Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
HENRIKA SAUGMANDSGAARDA ØEJA,
predstavljeni 19. decembra 2019[1]

Zadeva C-311/18

Data Protection Commissioner
proti
Facebook Ireland Limited,
Maximillianu Schremsu,
ob udeležbi
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo High Court (višje sodišče, Irska))

„Predhodno odločanje – Varstvo posameznikov pri obdelavi osebnih podatkov – Uredba (EU) 2016/679 – Člen 2(2) – Področje uporabe – Prenos osebnih podatkov v Združene države Amerike za komercialne namene – Obdelava prenesenih podatkov, ki jo javni organi Združenih držav Amerike izvajajo zaradi nacionalne varnosti – Člen 45 – Presoja ustreznosti ravni varstva, zagotovljene v tretji državi – Člen 46 – Ustrezni zaščitni ukrepi, ki jih zagotovi upravljavec – Standardna določila o varstvu – Člen 58(2) – Pooblastila nadzornih organov – Sklep 2010/87/EU – Veljavnost – Izvedbeni sklep (EU) 2016/1250 – ‚Zasebnostni ščit EU-ZDA‘ – Veljavnost – Členi 7, 8 in 47 Listine Evropske unije o temeljnih pravicah“

Kazalo

I. Uvod 3

II. Pravni okvir 4

A. Direktiva 95/46/ES 4

B. GDPR 6

C. Sklep 2010/87 10

D. Sklep o zasebnostnem ščitu 14

1 Jezik izvirnika: francoščina.

III. Spor o glavni stvari, vprašanja za predhodno odločanje in postopek pred Sodiščem 14

IV. Analiza 22

A. Uvodne ugotovitve 22

B. Dopustnost predloga za sprejetje predhodne odločbe 24

1. Uporaba ratione temporis Direktive 95/46 24

2. Začasnost dvomov, ki jih je izrazil DPC 25

3. Negotovosti v zvezi z opredelitvijo dejanskega okvira 25

C. Uporaba prava Unije za prenose osebnih podatkov za komercialne namene v tretjo državo, ki jih lahko obdeluje zaradi nacionalne varnosti (prvo vprašanje) 26

D. Raven varstva, zahtevana v okviru prenosa, ki temelji na standardnih pogodbenih klavzulah (prvi del šestega vprašanja) 28

E. Veljavnost Sklepa 2010/87 glede na člene 7, 8 in 47 Listine (sedmo, osmo in enajsto vprašanje) . 29

1. Obveznosti, ki jih imajo upravljavci 30

2. Obveznosti, ki jih imajo nadzorni organi 32

F. Neobstoj nujnosti odgovoriti na preostala vprašanja za predhodno odločanje in preizkusiti veljavnost Sklepa o zasebnostnem ščitu 35

1. Neobstoj nujnosti odgovorov Sodišča glede na predmet spora o glavni stvari 36

2. Razlogi proti preučitvi, ki bi jo Sodišče opravilo z vidika predmeta postopka, ki poteka pred DPC 37

G. Podredni preudarki glede učinkov in veljavnosti Sklepa o zasebnostnem ščitu 39

1. Učinki Sklepa o zasebnostnem ščitu v okviru obravnave, ki jo nadzorni organ nameni pritožbi v zvezi z zakonitostjo prenosa, temelječega na pogodbenih zaščitnih ukrepih 39

2. Veljavnost Sklepa o zasebnostnem ščitu 41

a) Pojasnila v zvezi z vsebino preizkusa veljavnosti sklepa o ustreznosti 41

1) Pogoji primerjave, ki omogočajo ocenjevanje „bistvene enakosti“ ravni varstva 41

2) Nujnost zagotoviti ustrezno raven varstva v fazi tranzita podatkov 46

3) Upoštevanje dejanskih ugotovitev Komisije in predložitvenega sodišča glede prava Združenih držav 47

4) Obseg standarda „bistvene enakosti“ 49

b) Veljavnost Sklepa o zasebnostnem ščitu glede na pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov 50

1) Obstoj posegov 50

2) Zahteva, da so posegi „predpisani z zakonom“ 52

3) Neposeganje v bistveno vsebino temeljnih pravic 54

4) Uresničevanje legitimnega cilja 56

5) Potrebnost in sorazmernost posegov 58

c) Veljavnost Sklepa o zasebnostnem ščitu glede na pravico do učinkovitega pravnega sredstva 61

1) Učinkovitost pravnih sredstev, določenih v pravu Združenih držav 62

2) Vpliv mehanizma varuha človekovih pravic na raven varstva pravice do učinkovitega pravnega sredstva 65

V. Predlog 66

I. Uvod

1. Ob neobstoju skupnih zaščitnih ukrepov na področju varstva osebnih podatkov na svetovni ravni se ob čezmejnem pretoku takih podatkov pojavlja tveganje, da bo kontinuiteta ravni varstva, zagotovljenega v Evropski uniji, pretrgana. Ker je zakonodajalec Unije želel olajšati ta pretok, hkrati pa omejiti to tveganje, je uvedel tri mehanizme, na podlagi katerih se lahko osebni podatki prenašajo iz Unije v tretjo državo.

2. Prvič, tak prenos je mogoč na podlagi sklepa, s katerim Evropska komisija ugotovi, da zadevna tretja država zagotavlja „ustrezno raven varstva“ podatkov, ki se prenašajo vanjo.[2] Drugič, če takega sklepa ni, je prenos dovoljen, če ga spremljajo „ustrezni zaščitni ukrepi“.[3] Ti zaščitni ukrepi so lahko v obliki pogodbe med izvoznikom in uvoznikom podatkov, ki vključuje standardna določila o varstvu, ki jih sprejme Komisija. Tretjič, GDPR določa nekatera odstopanja, temelječa zlasti na privolitvi posameznika, na katerega se nanašajo osebni podatki, ki omogoča prenos v tretjo državo tudi ob neobstoju sklepa o ustreznosti ali ustreznih zaščitnih ukrepov.[4]

3. Predlog za sprejetje predhodne odločbe, ki ga je vložilo High Court (višje sodišče, Irska), se nanaša na drugega od teh mehanizmov. Natančneje, nanaša se na veljavnost Sklepa 2010/87/EU,[5] s katerim je Komisija določila standardne pogodbene klavzule za nekatere vrste prenosov, glede na člene 7, 8 in 47 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina).

2 Glej člen 45 Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46 (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1; v nadaljevanju: GDPR).

3 Glej člen 46 GDPR.

4 Glej člen 49 GDPR.

5 Sklep Komisije z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES (UL 2010, L 39, str. 5), kakor je bil spremenjen z Izvedbenim sklepom Komisije (EU) 2016/2297 z dne 16. decembra 2016 (UL 2016, L 344, str. 100) (v nadaljevanju: Sklep 2010/87).

4. Ta predlog je bil vložen v okviru spora med Data Protection Commissioner (pooblaščenec za varstvo podatkov, Irska; v nadaljevanju: DPC) na eni strani ter družbo Facebook Ireland Ltd in Maximillianom Schremsom na drugi. Slednji je pri DPC vložil pritožbo glede prenosa njegovih osebnih podatkov, ki jih družba Facebook Ireland posreduje svoji matični družbi Facebook Inc. s sedežem v Združenih državah Amerike (v nadaljevanju: Združene države). DPC meni, da je obravnava te pritožbe odvisna od tega, ali je Sklep 2010/87 veljaven. V tem okviru je sprožil postopek pred predložitvenim sodiščem in ga zaprosil, naj o tem povpraša Sodišče.

5. Najprej moram navesti, da preučitev vprašanj za predhodno odločanje po mojem mnenju ni razkrila nobenega elementa, ki bi lahko vplival na veljavnost Sklepa 2010/87.

6. Poleg tega je predložitveno sodišče poudarilo nekatere dvome, v bistvu povezane z ustreznostjo ravni zaščite, ki jo zagotavljajo Združene države, glede na posege, povzročene z dejavnostmi ameriških obveščevalnih organov, v uresničevanje temeljnih pravic oseb, katerih podatki se prenašajo v to tretjo državo. S temi dvomi se posredno postavljajo pod vprašaj presoje, ki jih je Komisija v zvezi s tem opravila v Izvedbenem sklepu (EU) 2016/1250.[6] Čeprav za rešitev spora o glavni stvari ni potrebno, da Sodišče razreši to vprašanje, in čeprav mu bom posledično predlagal, naj tega ne stori, bom podredno predstavil razloge, iz katerih se sprašujem o veljavnosti tega sklepa.

7. Mojo celotno analizo bo usmerjalo iskanje ravnovesja med potrebo po tem, da se pokaže „razumn[a] mer[a] pragmatizma, da bi se omogočila povezanost s preostankom sveta“,[7] na eni strani in potrebo po potrditvi temeljnih vrednot, ki so priznane v pravnih redih Unije in njenih držav članic, zlasti v Listini, na drugi.

II. Pravni okvir

A. Direktiva 95/46/ES

8. Člen 3(2) Direktive 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov[8] je določal:

„Ta direktiva se ne uporablja za obdelavo osebnih podatkov:

– med dejavnostjo, ki ne sodi na področje uporabe zakonodaje Skupnosti, kot so tiste, opredeljene v naslovih V in VI Pogodbe o Evropski uniji, in v vsakem primeru v postopkih obdelave v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se postopek obdelave nanaša na zadeve državne varnosti) in pri dejavnostih države na področju kazenskega prava,

– […]“

6 Sklep Komisije z dne 12. julija 2016 na podlagi Direktive [95/46] o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA (UL 2016, L 207, str. 1).

