija zato što su […] osobni podaci podvrgnuti automatskoj obradi te postoji značajan rizik od nezakonitog pristupa tim podacima“ [76].

194. Smatram da postoji analogija između Priloga I. četvrtog stavka točke (a) Odluke 2000/520 i članka 13. stavka 1. Direktive 95/46. U prvoj odredbi je navedeno da pridržavanje načela „sigurne luke“ može biti ograničeno „u onoj mjeri koja je potrebna da se ispune uvjeti nacionalne sigurnosti, javnog interesa, ili uvjeti za provedbu zakona SAD-a“. U drugoj odredbi je predviđeno da države članice mogu donijeti propise za ograničavanje područja primjene obveza i prava iz članka 6. stavka 1., članka 10., članka 11. stavka 1. te članka 12. i 21. ove direktive kada takvo ograničavanje predstavlja potrebne mjere za zaštitu, među ostalim, nacionalne sigurnosti, obrane, javne sigurnosti kao i sprečavanja, istrage, otkrivanja i progona kaznenih djela.

195. Kao što je Sud to istaknuo u svojoj presudi IPI [77], iz teksta članka 13. stavka 1. Direktive 95/46 proizlazi da države članice donose mjere iz te odredbe samo kada su one potrebne. Zahtjev da su te mjere nužno potrebne je preduvjet za ovlast država članica koja je dodijeljena tom odredbom [78]. Za obrade osobnih podataka unutar Unije ograničenja iz članka 13. te direktive moraju se razumjeti tako da se ona odnose na ono što je nužno potrebno da bi se postigao željeni cilj. Smatram da isto vrijedi u pogledu ograničenja načela „sigurne luke“ koja su predviđena u Prilogu I. četvrtom stavku Odluke 2000/520.

196. Međutim, treba navesti da ne navode sve jezične verzije kriterij nužnosti u tekstu Priloga I. četvrtog stavka točke (a) Odluke 2000/520. To osobito vrijedi za francusku verziju koja upućuje da „[l]'adhésion aux principes peut être limitée par [...] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis“ dok na primjer španjolska, njemačka i engleska verzija upućuju da ograničenja koja se nameću moraju biti nužna da bi se ostvarili gore navedeni ciljevi.

197. Bez obzira na sve, činjenični elementi koje su istaknuli sud koji je uputio zahtjev i Komisija u gore navedenim komunikacijama jasno pokazuju da u praksi provedba tih ograničenja nije ograničena na ono što je nužno kako bi se postigli željeni ciljevi.

198. U tom pogledu ističem da pristup prenesenim osobnim podacima kojima raspolažu američke obavještajne službe na općenit način obuhvaća svaku osobu i sva sredstva elektroničke komunikacije kao i sve prenesene podatke, uključujući i sadržaj komunikacija, bez ikakvog razlikovanja, ograničenja ili iznimke s obzirom na cilj u javnom interesu [79].

199. Naime, pristup američkih obavještajnih službi prenesenim podacima odnosi se općenito na sve osobe koje koriste usluge elektroničkih komunikacija, a da se pritom ne zahtijeva da osobe o kojima je riječ predstavljaju prijetnju javnoj sigurnosti [80].

200. Takav masovni i neciljani nadzor sam po sebi nije proporcionalan i predstavlja neopravdano miješanje u prava zajamčena u člancima 7. i 8. Povelje.

75 — *Ibidem* (t. 54. i navedena sudska praksa).

76 — *Ibidem* (t. 55. i navedena sudska praksa).

77 — C-473/12, EU:C:2013:715.

78 — Točka 32.

79 — Vidjeti po analogiji presudu Digital Rights Ireland i dr. (C-293/12 et C-594/12, EU:C:2014:238, t. 57. i navedena sudska praksa).

80 — *Ibidem* (t. 58. i 59.).

