Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
HENRIKA SAUGMANDSGAARDA ØEA
od 19. prosinca 2019.[1]

Predmet C-311/18

Data Protection Commissioner
protiv
Facebook Ireland Limited,
Maximilliana Schremsa,
uz sudjelovanje
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

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

„Zahtjev za prethodnu odluku – Zaštita pojedinaca u vezi s obradom osobnih podataka – Uredba (EU) 2016/679 – Članak 2. stavak 2. – Područje primjene – Prijenos osobnih podataka u komercijalne svrhe u Sjedinjenim Američkim Državama – Obrada prenesenih podataka koju tijela javne vlasti Sjedinjenih Američkih Država provode u svrhu nacionalne sigurnosti – Članak 45. – Procjena primjerenosti razine zaštite osigurane u trećoj zemlji – Članak 46. – Odgovarajuće zaštitne mjere koje nudi voditelj obrade – Standardne klauzule o zaštiti – Članak 58. stavak 2. – Ovlasti nadzornih tijela – Odluka 2010/87/EU – Valjanost – Provedbena odluka (EU) 2016/1250 – ‚Europsko-američki sustav zaštite privatnosti' – Valjanost – Članci 7., 8. i 47. Povelje Europske unije o temeljnim pravima"

Sadržaj

1 Izvorni jezik: francuski

I. Uvod

1. Bez zajedničkih zaštitnih mjera u području zaštite osobnih podataka na svjetskoj razini postoji opasnost od prekida u razini zaštite koja se u Europskoj uniji osigurava prekograničnim protocima takvih podataka. Kako bi pojednostavnio te protoke i pritom smanjio tu opasnost, zakonodavac Unije uspostavio je tri mehanizma na temelju kojih se osobni podaci mogu prenijeti iz Unije u treću državu.

2. Kao prvo, takav se prijenos može provesti na temelju odluke kojom Europska komisija utvrđuje da dotična treća država osigurava „primjerenu razinu zaštite" podataka koji se u nju prenose [2]. Kao drugo, ako ne postoji takva odluka, prijenos se odobrava kada je osiguran „odgovarajućim zaštitnim mjerama" [3]. Te zaštitne mjere mogu biti u obliku ugovora između izvoznika i uvoznika podataka koji uključuju standardne klauzule o zaštiti podataka koje donosi Komisija. GDPR-om se predviđaju, kao treće, određena odstupanja, temeljena osobito na privoli ispitanika, kojima se omogućuje prijenos u treću zemlju čak i ako ne postoji odluka o primjerenosti ili odgovarajuće zaštitne mjere [4].

3. Zahtjev za prethodnu odluku koji je uputio High Court (Visoki sud, Irska) odnosi se na drugi od tih mehanizama. Konkretnije, odnosi se na valjanost Odluke 2010/87/EU [5], kojom je Komisija utvrdila standardne ugovorne klauzule za određene kategorije prijenosa, s obzirom na članke 7., 8. i 47. Povelje Europske unije o temeljnim pravima (u daljnjem tekstu: Povelja).

2 Vidjeti članak 45. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46 (Opća uredba o zaštiti podataka) (SL 2016., L 119, str. 1. i ispravak SL 2018., L 127, str. 2.) (u daljnjem tekstu: GDPR).

3 Vidjeti članak 46. GDPR-a.

4 Vidjeti članak 49. GDPR-a.

5 Odluka Komisije od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća (SL 2010., L 39, str. 5.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 250.), kako je izmijenjena Provedbenom odlukom Komisije (EU) 2016/2297 od 16. prosinca 2016. (SL 2016., L 344, str. 100.) (u daljnjem tekstu: Odluka 2010/87)

4. Taj je zahtjev podnesen u okviru spora između Data Protection Commissionera (povjerenik za zaštitu podataka, Irska, u daljnjem tekstu: DPC), s jedne strane, te društva Facebook Ireland Ltd i Maximilliana Schremsa, s druge strane. Potonji je DPC-u podnio pritužbu u pogledu osobnih podataka koji se odnose na njega koje je društvo Facebook Ireland prenijelo društvu Facebook Inc., njegovu društvu majci sa sjedištem u Sjedinjenim Američkim Državama (u daljnjem tekstu: SAD). DPC smatra da postupanje sa tom pritužbom ovisi o tome je li Odluka 2010/87 valjana. U tom se kontekstu obratio sudu koji je uputio zahtjev za prethodnu odluku tražeći od njega da s tim u vezi postavi pitanje Sudu.

5. Najprije navodim da ispitivanjem prethodnih pitanja, prema mojem mišljenju, nije otkriven nikakav element koji bi mogao utjecati na valjanost Odluke 2010/87.

6. Osim toga, sud koji je uputio zahtjev iznio je određene dvojbe koje se u biti odnose na primjerenost razine zaštite koju SAD osigurava s obzirom na miješanja koja američka obavještajna tijela svojim djelovanjem unose u ostvarivanje temeljnih prava osoba čiji se podaci prenose u tu treću zemlju. Tim se dvojbama neizravno dovode u pitanje ocjene koje je Komisija u tom pogledu provela u Provedbenoj odluci (EU) 2016/1250[6]. Iako za rješavanje glavnog postupka nije potrebno da Sud odluči o tom pitanju te mu stoga predlažem da to ne učini, podredno ću iznijeti razloge koji me navode na preispitivanje valjanosti te odluke.

7. Cijela moja analiza temeljit će se na postizanju ravnoteže između, s jedne strane, potrebe za uspostavom „razumnog stupnja pragmatičnosti kako bi se omogućila interakcija s ostatkom svijeta”[7] i, s druge strane, potrebe za utvrđivanjem temeljnih vrijednosti priznatih u pravnim poredcima Unije i njezinih država članica, konkretno u Povelji.

II. Pravni okvir

A. Direktiva 95/46/EZ

8. Člankom 3. stavkom 2. Direktive 95/46/EZ o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka[8] određivalo se da:

„Ova se Direktiva ne primjenjuje na obradu osobnih podataka:

– tijekom aktivnosti koja je izvan područja primjene prava Zajednice, kao što je predviđeno u glavama V. i VI. Ugovora o Europskoj uniji i u svakom slučaju na postupke obrade koji se odnose na javnu sigurnost, obranu, nacionalnu sigurnost (uključujući gospodarsku dobrobit države kada se operacija obrade odnosi na pitanja nacionalne sigurnosti) i aktivnosti države u području kaznenog prava,

[…]”

6 Odluka Komisije od 12. srpnja 2016. u skladu s [Direktivom 95/46] o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti (SL 2016., L 207, str. 1.) (u daljnjem tekstu: Odluka o sustavu zaštite privatnosti)

7 Vidjeti govor bivšeg Europskog nadzornika za zaštitu podataka (EDPS) Petera Hustinxa, „Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données”, str. 49., dostupan na adresi https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf.

8 Direktiva Europskog parlamenta i Vijeća od 24. listopada 1995. (SL 1995., L 281, str. 31.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 7., str. 88.), kako je izmijenjena Uredbom (EZ) br. 1882/2003 Europskog parlamenta i Vijeća od 29. rujna 2003. (SL 2003., L 284, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 1., svezak 16., str. 96.; u daljnjem tekstu: Direktiva 95/46)

9. Članak 13. stavak 1. te direktive stoga je glasio kako slijedi:

„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:

(a) nacionalne sigurnosti;

(b) obrane;

(c) javne sigurnosti;

(d) sprečavanja, istrage, otkrivanja i progona kaznenih djela ili kršenja etike zakonom uređenih djelatnosti;

(e) važnoga gospodarskog ili financijskog interesa države članice ili [Unije], uključujući novčana, proračunska i porezna pitanja;

(f) nadzora, inspekcije ili regulatorne funkcije povezane, čak i povremeno, s izvršavanjem javnih ovlasti u slučajevima iz točke (c), (d) i (e);

(g) zaštite osobe čiji se podaci obrađuju ili prava i slobode drugih."

10. Člankom 25. navedene direktive određivalo se:

„1. Države članice osiguravaju da se prijenos osobnih podataka koji se obrađuju ili koje je potrebno obraditi nakon prijenosa trećoj zemlji može izvršiti jedino ako, ne dovodeći u pitanje nacionalne odredbe donesene u skladu s drugim odredbama ove Direktive, te treće zemlje osiguraju odgovarajuću razinu zaštite.

2. Odgovarajuća 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.

[…]"

6. 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.

Države članice poduzimaju mjere potrebne za usklađivanje s odlukom Komisije."

11. Člankom 26. stavcima 2. i 4. te direktive predviđalo se:

„2. Ne dovodeći u pitanje stavak 1. ovog članka, država članica može odobriti prijenos ili skup prijenosa osobnih podataka trećoj zemlji koja ne osigurava odgovarajuću razinu zaštite u smislu članka 25. stavka 2. ove Direktive, kada nadzornik daje dovoljna jamstva u vezi zaštite privatnosti i temeljnih prava i sloboda pojedinaca te u vezi ostvarivanja tih prava; takva jamstva mogu posebno proizlaziti iz odgovarajućih ugovornih klauzula.

[…]"

4. Ako Komisija odluči […] da neke standardne ugovorne klauzule daju dovoljna jamstva iz stavka 2. ovog članka, države članice poduzimaju odgovarajuće mjere za usklađivanje s odlukom Komisije."

12. Članak 28. stavak 3. Direktive 95/46 glasio je kako slijedi:

„Svako tijelo posebno ima:

[…]

– učinkovite ovlasti za posredovanje, kao što je na primjer davanje mišljenja prije nego li se izvrše postupci obrade, u skladu s člankom 20. ove Direktive, te osiguranje odgovarajuće objave takvih mišljenja te ovlasti naređivanja blokiranja, brisanja ili uništavanja podataka, nametanja privremene ili konačne zabrane obrade, upozoravanja ili opominjanja nadzornika ili upućivanja predmeta nacionalnim parlamentima ili drugim političkim institucijama,

[…]"

B. GDPR

13. Na temelju njegova članka 94. stavka 1., GDPR-om je stavljena izvan snage Direktiva 95/46 s učinkom od 25. svibnja 2018., kada se ta uredba počela primjenjivati u skladu s njezinim člankom 99. stavkom 2.

14. Člankom 2. stavkom 2. navedene uredbe određuje se:

„Ova se Uredba ne odnosi na obradu osobnih podataka:

(a) tijekom djelatnosti koja nije obuhvaćena opsegom prava nije;

(b) koju obavljaju države članice kada obavljaju aktivnosti koje su obuhvaćene područjem primjene glave V. poglavlja 2. UEU-a;

[…]

(d) koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja."

15. Člankom 4. točkom 2. te uredbe „obrada" se definira kao „svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje".

16. Člankom 23. GDPR-a predviđa se:

„1. Na temelju prava Unije ili prava države članice kojem podliježu voditelj obrade podataka ili izvršitelj obrade zakonskom mjerom može se ograničiti opseg obveza i prava iz članaka od 12. do 22. i članka 34. te članka 5. ako te odredbe odgovaraju pravima i obvezama predviđenima u člancima od 12. do 22., ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu:

(a) nacionalne sigurnosti;

(b) obrane;

(c) javne sigurnosti;

(d) sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;

(e) drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, osobito važnog gospodarskog ili financijskog interesa Unije ili države članice […];

[…]

2. Osobito, svaka zakonodavna mjera iz stavka 1. sadrži posebne odredbe, prema potrebi, najmanje o:

(a) svrhama obrade ili kategorijama obrade,

(b) kategorijama osobnih podataka,

(c) opsegu uvedenih ograničenja,

(d) zaštitnim mjerama za sprečavanje zlouporabe ili nezakonitog pristupa ili prijenosa;

(e) specifikaciji voditelja obrade ili kategorija voditeljâ obrade,

(f) razdoblju pohrane i zaštitnim mjerama koje se mogu primijeniti uzimajući u obzir prirodu, opseg i svrhe obrade ili kategorije obrade;

(g) rizicima za prava i slobode ispitanika; i

(h) pravu ispitanika da budu obaviješteni o ograničenju, osim ako može biti štetno za svrhu tog ograničenja.”

17. Člankom 44. te uredbe, naslovljenim „Opća načela prijenosa”, određuje se:

„Svaki prijenos osobnih podataka koji se obrađuju ili su namijenjeni za obradu nakon prijenosa u treću zemlju ili međunarodnu organizaciju odvija se jedino ako, u skladu s drugim odredbama ove Uredbe, voditelj obrade i izvršitelj obrade djeluju u skladu s uvjetima iz ovog poglavlja koji vrijede i za daljnje prijenose osobnih podataka iz treće zemlje ili međunarodne organizacije u još jednu treću zemlju ili međunarodnu organizaciju. Sve odredbe iz ovog poglavlja primjenjuju se kako bi se osiguralo da se ne ugrozi razina zaštite pojedinaca zajamčena ovom Uredbom.”

18. U skladu s člankom 45. navedene uredbe, naslovljenim „Prijenosi na temelju odluke o primjerenosti”:

„1. Prijenos osobnih podataka trećoj zemlji ili međunarodnoj organizaciji može se dogoditi kada Komisija odluči da treća zemlja, područje, ili jedan ili više određenih sektora unutar te treće zemlje, ili međunarodna organizacija o kojoj je riječ osigurava primjerenu razinu zaštite. Takav prijenos ne zahtijeva posebno odobrenje.

2. Prilikom procjene primjerenosti stupnja zaštite Komisija osobito uzima u obzir sljedeće elemente:

(a) vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, relevantno zakonodavstvo, i opće i sektorsko, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, nacionalnoj sigurnosti, kaznenom pravu i pristupu tijela javne vlasti osobnim podacima, kao i provedbu tog zakonodavstva, pravila o zaštiti podataka, pravila struke i mjere sigurnosti, što uključuje pravila za daljnji prijenos osobnih podataka još jednoj trećoj zemlji ili međunarodnoj organizaciji, koja se poštuju u toj trećoj zemlji ili međunarodnoj organizaciji, sudsku praksu te postojanje djelotvornih i provedivih prava ispitanika te učinkovite upravne i sudske zaštite ispitanika čiji se osobni podaci prenose;

(b) postojanje i djelotvorno funkcioniranje jednog neovisnog nadzornog tijela ili više njih u trećoj zemlji, ili tijela kojem podliježe međunarodna organizacija, s odgovornošću osiguravanja i provođenja poštovanja pravila o zaštiti podataka, što uključuje primjerene provedbene ovlasti za pomoć ispitanicima i savjetovanje ispitanika u ostvarivanju njihovih prava te za suradnju s nadzornim tijelima država članica; i

(c) međunarodne obveze koje je dotična treća zemlja ili međunarodna organizacija preuzela, ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata, kao i iz njezina sudjelovanja u multilateralnim ili regionalnim sustavima, osobito u vezi sa zaštitom osobnih podataka.

3. Komisija nakon procjene primjerenosti stupnja zaštite može putem provedbenog akta odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija osigurava primjerenu razinu zaštite u smislu stavka 2. ovog članka. U provedbenom aktu predviđa se mehanizam za periodično preispitivanje, najmanje svake četiri godine, kojim će se uzeti u obzir svi relevantni događaji u toj trećoj zemlji ili međunarodnoj organizaciji. […]

4. Komisija kontinuirano prati razvoj događaja u trećim zemljama i međunarodnim organizacijama koji bi mogli utjecati na funkcioniranje odluka donesenih u skladu sa stavkom 3. ovog članka i odluka donesenih na temelju članka 25. stavka 6. [Direktive 95/46].

5. Ako dostupne informacije otkrivaju, a osobito nakon preispitivanja iz stavka 3. ovog članka, da treća zemlja, područje ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija više ne osigurava primjerenu razinu zaštite u smislu stavka 2. ovog članka u mjeri u kojoj je to potrebno, Komisija provedbenim aktima stavlja izvan snage, mijenja ili suspendira odluku iz stavka 3. ovog članka bez retroaktivnog učinka. […]

6. Komisija započinje savjetovanje s trećom zemljom ili međunarodnom organizacijom radi popravljanja stanja koje je dovelo do odluke u skladu sa stavkom 5.

[…]

9. Odluke koje je Komisija donijela na temelju članka 25. stavka 6. [Direktive 95/46] ostaju na snazi dok se ne izmijene, zamijene ili stave izvan snage odlukom Komisije donesenom u skladu sa stavkom 3. ili 5. ovog članka.”

19. Članak 46. te uredbe, naslovljen „Prijenosi koji podliježu odgovarajućim zaštitnim mjerama”, glasi kako slijedi:

„1. Ako nije donesena odluka na temelju članka 45. stavka 3., voditelj obrade ili izvršitelj obrade trećoj zemlji ili međunarodnoj organizaciji osobne podatke mogu prenijeti samo ako je voditelj obrade ili izvršitelj obrade predvidio odgovarajuće zaštitne mjere i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkoviti pravni lijekovi.

2. Odgovarajuće zaštitne mjere iz stavka 1. mogu, bez potrebe za ikakvim posebnim ovlaštenjem nadzornog tijela, pružati:

[…]

(c) standardne klauzule o zaštiti podataka koje donosi Komisija u skladu s postupkom ispitivanja iz članka 93. stavka 2.;

[…]

5. Odobrenja države članice ili nadzornog tijela na temelju članka 26. stavka 2. [Direktive 95/46] ostaju valjana dok ih nadzorno tijelo prema potrebi ne izmijeni, zamijeni ili stavi izvan snage. Odluke koje je Komisija donijela na osnovi članka 26. stavka 4. [Direktive 95/46] ostaju na snazi dok se prema potrebi ne izmijene, zamijene ili stave izvan snage odlukom Komisije donesenom u skladu sa stavkom 2. ovog članka.”

20. U skladu s člankom 58. stavcima 2., 4. i 5. GDPR-a:

„2. Svako nadzorno tijelo ima sve sljedeće korektivne ovlasti:

(a) izdavati upozorenja voditelju obrade ili izvršitelju obrade da bi namjeravani postupci obrade lako mogli prouzročiti kršenje odredaba ove Uredbe;

(b) izdavati službene opomene voditelju obrade ili izvršitelju obrade ako se postupcima obrade krše odredbe ove Uredbe;

(c) narediti voditelju obrade ili izvršitelju obrade da poštuje zahtjeve ispitanika za ostvarivanje njegovih prava u skladu s ovom Uredbom;

(d) narediti voditelju obrade ili izvršitelju obrade da postupke obrade uskladi s odredbama ove Uredbe, prema potrebi na točno određen način i u točno zadanom roku;

(e) narediti voditelju obrade da ispitanika obavijesti o povredi osobnih podataka;

(f) privremeno ili konačno ograničiti, među ostalim zabraniti, obradu;

[…]

(i) izreći upravnu novčanu kaznu u skladu s člankom 83. uz mjere, ili umjesto mjera koje se navode u ovom stavku, ovisno o okolnostima svakog pojedinog slučaja;

(j) narediti suspenziju protoka podataka primatelju u trećoj zemlji ili međunarodnoj organizaciji.

[…]

4. Izvršavanje ovlasti dodijeljenih nadzornom tijelu u skladu s ovim člankom podliježe odgovarajućim zaštitnim mjerama, među ostalim djelotvornom pravnom lijeku i odgovarajućem postupku utvrđenim u pravu Unije i pravu države članice u skladu s Poveljom.

5. Svaka država članica zakonom propisuje da njezino nadzorno tijelo ima ovlasti obavijestiti pravosudna tijela o povredama ove Uredbe i, prema potrebi, pokrenuti pravne postupke ili u njima na drugi način sudjelovati kako bi se provele odredbe ove Uredbe."

C. Odluka 2010/87

21. Na temelju članka 26. stavka 4. Direktive 95/46 Komisija je donijela tri odluke kojima je utvrdila da standardne ugovorne klauzule koje se navode u toj direktivi daju dovoljna jamstva u vezi zaštite privatnosti i temeljnih prava i sloboda pojedinaca te u vezi ostvarivanja tih prava (u daljnjem tekstu: Odluke o SUK-ovima) [9].

22. Jedna od njih je Odluka 2010/87, u čijem se članku 1. određuje da „[s]tandardne ugovorne klauzule utvrđene u Prilogu pružaju odgovarajuće zaštitne mjere u smislu zaštite privatnosti i temeljnih prava i sloboda pojedinaca u pogledu izvršavanja odgovarajućih prava kako zahtijeva članak 26. stavak 2. [Direktive 95/46]".

23. Na temelju članka 3. te odluke:

„Za potrebe ove Odluke primjenjuju se slijedeće definicije:

[…]

(c) ‚izvoznik podataka' znači nadzornik koji obavlja prijenos osobnih podataka;

(d) ‚uvoznik podataka' znači obrađivač s poslovnim nastanom u trećoj zemlji koji je od izvoznika podataka suglasan primiti osobne podatke radi njihove obrade u korist izvoznika podataka po prijenosu, u skladu s njegovim uputama i uvjetima ove Odluke, i koji nije podložan sustavu treće zemlje koji osigurava odgovarajuću zaštitu u smislu članka 25. stavka 1. Direktive [95/46];

[…]

(f) ‚pravo koje se primjenjuje na zaštitu podataka' znači zakonodavstvo, koje štiti temeljna prava i slobode pojedinaca i posebno njihovo pravo na privatnost u pogledu obrade osobnih podataka, koje primjenjuje nadzornik podataka u državi članici u kojoj izvoznik podataka ima poslovni nastan;

[…]"

9 Odluka Komisije 2001/497/EZ od 15. lipnja 2001. o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje, u skladu s [Direktivom 95/46] (SL 2001., L 181, str. 19.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 51., str. 31.), Odluka Komisije 2004/915/EZ od 27. prosinca 2004. o izmjeni Odluke [2001/497] u pogledu uvođenja alternativnog skupa standardnih ugovornih klauzula za prijenos osobnih podataka u treće zemlje (SL 2004., L 385, str. 74.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 16., str. 210.), kao i Odluka 2010/87.

24. U prvoj verziji članka 4. navedene odluke, njegovim se stavkom 1. predviđalo:

„Ne dovodeći u pitanje svoje ovlasti da poduzimaju mjere za osiguranje usklađenosti s nacionalnim odredbama usvojenima u skladu s poglavljima II., III., V. i VI. [Direktive 95/46], nadležna tijela država članica mogu koristiti svoje postojeće ovlasti da zabrane ili obustave protok podataka u treće zemlje kako bi zaštitile pojedince s obzirom na obradu njihovih osobnih podataka u slučajevima gdje:

(a) je utvrđeno da pravo, kojem je uvoznik podataka ili podobrađivač podložan, njemu nameće zahtjeve koji odstupaju od prava koje se primjenjuje na zaštitu podataka, koji nadilaze ograničenja nužna u demokratskom društvu u skladu s člankom 13. [Direktive 95/46] gdje bi ti zahtjevi mogli imati bitne neželjene posljedice na jamstva utvrđena pravom koje se primjenjuje na zaštitu podataka i standardnim ugovornim klauzulama;

(b) je nadležno tijelo utvrdilo da uvoznik podataka ili podobrađivač nisu poštovali standardne ugovorne klauzule u Prilogu; ili

(c) postoji stvarna vjerojatnost da se standardne ugovorne klauzule u Prilogu nisu ili neće poštovati i da bi daljnji prijenos prouzročio neposrednu opasnost od nanošenja teške štete osobama na koje se odnose podaci.”

25. U trenutačnoj verziji, kako proizlazi iz izmjene Odluke 2010/87 koja je uvedena Provedbenom odlukom (EU) 2016/2297[10], člankom 4. Odluke 2010/87 određuje se da „[k]ad god nadležna tijela država članica izvršavaju svoje ovlasti u skladu s člankom 28. stavkom 3. [Direktive 95/46], a čiji je ishod suspenzija ili potpuna zabrana protoka podataka prema trećim zemljama radi zaštite osoba u pogledu obrade njihovih osobnih podataka, predmetna država članica bez odgode o tome obavješćuje Komisiju koja informacije prosljeđuje drugim državama članicama”.

26. Prilog Odluci 2010/87 sadržava niz standardnih ugovornih klauzula. Konkretno, klauzulom 3., sadržanom u tom prilogu i naslovljenom „Klauzula u korist treće strane”, predviđa se:

„1. Subjekt podataka može protiv izvoznika podataka upotrijebiti ovu klauzulu i klauzulu 4. točke (b) do (i), klauzulu 5. točke (a) do (e) i (g) do (j), klauzulu 6. stavke 1. i 2., klauzulu 7., klauzulu 8. stavak 2. i klauzule 9. do 12. u korist treće stranke.

2. Subjekt podataka može protiv uvoznika podataka upotrijebiti ovu klauzulu, klauzulu 5. točke (a) do (e) i (g), klauzulu 6., klauzulu 7., klauzulu 8. stavak 2. i klauzule 9. do 12. u slučaju kada izvoznik podataka prestane postojati ili prestane postojati pred zakonom, osim ako bilo koji pravni nasljednik ne preuzme sve zakonske obveze izvoznika podataka prema ugovoru ili zakonu; u tom slučaju subjekt podataka preuzima prava i obveze izvoznika podataka te ih može upotrijebiti protiv pravnih nasljednika.

[…]”

27. Klauzulom 4. iz navedenog priloga, naslovljenom „Obveze izvoznika podataka”, određuje se:

„Izvoznik podataka suglasan je i jamči:

(a) da se obrada osobnih podataka, uključujući i sam prijenos podataka, obavljala i da će se obavljati u skladu s odgovarajućim odredbama prava primjenjivog na zaštitu podataka (te da su, prema potrebi, o tome obaviještena odgovarajuća nadležna tijela država članica u kojima izvoznik podataka ima poslovni nastan) i da neće kršiti odgovarajuće odredbe te države;

10 Odluka Komisije od 16. prosinca 2016. o izmjeni odluka [2001/497] i [2010/87] o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje i obrađivačima u tim zemljama u skladu s [Direktivom 95/46] (SL 2016., L 344, str. 100.).

(b) da je dao upute i da će davati upute uvozniku podataka tijekom trajanja usluga obrade osobnih podataka kako bi obradio osobne podatke koji su preneseni jedino u korist izvoznika podataka i u skladu s odgovarajućim odredbama prava primjenjivog na zaštitu podataka i klauzulama;

(c) da će uvoznik podataka osigurati dostatna jamstva u smislu tehničkih i organizacijskih zaštitnih mjera navedenih u Dodatku 2. ovom Ugovoru;

(d) da su nakon procjene zahtjeva prava primjenjivog na zaštitu podataka, zaštitne mjere prikladne kako bi zaštitile osobne podatke protiv slučajnog ili nezakonitog uništenja ili slučajnog gubitka, izmjene, neovlaštenog objavljivanja ili pristupa, posebno kada obrada uključuje prijenos podataka putem mreže, i protiv bilo kojeg drugog nezakonitog oblika obrade te da te mjere osiguravaju razinu sigurnosti koja je prikladna rizicima koje donosi obrada i priroda podataka koji se štite uzimajući u obzir najnovije tehnologije i trošak njihove primjene;

(e) da će osigurati poštovanje zaštitnih mjera;

(f) da je u slučaju kada prijenos uključuje posebne kategorije podataka, obavijestio subjekta podataka ili će ga unaprijed obavijestiti ili netom poslije prijenosa kako bi podaci mogli biti preneseni u treću zemlju bez odgovarajuće zaštite u skladu s [Direktivom 95/46];

(g) da će u skladu s klauzulom 5. točkom (b) i klauzulom 8. stavkom 3. proslijediti svaku obavijest zaprimljenu od uvoznika podataka ili podobrađivača nadzornim tijelima za zaštitu podataka ako izvoznik podataka odluči nastaviti s prijenosom ili ukinuti suspenziju;

(h) da će subjektu podataka, po njihovu zahtjevu, staviti na raspolaganje kopiju klauzula, izuzev Dodatka 2., i sažeti opis zaštitnih mjera kao i kopiju svakog ugovora za usluge podobrade koji mora biti u skladu s klauzulama, osim ako klauzule ili ugovor sadržavaju komercijalne podatke u kojem slučaju se ti komercijalni podaci uklanjaju;

(i) da u slučaju podobrade, podobrađivač obavlja aktivnost obrade u skladu s klauzulom 11. osiguravajući barem istu razinu zaštite osobnih podataka i prava subjekta podataka poput uvoznika podataka u skladu s klauzulama; i

(j) da će osigurati poštovanje klauzule 4. točke a) do (i).”

28. Klauzulom 5., predviđenom u tom prilogu i naslovljenom „Obveze uvoznika podataka ([1])”, određuje se:

„Uvoznik podataka suglasan je i jamči:

(a) obradu osobnih podatke jedino u korist izvoznika podataka i u skladu s njegovim uputama i klauzulama; ako to iz bilo kojih razloga ne može osigurati, suglasan je da o tome odmah obavijesti izvoznika podataka, te u tom slučaju izvoznik podataka ima pravo obustaviti prijenos podataka i/ili prekinuti ugovor;

(b) da nema razloga za vjerovanje da ga zakonodavstvo koje se na njega primjenjuje onemogućava u ispunjavanju uputa primljenih od izvoznika podataka i njegovih obveza prema ugovoru te da će u slučaju promjene u zakonodavstvu koja bi mogla imati bitan negativan učinak na jamstva i obveze iz klauzula, o promjeni odmah obavijestiti izvoznika podataka čim toga postane svjestan, te u tom slučaju izvoznik podataka ima pravo obustaviti prijenos podataka i/ili prekinuti ugovor;

(c) da je prije obrade osobnih podataka koji se prenose proveo tehničke i organizacijske zaštitne mjere navedene u Dodatku 2.;

(d) da će odmah obavijestiti izvoznika podataka o:

i. svakom pravno obvezujućem zahtjevu od strane tijela kaznenog progona za otkrivanje osobnih podataka osim ako drukčije nije zabranjeno poput zabrane prema kaznenom pravu radi očuvanja povjerljivosti kaznene istrage;

ii. svakom slučajnom ili neovlaštenom pristupu; i

iii. svakom zahtjevu primljenom izravno od osoba čiji se podaci obrađuju bez odgovaranja na taj zahtjev osim ako za to nije ovlašten;

(e) da odmah i na odgovarajući način postupa sa svim upitima izvoznika podataka koji se odnose na obradu osobnih podataka podložnim prijenosu i da poštuje savjet nadzornih tijela u pogledu obrade podataka koji se prenose;

(f) da na zahtjev izvoznika podataka, preda svoju opremu za obradu podataka radi revizije aktivnosti obrade obuhvaćene klauzulama, koju obavlja izvoznik podataka ili inspekcijsko tijelo, sastavljeno od nezavisnih članova, koji posjeduju odgovarajuće stručne kvalifikacije vezani obvezom čuvanja tajne, koje prema potrebi izabire izvoznik podataka u dogovoru s nadležnim tijelima;

[…]”

29. U skladu s bilješkom na dnu stranice 1., koja se navodi u naslovu klauzule 5. iz Priloga Odluci 2010/87:

„Obvezni zahtjevi nacionalnog zakonodavstva primjenjivi na uvoznika podataka koji ne nadilaze neophodno u demokratskom društvu na temelju jednog od interesa navedenog u članku 13. stavku 1. [Direktive 95/46] to jest, ako oni predstavljaju nužnu mjeru za očuvanje nacionalne sigurnosti, obrane, javne sigurnosti, prevencije, istrage, otkrivanja i progona kaznenih djela ili kršenje etike za zakonski zaštićena zanimanja, važan ekonomski ili financijski interes države ili zaštitu osoba na koje se odnose podaci ili prava i slobode drugih, a nisu protivni standardnim ugovornim klauzulama. Neki primjeri takvih obveznih zahtjeva koji ne nadilaze neophodno u demokratskom društvu su, između ostalog, međunarodno priznate sankcije, zahtjevi za prijavu poreza ili zahtjevi za izvješća o borbi protiv pranja novca.”

30. Klauzula 6., sadržana u tom prilogu i naslovljena „Odgovornost”, glasi kako slijedi:

„1. Stranke su suglasne da svaki subjekt podataka koji trpi štetu kao posljedicu svakog kršenja obveza navedenih u klauzulu 3. i klauzuli 11. od strane bilo koje stranke ili podobrađivača, ima pravo od izvoznika podataka primiti naknadu štete.

2. Ako subjekt podataka radi kršenja obveza navedenih u klauzuli 3. i klauzuli 11. od strane uvoznika podataka ili njegovog podobrađivača ne može podnijeti zahtjev za naknadu štete protiv izvoznika podataka u skladu sa stavkom 1. zbog toga što je izvoznik podataka prestao postojati ili prestao postojati pred zakonom ili postao nelikvidan, uvoznik podataka suglasan je da subjekt podataka može podnijeti zahtjev protiv uvoznika podataka umjesto izvoznika podataka, osim ako je neki pravni nasljednik preuzeo sve zakonske obveze izvoznika podataka po ugovoru ili po zakonu, te u tom slučaju subjekt podataka može prisilno koristiti svoja prava protiv tog nasljednika.

[…]”

31. Klauzulom 7. iz navedenog priloga, naslovljenom „Medijacija i nadležnost”, određuje se:

„1. Uvoznik podataka suglasan je da ako subjekt podataka protiv njega upotrijebi prava u korist treće stranke i/ili traže naknadu štete sukladno klauzulama, uvoznik podataka prihvaća odluku subjekta podataka:

(a) da nezavisna osobe ili, prema potrebi, nadležna tijela upute spor na medijaciju;

(b) da spor uputi sudovima u državama članicama u kojima izvoznik podataka ima poslovni nastan.

2. Stranke su suglasne da izbor subjekta podataka ne utječe na njihova temeljna ili postupovna prava da traže rješenja u skladu s ostalim odredbama nacionalnog ili međunarodnog prava.”

32. Klauzulom 9. iz tog priloga, naslovljenom „Mjerodavno pravo”, predviđa se da se standardne ugovorne klauzule ravnaju pravom države članice u kojoj izvoznik podataka ima poslovni nastan.

D. Odluka o sustavu zaštite privatnosti

33. Na temelju članaka 25. stavka 6. Direktive 95/46 Komisija je donijela dvije uzastopne odluke kojima je utvrdila da SAD osigurava primjerenu razinu zaštite osobnih podataka, koji se prenose u poduzeća osnovana u Sjedinjenim Američkim Državama koja su izjavila da se, provođenjem postupka samocertificiranja, pridržavaju načela iz tih odluka.

34. Kao prvo, Komisija je donijela Odluku 2000/520/EZ o primjerenosti zaštite koju pružaju načela privatnosti „sigurne luke” i uz njih vezana često postavljana pitanja koje je izdalo Ministarstvo trgovine SAD-a [11]. U presudi od 6. listopada 2015., Schrems [12], Sud je tu odluku proglasio nevaljanom.

35. Nakon te presude Komisija je, kao drugo, donijela Odluku o sustavu zaštite privatnosti.

36. Člankom 1. te direktive određuje se:

„1. Za potrebe članka 25. stavka 2. [Direktive 95/46] Sjedinjene Američke Države osiguravaju odgovarajuću razinu zaštite osobnih podataka koji se prenose iz Unije organizacijama u Sjedinjenim Američkim Državama u okviru europsko-američkog sustava zaštite privatnosti.

2. Europsko-američki sustav zaštite privatnosti uspostavljen je u skladu s Načelima koje je 7. srpnja 2016. izdalo američko Ministarstvo trgovine, kako je navedeno u Prilogu II. te u službenim izjavama i obvezama iz dokumenata navedenih u Prilogu I. i prilozima od III. do VII.

3. Za potrebe stavka 1. osobni se podaci u okviru europsko-američkog sustava zaštite privatnosti iz Unije prenose organizacijama u Sjedinjenim Američkim Državama koje se nalaze na ‚Popisu organizacija u sustavu zaštite privatnosti’, koji vodi i objavljuje američko Ministarstvo trgovine u skladu s odjeljcima I. i III. Načela navedenih u Prilogu II.”