7 Glej govor nekdanjega evropskega nadzornika za varstvo podatkov (ENVP) P. Hustinxa, „EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation“, str. 43, na voljo na naslovu https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

8 Direktiva Evropskega parlamenta in Sveta z dne 24. oktobra 1995 (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355), kakor je bila spremenjena z Uredbo (ES) št. 1882/2003 Evropskega parlamenta in Sveta z dne 29. septembra 2003 (UL, posebna izdaja v slovenščini, poglavje 1, zvezek 4, str. 447) (v nadaljevanju: Direktiva 95/46).

9. Člen 13(1) te direktive je določal:

„Države članice lahko sprejmejo predpise za omejitev obsega obveznosti in pravic, opredeljenih v členih 6(1), 10, 11(1), 12 in 21, kadar taka omejitev predstavlja potrebni ukrep za zaščito:

(a) državne varnosti;

(b) obrambe;

(c) javne varnosti;

(d) preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali kršitve etike za zakonsko urejene poklice;

(e) pomembnega gospodarskega ali finančnega interesa države članice ali [Unije], vključno z denarnimi, proračunskimi in davčnimi zadevami;

(f) spremljanja, pregledovanja ali urejanja, povezanega, četudi občasno, z izvajanjem javne oblasti v primerih iz (c), (d) in (e);

(g) posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih.“

10. Člen 25 navedene direktive je določal:

„1. Države članice predvidijo, da se lahko prenos osebnih podatkov, ki so v obdelavi ali so namenjeni obdelavi po dovoljenem prenosu, v tretjo državo izvede le, če brez poseganja v skladnost z nacionalnimi določbami, ki so sprejete v skladu z drugimi določbami te direktive, ta tretja država zagotovi ustrezno raven varstva.

2. Ustreznost ravni varstva, ki jo nudi tretja država, se oceni glede na vse okoliščine, ki so povezane s postopkom prenosa ali z nizom postopkov prenosa podatkov; predvsem je treba upoštevati značaj podatkov, namen in trajanje predlaganega postopka ali postopkov obdelave, državo izvora in ciljno državo, pravno ureditev, bodisi splošno ali sektorsko, ki je v veljavi v tretji državi, ter strokovne predpise in varnostne ukrepe, ki se uporabljajo v tej državi.

[…]

6. Komisija lahko v skladu s postopkom iz člena 31(2) ugotovi, da tretja država zagotavlja ustrezno raven varstva v smislu odstavka 2 tega člena zaradi svoje domače zakonodaje ali mednarodnih obveznosti, ki jih je prevzela, predvsem na podlagi zaključka pogajanj iz odstavka 5, za zaščito zasebnega življenja in temeljnih svoboščin in pravic posameznikov.

Države članice sprejmejo ukrepe, ki so potrebni za uskladitev z odločitvijo Komisije.“

11. Člen 26(2) in (4) iste direktive je določal:

„2. Brez poseganja v odstavek 1 lahko država članica dovoli prenos ali niz prenosov osebnih podatkov v tretjo državo, ki ne zagotavlja ustrezne ravni varstva v smislu člena 25(2), kadar upravljavec navede ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic; takšni zaščitni ukrepi lahko predvsem izhajajo iz ustreznih pogodbenih klavzul.

[…]

4. Kadar Komisija […] odloči, da nekatera standardna pogodbena določila nudijo zadostno zaščito iz odstavka 2, države članice sprejmejo potrebne ukrepe za uskladitev z odločitvijo Komisije.“

12. Člen 28(3) Direktive 95/46 je določal:

„Vsakemu organu se podeli predvsem:

[…]

– učinkovita pooblastila za posredovanje, kakšna so npr. dajanje mnenj pred izvajanjem postopkov obdelave v skladu s členom 20 in zagotavljanje ustrezne objave takih mnenj, odrejanje blokiranja, izbrisa ali uničenja podatkov, naložitev začasne ali dokončne prepovedi obdelave, opozarjanje ali opominjanje upravljavca ali napotitev zadeve v nacionalne parlamente ali druge politične institucije,

– […]“

B. GDPR

13. Na podlagi člena 94(1) GDPR je bila s to uredbo Direktiva 95/46/ES razveljavljena z učinkom od 25. maja 2018, ko se je začela uporabljati ta uredba v skladu z njenim členom 99(2).

14. Člen 2(2) navedene uredbe določa:

„Ta uredba se ne uporablja za obdelavo osebnih podatkov:

(a) v okviru dejavnosti zunaj področja uporabe prava Unije;

(b) s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 2 naslova V [Pogodbe EU];

[…]

(d) s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.“

15. V členu 4, točka 2, iste uredbe je „obdelava“ opredeljena kot „vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje“.

16. Člen 23 GDPR določa:

„1. Pravo Unije ali pravo države članice, ki velja za upravljavca ali obdelovalca podatkov, lahko z zakonodajnim ukrepom omeji obseg obveznosti in pravic iz členov 12 do 22 in člena 34, pa tudi člena 5, kolikor njegove določbe ustrezajo pravicam in obveznostim iz členov 12 do 22, če taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje:

(a) državne varnosti;

(b) obrambe;

(c) javne varnosti;

(d) preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

(e) drugih pomembnih ciljev v splošnem javnem interesu Unije ali države članice, zlasti pomembnega gospodarskega ali finančnega interesa Unije ali države članice […];

[…]

2. Zlasti vsak zakonodajni ukrep iz odstavka 1 vsebuje posebne določbe vsaj, kjer je ustrezno, glede:

(a) namenov obdelave ali vrst obdelave;

(b) vrst osebnih podatkov;

(c) obsega uvedenih omejitev;

(d) zaščitnih ukrepov za preprečitev zlorab ali nezakonitega dostopa ali prenosa;

(e) natančnejše ureditve upravljavca ali vrst upravljavcev;

(f) obdobij hrambe in veljavnih zaščitnih ukrepov, pri čemer se upoštevajo narava, obseg in nameni obdelave ali vrste obdelave;

(g) tveganj za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter

(h) pravice posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o omejitvi, razen če bi to posegalo v namen omejitve.“

17. Člen 44 te uredbe, naslovljen „Splošno načelo za prenose“, določa:

„Vsak prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo, se ob upoštevanju drugih določb te uredbe izvede le, če upravljavec in obdelovalec ravnata v skladu s pogoji iz tega poglavja, kar velja tudi za nadaljnje prenose osebnih podatkov iz tretje države ali mednarodne organizacije v drugo tretjo državo ali drugo mednarodno organizacijo. Vse določbe tega poglavja se uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja ta uredba.“

18. Člen 45 navedene uredbe, naslovljen „Prenosi na podlagi sklepa o ustreznosti“, določa:

„1. Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo se lahko izvede, če Komisija odloči, da zadevna tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva podatkov. Za tak prenos ni potrebno posebno dovoljenje.

2. Komisija pri ocenjevanju ustreznosti ravni varstva upošteva zlasti naslednje elemente:

(a) načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, ustrezno splošno in področno zakonodajo, tudi na področju javne varnosti, obrambe, nacionalne varnosti in kazenskega prava ter dostopa javnih organov do osebnih podatkov, pa tudi izvajanje take zakonodaje, pravila o varstvu podatkov, strokovna pravila ter varnostne ukrepe, vključno s pravili

za nadaljnji prenos osebnih podatkov v drugo tretjo državo ali mednarodno organizacijo, ki se spoštujejo v navedeni tretji državi ali mednarodni organizaciji, sodno prakso, pa tudi dejanske in izvršljive pravice ter učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo;

(b) obstoj enega ali več učinkovito delujočih neodvisnih nadzornih organov v tretji državi članici ali pristojnih za mednarodno organizacijo, ki so odgovorni za zagotavljanje in izvrševanje predpisov o varstvu podatkov, kar vključuje tudi ustrezna pooblastila za izvrševanje, za pomoč in svetovanje posameznikom, na katere se nanašajo osebni podatki, pri uresničevanju njihovih pravic ter za sodelovanje z nadzornimi organi držav članic, in

(c) mednarodne zaveze, ki jih je sprejela zadevna tretja država ali mednarodna organizacija, ali druge obveznosti, ki izhajajo iz pravno zavezujočih konvencij ali instrumentov, pa tudi iz sodelovanja tretje države ali mednarodne organizacije v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov.

3. Komisija lahko po oceni ustreznosti ravni varstva z izvedbenim aktom odloči, da tretja država, ozemlje ali en ali več določenih sektorjev v zadevni tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva v smislu odstavka 2 tega člena. V izvedbenem aktu se določi mehanizem za redni pregled, vsaj vsaka štiri leta, ki v celoti upošteva razvoj dogodkov na zadevnem področju v tretji državi ali mednarodni organizaciji. […]

4. Komisija redno spremlja razvoj dogodkov v tretjih državah in mednarodnih organizacijah, ki bi lahko vplival na izvajanje sklepov, sprejetih v skladu z odstavkom 3 tega člena, in odločitev, sprejetih na podlagi člena 25(6) Direktive [95/46].

5. Komisija v primeru, ko razpoložljive informacije, zlasti na podlagi pregleda iz odstavka 3 tega člena, pokažejo, da tretja država, ozemlje ali eden ali več določenih sektorjev v zadevni tretji državi ali mednarodna organizacija ne zagotavlja več ustrezne ravni varstva v smislu odstavka 2 tega člena, z izvedbenim aktom, v potrebnem obsegu, razveljavi, spremeni ali začasno odloži izvajanje sklepa iz odstavka 3 tega člena brez retroaktivnega učinka. […]

6. Komisija se začne posvetovati s tretjo državo ali mednarodno organizacijo, kako izboljšati stanje, zaradi katerega je bil sprejet sklep na podlagi odstavka 5.