201. Kao što je to ispravno naveo Parlament u svojim očitovanjima, s obzirom na to da je nemoguće da zakonodavac Unije ili države članice donose zakonske odredbe koje bi protivno Povelji predviđale masovni i neciljani nadzor, iz tog nužno proizlazi da, *a fortiori*, za te treće zemlje se ni u kojem slučaju ne bi moglo smatrati da osiguravaju odgovarajuću razinu zaštite osobnih podataka građana Unije kada njihovo zakonodavstvo stvarno dozvoljava masovni i neciljani nadzor i presretanje tih vrsta podataka.

202. Osim toga treba istaknuti da sustav „sigurne luke" kako ga definira Odluka 2000/520 ne sadrži jamstva kojima je moguće izbjeći masovan i opći pristup prenesenim podacima.

203. U tom pogledu treba primijetiti da je Sud u svojoj presudi Digital Rights Ireland i dr.[81], istaknuo da je važno predvidjeti „jasna i precizna pravila koja bi uredila doseg miješanja u temeljna prava iz članaka 7. i 8. Povelje"[82]. Takvo miješanje prema mišljenju Suda mora biti „precizno ograničeno odredbama koje bi jamčile da je stvarno ograničeno na ono što je strogo nužno"[83]. Sud je također u toj presudi naglasio da je nužno predvidjeti „jamstva, kakva zahtijeva članak 8. Povelje, koja bi omogućila učinkovitu zaštitu zadržanih [osobnih] podataka od rizika zloporaba kao i od svih nezakonitih pristupa ili korištenja tih podataka"[84].

204. Treba zaključiti da mehanizmi privatne arbitraže i FTC–a zbog njegove uloge koja je ograničena na trgovačke sporove ne predstavljaju sredstvo kojim bi se mogao osporavati pristup američkih obavještajnih službi osobnim podacima koji su preneseni iz Unije.

205. Nadležnost FTC-a pokriva nepoštene i prijevarne radnje u trgovačkom području i stoga ne uključuje prikupljanje i korištenje osobnih podataka u netrgovačke ciljeve[85]. Ograničena nadležnost FTC-a ograničava prava pojedinaca na zaštitu njihovih osobnih podataka. FTC je uspostavljen ne kao što je to slučaj u Uniji s nacionalnim nadzornim tijelima radi zaštite prava pojedinaca na privatni život već da bi se zajamčila poštena i pouzdana trgovina za potrošače, što, *de facto*, ograničava njegove intervencijske ovlasti u sustav koji se odnosi na zaštitu osobnih podataka. FTC stoga nema ulogu koja se može usporediti s nacionalnim nadzornim tijelima predviđenim u članku 28. Direktive 95/46.

206. Građani Unije čiji su podaci preneseni mogu se obratiti tijelima specijalizirane arbitraže sa sjedištem u SAD-u kao što su TRUSTe i BBBOnline s pitanjima da li poduzeće koje ima njihove osobne podatke krši uvjete sustava samocertificiranja. Privatna arbitraža koju osiguravaju organizacije kao što je TRUSTe ne može rješavati povrede prava na zaštitu osobnih podataka koje su počinile organizacije ili tijela koja nisu samocertificirana poduzeća. Ta arbitražna tijela nisu nadležna za odlučivanje o zakonitosti aktivnosti američkih sigurnosnih agencija.

207. Ni FTC ni tijela privatne arbitraže stoga nisu nadležna za nadzor mogućih povreda načela zaštite osobnih podataka koje su počinili javni subjekti kao što su američke sigurnosne agencije. Takva bi nadležnost, međutim bila bitna za puno jamstvo prava na djelotvornu zaštitu tih podataka. Stoga Komisija nije mogla zaključiti, pri donošenju Odluke 2000/520 i održavajući ju na snazi, da za sve osobne podatke koji su preneseni u SAD postoji odgovarajuća zaštita prava koje je određeno u članku 8. Povelje, to jest da neovisno tijelo vrši djelotvorni nadzor poštovanja zahtjeva zaštite i sigurnosti tih podataka.

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

82 — Točka 65.

83 — *Idem.*

84 — *Ibidem* (t. 66.).