11 Odluka od 26. srpnja 2000. sukladno s [Direktivom 95/46] (SL 2000., L 215, str. 7.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 16., svezak 3., str. 9., u daljnjem tekstu: Odluka o privatnosti ‚sigurne luke’)

12 C-362/14 (EU:C:2015:650), u daljnjem tekstu: presuda Schrems

37. Prilog III. A toj odluci, naslovljen „Mehanizam pravobranitelja za europsko-američki sustav za zaštitu privatnosti u vezi prikupljanja obavještajnih podataka elektroničkim izviđanjem”, priložen dopisu Johna Kerryja, koji je tada bio Secretary of State (ministar vanjskih poslova, SAD), od 7. srpnja 2016., sadržava Memorandum u kojem se utvrđuje novi postupak pravobranitelja kod „Višeg koordinatora međunarodne diplomacije u području informacijske tehnologije” (u daljnjem tekstu: pravobranitelj) kojeg imenuje ministar vanjskih poslova.

38. U skladu s tim memorandumom, taj je postupak uspostavljen „da [se] lakše obrađuj[u] zahtjev[i] povezan[i] s pristupom podacima prenesenima iz [Unije] u Sjedinjene Američke Države u okviru sustava zaštite privatnosti za potrebe nacionalne sigurnosti, sa standardnim ugovornim odredbama, obvezujućim korporativnim pravilima, ‚odstupanjima' […] ili ‚mogućim budućim odstupanjima' […] sredstvima utvrđenima u primjenjivim zakonima i politikama Sjedinjenih Američkih Država te da odgovara na te zahtjeve”.

III. Glavni postupak, prethodna pitanja i postupak pred Sudom

39. M. Schrems austrijski je državljanin s boravištem u Austriji koji je korisnik društvene mreže Facebook. Svi korisnici te društvene mreže s boravištem na državnom području Unije dužni su prilikom registriranja sklopiti ugovor s Facebookom Ireland, društvom kćeri Facebooka Inc. koje ima sjedište u SAD-u. Osobni podaci tih korisnika prenose se u cijelosti ili djelomično na poslužitelje koji pripadaju Facebooku Inc., koji su smješteni na državnom području SAD-a, gdje su predmet obrade.

40. M. Schrems uputio je 25. lipnja 2013. pritužbu DPC-u kojom je u biti od njega zatražio da zabrani Facebooku Ireland da prenosi osobne podatke koji se odnose na njega u SAD. On je u pritužbi tvrdio da važeće pravo i praksa u toj trećoj zemlji ne jamče dovoljnu razinu zaštite osobnih podataka pohranjenih na njezinu državnom području od zadiranja u okviru nadzornih aktivnosti koje tamo provode javna tijela. U tom je pogledu M. Schrems uputio na otkrića Edwarda Snowdena u vezi s aktivnostima obavještajnih službi SAD-a, posebice National Security Agencyja (Nacionalna sigurnosna agencija, SAD, u daljnjem tekstu: NSA).

41. Ta je pritužba odbijena, među ostalim, zato što je o svakom pitanju u vezi s primjerenosti zaštite osobnih podataka koja se osigurava u SAD-u trebalo odlučiti u skladu s Odlukom o privatnosti „sigurne luke”. U toj je odluci Komisija utvrdila da je ta zemlja nudila primjerenu razinu zaštite osobnih podataka koji se prenose u poduzeća koja se nalaze na njezinu državnom području i koja se pridržavaju načela iz navedene odluke.

42. M. Schrems podnio je tužbu protiv odluke o odbijanju njegove pritužbe High Courtu (Visoki sud). Taj je sud smatrao da se, iako M. Schrems nije formalno doveo u pitanje valjanost Odluke o privatnosti „sigurne luke”, u njegovoj pritužbi zapravo tvrdi da je sustav uspostavljen tom odlukom nezakonit. U tim okolnostima, navedeni je sud uputio pitanja koja se u biti odnose na to jesu li tijela država članica zadužena za zaštitu podataka (u daljnjem tekstu: nadzorna tijela), kada im se podnese pritužba u vezi sa zaštitom prava i sloboda osobe u pogledu obrade osobnih podataka koji se na nju odnose i koji su preneseni u treću državu, obvezana utvrđenjima o primjerenosti razine zaštite koju pruža ta treća država koja je Komisija iznijela na temelju članka 25. stavka 6. Direktive 95/46, čak i ako podnositelj pritužbe osporava ta utvrđenja.

43. Nakon što je u točkama 51. i 52. presude Schrems smatrao da odluka o primjerenosti obvezuje nadzorna tijela sve dok je se ne proglasi nevaljanom, Sud je u točkama 63. i 65. te presude iznio sljedeće:

„63. […] [K]ada osoba čiji su osobni podaci preneseni ili bi mogli biti preneseni u treću zemlju na koju se odnosi Komisijina odluka na temelju članka 25. stavka 6. Direktive 95/46, podnese zahtjev nacionalnom nadzornom tijelu u vezi sa zaštitom svojih prava i sloboda u odnosu na obradu tih podataka i tom prilikom osporava […] usklađenost te odluke sa zaštitom privatnosti i temeljnih prava i sloboda pojedinaca, to tijelo mora ispitati navedeni zahtjev sa svom dužnom pažnjom.

[…]

65. U [slučaju] kada navedeno tijelo smatra da su prigovori [te osobe] osnovani, to isto tijelo mora u skladu s člankom 28. stavkom 3. prvim podstavkom trećom alinejom Direktive 95/46, povezano osobito s člankom 8. stavkom 3. Povelje, imati ovlasti za sudjelovanje u sudskim postupcima. U tom je pogledu nacionalni zakonodavac dužan predvidjeti pravna sredstva koja neovisnom nadzornom tijelu omogućavaju isticanje prigovora pred nacionalnim sudovima koje smatra osnovanima, kako bi ti sudovi mogli, u slučaju da dijele sumnje tog tijela u vezi s valjanošću Komisijine odluke, uputiti zahtjev za prethodnu odluku radi ispitivanja valjanosti te odluke."

44. Sud je u navedenoj presudi također ispitao valjanost Odluke o privatnosti „sigurne luke" s obzirom na zahtjeve koji proizlaze iz Direktive 95/46, u vezi s Poveljom. Po završetku tog ispitivanja proglasio je tu odluku nevaljanom [13].

45. Nakon presude Schrems sud koji je uputio zahtjev poništio je odluku kojom je DPC odbio pritužbu M. Schremsa te ju je vratio DPC-u na ispitivanje. Potonji povjerenik otvorio je istragu te je pozvao M. Schremsa da preformulira svoju pritužbu uzimajući u obzir to da je Odluka o privatnosti „sigurne luke" proglašena nevaljanom.

46. U tu je svrhu M. Schrems zatražio od Facebooka Ireland da utvrdi pravne temelje na kojima se zasnivaju prijenosi osobnih podataka korisnika društvene mreže Facebook iz Unije u SAD. Facebook Ireland pozvao se na sporazum o prijenosu i obradi podataka (*data transfer processing agreement*) koji je sklopio s Facebookom Inc., koji se primjenjuje od 20. studenoga 2015., a da nije utvrdio sve pravne temelje na koje se oslanja, te je uputio na Odluku 2010/87.

47. U svojoj preformuliranoj pritužbi M. Schrems tvrdio je, s jedne strane, da klauzule sadržane u tom sporazumu nisu u skladu sa standardnim ugovornim klauzulama iz Priloga Odluci 2010/87. S druge strane, M. Schrems navodi da se na tim standardnim ugovornim klauzulama ni u kojem slučaju nije mogao temeljiti prijenos osobnih podataka koji se odnose na njega u SAD. To je tako zato što se američkim pravom Facebooku Inc. nalaže da osobne podatke svojih korisnika stavi na raspolaganje američkim tijelima, kao što su NSA i Federal Bureau of Investigation (Savezni istražni ured, SAD, u daljnjem tekstu: FBI), u okviru programa nadzora kojima se ometa ostvarivanje prava zajamčenih člancima 7., 8. i 47. Povelje. M. Schrems tvrdi da se nijednim pravnim lijekom ispitanicima ne omogućuje pozivanje na njihova prava na poštovanje privatnog života i zaštitu osobnih podataka. U tim okolnostima M. Schrems zahtijeva od DPC-a da obustavi taj prijenos u skladu s člankom 4. Odluke 2010/87.

48. Facebook Ireland priznao je u okviru DPC-ove istrage da i dalje prenosi u SAD osobne podatke korisnika društvene mreže Facebook koji imaju boravište u Uniji i da se u tu svrhu u velikom dijelu oslanja na standardne ugovorne klauzule iz Priloga Odluci 2010/87.

13 Vidjeti presudu Schrems (t. 106.).

49. Cilj DPC-ove istrage bio je utvrditi, s jedne strane, osigurava li SAD primjerenu zaštitu osobnih podatka građana Unije i, s druge strane, ako to nije slučaj, jesu li Odluke o SUK-ovima dovoljna jamstva u vezi sa zaštitom temeljnih sloboda i prava tih građana.

50. U tom pogledu, u nacrtu odluke (*draft decision*), DPC je privremeno smatrao da se u američkom pravu ne nude djelotvorni pravni lijekovi u smislu članka 47. Povelje građanima Unije čiji se podaci prenose u SAD, gdje postoji opasnost da ih američke agencije obrađuju u svrhu nacionalne sigurnosti na način koji nije u skladu s člancima 7. i 8. Povelje. Jamstvima koja su predviđena klauzulama iz Priloga Odluka o SUK-ovima ne rješava se taj nedostatak jer one nisu obvezujuće za tijela ili agencije SAD-a i jer se njima ispitanicima ne daju ugovorna prava u odnosu na izvoznika i/ili uvoznika podataka.

51. U tim okolnostima DPC je smatrao da ne može odlučivati o pritužbi M. Schremsa a da Sud ne ispita valjanost Odluka o SUK-ovima. U skladu s onim što se predviđa u točki 65. presude Schrems, DPC je stoga pokrenuo postupak pred sudom koji je uputio zahtjev kako bi potonji sud, ako se slaže s DPC-ovim dvojbama, podnio Sudu zahtjev za prethodnu odluku u pogledu valjanosti tih odluka.

52. Vladi SAD-a te organizacijama Electronic Privacy Information Centre (u daljnjem tekstu: EPIC), Business Software Alliance (u daljnjem tekstu: BSA) i Digitaleurope odobrena je intervencija pred sudom koji je uputio zahtjev.

53. Kako bi utvrdio slaže li se s dvojbama koje je DPC izrazio u pogledu valjanosti Odluka o SUK-ovima, High Court (Visoki sud) primio je dokaze koje su predočile stranke spora te je saslušao njihove argumente i argumente intervenijenata. Konkretno, vještaci su iznijeli dokaze o odredbama prava SAD-a. U irskom se pravu strano pravo smatra činjeničnim pitanjem koje treba utvrditi dokazom jednako kao i svaku drugu činjenicu. Na temelju tih dokaza sud koji je uputio zahtjev ocijenio je odredbe prava SAD-a kojima se vladinim tijelima i agencijama odobrava nadzor, funkcioniranje dvaju javno priznatih programa nadzora (PRISM i Upstream), razna pravna sredstva dostupna pojedincima čija su prava povrijeđena mjerama nadzora, kao i sustavne zaštitne mjere i mehanizmi nadzora. Taj je sud rezultate te ocjene iznio u presudi od 3. listopada 2017., priloženoj njegovu rješenju kojim se upućuje zahtjev za prethodnu odluku (u daljnjem tekstu: presuda High Courta (Visoki sud) od 3. listopada 2017.).

54. U toj je presudi sud koji je uputio zahtjev uputio, među pravnim temeljima kojima se američkim obavještajnim službama omogućuje presretanje inozemne komunikacije, na članak 702. Foreign Intelligence Surveillance Acta (Zakon o nadzoru stranih obavještajnih informacija, u daljnjem tekstu: FISA) i na Executive Order 12333 (Izvršni nalog br. 12333, u daljnjem tekstu: EO br. 12333).

55. U skladu s utvrđenjima iz navedene presude, na temelju članka 702. FISA-e, Attorney General (državni odvjetnik, SAD) i Director of National Intelligence (direktor Nacionalne obavještajne službe, SAD, u daljnjem tekstu: DNI) mogu zajedno odobriti, na trajanje od godinu dana, u svrhu pribavljanja stranih obavještajnih informacija, nadzor osoba koje nisu američki građani niti imaju trajno boravište u SAD-u (takozvane „osobe koje nisu američki državljani") kada je razumno smatrati da se nalaze izvan državnog područja SAD-a [14]. U skladu s FISA-om, pojam „strane obavještajne informacije" označava informacije o mogućnosti vlade da štiti od inozemnih napada, terorizma, širenja oružja masovnog uništenja, kao i o vođenju vanjskih poslova SAD-a [15].

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

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

56. Ta godišnja odobrenja, kao i postupke kojima se uređuje odabir osoba koje treba nadzirati i obrada (smanjenje količine) prikupljenih informacija[16] treba odobriti Foreign Intelligence Surveillance Court (Sud za nadzor stranih obavještajnih informacija, SAD, u daljnjem tekstu: FISC). Dok „tradicionalni" nadzor koji se provodi na temelju drugih odredbi FISA-e zahtijeva utvrđivanje „vjerojatnog uzroka" na kojem se može temeljiti sumnja u to da nadzirane osobe pripadaju stranoj sili ili da su njezini agenti, nadzorne aktivnosti koje se obavljaju na temelju članka 702. FISA-e nisu uvjetovane ni utvrđivanjem takvog „vjerojatnog uzroka" ni FISC-ovim odobrenjem odabira određenih osoba. K tomu, i dalje u skladu s utvrđenjima suda koji je uputio zahtjev, postupci smanjenja količine podataka ne primjenjuju se na osobe koje nisu američki državljani, a nalaze se izvan SAD-a.

57. U praksi, kada FISC izda odobrenje, NSA šalje pružateljima usluga elektroničke komunikacije sa sjedištem u SAD-u upute koje sadržavaju kriterije pretraživanja, koji se nazivaju „čimbenici za odabir", povezane s ciljanim osobama (kao što su telefonski brojevi ili adrese e-pošte). Ti su pružatelji usluga tada obvezni NSA-i prenijeti podatke koji odgovaraju čimbenicima za odabir i moraju čuvati tajnu u pogledu uputa koje su im dane. Oni mogu FISC-u podnijeti zahtjev kako bi izmijenili ili uklonili neku NSA-inu uputu. Protiv FISC-ove odluke može se podnijeti prigovor pred Foreign Intelligence Surveillance Court of Review (FISCR) (Žalbeni sud za nadzor stranih obavještajnih informacija, SAD, u daljnjem tekstu: FISCR).

58. High Court (Visoki sud) utvrdio je da je članak 702. FISA-e pravni temelj programa PRISM i Upstream.

59. U okviru programa PRISM, pružatelji usluga elektroničke komunikacije dužni su NSA-i podnijeti sve komunikacije koje „šalje" ili „prima" čimbenik za odabir koji je priopćila NSA. Dio tih komunikacija prosljeđuje se FBI-u i Central Intelligence Agencyju (Središnja obavještajna agencija, SAD, u daljnjem tekstu: CIA). U 2015. nadziralo se 94 386 osoba te je u 2011. vlada SAD-a u okviru tog programa prikupila više od 250 milijuna komunikacija.

60. Program Upstream temelji se na obveznoj pomoći poduzetnika koji čine „kostur", odnosno mrežu kablova, preklopnika i usmjerivača, preko kojeg se prenose telefonske i internetske komunikacije. Ti su poduzetnici obvezni NSA-i omogućiti da kopira i filtrira protok internetskog prometa kako bi prikupila komunikacije koje „šalje" ili „prima" čimbenik za odabir naveden u uputi te agencije ili koje se na njega „odnose". Komunikacije koje se „odnose" na čimbenik za odabir jesu komunikacije u kojima se navodi taj čimbenik za odabir a da osoba koja nije američki državljanin povezana s navedenim čimbenikom za odabir ne sudjeluje nužno u njima. Iako iz FISC-ova mišljenja od 26. travnja 2017. proizlazi da od tog datuma američka vlada više ne prikuplja niti stječe komunikacije koje se „odnose" na čimbenik za odabir, u tom se mišljenju ne navodi da NSA prestaje kopirati i filtrirati protok komunikacija koji se prenosi preko njezine nadzorne opreme. Program Upstream tako podrazumijeva da NSA ima pristup metapodacima, kao i sadržaju komunikacija. Od 2011. NSA je prikupljala oko 26,5 milijuna komunikacija godišnje u okviru programa Upstream, što ipak čini samo mali dio komunikacija koje prolaze kroz postupak filtriranja koji se provodi na temelju tog programa.

16 Sud koji je uputio zahtjev utvrdio je da se postupci odabira odnose na način na koji izvršna vlast utvrđuje da je razumno smatrati da je konkretan pojedinac osoba koja nije američki državljanin, a nalazi se izvan SAD-a i da odabir takvog pojedinca može dovesti do stjecanja stranih obavještajnih informacija. Postupci smanjenja količine obuhvaćaju stjecanje, zadržavanje, uporabu i širenje svih informacija o američkim državljanima koje nisu javne i prikupljene su na temelju članka 702. FISA-e.

61. Osim toga, u skladu s utvrđenjima High Courta (Visoki sud), na temelju EO-a br. 12333 odobrava se nadzor elektroničkih komunikacija izvan državnog područja SAD-a, čime se omogućuje pristup, u svrhu prikupljanja stranih obavještajnih informacija, podacima koji su „u prijelazu" do tog državnog područja ili koji „prelaze" preko tog državnog područja, ali za koje ondje nije predviđena obrada, te prikupljanje i zadržavanje tih podataka. U EO-u br. 12333 pojam „strane obavještajne informacije" definira se na način da on uključuje informacije o mogućnostima, namjerama ili aktivnostima stranih vlada, stranih organizacija ili stranih osoba [17].

62. Na temelju EO-a br. 12333 NSA ima ovlašten pristup podmorskim kablovima koji se nalaze na dnu Atlantskog oceana, s pomoću kojih se podaci prenose iz Unije u SAD, prije nego što ti podaci stignu u SAD i tako podlegnu odredbama FISA-e. Međutim, ne postoji nikakav dokaz o bilo kakvom programu uspostavljenom na temelju tog izvršnog naloga.

63. Iako se EO-om br. 12333 predviđaju ograničenja u pogledu prikupljanja, zadržavanja i širenja informacija, ta se ograničenja ne primjenjuju na osobe koje nisu američki državljani. Potonje osobe imaju samo pravo na zaštitne mjere utvrđene u okviru Presidential Policy Directive 28 (Predsjednički ukaz br. 28, u daljnjem tekstu: PPD 28), koji se primjenjuje na sve aktivnosti prikupljanja i upotrebe stranih obavještajnih informacija prikupljenih elektroničkim izviđanjem. PPD-om 28 određuje se da je poštovanje privatnog života sastavni dio razmatranja koja treba uzeti u obzir pri planiranju tih aktivnosti, da jedini cilj prikupljanja treba biti stjecanje stranih obavještajnih informacija, kao i protuobavještajnih informacija te da navedene aktivnosti trebaju biti „što usmjerenije".

64. Sud koji je uputio zahtjev navodi da NSA-ine aktivnosti temeljene na EO-u br. 12333, koji predsjednik SAD-a u bilo kojem trenutku može izmijeniti ili ukinuti, nisu uređene zakonom, nisu predmet sudskog nadzora i protiv njih se ne može podnijeti pravni lijek.

65. Na temelju tih utvrđenja, taj sud smatra da SAD provodi masovne i nediskriminirajuće obrade osobnih podataka koji određene ispitanike mogu izložiti opasnosti od povrede prava koja imaju na temelju članaka 7. i 8. Povelje.

66. Štoviše, navedeni sud tvrdi da građani Unije nemaju pristup istim pravnim lijekovima protiv nezakonitih obrada njihovih osobnih podataka koje provode američka tijela kao i američki državljani. Četvrti amandman Ustava SAD-a, koji čini najvažniju zaštitu od nezakonitog nadziranja, ne primjenjuje se na građane Unije koji nemaju značajnu dobrovoljnu vezu sa SAD-om. Iako potonji građani ipak raspolažu nekim drugim pravnim lijekovima, oni nailaze na znatne prepreke.

67. Konkretno, člankom III. Ustava SAD-a taj se pravni lijek pred saveznim sudovima uvjetuje time da ispitanik mora utvrditi svoju aktivnu procesnu legitimaciju (*standing*). Aktivna procesna legitimacija podrazumijeva, među ostalim, da ta osoba mora dokazati da je pretrpjela stvarnu štetu koja je, s jedne strane, konkretna i osobna te, s druge strane, trenutačna ili neposredna. Upućivanjem, među ostalim, na presudu Supreme Courta of the United States (Vrhovni sud SAD-a), Clapper v. Amnesty International US [18], sud koji je uputio zahtjev smatra da je taj uvjet u praksi pretjerano težak za ispuniti osobito s obzirom na to da ne postoji nikakva obveza da se ispitanike obavijesti o mjerama

17 EO br. 12333, točka 3.5., podtočka (e)

18 133 S.Ct. 1138 (2013.)

nadzora koje su u pogledu njih donesene [19]. Dio pravnih lijekova kojima raspolažu građani Unije usto podliježe drugim ograničavajućim uvjetima, kao što je potreba utvrđivanja novčane štete. Suvereni imunitet priznat obavještajnim agencijama i klasifikacija predmetnih informacija također su prepreka podnošenju određenih pravnih lijekova [20].

68. High Court (Visoki sud) usto navodi razne mehanizme nadzora i nadgledanja aktivnosti obavještajnih agencija.

69. Među tim se mehanizmima navodi, s jedne strane, mehanizam FISC-ova godišnjeg certificiranja programa koji se temelje na članku 702. FISA-e, u okviru kojeg FISC ipak ne odobrava pojedinačne čimbenike za odabir. Osim toga, nikakvim se prethodnim sudskim nadzorom ne uređuje prikupljanje stranih obavještajnih informacija na temelju EO-a br. 12333.

70. S druge strane, sud koji je uputio zahtjev upućuje na nekoliko mehanizama izvansudskog nadgledanja obavještajnih aktivnosti. Konkretno, navodi ulogu Inspectors Generala (glavni inspektori, SAD) koji su, unutar svake obavještajne agencije, zaduženi za nadgledanje nadzornih aktivnosti. K tomu, Privacy and Civil Liberties Oversight Board (Odbor za nadzor privatnosti i građanskih sloboda, SAD, u daljnjem tekstu: PCLOB), neovisna agencija unutar izvršne vlasti, prima izvješća osoba koje su u okviru svake agencije imenovane kao službenici za građanske slobode ili privatnost (*civil liberties or privacy officers*). PCLOB redovno priprema izvješća za kongresne odbore i Predsjednika. Predmetne agencije moraju o incidentima koji se odnose na povredu pravila i postupaka kojima je uređeno prikupljanje stranih obavještajnih informacija obavijestiti, među ostalim, DNI-ja. Ti se incidenti također priopćuju FISC-u. I sam kongres SAD-a, posredstvom obavještajnih odbora Zastupničkog doma i Senata, ima odgovornost nadzirati strane obavještajne aktivnosti.

71. Međutim, High Court (Visoki sud) ističe temeljnu razliku između, s jedne strane, pravila kojima se nastoji osigurati da su podaci prikupljeni zakonito i da ih se, kada su prikupljeni, ne zloupotrebljava te, s druge strane, pravnih lijekova dostupnih kada su ta pravila povrijeđena. Zaštita temeljnih prava ispitanika osigurana je samo ako im djelotvorni pravni lijekovi omogućuju ostvarivanje prava u slučaju povrede navedenih pravila.

72. U tim okolnostima, sud koji je uputio zahtjev smatra da su utemeljeni DPC-ovi argumenti, prema kojima ograničenja koja su američkim pravom uspostavljena u pogledu prava na pravni lijek osoba čiji su podaci preneseni iz Unije ne poštuju ključni sadržaj prava zajamčenog člankom 47. Povelje i, u svakom slučaju, čine neproporcionalna miješanja u ostvarivanje tog prava.

73. High Court (Visoki sud) smatra da ta ocjena nije dovedena u pitanje time što je vlada SAD-a uvela mehanizam pravobranitelja opisan u Odluci o sustavu zaštite privatnosti. Nakon što je naglasio da tom mehanizmu mogu pristupiti građani Unije koji razumno smatraju da su njihovi podaci preneseni u skladu s Odlukama o SUK-ovima [21], taj je sud napomenuo da pravobranitelj nije sud koji ispunjava zahtjeve iz članka 47. Povelje i da, konkretno, nije neovisan o izvršnoj vlasti [22]. Navedeni sud također dvoji u pogledu toga je li intervencija pravobranitelja, protiv čijih se odluka ne može podnijeti pravni lijek, djelotvoran pravni lijek. Naime, tom se intervencijom osobama čiji su osobni podaci nezakonito prikupljeni, obrađeni ili dijeljeni ne omogućuje da dobiju naknadu štete ili nalog za prestanak nezakonitih radnji jer pravobranitelj ne potvrđuje niti poriče da je ispitanik bio predmet mjere elektroničkog nadzora.

19 Sud koji je uputio zahtjev ipak je utvrdio da se na načelo prema kojem nije potrebno obavješćivanje osobe na koju se odnosi mjera nadzora primjenjuje iznimka kada američka vlada želi podatke prikupljene na temelju članka 702. FISA-e upotrijebiti protiv te osobe u okviru kaznenog ili upravnog postupka.

20 Konkretno, sud koji je uputio zahtjev istaknuo je da, iako su Judicial Redress Actom (Zakon o sudskoj zaštiti, u daljnjem tekstu: JRA) odredbe Privacy Acta (Zakon o zaštiti privatnog života), kojim se fizičkim osobama omogućuje pristup informacijama koje se odnose na njih i koje neke agencije posjeduju u pogledu određenih trećih zemalja, proširene na građane Unije, NSA nije među agencijama navedenima u JRA-i.

21 Sud koji je uputio zahtjev u tom pogledu upućuje na Prilog III. A Odluke o sustavu zaštite privatnosti (vidjeti točke 37. i 38. ovog mišljenja).

22 Sud koji je uputio zahtjev poziva se na presudu od 27. siječnja 2005., Denuit i Cordenier (C-125/04, EU:C:2005:69, t. 12.).

74. Budući da je tako iznio svoje dvojbe o bitnoj ekvivalentnosti zaštitnih mjera predviđenih američkim pravom i zahtjeva koji proizlaze iz članaka 7., 8. i 47. Povelje, sud koji je uputio zahtjev izjavio je da dvoji u pogledu toga da standardne ugovorne klauzule predviđene u Odlukama o SUK-ovima, koje po svojoj prirodi ne obvezuju američka tijela, ipak mogu osigurati zaštitu temeljnih prava ispitanika. Taj je sud iz toga zaključio da se slaže s DPC-ovim dvojbama u pogledu valjanosti tih odluka.

75. U tom pogledu, sud koji je uputio zahtjev konkretno smatra da za otklanjanje tih dvojbi nije dovoljan članak 28. stavak 3. Direktive 95/46, na koji se upućuje u članku 4. Odluke 2010/87, u dijelu u kojem se nadzornim tijelima daje ovlast obustave ili zabrane prijenosa koji se temelje na standardnim ugovornim klauzulama predviđenim u toj odluci. Osim što je ta ovlast, prema njegovu mišljenju, samo diskrecijska, sud koji je uputio zahtjev pita, s obzirom na uvodnu izjavu 11. Odluke 2010/87, je li tu ovlast moguće izvršiti kada se utvrđeni nedostaci ne odnose na pojedinačan i izniman slučaj, nego kada su ti nedostaci opći i sustavni [23]. Također smatra da se povjeravanju utvrđivanja takvih nedostataka nadzornim tijelima može protiviti opasnost od donošenja drukčijih odluka u različitim državama članicama.

76. U tim je okolnostima High Court (Visoki sud) odlukom od 4. svibnja 2018. [24], koju je Sud zaprimio 9. svibnja 2018., odlučio prekinuti postupak i postaviti Sudu sljedeća prethodna pitanja:

„1. Kada privatno trgovačko društvo iz države članice [Unije] u komercijalne svrhe prenosi osobne podatke privatnom trgovačkom društvu u trećoj zemlji na temelju Odluke [2010/87] te bi tijela treće zemlje te podatke mogla podvrgnuti daljnjoj obradi za potrebe nacionalne sigurnosti, ali i za potrebe izvršavanja zakonodavstva i vođenja vanjskih poslova te treće zemlje, primjenjuje li se pravo Unije[, uključujući Povelju,] na prijenos podataka, neovisno o odredbama članka 4. stavka 2. UEU-a koje se odnose na nacionalnu sigurnost i odredbama članka 3. stavka 2. prve alineje Direktive [95/46] koje se odnose na javnu sigurnost, obranu i nacionalnu sigurnost?

2. (a) Pri utvrđivanju jesu li prava pojedinca povrijeđena prijenosom podataka na temelju Odluke [2010/87] iz Unije u treću zemlju, gdje ti podaci mogu biti podvrgnuti daljnjoj obradi za potrebe nacionalne sigurnosti, je li za potrebe Direktive [95/46] relevantno mjerilo za usporedbu:

i. Povelja, UEU, UFEU, Direktiva [95/46], [Europska konvencija za zaštitu ljudskih prava i temeljnih sloboda, potpisana u Rimu 4. studenoga 1950. (u daljnjem tekstu: EKLJP)] (ili bilo koja druga odredba prava Unije); ili

ii. nacionalno zakonodavstvo jedne ili više država članica?

(b) Ako je ii. relevantno mjerilo za usporedbu, trebaju li dio takvog mjerila biti i prakse koje se u kontekstu nacionalne sigurnosti primjenjuju u jednoj ili više država članica?

23 U uvodnoj izjavi 11. Odluke 2010/87 navodi se: „Nadzorna tijela država članica igraju ključnu ulogu u ovom ugovornom mehanizmu osiguravajući da su tijekom prijenosa osobni podaci odgovarajuće zaštićeni. U iznimnim slučajevima kada izvoznici podataka odbiju ili nisu u stanju dati odgovarajuće upute uvozniku podataka, te kada postoji neizbježna opasnost od nanošenja teške štete osobama na koje se odnose podaci, standardne ugovorne klauzule trebaju omogućiti nadzornim tijelima reviziju uvoznika podataka i podobrađivača te, gdje je to prikladno, donesu odluke koje obvezuju uvoznike podataka i podobrađivače. Nadzorna tijela trebaju imati moć da zabrane ili obustave prijenos podataka ili skup prijenosa na temelju standardnih ugovornih klauzula u takvim iznimnim slučajevima u kojima se ustanovi da je vjerojatno da prijenos na ugovornoj osnovi ima značajan nepovoljni učinak na jamstva i obveze koji osiguravaju odgovarajuću zaštitu korisnika."

24 Facebook Ireland podnio je žalbu protiv odluke kojom se upućuje zahtjev za prethodnu odluku Supreme Courtu (Vrhovni sud, Irska). Ta je žalba odbijena presudom od 31. svibnja 2019., The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Appeal n°2018/68 (u daljnjem tekstu: presuda Supreme Courta (Vrhovni sud) od 31. svibnja 2019.).

3. Kada se za potrebe članka 26. Direktive [95/46] ocjenjuje osigurava li treća zemlja za podatke koji se prenose u tu zemlju razinu zaštite koju zahtijeva pravo Unije, treba li razinu zaštite u trećoj zemlji ocijeniti s obzirom na:

   (a) primjenjiva pravila u trećoj zemlji koja proizlaze iz domaćih propisa ili međunarodnih obveza i praksu kojoj je svrha osigurati poštovanje tih pravila, uključujući strukovna pravila i sigurnosne mjere u toj trećoj zemlji;

   ili

   (b) pravila pod (a) i upravne, regulatorne i provedbene prakse te sustavna jamstva, postupke, protokole, nadzorne mehanizme i izvansudske pravne lijekove koji postoje u trećoj zemlji?

4. S obzirom na utvrđenja High Courta (Visoki sud) u pogledu prava [SAD-a], radi li se o povredi pravâ pojedinaca iz članka 7. i/ili članka 8. Povelje ako se osobni podaci prenose iz Unije u [SAD] na temelju Odluke [2010/87]?

5. S obzirom na utvrđenja High Courta (Visoki sud) u pogledu prava [SAD-a], ako se osobni podaci prenose iz Unije u [SAD] na temelju Odluke [2010/87]:

   (a) Poštuje li razina zaštite koju pruža [SAD] bit prava pojedinca na pravni lijek protiv povrede njegovih prava na privatnost zajamčenih člankom 47. Povelje?

Ako je odgovor na (a) potvrdan,

   (b) Jesu li ograničenja prava pojedinca na pravni lijek koja pravo [SAD-a] predviđa u kontekstu nacionalne sigurnosti [SAD-a] neproporcionalna u smislu članka 52. Povelje te prekoračuju li ono što je u demokratskom društvu nužno za potrebe nacionalne sigurnosti?

6. (a) Koju razinu zaštite, s obzirom na odredbe Direktive [95/46], a osobito s obzirom na njezine članke 25. i 26. tumačene u vezi s Poveljom, treba pružiti osobnim podacima koji se u treću zemlju prenose na temelju standardnih ugovornih klauzula usvojenih u skladu s odlukom Komisije utemeljenom na članku 26. stavku 4. [te direktive]?

   (b) Koje čimbenike treba uzeti u obzir u ocjeni ispunjava li razina zaštite podataka koji se prenose u treću zemlju na temelju Odluke [2010/87] zahtjeve iz Direktive [95/46] i Povelje?

7. Onemogućuje li činjenica da se standardne ugovorne klauzule primjenjuju na odnos izvoznika podataka i uvoznika podataka te da ne obvezuju nacionalna tijela treće zemlje, koja od uvoznika podataka mogu zatražiti da sigurnosnim službama te zemlje stavi na raspolaganje osobne podatke prenesene na temelju klauzula Odluke [2010/87], da se u tim klauzulama predvide dovoljna jamstva u skladu s člankom 26. stavkom 2. Direktive [95/46]?

8. Ako uvoznik podataka s poslovnim nastanom u trećoj zemlji podliježe zakonima o nadzoru koje [nadzorno tijelo] smatra suprotnima standardnim ugovornim klauzulama ili člancima 25. i 26. Direktive [95/46] ili Povelji, mora li [nadzorno tijelo] upotrijebiti svoje ovlasti iz članka 28. stavka 3. Direktive [95/46] kako bi suspendiralo protoke podataka ili je upotreba tih ovlasti ograničena samo na iznimne slučajeve, s obzirom na uvodnu izjavu 11. [Odluke 2010/87], ili [nadzorno] tijelo može diskrecijski odlučiti da neće suspendirati protoke podataka?

9. (a) Za potrebe članka 25. stavka 6. Direktive [95/46], čini li Odluka [o sustavu zaštite privatnosti] utvrđenje opće primjene koje obvezuje [nadzorna tijela] i sudove država članica da smatraju da [SAD] u svojim propisima ili na temelju međunarodnih obveza koje [je] preuze[o osigurava] odgovarajuću razinu zaštite u smislu članka 25. stavka 2. Direktive [95/46]?

(b) Ako ne čini, koliko je Odluka o sustavu zaštite privatnosti relevantna, ako je uopće relevantna, u ocjeni dostatnosti jamstava predviđenih u pogledu podataka koji se u [SAD] prenose na temelju Odluke [2010/87]?

10. S obzirom na utvrđenja High Courta (Visoki sud) u pogledu prava [SAD-a], znači li uspostava mehanizma pravobranitelja za zaštitu podataka na temelju [Priloga III A] Odluci o sustavu zaštite privatnosti, kada ju se promatra u vezi s postojećim uređenjem u [SAD-u], da [SAD] osobama čiji se [osobni] podaci prenose u [SAD] na temelju Odluke [2010/87 osigurava] pravni lijek koji je u skladu s člankom 47. Povelje?