[…]

9. Odločitve, ki jih je Komisija sprejela na podlagi člena 25(6) Direktive [95/46], ostanejo veljavne, dokler jih Komisija ne spremeni, nadomesti ali razveljavi s sklepom, sprejetim v skladu z odstavkom 3 ali 5 tega člena.“

19. Člen 46 iste uredbe, naslovljen „Prenosi, za katere se uporabljajo ustrezni zaščitni ukrepi“, določa:

„1. Kadar sklep v skladu s členom 45(3) ni sprejet, lahko upravljavec ali obdelovalec osebne podatke prenese v tretjo državo ali mednarodno organizacijo le, če je upravljavec ali obdelovalec predvidel ustrezne zaščitne ukrepe, in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva.

2. Ustrezni zaščitni ukrepi iz odstavka 1 se lahko, ne da bi bilo potrebno posebno dovoljenje nadzornih organov, zagotovijo s:

[…]

(c) standardnimi določili o varstvu podatkov, ki jih sprejme Komisija v skladu s postopkom pregleda iz člena 93(2);

[…]

5. Dovoljenja države članice ali nadzornega organa na podlagi člena 26(2) Direktive [95/46] ostanejo veljavna, dokler jih zadevni nadzorni organ ne spremeni, nadomesti ali razveljavi, če je to potrebno. Odločitve, ki jih je Komisija sprejela na podlagi člena 26(4) Direktive [95/46], ostanejo veljavne, dokler jih Komisija ne spremeni, nadomesti ali razveljavi, če je to potrebno, z odločitvijo, sprejeto v skladu z odstavkom 2 tega člena.“

20. Člen 58(2), (4) in (5) GDPR določa:

„2. Vsak nadzorni organ ima vsa naslednja popravljalna pooblastila:

(a) da izda upravljavcu ali obdelovalcu opozorilo, da bi predvidena dejanja obdelave verjetno kršila določbe te uredbe;

(b) da upravljavcu ali obdelovalcu izreče opomin, kadar so bile z dejanji obdelave kršene določbe te uredbe;

(c) da upravljavcu ali obdelovalcu odredi, naj ugodi zahtevam posameznika, na katerega se nanašajo osebni podatki, glede uresničevanja njegovih pravic na podlagi te uredbe;

(d) da upravljavcu ali obdelovalcu odredi, naj dejanja obdelave, če je to ustrezno, na določen način in v določenem roku uskladi z določbami te uredbe;

(e) da upravljavcu odredi, naj posameznika, na katerega se nanašajo osebni podatki, obvesti o kršitvi varnosti osebnih podatkov;

(f) da uvede začasno ali dokončno omejitev obdelave, vključno s prepovedjo obdelave;

[…]

(i) da glede na okoliščine posameznega primera poleg ali namesto ukrepov iz tega odstavka naloži upravno globo v skladu s členom 83;

(j) da odredi prekinitev prenosov podatkov uporabniku v tretji državi ali mednarodni organizaciji.

[…]

4. Nadzorni organ izvaja pooblastila, ki so mu dodeljena v skladu s tem členom, na podlagi ustreznih zaščitnih ukrepov, vključno z učinkovitim pravnim sredstvom in ustreznim pravnim postopkom, kot je določeno v pravu Unije in pravu države članice v skladu z Listino.

5. Vsaka država članica z zakonom določi, da ima njen nadzorni organ pooblastila, da sodne organe opozori na kršitve te uredbe in po potrebi začne sodne postopke ali v njih drugače sodeluje, da se zagotovi izvajanje določb te uredbe.“

C. Sklep 2010/87

21. Komisija je na podlagi člena 26(4) Direktive 95/46 sprejela tri odločbe oziroma sklepe, s katerimi je ugotovila, da standardne pogodbene klavzule, določene v njih, zagotavljajo ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic (v nadaljevanju: sklepi SPK).[9]

22. Med njimi je Sklep 2010/87, katerega člen 1 določa, da „[s]tandardne pogodbene klavzule iz Priloge veljajo za takšne, ki zagotavljajo ustrezne zaščitne ukrepe glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic, kakor zahteva člen 26(2) Direktive [95/46]“.

23. Člen 3 tega sklepa določa:

„V tem sklepu se uporabljajo naslednje opredelitve pojmov:

[…]

(c) ‚izvoznik podatkov‘ pomeni upravljavca, ki prenaša osebne podatke;

(d) ‚uvoznik podatkov‘ pomeni obdelovalca s sedežem v tretji državi, ki soglaša, da od izvoznika podatkov prejema osebne podatke, namenjene za obdelavo v imenu izvoznika podatkov po prenosu v skladu z njegovimi navodili in pogoji tega sklepa, ter ki ni podvržen sistemu tretje države za zagotovitev primernega varstva v smislu člena 25(1) Direktive [95/46];

[…]

(f) ‚veljavno pravo o varstvu podatkov‘ pomeni zakonodajo, ki varuje temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do zasebnosti glede obdelave osebnih podatkov, ki jo uporablja upravljavec podatkov v državi članici, v kateri je sedež izvoznika podatkov;

[…]“

24. V prvotni različici je člen 4 navedenega sklepa v odstavku 1 določal:

„Pristojni organi v državah članicah lahko ne glede na svoja pooblastila za sprejetje ukrepov za zagotovitev skladnosti z nacionalnimi predpisi, sprejetimi v skladu s poglavji II, III, V in VI Direktive [95/46], izvajajo svoja obstoječa pooblastila, da prepovejo ali začasno ustavijo pretok podatkov v tretje države zaradi varstva posameznikov pri obdelavi njihovih osebnih podatkov v primerih, če:

(a) je ugotovljeno, da zakonodaja, ki velja za uvoznika podatkov ali podobdelovalca, temu nalaga zahteve po odstopanju od veljavnega prava o varstvu podatkov, ki presegajo omejitve, potrebne v demokratični družbi, kakor jih predvideva člen 13 Direktive [95/46], če zaradi teh zahtev obstaja verjetnost precejšnjih škodljivih posledic za jamstva, zagotovljena z veljavnim pravom o varstvu podatkov in standardnimi pogodbenimi klavzulami;

(b) pristojni organ ugotovi, da uvoznik podatkov ali podobdelovalec ni spoštoval standardnih pogodbenih klavzul iz Priloge, ali

9 Odločba Komisije 2001/497/ES z dne 15. junija 2001 o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države v skladu z Direktivo [95/46] (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 26, str. 347); Odločba Komisije 2004/915/ES z dne 27. decembra 2004 o spremembi Odločbe [2001/497] glede uvedbe alternativnega sklopa standardnih pogodbenih klavzul za prenos osebnih podatkov v tretje države (UL 2004, L 385, str. 74) ter Sklep 2010/87.

(c) obstaja precejšnja verjetnost, da standardne pogodbene klavzule iz Priloge niso ali ne bodo izpolnjene ter da bi nadaljnji prenos povzročil neposredno tveganje z resno škodo za posameznike, na katere se nanašajo osebni podatki.“

25. Člen 4 Sklepa 2010/87 v sedanji različici, kot ta izhaja iz spremembe tega sklepa z Izvedbenim sklepom (EU) 2016/2297,[10] določa, da „[k]adar pristojni organi v državah članicah izvajajo svoja pooblastila v skladu s členom 28(3) Direktive [95/46], na podlagi česar pride do začasne ustavitve ali dokončne prepovedi prenosa podatkov v tretje države, da se zaščitijo posamezniki pri obdelavi njihovih osebnih podatkov, zadevna država članica nemudoma obvesti Komisijo, ta pa informacije posreduje drugim državam članicam“.

26. Priloga k Sklepu 2010/87 vsebuje sklop standardnih pogodbenih klavzul. Natančneje, klavzula 3 iz te priloge, naslovljena „Klavzula v korist tretjega“, določa:

„1. Posameznik, na katerega se nanašajo osebni podatki, lahko kot upravičena tretja stranka proti izvozniku podatkov uveljavlja to klavzulo, klavzulo 4(b) do (i), klavzulo 5(a) do (e) in (g) do (j), klavzulo 6(1) in (2), klavzulo 7, klavzulo 8(2) ter klavzule 9 do 12.

2. Posameznik, na katerega se nanašajo osebni podatki, lahko proti uvozniku podatkov uveljavlja to klavzulo, klavzulo 5(a) do (e) in (g), klavzulo 6, klavzulo 7, klavzulo 8(2) ter klavzule 9 do 12, če izvoznik podatkov dejansko izgine ali pravno preneha obstajati, razen če je pravni naslednik s pogodbo ali po zakonu prevzel vse pravice in obveznosti izvoznika podatkov; v tem primeru lahko posameznik, na katerega se nanašajo osebni podatki, navedene klavzule uveljavlja proti pravnemu nasledniku.