85 — Vidjeti u tom pogledu Prilog II., često postavljano pitanje 11., Odluka 2000/520 pod naslovom „Djelovanje Federal Trade Commissiona" i Prilog III., V. i VII iste.

208. Posljedično treba zaključiti da unutar sustava „sigurne luke“ predviđene Odlukom 2000/520 ne postoji neovisno tijelo koje bi moglo vršiti nadzor jesu li provedbe odstupanja od načela „sigurne luke“ ograničene na ono što je strogo nužno. Vidjeli smo da takav nadzor neovisnog tijela, s gledišta prava Unije, predstavlja suštinski element poštovanja zaštite osoba u pogledu obrade osobnih podataka [86].

209. U tom pogledu treba istaknuti ulogu koju imaju nacionalna nadzorna tijela u sustavu zaštite osobnih podataka koji je na snazi unutar Unije, u nadziranju ograničenja predviđenih u članku 13. Direktive 95/46. U skladu s člankom 28. stavkom 4. drugim podstavkom te direktive „[s]vako nadzorno tijelo posebno razmatra zahtjev za provjeru zakonitosti obrade podataka koji preda bilo koja osoba kada se primjenjuju nacionalne odredbe donesene u skladu s člankom 13. ove direktive“. Po analogiji smatram da je uz navođenje granica primjene načela „sigurne luke“ u Prilogu I. četvrtom stavku Odluke 2000/520 trebalo dodati i uspostavu mehanizma nadzora koji bi osiguravalo neovisno tijelo specijalizirano za područje zaštite osobnih podataka.

210. Intervencija neovisnih nadzornih tijela je naime u središtu europskog sustava za zaštitu osobnih podataka. Stoga je prirodno da se postojanje takvih tijela smatra jednim od nužnih uvjeta za utvrđivanje odgovarajuće razine zaštite koju osiguravaju treće zemlje. To je uvjet da protok podataka iz područja država članica prema području treće zemlje ne bude zabranjen u skladu s člankom 25. Direktive 95/46 [87]. Kao što navodi dokument za raspravu koji je donijela radna skupina uspostavljena na temelju članka 29. te direktive, u Europi postoji široka suglasnost da „je mehanizam ’vanjske kontrole’ koju obavlja neovisno tijelo, nužan element cijelog sustava koji ima za cilj osigurati poštovanje pravila o zaštiti tih podataka“ [88].

211. Osim toga, treba primijetiti da FISC građanima Unije čiji su osobni podaci bili preneseni u SAD ne omogućava ulaganje djelotvornog pravnog lijeka. Naime, zaštita protiv nadzora vladinih službi u okviru Odjeljka 702. Zakona o nadzoru inozemnih obavještajnih službi iz 1978. primjenjuje se samo na američke državljane kao i strane državljane koji zakonito i trajno borave u SAD-u. Kao što je to sama Komisija navela, nadzor američkih programa prikupljanja obavijesti mogao bi se popraviti time da se poveća uloga FISC-a i da se uspostave mogućnosti pravnih lijekova za pojedince. Ti bi mehanizmi mogli smanjiti obradu osobnih podataka koji se odnose na građane Unije koji nisu relevantni za ciljeve zaštite nacionalne sigurnosti [89].

212. Osim toga Komisija je sama navela da građani Unije nemaju nikakvu mogućnost pristupiti podacima, ispraviti ih ili izbrisati ili imati pristup administrativnoj ili sudskoj zaštiti ako su njihovi osobni podaci sakupljeni i kasnije obrađeni u okviru američkih programa nadzora [90].

213. Naposljetku treba navesti da se američke norme koje se odnose na zaštitu privatnog života mogu različito primijeniti na američke državljane i inozemne državljane [91].

214. Iz gore navedenog proizlazi da Odluka 2000/520 ne predviđa jasna i precizna pravila koja uređuju doseg miješanja u temeljna prava iz članaka 7. i 8. Povelje. Stoga treba zaključiti da se ta odluka i njena primjena u velikom opsegu i osobito ozbiljno miješaju u temeljna prava a da takvo miješanje nije precizno ograničeno odredbama koje bi jamčile da je ono učinkovito ograničeno na strogo nužno.