11. Povrjeđuje li se [Odlukom 2010/87] članak 7. i/ili članak 8. i/ili članak 47. Povelje?"

77. DPC, Facebook Ireland, M. Schrems, vlada SAD-a, EPIC, BSA, Digitaleurope, Irska, belgijska, češka, njemačka, nizozemska, austrijska, poljska i portugalska vlada te vlada Ujedinjene Kraljevine, Europski parlament i Komisija podnijeli su pisana očitovanja Sudu. DPC, Facebook Ireland, M. Schrems, vlada SAD-a, EPIC, BSA, Digitaleurope, Irska, njemačka, francuska, nizozemska i austrijska vlada te vlada Ujedinjene Kraljevine, Parlament, Komisija i Europski odbor za zaštitu podataka (European Data Protection Board; u daljnjem tekstu: EOZP) 9. srpnja 2019. bili su zastupani na raspravi.

IV. Analiza

A. Uvodna razmatranja

78. Nakon što je Sud u presudi Schrems proglasio nevaljanom Odluku o privatnosti „sigurne luke", prijenosi osobnih podataka u SAD nastavili su se na drugim pravnim temeljima. Konkretno, društva za izvoz podataka mogla su sklapati ugovore s uvoznicima podataka koji su uključivali standardne klauzule koje je sastavila Komisija. Te klauzule također služe kao pravni temelj za prijenose u brojne druge treće zemlje u pogledu kojih Komisija nije donijela odluku o primjerenosti [25]. Odlukom o sustavu zaštite privatnosti sada se poduzetnicima koji su samocertificirali pridržavanje načela navedenih u toj odluci omogućuje prijenos osobnih podataka u SAD bez drugih formalnosti.

79. Kao što se to izričito navodi u odluci kojom se upućuje zahtjev za prethodnu odluku i kao što su to istaknuli BSA, Digitaleurope, Irska, austrijska i francuska vlada, Parlament i Komisija, glavni postupak koji je u tijeku pred High Courtom (Visoki sud) ima za jedini cilj utvrditi valjanost odluke kojom je Komisija uvela standardne ugovorne klauzule istaknute u prilog prijenosima na koje se odnosi pritužba M. Schremsa, odnosno Odluke 2010/87 [26].

80. Taj spor proizlazi iz pritužbe kojom je DPC od suda koji je uputio zahtjev tražio da uputi Sudu prethodno pitanje u pogledu valjanosti Odluke 2010/87. Taj sud tvrdi da se glavni postupak stoga odnosi na podnošenje pravnog lijeka čije je uvođenje Sud naložio državama članicama u točki 65. presude Schrems.

25 BSA tvrdi da je 70 % poduzetnika koji su članovi tog udruženja i koji su odgovorili na anketu na tu temu izjavili da su se koristili standardnim ugovornim klauzulama kao glavnim temeljem za prijenos osobnih podataka u treće zemlje. Digitaleurope također smatra da su standardne ugovorne klauzule glavni pravni instrument koji se ističe u prilog tim prijenosima.

26 Iako sud koji je uputio zahtjev navodi da se njegov zahtjev za prethodnu odluku odnosi na valjanost triju Odluka o SUK-ovima, pri čemu su te odluke ispitane u DPC-ovu nacrtu odluke i u presudi od 3. listopada 2017., prethodna pitanja pozivaju se isključivo na Odluku 2010/87. To je slučaj jer je Facebook Ireland pred tim sudom utvrdio tu odluku kao pravni temelj za prijenose podataka europskih korisnika društvene mreže Facebook u SAD. Moja će se analiza stoga odnositi samo na navedenu odluku.

81. Podsjećam da je Sud u točki 63. te presude odlučio da nadzorno tijelo mora sa svom dužnom pažnjom ispitati pritužbu u okviru koje određena osoba, čiji su osobni podaci preneseni ili mogli biti preneseni u treću zemlju na koju se odnosi odluka o primjerenosti, osporava usklađenost te odluke s temeljnim pravima koja su zajamčena Poveljom. U skladu s točkom 65. navedene presude, u slučaju kada to tijelo smatra da su prigovori istaknuti u toj pritužbi osnovani, to isto tijelo mora u skladu s člankom 28. stavkom 3. prvim podstavkom trećom alinejom Direktive 95/46 (koja odgovara članku 58. stavku 5. GDPR-a), povezano osobito s člankom 8. stavkom 3. Povelje, imati ovlasti za sudjelovanje u sudskim postupcima. U tom pogledu, nacionalni zakonodavac treba utvrditi pravne lijekove koji omogućuju isticanje tih prigovora pred nacionalnim sudovima kako bi oni mogli, ako se slažu s dvojbama navedenog tijela, podnijeti zahtjev za prethodnu odluku u pogledu valjanosti predmetne odluke.

82. Kao i sud koji je uputio zahtjev, smatram da se ti zaključci po analogiji primjenjuju kada povodom obrade pritužbe podnesene nadzornom tijelu, to tijelo ne dvoji o valjanosti odluke o primjerenosti, nego odluke, kao što je Odluka 2010/87, kojom se utvrđuju standardne ugovorne klauzule za prijenos osobnih podataka u treće zemlje. Protivno onomu što navodi njemačka vlada, nije relevantno što te dvojbe odgovaraju prigovorima koje mu je podnio podnositelj pritužbe ili što to tijelo samo dovodi u pitanje valjanost predmetne odluke. Naime, zahtjevi iz članka 58. stavka 5. GDPR-a i članka 8. stavka 3. Povelje, na kojima se temelji obrazloženje Suda, primjenjuju se neovisno o pravnom temelju prijenosa na koji se odnosi pritužba podnesena nadzornom tijelu i razlozima zbog kojih to tijelo dvoji o valjanosti predmetne odluke u okviru obrade te pritužbe.

83. Unatoč tomu, DPC je od suda koji je uputio zahtjev zatražio da pita Sud o valjanosti Odluke 2010/87 upravo zato što smatra da je u tom pogledu pojašnjenje Suda potrebno za odlučivanje o pritužbi kojom M. Schrems od njega traži da izvrši ovlast, koja mu je bila povjerena člankom 28. stavkom 3. drugom alinejom Direktive 95/46 i koju sada ima na temelju članka 58. stavka 2. točke (f) GDPR-a, i obustavi da Facebook Ireland prenosi Facebooku Inc. osobne podatke koji se odnose na njega.

84. Stoga, dok se glavni postupak odnosi samo na valjanost *in abstracto* Odluke 2010/87, postupak iz kojeg proizlazi taj postupak i koji je u tijeku pred DPC-om odnosi se na njegovo izvršavanje ovlasti donošenja korektivnih mjera *u konkretnom slučaju*. Predložit ću Sudu da postavljena pitanja ispita samo koliko je potrebno da bi se odlučilo o valjanosti Odluke 2010/87 jer će takvo ispitivanje biti dovoljno kako bi sud koji je uputio zahtjev mogao riješiti spor koji se pred njim vodi[27].

85. Prije ocjene valjanosti te odluke, treba odbiti određene prigovore istaknute u pogledu dopuštenosti zahtjeva za prethodnu odluku.

B. Dopuštenost zahtjeva za prethodnu odluku

86. Dopuštenost zahtjeva za prethodnu odluku osporavana je iz nekoliko razloga koji se u biti odnose na neprimjenjivost *ratione temporis* Direktive 95/46 iz prethodnih pitanja (dio 1), na činjenicu da postupak pred DPC-om nije u dovoljno uznapredovaloj fazi da bi se opravdala njegova korisnost (dio 2) i na daljnje neizvjesnosti u pogledu činjeničnog okvira koji je opisao sud koji je uputio zahtjev (dio 3).

27 Vidjeti točke 167. do186. ovog mišljenja.

87. Na te ću argumente o postojanju zapreke vođenju postupka odgovoriti uzimajući u obzir pretpostavku relevantnosti koja se primjenjuje na pitanja upućena Sudu na temelju članka 267. UFEU-a. Prema ustaljenoj sudskoj praksi, Sud može odbiti odlučivati o zahtjevu za prethodnu odluku samo ako je očito da zatraženo tumačenje prava Unije nema nikakve veze s činjeničnim stanjem ili predmetom spora u glavnom postupku, ako je problem hipotetski ili ako Sud ne raspolaže činjeničnim i pravnim elementima potrebnima za davanje korisnog odgovora na upućena pitanja [28].

1. Primjenjivost ratione temporis Direktive 95/46

88. Facebook Ireland ističe da su prethodna pitanja nedopuštena jer se u njima upućuje na Direktivu 95/46, iako je ta direktiva stavljena izvan snage i zamijenjena GDPR-om s učinkom od 25. svibnja 2018. [29].

89. Slažem se sa stajalištem prema kojem valjanost Odluke 2010/87 treba ispitati s obzirom na odredbe GDPR-a.

90. U skladu s člankom 94. stavkom 2. te uredbe, „[u]pućivanja na direktivu koja je stavljena izvan snage tumače se kao upućivanja na [navedenu uredbu]". Čini mi se da iz toga proizlazi da Odluku 2010/87, u dijelu u kojem se u njoj kao pravni temelj navodi članak 26. stavak 4. Direktive 95/46, treba shvatiti kao da se u njoj upućuje na članak 46. stavak 2. točku (c) GDPR-a u kojem je u biti preuzet njegov sadržaj [30]. Prema tome, provedbene odluke koje je Komisija donijela na temelju članka 26. stavka 4. Direktive 95/46 prije stupanja na snagu GDPR-a treba tumačiti s obzirom na tu uredbu. Njihovu valjanost treba također, ako je potrebno, ocijeniti s obzirom na navedenu uredbu.

91. Taj se zaključak ne dovodi u pitanje sudskom praksom prema kojoj zakonitost akta Unije treba ocijeniti u skladu s činjeničnim i pravnim elementima koji su postojali na dan kada je taj akt donesen. Naime, ta se sudska praksa odnosi na ispitivanje valjanosti akta Unije s obzirom na činjenične okolnosti koje su bile relevantne prilikom njegova donošenja [31] ili na postupovna pravila kojima je uređeno njegovo donošenje [32]. Suprotno tomu, Sud je više puta ispitao valjanost akata sekundarnog prava s obzirom na viša materijalna pravna pravila koja su na bila na snazi nakon donošenja tih akata [33].

92. Međutim, iako navođenje, u tekstu prethodnih pitanja, akta koji više nije primjenjiv *ratione temporis* opravdava preoblikovanje tih pitanja, ono ne može dovesti do njihove nedopuštenosti [34]. Kao što su to tvrdili DPC i M. Schrems, upućivanja na Direktivu 95/46 u tekstu prethodnih pitanja mogu se uostalom objasniti vremenskim okvirom postupka u ovom predmetu, pri čemu su ta pitanja upućena Sudu prije stupanja na snagu GDPR-a.

28 Vidjeti osobito presude od 10. prosinca 2018., Wightman i dr. (C-621/18, EU:C:2018:999, t. 27.) i od 19. studenoga 2019., A. K. i dr. (Neovisnost disciplinskog vijeća Vrhovnog suda) (C-585/18, C-624/18 i C-625/18, EU:C:2019:982, t. 98.).

29 Vidjeti članak 94. stavak 1. i članak 99. stavak 1. GDPR-a.

30 Ističem da, u skladu s člankom 46. stavkom 5. GDPR-a, odluke koje je Komisija donijela na temelju članka 26. stavka 4. Direktive 95/46 ostaju na snazi dok se ne izmijene, zamijene ili stave izvan snage.

31 Vidjeti osobito presude od 7. veljače 1979., Francuska/Komisija (15/76 i 16/76, EU:C:1979:29, t. 7.); od 17. svibnja 2001., IECC/Komisija (C-449/98 P, EU:C:2001:275, t. 87.) i od 17. listopada 2013., Schaible (C-101/12, EU:C:2013:661, t. 50.).

32 Vidjeti osobito presude od 16. travnja 2015., Parlament/Vijeće (C-540/13, EU:C:2015:224, t. 35.); od 16. travnja 2015., Parlament/Vijeće (C-317/13 i C-679/13, EU:C:2015:223, t. 45.) i od 22. rujna 2016., Parlament/Vijeće (C-14/15 i C-116/15, EU:C:2016:715, t. 48.).

33 Konkretno, u presudi Schrems Sud je ocijenio valjanost Odluke o privatnosti „sigurne luke" s obzirom na odredbe Povelje, koja je donesena nakon te odluke. Vidjeti i presude od 17. ožujka 2011., AJD Tuna (C-221/09, EU:C:2011:153, t. 48.) i od 11. lipnja 2015., Pfeifer & Langen (C-51/14, EU:C:2015:380, t. 42.).

34 Vidjeti osobito presude od 15. srpnja 2010., Pannon Gép Centrum (C-368/09, EU:C:2010:441, t. 30. do 35.); od 10. veljače 2011., Andersson (C-30/10, EU:C:2011:66, t. 20. i 21.), kao i od 25. listopada 2018., Roche Lietuva (C-413/17, EU:C:2018:865, t. 17. do 20.).

93. U svakom slučaju, u odredbama GDPR-a koje ću ispitati u svrhu analize prethodnih pitanja, odnosno konkretno u njezinim člancima 45., 46. i 58., u biti je preuzet, uz neke dopune i manje izmjene, sadržaj članaka 25., 26. i 28. Direktive 95/46. Što se tiče njihovih aspekata relevantnih za odlučivanje o valjanosti Odluke 2010/87, ne vidim nijedan razlog iz kojeg bi se tim odredbama GDPR-a dao drukčiji doseg u odnosu na odgovarajuće odredbe Direktive 95/46[35].

2. Privremenost dvojbi koje je izrazio DPC

94. Prema mišljenju njemačke vlade, zahtjev za prethodnu odluku nedopušten je jer postupak povodom pravnog sredstva iz točke 65. presude Schrems podrazumijeva da nadzorno tijelo iznese konačno mišljenje o osnovanosti prigovora koje je podnositelj pravnog sredstva istaknuo protiv valjanosti predmetne odluke. To ovdje nije slučaj jer je DPC izrazio dvojbe u pogledu valjanosti Odluke 2010/87, koju M. Schrems osim toga ne osporava, u nacrtu odluke koji je donesen privremeno ne dovodeći u pitanje dodatna očitovanja koja će eventualno podnijeti Facebook Ireland i M. Schrems.

95. Prema mojem mišljenju, privremenost dvojbi koje je izrazio DPC ne utječe na dopuštenost zahtjeva za prethodnu odluku. Naime, kriterije dopuštenosti prethodnog pitanja treba ocijeniti s obzirom na predmet spora kako ga je definirao sud koji je uputio zahtjev[36]. Međutim, nesporno je da je predmet spora valjanost Odluke 2010/87. U skladu s odlukom kojom se upućuje zahtjev za prethodnu odluku i presudom koja joj je priložena, taj je sud smatrao da su dvojbe koje je izrazio DPC, a da pritom nije važno jesu li one bile privremene ili konačne, osnovane te je posljedično pitao Sud o valjanosti te odluke. U tim okolnostima, pojašnjenje Suda u tom pogledu nedvojbeno je relevantno za rješavanje spora koji je pred njim pokrenut.

3. Neizvjesnosti u pogledu utvrđivanja činjeničnog okvira

96. Vlada Ujedinjene Kraljevine tvrdi da činjenični okvir koji je opisao sud koji je uputio zahtjev ima nekoliko nedostataka koji dovode u pitanje dopuštenost prethodnih pitanja. Taj sud nije pojasnio jesu li osobni podaci koji se odnose na M. Schremsa stvarno preneseni u SAD niti, ako jesu, jesu li ih američka tijela prikupila. Nije sa sigurnošću utvrđen ni pravni temelj tih eventualnih prijenosa s obzirom na to da se u odluci kojom se upućuje zahtjev za prethodnu odluku samo navodi da su podaci europskih korisnika društvene mreže Facebook „uvelike" preneseni na temelju standardnih ugovornih klauzula predviđenih Odlukom 2010/87. U svakom slučaju, nije utvrđeno da ugovor između Facebooka Ireland i Facebooka Inc., na koji se upućuje u prilog spornom prijenosu, vjerno odražava te klauzule. Njemačka vlada također osporava dopuštenost zahtjeva za prethodnu odluku jer sud koji je uputio zahtjev nije ispitao je li M. Schrems nedvojbeno dao pristanak za predmetne prijenose, u kojem slučaju bi se ti prijenosi valjano temeljili na članku 26. stavku 1. Direktive 95/46 (čiji je sadržaj u biti preuzet u članku 49. stavku 1. točki (a) GDPR-a).

97. Tim se argumentima nipošto ne dovodi u pitanje relevantnost zahtjeva za prethodnu odluku s obzirom na predmet glavnog postupka. Budući da je taj spor nastao tako što je DPC podnio pravno sredstvo predviđeno u točki 65. presude Schrems, sam njegov predmet odnosi se na to da se od nacionalnog suda zatraži da podnese zahtjev za prethodnu odluku u pogledu valjanosti Odluke 2010/87. Njemačka vlada i vlada Ujedinjene Kraljevine zapravo ne osporavaju nužnost prethodnih pitanja za utvrđivanje je li ta odluka valjana, nego za to da bi DPC mogao odlučiti *in concreto* o pritužbi M. Schremsa.

35 Vidjeti u tom pogledu mišljenje nezavisnog odvjetnika M. Bobeka u predmetu Fashion ID (C-40/17, EU:C:2018:1039, t. 87.).

36 Vidjeti točku 87. ovog mišljenja.

98. U svakom slučaju, prethodna pitanja o valjanosti Odluke 2010/87 nisu nerelevantna ni sa stajališta tog postupka iz kojeg proizlazi glavni postupak. Naime, sud koji je uputio zahtjev utvrdio je da je Facebook Ireland nastavio prenositi podatke svojih korisnika u SAD nakon što je Odluka o privatnosti „sigurne luke" proglašena nevaljanom i da su se ti prijenosi, barem djelomično, temeljili na Odluci 2010/87. Usto, iako može predstavljati prednost to da su sve relevantne činjenice utvrđene prije nego što je izvršio nadležnost na temelju članka 267. UFEU-a, na samom je sudu koji je uputio zahtjev da ocijeni u kojoj mu fazi postupka treba prethodna odluka Suda [37].

99. S obzirom na sve prethodno navedeno, smatram da je zahtjev za prethodnu odluku dopušten.

C. Primjenjivost prava Unije na prijenose u komercijalne svrhe osobnih podataka u treću državu koja bi ih mogla obraditi za potrebe nacionalne sigurnosti (prvo pitanje)

100. Svojim prvim pitanjem sud koji je uputio zahtjev želi znati primjenjuje li se pravo Unije na prijenos osobnih podataka koji provodi društvo koje se nalazi u državi članici u korist društva sa sjedištem u trećoj zemlji iz komercijalnih razloga kada, nakon što je prijenos započet, javna tijela te zemlje mogu obraditi podatke u svrhu, među ostalim, zaštite nacionalne sigurnosti.

101. To je pitanje važno za rješavanje glavnog postupka jer bi se, ako takav prijenos ne bi bio obuhvaćen područjem primjene prava Unije, pokazalo da su svi prigovori istaknuti protiv valjanosti Odluke 2010/87 u ovom predmetu neutemeljeni.

102. Kao što je to napomenuo sud koji je uputio zahtjev, obrade podataka čiji je cilj nacionalna sigurnost isključene su iz područja primjene Direktive 95/46 na temelju njezina članka 3. stavka 2. Člankom 2. stavkom 2. GDPR-a sada se pojašnjava da se ta uredba ne primjenjuje, među ostalim, na obradu podataka tijekom djelatnosti koja nije obuhvaćena opsegom prava Unije ili koju obavljaju nadležna tijela u svrhu zaštite javne sigurnosti. Te odredbe održavaju pridržaj ovlasti koji se člankom 4. stavkom 2. UEU-a priznaje državama članicama u području zaštite nacionalne sigurnosti.

103. DPC, M. Schrems, Irska, njemačka, austrijska, belgijska, češka, nizozemska, poljska i portugalska vlada, kao i Parlament i Komisija tvrde da prijenosi kao što su oni na koje se odnosi pritužba M. Schremsa nisu obuhvaćeni tim odredbama i da su stoga obuhvaćeni područjem primjene prava Unije. Facebook Ireland zagovara suprotnu tezu. Ja se slažem s prvonavedenim stajalištem.

104. U tom pogledu, važno je istaknuti da je prijenos osobnih podataka iz države članice u treću zemlju, kao takav, „obrada" u smislu članka 4. točke 2. GDPR-a koja je provedena na državnom području države članice [38]. Cilj je prvog prethodnog pitanja upravo utvrditi primjenjuje li se pravo Unije *na obradu koja obuhvaća sam prijenos*. To se pitanje ne odnosi na primjenjivost prava Unije na eventualne kasnije obrade koje američka tijela provode u svrhu nacionalne sigurnosti u pogledu podataka prenesenih u SAD, koje nisu obuhvaćene teritorijalnim područjem primjene GDPR-a [39].

37 Vidjeti u tom smislu presude od 1. travnja 1982., Holdijk i dr. (141/81 do 143/81, EU:C:1982:122, t. 5.) i od 9. prosinca 2003., Gasser (C-116/02, EU:C:2003:657, t. 27.).

38 Vidjeti u tom smislu presudu od 30. svibnja 2006., Parlament/Vijeće i Komisija (C-317/04 i C-318/04, EU:C:2006:346, u daljnjem tekstu: presuda PNR, t. 56.), kao i presudu Schrems (t. 45.). U članku 4. točki 2. GDPR-a u biti je preuzeta definicija pojma „obrada" iz članka 2. točke (b) Direktive 95/46.

39 U skladu s člankom 3. stavkom 1. GDPR-a, ta se uredba odnosi na svaku obradu u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u Uniji, neovisno o tome obavlja li se obrada u Uniji ili ne. Pitanje primjenjivosti prava Unije na obrade koje provode obavještajne službe treće zemlje izvan Unije treba razlikovati od pitanja relevantnosti pravila i praksa koje se na te obrade primjenjuju u dotičnoj trećoj zemlji radi utvrđivanja je li u toj zemlji osigurana primjerena razina zaštite. Potonja je tema predmet drugog prethodnog pitanja te ću nju razmotriti u točkama 201. do 229. ovog mišljenja.

105. S tog stajališta, u svrhu utvrđivanja primjenjuje li se pravo Unije na predmetni prijenos podataka jedino treba uzeti u obzir aktivnost u okviru koje se provodi taj prijenos a da pritom nije važan cilj eventualnih kasnijih obrada podataka koje su javna tijela prenijela u treću zemlju odredišta [40].

106. Međutim, iz odluke kojom se upućuje zahtjev za prethodnu odluku proizlazi da je prijenos na koji se odnosi pritužba M. Schremsa dio komercijalne aktivnosti. Usto, taj prijenos nije proveden kako bi se američkim tijelima omogućilo da kasnije obrade predmetne podatke u svrhu nacionalne sigurnosti.

107. Uostalom, pristupom koji predlaže Facebook Ireland oduzeo bi se koristan učinak odredbama GDPR-a koje se odnose na prijenos u treće zemlje jer se nikad ne može isključiti da će se podaci preneseni u okviru komercijalne aktivnosti obraditi u svrhu nacionalne sigurnosti nakon prijenosa.

108. Tumačenje koje predlažem potkrijepljeno je tekstom članka 45. stavka 2. točke (a) GDPR-a. U toj se odredbi navodi da, prilikom donošenja odluke o primjerenosti, Komisija među ostalim uzima u obzir zakonodavstvo treće zemlje *u pogledu nacionalne sigurnosti*. Iz toga se može zaključiti da to što tijela treće zemlje odredišta mogu obrađivati podatke u svrhu zaštite nacionalne sigurnosti ne znači da je pravo Unije neprimjenjivo na obradu koja obuhvaća prijenos podataka u tu treću zemlju.

109. Rasuđivanje i zaključci koje je Sud donio u presudi Schrems temelje se također na toj pretpostavci. Konkretno, Sud je u toj presudi ispitao valjanost Odluke o privatnosti „sigurne luke" jer se ta odluka odnosila na prijenose osobnih podataka iz SAD-a u kojem su mogli biti prikupljeni i obrađeni u svrhu zaštite nacionalne sigurnosti, u smislu članka 25. stavka 6. Direktive 95/46, u vezi s Poveljom [41].

110. S obzirom na ta razmatranja, smatram da se pravo Unije primjenjuje na prijenos osobnih podataka iz države članice u treću zemlju kada je taj prijenos obuhvaćen komercijalnom aktivnošću a da pritom nije važno da javna tijela te treće zemlje prenesene podatke mogu obraditi radi zaštite nacionalne sigurnosti.

D. Razina zaštite koja je potrebna u okviru prijenosa koji se temelji na standardnim ugovornim klauzulama (prvi dio šestog pitanja)

111. U skladu s prvim dijelom šestog pitanja, sud koji je uputio zahtjev želi znati koju razinu zaštite temeljnih prava ispitanika treba osigurati kako bi se osobni podaci mogli prenijeti u treću zemlju na temelju standardnih ugovornih klauzula predviđenih u Odluci 2010/87.

112. Taj sud ističe da je Sud u presudi Schrems protumačio članak 25. stavak 6. Direktive 95/46 (čiji je sadržaj u biti preuzet u članku 45. stavku 3. GDPR-a), u dijelu u kojem se predviđa da Komisija može donijeti odluku o primjerenosti tek nakon što se uvjeri da dotična treća zemlja jamči *odgovarajuću* razinu zaštite, na način da se njime podrazumijeva da Komisija utvrdi da ta zemlja osigurava razinu zaštite temeljnih prava i sloboda koja je *bitno ekvivalentna* onoj zaštiti koja se jamči u okviru Unije na temelju te direktive, tumačene s obzirom na Povelju [42].

40 U mojem mišljenju u predmetu Ministerio Fiscal (C-207/16, EU:C:2018:300, t. 47.), ističem razliku između, s jedne strane, izravne obrade osobnih podataka u okviru suverenih aktivnosti države i, s druge strane, komercijalne obrade nakon koje te podatke upotrebljavaju javna tijela.

41 Jednako tako, u mišljenju 1/15 (Sporazum o PNR-u između EU-a i Kanade) od 26. srpnja 2017. (EU:C:2017:592, u daljnjem tekstu: mišljenje 1/15) Sud je ispitao usklađenost s člancima 7., 8. i 47. Povelje nacrta međunarodnog sporazuma između Kanade i Unije u pogledu podataka koji su namijenjeni da ih, nakon što se prenesu u Kanadu, javna tijela obrade u svrhu zaštite nacionalne sigurnosti.

42 Presuda Schrems (t. 73.). Sud je taj zaključak potvrdio u mišljenju 1/15 (točka 134.).

113. U tom kontekstu, prvim dijelom šestog prethodnog pitanja od Suda se traži da utvrdi treba li primjena „standardnih ugovornih klauzula" koje je Komisija donijela u skladu s člankom 26. stavkom 4. Direktive 95/46 – koje odgovaraju „standardnim klauzulama o zaštiti" sada spomenutima u članku 46. stavku 2. točki (c) GDPR-a – omogućiti postizanje razine zaštite koja odgovara istom standardu „bitne ekvivalentnosti".

114. U tom pogledu, člankom 46. stavkom 1. GDPR-a predviđa se da, ako nije donesena odluka o primjerenosti, voditelj obrade trećoj zemlji osobne podatke može prenijeti „samo ako je voditelj obrade […] predvidio *odgovarajuće zaštitne mjere* i pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkoviti pravni lijekovi" (moje isticanje)[43]. U skladu s člankom 46. stavkom 2. točkom (c) GDPR-a, te zaštitne mjere mogu, među ostalim, proizlaziti iz standardnih klauzula o zaštiti koje je sastavila Komisija.

115. Kao i DPC, M. Schrems i Irska, smatram da se „odgovarajućim zaštitnim mjerama" koje nudi voditelj obrade i na koje se upućuje u članku 46. stavku 1. GDPR-a treba osigurati da se na prava osoba čiji se podaci prenose primjenjuje, kao u okviru prijenosa koji se temelji na odluci o primjerenosti, razina zaštite koja je bitno ekvivalentna razini zaštite koja proizlazi iz GDPR-a, s obzirom na Povelju.

116. Taj zaključak proizlazi iz cilja te odredbe i instrumenta čiji je dio.

117. Članci 45. i 46. GDPR-a imaju za cilj osigurati kontinuirano visoku razinu zaštite osobnih podataka koja se osigurava tom uredbom kada se ti podaci prenose izvan Unije. Naime, člankom 44. GDPR-a, naslovljenim „Opća načela prijenosa", započinje poglavlje V. koje se odnosi na prijenose trećim zemljama, pri čemu se navodi da se sve odredbe iz tog poglavlja primjenjuju kako bi se osiguralo da se ne ugrozi razina zaštite zajamčena GDPR-om u slučaju prijenosa trećoj državi[44]. Tim se pravilom nastoji izbjeći da se standardi zaštite koji proizlaze iz prava Unije zaobiđu prenošenjem osobnih podataka u treću zemlju kako bi ih se ondje obradilo[45]. S obzirom na taj cilj, nije važno temelji li se prijenos na odluci o primjerenosti ili na zaštitnim mjerama koje nudi voditelj obrade, osobito s pomoću ugovornih klauzula. Zahtjevi zaštite temeljnih prava zajamčenih Poveljom ne razlikuju se ovisno o pravnom temelju određenog prijenosa[46].

118. Suprotno tomu, način na koji se osigurava kontinuirano visoka razina zaštite razlikuje se ovisno o pravnom temelju prijenosa.

119. S jedne strane, cilj je odluke o primjerenosti utvrditi da sama dotična treća zemlja osigurava razinu zaštite koja je bitno ekvivalentna razini zaštite koja se mora postići u okviru prava Unije. Donošenje odluke o primjerenosti podrazumijeva da Komisija prethodno procijeni, za određenu treću zemlju, razinu zaštite koja se jamči pravom i praksama te treće zemlje s obzirom na čimbenike navedene u članku 45. stavku 3. GDPR-a. Osobni podaci zatim se mogu prenijeti u navedenu treću zemlju a da voditelj obrade ne treba dobiti posebno odobrenje.

43 Člankom 26. stavkom 2. Direktive 95/46 predviđalo se da država članica može odobriti takav prijenos „kada nadzornik daje *dovoljna jamstva* u vezi zaštite privatnosti i temeljnih prava i sloboda pojedinaca te u vezi ostvarivanja tih prava" (moje isticanje). Pojmovi „dovoljna jamstva" i „odgovarajuće zaštitne mjere", koji se navode u toj odredbi odnosno u članku 46. stavku 1. GDPR-a, prema mojem mišljenju, imaju isti sadržaj.

44 U tom pogledu, u uvodnoj izjavi 6. GDPR-a navodi se da „visoku razinu" zaštite osobnih podataka treba osigurati u Uniji, kao i prilikom prijenosa izvan Unije. Vidjeti također uvodnu izjavu 101. GDPR-a.

45 Vidjeti presudu Schrems (t. 73.) i mišljenje 1/15 (t. 214.).

46 Time se ne dovodi u pitanje mogućnost prijenosa osobnih podataka, čak i ako ne postoje odgovarajuće zaštitne mjere, na temelju razloga za odstupanje koji su predviđeni u članku 49. stavku 1. GDPR-a.

120. S druge strane, kao što je detaljnije izneseno u sljedećem odjeljku, odgovarajuće zaštitne mjere koje nudi voditelj obrade imaju za cilj osigurati visoku razinu zaštite u slučaju da zaštitne mjere dostupne u trećoj zemlji odredišta nisu dostatne. Stoga, iako se člankom 46. stavkom 1. GDPR-a omogućuje da se osobni podaci prenose u treće zemlje koje ne osiguravaju primjerenu razinu zaštite, tom se odredbom takvi prijenosi odobravaju samo kada se odgovarajuće zaštitne mjere pružaju na druge načine. Standardne ugovorne klauzule koje je donijela Komisija u tom pogledu čine opći mehanizam primjenjiv na prijenose neovisno o trećoj zemlji odredišta i razini zaštite koja se ondje osigurava.

E. Valjanost Odluke 2010/87 s obzirom na članke 7., 8. i 47. Povelje (sedmo, osmo i jedanaesto pitanje)

121. Sedmim pitanjem sud koji je uputio zahtjev u biti pita je li Odluka 2010/87 nevaljana jer se njome ne obvezuju tijela trećih država u koje su podaci preneseni na temelju standardnih ugovornih klauzula predviđenih u prilogu toj odluci i, konkretno, jer ih ona ne sprečava da od uvoznika zahtijevaju da im te podatke stavi na raspolaganje. Stoga se tim pitanjem dovodi u pitanje sama mogućnost osiguravanja primjerene razine zaštite takvih podataka primjenom isključivo ugovornih mehanizama. Jedanaesto pitanje odnosi se općenitije na valjanost Odluke 2010/87 s obzirom na članke 7., 8. i 47. Povelje.

122. Osmim se pitanjem od Suda traži da utvrdi je li nadzorno tijelo dužno izvršiti ovlasti koje su mu povjerene člankom 58. stavkom 2. točkama (f) i (j) GDPR-a kako bi obustavio prijenos u treću zemlju koji se temelji na standardnim ugovornim klauzulama predviđenim Odlukom 2010/87 kada smatra da uvoznik podataka u toj zemlji ima obveze koje ga sprečavaju da poštuje te klauzule i imaju za učinak da se ne osigurava odgovarajuća zaštita prenesenih podataka. Budući da odgovor na to pitanje, prema mojem mišljenju, utječe na valjanost Odluke 2010/87[47], razmatram ga zajedno sa sedmim i jedanaestim pitanjem.

123. U tekstu članka 46. stavka 1. GDPR-a, u dijelu u kojem se predviđa da, *„[a]ko nije donesena odluka na temelju članka 45. stavka 3.*, voditelj obrade ili izvršitelj obrade trećoj zemlji […] osobne podatke mogu prenijeti samo *ako je voditelj obrade ili izvršitelj obrade predvidio* odgovarajuće zaštitne mjere" (moje isticanje), ističe se logika iz koje proizlaze ugovorni mehanizmi kao što su oni predviđeni Odlukom 2010/87. Kao što se to naglašava u uvodnim izjavama 108. i 114. GDPR-a, ti mehanizmi imaju za cilj omogućiti prijenose u treće zemlje za koje Komisija nije donijela odluke o primjerenosti, pri čemu se eventualni nedostaci zaštite koja se osigurava pravnim poretkom te treće zemlje tada *nadomještaju* zaštitnim mjerama koje se izvoznik i uvoznik podataka ugovorno obvezuju poštovati.

124. Budući da je svrha ugovornih zaštitnih mjera upravo nadoknaditi moguće nedostatke u zaštiti koju nude treće zemlje odredišta, neovisno o tome o kojim je nedostacima riječ, valjanost odluke kojom Komisija utvrđuje da se određenim standardnim klauzulama primjereno popunjavaju ti nedostaci ne može ovisiti o razini zaštite koja se pruža u svakoj od trećih zemalja u koje je moguće prenijeti podatke. Valjanost takve odluke ovisi samo o jačini zaštitnih mjera koje se predviđaju tim klauzulama radi nadoknađivanja eventualne nedostatne zaštite u trećoj zemlji odredišta. Djelotvornost tih zaštitnih mjera treba ocijeniti uzimajući u obzir i zaštitne mjere koje obuhvaćaju ovlasti nadzornih tijela na temelju članka 58. stavka 2. GDPR-a.

47 Vidjeti točku 128. ovog mišljenja.

125. U tom pogledu, kao što su to u biti istaknuli DPC, M. Schrems, BSA, Irska, austrijska, francuska, poljska i portugalska vlada, kao i Komisija, zaštitne mjere koje sadržavaju standardne ugovorne klauzule mogu se umanjiti ili čak poništiti kada se pravom treće zemlje odredišta uvozniku nameću obveze koje su suprotne onomu što se zahtijeva tim klauzulama. Stoga se pravnim kontekstom u trećoj zemlji odredišta može, ovisno o konkretnim okolnostima prijenosa [48], onemogućiti izvršenje obveza predviđenih tim klauzulama.