[…]“

27. Klavzula 4 iz navedene priloge, naslovljena „Obveznosti izvoznika podatkov“, določa:

„Izvoznik podatkov soglaša z naslednjim in zagotavlja:

(a) da se je obdelava osebnih podatkov vključno s prenosom izvajala in se bo še naprej izvajala v skladu z ustreznimi določbami veljavnega prava o varstvu podatkov (ter so bili po potrebi o tem obveščeni pristojni organi v državi članici, v kateri je sedež izvoznika podatkov) in da ne krši ustreznih predpisov te države;

(b) da je uvoznika podatkov poučil in mu bo med trajanjem obdelave osebnih podatkov še naprej dajal navodila, da naj obdeluje prenesene osebne podatke samo v imenu izvoznika podatkov ter v skladu z veljavnim pravom o varstvu podatkov in klavzulami;

(c) da bo uvoznik podatkov zagotovil zadostna jamstva glede tehničnih in organizacijskih varnostnih ukrepov iz Dodatka 2 k tej pogodbi;

(d) da so varnostni ukrepi ob upoštevanju zahtev veljavnega prava o varstvu podatkov, najsodobnejše tehnologije in stroškov njihovega izvajanja primerni za varstvo osebnih podatkov pred naključnim ali nezakonitim uničenjem ali naključno izgubo, spreminjanjem, nepooblaščenim posredovanjem ali dostopom, zlasti kadar obdelava vključuje prenos podatkov prek omrežja, ter pred katero koli drugo nezakonito obliko obdelave, in da ti ukrepi zagotavljajo raven varnosti, primerno tveganju, ki ga predstavljata obdelava in narava podatkov, ki jih je treba varovati;

(e) da bo zagotovil upoštevanje varnostnih ukrepov;

10 Sklep Komisije z dne 16. decembra 2016 o spremembi Odločbe [2001/497] in Sklepa [2010/87] o standardnih pogodbenih klavzulah za prenos osebnih podatkov v tretje države in obdelovalcem s sedežem v navedenih državah v skladu z Direktivo [95/46] (UL 2016, L 344, str. 100).

(f) da je bil oziroma bo posameznik, na katerega se nanašajo osebni podatki, v primeru prenosa posebnih vrst podatkov pred prenosom ali čim prej po njem obveščen o tem, da bi se njegovi podatki lahko prenesli v tretjo državo, ki ne zagotavlja primernega varstva v smislu Direktive [95/46];

(g) da v skladu s klavzulo 5(b) in klavzulo 8(3) vsako obvestilo, prejeto od uvoznika podatkov ali katerega koli podobdelovalca, posreduje nadzornemu organu za varstvo osebnih podatkov, če se odloči nadaljevati prenos ali odpraviti začasno ustavitev;

(h) da posameznikom, na katere se nanašajo osebni podatki, na zahtevo da na voljo izvod klavzul razen Dodatka 2 in kratek opis varnostnih ukrepov, kot tudi izvod kakršne koli pogodbe o storitvah podobdelave, ki mora biti v skladu s klavzulami sklenjena s podobdelovalcem, razen če klavzule ali pogodba vsebujejo poslovne informacije; v tem primeru se take poslovne informacije lahko izvzamejo;

(i) da podobdelovalec v primeru podobdelave obdeluje podatke v skladu s klavzulo 11 in zagotavlja najmanj enako raven varstva osebnih podatkov in pravic posameznika, na katerega se nanašajo osebni podatki, kot jo zagotavlja uvoznik podatkov v skladu s klavzulami; ter

(j) da bo zagotovil upoštevanje klavzule 4(a) do (i).“

28. Klavzula 5 iz iste priloge, naslovljena „Obveznosti uvoznika podatkov([1])“, določa:

„Uvoznik podatkov soglaša z naslednjim in zagotavlja:

(a) da obdeluje osebne podatke samo v imenu izvoznika podatkov ter v skladu z njegovimi navodili in klavzulami; če jih iz kakršnih koli razlogov ne more upoštevati, soglaša, da o tem nemudoma obvesti izvoznika podatkov, ki je v tem primeru upravičen začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe;

(b) da nima razloga za domnevo, da mu zakonodaja, ki velja zanj, preprečuje izpolnjevanje navodil izvoznika podatkov in obveznosti iz pogodbe, ter da bo v primeru spremembe te zakonodaje, ki bo verjetno imela znaten negativen učinek na jamstva in obveznosti iz klavzul, to spremembo sporočil izvozniku podatkov takoj, ko bo zanjo izvedel, izvoznik podatkov pa je v tem primeru upravičen začasno ustaviti prenos podatkov in/ali odstopiti od pogodbe;

(c) da je pred obdelavo prenesenih osebnih podatkov izvedel tehnične in organizacijske varnostne ukrepe iz Dodatka 2;

(d) da bo izvoznika podatkov nemudoma obvestil o:

  (i) vseh pravno zavezujočih zahtevah organa kazenskega pregona za posredovanje osebnih podatkov, razen če je to kako drugače prepovedano, na primer s prepovedjo po kazenski zakonodaji zaradi ohranjanja zaupnosti kazenske preiskave;

  (ii) vsakem naključnem ali nepooblaščenem dostopu; ter

  (iii) vseh zahtevah, prejetih neposredno od posameznikov, na katere se nanašajo osebni podatki, ne da bi nanje odgovoril, razen če dobi za to pooblastilo;

(e) da nemudoma in ustrezno obravnava vse poizvedbe izvoznika podatkov v zvezi z obdelavo prenesenih osebnih podatkov ter upošteva nasvete nadzornega organa glede obdelave prenesenih podatkov;

(f) da na zahtevo izvoznika podatkov predloži svojo opremo za obdelavo podatkov v pregled dejavnosti obdelave, zajetih v klavzulah, ki ga izvede izvoznik podatkov ali inšpekcijski organ, sestavljen iz neodvisnih članov, ki so primerno strokovno usposobljeni ter zavezani k molčečnosti, izbere pa jih izvoznik podatkov, po potrebi v dogovoru z nadzornim organom;

[…]“

29. V opombi 1, na katero se sklicuje naslov klavzule 5 iz Priloge k Sklepu 2010/87, je navedeno:

„Obvezne zahteve nacionalne zakonodaje, veljavne za uvoznika podatkov, ki ne presegajo tega, kar je potrebno v demokratični družbi na podlagi enega od interesov iz člena 13(1) Direktive [95/46], to je, če predstavljajo ukrep, potreben za zaščito nacionalne varnosti, obrambe, javne varnosti, preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ali etičnih kršitev za zakonsko urejene poklice, pomembnega gospodarskega ali finančnega interesa države, varstva posameznika, na katerega se nanašajo osebni podatki, ali pravic in svoboščin drugih, niso v nasprotju s standardnimi pogodbenimi klavzulami. Nekateri primeri takšnih obveznih zahtev, ki ne presegajo tega, kar je potrebno v demokratični družbi, so med drugim mednarodno priznane sankcije, zahteve za prijavo davka ali zahteve za poročanje o ukrepih na področju boja proti pranju denarja.“

30. Klavzula 6 iz te priloge, naslovljena „Odgovornost“, določa:

1. Stranki soglašata, da je vsak posameznik, na katerega se nanašajo osebni podatki, ki je zaradi kršitve obveznosti iz klavzule 3 ali klavzule 11 s strani stranke ali podobdelovalca utrpel škodo, upravičen od izvoznika podatkov prejeti odškodnino za utrpelo škodo.

2. Če posameznik, na katerega se nanašajo osebni podatki, zaradi kršitve katere koli obveznosti iz klavzule 3 ali klavzule 11 s strani uvoznika podatkov ali njegovega podobdelovalca ne more uveljavljati odškodninskega zahtevka v skladu z odstavkom 1 zoper izvoznika podatkov, ker je izvoznik podatkov dejansko izginil, pravno prenehal obstajati ali pa postal insolventen, uvoznik podatkov soglaša, da lahko posameznik zahtevek uveljavlja zoper njega namesto zoper izvoznika podatkov, razen če je kak pravni naslednik s pogodbo ali po zakonu prevzel vse pravne obveznosti izvoznika podatkov; v tem primeru lahko posameznik, na katerega se nanašajo osebni podatki, uveljavlja svoj zahtevek zoper pravnega naslednika.

[…]“

31. Klavzula 7 iz navedene priloge, naslovljena „Mediacija in pristojnost“, določa:

„1. Če posameznik, na katerega se nanašajo osebni podatki, na podlagi klavzul zoper uvoznika podatkov uveljavlja pravice kot upravičena tretja stranka in/ali odškodninski zahtevek, uvoznik podatkov soglaša, da bo sprejel odločitev posameznika, da:

(a) spor predloži v mediacijo, ki jo izvede neodvisna oseba ali, kjer je primerno, nadzorni organ;

(b) spor predloži sodiščem v državi članici, v kateri je sedež izvoznika podatkov.

2. Stranki soglašata, da izbira posameznika, na katerega se nanašajo osebni podatki, ne vpliva na njegove materialne ali procesne pravice za uveljavljanje pravnih sredstev v skladu z drugimi določbami nacionalnega ali mednarodnega prava.“

32. Klavzula 9 iz iste priloge, naslovljena „Pravo, ki se uporablja“, določa, da za standardne pogodbene klavzule velja pravo države članice, v kateri je sedež izvoznika podatkov.

D. Sklep o zasebnostnem ščitu

33. Komisija je na podlagi člena 25(6) Direktive 95/46 zaporedoma sprejela odločbo in sklep, s katerima je ugotovila, da Združene države zagotavljajo ustrezno raven varstva osebnih podatkov, prenesenih v podjetja s sedežem v Združenih državah, ki so z uporabo postopka samocertificiranja izjavila, da bodo spoštovala načela, določena v tej odločbi oziroma sklepu.