86 — Vidjeti presudu Digital Rights Ireland i dr. (C-293/12 i C-594/12, EU:C:2014:238, t. 68. kao i navedena sudska praksa).

87 — Vidjeti Poullet, Y., „L’autorité de contrôle: ‘vues’ de Bruxelles“, *Revue française d’administration publique*, br. 89., siječanj-ožujak 1999., str. 69., osobito str. 71.

88 — Vidjeti str. 7. Komisijinog radnog dokumenta WP 12 navedenog u bilješci 56.

89 — Stranice 10. i 11. Komunikacije Komisije navedene u bilješci 2.

90 — Vidjeti točku 7.2, str. 20., Komunikacije Komisije navedene u bilješci 2.

91 — Vidjeti o tom pitanju, Kuner, C., „Foreign Nationals and Data Protection Law: A Transatlantic Analysis“, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014., str. 213., osobito str. 216. i slj.

215. Komisija je donoseći Odluku 2000/520, te je održavajući na snazi prekoračila granice koja joj nameće poštovanje načela proporcionalnosti u smislu članaka 7. i 8. i članka 52. stavka 1. Povelje. Tome se treba dodati utvrđenje neopravdanog miješanja u pravo građana Unije na djelotvoran pravni lijek iz članka 47. Povelje.

216. Posljedično ta se odluka mora proglasiti nevaljanom jer se zbog prethodno opisanih povreda temeljnih prava, za sustav „sigurne luke“ koju uspostavlja ne može smatrati da osigurava odgovarajuću razinu zaštite osobnih podataka koji su iz Unije preneseni u SAD u okviru tog sustava.

217. S obzirom na takvo utvrđenje povreda temeljnih prava građana Unije, smatram da je Komisija trebala suspendirati primjenu Odluke 2000/520.

218. Ta odluka nije vremenski ograničena. Međutim, ovaj predmet pokazuje da se odgovarajuća razina zaštite koju pruža treća zemlja vremenom može mijenjati s obzirom na promjene činjeničnih i pravnih okolnosti na temelju kojih je donesena navedena odluka.

219. Navodim da sama Odluka 2000/520 sadrži odredbe koje predviđaju mogućnost da Komisija prilagodi tu odluku s obzirom na okolnosti.

220. Tako iz uvodne izjave 9. te odluke proizlazi da je „[m]oguće […] da će se morati ponovno razmatrati zaštita privatnosti ‘sigurne luke’ koju su stvorila načela i često postavljana pitanja, s obzirom na iskustvo, razvoj što se tiče zaštite privatnosti u okolnostima u kojima tehnologija stalno olakšava prijenos i obradu osobnih podataka te s obzirom na izvješća uključenih provedbenih tijela o samom provođenju“.

221. Štoviše, u skladu s člankom 3. stavkom 4. navedene odluke „[a]ko podaci prikupljeni sukladno stavcima 1., 2. i 3. pruže dokaz da neko tijelo odgovorno za osiguranje usklađenosti s načelima provedenima u skladu s često postavljanim pitanjima u Sjedinjenim Američkim Državama stvarno ne izvršava svoju ulogu, Komisija obavješćuje Ministarstvo trgovine SAD-a i prema potrebi, iznosi prijedloge mjera […] radi ukidanja ili suspenzije ove Odluke ili ograničenja njezina područja primjene“.