126. U tim okolnostima, kao što su to naglasili M. Schrems i Komisija, ugovorni mehanizam predviđen u članku 46. stavku 2. točki (c) GDPR-a temelji se na davanju odgovornosti izvozniku, kao i, podredno, nadzornim tijelima. Voditelj obrade ili, ako on ne postoji, nadzorno tijelo, ispitat će *u svakom slučaju zasebno*, za svaki pojedinačni prijenos, sprečava li se pravom treće zemlje odredišta izvršenje standardnih klauzula i stoga odgovarajuća zaštita prenesenih podataka na način da je prijenose potrebno zabraniti ili obustaviti.

127. S obzirom na ta očitovanja, smatram da sama činjenica da tijela treće zemlje odredišta nisu obvezane Odlukom 2010/87 i standardnim ugovornim klauzulama koje ta odluka sadržava ne podrazumijeva da je navedena odluka nevaljana. Usklađenost Odluke 2010/87 s člancima 7., 8. i 47. Povelje ovisi, prema mojem mišljenju, o tome postoje li dovoljno snažni mehanizmi kojima se može osigurati da se prijenosi koji se temelje na standardnim ugovornim klauzulama obustave ili zabrane u slučaju povrede tih klauzula ili nemogućnosti njihova ispunjavanja.

128. U tom pogledu, člankom 46. stavkom 1. GDPR-a predviđa se da je prijenos koji se temelji na odgovarajućim zaštitnim mjerama moguć samo „pod uvjetom da su ispitanicima na raspolaganju provediva prava i učinkoviti pravni lijekovi”. Valjat će provjeriti može li se na temelju zaštitnih mjera koje su predviđene klauzulama iz Priloga Odluci 2010/87, koje su dopunjene ovlastima nadzornih tijela, osigurati poštovanje tog uvjeta. Prema mojem mišljenju, to je slučaj samo ako postoji *obveza* koju imaju voditelji obrade (dio 1) i, ako oni ne djeluju, nadzorna tijela (dio 2) da obustave ili zabrane prijenos kada, zbog sukoba između obveza koje proizlaze iz standardnih klauzula i obveza propisanim pravom treće zemlje odredišta, te klauzule nije moguće poštovati.

1. Obveze koje imaju voditelji obrade

129. Kao prvo, standardnim ugovornim klauzulama iz Priloga Odluci 2010/87 zahtijeva se da se u slučaju sukoba između obveza koje se njima predviđaju i zahtjeva koji proizlaze iz prava treće zemlje odredišta, na te klauzule ne poziva u prilog prijenosu u tu treću zemlju ili, ako je prijenos već započet na temelju navedenih klauzula, da se izvoznika obavijesti o tom sukobu i da on može obustaviti taj prijenos.

130. Stoga, na temelju klauzule 5. točke (a), uvoznik se obvezuje da će prenesene osobne podatke obraditi jedino u korist izvoznika te u skladu s njegovim uputama i standardnim ugovornim klauzulama. Ako uvoznik ne može postupiti u skladu s tim klauzulama, suglasan je da o tome odmah obavijesti izvoznika, te u tom slučaju izvoznik ima pravo obustaviti prijenos i/ili prekinuti ugovor [49].

48 Na primjer, moguće je zamisliti slučaj u kojem treća zemlja predviđa obvezu za pružatelje telekomunikacijskih usluga da javnim tijelima daju pristup prenesenim podacima bez ikakvih ograničenja i zaštitnih mjera. Iako takvi pružatelji usluga ne bi mogli poštovati standardne ugovorne klauzule, poduzetnici koji ne podliježu toj obvezi ipak bi ih mogli poštovati.

49 Osim toga, napominjem da se u klauzuli 5. točki (d) podtočki i. uvoznika oslobađa obveze da izvoznika obavijesti o pravno obvezujućem zahtjevu od strane tijela kaznenog progona treće zemlje za otkrivanje podataka kada se pravu te treće zemlje protivi takvo obavješćivanje. U takvom slučaju, izvoznik neće moći obustaviti prijenos ako to otkrivanje, za koje on ne zna, povređuje standardne klauzule. Međutim, uvoznik je, na temelju članka 5. točke (a), i dalje dužan obavijestiti, po potrebi, izvoznika o tome da smatra da ga zakonodavstvo te treće zemlje sprečava da ispuni obveze koje ima na temelju dogovorenih ugovornih klauzula.

131. U bilješci 5. koja se odnosi na klauzulu 5. pojašnjava se da standardne klauzule nisu povrijeđene kada uvoznik ispunjava obvezne zahtjeve nacionalnog zakonodavstva koje se na njega primjenjuje u trećoj zemlji, pod uvjetom da ti zahtjevi ne nadilaze neophodno u demokratskom društvu kako bi se zaštitio jedan od interesa navedenih u članku 13. stavku 1. Direktive 95/46 (čiji je sadržaj u bitnome preuzet u članku 23. stavku 1. GDPR-a), među kojima su nacionalna i državna sigurnost. U obrnutom slučaju, nepoštovanje tih klauzula kako bi se ispunila suprotna obveza koja se temelji na pravu treće zemlje odredišta koja prekoračuje ono što je proporcionalno za zaštitu legitimnog interesa koji priznaje Unija smatra se povredom navedenih klauzula.

132. Prema mojem mišljenju, kao što su to tvrdili M. Schrems i Komisija, klauzula 5. točka (a) ne može se tumačiti na način da su obustava prijenosa ili prekid ugovora samo opcionalni u slučaju da uvoznik ne može poštovati standardne klauzule. Iako se u toj klauzuli navodi samo pravo koje u tom smislu ima izvoznik, taj tekst treba shvatiti kao upućivanje na ugovorni okvir kojim je obuhvaćen. Činjenicom da izvoznik ima pravo, *u bilateralnim odnosima s uvoznikom*, obustaviti prijenos ili prekinuti ugovor kada taj uvoznik ne može poštovati standardne klauzule ne dovodi se u pitanje obveza izvoznika da tako postupi *s obzirom na zahtjeve zaštite prava ispitanika koji proizlaze iz GDPR-a*. Svako drugo tumačenje dovelo bi do nevaljanosti Odluke 2010/87 u dijelu u kojem se standardnim ugovornim klauzulama koje se tom odlukom predviđaju ne omogućuje da se prijenos izvrši uz „odgovarajuće zaštitne mjere" kao što se to zahtijeva člankom 46. stavkom 1. GDPR-a, s obzirom na odredbe Povelje [50].

133. K tomu, u skladu s klauzulom 5. točkom (b), uvoznik jamči da nema razloga za vjerovanje da ga zakonodavstvo koje se na njega primjenjuje onemogućava u ispunjavanju uputa primljenih od izvoznika i njegovih obveza prema ugovoru. U slučaju promjene u tom zakonodavstvu koja bi mogla imati bitan negativan učinak na jamstva i obveze iz standardnih klauzula, uvoznik će o promjeni odmah obavijestiti izvoznika, te u tom slučaju izvoznik ima pravo obustaviti prijenos podataka i/ili prekinuti ugovor. U skladu s klauzulom 4. točkom (g), izvoznik treba proslijediti obavijest zaprimljenu od uvoznika nadležnom nadzornom tijelu ako izvoznik odluči nastaviti s prijenosom.

134. Smatram da je ovdje potrebno iznijeti nekoliko pojašnjenja u pogledu sadržaja ispitivanja koje trebaju provesti ugovorne strane kako bi utvrdile, s obzirom na bilješku koja se odnosi na klauzulu 5., povređuju li se obvezama koje uvoznik ima na temelju prava treće države standardne klauzule i stoga sprečava li se njima to da se prijenos izvrši uz odgovarajuće zaštitne mjere. Ta je problematika u biti istaknuta u okviru drugog dijela šestog prethodnog pitanja.

135. Takvo ispitivanje podrazumijeva, prema mojem mišljenju, uzimanje u obzir svih okolnosti svakog prijenosa, među koje se mogu ubrojiti priroda podataka i njihov eventualno osjetljiv karakter, mehanizmi koje primjenjuju izvoznik i/ili uvoznik kako bi se osigurala njihova sigurnost [51], priroda i svrha obrada koje provode javna tijela treće zemlje kojima će biti izloženi podaci, načini tih obrada, kao i ograničenja i zaštitne mjere koje osigurava ta treća zemlja. Elementi koji obilježavaju aktivnosti obrade koje provode javna tijela i zaštitne mjere primjenjive u pravnom poretku navedene treće zemlje mogu se, prema mojem mišljenju, preklapati s onima iz članka 45. stavka 2. GDPR-a.

136. Kao drugo, standardnim ugovornim klauzulama iz Priloga Odluci 2010/87 uvode se provediva prava i pravni lijekovi u korist subjekta podataka na koje se mogu pozvati protiv izvoznika i, podredno, protiv uvoznika.

50 Iz sudske prakse proizlazi da odredbe provedbenog akta treba tumačiti u skladu s odredbama temeljnog akta kojim je zakonodavac odobrio donošenje tog provedbenog akta (vidjeti u tom smislu osobito presude od 26. srpnja 2017., Češka Republika/Komisija (C-696/15 P, EU:C:2017:595, t. 51.); od 17. svibnja 2018., Evonik Degussa (C-229/17, EU:C:2018:323, t. 29.) i od 20. lipnja 2019., ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518, t. 112.)). K tomu, akt Unije mora se tumačiti u najvećoj mogućoj mjeri tako da se ne dovede u pitanje njegova valjanost i u skladu s cjelokupnim primarnim pravom i osobito odredbama Povelje (vidjeti osobito presudu od 14. svibnja 2019., M i dr. (Opoziv statusa izbjeglice) (C-391/16, C-77/17 i C-78/17, EU:C:2019:403, t. 77. i navedena sudska praksa)).

51 U tom pogledu, u uvodnoj izjavi 109. GDPR-a izvoznika i uvoznika potiče se na to da standardnim klauzulama o zaštiti dodaju dodatne zaštitne mjere, osobito putem ugovora.

137. Stoga se klauzulom 3., naslovljenom „Klauzula u korist treće strane”, u njezinu stavku 1. predviđa pravo na podnošenje pravnog lijeka koje subjekt podataka ima protiv izvoznika u slučaju povrede, među ostalim, klauzule 5. točke (a) ili (b). U skladu s klauzulom 3. stavkom 2., kada izvoznik prestane postojati ili prestane postojati pred zakonom, subjekt podataka može tu klauzulu upotrijebiti protiv uvoznika.

138. Klauzulom 6. stavkom 1. svakom se subjektu podataka koji trpi štetu kao posljedicu kršenja obveza navedenih u klauzuli 3. priznaje pravo da od izvoznika primi naknadu štete. Na temelju klauzule 7. stavka 1., uvoznik je suglasan da ako subjekt podataka protiv njega upotrijebi prava u korist treće stranke i/ili traži naknadu štete, uvoznik prihvaća odluku subjekta podataka da nezavisna osoba ili, prema potrebi, nadležna tijela upute spor na medijaciju odnosno da spor uputi sudovima u državama članicama u kojima izvoznik ima poslovni nastan.

139. Uz pravne lijekove kojima raspolažu na temelju standardnih ugovornih klauzula predviđenih u Prilogu Odluke 2010/87, ispitanici mogu, kada smatraju da su te klauzule povrijeđene, od nadzornih tijela tražiti donošenje korektivnih mjera na temelju članka 58. stavka 2. GDPR-a, na koji se upućuje u članku 4. Odluke 2010/87 [52].

2. Obveze koje imaju nadzorna tijela

140. Zbog sljedećih razloga smatram, kao i M. Schrems, Irska, njemačka, austrijska, belgijska, nizozemska i portugalska vlada te EOZP, da se člankom 58. stavkom 2. GDPR-a obvezuje nadzorna tijela, kada smatraju, po završetku savjesnog ispitivanja, da podaci preneseni u treću zemlju nisu primjereno zaštićeni zbog nepoštovanja dogovorenih standardnih klauzula, na poduzimanje odgovarajućih mjera za otklanjanje te nezakonitosti, po potrebi nalaganjem obustave prijenosa.

141. Kao prvo, napominjem da se, suprotno onomu što tvrdi DPC, nijedna odredba Odluke 2010/87 ne ograničava na iznimne slučajeve izvršavanja ovlasti „privremeno[g] ili konačno[g] ograničavanja], među ostalim zabran[e], obrad[e]” i „nare[đivanja] suspenzij[e] protoka podataka primatelju u trećoj zemlji”, kojima nadzorna tijela raspolažu na temelju članka 58. stavka 2. točaka (f) i (j) GDPR-a.

142. Točno je da je u prvotnoj verziji članka 4. Odluke 2010/87, u njegovu stavku 1., izvršavanje ovlasti nadzornih tijela da obustave ili zabrane prekogranične protoke podataka ograničeno na određene situacije u kojima se ustanovi da je vjerojatno da prijenos na ugovornoj osnovi može imati značajan nepovoljni učinak na jamstva namijenjena zaštiti predmetne osobe. Međutim, u članku 4. te odluke, kako ju je Komisija izmijenila 2016. kako bi postupila u skladu s presudom Schrems [53], sada se samo upućuje na te ovlasti a da ih se nipošto ne ograničava. U svakom slučaju, provedbenom odlukom Komisije, kao što je Odluka 2010/87, ne mogu se valjano ograničiti ovlasti koje su nadzornim tijelima dodijeljene na temelju samog GDPR-a [54].

143. Taj se zaključak ne dovodi u pitanje uvodnom izjavom 11. Odluke 2010/87, u kojoj se navodi da nadzorna tijela mogu izvršavati ovlasti obustave i zabrane prijenosa samo u „iznimnim slučajevima”. Ta se uvodna izjava, koja je već bila sadržana u prvotnoj verziji te odluke, odnosila na bivši članak 4. stavak 1. navedene odluke kojim su se ograničavale ovlasti nadzornih tijela. Dok je Odluka 2010/87 bila revidirana Odlukom 2016/2297 Komisija nije povukla ili izmijenila navedenu uvodnu izjavu kako bi njezin sadržaj prilagodila sadržaju novog članka 4. Međutim, u uvodnoj izjavi 5. Odluke 2016/2297

52 Iako se u članku 4. stavku 1. Odluke 2010/87 upućuje na članak 28. stavak 3. Direktive 95/46, podsjećam da, na temelju članka 94. stavka 2. GDPR-a, upućivanja na tu direktivu treba tumačiti kao upućivanja na odgovarajuće odredbe GDPR-a.

53 Vidjeti uvodne izjave 6. i 7. Odluke 2016/2297. U točkama 101. do 104. presude Schrems, Sud je već proglasio nevaljanom odredbu Odluke o privatnosti „sigurne luke” kojom su na „iznimne slučajeve” bile ograničene ovlasti koje su nadzornim tijelima bile dodijeljene člankom 28. Direktive 95/46 jer Komisija nije bila nadležna za ograničavanje tih ovlasti.

54 Vidjeti presudu Schrems (t. 103.).

ponovno su potvrđene ovlasti nadzornih tijela da obustave ili zabrane svaki prijenos koji smatraju protivnim pravu Unije, osobito ako uvoznik ne poštuje standardne ugovorne klauzule. Uvodnu izjavu 11. Odluke 2010/87, u dijelu u kojem se njome sada proturječi tekstu i cilju pravno obvezujuće odredbe te odluke, treba smatrati zastarjelom [55].

144. Kao drugo, suprotno onomu što tvrdi i DPC, izvršavanje ovlasti obustave i zabrane iz članka 58. stavka 2. točaka (f) i (j) GDPR-a ne predstavlja ni samu mogućnost prepuštenu diskreciji nadzornih tijela. Prema mojem mišljenju, taj zaključak proizlazi iz tumačenja članka 58. stavka 2. GDPR-a s obzirom na druge odredbe te uredbe i Povelje, kao i iz opće strukture i ciljeva Odluke 2010/87.

145. Konkretno, članak 58. stavak 2. GDPR-a treba tumačiti s obzirom na članak 8. stavak 3. Povelje i članak 16. stavak 2. UFEU-a. U skladu s tim odredbama, poštovanje zahtjeva koje podrazumijeva temeljno pravo na zaštitu osobnih podataka podliježe nadzoru neovisnih tijela. Ta zadaća nadzora nad time jesu li poštovani zahtjevi koji se odnose na zaštitu osobnih podataka, koja se navodi i u članku 57. stavku 1. točki (a) GDPR-a, uključuje obvezu nadzornih tijela da djeluju na način da osiguraju pravilnu primjenu te uredbe.

146. Stoga nadzorno tijelo mora sa svom dužnom pažnjom ispitati pritužbu koju je podnijela osoba čiji su podaci navodno preneseni u treću državu, pri čemu su povrijeđene standardne ugovorne klauzule koje se primjenjuju na prijenos [56]. Člankom 58. stavkom 1. GDPR-a u tu se svrhu nadzornim tijelima povjeravaju znatne istražne ovlasti [57].

147. Nadležno nadzorno tijelo također je dužno na odgovarajući način reagirati na eventualne povrede prava ispitanika koje utvrdi nakon istrage. U tom pogledu, svako nadzorno tijelo, na temelju članka 58. stavka 2. GDPR-a, raspolaže širokim rasponom sredstava, odnosno raznim ovlastima donošenja korektivnih mjera navedenim u toj odredbi, za provedbu zadaće koja mu je povjerena [58].

148. Iako je odabir najučinkovitijeg sredstva pod diskrecijom nadležnog nadzornog tijela s obzirom na sve okolnosti predmetnog prijenosa, to je tijelo dužno u potpunosti ispuniti zadaću nadzora koja mu je povjerena. Po potrebi, to tijelo mora obustaviti prijenos ako zaključi da nisu poštovane standardne ugovorne klauzule i da se odgovarajuća zaštita prenesenih podataka ne može osigurati drugim sredstvima, u slučaju da sam izvoznik nije okončao prijenos.

149. To je tumačenje potkrijepljeno člankom 58. stavkom 4. GDPR-a, kojim se predviđa da izvršavanje ovlasti dodijeljenih nadzornim tijelima u skladu s tim člankom podliježe odgovarajućim zaštitnim mjerama, među ostalim djelotvornom pravnom lijeku u skladu s člankom 47. Povelje. Člankom 78. stavcima 1. i 2. GDPR-a priznaje se, osim toga, pravo svake osobe na učinkoviti pravni lijek protiv pravno obvezujuće odluke nekog nadzornog tijela koja se na nju odnosi ili ako to tijelo ne riješi njezinu pritužbu [59].

150. Te odredbe podrazumijevaju, kao što to u biti tvrde M. Schrems, BSA, Irska, poljska vlada i vlada Ujedinjene Kraljevine te Komisija, da se protiv odluke kojom se nadzorno tijelo suzdržava od zabrane ili obustave prijenosa u treću zemlju, na zahtjev osobe koja se poziva na opasnost od toga da će se obradom podataka koji se odnose na nju u trećoj zemlji povrijediti njezina temeljna prava, može

55 U svakom slučaju, preambula akta Unije nema pravno obvezujuću snagu te se na nju ne može pozivati da bi se odstupilo od samih odredbi tog akta. Vidjeti presude od 19. studenoga 1998., Nilsson i dr. (C-162/97, EU:C:1998:554, t. 54.); od 12. svibnja 2005., Meta Fackler (C-444/03, EU:C:2005:288, t. 25.) i od 10. siječnja 2006., IATA i ELFAA (C-344/04, EU:C:2006:10, t. 76.).

56 Vidjeti po analogiji presudu Schrems (t. 63.).

57 Dodajem da su, na temelju klauzule 8. stavka 2. koja se navodi u Prilogu Odluci 2010/87, ugovorne strane suglasne da se nadzornom tijelu dodjeljuje ovlast izvršavanja revizije uvoznika koja je podložna istim uvjetima koji se primjenjuju na reviziju izvoznika sukladno pravu koje se primjenjuje.

58 Vidjeti u tom smislu presudu Schrems (t. 43.).

59 U skladu s uvodnom izjavom 141. GDPR-a, svaka osoba treba imati pravo na učinkoviti pravni lijek u skladu s člankom 47. Povelje ako nadzorno tijelo „ne djeluje kada je takvo djelovanje nužno radi zaštite prava [te osobe]”. Vidjeti i uvodne izjave 129. i 143. GDPR-a.

podnijeti pravni lijek. Međutim, priznavanje prava na pravni lijek pretpostavlja postojanje ograničene, a ne isključivo diskrecijske nadležnosti nadzornih tijela. K tomu, M. Schrems i Komisija pravilno su istaknuli da izvršenje djelotvornog sudskog nadzora podrazumijeva da tijelo koje je autor osporavanog akta primjereno obrazloži taj akt [60]. Ta obveza obrazlaganja primjenjuje se, prema mojem mišljenju, na odluku nadzornih tijela da izvršavaju određene ovlasti koje su mu povjerene člankom 58. stavkom 2. GDPR-a.

151. Međutim, također treba odgovoriti na argumente kojima DPC tvrdi da, iako nadzorna tijela imaju obvezu obustaviti ili zabraniti prijenos kad zaštita prava predmetne osobe to zahtijeva, valjanost Odluke 2010/87 time ipak nije osigurana.

152. Kao prvo, DPC smatra da se takvom obvezom ne rješavaju sustavni problemi u pogledu primjerenih zaštitnih mjera u trećoj državi kao što je SAD. Naime, ovlasti nadzornih tijela mogu se izvršavati samo u svakom slučaju zasebno, iako su nedostaci koji su svojstveni američkom pravu opći i strukturni. To dovodi do opasnosti od toga da različita nadzorna tijela donesu drukčije odluke o usporedivim prijenosima.

153. U tom pogledu ne mogu zanemariti praktične poteškoće povezane sa zakonodavnim odabirom da se nadzornim tijelima prepusti odgovornost da osiguraju poštovanje temeljnih načela ispitanika u okviru konkretnih prijenosa ili protoka prema određenom primatelju. Te poteškoće ipak ne dovode do nevaljanosti Odluke 2010/87.

154. Naime, čini mi se da se pravom Unije ne zahtijeva da se utvrdi opće i preventivno rješenje za sve prijenose u određenu treću zemlju u pogledu kojih mogu postojati iste opasnosti od povrede temeljnih prava.

155. Usto, rizik od podjele pristupa koje primjenjuju različita nadzorna tijela svojstven je strukturi decentraliziranog nadzora koji je htio zakonodavac [61]. Uostalom, kao što je to istaknula njemačka vlada, poglavljem VII. GDPR-a, naslovljenim „Suradnja i konzistentnost", uspostavljaju se mehanizmi namijenjeni izbjegavanju tog rizika. Člankom 60. te uredbe predviđa se, u slučaju prekogranične obrade podataka, postupak suradnje između predmetnih nadzornih tijela i nadzornog tijela poslovnog nastana voditelja obrade, takozvanog „vodećeg nadzornog tijela" [62]. U slučaju oprečnih mišljenja, nesuglasice mora riješiti EOZP [63]. Potonji odbor također je nadležan donijeti, na zahtjev nadzornog tijela, mišljenja o svim pitanjima koja se tiču nekoliko država članica [64].

156. Kao drugo, DPC ističe da je Odluka 2010/87 nevaljana s obzirom na članak 47. Povelje jer nadzorna tijela mogu zaštititi prava ispitanikâ tek ubuduće te pritom ne nude rješenje ispitanicima čiji su podaci već preneseni. Konkretno, DPC naglašava da se člankom 58. stavkom 2. GDPR-a ne predviđa pravo na pristup, ispravak ili brisanje podataka koje su prikupila javna tijela treće države ni mogućnost naknade štete koju su pretrpjeli ispitanici.

157. Što se tiče navodnog nepostojanja prava na pristup, ispravak i brisanje prikupljenih podataka, treba utvrditi da, ako u trećoj zemlji odredišta ne postoji nikakav djelotvoran pravni lijek, na temelju pravnih lijekova predviđenih u Uniji protiv voditelja obrade ne može se od javnih tijela te treće zemlje dobiti pristup tim podacima ili pak njihov ispravak ili brisanje.

60 Vidjeti osobito presude od 28. srpnja 2011., Samba Diouf (C-69/10, EU:C:2011:524, t. 57.) i od 17. studenoga 2011., Gaydarov (C-430/10, EU:C:2011:749, t. 41.).

61 Vidjeti u tom pogledu presudu od 5. lipnja 2018., Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, t. 69. do 73.).

62 Vidjeti članak 56. stavak 1. GDPR-a. U skladu s člankom 61. te uredbe, nadzorna tijela dužna su pružati si uzajamnu pomoć. Člankom 62. navedene uredbe nadzorna tijela ovlašćuje se za provedbu zajedničkih operacija.

63 Vidjeti članak 65. GDPR-a.

64 Vidjeti članak 64. stavak 2. GDPR-a.

158. Prema mojem mišljenju, tim se prigovorom ipak ne opravdava neusklađenost Odluke 2010/87 s člankom 47. Povelje. Naime, valjanost te odluke ne ovisi o razini zaštite koja postoji u svakoj trećoj zemlji u koju se podaci mogu prenijeti na temelju standardnih ugovornih klauzula koje navedena odluka sadržava. Ako se pravom treće države odredišta uvoznika sprečava da postupa u skladu s tim klauzulama tako što se od njega zahtijeva da javnim tijelima ustupi pristup podacima u pogledu kojeg ne postoji mogućnost podnošenja odgovarajućeg pravnog lijeka, nadzorna tijela dužna su donijeti korektivne mjere ako izvoznik nije obustavio prijenos na temelju klauzule 5. točke (a) ili (b) iz Priloga Odluci 2010/87.

159. Osim toga, kao što je to istaknuo M. Schrems, osobe čija su prava povrijeđena sada imaju, na temelju članka 82. GDPR-a, pravo na naknadu materijalne ili nematerijalne štete pretrpljene zbog povrede te uredbe od voditelja ili izvršitelja obrade [65].

160. Kao što proizlazi iz svih tih razmatranja, moja analiza nije pokazala nikakav element koji bi mogao utjecati na valjanost Odluke 2010/87 s obzirom na članke 7., 8. i 47. Povelje.

F. Nepostojanje potrebe da se odgovori na druga prethodna pitanja i ispita valjanost Odluke o sustavu zaštite privatnosti

161. U ovom ću dijelu iznijeti razloge, koji se uglavnom odnose na ograničenje predmeta glavnog postupka na valjanost Odluke 2010/87, iz kojih smatram da nije potrebno odgovoriti na drugo, treće, četvrto, peto, deveto i deseto prethodno pitanje niti odlučiti o valjanosti Odluke o sustavu zaštite privatnosti.

162. Drugo prethodno pitanje odnosi se na utvrđivanje standarda zaštite koje treća zemlja treba poštovati kako bi se podaci u nju mogli zakonski prenijeti na temelju standardnih ugovornih klauzula ako te podatke, nakon njihova prijenosa, tijela te treće zemlje mogu obraditi u svrhu nacionalne sigurnosti. Treće pitanje upućeno Sudu odnosi se na utvrđivanje elemenata koji obilježavaju sustav zaštite primjenjiv u trećoj državi odredišta koje treba uzeti u obzir pri provjeri toga zadovoljava li navedeni sustav te standarde.

163. Svojim četvrtim, petim i desetim pitanjem sud koji je uputio zahtjev u biti želi znati jesu li, s obzirom na činjenice koje je utvrdio u pogledu prava SAD-a, tim pravom predviđene odgovarajuće zaštitne mjere od miješanja američkih obavještajnih tijela u ostvarivanje temeljnih prava na poštovanje privatnog života, zaštitu osobnih podataka i djelotvornu sudsku zaštitu.

164. Deveto prethodno pitanje odnosi se na utjecaj koji, u okviru ispitivanja kojim nadzorno tijelo provjerava primjenjuju li se na prijenos u SAD na temelju standardnih ugovornih klauzula predviđenih u Odluci 2010/87 odgovarajuće zaštitne mjere, ima okolnost da je Komisija u Odluci o sustavu zaštite privatnosti utvrdila da SAD nudi primjerenu razinu zaštite ispitanikovih temeljnih prava od takvih miješanja.

165. Sud koji je uputio zahtjev pak nije izričito postavio pitanje o valjanosti Odluke o sustavu zaštite privatnosti, iako se, kao što je to objašnjeno u nastavku [66], četvrtim, petim i desetim prethodnim pitanjem neizravno dovodi u pitanje osnovanost utvrđenja primjerenosti koje je Komisija provela u toj odluci.

65 Člankom 83. stavkom 5. točkom (c) GDPR-a predviđaju se i novčane kazne za voditelja obrade u slučaju povrede članaka 44. do 49. te uredbe.

66 Vidjeti točku 175. ovog mišljenja.

166. Prema mojem mišljenju, s obzirom na elemente koji proizlaze iz prethodne analize, pojašnjenje Suda o tim pitanjima ne može utjecati na njegov zaključak o valjanosti *in abstracto* Odluke 2010/87 niti stoga utjecati na rješavanje glavnog postupka (dio 1). Osim toga, iako bi se odgovori Suda na navedena pitanja u kasnijoj fazi mogli pokazati korisnima DPC-u za utvrđivanje treba li, u okviru postupka iz kojeg proizlazi taj spor, predmetne prijenose *in concreto* obustaviti zbog navodnog nepostojanja odgovarajućih zaštitnih mjera, prema mojem bi mišljenju bilo preuranjeno o njima odlučiti u okviru ovog predmeta (dio 2).

1. Nepostojanje potrebe za odgovorima Suda s obzirom na predmet glavnog postupka

167. Podsjećam da glavni postupak proizlazi iz DPC-ova podnošenja pravnog lijeka opisanog u točki 65. presude Schrems, u skladu s kojom svaka država članica treba omogućiti nadzornom tijelu da, kada smatra potrebnim u svrhu obrade pritužbe o kojoj odlučuje, zatraži od nacionalnog suda da Sudu uputi prethodno pitanje o valjanosti odluke o primjerenosti ili, po analogiji, odluke kojom se uvode standardne ugovorne klauzule.

168. U tom pogledu, High Court (Visoki sud) istaknuo je da je, nakon što je DPC pred njim pokrenuo postupak, mogao samo podnijeti zahtjev za prethodnu odluku o valjanosti Odluke 2010/87 što je zatražio DPC u slučaju da taj sud dijeli njegove dvojbe u pogledu valjanosti te odluke ili odbiti to učiniti u obrnutom slučaju. Taj sud smatra da bi, u slučaju da se odlučio za tu drugu opciju, trebao odbaciti postupak jer DPC-ova pritužba nije imala drugi predmet [67].

169. U tom smislu, Supreme Court (Vrhovni sud), kojem je Facebook Ireland podnio žalbu protiv odluke kojom se upućuje zahtjev za prethodnu odluku, opisao je glavni postupak kao deklaratoran postupak kojim je DPC od suda koji je uputio zahtjev tražio da Sudu postavi prethodno pitanje o valjanosti Odluke 2010/87. Prema mišljenju irskog Supreme Courta (Vrhovni sud), jedino materijalno pitanje postavljeno sudu koji je uputio zahtjev i Sudu stoga se odnosi na valjanost te odluke [68].

170. S obzirom na tako opisan predmet glavnog postupka, sud koji je uputio zahtjev postavio je Sudu prvih deset pitanja jer je smatrao da bi njihovo ispitivanje pridonijelo ukupnoj ocjeni koja je Sudu potrebna kako bi, u odgovoru na jedanaesto pitanje, odlučio o valjanosti Odluke 2010/87 s obzirom na članke 7., 8. i 47. Povelje. To je pitanje, u skladu s odlukom kojom se upućuje zahtjev za prethodnu odluku, logički slijed pitanja koja mu prethode.

171. S tog gledišta, čini mi se da se drugo, treće, četvrto, peto, deveto i deseto pitanje temelje na pretpostavci prema kojoj valjanost Odluke 2010/87 ovisi o razini zaštite temeljnih prava koja se predviđa u svakoj trećoj državi u koju se podaci mogu prenijeti na temelju standardnih ugovornih klauzula koje se predviđaju tom odlukom. Međutim, kao što proizlazi iz moje analize sedmog pitanja [69], ta je pretpostavka, prema mojem mišljenju, pogrešna. Ispitivanje prava treće zemlje odredišta bitno je samo kada Komisija donese odluku o primjerenosti ili kada voditelj obrade ili, ako on ne postoji, nadležno nadzorno tijelo provjeri dovode li, u okviru prijenosa koji se temelji na odgovarajućim zaštitnim mjerama u smislu članka 46. stavka 1. GDPR-a, obveze koje se pravom te treće zemlje nalažu uvozniku u pitanje djelotvornost zaštite koja se osigurava tim zaštitnim mjerama.

67 Presuda High Courta (Visoki sud) od 3. listopada 2017. (t. 337.)

68 U skladu s presudom Supreme Courta (Vrhovni sud) od 31. svibnja 2019. (t. 2.7.), „[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]". U točki 2.9. te presude navodi se: „Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*" (moje isticanje).

69 Vidjeti točku 124. ovog mišljenja.

172. Prema tome, odgovori Suda na prethodno navedena pitanja ne mogu utjecati na njegov zaključak u pogledu jedanaestog pitanja[70]. Na ta pitanja također nije potrebno odgovoriti sa stajališta predmeta glavnog postupka.

173. Predlažem Sudu da ovaj predmet razmotri samo s gledišta predmeta tog spora. Prema mojem mišljenju, Sud ne smije prekoračiti ono što je nužno za rješavanje navedenog spora razmatranjem prethodnih pitanja sa stajališta postupka iz kojeg proizlazi taj postupak i koji je u tijeku pred DPC-om. Kao što je kasnije izneseno, taj poziv na ograničenje postupka proizlazi, s jedne strane, iz nastojanja da se ne naruši normalno odvijanje postupka koje će se nastaviti pred DPC-om nakon što Sud odluči o valjanosti Odluke 2010/87. S druge strane, s obzirom na predmetne činjenice, činilo bi mi se naglim, čak i sa stajališta važnosti tog postupka, da Sud ispita problematike istaknute u okviru drugog, trećeg, četvrtog, petog, devetog i desetog pitanja.

2. Razlozi protiv toga da Sud provede ispitivanje s obzirom na predmet postupka koji je u tijeku pred DPC-om

174. U svojoj pritužbi pred DPC-om, M. Schrems zahtijeva od tog nadzornog tijela da izvrši ovlasti koje ima na temelju članka 58. stavka 2. točke (f) GDPR-a tako da Facebooku Ireland naloži obustavu prijenosa u SAD, koji se provodi na temelju ugovornih klauzula, osobnih podataka koji se odnose na njega. U prilog tom zahtjevu M. Schrems u biti ističe neprimjerenost tih ugovornih zaštitnih mjera s obzirom na miješanja u ostvarivanje njegovih temeljnih prava koja proizlaze iz aktivnosti američkih obavještajnih službi.

175. Argumentacijom M. Schremsa dovodi se u pitanje utvrđenje, koje je Komisija iznijela u Odluci o sustavu zaštite privatnosti, prema kojem SAD osigurava primjerenu razinu zaštite podataka prenesenih na temelju te odluke s obzirom na ograničenja pristupa tim podacima i načina na kojih ih upotrebljavaju američka tijela, kao i pravne zaštite koja se nudi ispitanicima[71]. Zabrinutosti koje je privremeno izrazio DPC[72], kao i sud koji je uputio zahtjev u okviru četvrtog, petog i desetog pitanja, također neizravno proizlaze iz dvojbi u pogledu osnovanosti tog utvrđenja.

176. Doista, Odlukom o sustavu zaštite privatnosti samo se utvrđuje da je primjerena razina zaštite osobnih podataka, u skladu s načelima koja ta odluka sadržava, prenesenih u poduzeće sa sjedištem u SAD-u koje je samocertificiralo pridržavanje tih načela[73]. Međutim, razmatranja iz te odluke nadilaze kontekst prijenosa obuhvaćenih tom odlukom jer se odnose na pravo i prakse koje su na snazi u toj trećoj zemlji u pogledu obrade prenesenih podataka u svrhu zaštite nacionalne sigurnosti. Kao što su

70 Iz tog je istog razloga Supreme Court (Vrhovni sud), u svojoj presudi od 31. svibnja 2019. (točke 8.1. do 8.5.) izrazio dvojbe u pogledu nužnosti nekih od tih pitanja, pri čemu je priznao da nije nadležan dovoditi u pitanje odluku suda koji je uputio zahtjev da Sudu uputi prethodna pitanja i mijenjati njihov sadržaj. Konkretno, u točki 8.5. te presude navodi se: „The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures […].”