34. Najprej je Komisija sprejela Odločbo 2000/520/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogosteje zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA.[11] Sodišče je v sodbi z dne 6. oktobra 2015, Schrems[12], to odločbo razglasilo za neveljavno.

35. Zaradi te sodbe je Komisija nato sprejela Sklep o zasebnostnem ščitu.

36. Člen 1 tega sklepa določa:

„1. Za namene člena 25(2) Direktive [95/46] ZDA zagotavljajo ustrezno raven varstva osebnih podatkov, ki se v okviru zasebnostnega ščita EU-ZDA prenašajo iz Unije organizacijam v ZDA.

2. Zasebnostni ščit EU-ZDA sestavljajo načela, ki jih je 7. julija 2016 izdalo Ministrstvo za trgovino ZDA, kakor so navedena v Prilogi II, ter uradna zagotovila in zaveze iz dokumentov, navedenih v prilogah I in III–VII.

3. Za namene odstavka 1 se osebni podatki prenašajo v okviru zasebnostnega ščita EU-ZDA, kadar se prenašajo iz Unije organizacijam v ZDA, ki so vključene na ‚seznam zasebnostnega ščita', ki ga vodi in objavlja Ministrstvo za trgovino ZDA, v skladu s členoma I in III načel iz Priloge II."

37. Priloga III A k navedenemu sklepu, naslovljena „Mehanizem varuha človekovih pravic na področju zasebnostnega ščita EU-ZDA v zvezi z obveščevalno dejavnostjo SIGINT" in priložena dopisu Johna Kerryja, tedanjega Secretary of State (zunanji minister, Združene države), z dne 7. julija 2016, vsebuje memorandum, v katerem je opisan nov postopek mediacije pred „višjim koordinatorjem za mednarodno diplomacijo v informacijski tehnologiji" (v nadaljevanju: varuh človekovih pravic), ki ga imenuje zunanji minister.

38. V skladu s tem memorandumom je bil ta postopek uveden za „lajšanj[e] obravnave zahtev v zvezi z dostopom za potrebe nacionalne varnosti do podatkov, prenesenih iz [Unije] v Združene države v skladu z zasebnostnim ščitom, standardnimi pogodbenimi klavzulami, zavezujočimi poslovnimi pravili, odstopanji ali morebitnimi prihodnjimi odstopanji po ustaljenih poteh v skladu z veljavnimi zakoni in politiko Združenih držav, ter odgovor na te zahteve".

III. Spor o glavni stvari, vprašanja za predhodno odločanje in postopek pred Sodiščem

39. M. Schrems, avstrijski državljan, ki prebiva v Avstriji, je uporabnik družabnega omrežja Facebook. Vsi uporabniki tega družabnega omrežja, ki prebivajo na ozemlju Unije, morajo ob registraciji skleniti pogodbo z družbo Facebook Ireland, ki je hčerinska družba družbe Facebook Inc. s sedežem v Združenih državah. Osebni podatki teh uporabnikov se v celoti ali delno prenesejo na strežnike družbe Facebook Inc., ki so na ozemlju Združenih držav in na katerih se obdelujejo.

11 Odločba z dne 26. julija 2000 po Direktivi [95/46] (UL, posebna izdaja v slovenščini, poglavje 16, zvezek 1, str. 119, v nadaljevanju: Odločba o varnem pristanu).

12 C-362/14 (EU:C:2015:650, v nadaljevanju: sodba Schrems).

40. M. Schrems je 25. junija 2013 pri DPC vložil pritožbo, s katero je v bistvu zahteval, naj ta družbi Facebook Ireland prepove prenašanje osebnih podatkov, ki se nanašajo nanj, v Združene države. V pritožbi je trdil, da veljavno pravo in praksa v tej tretji državi ne zagotavljata zadostnega varstva osebnih podatkov, ki se hranijo na njenem ozemlju, pred posegi, izhajajočimi iz dejavnosti nadzora, ki jih izvajajo javni organi. M. Schrems se je glede tega skliceval na razkritja Edwarda Snowdna v zvezi z dejavnostmi obveščevalnih služb Združenih držav, zlasti National Security Agency (NSA) (agencija za nacionalno varnost, Združene države).

41. Ta pritožba je bila med drugim zavržena z obrazložitvijo, da je treba vsa vprašanja glede ustreznosti varstva v Združenih državah reševati v skladu z Odločbo o varnem pristanu. V navedeni odločbi je Komisija ugotovila, da ta tretja država zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih v podjetja na njenem ozemlju, ki spoštujejo načela, določena v navedeni odločbi.

42. M. Schrems je zoper odločbo o zavrženju njegove pritožbe vložil tožbo pri High Court (višje sodišče). To sodišče je presodilo, da M. Schrems formalno sicer ne izpodbija Odločbe o varnem pristanu, vendar s svojo pritožbo v bistvu izpodbija zakonitost sistema, uvedenega s to odločbo. V teh okoliščinah je navedeno sodišče Sodišču predložilo vprašanji, s katerima je v bistvu želelo izvedeti, ali organe držav članic, odgovorne za varstvo podatkov (v nadaljevanju: nadzorni organi), pri odločanju o pritožbi v zvezi z varstvom pravic in svoboščin posameznika glede osebnih podatkov, ki se nanašajo nanj in so bili preneseni v tretjo državo, zavezujejo ugotovitve Komisije o ustreznosti ravni varstva, ki jo zagotavlja ta tretja država, podane na podlagi člena 25(6) Direktive 95/46, medtem ko pritožnik izpodbija te ugotovitve.

43. Potem ko je Sodišče v točkah 51 in 52 sodbe Schrems odločilo, da je odločba o ustreznosti za nadzorne organe zavezujoča, dokler ni razglašena za neveljavno, je v točkah 63 in 65 te sodbe navedlo:

„63. […] [N]acionalni nadzorni organ [mora], kadar mu posameznik, katerega osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, na katero se nanaša odločba Komisije, sprejeta na podlagi člena 25(6) Direktive 95/46, predloži zahtevo v zvezi z varstvom svojih pravic in svoboščin glede obdelave teh podatkov in v tej zahtevi […] izpodbija skladnost te odločbe z varstvom zasebnega življenja ter temeljnih svoboščin in pravic, navedeno zahtevo preučiti z vso potrebno skrbnostjo.

[…]

65. [Če] navedeni organ […] meni, da so očitki [tega posameznika] utemeljeni, [mora] v skladu s členom 28(3), prvi pododstavek, tretja alinea, Direktive 95/46, zlasti ob upoštevanju člena 8(3) Listine, imeti možnost sodelovati v sodnih postopkih. V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki zadevnemu nacionalnemu nadzornemu organu omogočajo, da očitke, ki jih šteje za utemeljene, predloži nacionalnim sodiščem, da bi ta, če bi prav tako kot ta organ dvomila o veljavnosti odločbe Komisije, sprožila postopek predhodnega odločanja za preizkus veljavnosti navedene odločbe.“

44. Sodišče je v navedeni sodbi tudi preizkusilo veljavnost Odločbe o varnem pristanu glede na zahteve, ki izhajajo iz Direktive 95/46, razlagane ob upoštevanju Listine. Po tem preizkusu je to odločbo razglasilo za neveljavno. [13]

45. Zaradi sodbe Schrems je predložitveno sodišče odpravilo odločbo, s katero je DPC zavrgel pritožbo M. Schremsa, in zadevo vrnilo DPC v preučitev. Ta je začel preiskavo in M. Schremsa pozval, naj preoblikuje svojo pritožbo ob upoštevanju razglasitve neveljavnosti Odločbe o varnem pristanu.

13 Glej sodbo Schrems (točka 106).

46. M. Schrems je zato od družbe Facebook Ireland zahteval, naj opredeli pravne podlage, na katerih temeljijo prenosi osebnih podatkov uporabnikov družabnega omrežja Facebook iz Unije v Združene države. Družba Facebook Ireland se je, ne da bi opredelila vse pravne podlage, na katere se opira, sklicevala na sporazum o prenosu in obdelavi podatkov (*data transfer processing agreement*), ki je bil sklenjen med njo in družbo Facebook Inc. ter se uporablja od 20. novembra 2015, in omenila Sklep 2010/87.

47. M. Schrems v preoblikovani pritožbi po eni strani trdi, da klavzule, ki jih vsebuje ta sporazum, niso v skladu s standardnimi pogodbenimi klavzulami iz Priloge k Sklepu 2010/87. Po drugi strani M. Schrems zatrjuje, da te standardne pogodbene klavzule nikakor ne morejo biti podlaga za prenos osebnih podatkov, ki se nanašajo nanj, v Združene države. Tako naj bi bilo zato, ker ameriško pravo družbi Facebook Inc. nalaga, da osebne podatke svojih uporabnikov daje na voljo ameriškim organom, kot sta NSA in Federal Bureau of Investigation (FBI) (zvezni preiskovalni urad, Združene države), v okviru programov nadzora, ki naj bi ovirali uresničevanje pravic, zagotovljenih s členi 7, 8 in 47 Listine. M. Schrems navaja, da posameznikom, na katere se nanašajo osebni podatki, nobeno pravno sredstvo ne omogoča, da uveljavljajo svoji pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov. V teh okoliščinah M. Schrems od DPC zahteva, naj prekine ta prenos na podlagi člena 4 Sklepa 2010/87.

48. Družba Facebook Ireland je v okviru preiskave DPC priznala, da še naprej prenaša osebne podatke uporabnikov družabnega omrežja Facebook, ki prebivajo v Uniji, v Združene države in da se pri tem v veliki meri opira na standardne pogodbene klavzule iz Priloge k Sklepu 2010/87.