222. Osim toga, u skladu s člankom 4. stavkom 1. Odluke 2000/520, ona se „može izmijeniti bilo kada uzimajući u obzir iskustva u njezinoj provedbi i/ili ako razinu zaštite koju pružaju načela i često postavljana pitanja usvoji zakonodavstvo SAD-a. Komisija u svakom slučaju ocjenjuje provedbu ove Odluke na temelju dostupnih informacija tri godine nakon njezina priopćenja državama članicama, te o relevantnim rezultatima izvješćuje Odbor osnovan sukladno s člankom 31. Direktive 95/46 […] uključujući sve dokaze koji mogu utjecati na procjenu da odredbe članka 1. ove Odluke pružaju adekvatnu zaštitu u smislu članka 25. Direktive 95/46“. U skladu s člankom 4. stavkom 2. Odluke 2000/520, „Komisija prema potrebi iznosi nacrt mjera u skladu s postupkom utvrđenim u članku 31. Direktive 95/46/EZ.“

223. Komisija je u svojim očitovanjima zaključila da postoji „velika vjerojatnost […] da je pridržavanje načela ’sigurne luke’ ograničeno tako da nije u skladu sa strogo ograničenim uvjetima izuzetaka predviđenih u području nacionalne sigurnosti“ [92]. Komisija u tom pogledu primjećuje da „otkrića o kojima je riječ upućuju na razinu neselektivnog masovnog nadzora koji nije u skladu s kriterijem nužnosti koji je predviđen u tom izuzetku niti općenito s pravom na zaštitu osobnih podataka propisanog u članku 8. Povelje“ [93]. Komisija je, osim toga sama zaključila da „[d]oseg […] programa nadzora, zajedno s nejednakim tretmanom građana [Unije] dovodi u pitanje razinu zaštite koja se pruža aranžmanom ’sigurne luke’“ [94].

92 — Točka 44.

93 — *Idem.*

94 — Vidjeti str. 5. Komunikacije Komisije navedene u bilješci 2.

224. Štoviše, Komisija je na raspravi izričito priznala da u okviru Odluke 2000/520 kako se trenutačno primjenjuje nema jamstva da će se osigurati pravo građana Unije na zaštitu njihovih podataka. To utvrđenje međutim po njezinom mišljenju nije takve naravi da učini tu odluku nevaljanom. Iako se Komisija slaže s tvrdnjom prema kojoj ona mora djelovati ako nastupe nove okolnosti, Komisija smatra da je poduzela primjerene i proporcionalne mjere započevši pregovore sa SAD-om kako bi se izmijenio sustav „sigurne luke“.

225. Ne slažem se s tim mišljenjem. Naime u međuvremenu prijenos osobnih podataka u SAD mora biti moguće suspendirati na inicijativu nacionalnih nadzornih tijela ili povodom njima podnesenih pritužbi.

226. Osim toga, smatram da je, suočena s takvim utvrđenjima, Komisija trebala suspendirati primjenu Odluke 2000/520. Naime, cilj zaštite osobnih podataka koji žele postići Direktive 95/46 kao i članak 8. Povelje obvezuje ne samo države članice već i institucije Unije, kao što to proizlazi iz članka 51. stavka 1. Povelje.

227. Komisija u svojoj ocjeni razine zaštite koju pruža treća zemlja mora ispitati ne samo unutarnje zakonodavstvo i međunarodne obveze treće zemlje, već i način na koji se u praksi osigurava zaštita osobnih podataka. Ako se pri ispitivanju prakse otkriju nepravilnosti Komisija mora reagirati i po potrebi bez odgode suspendirati i/ili primijeniti svoju odluku.

228. Kao što sam pokazao u prethodnim razlaganjima, obveza država članica sastoji se prije svega u tome da osigura, djelovanjem njezinih nacionalnih nadzornih tijela, poštovanje pravila predviđenih u Direktivi 95/46.

229. Obveza Komisije je suspendirati primjenu odluke koju je donijela na temelju članak 25. stavka 6. te direktive u slučaju da su dokazani nedostaci u vezi s trećom zemljom o kojoj je riječ, dok ona vodi pregovore s tom trećom zemljom da bi se ispravili ti nedostaci.

230. Podsjećam da odluka koju je donijela Komisija na temelju te odredbe ima za cilj utvrditi da treća zemlja „osigurava“ odgovarajuću razinu zaštite osobnih podataka koji su bili preneseni u tu treću zemlju. Izraz „osigurava“ koji se konjugira u prezentu znači da se takva odluka, kako bi se zadržala, mora odnositi na treću zemlju koja nakon donošenja navedene odluke nastavlja jamčiti takvu razinu odgovarajuće zaštite.