71 Vidjeti uvodne izjave 64. do 141. Odluke o sustavu zaštite privatnosti. Podsjećam da je, kao što proizlazi iz članka 1. stavka 2. te odluke, sustav zaštite privatnosti uspostavljen ne samo u skladu s Načelima kojih se trebaju pridržavati poduzetnici koji žele prenositi podatke na temelju navedene odluke, nego i sa službenim izjavama i obvezama vlade SAD-a iz dokumenata navedenih u prilozima toj odluci.

72 DPC-ov nacrt odluke donesen je prije Odluke o sustavu zaštite privatnosti. Kao što je to DPC pojasnio u tom nacrtu, iako je privremeno zaključeno da se zaštitnim mjerama predviđenim pravom SAD-a ne omogućuje barem da se osigura usklađenost prijenosa u tu treću zemlju s člankom 47. Povelje, *u toj fazi nije ispitao ili uzeo u obzir nove dogovore predviđene u nacrtu sporazuma o sustavu zaštite privatnosti jer on još nije bio donesen*. Međutim, u točki 307. svoje presude od 3. listopada 2017. High Court (Visoki sud) smatra: „It is fair to conclude […] that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U. S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U. S.], conflicts with the case made by the DPC to this court”.

73 Vidjeti članak 1. stavke 1. i 3., kao i uvodne izjave 14. do 16. Odluke o sustavu zaštite privatnosti.

to u biti napomenuli Facebook Ireland, M. Schrems, vlada SAD-a i Komisija, nadzor koji provode američka obavještajna tijela, kao i zaštitne mjere od opasnosti zlouporabe koje taj nadzor uključuje i mehanizmi kojima se nastoji pratiti poštovanje tih zaštitnih mjera primjenjuju se, sa stajališta prava Unije, neovisno o pravnoj osnovi koja se ističe u potporu prijenosu.

177. S tog gledišta, pitanje obvezuju li utvrđenja koja su u tom pogledu iznesena u Odluci o sustavu zaštite privatnosti nadzorna tijela kada ispituju zakonitost prijenosa provedenog na temelju standardnih ugovornih klauzula moglo bi se pokazati relevantnim za DPC-ovo odlučivanje o pritužbi M. Schremsa. U slučaju potvrdnog odgovora na to pitanje, postavilo bi se pitanje je li ta odluka zaista valjana.

178. Međutim, predlažem Sudu da ne odgovara na ta pitanja samo kako bi DPC-u pomogao da odluči o toj pritužbi s obzirom na to da na njega nije potrebno odgovoriti kako bi se sudu koji je uputio zahtjev omogućilo da riješi spor u glavnom postupku. Budući da se postupkom predviđenim u članku 267. UFEU-a uspostavlja dijalog među sudovima, Sud nije dužan iznositi pojašnjenja samo kako bi pomogao upravnom tijelu u postupku iz kojeg proizlazi taj spor.

179. Prema mojem mišljenju, u tom se pogledu tim više treba suzdržati jer Sudu nije izričito upućeno pitanje o valjanosti Odluke o sustavu zaštite privatnosti te je protiv te odluke, osim toga, već podnesena tužba za poništenje koja je u tijeku pred Općim sudom Europske unije [74].

180. Usto, kada bi odlučio o prethodno opisanim problematikama, Sud bi, prema mojem mišljenju, narušio normalan slijed postupka koji se treba odviti nakon što donese svoju presudu u ovom predmetu. U okviru tog postupka DPC je dužan odlučiti o pritužbi M. Schremsa uzimajući u obzir odgovor Suda na jedanaesto prethodno pitanje. Ako Sud presudi, kao što to predlažem i suprotno onomu što je DPC pred njim tvrdio, da Odluka 2010/87 nije nevaljana s obzirom na članke 7., 8. i 47. Povelje, smatram da bi DPC-u trebalo omogućiti da preispita spis postupka koji je pred njim u tijeku. U slučaju da DPC procijeni da ne može odlučivati o pritužbi M. Schremsa ako Sud najprije ne utvrdi predstavlja li Odluka o sustavu zaštite privatnosti prepreku izvršenju njegovih ovlasti obustave predmetnog prijenosa i potvrdi da dvoji u pogledu valjanosti te odluke, taj bi povjerenik mogao ponovno pokrenuti postupak pred nacionalnim sudovima kako bi ti sudovi o tome pitali Sud [75].

181. Tako bi se pokrenuo postupak kojim bi se svim strankama i zainteresiranim osobama iz članka 23. drugog stavka Statuta Suda omogućilo da Sudu podnesu očitovanja osobito o valjanosti Odluke o sustavu zaštite privatnosti i pritom navedu, po potrebi, konkretne ocjene koje osporavaju, kao i razloge iz kojih smatraju da je Komisija u toj odluci prekoračila smanjenu marginu prosudbe kojom je raspolagala [76]. U okviru takvog postupka, Komisija bi mogla konkretno i detaljno odgovoriti na svaku eventualnu kritiku upućenu protiv navedene odluke. Iako je u ovom predmetu strankama i zainteresiranim osobama koje su Sudu podnijele očitovanja pružena prilika da rasprave o određenim aspektima relevantnima za procjenu usklađenosti Odluke o sustavu zaštite privatnosti s člancima 7., 8. i 47. Povelje, to pitanje, s obzirom na njegovu važnost, zahtijeva iscrpno i temeljito razmatranje.

182. Prema mojem mišljenju, oprez nalaže da bi Sud trebao pričekati da se te postupovne faze dovrše prije nego što ispita utjecaj koji Odluka o sustavu zaštite privatnosti ima na način na koji nadzorno tijelo odlučuje o zahtjevu za obustavu prijenosa u SAD na temelju članka 46. stavka 1. GDPR-a i odluči o valjanosti te odluke.

74 Predmet u tijeku T-738/16, La Quadrature du Net i dr./Komisija (SL 2017., C 6, str. 39.)

75 Osim toga napominjem da DPC u svojim pisanim očitovanjima nije zauzeo stajalište o utjecaju Odluke o sustavu zaštite privatnosti na odlučivanje o pritužbi koja mu je podnesena.

76 Vidjeti u tom pogledu presudu Schrems (t. 78.).

183. To tim više vrijedi što na temelju spisa koji je podnesen Sudu nije moguće zaključiti da će DPC-ovo odlučivanje o pritužbi M. Schremsa nužno ovisiti o tome protivi li se Odluci o sustavu zaštite privatnosti to da nadzorna tijela izvršavaju svoju ovlast obustave prijenosa koji se temelji na standardnim ugovornim klauzulama.

184. U tom pogledu, kao prvo, nije isključeno da bi DPC mogao obustaviti predmetni prijenos iz razloga koji se ne odnose na navodnu neprimjerenost razine zaštite koja se u SAD-u osigurava od povreda ispitanikovih temeljnih prava koja proizlaze iz aktivnosti američkih obavještajnih službi. Konkretno, sud koji je uputio zahtjev pojasnio je da M. Schrems u svojoj pritužbi pred DPC-om tvrdi da ugovorne klauzule koje Facebook Ireland ističe u prilog tom prijenosu ne odražavaju vjerno klauzule sadržane u Prilogu Odluci 2010/87. K tomu, M. Schrems tvrdi da navedeni prijenos nije obuhvaćen područjem primjene te odluke, nego drugih Odluka o SUK-ovima[77].

185. Kao drugo, DPC i sud koji je uputio zahtjev istaknuli su da se Facebook Ireland, u prilog prijenosu iz pritužbe M. Schremsa, nije pozvao na Odluku o sustavu zaštite privatnosti[78], što je to društvo potvrdilo na raspravi. Iako je Facebook Inc. samocertificirao svoje pridržavanje načela sustava zaštite privatnosti podataka od 30. rujna 2016.[79], Facebook Ireland tvrdi da se to pridržavanje odnosi samo na prijenos određenih kategorija podataka, odnosno kategorija poslovnih partnera Facebooka Inc. Činilo bi mi se neprimjerenim da Sud predvidi pitanja koja bi se u tom pogledu mogla pojaviti ispitivanjem toga bi li, pod pretpostavkom da se Facebook Ireland ne može pozvati na Odluku 2010/87 u potporu predmetnom prijenosu, taj prijenos ipak bio obuhvaćen Odlukom o sustavu zaštite privatnosti, iako potonje društvo nije istaknulo taj argument ni pred sudom koji je uputio zahtjev ni pred DPC-om.

186. Iz toga zaključujem da nije potrebno odgovoriti na drugo, treće, četvrto, peto, deveto i deseto prethodno pitanje niti ispitati valjanost Odluke o sustavu zaštite privatnosti.

G. Podredne napomene o učincima i valjanosti Odluke o sustavu zaštite privatnosti

187. Iako na temelju prethodne analize najprije predlažem Sudu da ne odluči o utjecaju Odluke o sustavu zaštite privatnosti na odlučivanje o pritužbi kao što je ona koju je M. Schrems podnio DPC-u i na valjanost te odluke, čini mi se korisnim, podredno i uz određene rezerve, iznijeti nekoliko neiscrpnih napomena u tom pogledu.

1. Utjecaj Odluke o sustavu zaštite privatnosti u okviru postupka u kojem nadzorno tijelo odlučuje o pritužbi koja se odnosi na zakonitost prijenosa koji se temelji na ugovornim zaštitnim mjerama

188. Devetim prethodnim pitanjem nastoji se odrediti je li utvrđenje izneseno u Odluci o sustavu zaštite privatnosti koje se odnosi na primjerenost, s obzirom na ograničenja pristupa prenesenim podacima i načina na koji ih američka tijela upotrebljavaju u svrhu nacionalne sigurnosti, kao i pravne zaštite ispitanika, te na razinu zaštite koja se osigurava u SAD-u prepreka tomu da nadzorno tijelo obustavi prijenos u tu treću zemlju proveden na temelju standardnih ugovornih klauzula.

77 M. Schrems u prilog toj tvrdnji navodi da Facebook Inc. ne treba smatrati samo izvršiteljem obrade, nego i „voditeljem obrade”, u smislu članka 4. točke 7. GDPR-a kada je riječ o obradi osobnih podataka korisnika društvene mreže Facebook. Vidjeti u tom pogledu presudu od 5. lipnja 2018., Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, t. 30.).

78 Vidjeti presudu High Courta (Visoki sud) od 3. listopada 2017. (t. 66.).

79 Vidjeti internetsku stranicu sustava zaštite privatnosti (https://www.privacyshield.gov/participant_search).

189. Čini mi se da tu problematiku treba razmotriti s obzirom na točke 51. i 52. presude Schrems, iz koje proizlazi da je odluka o primjerenosti obvezujuća za nadzora tijela sve dok je se ne proglasi nevaljanom. Nadzorno tijelo kojem je pritužbu podnijela osoba čiji su podaci preneseni u treću zemlju na koju se odnosi odluka o primjerenosti stoga ne može obustaviti prijenos zato što je razina zaštite u toj zemlji neprimjerena ako Sud prije toga nije tu odluku proglasio nevaljanom [80].

190. Sud koji je uputio zahtjev u biti želi znati vrijedi li, u pogledu odluke o primjerenosti, kao što je Odluka o sustavu zaštite privatnosti ili, prije nje, Odluka o privatnosti „sigurne luke", koja se temelji na tome da se poduzetnici dobrovoljno pridržavaju načela koja sadržava ta odluka, taj zaključak samo kada je prijenos u dotičnu treću zemlju obuhvaćen tom odlukom ili također kada ima drukčiju pravnu osnovu.

191. Prema mišljenju M Schremsa, njemačke, nizozemske, poljske i portugalske vlade te Komisije, utvrđenjem primjerenosti u okviru Odluke o sustavu zaštite privatnosti nadzornim se tijelima ne uskraćuje njihova ovlast obustave ili zabrane prijenosa u SAD koji se provodi na temelju standardnih ugovornih klauzula. Kada se prijenos u SAD ne temelji na Odluci o sustavu zaštite privatnosti, nadzorna tijela nisu formalno obvezana tom odlukom u okviru izvršavanja ovlasti koje su im povjerene člankom 58. stavkom 2. GDPR-a. Drugim riječima, ta tijela mogu odstupiti od Komisijinih utvrđenja o primjerenosti razine zaštite od miješanja američkih javnih tijela u ostvarivanje ispitanikovih temeljnih prava. Nizozemska vlada i Komisija pojašnjavaju da ih nadzorna tijela ipak trebaju uzeti u obzir kada izvršavaju te ovlasti. Prema mišljenju njemačke vlade, ta su tijela mogla doći do suprotnih ocjena tek po završetku ispitivanja, koje uključuje relevantne provjere, u pogledu merituma Komisijinih utvrđenja.

192. Suprotno tomu, Facebook Ireland i vlada SAD-a u biti tvrde da obvezujući učinak odluke o primjerenosti podrazumijeva, s obzirom na zahtjeve pravne sigurnosti i ujednačene primjene prava Unije, da nadzorna tijela nisu ovlaštena dovoditi u pitanje, čak i u okviru odlučivanja o pritužbi za obustavu prijenosa u dotičnu treću zemlju na drugom temelju koji nije ta odluka, utvrđenja sadržana u navedenoj odluci.

193. Slažem se s prvim od tih dvaju pristupa. Budući da je područje primjene Odluke o sustavu zaštite privatnosti ograničeno na prijenose u poduzeće koje je samocertificirano na temelju te odluke, navedenom odlukom nadzorna tijela nije moguće formalno obvezati u pogledu prijenosa koji nisu obuhvaćeni tim područjem primjene. Stoga se Odlukom o sustavu zaštite privatnosti jednako tako nastoji pružiti pravna sigurnost samo u korist izvoznika koji prenose podatke u okviru koji je uspostavljen tom odlukom. Prema mojem mišljenju, neovisnosti koja se člankom 52. GDPR-a priznaje nadzornim tijelima također se protivi to da su za njih obvezujuća utvrđenja koja je Komisija iznijela u odluci o primjerenosti koja je čak izvan njegova područja primjene.

194. Očito je da su utvrđenja sadržana u Odluci o sustavu zaštite privatnosti koja se odnose na primjerenost razine zaštite koja se u SAD-u osigurava od miješanja povezanih s aktivnostima njegovih obavještajnih službi, polazišna točka analize kojom nadzorno tijelo u svakom slučaju zasebno ocjenjuje treba li prijenos koji se temelji na standardnim ugovornim klauzulama obustaviti zbog takvih miješanja. Međutim, ako po završetku temeljite istrage smatra da se ne može složiti s tim utvrđenjima u pogledu prijenosa o kojem je obaviješteno, nadležno nadzorno tijelo i dalje, prema mojem mišljenju, može izvršavati ovlasti koje su mu povjerene člankom 58. stavkom 2. točkama (f) i (j) GDPR-a.

195. U slučaju da Sud na pitanje koje se ovdje ispituje dâ odgovor suprotan onomu koji ja zagovaram, bilo bi potrebno ispitati ne bi li te ovlasti ipak trebalo ponovno uspostaviti zbog nevaljanosti Odluke o sustavu zaštite privatnosti.

80 Vidjeti u tom smislu presudu Schrems (t. 59.).

2. Valjanost Odluke o sustavu zaštite privatnosti

196. Napomene koje slijede sadržavaju određena pitanja o osnovanosti ocjena sadržanih u Odluci o sustavu zaštite privatnosti u pogledu primjerenosti, u smislu članka 45. stavka 1. GDPR-a, razine zaštite koju osigurava SAD s obzirom na aktivnosti nadzora elektroničkih komunikacija koje provode američka obavještajna tijela. Cilj tih napomena nije iznijeti konačno ili iscrpno stajalište o valjanosti te odluke. Njima se samo iznose određena razmatranja koja se mogu pokazati korisnima Sudu ako će htjeti, suprotno onomu što ja predlažem, odlučivati o tom pitanju.

197. U tom pogledu, iz uvodne izjave 64. i točke I.5. Priloga II. Odluci o sustavu zaštite privatnosti proizlazi da se poduzetnikova pridržavanja načela iz te odluke može ograničiti, osobito, zahtjevima u pogledu nacionalne sigurnosti, javnog interesa i kaznenog progona ili proturječnim obvezama koje se temelje na američkom pravu.

198. Komisija je stoga zaštitne mjere dostupne u pravu SAD-a procijenila u vezi s pristupom prenesenim podacima i načinom na koji ih američka javna tijela upotrebljavaju u svrhu, konkretno, nacionalne sigurnosti[81]. Američka vlada obvezala se prema Komisiji u pogledu, s jedne strane, ograničenja načina na koji američka tijela pristupaju prenesenim podacima i upotrebljavaju ih, kao i, s druge strane, pravne zaštite ponuđene ispitanicima[82].

199. M. Schrems pred Sudom tvrdi da je Odluka o sustavu zaštite privatnosti nevaljana jer tako opisane zaštitne mjere nisu dovoljne da bi se osigurala primjerena razina zaštite temeljnih prava osoba čiji su podaci preneseni u SAD. DPC, EPIC te austrijska, poljska i portugalska vlada osporavaju, a da pritom ne dovode u pitanje valjanost te odluke, ocjene koje je Komisija u toj odluci utvrdila u pogledu primjerenosti razine zaštite od miješanja koja proizlaze iz aktivnosti američkih obavještajnih službi. Te dvojbe odražavaju zabrinutosti koje su izrazili Parlament[83], EOZP[84] i EDPS[85].

200. Prije ispitivanja osnovanosti utvrđenja primjerenosti iznesenog u Odluci o sustavu zaštite privatnosti, potrebno je pojasniti metodologiju koju treba primijeniti pri tom ispitivanju.

a) Pojašnjenja u pogledu sadržaja ispitivanja koje se odnosi na valjanost odluke o primjerenosti

1) Elementi usporedbe na temelju kojih je moguća procjena „bitne ekvivalentnosti” razine zaštite

201. U skladu s člankom 45. stavkom 3. GDPR-a i sudskom praksom Suda[86], Komisija može utvrditi da treća zemlja osigurava primjerenu razinu zaštite samo ako je zaključila, propisno obrazloženo, da je razina zaštite temeljnih prava ispitanikâ u toj zemlji „bitno ekvivalentna” razini zaštite koja se zahtijeva u Uniji na temelju te uredbe s obzirom na Povelju.

81 Vidjeti uvodnu izjavu 65. Odluke o sustavu zaštite privatnosti.

82 Vidjeti Priloge III. do VII. Odluke o sustavu zaštite privatnosti.

83 Rezolucije Parlamenta od 6. travnja 2017. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti, P8_TA(2017)0131 i od 5. srpnja 2018. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti, P8_TA-PROV(2018)0315

84 Vidjeti radnu skupinu iz članka 29. za zaštitu podataka (u daljnjem tekstu: radna skupina 29), Opinion 1/2016 on the EU-U. S. Privacy Shield draft adequacy decision, 13. travnja 2016., WP 238; Groupe 29, EU-US Privacy Shield – First Annual Joint Review, 28. studenoga 2017., WP 255 i EOZP, EU-US Privacy Shield – Second Annual Joint Review, 22. siječnja 2019. Radna skupina 29 uvedena je člankom 29. stavkom 1. Direktive 95/46 kojim se predviđa da ima savjetodavni status i da djeluje neovisno. U skladu sa stavkom 2. tog članka, ta je radna skupina bila sastavljena od predstavnika svakog nacionalnog nadzornog tijela i predstavnika svakog tijela osnovanog za ustanove i tijela Zajednice te predstavnika Komisije. Od stupanja na snagu GDPR-a radna skupina 29 zamijenjena je EOZP-om (vidjeti članak 94. stavak 2. te uredbe).

85 Vidjeti EDPS, Mišljenje 4/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti, od 30. svibnja 2016. EDPS uveden je člankom 1. stavkom 2. Uredbe (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL 2001., L 8, str. 1.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 34., str. 6.). On nadzire primjenu odredbi te uredbe.

86 Vidjeti točku 112. ovog mišljenja.

202. Stoga provjera primjerenosti razine zaštite koja se osigurava u trećoj zemlji nužno podrazumijeva usporedbu, s jedne strane, pravila i praksa koje se primjenjuju u toj trećoj zemlji i, s druge strane, standarda zaštite koji su na snazi u Uniji. Drugim pitanjem sud koji je uputio zahtjev zahtijeva od Suda da pojasni elemente te usporedbe [87].

203. Točnije, taj sud želi znati podrazumijeva li pridržaj ovlasti koji se člankom 4. stavkom 2. UEU-a i člankom 2. stavkom 2. GDPR-a priznaje državama članicama u području zaštite nacionalne sigurnosti da pravni poredak Unije ne sadržava standarde zaštite s kojima treba usporediti, kako bi se procijenila njihova primjerenost, zaštitne mjere kojima se, u svrhu zaštite nacionalne sigurnosti, u trećoj zemlji ograničava obrada od strane javnih tijela podataka koji su im preneseni. U slučaju potvrdnog odgovora, navedeni sud nastoji saznati kako treba utvrditi relevantni referentni okvir.

204. U tom pogledu, valja uzeti u obzir da je svrha ograničenja koja Unija primjenjuje na međunarodne prijenose osobnih podataka, pri čemu zahtijeva da se osigura kontinuirana razina zaštite prava ispitanikâ, izbjeći opasnost od zaobilaženja standarda primjenjivih u Uniji [88]. Kao što je to u biti tvrdio Facebook Ireland, nipošto se ne može od treće zemlje opravdano očekivati, s obzirom na taj cilj, da poštuje zahtjeve koji ne odgovaraju obvezama koje imaju države članice.

205. Međutim, u skladu s njegovim člankom 51. stavkom 1., Povelja se primjenjuje na države članice samo kada provode pravo Unije. Prema tome, valjanost odluke o primjerenosti s obzirom na ograničenja ostvarivanja ispitanikovih temeljnih prava koja proizlaze iz propisa treće zemlje odredišta ovisi o usporedbi između tih ograničenja i ograničenja koja na temelju odredbi Povelje države članice nalažu *samo ako je sličan propis države članice obuhvaćen područjem primjene prava Unije*.

206. Međutim, pri ocjenjivanju primjerenosti razine zaštite koja se osigurava u trećoj državi odredišta ne mogu se zanemariti eventualna miješanja u ostvarivanje temeljnih prava predmetnih osoba koja proizlaze iz državnih mjera, osobito u području nacionalne sigurnosti, koje, ako ih je donijela država članica, nisu obuhvaćene područjem primjene prava Unije. U svrhu te ocjene, člankom 45. stavkom 2. točkom (a) GDPR-a zahtijeva se uzimanje u obzir, bez ikakvog ograničenja, propisa u području nacionalne sigurnosti koji su na snazi u toj državi članici.

207. Procjena primjerenosti razine zaštite s obzirom na takve državne mjere podrazumijeva, prema mojem mišljenju, usporedbu zaštitnih mjera koje se na njih primjenjuju s razinom zaštite koja se zahtijeva u Uniji na temelju prava država članica, uključujući obveze koje imaju na temelju EKLJP-a. Budući da pridržavanje EKLJP-a države članice obvezuje na to da svoja nacionalna prava usklade s odredbama te konvencije i da je ono stoga, kao što su to u biti istaknuli Facebook Ireland, njemačka i češka vlada te Komisija, zajedničko državama članicama, te ću odredbe smatrati relevantnim elementom usporedbe za potrebe te procjene.

208. U ovom slučaju, kao što je prethodno navedeno [89], zahtjevi u pogledu nacionalne sigurnosti SAD-a imaju prednost pred obvezama poduzetnika koji su samocertificirani na temelju Odluke o sustavu zaštite privatnosti. Valjanost te odluke također ovisi o tome primjenjuju li se na te zahtjeve zaštitne mjere kojima se nudi razina zaštite koja je bitno ekvivalentna razini zaštite koju je potrebno osigurati u Uniji.

87 Podsjećam da se bitna ekvivalentnost razine zaštite koju jamči treća država u odnosu na razinu zaštite koja se zahtijeva u Uniji također treba procijeniti i kada, u okviru konkretnog prijenosa koji se temelji na standardnim ugovornim klauzulama predviđenim u Odluci 2010/87, voditelj obrade ili, ako on ne postoji, nadležno nadzorno tijelo provjerava jesu li javna tijela treće zemlje odredišta uvoznika podvrgnula zahtjevima koji prekoračuju granice onoga što je neophodno u demokratskom društvu (vidjeti klauzulu 5. iz Priloga Odluci 2010/87, kao i bilješku koja se odnosi na tu klauzulu). Vidjeti točke 115., 134. i 135. ovog mišljenja.

88 Vidjeti točku 117. ovog mišljenja.

89 Vidjeti točku 197. ovog mišljenja.

209. Da bi se odgovorilo na to pitanje najprije je potrebno utvrditi standarde, koji se temelje na Povelji ili pak na EKLJP-u, koje u Uniji moraju ispunjavati propisi u području nadzora elektroničkih komunikacija koji su slični propisima koje je Komisija ispitala u Odluci o sustavu zaštite privatnosti. Određivanje primjenjivih standarda ovisi o tome primjenjuje li se na propise kao što su članak 702. FISA-e i EO br. 12333, ako ih je donijela država članica, ograničenje koje je obuhvaćeno područjem primjene GDPR-a na temelju članka 2. stavka 2. te uredbe, s obzirom na članak 4. stavak 2. UEU-a.

210. U tom pogledu, iz teksta članka 4. stavka 2. UEU-a i iz ustaljene sudske prakse proizlazi da se pravo Unije i, među ostalim, instrumenti sekundarnog prava u pogledu zaštite osobnih podataka ne primjenjuju na aktivnosti u području zaštite nacionalne sigurnosti ako su one aktivnosti država odnosno državnih tijela koje ne ulaze u područje aktivnosti pojedinaca [90].

211. To načelo podrazumijeva, *s jedne strane*, da propis u području zaštite nacionalne sigurnosti nije obuhvaćen područjem primjene prava Unije kada se njime uređuju samo državne aktivnosti a da se ne primjenjuje ni na jednu aktivnost koju obavljaju pojedinci. Prema tome, to se pravo ne primjenjuje, prema mojem mišljenju, na nacionalne mjere u pogledu prikupljanja i upotrebe osobnih podataka koje je država izravno provela u svrhu zaštite nacionalne sigurnosti a da nije nametnula konkretne obveze privatnim subjektima. Konkretno, kao što je to Komisija tvrdila na raspravi, mjera koju je donijela država članica i kojom se, kao i EO-om br. 12333, njezinim sigurnosnim službama odobrava izravan pristup podacima u prijelazu, bila bi isključena iz područja primjene prava Unije [91].

212. Znatno je složenije pitanje jesu li, *s druge strane*, nacionalne odredbe kojima se, jednako kao i člankom 702. FISA-e, pružatelji usluga elektroničkih komunikacija obvezuju na to da pružaju potporu nadležnim tijelima u području nacionalne sigurnosti kako bi im omogućili da pristupe određenim osobnim podacima, također isključene iz područja primjene prava Unije.

213. Iako presuda PNR ide u prilog potvrdnom odgovoru na to pitanje, rasuđivanjem iz presuda Tele2 Sverige i Ministerio Fiscal mogao bi se opravdati negativan odgovor na navedeno pitanje.

214. U presudi PNR, Sud je poništio odluku kojom je Komisija utvrdila primjerenost razine zaštite osobnih podataka iz popisa imena zrakoplovnih putnika (Passenger Name Records, PNR) prenesenih američkom tijelu nadležnom za carinu i zaštitu granica [92]. Sud je presudio da je obrada na koju se odnosila ta odluka, odnosno prijenos podataka iz PNR-a koji zračni prijevoznici provode u korist predmetnog tijela, *s obzirom na njezin predmet*, isključena iz područja primjene Direktive 95/46 predviđenog u njezinu članku 3. stavku 2. Prema mišljenju Suda, ta obrada nije bila nužna za pružanje usluga, nego upravo za zaštitu javne sigurnosti i za potrebe kaznenog progona. Budući da je predmetni

90 Vidjeti osobito presudu od 6. studenoga 2003., Lindqvist (C-101/01, EU:C:2003:596, t. 43. i 44.); presuda PNR (t. 58.); presuda od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia (C-73/07, EU:C:2008:727, t. 41.); presuda od 21. prosinca 2016., Tele2 Sverige i Watson i dr. (C-203/15 i C-698/15, EU:C:2016:970, u daljnjem tekstu: presuda Tele2 Sverige, t. 69.), kao i presuda od 2. listopada 2018., Ministerio Fiscal (C-207/16, EU:C:2018:788, u daljnjem tekstu: presuda Ministerio Fiscal, t. 32.).

91 Kako bi se izbjegle sve nejasnoće u tom pogledu, naglašavam da u Odluci o sustavu zaštite privatnosti Komisija nije mogla utvrditi presreće li SAD stvarno komunikacije koje prelaze prekoatlantskim kablovima jer američka tijela nisu niti potvrdila niti opovrgnula to stajalište (vidjeti uvodnu izjavu 75. te odluke, kao i dopis Roberta Litta od 22. veljače 2016. naveden u točki I. podtočki (a) Priloga VI. navedenoj odluci). Međutim, budući da vlada SAD-a nije porekla da je prikupljala podatke u prijelazu na temelju EO-a br. 12333, čini mi se da je Komisija, prije utvrđivanja primjerenosti, trebala od potonje vlade dobiti jamstva da bi se na takvo prikupljanje, kada bi do njega došlo, primjenjivala dovoljne zaštitne mjere od rizika zlouporabe. S tog je gledišta Komisija u uvodnim izjavama 68. do 77. navedene odluke ispitala ograničenja i zaštitne mjere koje se bi se trebale primijeniti u takvom slučaju na temelju PPD-a 28.

92 Bila je riječ o Odluci Komisije 2004/535/EZ od 14. svibnja 2004. o primjerenoj razini zaštite osobnih podataka iz popisa imena zrakoplovnih putnika koji se prenose Uredu za carinu i zaštitu granica Sjedinjenih Američkih Država (SL 2004., L 235, str. 11.).

prijenos bio obuhvaćen okvirom koji su uspostavile javne vlasti u pogledu javne sigurnosti, bio je isključen iz područja primjene te direktive unatoč tomu što su podatke iz PNR-a prvotno prikupili privatni subjekti u okviru komercijalne aktivnosti obuhvaćene tim područjem primjene i što su taj prijenos organizirali potonji subjekti [93].

215. U kasnijoj presudi Tele2 Sverige [94], Sud je odlučio da su nacionalne odredbe, koje se temelje na članku 15. stavku 1. Direktive 2002/58/EZ [95], kojima se uređuje zadržavanje podataka o prometu i lokaciji koje provode pružatelji telekomunikacijskih usluga, kao i pristup tijela javne vlasti podacima zadržanima u svrhe navedene u toj odredbi, koje uključuju kazneni progon i zaštitu nacionalne sigurnosti, obuhvaćene područjem primjene te direktive i stoga Povelje. Prema mišljenju Suda, ni odredbe o zadržavanju podataka ni odredbe o pristupu zadržanim podacima nisu obuhvaćene isključenjem iz područja primjene te direktive koje je predviđeno u njezinu članku 1. stavku 3., u kojem se upućuje, među ostalim, na aktivnosti države u području kaznenog progona i zaštite nacionalne sigurnosti [96]. Sud je potvrdio tu sudsku praksu u presudi Ministerio Fiscal [97].

216. Međutim, članak 702. FISA-e razlikuje se od takvog propisa jer se tim propisom pružateljima elektroničkih komunikacijskih usluga ne nalaže nikakva obveza čuvanja podataka ni provedbe bilo kakve druge obrade ako obavještajna tijela nisu podnijela zahtjev za pristup podacima.

217. Prema tome, postavlja se pitanje jesu li područjem primjene GDPR-a i, stoga, Povelje obuhvaćene nacionalne mjere kojima se tim pružateljima nalaže obveza da tijelima javne vlasti stave podatke na raspolaganje u svrhu nacionalne sigurnosti *neovisno o bilo kakvoj obvezi zadržavanja* [98].

218. *Prvi pristup* mogao bi obuhvaćati usklađivanje, koliko je moguće, dvaju prethodno navedenih smjerova sudske prakse na način da se zaključak koji je Sud izveo u presudama Tele2 Sverige i Ministerio Fiscal, u pogledu primjenjivosti prava Unije na mjere kojima se uređuje pristup nacionalnih tijela podacima u svrhu, među ostalim, zaštite nacionalne sigurnosti [99], odnosi samo na slučajeve u kojima su podaci zadržani *na temelju zakonske obveze* uvedene na temelju članka 15. stavka 1. Direktive 2002/58. Suprotno tomu, taj se zaključak ne bi primijenio na drukčiji činjenični kontekst presude PNR, u kojem su podaci koje su zračni prijevoznici zadržali, u komercijalnu svrhu, na njihovu inicijativu bili preneseni američkom tijelu nadležnom za unutarnju sigurnosti.

93 Presuda PNR (t. 56. do 58.). Osim toga, u presudi od 10. veljače 2009., Irska/Parlament i Vijeće (C-301/06, EU:C:2009:68, t. 90. i 91.), Sud je odlučio da se razmatranja iz presude PNR ne mogu primijeniti na obrade iz Direktive 2006/24/EZ Europskog parlamenta i Vijeća od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmjeni Direktive 2002/58/EZ (SL 2006., L 105, str. 54.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 50., str. 30.). Sud je taj zaključak opravdao činjenicom da su Direktivom 2006/24, za razliku od odluke o kojoj je riječ u presudi PNR, bile uređene samo aktivnosti pružatelja usluga na unutarnjem tržištu, a ne i aktivnosti tijela javne vlasti za potrebe kaznenog progona. Čini se da je tim rasuđivanjem Sud tvrdio da bi se, *a contrario*, zaključak iznesen u presudi PNR primjenjivao na odredbe o pristupu zadržanim podacima ili načinu na koji ih upotrebljavaju ta tijela.

94 Presuda Tele2 Sverige (t. 67. do 81.)

95 Direktiva Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL 2002., L 201, str. 37.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.)

96 Budući da su u Direktivi 2002/58 konkretizirani zahtjevi iz Direktive 95/46, koja je sada stavljena izvan snage GDPR-om kojim je uvelike preuzet njezin sadržaj, čini mi se da se sudska praksa u pogledu tumačenja članka 1. stavka 3. Direktive 2002/58 po analogiji primjenjuje na tumačenje članka 2. stavka 2. GDPR-a. Vidjeti u tom smislu presude Tele2 Sverige (t. 69.) i Ministerio Fiscal (t. 32.).

97 Presuda Ministerio Fiscal (t. 34., 35. i 37.)

98 To je pitanje postavljeno i u okviru druga tri prethodna postupka koji su u tijeku pred Sudom. Vidjeti predmet C-623/17, Privacy International (SL 2018., C 22, str. 29.), kao i spojene predmete C-511/18 i C-512/18, La Quadrature du Net i dr. i French Data Network i dr. (SL 2018., C 392, str. 7.).

99 U presudi Tele2 Sverige, iako se Sud usredotočio na ispitivanje opravdanosti miješanja koja proizlaze iz predmetnih mjera zadržavanja i pristupa s obzirom na cilj borbe protiv kaznenih djela, zaključak do kojeg je došao također se primjenjuje, *mutatis mutandis*, kada takve mjere imaju za cilj zaštitu nacionalne sigurnosti. Naime, u članku 15. stavku 1. Direktive 2002/58 navode se, među ciljevima kojima se mogu opravdati takve mjere, borba protiv kaznenih djela i zaštita nacionalne sigurnosti. Osim toga, člankom 1. stavkom 3. Direktive 2002/58 i člankom 2. stavkom 2. GDPR-a isključuju se iz područja primjene tih instrumenata aktivnosti države u području nacionalne sigurnosti, kao i kaznenog prava. Uostalom, mjerama o kojima je riječ u predmetu u kojem je donesena presuda Tele2 Sverige također se nastoji postići cilj koji je povezan s nacionalnom sigurnosti. U točki 119. te presude Sud je izričito ispitao problematiku opravdanosti mjera zadržavanja i pristupa podacima o prometu i lokaciji s obzirom na cilj zaštite nacionalne sigurnosti koji uključuje borbu protiv terorizma.