49. Namen preiskave DPC je bil ugotoviti, prvič, ali Združene države zagotavljajo ustrezno varstvo osebnih podatkov državljanov Unije, in drugič, če ne, ali sklepi SPK vključujejo ustrezne zaščitne ukrepe glede varstva temeljnih pravic in svoboščin teh državljanov.

50. V zvezi s tem je DPC v osnutku odločbe (*draft decision*) začasno presodil, da ameriško pravo ne zagotavlja učinkovitih pravnih sredstev v smislu člena 47 Listine državljanom Unije, katerih podatki se prenašajo v Združene države, kjer obstaja tveganje, da jih bodo ameriške agencije zaradi nacionalne varnosti obdelovale na način, nezdružljiv s členoma 7 in 8 Listine. Zaščitni ukrepi, ki jih določajo klavzule iz prilog k sklepom SPK, naj ne bi odpravljali te vrzeli, ker niso zavezujoči za organe ali agencije Združenih držav in ker so z njimi posameznikom, na katere se nanašajo osebni podatki, podeljene le pogodbene pravice zoper izvoznika in/ali uvoznika podatkov.

51. V teh okoliščinah je DPC menil, da ne more odločiti o pritožbi M. Schremsa, ne da bi Sodišče preizkusilo veljavnost sklepov SPK. Zato je DPC v skladu s tem, kar se zahteva v točki 65 sodbe Schrems, začel postopek pred predložitvenim sodiščem, da bi to, če bi se strinjalo z dvomi DPC, Sodišču predložilo predlog za sprejetje predhodne odločbe glede veljavnosti teh sklepov.

52. Dovoljenje, da intervenirajo pred predložitvenim sodiščem, so dobile vlada Združenih držav ter organizacije Electronic Privacy Information Centre (EPIC), Business Software Alliance (BSA) in Digitaleurope.

53. Da bi High Court (višje sodišče) ugotovilo, ali se strinja z dvomi glede veljavnosti sklepov SPK, ki jih je izrazil DPC, je sprejelo dokaze, ki so jih predložile stranke spora, ter tem strankam in intervenientkam omogočilo, da predstavijo svoje trditve. Zlasti določbe prava Združenih držav so predstavili izvedenci. V irskem pravu se tuje pravo šteje za dejansko vprašanje, ki ga je treba z dokazi enako dokazati kot vsa druga dejstva. Na podlagi teh dokazov je predložitveno sodišče presodilo določbe prava Združenih držav, ki omogočajo izvajanje nadzora vladnim organom in agencijam, delovanje dveh javno priznanih programov nadzora („PRISM“ in „Upstream“), različna sredstva, ki so

na voljo posameznikom, katerih pravice so bile kršene z ukrepi nadzora, ter sistemske zaščitne ukrepe in nadzorne mehanizme. To sodišče je ugotovitve te presoje zapisalo v sodbi z dne 3. oktobra 2017, priloženi predložitvenemu sklepu (v nadaljevanju: sodba High Court (višje sodišče) z dne 3. oktobra 2017).

54. V tej sodbi je predložitveno sodišče med pravnimi podlagami, s katerimi je ameriškim obveščevalnim službam dovoljeno prestrezanje tujih komunikacij, omenilo člen 702 Foreign Intelligence and Surveillance Act (FISA) (zakon o nadzoru tujih obveščevalnih podatkov) in Executive Order 12333 (predsedniška odredba št. 12333; v nadaljevanju EO 12333).

55. Glede na ugotovitve iz navedene sodbe člen 702 FISA omogoča, da Attorney General (generalni državni tožilec, Združene države) in Director of National Intelligence (DNI) (direktor nacionalnih obveščevalnih služb, Združene države) skupaj za eno leto in zaradi pridobitve tujih obveščevalnih podatkov dovolita nadzor oseb, ki niso ameriški državljani in ne prebivajo stalno v Združenih državah (tako imenovane „neameriške osebe“), kadar je mogoče razumno šteti, da so te osebe zunaj ozemlja Združenih držav.[14] Kot določa FISA, pojem „tuji obveščevalni podatki“ pomeni podatke, povezane s sposobnostjo vlade, da zagotovi zaščito pred tujimi napadi, terorizmom in širjenjem orožja za množično uničevanje, pa tudi z vodenjem zunanjih zadev Združenih držav.[15]

56. Ta letna dovoljenja ter postopke, s katerimi sta urejeni izbira cilja v smislu osebe, ki jo je treba nadzirati, in obdelava („zmanjšanje količine“) zbranih podatkov,[16] mora odobriti Foreign Intelligence Surveillance Court (FISC) (sodišče za nadzor tujih obveščevalnih podatkov, Združene države). Medtem ko je za „tradicionalni“ nadzor, ki se izvaja na podlagi drugih določb FISA, potrebno, da se izkaže „utemeljen razlog“, na podlagi katerega je mogoče sumiti, da nadzorovane osebe pripadajo tuji sili ali so njeni agenti, dejavnosti nadzora, ki se izvajajo v skladu s členom 702 FISA, niso pogojene niti z izkazanostjo takega „utemeljenega razloga“ niti s tem, da FISC odobri izbiro določenih oseb kot ciljev. Poleg tega se v skladu z ugotovitvami predložitvenega sodišča postopki za zmanjšanje količine podatkov ne uporabljajo za neameriške osebe, ki so zunaj Združenih držav.

57. Ko v praksi FISC odobri dovoljenje, NSA pošlje ponudnikom elektronskih komunikacijskih storitev s sedežem v Združenih državah odredbe, te pa vsebujejo iskalna merila, imenovana „izbirniki“, ki se navezujejo na ciljne osebe (kot so telefonske številke ali elektronski naslovi). Ti ponudniki so nato podatke, ki ustrezajo izbirnikom, zavezani posredovati agenciji NSA in morajo varovati tajnost odredb, ki so jih prejeli. Zadevni ponudniki lahko pri FISC vložijo zahtevek, naj se odredba NSA spremeni ali odpravi. Zoper odločbo FISC je dovoljena pritožba pri Foreign Intelligence Surveillance Court of Review (FISCR) (drugostopenjsko sodišče za nadzor tujih obveščevalnih podatkov, Združene države).

58. High Court (višje sodišče) je ugotovilo, da je člen 702 FISA pravna podlaga za programa PRISM in Upstream.

59. V okviru programa PRISM so ponudniki elektronskih komunikacijskih storitev zavezani agenciji NSA predložiti vse komunikacije, poslane „z“ izbirnika ali „na“ izbirnik, ki ga je sporočila ta agencija. Del teh komunikacij naj bi bil poslan uradu FBI in Central Intelligence Agency (CIA) (centralna obveščevalna agencija, Združene države). V okviru tega programa naj bi bilo v letu 2015 nadzorovanih 94.386 oseb, vlada Združenih držav pa naj bi v letu 2011 pridobila več kot 250 milijonov komunikacij.

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

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

16 Predložitveno sodišče je ugotovilo, da postopki za izbiro ciljev zadevajo to, kako izvršilna oblast odloči, da je nekega posameznika mogoče razumno šteti za neameriško osebo, ki je zunaj Združenih držav, in da izbira tega posameznika kot cilja lahko pripelje do pridobitve tujih obveščevalnih podatkov. Postopki za zmanjšanje količine podatkov zajemajo pridobivanje, hrambo in razširjanje vseh nejavnih podatkov o ameriški osebi, pridobljenih na podlagi člena 702 FISA.

60. Program Upstream temelji na obvezni pomoči podjetij, ki upravljajo „hrbtenico“ – in sicer mrežo kablov, stikal in usmerjevalnikov – po kateri prehajajo telefonske in internetne komunikacije. Ta podjetja morajo agenciji NSA dovoliti, da kopira in filtrira tokove internetnega prometa, da pridobi komunikacije, poslane „z“ izbirnika, „na“ izbirnik oziroma „v zvezi z“ izbirnikom, ki je naveden v odredbi te agencije. Komunikacije „v zvezi z“ izbirnikom pomenijo tiste, v katerih je ta izbirnik omenjen, ne da bi bila neameriška oseba, na katero se navedeni izbirnik navezuje, v njih nujno udeležena. Čeprav iz mnenja FISC z dne 26. aprila 2017 izhaja, da od tega datuma ameriška vlada ne zbira in ne pridobiva več komunikacij „v zvezi z“ izbirnikom, v tem mnenju ni navedeno, da je NSA prenehala kopirati in filtrirati tokove komunikacij, ki prehajajo skozi njene nadzorne naprave. Program Upstream naj bi tako vključeval dostop NSA do metapodatkov in do vsebine komunikacij. NSA naj bi od leta 2011 v okviru programa Upstream zbrala približno 26,5 milijona komunikacij na leto, vendar naj bi bil to le majhen del komunikacij, ki so predmet postopka filtriranja, ki se izvaja na podlagi tega programa.