231. Prema uvodnoj izjavi 57. Direktive 95/46 „prijenos osobnih podataka trećoj zemlji koja ne pruža odgovarajuću razinu zaštite mora [se] zabraniti“.

232. U skladu s člankom 25. stavkom 4. te direktive „[a]ko Komisija na temelju postupka iz članka 31. stavka 2. ove Direktive utvrdi da treća zemlja ne osigurava odgovarajuću razinu zaštite u smislu stavka 2. ovog članka, države članice poduzimaju mjere potrebne za sprečavanje bilo kakvog prijenosa podataka iste vrste toj trećoj zemlji“. Osim toga, članak 25. stavak 5. navedene direktive određuje da „[k]ada je primjereno, Komisija započinje pregovore s ciljem ispravljanja položaja koji je doveo do činjeničnog stanja iz stavka 4. ovog članka“.

233. Iz zadnje navedene odredbe proizlazi da u sustavu koji je uspostavljen člankom 25. Direktive 95/46 započeti pregovori s trećom zemljom imaju za cilj ispraviti nepostojanje utvrđene odgovarajuće razine zaštite u skladu s postupkom predviđenim u članku 31. stavku 2. te direktive. U slučaju koji nas zanima, Komisija nije formalno utvrdila, u skladu s tim postupkom, da sustav „sigurne luke“ više ne osigurava odgovarajuću razinu zaštite. U vezi s tim, ako je Komisija odlučila započeti pregovore sa SAD-om to je zato što je prethodno zaključila da razina zaštite koju osigurava treća zemlja više nije odgovarajuća.

234. Iako je Komisija bila svjesna nedostataka u primjeni Odluke 2000/520, ona nije niti suspendirala niti prilagodila tu odluku, čime je omogućila daljnju povredu temeljnih prava osoba čiji su osobni podaci bili preneseni i nastavljaju se prenositi u okviru sustava „sigurne luke“.

235. Sud je već presudio, iako u drugom kontekstu, da je na Komisiji da pazi na prilagodbu pravnih propisa na nove podatke [95].

236. Takvo nedjelovanje Komisije koje neposredno povređuje temeljna prava koja su zaštićena u člancima 7., 8. i 47. Povelje, po mom mišljenju predstavlja dodatni razlog da se u okviru ovog zahtjeva za prethodnu odluku, Odluka 2000/520 proglasi nevaljanom [96].

III – **Zaključak**

237. S obzirom na prethodna razmatranja, predlažem Sudu da na prethodna pitanja koja je postavio Visoki sud odgovori na sljedeći način:

Članak 28. Direktive 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, tumačen u svjetlu članaka 7. i 8. Povelje Europske unije o temeljnim pravima, treba tumačiti na način da postojanje odluke koju je donijela Europska komisija na temelju članka 25. stavka 6. Direktive 95/46 ne onemogućava nacionalno nadzorno tijelo da ispituje pritužbu u kojoj se tvrdi da treća zemlja ne osigurava odgovarajuću razinu zaštite prenesenih osobnih podataka i, po potrebi, da suspendira prijenos tih podataka.

Odluka Komisije 2000/520/EZ od 26. srpnja 2000. sukladno s Direktivom 95/46/EZ Europskog parlamenta i Vijeća o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a je nevaljana.

95 — Vidjeti u tom smislu presudu Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, t. 40.).

96 — Iako je Sud u presudi T. Port (C-68/95, EU:C:1996:452) presudio da „Ugovor nije predvidio mogućnost za upućivanje zahtjeva za prethodnu odluku kojim bi nacionalni sud tražio od Suda da prethodno odluči o propustu institucije“ (t. 53.), čini se da je on zauzeo o tome povoljnije stajalište u presudi Ten Kate Holding Musselkanaal i dr. (C-511/03, EU:C:2005:625, t. 29.).