219. U skladu s *drugim pristupom*, koji predlaže Komisija i koji ja smatram uvjerljivijim, rasuđivanjem iz presuda Tele2 Sverige i Ministerio Fiscal opravdala bi se primjenjivost prava Unije na nacionalna pravila kojima se od pružatelja elektroničkih komunikacijskih usluga zahtijeva da pomognu tijelima zaduženima za nacionalnu sigurnost kako bi ona mogla pristupiti određenim podacima, *pri čemu je nevažno primjenjuje li se na ta pravila ranija obveza zadržavanja podataka*.

220. Srž tog rasuđivanja ne temelji se, naime, na predmetu predmetnih odredbi kao što je to slučaj u presudi PNR, nego na činjenici da su tim odredbama bile uređene aktivnosti pružatelja usluga na način da su bili obvezni obrađivati podatke. Te aktivnosti nisu bile aktivnosti države u područjima iz članka 1. stavka 3. Direktive 2002/58 i članka 3. stavka 2. Direktive 95/46, čiji je sadržaj u biti preuzet u članku 2. stavku 2. GDPR-a.

221. Stoga je Sud u presudi Tele2 Sverige napomenuo da se „pristup podacima koje su zadržali navedeni pružatelji odnosi […] na *njihovu* obradu osobnih podataka koja spada u područje primjene iste direktive” [100]. Jednako tako, u presudi Ministerio Fiscal presudio je da zakonske mjere kojima se pružateljima usluga nalaže da nadležnim tijelima odobre pristup zadržanim podacima „nužno podrazumijevaju da *ti pružatelji* obrađuju te podatke” [101].

222. Međutim, stavljanje podataka na raspolaganje koje voditelj obrade provodi u korist tijela javne vlasti odgovara definiciji „obrade” predviđenoj u članku 4. stavku 2. GDPR-a [102]. Isto vrijedi za prethodno filtriranje podataka na temelju kriterija pretraživanja radi izdvajanja podataka za koje su tijela javne vlasti tražila pristup [103].

223. Iz toga zaključujem da se, u skladu s rasuđivanjem koje je Sud iznio u presudama Tele2 Sverige i Ministerio Fiscal, GDPR i, stoga, Povelja primjenjuju na nacionalni propis kojim se pružatelja elektroničkih komunikacijskih usluga obvezuje da ponudi svoju pomoć tijelima zaduženima za nacionalnu sigurnost tako da im stavi podatke na raspolaganje, po potrebi nakon što ih je filtrirao, čak neovisno o bilo kakvoj zakonskoj obvezi zadržavanja tih podataka.

224. Usto, čini se da to tumačenje proizlazi, barem implicitno, iz presude Schrems. Kao što su to istaknuli DPC, austrijska i poljska vlada te Komisija, Sud je u okviru ispitivanja valjanosti Odluke o privatnosti „sigurne luke” u toj presudi odlučio da se pravom treće zemlje na koju se odnosi odluka o primjerenosti trebaju predviđati zaštitne mjere koje su bitno ekvivalentne zaštitnim mjerama koje proizlaze, među ostalim, iz članaka 7., 8. i 47. Povelje od miješanja njezinih tijela javne vlasti u temeljna prava ispitanikâ u svrhu nacionalne sigurnosti [104].

225. Konkretnije, iz toga slijedi da člankom 2. stavkom 2. GDPR-a nije obuhvaćena nacionalna mjera kojom se pružatelje elektroničkih komunikacijskih usluga obvezuje na to da prihvate zahtjev nadležnih tijela za nacionalnu sigurnost za pristup određenim podacima koje su ti pružatelji zadržali u okviru svojih komercijalnih aktivnosti neovisno o bilo kakvoj zakonskoj obvezi, na način da unaprijed utvrde podatke zatražene primjenom čimbenikâ za odabir (kao u okviru programa PRISM). Isto bi vrijedilo za nacionalnu mjeru kojom se od poduzetnika koji čine „kostur” telekomunikacija zahtijeva da tijelima zaduženima za nacionalnu sigurnost daju pristup podacima koji prelaze infrastrukturama kojima upravljaju (kao u okviru programa Upstream).

100 Presuda Tele2 Sverige (t. 78., moje isticanje). Kao što to potvrđuje uporaba izraza „[n]adalje”, Sud je u točki 79. te presude istaknuo usku vezu između obveze zadržavanja podataka o kojoj je riječ u predmetu u kojem je donesena ta presuda i odredbi o pristupu nacionalnih tijela zadržanim podacima samo kako bi potkrijepio svoj zaključak o primjenjivosti Direktive 2002/58.

101 Presuda Ministerio Fiscal (t. 37., moje isticanje)

102 Vidjeti u tom smislu presudu Ministerio Fiscal (t. 38.).

103 Vidjeti u tom smislu presudu od 13. svibnja 2014., Google Spain i Google (C-131/12, EU:C:2014:317, t. 28.).

104 Presuda Schrems (t. 91. do 96.). U uvodnim izjavama 90., 124. i 141. Odluke o sustavu zaštite privatnosti, Komisija uostalom upućuje na odredbe Povelje, čime prihvaća načelo prema kojem ograničenja temeljnih prava s ciljem zaštite nacionalne sigurnosti trebaju biti u skladu s Poveljom.

226. Suprotno tomu, kad se predmetni podaci dostave državnim tijelima, njihovo zadržavanje i kasnija upotreba od strane tih tijela u svrhu nacionalne sigurnosti, prema mojem su mišljenju, iz istih razloga koji se navode u točki 211. ovog mišljenja, obuhvaćeni odstupanjem predviđenim u članku 2. stavku 2. GDPR-a tako da ne ulaze u područje primjene te uredbe ni, stoga, Povelje.

227. Sobzirom na sve prethodno navedeno, smatram da nadzor nad valjanosti Odluke o sustavu zaštite privatnosti s obzirom na ograničenja primjenjiva na načela iz te odluke koja mogu proizlaziti iz aktivnosti američkih obavještajnih tijela uključuje dvostruku provjeru.

228. *Kao prvo*, valjat će ispitati osigurava li SAD razinu zaštite koja je bitno ekvivalentna razini zaštite koja proizlazi iz odredbi GDPR-a i Povelje od ograničenja koja proizlaze iz primjene članka 702. FISA-e jer se tom odredbom omogućava da NSA pružatelje usluga obvežu na to da mu stave na raspolaganje osobne podatke.

229. *Kao drugo*, odredbe EKLJP-a bit će relevantan referentan okvir za procjenu toga dovode li ograničenja koja može uzrokovati primjena EO-a br. 12333, s obzirom na to da se njime ovlašćuje obavještajna tijela da sama prikupljaju osobne podatke, bez pomoći privatnih subjekata, u pitanje primjerenost razine zaštite koja se osigurava u SAD-u. Te će odredbe također pružiti standarde za usporedbu na temelju kojih će se moći ocijeniti primjerenost te razine zaštite s obzirom na zadržavanje i upotrebu podataka koje su ta tijela stekla u svrhu nacionalne sigurnosti.

230. Međutim, također treba utvrditi pretpostavlja li utvrđenje primjerenosti da prikupljanje podataka na temelju EO-a br. 12333 bude popraćeno razinom zaštite koja je bitno ekvivalentna razini zaštite koju valja osigurati u Uniji *čak i u situacijama u kojima se to prikupljanje odvilo izvan državnog područja SAD-a*, tijekom faze prijelaza podataka iz Unije u tu treću zemlju.

2) Potreba osiguravanja primjerene razine zaštite tijekom faze prijelaza podataka

231. Pred Sudom su zagovarana tri različita stajališta u pogledu toga treba li Komisija uzeti u obzir, u svrhu procjene primjerenosti razine zaštite koja se osigurava u trećoj zemlji, nacionalne mjere za pristup tijelâ te treće zemlje podacima, izvan njezina državnog područja, tijekom faze prijelaza podataka iz Unije na to državno područje.

232. Kao prvo, Facebook Ireland, vlada SAD-a i Ujedinjena Kraljevina u biti tvrde da postojanje takvih mjera ne utječe na utvrđenje primjerenosti. Oni se u potporu tom pristupu pozivaju na to da treća država ne može kontrolirati sva komunikacijska sredstva izvan njezina državna područja kojima prelaze podaci iz Unije, tako da se u teoriji nikad ne može zajamčiti da druga treća država ne prikuplja tajno podatke tijekom njihova prijelaza.

233. Kao drugo, DPC, M. Schrems, EPIC, austrijska i nizozemska vlada, Parlament i EOZP tvrde da zahtjev za kontinuiranom razinom zaštite, iz članka 44. GDPR-a, podrazumijeva da ta razina treba biti primjerena tijekom cijelog prijenosa, uključujući kada podaci prelaze podmorskim kablovima prije nego što pristignu na državno područje treće zemlje odredišta.

234. Iako priznaje to načelo, kao treće, Komisija tvrdi da je cilj utvrđenja primjerenosti isključivo zaštita koju dotična treća zemlja osigurava *unutar svojih granica*, tako da se okolnošću da primjerena razina zaštite nije zajamčena *tijekom prijelaza u* tu treću zemlju ne dovodi u pitanje valjanost odluke o primjerenosti. Međutim, voditelj obrade dužan je, u skladu s člankom 32. GDPR-a, pobrinuti se za sigurnost prijenosa tako da, koliko je to moguće, zaštiti osobne podatke tijekom faze prijelaza u navedenu treću zemlju.

235. U tom pogledu, primjećujem da se člankom 44. GDPR-a prijenos u treću zemlju uvjetuje ispunjavanjem uvjeta iz odredbi poglavlja V. te uredbe ako se podaci mogu obraditi „nakon [tog] prijenosa”. Taj se izraz može shvatiti kao da znači, kao što je to vlada SAD-a tvrdila u svojem pisanom odgovoru na pitanja Suda, da te uvjete treba poštovati *kada podaci pristignu na odredište* odnosno da se ti uvjeti primjenjuju *nakon što je prijenos započet* (uključujući tijekom faze prijelaza).

236. Budući da se iz teksta članka 44. GDPR-a ne može izvesti jasan zaključak, na temelju teleološkog tumačenja slažem se s drugim od tih tumačenja te se, stoga, slažem s drugim od prethodno navedenih pristupa. Naime, kada bi se smatralo da zahtjev za kontinuiranom razinom zaštite predviđen u toj odredbi obuhvaća samo mjere nadzora provedene na državnom području treće zemlje odredišta, taj bi se zahtjev mogao zaobići kada bi ta treća zemlja takve mjere primjenjivala izvan svojeg državnog područja tijekom faze prijelaza podataka. Kako bi se to izbjeglo, procjena primjerenosti razine zaštite koju osigurava treća zemlja treba se odnositi na sve odredbe, osobito u području nacionalne sigurnosti, pravnog poretka te treće zemlje [105], među koji su odredbe o nadzoru koji se provodi na njezinu državnom području, kao i odredbe kojima se omogućuje nadzor podataka u prijelazu na to državno područje [106].

237. S obzirom na to, nitko ne osporava da se, kao što je to istaknuo EOZP, procjena primjerenosti razine zaštite odnosi, kao što proizlazi iz članka 45. stavka 1. GDPR-a, samo na odredbe pravnog poretka *treće zemlje odredišta podataka*. Činjenica da nije moguće, kao što to ističu Facebook Ireland te vlade SAD-a i Ujedinjene Kraljevine, jamčiti da druga treća država ne prikuplja potajno te podatke tijekom njihova prijelaza ne utječe na tu procjenu. Uostalom, ta se nemogućnost ne može isključiti čak ni nakon što podaci pristignu na državno područje treće države odredišta.

238. Osim toga, također je točno da Komisija, kada ocjenjuje primjerenost razine zaštite koju jamči treća zemlja, može po potrebi saznati da joj ta treća zemlja nije otkrila da postoje određeni tajni nadzorni programi. Međutim, iz toga ne proizlazi da, *kada je se obavijesti o takvim programima*, Komisija može to zanemariti u okviru svojeg ispitivanja primjerenosti. Usto, u slučaju da nakon donošenja odluke o primjerenosti sazna da postoje određeni tajni nadzorni programi, koje dotična treća zemlja provodi na svojem državnom području ili tijekom prijelaza preko tog područja, Komisija je dužna preispitati svoje utvrđenje u pogledu primjerenosti razine zaštite koju osigurava ta treća zemlja ako takvo saznanje izaziva dvojbe u tom pogledu [107].

3) Uzimanje u obzir činjeničnih utvrđenja koja su Komisija i sud koji je uputio zahtjev iznijeli u pogledu prava SAD-a

239. Iako je točno da Sud nije nadležan tumačiti pravo treće zemlje što bi bilo obvezno u pravnom poretku te zemlje, valjanost Odluke o sustavu zaštite privatnosti ovisi o osnovanosti ocjena koje je Komisija utvrdila u pogledu razine zaštite koja se pravom i praksama SAD-a osigurava u pogledu temeljnih prava osoba čiji su podaci preneseni u tu treću zemlju. Naime, Komisija je bila dužna obrazložiti svoje utvrđenje primjerenosti s obzirom na elemente koji se odnose, među ostalim, na sadržaj prava navedene treće zemlje te su navedeni u članku 45. stavku 2. GDPR-a [108].

105 Vidjeti u tom smislu presudu Schrems (t. 74. i 75.).

106 Vidjeti u tom smislu EOZP, EU-US Privacy Shield – Second Annual Joint Review, od 22. siječnja 2019. (str. 17., t. 86.).

107 Vidjeti članak 45. stavak 5. GDPR-a. Vidjeti i presudu Schrems (t. 76.).

108 Stoga je Odluka o privatnosti „sigurne luke” proglašena nevaljanom jer Komisija u toj odluci nije utvrdila da SAD stvarno osigurava primjerenu razinu zaštite zbog svojeg nacionalnog zakonodavstva ili svojih međunarodnih obveza (presuda Schrems, točka 97.). Konkretno, Komisija nije utvrdila da postoje državna pravila za ograničavanje mogućih miješanja u temeljna prava ispitanikâ (presuda Schrems, točka 88.) ni učinkovita pravna zaštita protiv takvih miješanja (presuda Schrems, točka 89.).

240. High Court (Visoki sud) u svojoj je presudi od 3. listopada 2017. iznio detaljna utvrđenja u kojima je opisao relevantne aspekte američkog prava nakon što je ocijenio dokaze koje su podnijele stranke spora [109]. To se izlaganje uvelike preklapa s Komisijinim utvrđenjima u Odluci o sustavu zaštite privatnosti koja se odnose na sadržaj pravila o prikupljanju i pristupu američkih obavještajnih tijela prenesenim podacima, kao i na pravne lijekove i mehanizme nadgledanja povezane s tim aktivnostima.

241. Sud koji je uputio zahtjev te nekoliko stranaka i zainteresiranih osoba koje su podnijele očitovanja Sudu prije dovode u pitanje pravne posljedice koje je Komisija izvela iz tih utvrđenja, odnosno zaključak da SAD osigurava primjerenu razinu zaštite temeljnih prava osoba čiji su podaci prenesi na temelju te odluke, nego Komisijin opis sadržaja američkog prava.

242. U tim ću okolnostima u biti procijeniti valjanost Odluke o sustavu zaštite privatnosti s obzirom na utvrđenja koja je sama Komisija iznijela u pogledu sadržaja američkog prava, pri čemu ću ispitati je li na temelju tih utvrđenja opravdano donošenje te odluke o primjerenosti.

243. U tom se pogledu ne slažem sa stajalištem koje zagovaraju DPC i M. Schrems prema kojem utvrđenja koja je High Court (Visoki sud) iznio u pogledu prava SAD-a obvezuju Sud u okviru ispitivanja valjanosti Odluke o sustavu zaštite privatnosti. SAD tvrdi da, s obzirom na to da strano pravo predstavlja činjenično pitanje na temelju irskog postupovnog prava, sud koji je uputio zahtjev jedini je nadležan utvrditi njegov sadržaj.

244. Točno je da se u ustaljenoj sudskoj praksi nacionalnom sudu priznaje isključiva nadležnost za utvrđivanje relevantnih činjeničnih pitanja, kao i za tumačenje prava države članice i njegovu primjenu na spor koji se pred njim vodi [110]. Ta sudska praksa odražava podjelu funkcija između Suda i suda koji je uputio zahtjev u okviru postupka uspostavljenog člankom 267. UFEU-a. Dok je Sud jedini nadležan za tumačenje prava Unije i odlučivanje o valjanosti sekundarnog prava, na nacionalnom je sudu, od kojeg se traži rješavanje konkretnog spora koji se pred njim vodi, da utvrdi njegov činjenični i regulatorni kontekst kako bi mu Sud mogao dati koristan odgovor.

245. Ne čini mi se da se svrha te isključive nadležnosti suda koji je uputio zahtjev može primijeniti na utvrđivanje prava treće zemlje kao elementa koji može utjecati na zaključak Suda o valjanosti akta sekundarnog prava [111]. Budući da je proglašenje nevaljanosti takvog akta obvezujuće *erga omnes* u pravnom poretku Unije [112], zaključak Suda ne može ovisiti o podrijetlu zahtjeva za prethodnu odluku. Međutim, kao što su to istaknuli Facebook Ireland i vlada SAD-a, taj zaključak ovisi o tome je li Sud bio obvezan utvrđenjima koja je sud koji je uputio zahtjev iznio u pogledu prava treće države, pri čemu se ta utvrđenja mogu mijenjati ovisno o nacionalnom sudu koji ih iznosi.

246. S obzirom na ta utvrđenja, smatram da, kada odgovor na prethodno pitanje o valjanosti akta Unije podrazumijeva ocjenu sadržaja prava treće države, Sud, iako ih može uzeti u obzir, nije obvezan utvrđenjima suda koji je uputio zahtjev o pravu te treće države. Sud po potrebi može od njih odstupiti ili ih dopuniti uzimajući u obzir, u okviru poštovanja načela kontradiktornosti, druge izvore u svrhu utvrđivanja elemenata potrebnih za procjenu valjanosti predmetnog akta [113].

109 Ta su utvrđenja sažeta u točkama 54. do 73. ovog mišljenja.

110 Vidjeti osobito presude od 4. svibnja 1999., Sürül (C-262/96, EU:C:1999:228, t. 95.); od 11. rujna 2008., Eckelkamp i dr. (C-11/07, EU:C:2008:489, t. 32.) i od 26. listopada 2016., Senior Home (C-195/15, EU:C:2016:804, t. 20.).

111 Vidjeti u tom pogledu presudu Supreme Courta (Vrhovni sud) od 31. svibnja 2019. (t. 6.18.).

112 Vidjeti presudu od 13. svibnja 1981., International Chemical Corporation (66/80, EU:C:1981:102, t. 12. i 13.).

113 Vidjeti u tom pogledu presudu od 22. ožujka 2012., GLS (C-338/10, EU:C:2012:158, t. 15., 33. i 34.), u kojoj je Sud, za potrebe ocjene valjanosti uredbe kojom se uvodi antidampinška pristojba, uzeo u obzir statistike Eurostata koje je Komisija predočila na zahtjev Suda. Vidjeti i presudu od 22. listopada 1991., Nölle (C-16/90, EU:C:1991:402, t. 17., 23. i 24.). Usto, u presudi Schrems (točka 90.), Sud je tijekom ispitivanja valjanosti Odluke o privatnosti „sigurne luke" uzeo u obzir određene Komisijine komunikacije.

4) Doseg standarda „bitne ekvivalentnosti”

247. Podsjećam da valjanost Odluke o sustavu zaštite privatnosti ovisi o tome je li pravnim poretkom SAD-a osigurana, u korist osoba čiji se podaci prenose iz Unije u tu treću zemlju, razina zaštite koja je „bitno ekvivalentna” razini zaštite zajamčenoj u državama članicama na temelju GDPR-a i Povelje, kao i, u područjima koja su isključena iz područja primjene prava Unije, na temelju njegovih obveza u okviru EKLJP-a.

248. Kao što je to Sud istaknuo u presudi Schrems [114], taj standard ne znači da razina zaštite treba biti „istovjetna” razini zaštite koja se zahtijeva u Uniji. Iako se pravna sredstva kojima se koristi treća zemlja za zaštitu prava ispitanikâ mogu razlikovati od pravnih sredstava propisanih GDPR-om s obzirom na Povelju, „ta se sredstva […] moraju u praksi pokazati djelotvornima za osiguranje bitno ekvivalentne zaštite poput one koja se jamči u okviru Unije”.

249. Prema mojem mišljenju, iz toga također proizlazi da pravo treće države može odražavati vlastiti sustav vrijednosti prema kojem se težina svakog od različitih postojećih interesa može razlikovati od sustava vrijednosti koji im je pridan u pravnom poretku Unije. Uostalom, zaštita osobnih podataka u Uniji odgovara osobito visokom standardu u usporedbi s razinom zaštite koja je na snazi u ostatku svijeta. Stoga bi kriterij „bitne ekvivalentnosti”, prema mojem mišljenju, trebalo primijeniti na način da se zadrži određena fleksibilnost pri uzimanju u obzir različitih pravnih i kulturnih tradicija. Međutim, taj kriterij podrazumijeva, ako ga se ne liši njegove biti, da određene minimalne zaštitne mjere i opći zahtjevi zaštite temeljnih prava koji proizlaze iz Povelje i EKLJP-a imaju svoj ekvivalent u pravnom poretku treće zemlje odredišta [115].

250. U tom pogledu, 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. Podložno načelu proporcionalnosti, ograničenja 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. Ti zahtjevi u biti odgovaraju zahtjevima iz članka 8. stavka 2. EKLJP-a [116].

251. U skladu s člankom 52. stavkom 3. Povelje, u onoj mjeri u kojoj prava zajamčena u njezinim člancima 7., 8. i 47. odgovaraju pravima zajamčenima u člancima 8. i 13. EKLJP-a, imaju jednako značenje i opseg primjene, s obzirom na to da im pravo Unije ipak može pružiti širu zaštitu. S tog gledišta, kao što će to jasno proizlaziti iz mojeg izlaganja, standardi iz članaka 7., 8. i 47. Povelje, kako ih tumači Sud, u nekoliko su aspekata stroži od standarda iz članka 8. EKLJP-a kako ih tumači Europski sud za ljudska prava (u daljnjem tekstu: ESPLJP).

252. Također napominjem da se u predmetima koji su u tijeku pred bilo kojim od tih sudova od navedenih sudova traži da ponovno razmotre određene aspekte svojih sudskih praksi. Stoga, s jedne strane, dvije su novije presude ESLJP-a u području nadzora elektroničkih komunikacija, odnosno presude Centrüm för Rättvisa protiv Švedske [117] i Big Brother Watch protiv Ujedinjene Kraljevine [118], bile upućene velikom vijeću na preispitivanje. S druge strane, tri nacionalna suda uputila su Sudu zahtjeve za prethodnu odluku kojima se otvara rasprava o tome treba li izmijeniti njegovu sudsku praksu koja proizlazi iz presude Tele2 Sverige [119].

114 Presuda Schrems (t. 73. i 74.)

115 Vidjeti u tom smislu Groupe 29, „Adequacy Referential (updated)”, 28. studenoga 2017., WP 254 (str. 3., 4. i 9.).

116 U članku 8. stavku 2. EKLJP-a ipak se ne upućuje na pojam „bit” prava na privatan život. Vidjeti u tom pogledu bilješku 161. ovog mišljenja.

117 ESLJP, 19. lipnja 2018. (CE:ECHR:2018:0619JUD003525208, u daljnjem tekstu: presuda Centrüm för Rättvisa)

118 ESLJP, 13. rujna 2018. (CE:ECHR:2018:0913JUD005817013, u daljnjem tekstu: Big Brother Watch)

119 Vidjeti predmete navedene u bilješci 98. ovog mišljenja, kao i predmet C-520/18, Ordre des barreaux francophones et germanophones i dr. (SL 2018., C 408, str. 39.).

253. Nakon što sam iznio ta pojašnjenja, sada ću ispitati valjanost Odluke o sustavu zaštite privatnosti s obzirom na članak 45. stavak 1. GDPR-a s obzirom na Povelju i EKLJP jer se njima jamče prava, s jedne strane, na poštovanje privatnog života i na zaštitu osobnih podataka (dio (b)) i, s druge strane, na djelotvornu sudsku zaštitu (dio (c)).

b) Valjanost Odluke o sustavu zaštite privatnosti s obzirom na prava na poštovanje privatnog života i zaštitu osobnih podataka

254. U okviru četvrtog pitanja sud koji je uputio zahtjev u biti dovodi u pitanje bitnu ekvivalentnost između razine zaštite koju osigurava SAD i razine zaštite koju ispitanici u Uniji ostvaruju na temelju svojih temeljnih prava na poštovanje privatnog života i zaštitu osobnih podataka.

1) Postojanje miješanja

255. U uvodnim izjavama 67. do 124. Odluke o sustavu zaštite privatnosti, Komisija navodi da američka javna tijela mogu pristupiti podacima prenesenima iz Unije te ih upotrebljavati u svrhu nacionalne sigurnosti u okviru programa koji se temelje, konkretno, na članku 702. FISA-e ili na EO-u br. 12333.

256. Provedba tih programa dovodi do zadiranja američkih obavještajnih službi koje se, ako ih provode tijela države članice, smatraju miješanjima u ostvarivanje prava na poštovanje privatnog života koje je zajamčeno člankom 7. Povelje i člankom 8. EKLJP-a. Tom se provedbom također ispitanike dovodi u opasnost od obrade njihovih osobnih podataka na način koji nije u skladu sa zahtjevima iz članka 8. Povelje [120].

257. Najprije pojašnjavam da prava na poštovanje privatnog života i na zaštitu osobnih podataka obuhvaćaju ne samo zaštitu sadržaja komunikacija, nego i podatke o prometu [121] i lokaciji (koje zajedno označava pojam „metapodaci"). Naime, Sud i ESLJP priznali su da metapodaci, jednako kao podaci o sadržaju, mogu otkriti vrlo precizne informacije o privatnom životu pojedinca [122].

258. Prema sudskoj praksi Suda, radi utvrđivanja postojanja miješanja u ostvarivanje prava zajamčenog u članku 7. Povelje, nevažno je imaju li ili ne dotične informacije osjetljiv karakter, odnosno jesu li ili ne zainteresirane osobe pretrpjele eventualne nepogodnosti zbog predmetne mjere nadzora [123].

259. S obzirom na navedeno, programi nadzora koji se temelje na članku 702. FISA-e dovode, najprije, do miješanja u ostvarivanje temeljnih prava osoba čije komunikacije odgovaraju čimbenicima za odabir koje je odabrala NSA te ih, zatim, toj agenciji prenose pružatelji usluga elektroničkih komunikacija [124]. Konkretnije, obveza koju pružatelji usluga imaju da *stave* podatke *na raspolaganje* NSA-i, s obzirom

120 Iako se obradom mogu istodobno povrijediti članci 7. i 8. Povelje, relevantan okvir analize za primjenu članka 8. strukturno se razlikuje od onog koji se povezuje s člankom 7. Pravo na zaštitu osobnih podataka podrazumijeva, u skladu s člankom 8. stavkom 2. Povelje, da se „[t]akvi podaci moraju […] obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom" i da „[s]vatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje". Povreda tog prava znači da su pri obradi osobnih podataka povrijeđeni ti zahtjevi. To je slučaj, među ostalim, kada se obrada ne temelji ni na suglasnosti ispitanika, *ni na bilo kakvom drugom legitimnom temelju koji je predviđen zakonom*. U takvoj situaciji, iako se pitanja o postojanju miješanja i njegova opravdanja konceptualno razlikuju u okviru članka 7., ona se preklapaju u pogledu članka 8. Povelje.

121 U članku 2. drugom stavku točki (b) Direktive 2002/58 pojam „podaci o prometu" definiran je kao „svi podaci koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje".

122 Vidjeti presudu od 8. travnja 2014., Digital Rights Ireland i dr. (C-293/12 i C-594/12, EU:C:2014:238, u daljnjem tekstu: presuda Digital Rights Ireland, t. 27.) i presudu Tele2 Sverige (t. 99.). Vidjeti i ESLJP, 2. kolovoza 1984., Malone protiv Ujedinjene Kraljevine (CE:ECHR:1984:0802JUD000869179, t. 84.) i 8. veljače 2018., Ben Faiza protiv Francuske CE:ECHR:2018:0208JUD003144612, t. 66.) (

123 Vidjeti presudu Digital Rights Ireland (t. 33.); mišljenje 1/15 (t. 124.), kao i presudu Ministerio Fiscal (t. 51.).

124 Vidjeti uvodne izjave 78. do 81., kao i točku II. Priloga VI. Odluci o sustavu zaštite privatnosti.

na to da se njome odstupa od načela povjerljivosti komunikacija [125], sama po sebi uključuje miješanje čak i ako obavještajna tijela te podatke kasnije nisu pregledala ni upotrebljavala [126]. *Zadržavanje* i stvaran *pristup* tih tijela metapodacima i sadržaju komunikacija koje su im stavljene na raspolaganje, kao i *upotreba* tih podataka također čine dodatna miješanja [127].

260. Štoviše, u skladu s utvrđenjima suda koji je uputio zahtjev [128] i drugim izvorima kao što je izvješće PCLOB-a o programima provedenima na temelju članka 702. FISA-e o kojem je američka vlada obavijestila Sud [129], NSA je, u okviru programa Upstream, već imala *pristup u svrhu filtriranja* opširnom korpusu („paketi") podataka koji su dio protoka komunikacija koji prelaze preko „kostura" telekomunikacija i obuhvaćaju komunikacije koje ne sadržavaju čimbenike za odabir koje je utvrdila NSA. NSA je te korpuse mogla ispitati samo kako bi brzo i automatizirano utvrdila sadržavaju li te čimbenike za odabir. Jedino se tako filtrirane komunikacije tada čuvaju u NSA-inim bazama podataka. Taj pristup podacima radi njihova filtriranja, prema mojem mišljenju, također predstavlja miješanje u ostvarivanje prava na poštovanje privatnog života ispitanikâ, neovisno o kasnijoj upotrebi zadržanih podataka [130].

261. Osim toga, stavljanje na raspolaganje i filtriranje predmetnih podataka [131], pristup obavještajnih tijela tim podacima, kao i eventualna pohrana, analiza i uporaba navedenih podataka obuhvaćeni su pojmom „obrada" u smislu članka 4. točke 2. GDPR-a i članka 8. stavka 2. Povelje. Te obrade stoga trebaju ispunjavati zahtjeve predviđene u toj odredbi [132].

262. Nadgledanje na temelju EO-a br. 12333 moglo bi pak podrazumijevati izravan pristup obavještajnih tijela podacima u prijelazu, koji uključuje miješanje u ostvarivanje prava zajamčenog člankom 8. EKLJP-a. Uz to miješanje postoji i miješanje koje čini eventualna kasnija uporaba tih podataka.

2) Uvjet da su miješanja „utvrđena zakonom"

263. Na temelju sudske prakse Suda [133] i ESLJP-a [134], zahtjev prema kojem svako miješanje u ostvarivanje temeljnih prava treba biti „utvrđeno zakonom", u smislu članka 52. stavka 1. Povelje i članka 8. stavka 2. EKLJP-a, ne podrazumijeva samo da mjera kojom se predviđa miješanje mora imati pravnu osnovu u nacionalnom pravu, nego i da ta pravna osnova treba imati određena svojstva pristupačnosti i utvrdivosti kako ne bi bila proizvoljna.

264. U tom pogledu, stranke i zainteresirane osobe koje su podnijele očitovanja Sudu u biti se ne slažu u pogledu toga ispunjavaju li članak 702. FISA-e i EO br. 12333 uvjet utvrdivosti zakonom.

125 Vidjeti u tom pogledu presudu Digital Rights Ireland (t. 32.).

126 Vidjeti u tom smislu mišljenje 1/15 (točke 124. i 125.), iz kojeg proizlazi da dostavljanje podataka trećoj osobi predstavlja miješanje u ostvarivanje temeljnih prava ispitanika neovisno o njihovom kasnijem korištenju.

127 Vidjeti u tom smislu presudu Digital Rights Ireland (t. 35.); presuda Schrems (t. 87.) i mišljenje 1/15 (t. 123. do 126.).

128 Vidjeti točku 60. ovog mišljenja.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2. srpnja 2014. (u daljnjem tekstu: izvješće PCLOB-a, str. 84. i 111.). Vidjeti također radnu skupinu 29, EU-U. S. Privacy Shield – First Annual Joint Review, 28. studenoga 2017., WP 255 (točka B.1.1., str. 15.).

130 Vidjeti bilješku 126. ovog mišljenja.

131 Vidjeti u tom pogledu točku 222. ovog mišljenja.

132 Vidjeti mišljenje 1/15 (t. 123. i navedena sudska praksa).

133 Vidjeti osobito mišljenje 1/15 (t. 146.).

134 Vidjeti osobito ESLJP, presuda od 2. kolovoza 1984., Malone protiv Ujedinjene Kraljevine (CE:ECHR:1984:0802JUD000869179, t. 66.), odluka od 29. lipnja 2006., Weber i Saravia protiv Njemačke (CE:ECHR:2006:0629DEC005493400; u daljnjem tekstu: Odluka Weber i Saravia; t. 84. i navedena sudska praksa) kao i presuda od 4. prosinca 2015., Zakharov protiv Rusije (CE:ECHR:2015:1204JUD004714306, u daljnjem tekstu: presuda Zakharov, t. 228.).

265. Taj uvjet, kako ga tumače Sud [135] i ESLJP [136], zahtijeva da se propisom koji uključuje miješanje u ostvarivanje prava na poštovanje privatnog života uspostavljaju jasna i precizna pravila kojima se uređuju doseg i primjena predmetne mjere i propisuju minimalni zahtjevi, tako da se ispitanicima pruže dovoljna jamstva kako bi se njihovi podaci zaštitili od rizika zlouporabe, kao i od svakog nezakonitog pristupa ili uporabe tih podataka. U takvim se pravilima mora, konkretno, navoditi u kojim okolnostima i pod kojim uvjetima tijela javne vlasti mogu zadržavati osobne podatke, pristupiti im i upotrebljavati ih [137]. Osim toga, samom se pravnom osnovom na temelju koje se omogućuje miješanje mora utvrditi doseg ograničenja ostvarivanja prava na poštovanje privatnog života [138].

266. Kao i M. Schrems i EPIC, dvojim o tome da su EO br. 12333, kao i PPD 28 u kojem se navode zaštitne mjere primjenjive na sve obavještajne aktivnosti koje se odnose na elektronički prijenos [139], dovoljno utvrdivi kako bi imali „svojstvo zakona”.

267. U tim se instrumentima izričito navodi da se njima ne dodjeljuju pravno ostvariva prava ispitanicima [140]. Stoga se potonje osobe ne mogu pred sudovima pozvati na zaštitne mjere predviđene PPD-om 28 [141]. Uostalom, Komisija je u Odluci o sustavu zaštite privatnosti smatrala da zaštitne mjere iznesene u tom predsjedničkom ukazu, iako obvezuju obavještajne službe [142], „nisu oblikovan[e] u takvom pravnom obliku” [143]. EO br. 12333 i PPD 28 više nalikuju unutarnjim upravnim uputama koje predsjednik SAD-a može opozvati ili izmijeniti. Međutim, ESLJP je već presudio da unutarnje upravne smjernice nemaju svojstvo „zakona” [144].

268. Što se tiče članka 702. FISA-e, M. Schrems doveo je u pitanje utvrdivost te odredbe jer njome nije definirano utvrđivanje kriterija za odabir koji se upotrebljavaju za filtriranje podataka na temelju dovoljnih jamstava od rizika zlouporabe. Budući da se ta problematika također odnosi na nužno potrebna miješanja predviđena člankom 702. FISA-e, ispitat ću je u nastavku svojeg izlaganja [145].