61. Poleg tega je glede na ugotovitve High Court (višje sodišče) z EO 12333 dovoljen nadzor elektronskih komunikacij zunaj ozemlja Združenih držav s tem, da je na podlagi te predsedniške odredbe za pridobivanje tujih obveščevalnih podatkov mogoče dostopati do podatkov, ki so bodisi „v tranzitu“ do tega ozemlja bodisi „prehajajo“ prek tega ozemlja, ne da bi bili namenjeni za obdelavo na njem, ter zbirati in hraniti te podatke. V EO 12333 je pojem „tuji obveščevalni podatki“ opredeljen tako, da zajema informacije v zvezi z zmogljivostmi, nameni ali dejavnostmi tujih vlad, tujih organizacij ali tujih oseb.[17]

62. Z EO 12333 naj bi bila NSA pooblaščena dostopati do podmorskih kablov na dnu Atlantskega oceana, po katerih se podatki prenašajo iz Unije v Združene države, preden ti podatki prispejo v Združene države in zato zanje začnejo veljati določbe FISA. Vendar ni nobenega dokaza o kakršnem koli programu, ki bi se izvajal na podlagi te predsedniške odredbe.

63. Čeprav EO 12333 določa omejitve glede zbiranja, hrambe in razširjanja podatkov, se te omejitve ne uporabljajo za neameriške osebe. Te so deležne samo zaščitnih ukrepov, določenih v Presidential Policy Directive 28 (predsedniška politična direktiva št. 28; v nadaljevanju: PPD 28), ki se uporablja za vse dejavnosti zbiranja in uporabe tujih obveščevalnih podatkov SIGINT. PPD 28 določa, da je spoštovanje zasebnega življenja sestavni del premislekov, ki se upoštevajo pri načrtovanju teh dejavnosti, da mora biti zbiranje namenjeno samo pridobivanju tujih obveščevalnih in protiobveščevalnih podatkov ter da morajo biti navedene dejavnosti „kolikor mogoče prilagojene“.

64. Po navedbah predložitvenega sodišča dejavnosti NSA, ki temeljijo na EO 12333, ki jo lahko predsednik Združenih držav kadar koli spremeni ali razveljavi, niso urejene z zakonom, niso predmet sodnega nadzora in zoper njih ni mogoče vložiti pravnega sredstva.

65. Na podlagi teh ugotovitev to sodišče presoja, da Združene države izvajajo množično in neselektivno obdelavo osebnih podatkov, zaradi katere bi bili posamezniki, na katere se nanašajo osebni podatki, lahko izpostavljeni tveganju kršitve pravic, ki so jim podeljene s členoma 7 in 8 Listine.

66. Še več, navedeno sodišče navaja, da državljani Unije nimajo dostopa do istih pravnih sredstev zoper nezakonito obdelavo njihovih osebnih podatkov, ki jo izvajajo ameriški organi, kot ameriški državljani. Četrti amandma ustave Združenih držav, ki naj bi bil najpomembnejša zaščita pred nezakonitim nadzorom, naj se ne bi uporabljal za državljane Unije, ki nimajo znatne prostovoljne povezave z Združenimi državami. Čeprav imajo državljani Unije vseeno na voljo nekatera druga pravna sredstva, naj bi se ta srečevala s precejšnjimi ovirami.

17 EO 12333, točka 3.5(e).

67. Natančneje, s členom III ustave Združenih držav je vsako pravno sredstvo pred zveznimi sodišči pogojeno s tem, da zadevna oseba izkaže procesno upravičenje (*standing*). Za procesno upravičenje je zlasti potrebno, da ta oseba dokaže, da je utrpela dejansko škodo, ki je na eni strani konkretna in se na njo posamično nanaša, na drugi strani pa je obstoječa ali neizbežna. Ob sklicevanju, med drugim, na sodbo Supreme Court of the United States (vrhovno sodišče Združenih držav), Clapper v. Amnesty International US,[18] predložitveno sodišče meni, da je ta pogoj v praksi izredno težko izpolniti zlasti zaradi neobstoja kakršne koli obveznosti obveščanja posameznikov, na katere se nanašajo osebni podatki, o ukrepih nadzora, sprejetih zoper njih.[19] Poleg tega naj bi bilo treba za del pravnih sredstev, ki so na voljo državljanom Unije, izpolnjevati druge omejujoče pogoje, kot je nujnost izkazati premoženjsko škodo. Uveljavljanje nekaterih pravnih sredstev naj bi ovirali tudi suverena imuniteta, priznana obveščevalnim agencijam, in zaupnost zadevnih podatkov.[20]

68. High Court (višje sodišče) poleg tega omenja različne mehanizme za nadzor in spremljanje dejavnosti obveščevalnih agencij.

69. Med njimi je, prvič, mehanizem, s katerim FISC letno potrjuje programe, ki temeljijo na členu 702 FISA, v okviru katerega pa to sodišče ne odobri posameznih izbirnikov. Poleg tega zbiranje tujih obveščevalnih podatkov na podlagi EO 12333 ni predmet nobenega predhodnega sodnega nadzora.

70. Drugič, predložitveno sodišče se sklicuje na več mehanizmov za izvensodni nadzor obveščevalnih dejavnosti. Zlasti omenja vlogo, ki jo imajo Inspectors General (generalni inšpektorji, Združene države), ki so znotraj vsake obveščevalne agencije odgovorni za nadzor dejavnosti nadzora. Poleg tega Privacy and Civil Liberties Oversight Board (PCLOB) (nadzorni odbor za zasebnost in državljanske svoboščine, Združene države), neodvisna agencija v okviru izvršilne oblasti, prejema poročila oseb, ki so znotraj vsake agencije imenovane kot uradniki za državljanske pravice ali varstvo zasebnosti (*civil liberties or privacy officers*). PCLOB redno pripravlja poročila, namenjena parlamentarnim odborom in predsedniku države. Zadevne agencije morajo s primeri, ki se nanašajo na neupoštevanje pravil in postopkov, ki urejajo zbiranje tujih obveščevalnih podatkov, seznaniti med drugim DNI. O teh primerih se poroča tudi sodišču FISC. Kongres Združenih držav je prek obveščevalnih odborov predstavniškega doma in senata prav tako odgovoren za nadzor dejavnosti v zvezi s tujimi obveščevalnimi podatki.

71. Vendar High Court (višje sodišče) poudarja bistveno razliko med pravili, katerih namen je zagotoviti, da se podatki pridobivajo zakonito in se po pridobitvi ne zlorabljajo, na eni strani ter pravnimi sredstvi, ki so na voljo, če se ta pravila kršijo, na drugi. Varstvo temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, naj bi bilo zagotovljeno, le če jim učinkovita pravna sredstva omogočajo, da uveljavljajo svoje pravice v primeru neupoštevanja navedenih pravil.

72. V teh okoliščinah predložitveno sodišče meni, da so trditve DPC, v skladu s katerimi omejitve, ki jih ameriško pravo določa za pravico oseb, katerih podatki se prenašajo iz Unije, do pravnega sredstva, ne spoštujejo bistvene vsebine pravice, zagotovljene v členu 47 Listine, in vsekakor pomenijo nesorazmerne posege v uresničevanje te pravice, utemeljene.

18 133 S.Ct. 1138 (2013).

19 Vendar je predložitveno sodišče ugotovilo, da načelo, v skladu s katerim ni treba obvestiti osebe, na katero se nanaša ukrep nadzora, pozna izjemo, kadar skuša ameriška vlada podatke, zbrane na podlagi člena 702 FISA, uporabiti zoper to osebo v okviru kazenskega ali upravnega postopka.

20 Predložitveno sodišče je zlasti poudarilo, da so bile sicer z Judicial Redress Act (JRA) (zakon o sodnem varstvu) na državljane Unije razširjene določbe Privacy Act (zakon o varstvu zasebnosti), ki omogoča dostop fizičnih oseb do podatkov, ki se nanašajo nanje in jih hranijo nekatere agencije, v povezavi z nekaterimi tretjimi državami, vendar agencije NSA ni med agencijami, ki so imenovane v okviru JRA.

73. Po mnenju High Court (višje sodišče) dejstvo, da je vlada Združenih držav uvedla mehanizem varuha človekovih pravic, opisan v Sklepu o zasebnostnem ščitu, ne omaje te presoje. Potem ko je to sodišče poudarilo, da je ta mehanizem na voljo državljanom Unije, ki na razumni podlagi ocenjujejo, da so bili njihovi podatki preneseni v skladu s sklepi SPK,[21] je opozorilo, da varuh človekovih pravic ni sodišče, ki bi izpolnjevalo zahteve iz člena 47 Listine, in zlasti ni neodvisen od izvršilne oblasti.[22] Navedeno sodišče tudi dvomi, da posredovanje varuha človekovih pravic, čigar odločb ni mogoče izpodbijati, pomeni učinkovito pravno sredstvo. To posredovanje namreč osebam, katerih podatki so bili nezakonito zbrani, obdelani ali izmenjani, ne omogoča, da pridobijo odškodnino ali dosežejo odreditev prenehanja nezakonitih dejanj, ker varuh človekovih pravic niti ne potrdi niti ne zanika, da je bil neki pritožnik predmet ukrepa elektronskega nadzora.

74. Potem ko je tako predstavilo svoje pomisleke glede bistvene enakosti med zaščitnimi ukrepi, določenimi z ameriškim pravom, in zahtevami, ki izhajajo iz členov 7, 8 in 47 Listine, je predložitveno sodišče izrazilo dvome glede tega, ali standardne pogodbene klavzule iz sklepov SPK – ki po naravi za ameriške organe niso zavezujoče – vseeno lahko zagotavljajo varstvo temeljnih pravic posameznikov, na katere se nanašajo osebni podatki. To sodišče je ugotovilo, da se strinja z dvomi DPC glede veljavnosti teh sklepov.