135 Vidjeti osobito presudu Digital Rights Ireland (t. 54. i 65.); presuda Schrems (t. 91.); presuda Tele2 Sverige (t. 109.) i mišljenje 1/15 (t. 141.).

136 Vidjeti osobito odluku Weber i Saravia (t. 94. i 95.); presuda Zakharov (t. 236.) i ESLJP, 12. siječnja 2016., Szabó i Vissy protiv Mađarske (CE:ECHR:2016:0112JUD003713814, u daljnjem tekstu: presuda Szabó i Vissy, t. 59.).

137 Vidjeti presudu Tele2 Sverige (t. 117.) i mišljenje 1/15 (t. 190.). Vidjeti i osobito ESLJP, 2. kolovoza 1984., Malone protiv Ujedinjene Kraljevine (CE:ECHR:1984:0802JUD000869179, t. 67.); presuda Zakharov (t. 229.) i presuda Szabó i Vissy (t. 62.). ESLJP je u toj sudskoj praksi pojasnio da zahtjev utvrdivosti nema jednak doseg u području presretanja komunikacija kao u drugim područjima. U kontekstu tajnih mjera nadzora, „zahtjev utvrdivosti ne može značiti da nekomu valja omogućiti da utvrdi jesu li njegove komunikacije i kada u opasnosti od toga da ih presretnu tijela kako bi mogao prema tome uskladiti svoje ponašanje”.

138 Mišljenje 1/15, (t. 139.). Vidjeti u tom smislu također ESLJP, 25. ožujka 1983., Silver i dr. protiv Ujedinjene Kraljevine (CE:ECHR:1983:0325JUD000594772, t. 88. i 89.).

139 Uvodne izjave 69. do 77., kao i točka I. Priloga VI. Odluci o sustavu zaštite privatnosti sadržavaju prikaz PPD-a 28. U njima se pojašnjava da se taj predsjednički ukaz primjenjuje jednako na obavještajne aktivnosti koje se temelje na članku 702. FISA-e, kao i na obavještajne aktivnosti koje se obavljaju izvan državnog područja SAD-a.

140 U točki 3.7. podtočki (c) EO-a br. 12333 navodi se: „[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person”. Člankom 6. točkom (d) PPD-a 28 također se predviđa: „This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person”.

141 Vidjeti u tom smislu EOZP, EU-U. S. Privacy Shield – Second Annual Joint Review, od 22. siječnja 2019. (t. 99.).

142 Vidjeti uvodne izjave 69. i 77. Odluke o sustavu zaštite privatnosti.

143 Uvodna izjava 76. Odluke o sustavu zaštite privatnosti.

144 Vidjeti ESLJP, 25. ožujka 1983., Silver i dr. protiv Ujedinjene Kraljevine (CE:ECHR:1983:0325JUD000594772, t. 26. i 86.).

145 Vidjeti točke 295. do 301. ovog mišljenja. U presudi Tele2 Sverige (t. 116. i 117.) i mišljenju 1/15 (t. 140. i 141.), uvjet utvrdivosti zakonom prikazan je kao usko povezan s uvjetom nužnosti i proporcionalnosti miješanja. Jednako tako, prema ustaljenoj sudskoj praksi ESLJP-a, postojanje djelotvornih zaštitnih mjera od rizika zlouporabe dio je uvjeta o „utvrdivosti” miješanja, kao i uvjeta da je to miješanje „nužn[o] u demokratskom društvu”, pri čemu se poštovanje tih dvaju uvjeta zajedno ispituje. Vidjeti osobito ESLJP, 18. svibnja 2010., Kennedy protiv Ujedinjene Kraljevine (CE:ECHR:2010:0518JUD002683905, t. 155.); presuda Zakharov (t. 236.); presuda Centrüm för Rättvisa (t. 107.) i presuda Big Brother Watch (t. 322.).

269. Treće prethodno pitanje preklapa se s tematikom poštovanja uvjeta o „svojstvu zakona". Tim pitanjem sud koji je uputio zahtjev u biti želi znati treba li primjerenost razine zaštite koja se osigurava u trećoj zemlji ispitati samo s obzirom na pravno obvezujuća pravila koja su na snazi u toj trećoj zemlji i prakse čiji je cilj osigurati njihovo poštovanje ili pak i s obzirom na razne neobvezujuće instrumente i izvansudske mehanizme nadzora koji se ondje primjenjuju.

270. U tom pogledu, u članku 45. stavku 2. točki (a) GDPR-a navodi se netaksativan popis okolnosti koje Komisija treba uzeti u obzir u svrhu procjene primjerenosti razine zaštite koju nudi treća zemlja. Te okolnosti uključuju primjenjivo zakonodavstvo i način na koji se ono provodi. U toj se odredbi također navodi utjecaj drugih vrsta pravnih pravila, kao što su strukovna pravila i sigurnosne mjere. K tomu, tom se odredbom zahtijeva uzimanje u obzir „djelotvornih i provedivih prava" i „učinkovite upravne i sudske zaštite ispitanika čiji se osobni podaci prenose"[146].

271. Navedena odredba tumačena u cjelini i s obzirom na nerestriktivnu narav popisa koji sadržava, prema mojem mišljenju, podrazumijeva da se prakse ili instrumenti koji se ne temelje na pristupačnoj i utvrdivoj pravnoj osnovi mogu uzeti u obzir u okviru procjene ukupne razine zaštite koju osigurava dotična treća zemlja kako bi se potkrijepile zaštitne mjere koje se temelje na pravnom temelju koji ima ta svojstva. Nasuprot tomu, kao što su to u biti tvrdili DPC, M. Schrems, austrijska vlada i EOZP, slični instrumenti ili prakse ne mogu zamijeniti takve zaštitne mjere niti, stoga, sami osigurati potrebnu razinu zaštite.

3) Nepostojanje povrede biti temeljnih prava

272. Zahtjev iz članka 52. stavka 1. Povelje, prema kojem svako ograničenje prava i sloboda zajamčenih Poveljom mora poštovati bit tih prava, podrazumijeva da se, kad se miješanjem povrijedi ta bit, ono ne može opravdati nikakvim legitimnim ciljem. Tada se miješanje smatra protivnim Povelji a da nije potrebno ispitati je li primjereno i nužno za ostvarenje postavljenog cilja.

273. U tom pogledu, Sud je presudio da se nacionalnim propisom na temelju kojeg se odobrava opći pristup tijela javne vlasti *sadržaju* elektroničkih komunikacija povređuje sama bit prava na poštovanje privatnog života koje je zajamčeno u članku 7. Povelje[147]. Suprotno tomu, Sud je istaknuo rizike povezane s pristupom i analizom *podataka o prometu i lokaciji*[148] te je smatrao da bit tog prava nije narušena kada se nacionalnim propisom odobrava opći pristup državnih tijela tim podacima[149].

274. Smatram da se članak 702. FISA-a ne može tumačiti na način da se njime američka obavještajna tijela ovlašćuju za opći pristup sadržaju elektroničkih komunikacija.

275. Naime, s jedne strane, pristup obavještajnih tijela podacima, na temelju članka 702. FISA-e, *u svrhu njihove eventualne analize i uporabe* ograničen je na podatke koji odgovaraju kriterijima za odabir povezanim s pojedinačnim ciljevima.

146 Vidjeti i uvodnu izjavu 104. GDPR-a.

147 Vidjeti presudu Schrems (t. 94.). Vidjeti i presude Digital Rights Ireland (t. 39.) i Tele2 Sverige (t. 101.). S obzirom na usku vezu između prava na privatan život i zaštitu osobnih podataka, čini mi se da bi se nacionalnom mjerom na temelju koje se tijelima javne vlasti daje opći pristup sadržaju komunikacija povrijedila bit prava zajamčenog člankom 8. Povelje.

148 Vidjeti točku 257. ovog mišljenja. U presudi Tele2 (točka 99.), Sud je naglasio da metapodaci osobito omogućuju utvrđivanje profila ispitanika. U svojem mišljenju 4/2014 o nadzoru elektroničkih komunikacija u svrhu obavještavanja i nacionalne sigurnosti, od 10. travnja 2014., WP 215 (str. 5.), radna skupina 29 napomenula je da je metapodatke, zbog njihove strukturiranosti, lakše ispitati i analizirati nego podatke o sadržaju.

149 Vidjeti presudu Tele2 Sverige (t. 99.). Neki su se komentatori pitali o osnovanosti razlikovanja između općeg pristupa sadržaju komunikacija i općeg pristupa metopodacima s obzirom na razvoj tehnologija i načine komunikacije. Vidjeti Falot, N. i Hijmans, H., „Tele2: de afweging tussen privacy en veiligheid nader omlijnd", *Nederlands Tijdschrift voor Europees Recht*, br. 3, 2017. (str. 48.), kao i Ojanen, T., „Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter" (komentar na presudu Schrems), *European Constitutional Law Review*, 2016. (str. 5.).

276. S druge strane, točno je da bi se program Upstream mogao primijeniti na opći pristup sadržaju elektroničkih komunikacija u *svrhu njihova automatiziranog filtriranja* u slučaju da se čimbenici za odabir ne primjenjuju samo na polja „od" i „do", nego i na sav sadržaj protoka komunikacija (pretraživanje „u pogledu" čimbenika za odabir)[150]. Međutim, kao što to tvrdi Komisija i suprotno onomu što navode M. Schrems i EPIC, privremeni pristup obavještajnih tijela cijelom sadržaju elektroničkih komunikacija samo u svrhu njihova filtriranja primjenom kriterija za odabir ne može se izjednačiti s općim pristupom tom sadržaju[151]. Prema mojem mišljenju, ozbiljnost miješanja koje proizlazi iz tog vremenski ograničenog pristupa u svrhu automatiziranog filtriranja nije jednaka ozbiljnosti miješanja koje proizlazi iz općeg pristupa tijela javne vlasti tom sadržaju u svrhu njegove analize i eventualne uporabe[152]. Privremeni pristup u svrhu filtriranja ne omogućuje tim tijelima da zadrže metapodatke ili sadržaj komunikacija koje ne odgovaraju kriterijima za odabir niti, konkretno, kao što je to napomenula američka vlada, da utvrde profile o pojedincima na koje se ne odnose ti kriteriji.

277. S obzirom na navedeno, pitanje ograničavaju li se stvarno ciljanjem na temelju čimbenika za odabir u okviru programa koji se temelje na članku 702. FISA-e ovlasti obavještajnih tijela ovisi o definiciji utvrđivanja čimbenika za odabir[153]. M. Schrems u tom pogledu tvrdi da se, zato što ne postoji dovoljan nadzor u tu svrhu, američkim pravom ne predviđa zaštitna mjera od općeg pristupa sadržaju komunikacija već u fazi filtriranja, čime se povređuje sama bit prava na poštovanje privatnog života ispitanika.

278. Kao što ću to u nastavku detaljnije iznijeti[154], sklon sam složiti se s tim dvojbama o dostatnosti okvira utvrđivanja čimbenika za odabir kako bi se ispunili kriteriji utvrdivosti i proporcionalnosti miješanja. Međutim, postojanju tog okvira, čak i nesavršenog, protivi se zaključak prema kojem se člankom 702. FISA-e odobrava opći pristup tijela javne vlasti sadržaju elektroničkih komunikacija i, stoga, odgovara povredi same biti prava zajamčenog člankom 7. Povelje.

279. Također ističem da je u mišljenju 1/15 Sud smatrao da je bit temeljnog prava na zaštitu osobnih podataka, koje je zajamčeno u članku 8. Povelje, očuvana kada su svrhe obrade ograničene i kada se na obradu primjenjuju pravila namijenjena osiguravanju, među ostalim, sigurnosti, povjerljivosti i integriteta podataka te njihove zaštite od nezakonitog pristupa i obrade[155].

150 Vidjeti bilješku 87. Odluke o sustavu zaštite privatnosti. Međutim, u skladu s EPIC-ovim očitovanjima i pisanim odgovorom vlade SAD-a na pitanja koja je postavio Sud, FISC je 2017. tražio obustavu pretraživanja „u pogledu" čimbenika za odabir zbog nepravilnosti kojima su bila zahvaćena pretraživanja te vrste. Kongres je ipak predvidio, u aktu o ponovnom odobrenju FISA-e donesenom 2018., mogućnost ponovnog uvođenja te vrste pretraživanja uz suglasnost FISC-a i Kongresa. Vidjeti također EOZP, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. siječnja 2019. (str. 27., t. 55.).

151 S tog gledišta, sud koji je uputio zahtjev razlikovao je, u točkama 188. i 189. svoje presude od 3. listopada 2017., skupno pretraživanje od skupnog stjecanja, prikupljanja ili zadržavanja. Taj sud u biti smatra da, ako program Upstream uključuje skupno pretraživanje u okviru svih protoka podataka koji prelaze preko „kostura" telekomunikacija, stjecanje, prikupljanje i zadržavanje ciljani su na način da su njihov predmet samo podaci koji sadržavaju predmetne čimbenike za odabir.

152 Vidjeti u tom smislu presudu Supreme Courta (Vrhovni sud) od 31. svibnja 2019. (t. 11.2. i 11.3.). Taj je sud u toj presudi istaknuo: „[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term ‚processing' covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis."

153 Vidjeti mišljenje 1/15 (t. 122.). Vidjeti i izvješće Europske komisije za demokraciju putem prava (Venecijanska komisija) o demokratskom nadzoru agencija za prikupljanje obavještajnih informacija elektroničkim izviđanjem od 15. prosinca 2015., studija br. 719/2013 (CDL-AD(2015)011, str. 11.): „U praksi, da bi se odgovorilo na pitanje ograničavaju li se primjereno tim postupkom nepotrebna zadiranja u bezazlene osobne komunikacije treba utvrditi je li čimbenik za odabir dovoljno relevantan i konkretan te je li zadovoljavajuće kvalitetan algoritam programa koji se upotrebljava za prepoznavanje relevantnih podataka u okviru odabranih parametara […]".

154 Vidjeti točke 297. do 301. ovog mišljenja.

155 Mišljenje 1/15, (t. 150.)

280. U Odluci o sustavu zaštite privatnosti Komisija je utvrdila da se člankom 702. FISA-e i PPD-om 28 ograničavaju svrhe u koje se podaci mogu prikupljati u okviru programa koji se provode na temelju članka 702. FISA-e [156]. Komisija je u toj odluci također istaknula da se PPD-om 28 predviđaju pravila o pristupu podacima te o njihovoj pohrani i širenju kako bi ih se zaštitilo i osiguralo od neovlaštenih pristupa [157]. Kao što će se pokazati u nastavku mojeg izlaganja [158], dvojim, konkretno, u pogledu toga jesu li svrhe predmetnih obrada dovoljno jasno i precizno definirane kako bi se osigurala razina zaštite koja je bitno ekvivalentna razini zaštite koja se pruža u pravnom poretku Unije. Međutim, smatram da ti eventualni nedostaci nisu dovoljni da bi se potkrijepilo utvrđenje da bi slični programi, da su provedeni u Uniji, povrijedili bit prava na zaštitu osobnih podataka.

281. Osim toga, podsjećam da primjerenost razine zaštite koja se osigurava u okviru nadzornih aktivnosti na temelju EO-a br. 12333 treba procijeniti s obzirom na odredbe EKLJP-a. U tom pogledu, iz Odluke o sustavu zaštite privatnosti proizlazi da su jedina ograničenja koja se primjenjuju na provedbu mjera koje se temelje na EO-u br. 12333 za prikupljanje podataka o osobama koje nisu američki državljani predviđena PPD-om 28 [159]. Tim se predsjedničkim ukazom određuje da uporaba stranih obavještajnih informacija mora biti „što usmjerenij[a]". Međutim, u tom se predsjedničkom ukazu izričito navodi mogućnost skupnog prikupljanja podataka, izvan američkog državnog područja, u svrhu postizanja određenih konkretnih ciljeva nacionalne sigurnosti [160]. Prema mišljenju M. Schremsa, odredbama PPD-a 28, iz kojeg uostalom ne proizlaze prava pojedinaca, ispitanici se ne štite od rizika općeg pristupa sadržaju njihovih elektroničkih komunikacija.

282. U tom ću pogledu samo napomenuti da ESLJP u svojoj sudskoj praksi o članku 8. EKLJP-a nije upotrijebio pojam povrede biti ili same srži prava na poštovanje privatnog života [161]. Potonji sud dosad nije smatrao da sustavi kojima se omogućuje presretanje elektroničkih komunikacija, čak i masovno, *sami po sebi prekoračuju marginu prosudbe država članica*. ESLJP smatra da su takvi sustavi u skladu s člankom 8. stavkom 2. EKLJP-a ako se na njih primjenjuje određeni broj minimalnih zaštitnih mjera [162]. U tim okolnostima, ne čini mi se primjerenim zaključiti da sustav nadzora kao što je onaj predviđen EO-om br. 12333 prekoračuje marginu prosudbe država članica a da se pritom ne provede nikakvo ispitivanje eventualnih zaštitnih mjera koje se primjenjuju na taj sustav.

156 Vidjeti uvodne izjave 70., 103. i 109. Odluke o sustavu zaštite privatnosti.

157 Vidjeti uvodne izjave 83. do 87., kao i točku I. podtočku (c) Priloga VI. Odluci o sustavu zaštite privatnosti. Napominjem da se, u skladu s izvješćem PCLOB-a (str. 51. do 66.), NSA-ini postupci „smanjenja količine podataka" na temelju članka 702. FISA-e odnose, u većini aspekata, samo na američke državljane. Cilj PPD-a 28 bio je proširiti zaštitne mjere koje se primjenjuju na osobe koje nisu američki državljani. Vidjeti PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, disponible à l'adresse https://www.pclob.gov/reports/report-PPD28/(str. 2.). S obzirom na navedeno, smatram da pohrana i uporaba podataka, u svrhu nacionalne sigurnosti, nakon što ih steknu tijela javne vlasti, nisu obuhvaćene područjem primjene prava Unije (vidjeti točku 226. ovog mišljenja). Primjerenost razine zaštite koja se osigurava u okviru tih aktivnosti stoga treba ocijeniti samo s obzirom na članak 8. EKLJP-a.

158 Vidjeti točke 283. do 289. ovog mišljenja.

159 Konkretno, Komisija je u uvodnoj izjavi 127. Odluke o sustavu zaštite privatnosti utvrdila da se osobe koje nisu državljani SAD-a ne mogu pozvati na Četvrti amandman Ustava SAD-a.

160 Vidjeti uvodne izjave 73. i 74., kao i točku I. podtočku (b) Priloga VI. Odluci o sustavu zaštite privatnosti. Ti ciljevi uključuju suzbijanje špijunaže i drugih prijetnji i aktivnosti koje protiv SAD-a i njegovih interesa provode strane vlasti, terorističkih prijetnji, prijetnji koje proizlaze iz razvoja, posjedovanja, širenja ili uporabe oružja za masovno uništenje, prijetnji povezanih s kibersigurnošću, prijetnji oružanim snagama SAD-a ili njezinim saveznicima i transnacionalnih kriminalnih prijetnji. Na temelju bilješke na dnu stranice 5. PPD-a 28, ograničenje ciljeva koje opravdava uporabu skupno prikupljenih podataka primjenjuje se samo ako je takvo prikupljanje privremeno i namijenjeno olakšanju ciljanog prikupljanja.

161 Iako se u odredbama EKLJP-a ne navodi „bit" temeljnih prava, u sudskoj praksi ESLJP-a o nekim od tih odredbi spominje se istovjetan pojam „sama srž" temeljnog prava. Vidjeti u pogledu same srži prava na pošteno suđenje zajamčenog člankom 6. EKLJP-a, osobito, ESLJP, 25. svibnja 1985., Ashingdane protiv Ujedinjene Kraljevine (CE:ECHR:1985:0528JUD000822578, t. 57. i 59.); od 21. prosinca 2000., Heaney and McGuinness protiv Irske (CE:ECHR:2000:1221JUD003472097, t. 55. i 58.) i od 23. lipnja 2016., Baka protiv Mađarske (CE:ECHR:2016:0623JUD002026112, t. 121.). Što se tiče same srži prava na brak zajamčenog u članku 12. EKLJP-a vidjeti ESLJP, 11. srpnja 2002., Christine Goodwin protiv Ujedinjene Kraljevine (CE:ECHR:2002:0711JUD002895795, t. 99. i 101.). U pogledu same srži prava na obrazovanje zajamčenog člankom 2. Protokola br. 1 uz EKLJP, vidjeti ESLJP, 23. srpnja 1968., predmet „o određenim aspektima jezičnog sustava u okviru obrazovanja u Belgiji" (CE:ECHR:1968:0723JUD000147462, t. 5.).

162 Vidjeti konkretno presude Centrüm för Rättvisa (t. 112. do 114. i navedena sudska praksa) i Big Brother Watch (t. 337.).

4) Postizanje legitimnog cilja

283. U skladu s člankom 52. stavkom 1. Povelje, svako ograničenje pri ostvarivanju prava priznatih Poveljom mora zaista odgovarati cilju od općeg interesa koji priznaje Unija. Člankom 8. stavkom 2. Povelje također se određuje da se svaka obrada osobnih podataka koja se ne temelji na suglasnosti osobe o kojoj je riječ mora temeljiti na „legitimnoj osnovi utvrđenoj zakonom". Članak 8. stavak 2. EKLJP-a propisuje ciljeve koji mogu opravdati zadiranje u izvršavanje prava na poštovanje privatnog života.

284. Na temelju Odluke o sustavu zaštite privatnosti, pridržavanje načela koja se u njoj navode može se ograničiti kako bi se ispunile obveze u pogledu nacionalne sigurnosti, javnog interesa i kaznenog progona[163] U uvodnim izjavama 67. do 124. te odluke konkretnije se ispituju ograničenja koja proizlaze iz pristupa podacima i njihove uporabe od strane američkih tijela javne vlasti u svrhu nacionalne sigurnosti.

285. Nesporno je da je zaštita nacionalne sigurnosti legitiman cilj kojim se mogu opravdati odstupanja od zahtjevâ iz GDPR-a[164], kao i od temeljnih prava iz članaka 7. i 8. Povelje[165] kao i članak 8. stavak 2. EKLJP-a. Međutim, M. Schrems, austrijska vlada i EPIC napomenuli su da se ciljevima postavljenim u okviru programa nadzora koji se temelje na članku 702. FISA-e i EO-u br. 12333 nadilazi sama nacionalna sigurnost. Naime, ti instrumenti imaju za cilj dobivanje „strane obavještajne informacije", pri čemu taj pojam obuhvaća razne vrste informacije koje uključuju informacije o nacionalnoj sigurnosti koje nisu nužno ograničene samo na to područje[166]. Tako su pojmom „strane obavještajne informacije", u smislu članka 702. FISA-e, obuhvaćeni podaci o vođenju vanjskih poslova[167]. U EO-u br. 12333 taj se pojam pak definira na način da on uključuje informacije o mogućnostima, namjerama ili aktivnostima stranih vlada, stranih organizacija ili stranih osoba[168]. M. Schrems dovodi u pitanje legitimnost tako predviđenog cilja jer se njime prekoračuje nacionalna sigurnost.

286. Prema mojem mišljenju, opseg nacionalne sigurnosti može, u određenoj mjeri, uključivati zaštitu interesa u pogledu vođenja vanjskih poslova[169]. Osim toga, nije nezamislivo da određene svrhe koje nisu zaštita nacionalne sigurnosti koju obuhvaća pojam „vanjske obavještajne informacije", kako je definiran u članku 702. FISA-e i EO-u br. 12333, odgovaraju ciljevima u općem interesu kojima se može opravdati miješanje u temeljna prava na poštovanje privatnog života i na zaštitu osobnih podataka. Ti ciljevi u svakom slučaju imaju manju težinu od zaštite nacionalne sigurnosti u okviru odvagivanja temeljnih prava ispitanika i cilja postavljenog miješanjem[170].

163 Vidjeti točku 197. ovog mišljenja.

164 Vidjeti članak 23. stavak 1. točku (a) GDPR-a.

165 Vidjeti presudu Schrems (t. 88.). Sud je smatrao da je sličan pojam „javna sigurnost", u smislu odredbi UFEU-a kojima se odobravaju odstupanja od temeljnih sloboda koje se njime jamče, autonoman pojam prava Unije koji obuhvaća unutarnju i vanjsku sigurnost država članica (vidjeti osobito presude od 26. listopada 1999., Sirdar (C-273/97, EU:C:1999:523, t. 17.), kao i od 13. rujna 2016,, CS (C-304/14, EU:C:2016:674, t. 39. i navedena sudska praksa)). Dok na unutarnju sigurnost, među ostalim, može utjecati izravna prijetnja za mir i fizičku sigurnost stanovništva dotične države članice, vanjsku sigurnost, među ostalim, može ugroziti opasnost od teških poremećaja u vanjskim odnosima ili miroljubivom suživotu naroda. Iako ne može jednostrano utvrditi sadržaj tih pojmova, svaka država članica ima marginu prosudbe pri određivanju svojih ključnih interesa u pogledu sigurnosti. Vidjeti osobito presudu od 2. svibnja 2018., K. i H. F. (Pravo boravka i tvrdnje o ratnim zločinima) (C-331/16 i C-366/16, EU:C:2018:296, t. 40. do 42. i navedena sudska praksa). Prema mojem mišljenju, ta se razmatranja mogu primijeniti na tumačenje pojma „nacionalna sigurnost" kao interes čija se zaštita može opravdati ograničenjima odredbi GDPR-a i prava zajamčenih člancima 7. i 8. Povelje.

166 Vidjeti u tom pogledu uvodnu izjavu 89. i bilješku 97. Odluke o sustavu zaštite privatnosti.

167 Vidjeti točku 55. ovog mišljenja.

168 Vidjeti točku 61. ovog mišljenja.

169 U presudi Centrüm för Rättvisa (t. 111.), ESLJP je presudio da nadzorne aktivnosti kojima se nastoji pružiti podrška vanjskoj politici, obrambenoj politici i sigurnosnoj politici Švedske, kao i prepoznati vanjske prijetnje organizirane u Švedskoj imaju legitimne ciljeve koji se odnose na nacionalnu sigurnost.

170 Vidjeti u tom pogledu presudu Tele2 Sverige (t. 115.) i presudu Ministerio Fiscal (t. 55.). Sud je u potonjoj presudi istaknuo vezu između stupnja ozbiljnosti miješanja i stupnja važnosti interesa na koji se poziva kako bi se to miješanje opravdalo.

287. Međutim, u skladu s člankom 52. stavkom 1. Povelje, još je potrebno da se nacionalna sigurnost ili drugi legitiman cilj stvarno nastoje postići mjerama kojima se predviđaju predmetna miješanja [171]. K tomu, svrhe miješanja treba odrediti tako da odgovaraju na zahtjeve jasnoće i preciznosti [172].

288. Međutim, prema mišljenju M. Schremsa, svrha nadzornih mjera predviđenih člankom 702. FISA-e i EO-om br. 12333 nije utvrđena dovoljno precizno da bi se poštovale zaštitne mjere u pogledu predvidivosti i proporcionalnosti. To je konkretno slučaj kada je tim instrumentima osobito široko definiran pojam „vanjske obavještajne informacije". Usto, Komisija je u uvodnoj izjavi 109. Odluke o sustavu zaštite privatnosti utvrdila da se člankom 702. FISA-e zahtijeva da prikupljanje vanjskih obavještajnih informacija čini „važn[u] svrh[u]" prikupljanja, pri čemu taj izraz, na prvi pogled i kao što je to istaknuo EPIC, ne isključuje ostvarivanje drugih neutvrđenih ciljeva.

289. Iz tih razloga, a da pritom nije isključeno da nadzorne mjere na temelju članka 702. FISA-e ili EO-a br. 12333 imaju legitimne ciljeve, može se postaviti pitanje jesu li ti ciljevi definirani dovoljno jasno i precizno kako bi se spriječila opasnost od zlouporabe i omogućio nadzor proporcionalnosti miješanja koja iz njih proizlaze [173].

5) Nužnost i proporcionalnost miješanja

290. Sud je više puta istaknuo da prava priznata u člancima 7. i 8. Povelje nisu apsolutna prava, nego ih treba poštovati s obzirom na njihovu funkciju u društvu i odvagnuti s drugim temeljnim pravima u skladu s načelom proporcionalnosti [174]. Kao što je to istaknuo Facebook Ireland, među tim je drugim pravima pravo na sigurnost koje je zajamčeno u članku 6. Povelje.

291. U tom pogledu, prema jednako ustaljenoj sudskoj praksi, u pogledu svakog miješanja u ostvarivanje prava zajamčenih u člancima 7. i 8. Povelje treba provesti strog nadzor proporcionalnosti [175].

292. Konkretno, iz presude Schrems proizlazi da „propis koji općenito dopušta zadržavanje cjelokupnih […] podataka […] bez ikakvog razlikovanja, ograničenja ili iznimke s obzirom na postavljeni cilj, i koji ne predviđa objektivan kriterij koji bi omogućavao ograničenje pristupa javnih tijela podacima i njihovu naknadnu uporabu u svrhe koje su točno određene, strogo ograničene i mogu opravdati miješanje koje obuhvaća i pristup i uporabu tih podataka, nije ograničen na ono što je strogo nužno" [176].

293. Sud je također presudio da, osim u valjano opravdanim hitnim slučajevima, pristup treba podvrgnuti prethodnom nadzoru suda ili neovisnog upravnog tijela čija odluka ima za cilj ograničiti pristup podacima i njihovu uporabu na ono što je strogo nužno za ostvarenje postavljenog cilja [177].

171 Radna skupina 29, u svojem radnom dokumentu o nadzoru elektroničkih komunikacija u svrhu obavještavanja i nacionalne sigurnosti, od 5. prosinca 2014., WP 228 (str. 27.), naglasila je važnost kritičke ocjene toga je li nadzor stvarno proveden u svrhu nacionalne sigurnosti.

172 Vidjeti mišljenje 1/15 (točka 181.), u kojem je Sud smatrao da tekst zakonodavnih odredbi kojima se predviđaju miješanja ne zadovoljavaju zahtjeve u pogledu jasnoće i preciznosti, tako da ta miješanja nisu bila ograničena samo na ono što je krajnje nužno. S tog gledišta, nezavisni odvjetnik Y. Bot smatrao je, u svojem mišljenju u predmetu Schrems (C-362/14, EU:C:2015:627, t. 181. do 184.), da su ciljevi nadzornih mjera bili preopćenito definirani da bi se mogli smatrati ciljevima od općeg interesa, osim što se tiče nacionalne sigurnosti.

173 Slične je dvojbe EDPS iznio u svojem mišljenju 4/2016 o nacrtu odluke o primjerenosti europsko-američkog sustava zaštite privatnosti (Privacy Shield) od 30. svibnja 2016. (str. 8.).

174 Vidjeti presudu od 9. studenoga 2010., Volker und Markus Schecke i Eifert (C-92/09 i C-93/09, EU:C:2010:662, t. 48.); mišljenje 1/15 (t. 136.) i presudu od 24. rujna 2019., Google (Teritorijalni doseg uklanjanja poveznica) (C-507/17, EU:C:2019:772, t. 60.).

175 Vidjeti osobito presudu od 16. prosinca 2008., Satakunnan Markkinapörssi i Satamedia (C-73/07, EU:C:2008:727, t. 56.); presuda Digital Rights Ireland (t. 48. i 52.); presuda Schrems (t. 78. i 92.), kao i mišljenje 1/15 (t. 139. i 140.). Vidjeti i uvodnu izjavu 140. Odluke o sustavu zaštite privatnosti.

176 Presuda Schrems (t. 93.). Vidjeti u tom smislu i presudu Digital Rights Ireland (t. 60.).

177 Vidjeti presudu Tele2 Sverige (t. 120.) i mišljenje 1/15 (t. 202.).

294. U članku 23. stavku 2. GDPR-a sada se utvrđuje niz zaštitnih mjera koje država članica treba predvidjeti kada odstupa od odredbi te uredbe. Propis kojim se omogućuje takvo odstupanje treba sadržavati odredbe, među ostalim, o svrhama obrade, opsegu odstupanja, zaštitnim mjerama za sprečavanje zlouporabe, razdoblju pohrane i pravu ispitanika da budu obaviješteni o odstupanju, osim ako to može biti štetno za svrhu tog odstupanja.

295. U ovom slučaju, M. Schrems tvrdi da članak 702. FISA ne sadržava dovoljna jamstva od rizika zlouporabe i nezakonitog pristupa podacima. Konkretno, utvrđivanje kriterija za odabir nije dovoljno određeno, tako da ta odredba ne nudi osiguranja od općeg pristupa sadržaju komunikacija.

296. Suprotno tomu, vlada SAD-a i Komisija tvrde da je člankom 702. FISA-e utvrđivanje čimbenika za odabir ograničeno objektivnim kriterijima jer se tom odredbom omogućuje samo prikupljanje podataka o elektroničkim komunikacijama osoba koje nisu američki državljani, a nalaze se izvan SAD-a u svrhu dobivanja stranih obavještajnih informacija.

297. Prema mojem mišljenju, opravdano je dvojiti o tome jesu li ti kriteriji dovoljno jasni i precizni, te postoje li dovoljna jamstva kako bi se spriječili rizici zlouporabe.

298. Najprije, u uvodnoj izjavi 109. Odluke o sustavu zaštite privatnosti navodi se da, prije njihove primjene, čimbenike za odabir ne odobrava pojedinačno FISC ni bilo koje drugo neovisno sudsko ili upravno tijelo. Komisija je u toj uvodnoj izjavi utvrdila da „FISC ne odobrava pojedinačne mjere nadzora, već odobrava programe nadzora […] na temelju godišnjih certifikacija”, što je vlada SAD-a potvrdila pred Sudom. U toj se uvodnoj izjavi pojašnjava da „certifikacije koje će odobriti FISC ne sadržavaju informacije o pojedinim osobama čiji će se podaci usmjereno prikupljati već se u njima navode kategorije stranih obavještajnih informacija” koje se mogu prikupiti. Komisija je u toj uvodnoj izjavi također utvrdila da „FISC ne procjenjuje – zbog opravdane sumnje ili na nekoj drugoj osnovi – jesu li osobe čiji se podaci prikupljaju radi pribavljanja stranih obavještajnih podataka ispravno odabrane”, iako provodi kontrolu pod uvjetom da je „važna svrha prikupljanja pribaviti strane obavještajne informacije”.

299. Zatim, u skladu s navedenom uvodnom izjavom, u skladu s člankom 702. FISA-e NSA smije prikupljati komunikacijske podatke „samo ako se opravdano vjeruje da se predmetno komunikacijsko sredstvo upotrebljava za dostavljanje stranih obavještajnih informacija”. U uvodnoj izjavi 70. Odluke o sustavu zaštite privatnosti dodaje se da se utvrđivanje čimbenika za odabir odvija unutar općeg „Okvira prioriteta nacionalne obavještajne službe” (National Intelligence Priorities Framework, NIPF). U toj se odluci ne utvrđuju zahtjevi preciznijeg obrazlaganja ili preciznijih opravdanja u pogledu utvrđivanja čimbenika za odabir s obzirom na te administrativne prioritete kojima je obvezana NSA [178].

300. Naposljetku, u uvodnoj izjavi 71. Odluke o sustavu zaštite privatnosti upućuje se na zahtjev, predviđen PPD-om 28, prema kojem prikupljanje stranih obavještajnih informacija treba biti „što usmjerenije”. Osim činjenice da se tim predsjedničkim ukazom pojedincima ne dodjeljuju prava, čini mi se da nije nimalo očita bitna ekvivalentnost između kriterija „što usmjerenije” aktivnosti i zahtjeva „stroge nužnosti” koji se člankom 52. stavkom 1. Povelje propisuje kako bi se opravdalo miješanje u ostvarivanje prava zajamčenih u njezinim člancima 7. i 8. [179].

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

179 Vidjeti u tom smislu radnu skupinu 29, Opinion 1/2016 on the EU-U. S. Privacy Shield draft adequacy decision, 13. travnja 2016., WP 238 (t. 3.3.1., str. 38.), Rezoluciju Parlamenta od 6. travnja 2017. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti, P8_TA(2017)0131 (t. 17.), kao i Izvješće Parlamenta o utjecaju velikih podataka na temeljna prava: privatnost, zaštita podataka, nediskriminacija, sigurnost i kazneni progon, od 20. veljače 2017., A8-0044/2017 (t. 17.).

301. S obzirom na ta razmatranja, nije izvjesno da se, na temelju elemenata iznesenih u Odluci o sustavu zaštite privatnosti, na nadzorne mjere koje se temelje na članku 702. FISA-e primjenjuju zaštitne mjere, kojima se ograničava broj osoba koje mogu biti predmet nadzornih mjera i ciljevi za koje se podaci mogu prikupiti, koje su bitno ekvivalentne zaštitnim mjerama koje se zahtijevaju na temelju GDPR-a, s obzirom na članke 7. i 8. Povelje [180].

302. Osim toga, što se tiče procjene primjerenosti razine zaštite u pogledu nadzora na temelju EO-a br. 12333, ESLJP priznaje državama članicama široku marginu prosudbe pri odabiru sredstava zaštite svoje nacionalne sigurnosti, pri čemu je ta margina ipak ograničena zahtjevom da se predvide primjerena i dovoljna jamstva od zlouporabe [181]. U svojoj sudskoj praksi o tajnim mjerama nadzora, ESLJP provjerava sadržava li nacionalno pravo, na kojem se temelje te mjere, dovoljne i djelotvorne zaštitne mjere i mehanizme za ispunjavanje zahtjeva „utvrdivosti" i „nužnosti u demokratskom društvu" [182].

303. ESLJP je u tom pogledu iznio određeni broj minimalnih zaštitnih mjera. Te se zaštitne mjere odnose na jasno navođenje prirode povreda koje mogu dovesti do naloga za presretanje, definiciju kategorija osoba čije se komunikacije mogu presresti, utvrđivanje ograničenja u pogledu trajanja izvršenja mjere, postupka koji treba provesti pri ispitivanju, upotrebi i zadržavanju prikupljenih podataka, mjere predostrožnosti koje treba poduzeti za priopćavanje podataka drugim strankama i okolnosti u kojima se zapisi mogu ili moraju izbrisati ili uništiti [183].

304. Primjerenost i djelotvornost zaštitnih mjera kojima se utvrđuje miješanje ovise o svim predmetnim okolnostima, uključujući o prirodi, opsegu i trajanju mjera, razlozima potrebnim za njihovo nalaganje, nadležnim tijelima za njihovo odobravanje, izvršenje i nadziranje te o vrsti pravnog sredstva dostupnog u nacionalnom pravu [184].

305. Konkretno, u svrhu procjene opravdanosti tajne nadzorne mjere, ESLJP uzima u obzir sve nadzore izvršene „tijekom njezina nalaganja", „tijekom njezine provedbe" i „nakon njezina prestanka" [185]. Što se tiče prve od tih triju faza, ESLJP zahtijeva da takvu mjeru odobri neovisno tijelo. Iako pravosudno tijelo, prema mišljenju ESLJP-a, nudi najbolje zaštitne mjere u pogledu neovisnosti, nepristranosti i pravilnosti postupka, predmetno tijelo ne treba nužno pripadati sudbenoj vlasti [186]. Temeljit sudski nadzor u kasnijoj fazi može ispraviti eventualne nepravilnosti u postupku odobrenja [187].

306. U ovom slučaju, iz Odluke o sustavu zaštite privatnosti proizlazi da se jedine zaštitne mjere kojima se ograničava prikupljanje i upotreba podataka izvan državnog područja SAD-a navode u PPD-u 28, s obzirom na to da se članak 702. FISA-e ne primjenjuje izvan tog državnog područja. Nisam uvjeren da te zaštitne mjere mogu biti dovoljne da bi se ispunili uvjeti „utvrdivosti" i „nužnosti u demokratskom društvu".

180 Vidjeti u tom smislu radnu skupinu 29, EU-U. S. Privacy Shield – First Annual Joint Review, 28. studenoga 2017., WP 255 (str. 3.), Rezoluciju Europskog parlamenta od 5. srpnja 2018. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti, P8_TA-PROV(2018)0315 (t. 22.) i EOZP, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. siječnja 2019. (t. 81. do 83. i 87.).

181 Vidjeti osobito presude Zakharov (t. 232.) i Szabó i Vissy (t. 57.).

182 Vidjeti osobito presude Zakharov (t. 237.); Centrüm för Rättvisa (t. 111.) i Big Brother Watch (t. 322.).

183 Vidjeti osobito odluku Weber i Saravia (t. 95.); ESLJP, 28. lipnja 2007., Association for European Integration and Human Rights i Ekimdjiev (CE:ECHR:2007:0628JUD006254000, t. 76.), kao i presuda Zakharov (t. 231.).

184 Vidjeti osobito odluku Weber i Saravia (t. 106.); presuda Zakharov (t. 232.) i presuda Centrüm för Rättvisa (t. 104.).

185 Vidjeti osobito ESLJP, 6. rujna 1978., Klass i dr. protiv Njemačke (CE:ECHR:1978:0906JUD000502971, t. 55.); presuda Zakharov (t. 233.), kao i presuda Centrüm för Rättvisa (t. 105.).

186 Vidjeti osobito presudu Klass (t. 56.); ESLJP, 18. svibnja 2010., Kennedy protiv Ujedinjene Kraljevine (CE:ECHR:2010:0518JUD002683905, t. 167.), kao i presuda Zakharov (t. 233. i 258.).

187 Vidjeti presude Szabó i Vissy (t. 77.) i Centrüm för Rättvisa (t. 133.).

307. Najprije, već sam istaknuo da se tim predsjedničkim ukazom ne dodjeljuju prava pojedincima. Zatim, dvojim u pogledu toga da je zahtjev osiguravanja „što usmjerenijeg" nadzora definiran dovoljno jasno i precizno kako bi se ispitanike primjereno zaštitilo od rizika zlouporabe [188]. Naposljetku, Odlukom o sustavu zaštite privatnosti ne utvrđuje se da nadzor koji se temelji na EO-u br. 12333 podliježe prethodnoj kontroli koju provodi neovisno tijelo ili da može biti predmet *a posteriori* sudskog nadzora [189].

308. U tim okolnostima, pitam se je li osnovano utvrđenje prema kojem SAD u okviru aktivnosti svojih obavještajnih službi na temelju članka 702. FISA-e i EO-a br. 12333 osigurava primjerenu razinu zaštite u smislu članka 45. stavka 1. GDPR-a, s obzirom na članke 7. i 8. Povelje te članak 8. EKLJP-a.

c) Valjanost Odluke o sustavu zaštite privatnosti s obzirom na pravo na djelotvoran pravni lijek

309. Petim prethodnim pitanjem od Suda se traži da utvrdi imaju li osobe čiji se podaci prenose u SAD ondje pristup sudskoj zaštiti koja je bitno ekvivalentna zaštiti koju treba osigurati u Uniji na temelju članka 47. Povelje. Svojim desetim pitanjem sud koji je uputio zahtjev u biti pita Sud treba li na peto pitanje odgovoriti potvrdno s obzirom na to da se Odlukom o sustavu zaštite privatnosti uvodi mehanizam pravobranitelja.

310. Najprije utvrđujem da u uvodnoj izjavi 115. te odluke Komisija priznaje da je američki pravni sustav manjkav u pogledu sudske zaštite pojedinaca.

311. U skladu s tom uvodnom izjavom, kao prvo, „barem neke pravne osnove koje američka obavještajna tijela (npr. Izvršni nalog br. 12333) mogu upotrijebiti [nemaju]" na raspolaganju mogućnosti sudske zaštite. Naime, EO br. 12333 i PPD 28 ne daju prava predmetnim osobama i one se na njih ne mogu pozvati pred sudovima. Međutim, djelotvorna sudska zaštita podrazumijeva, barem, da pojedinci imaju prava na koja se mogu pozvati pred sudom.

312. Kao drugo, „čak i ako osobe koje nisu američki državljani u načelu imaju na raspolaganju mogućnosti sudske zaštite, kao u slučaju nadzora u skladu s FISA-om, dostupne pravne osnove ograničene su […] i [podnesene] tužbe […] proglasit će se neprihvatljivima ako se ne može dokazati ‚osnovanost' […], kojom se ograničava pristup redovnim sudovima".

313. Iz uvodnih izjava 116. do 124. Odluke o sustavu zaštite privatnosti, proizlazi da se uvođenjem pravobranitelja nastoje nadoknaditi ta ograničenja. U uvodnoj izjavi 139. te odluke Komisija zaključuje da se „mehanizmima *nadzora* i *pravne zaštite u cjelini*, koji se osiguravaju u okviru sustava zaštite privatnosti […] osobi čiji se podaci obrađuju osiguravaju pravna sredstva za ostvarivanje pristupa njezinim osobnim podacima te za ispravak ili brisanje takvih podataka" (moje isticanje).

314. Nakon što podsjetim na opća načela koja proizlaze iz sudske prakse Suda i ESLJP-a u pogledu prava na pravni lijek protiv mjera nadzora u pogledu komunikacija, ispitat ću omogućuje li se pravnim sredstvima predviđenim američkim pravom, kako su opisana u Odluci o sustavu zaštite privatnosti, osiguravanje primjerene pravne zaštite ispitanika (dio 1). Zatim ću ispitati mogu li se na temelju uvođenja izvansudskog mehanizma, po potrebi, nadoknaditi eventualni nedostaci koji su svojstveni pravnoj zaštiti tih osoba (dio 2).

188 To je tim više slučaj s obzirom na razmatranja iz točke 281. ovog mišljenja.

189 Vidjeti točke 330. i 331. ovog mišljenja.

1) Djelotvornost pravnih lijekova predviđenih pravom SAD-a

315. Kao prvo, člankom 47. prvim stavkom Povelje utvrđuje se da svatko čija su prava i slobode zajamčeni pravom Unije povrijeđeni ima pravo na djelotvoran pravni lijek pred sudom [190]. U skladu s drugim stavkom tog članka, svatko ima pravo da neovisni i nepristrani sud ispita njegov slučaj [191]. Sud je presudio da je pristup neovisnom sudu dio biti prava zajamčenog člankom 47. Povelje [192].

316. Uz to pravo na pojedinačnu pravnu zaštitu postoji i obveza koju države članice imaju na temelju članaka 7. i 8. Povelje da svaku nadzornu mjeru, osim u valjano opravdanim hitnim slučajevima, podvrgnu prethodnom nadzoru suda ili neovisnog upravnog tijela [193].

317. Točno je, kao što su to istaknule njemačka i francuska vlada, da pravo na djelotvoran pravni lijek nije apsolutna zaštitna mjera [194] jer se to pravo može ograničiti iz razloga nacionalne sigurnosti. Odstupanja se ipak odobravaju samo ako se njima ne povređuje bit tog prava i ako su nužno potrebne za postizanje legitimnog cilja.

318. U tom pogledu, Sud je u presudi Schrems odlučio da propis koji pojedincima ne pruža *nikakvu mogućnost* korištenja pravnim sredstvima radi pristupa osobnim podacima koji se na njih odnose, ili radi ispravka ili brisanja takvih podataka, ne poštuje bitan sadržaj temeljnog prava koje je propisano u članku 47. Povelje [195].

319. Ističem da to pravo na pristup podrazumijeva mogućnost osobe da od tijela javne vlasti, podložno odstupanjima koja su nužno potrebna za ostvarivanje legitimnog interesa, dobiju *potvrdu obrađuju li se osobni podaci koji se odnose na nju* [196]. Prema mojem mišljenju, takav je praktični doseg prava na pristup kada ispitanik ne zna jesu li tijela javne vlasti zadržala osobne podatke koji se odnose na njega, osobito nakon automatiziranog postupka filtriranja protoka elektroničkih komunikacija.

190 U Objašnjenjima koja se odnose na Povelju u tom se pogledu navodi da je „prema pravu Unije zaštita [predviđena člankom 47. Povelje] širih razmjera [od zaštite predviđene člankom 13. EKLJP-a] jer jamči pravo na djelotvoran pravni lijek pred sudom". Vidjeti također mišljenje nezavisnog odvjetnika M. Watheleta u predmetu Berlioz Investment Fund (C-682/15, EU:C:2017:2, t. 37.).

191 Kako bi se ocijenilo ima li tijelo svojstvo „suda" u okviru primjene članka 47. Povelje, treba uzeti u obzir njegovu utemeljenost na zakonu, stalnost, svojstvo obvezne nadležnosti, kontradiktornu narav postupka, primjenu pravnih pravila te njegovu neovisnost. Vidjeti presudu od 27. veljače 2018., Associação Sindical dos Juízes Portugueses (C-64/16, EU:C:2018:117, t. 38. i navedena sudska praksa).

192 Vidjeti osobito presudu od 25. srpnja 2018., Minister for Justice and Equality (Nedostaci pravosudnog sustava) (C-216/18 PPU, EU:C:2018:586, t. 59. i 63.); od 5. studenoga 2019., Komisija/Poljska (Neovisnost redovnih sudova) (C-192/18, EU:C:2019:924, t. 106.), i od 19. studenoga 2019., A. K. i dr. (Neovisnost disciplinskog vijeća Vrhovnog suda) (C-585/18, C-624/18 i C-625/18, EU:C:2019:982, t. 120.).

193 Vidjeti točku 293. ovog mišljenja. Člankom 45. stavkom 3. točkom (a) GDPR-a predviđa se uzimanje u obzir, tijekom procjene primjerenosti razine zaštite koju pruža treća država, učinkovite „upravne i *sudske* zaštite" na koju se ispitanici ondje mogu pozvati (moje isticanje). Jednako tako, u skladu s uvodnom izjavom 104. GDPR-a, donošenje odluke o primjerenosti treba uvjetovati time da ispitanici u dotičnoj trećoj zemlji imaju „učinkovitu upravnu *i sudsku* zaštitu" (moje isticanje). Vidjeti također radnu skupinu 29, EU-U. S. Privacy Shield – First Annual Joint Review, 28. studenoga 2017., WP 255 (t. B.3.), Rezoluciju Parlamenta od 5. srpnja 2018. o primjerenosti zaštite u okviru europsko-američkog sustava zaštite privatnosti, P8_TA(2018)0315 (t. 25. i 30.) i EOZP, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. siječnja 2019. (t. 94. do 97.).

194 Vidjeti u tom smislu presudu od 28. veljače 2013., Preispitivanje Arango Jaramillo i dr./EIB (C-334/12 RX-II, EU:C:2013:134, t. 43.).

195 Presuda Schrems (t. 95.).

196 Člankom 15. GDPR-a, naslovljenim „Pravo ispitanika na pristup", u njegovu se stavku 1. određuje da taj ispitanik „ima pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup […] podacima". „Načelo pristupa" predviđeno u točki II.8. podtočki (a) Priloga II. Odluci o sustavu zaštite privatnosti ima isto značenje.

320. Osim toga, iz sudske prakse proizlazi da su tijela države članice u načelu dužna obavijestiti o pristupu podacima *čim takvo obavješćivanje ne može ugroziti istragu koja se vodi*[197]. Naime, takvo je obavješćivanje preduvjet za ostvarivanje prava na pravni lijek na temelju članka 47. Povelje[198]. Ta je obveza sada preuzeta u članku 23. stavku 2. točki (h) GDPR-a.

321. U uvodnim izjavama 111. do 135. Odluke o sustavu zaštite privatnosti sažeto se navode svi pravni lijekovi dostupni osobama čiji se podaci prenose ako ih zabrinjava obrađuju li američke obavještajne službe te podatke nakon prijenosa. Ti su pravni lijekovi također opisani u presudi High Courta (Visoki sud) od 3. listopada 2017., kao i u očitovanjima, među ostalim, vlade SAD-a.

322. Nije potrebno detaljno podsjetiti na sadržaj tih navoda. Naime, sud koji je uputio zahtjev dovodi u pitanje primjerenost zaštitnih mjera u pogledu pravne zaštite ispitanika jer bi osobito strogi zahtjevi o aktivnoj procesnoj legitimaciji (*standing*)[199], zajedno s nepostojanjem bilo kakve obveze da se osobe u pogledu kojih su donesene nadzorne mjere obavijeste *čak i kada se obavješćivanjem više ne bi ugrožavali ciljevi*, učinili pretjerano teškim upotrebu pravnih lijekova predviđenih u pravu SAD-a. Te dvojbe dijele DPC, M. Schrems, austrijska, poljska i portugalska vlada te EOZP[200].

323. U tom ću pogledu samo podsjetiti da se pravilima o aktivnoj procesnoj legitimaciji ne može dovesti u pitanje djelotvorna sudska zaštita[201], te ću utvrditi da se u Odluci o sustavu zaštite privatnosti ne navodi nikakav zahtjev o obavješćivanju ispitanika o činjenici da je u pogledu njih donesena nadzorna mjera[202]. Budući da bi takav zahtjev mogao spriječiti ostvarivanje pravnih lijekova, nepostojanje obveze obavijesti o takvoj mjeri, čak i kada se obavješćivanjem ispitanika više ne bi narušila njezina učinkovitost, problematično je s obzirom na sudsku praksu navedenu u točki 320. ovog mišljenja.

324. K tomu, u bilješci 169. Odluke o sustavu zaštite privatnosti priznaje se da dostupne pravne osnove „zahtijevaju postojanje štete […] ili dokaz da vlada planira upotrijebiti ili otkriti informacije dobivene ili izvedene iz elektroničkog nadzora predmetne osobe protiv te osobe". Kao što su to istaknuli sud koji je uputio zahtjev, DPC i M. Schrems, taj je zahtjev proturječan sudskoj praksi Suda prema kojoj, u svrhu utvrđivanja miješanja u pravo na poštovanje privatnog života ispitanika, nije potrebno da je taj ispitanik pretrpio eventualne nepogodnosti zbog navodnog miješanja[203].

325. Osim toga, ne smatram uvjerljivim stajalište koje su iznijeli Facebook Ireland i vlada SAD-a, prema kojem su nedostaci pravne zaštite osoba čiji se podaci prenose u SAD nadoknađeni prethodnim i naknadnim nadzorima koje provodi FISC, kao i višestrukim mehanizmima nadzora uspostavljenima u okviru izvršne i zakonodavne ovlasti[204].

197 Presuda Tele2 Sverige (t. 121.), kao i mišljenje 1/15 (t. 220.). Kao što je to napomenuo Facebook Ireland, obavijest o pristupu tijela javne vlasti podacima stoga se ne može sustavno zahtijevati. U tom pogledu ESLJP smatra da je „[u] praksi moguće da se ne može zahtijevati *a posteriori* obavijest" jer prijetnja u pogledu koje su donesene nadzorne mjere „može i dalje postojati još godinama ili čak desetljećima" nakon ukidanja tih mjera, tako da se obavješćivanjem mogu „narušiti dugoročni cilj kojim je prvotno potaknut nadzor" i „otkriti metode rada obavještajnih službi, njihova područja djelovanja i […] identitet njihovih agenata" (presuda Zakharov (t. 287. i navedena sudska praksa)). Ako ne postoji takvo obavješćivanje, iako se u slučaju povrede pravnih zahtjeva tada ne može pozvati na pojedinačnu pravnu zaštitu, druge zaštitne mjere mogu biti dovoljne kako bi se zaštitilo pravo na poštovanje privatnog života (vidjeti i presudu Centrüm för Rättvisa, t. 164. do 167. i 171. do 178.). Vidjeti točku 330. ovog mišljenja.

198 Vidjeti u tom pogledu bilješku 210. ovog mišljenja.

199 Vidjeti točku 67. ovog mišljenja.

200 Vidjeti EOZP, EU-U. S. Privacy Shield – Second Annual Joint Review, 22. siječnja 2019. (str. 18., t. 97.).

201 Vidjeti osobito presude od 11. srpnja 1991., Verholen i dr. (C-87/90 do C-89/90, EU:C:1991:314, t. 24. i navedena sudska praksa), kao i od 28. veljače 2013., Preispitivanje Arango Jaramillo i dr./EIB (C-334/12 RX-II, EU:C:2013:134, t. 43.).

202 Vlada SAD-a ipak je pojasnila, kao i sud koji je uputio zahtjev, da o nadzornoj mjeri na temelju članka 702. FISA-e treba obavijestiti osobu protiv koje je donesena ako su prikupljeni podaci upotrijebljeni protiv nje u okviru sudskog postupka.

203 Presuda od 20. svibnja 2003., Österreichischer Rundfunk i dr. (C-465/00, C-138/01 i C-139/01, EU:C:2003:294, t. 75.); presuda Digital Rights Ireland (t. 33.); presuda Schrems (t. 87.) i mišljenje 1/15 (t. 124.)

204 Ti su mehanizmi opisani u uvodnim izjavama 95. do 110. Odluke o sustavu zaštite privatnosti. Komisija u tim uvodnim izjavama, u okviru kategorije pravila o „učinkovitoj pravnoj zaštiti", razlikuje „mehanizme nadzora" (vidjeti uvodne izjave 92. do 110.) od pojedinačne pravne zaštite (vidjeti uvodne izjave 111. do 124.).

326. Već sam istaknuo da, s jedne strane, u skladu s utvrđenjima navedenim u Odluci o sustavu zaštite privatnosti, FISC ne nadzire pojedinačne mjere nadzora prije njihove provedbe [205]. Kao što se to navodi u uvodnoj izjavi 109. te odluke i kao što je to potvrdila vlada SAD-a u svojem pisanom odgovoru na pitanja koja je postavio Sud, nadzor *ex post* primjene čimbenika za odabir ima za cilj, s druge strane, provjeriti, kada obavještajna agencija obavijesti FISC o incidentu mogućeg nepoštovanja postupaka usmjeravanja i smanjenja količine podataka [206], jesu li ispunjeni uvjeti kojima se uređuje utvrđivanje čimbenika za odabir koji su predviđeni u godišnjoj certifikaciji. Čini se da postupak pred FISC-om stoga ne nudi djelotvorne pojedinačne pravne lijekove osobama čiji se podaci prenose u SAD.

327. Prema mojem mišljenju, izvansudski mehanizmi nadzora navedeni u uvodnim izjavama 95. do 110. Odluke o zaštiti privatnosti, iako se njima, po potrebi, mogu ojačati mogući sudski pravni lijekovi , ne mogu biti dovoljni da bi se osigurala primjerena razina zaštite u pogledu prava na pravni lijek ispitanika. Konkretno, čini mi se da glavni inspektori, koji su dio unutarnje strukture svake agencije, ne čine neovisne mehanizme nadzora. Nadzor koji provode PCLOB i obavještajni odbori američkog kongresa nije pak jednak mehanizmu pojedinačne pravne zaštite od mjera nadzora.

328. Stoga će valjati ispitati jesu li uvođenjem pravobranitelja nadoknađeni ti nedostaci tako da se ispitanicima pruži djelotvoran pravni lijek pred neovisnim i nepristranim tijelom [207].

329. Kao drugo, u svrhu procjene je li osnovano utvrđenje primjerenosti izneseno u Odluci o sustavu zaštite privatnosti s obzirom na pravne lijekove dostupne osobama koje misle da su predmet nadzora koji se temelji na EO-u br. 12333, podsjećam da se relevantan referentni okvir temelji na odredbama EKLJP-a.

330. Kao što je to prethodno navedeno [208], ESLJP provodi, kako bi procijenio ispunjuje li nadzorna mjera uvjete „utvrdivosti" i „nužnosti u demokratskom društvu" u smislu članka 8. stavka 2. EKLJP-a [209], ispitivanje svih mehanizama kontrole i nadzora koji se provode „prije, tijekom i nakon" njezine provedbe. Kad je ostvarivanje pojedinačne pravne zaštite spriječeno jer obavješćivanje o nadzornoj mjeri nije moguće a da se ne dovede u pitanje njegova učinkovitost [210], taj se nedostatak može nadoknaditi provedbom neovisnog nadzora prije primjene predmetne mjere [211]. Stoga ESLJP, iako takvo obavješćivanje smatra „poželjnim" ako ga je moguće provesti a da se ne naruši učinkovitost nadzorne mjere, nije utvrdio da se to obavješćivanje zahtijeva [212].

331. U tom pogledu, iz Odluke o sustavu zaštite privatnosti ne proizlazi da se o nadzornim mjerama koje se temelje na EO-u br. 12333 obavještavaju dotični pojedinci niti da su te mjere određene neovisnim mehanizmima sudskog ili upravnog nadzora u bilo kojoj fazi njihova donošenja ili provedbe.

205 Vidjeti točku 298. ovog mišljenja.

206 U skladu s uvodnom izjavom 109. Odluke o sustavu zaštite privatnosti, „[g]lavni državni odvjetnik i direktor [NSA-e] provjeravaju usklađenost, a agencije su dužne o svim slučajevima neusklađenosti obavijestiti FISC […], koji na osnovu toga može izmijeniti odobrenje".

207 Vidjeti točke 333. do 340. ovog mišljenja.

208 Vidjeti točku 305. ovog mišljenja.

209 U svojoj sudskoj praksi o mjerama nadzora telekomunikacija, ESLJP je razmatrao pitanje pravnih lijekova u okviru ispitivanja „svojstva zakona" i nužnosti miješanja u ostvarivanje prava zajamčenog člankom 8. EKLJP-a (vidjeti osobito presude Zakharov (t. 236.) i Centrüm för Rättvisa (t. 107.)). U presudi od 1. srpnja 2008., Liberty i dr. protiv Ujedinjene Kraljevine (CE:ECHR:2008:0701JUD005824300, t. 73.) i presudi Zakharov (t. 307.) ESLJP, nakon što je utvrdio povredu članka 8. EKLJP-a, nije smatrao potrebnim zasebno ispitati prigovor koji se temelji na članku 13. te konvencije.

210 Prema mišljenju ESLJP-a, iako neobavješćivanje u bilo kojoj fazi ne znači nužno da nadzorna mjera ne ispunjava uvjet „nužnosti u demokratskom društvu", njime se narušava pristup sudovima i stoga učinkovitost pravnih lijekova (vidjeti osobito presudu od 6. rujna 1978., Klass i dr. protiv Njemačke (CE:ECHR:1978:0906JUD000502971, t. 57. i 58.), odluku Weber i Saravia (t. 135.) i presudu Zakharov (t. 302.)).

211 Vidjeti u tom smislu presudu Centrum för Rättvisa (t. 105.).

212 U presudi Big Brother Watch (t. 317.), ESLJP je odbio među minimalne zaštitne mjere primjenjive na sustav nadzora popraćen masovnim presretanjem elektroničkih komunikacija dodati zahtjev obavješćivanja ispitanika o nadzoru. Vidjeti također presudu Centrüm för Rättvisa (t. 164.). Cilj vraćanja tih presuda velikom vijeću ESLJP-a je među ostalim ispitivanje tog zaključka.

332. U tim okolnostima, valja ispitati je li na temelju obraćanja pravobranitelju ipak moguće osigurati neovisnu kontrolu nadzornih mjera, uključujući mjera koje se temelje na EO-u br. 12333.

2) Utjecaj mehanizma pravobranitelja na razinu zaštite prava na djelotvoran pravni lijek

333. U skladu s uvodnom izjavom 116. Odluke o sustavu zaštite privatnosti, mehanizam pravobranitelja opisan u Prilogu III. A toj odluci ima za cilj pružiti dodatna pravna sredstva svim osobama čiji se podaci prenose iz Unije u SAD.

334. Kao što je to istaknula vlada SAD-a, dopuštenost pritužbe podnesene pravobranitelju nije uvjetovana poštovanjem pravila o aktivnoj procesnoj legitimaciji koja su slična pravilima kojima se uređuje pristup američkim sudovima. U uvodnoj izjavi 119. navedene odluke u tom se pogledu pojašnjava da obraćanje pravobranitelju ne podrazumijeva da dotična osoba mora dokazati da je vlada SAD-a pristupila osobnim podacima koji se odnose na nju.

335. Kao i DPC, M. Schrems, poljska i portugalska vlada te EPIC, dvojim u pogledu toga da se tim mehanizmom mogu nadoknaditi nedostaci pravne zaštite koja se nudi osobama čiji se podaci prenose iz Unije u SAD.

336. Najprije, iako mehanizam izvansudskog pravnog lijeka može biti djelotvoran pravni lijek u smislu članka 47. UFEU-a, to je ipak slučaj, konkretno, samo ako je predmetno tijelo ustanovljeno zakonom i ispunjava uvjet neovisnosti [213].

337. Međutim, iz Odluke o sustavu zaštite podataka proizlazi da mehanizam pravobranitelja, koji se temelji na PPD-u 28 [214], nema zakonsku osnovu. Pravobranitelja imenuje ministar vanjskih poslova te je sastavni dio Ministarstva vanjskih poslova SAD-a [215]. Ta odluka ne sadržava nikakav navod prema kojem se na razrješenje pravobranitelja njegove dužnosti ili opoziv njegova imenovanja primjenjuju posebne zaštitne mjere [216]. Iako je pravobranitelj predstavljen kao neovisan o „obavještajnoj zajednici", on odgovara ministru vanjskih poslova te stoga nije neovisan od izvršne vlasti [217].

338. Zatim, čini mi se da djelotvornost izvansudskog pravnog lijeka ovisi i o tome može li predmetno tijelo donositi pravno obvezujuće i obrazložene odluke. U tom pogledu, u Odluci o sustavu zaštite privatnosti uopće se ne navodi da pravobranitelje donosi takve odluke. Tom se odlukom ne utvrđuje da se uvođenjem pravobranitelja podnositeljima pravnog lijeka omogućuje pristup podacima koji se odnose na njih i da ih ispravljaju ili brišu ni da pravobranitelj dodjeljuje naknadu osobama oštećenima nadzornom mjerom. Konkretno, kao što proizlazi iz točke 4. podtočke (e) Priloga III.A toj odluci, „Pravobranitelj […] neće potvrditi ni poreći je li osoba bila predmetom nadzora i neće potvrditi je li

213 Pojam neovisnosti obuhvaća prvi aspekt, vanjske prirode, koji znači da je predmetno tijelo zaštićeno od vanjskih utjecaja ili pritisaka koji mogu narušiti neovisnu prosudbu njegovih članova u pogledu postupaka pred njima. Drugi aspekt, unutarnje prirode, odnosi se na „nepristranost" te ima za cilj osiguranje jednakog odmaka od stranaka u sporu i njihovih odnosnih interesa u pogledu predmeta spora. Vidjeti osobito presude od 19. rujna 2006., Wilson (C-506/04, EU:C:2006:587, t. 50. do 52.); od 25. srpnja 2018., Minister for Justice and Equality (Nedostaci pravosudnog sustava) (C-216/18 PPU, EU:C:2018:586, t. 63. i 65.) i od 19. studenoga 2019., A. K. i dr. (Neovisnost disciplinskog vijeća Vrhovnog suda) (C-585/18, C-624/18 i C-625/18, EU:C:2019:982, t. 121. i 122.).U skladu s načelom diobe vlasti, neovisnost sudova mora se jamčiti osobito u odnosu na izvršnu vlast. Vidjeti presudu od 19. studenoga 2019., A. K. i dr. (Neovisnost disciplinskog vijeća Vrhovnog suda) (C-585/18, C-624/18 i C-625/18, EU:C:2019:982, t. 127. i navedena sudska praksa).

214 U Prilogu III. A Odluci o sustavu zaštite privatnosti u tom se pogledu upućuje na odjeljak 4. točku (d) PPD-a 28.

215 Vidjeti uvodnu izjavu 116. Odluke o sustavu zaštite privatnosti.

216 U presudi od 31. svibnja 2005., Syfait i dr. (C-53/03, EU:C:2005:333, t. 31.), Sud je istaknuo važnost takvih zaštitnih mjera kako bi se ispunio uvjet neovisnosti. U tom pogledu vidjeti također presude od 24. lipnja 2019., Komisija/Poljska (Neovisnost Vrhovnog suda) (C-619/18, EU:C:2019:531, t. 76.) i od 5. studenoga 2019, Komisija/Poljska (Neovisnost redovnih sudova) (C-192/18, EU:C:2019:924, t. 113.).

217 Vidjeti uvodne izjave 65. i 121., kao i točku 1. Priloga III. A Odluci o sustavu zaštite privatnosti.

poduzeta određena pravna zaštita"[218]. Iako se američka vlada obvezala da će predmetna sastavnica obavještajnih službi biti dužna ispraviti svaku povredu primjenjivih pravnih pravila koje utvrdi pravobranitelj[219], u navedenoj odluci ne navode se zakonske zaštitne mjere kojima je popraćena ta obveza i na koje se dotične osobe mogu pozvati.

339. Prema tome, smatram da se uvođenjem pravobranitelja ne uspostavlja pravni lijek pred neovisnim tijelom koje osobama čiji se podaci prenose nudi mogućnost da ostvare svoje pravo na pristup podacima ili da osporavaju eventualne povrede primjenjivih pravila koje su počinile obavještajne službe.

340. Naposljetku, prema sudskoj praksi, poštovanje prava zajamčenog člankom 47. Povelje stoga podrazumijeva da je odluka tog upravnog tijela koje samo po sebi ne ispunjava uvjet neovisnosti podvrgnuta kasnijem nadzoru sudbenog tijela nadležnog za ispitivanje svih relevantnih pitanja[220]. Međutim, u skladu s navodima iz Odluke o sustavu zaštite privatnosti, odluke pravobranitelja nisu predmet neovisnog sudskog nadzora.

341. U tim okolnostima, kao što su to tvrdili DPC, M. Schrems, EPIC te poljska i portugalska vlada, čini mi se da je upitna bitna ekvivalentnost između pravne zaštite koja se u pravnom poretku SAD-a pruža osobama čiji se podaci prenose iz Unije u SAD i pravne zaštite koja proizlazi iz GDPR-a s obzirom na članak 47. Povelje i članak 8. EKLJP-a.

342. S obzirom na sva prethodna razmatranja, dvojim u pogledu usklađenosti Odluke o sustavu zaštite privatnosti s člankom 45. stavkom 1. GDPR-a s obzirom na članke 7., 8. i 47. Povelje te članak 8. EKLJP-a.

V. Zaključak

343. Predlažem Sudu da na prethodna pitanja koja mu je uputio High Court (Visoki sud, Irska) odgovori kako slijedi:

Analizom prethodnih pitanja nije utvrđen element koji bi mogao utjecati na valjanost Odluke Komisije 2010/87/EU od 5. veljače 2010. o standardnim ugovornim klauzulama za prijenos osobnih podataka obrađivačima u trećim zemljama u skladu s Direktivom 95/46/EZ Europskog parlamenta i Vijeća, kako je izmijenjena Provedbenom odlukom Komisije (EU) 2016/2297 od 16. prosinca 2016.

218 K tomu, u uvodnoj izjavi 121. Odluke o sustavu zaštite privatnosti navodi se da će „Pravobranitelj morati ‚potvrditi' da je i. pritužba pravilno istražena i da se ii. postupalo u skladu s američkim pravom, uključujući s ograničenjima i zaštitnim mjerama iz Priloga VI. ili da je, u slučaju neusklađenosti, takvo kršenje ispravljeno".

219 Komisija je u okviru trećeg godišnjeg preispitivanja sustava zaštite privatnosti utvrdila da, u skladu s tvrdnjama vlade SAD-a, u slučaju da istraga pravobranitelja pokaže da su povrijeđeni postupci usmjeravanja i smanjenja količine podataka koje je odobrio FISC, taj bi sud trebalo obavijestiti o toj povredi. FISC bi tada trebao provesti neovisnu istragu i, po potrebi, naložiti predmetnoj obavještajnoj agenciji da otkloni navedenu povredu. Vidjeti Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U. S. Privacy Shield, 23. listopada 2019., SWD(2019) 390 final, str. 28. Komisija se u njemu poziva na dokument naslovljen „Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure", dostupan na adresi https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (str. 4. i 5.).

220 Vidjeti presude od 16. svibnja 2017., Berlioz Investment Fund (C-682/15, EU:C:2017:373, t. 55.) i od 13. prosinca 2017., El Hassani (C-403/16, EU:C:2017:960, t. 39.).