75. V zvezi s tem predložitveno sodišče zlasti meni, da člen 28(3) Direktive 95/46, na katerega se sklicuje člen 4 Sklepa 2010/87, s tem, da nadzornim organom priznava pooblastilo, da prekinejo ali prepovejo prenose, ki temeljijo na standardnih pogodbenih klavzulah iz tega sklepa, ne zadostuje za odpravo teh dvomov. Poleg tega, da je to pooblastilo po njegovem mnenju zgolj diskrecijske narave, se predložitveno sodišče glede na točko 11 obrazložitve Sklepa 2010/87 sprašuje o možnosti izvrševanja navedenega pooblastila, kadar ugotovljene pomanjkljivosti ne zadevajo posameznega in izjemnega primera, temveč so splošne in sistemske.[23] Meni tudi, da bi tveganje, da bodo v različnih državah članicah sprejete razhajajoče se odločitve, lahko nasprotovalo temu, da se ugotovitev takih pomanjkljivosti zaupa nadzornim organom.

76. V teh okoliščinah je High Court (višje sodišče) s sklepom z dne 4. maja 2018,[24] ki je na Sodišče prispel 9. maja 2018, prekinilo odločanje in Sodišču v predhodno odločanje predložilo ta vprašanja:

„1. Ali v okoliščinah, kadar zasebno podjetje iz države članice [Unije] prenese osebne podatke zasebnemu podjetju v tretji državi v komercialne namene v skladu s Sklepom [2010/87] in jih lahko v tretji državi nadalje obdelujejo njeni organi zaradi nacionalne varnosti, pa tudi zaradi kazenskega pregona in vodenje zunanjih zadev tretje države, pravo [Unije,] vključno z Listino […][,] velja za prenos podatkov ne glede na določbe člena 4(2) PEU v zvezi z nacionalno varnostjo in določbe prve alinee člena 3(2) Direktive [95/46] v zvezi z javno varnostjo, obrambo in varnostjo države?

21 Predložitveno sodišče se v zvezi s tem sklicuje na Prilogo III A k Sklepu o zasebnostnem ščitu (glej točki 37 in 38 teh sklepnih predlogov).

22 Predložitveno sodišče navaja sodbo z dne 27. januarja 2005, Denuit in Cordenier (C-125/04, EU:C:2005:69, točka 12).

23 V točki 11 obrazložitve Sklepa 2010/87 je navedeno: „Nadzorni organi držav članic imajo v tem pogodbenem mehanizmu ključno vlogo pri zagotavljanju primernega varstva osebnih podatkov po prenosu. V izjemnih primerih, kadar izvozniki podatkov odklonijo dajanje primernih navodil uvozniku podatkov ali pa so jih nesposobni dati, ter kadar obstaja neizbežna nevarnost resne škode za posameznike, na katere se nanašajo osebni podatki, naj standardne pogodbene klavzule dovolijo nadzornim organom pregled uvoznikov podatkov in podobdelovalcev ter, kjer je to primerno, sprejemanje odločitev, zavezujočih za uvoznike in podobdelovalce. Nadzorni organi naj bi imeli pooblastilo za prepoved ali začasno ustavitev prenosa podatkov ali niza prenosov, ki temelji na standardnih pogodbenih klavzulah v tistih izjemnih primerih, kjer se ugotovi verjetnost, da ima lahko prenos na pogodbeni podlagi precej škodljivih posledic za jamstva in obveznosti, ki zagotavljajo primerno varstvo posameznika, na katerega se nanašajo osebni podatki.“

24 Družba Facebook Ireland je zoper predložitveni sklep vložila pritožbo pri Supreme Court (vrhovno sodišče, Irska). Ta pritožba je bila zavrnjena s sodbo z dne 31. maja 2019, The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Appeal nº 2018/68 (v nadaljevanju: sodba Supreme Court (vrhovno sodišče) z dne 31. maja 2019).

2. (a) Ali so pri določanju o tem, ali obstaja kršitev pravic posameznika prek prenosa podatkov iz [Unije] v tretjo državo v skladu s Sklepom [2010/87], kjer se lahko dalje obdelujejo zaradi nacionalne varnosti, pomembno merilo primerjave v smislu Direktive [95/46]:

   (i) Listina, PEU, PDEU, Direktiva [95/46], [Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin, podpisana v Rimu 4. novembra 1950 (v nadaljevanju: EKČP)] (ali katera koli druga določba prava [Unije]) ali

   (ii) nacionalni zakoni ene ali več držav članic?

   (b) Ali je treba v primeru, v katerem so pomembno merilo primerjave [(ii)], vanje vključiti tudi prakse v okviru nacionalne varnosti v eni ali več državah članicah?

3. Ali je treba pri ocenjevanju, ali tretja država zagotavlja raven varnosti, ki jo zahteva pravo [Unije] za osebne podatke, ki se prenesejo v to državo v smislu člena 26 Direktive [95/46], raven varstva v tretji državi ocenjevati s sklicevanjem na:

   (a) veljavna pravila v tretji državi, ki izhajajo iz domačega prava ali mednarodnih zavez, in prakso, oblikovano za zagotavljanje skladnosti s temi pravili, vključno s strokovnimi pravili in varnostnimi ukrepi, upoštevanimi v tretji državi,

   ali

   (b) pravila iz (a) skupaj s takimi upravnimi, regulativnimi praksami in praksami za zagotavljanje skladnosti, zaščitnimi političnimi ukrepi, postopki, protokoli, mehanizmi nadzora in izvensodnimi sredstvi, ki veljajo v tretji državi?

4. Ali so glede na dejstva, ki jih je ugotovilo High Court (višje sodišče) v zvezi s pravom [Združenih držav], če se osebni podatki prenesejo iz [Unije v Združene države] v skladu s Sklepom [2010/87], s tem kršene pravice posameznikov v skladu s členi 7 in/ali 8 Listine?

5. Glede na dejstva, ki jih je ugotovilo High Court (višje sodišče) v zvezi s pravom [Združenih držav], če se osebni podatki prenesejo iz [Unije v Združene države] v skladu s Sklepom [2010/87]:

   (a) ali raven varstva, ki jo nudijo [Združene države], spoštuje bistveno vsebino pravice posameznika do pravnega sredstva v primeru kršitve njegovih ali njenih pravic do varstva podatkov, ki jih zagotavlja člen 47 Listine?

Če je odgovor na vprašanje (a) pritrdilen:

   (b) ali so omejitve, ki jih pravo [Združenih držav] nalaga v zvezi s pravico posameznika do pravnega sredstva v okviru nacionalne varnosti [Združenih držav], sorazmerne v smislu člena 52 Listine in ne presegajo tistega, kar je potrebno v demokratični družbi za namene nacionalne varnosti?

6. (a) Kakšna je raven varstva, ki jo je treba zagotoviti za prenos osebnih podatkov v tretjo državo v skladu s standardnimi pogodbenimi klavzulami, sprejetimi v skladu s sklepom Komisije v skladu s členom 26(4) [Direktive 95/46] glede na določbe [te d]irektive ter zlasti [njenih] členov 25 in 26 ob upoštevanju Listine?

   (b) Katere dejavnike je treba upoštevati pri ocenjevanju, ali raven varstva, ki se zagotavlja za prenos podatkov v tretjo državo v skladu s Sklepom [2010/87], izpolnjuje zahteve Direktive [95/46] in Listine?

7. Ali dejstvo, da se standardne pogodbene klavzule uporabljajo med izvoznikom podatkov in uvoznikom podatkov ter ne zavezujejo nacionalnih organov tretje države, ki lahko od uvoznika podatkov zahtevajo, naj osebne podatke, prenesene v skladu s klavzulami iz Sklepa [2010/87], da na voljo varnostnim službam te države za nadaljnjo obdelavo, izključuje, da te klavzule zagotavljajo ustrezne zaščitne ukrepe, kakor to določa člen 26(2) Direktive [95/46]?

8. Če za uvoznika podatkov iz tretje države velja zakonodaja o nadzoru, ki je glede na [nadzorni organ] v navzkrižju s [standardnimi pogodbenimi] klavzulami […] ali s členoma 25 in 26 Direktive [95/46] in/ali Listino, ali mora [nadzorni organ] uporabiti svoja izvršilna pooblastila v skladu s členom 28(3) Direktive [95/46] za prekinitev pretoka podatkov ali je izvajanje takih pooblastil omejeno le na izjemne primere glede na [točko 11 obrazložitve Sklepa 2010/87] ali pa lahko [nadzorni organ] uporabi svojo diskrecijsko pravico, da ne prekine pretoka podatkov?

9. (a) Ali Sklep [o zasebnostnem ščitu] v smislu člena 25(6) Direktive [95/46] predstavlja ugotovitev o splošni uporabi, ki [nadzorne organe] in sodišča držav članic zavezuje tako, da se šteje, da [Združene države] zagotavljajo ustrezno raven varstva v smislu člena 25(2) Direktive [95/46] zaradi njihovega domačega prava ali mednarodnih zavez, ki so jih sklenile?

   (b) Če to ni tako, kakšen pomen, če sploh kakšen, ima Sklep o zasebnostnem ščitu pri ocenjevanju glede ustreznosti zaščitnih ukrepov, zagotovljenih za prenesene podatke v [Združenih državah], ki se prenašajo v skladu s Sklepom [2010/87]?

10. Ali glede na ugotovitve High Court (višje sodišče) v zvezi s pravom [Združenih držav] določba o varuhu človekovih pravic na področju zasebnostnega ščita v skladu s [Prilogo III A] k Sklepu o zasebnostnem ščitu v zvezi z obstoječim režimom v [Združenih državah] zagotavlja pravno sredstvo za posameznike, na katere se nanašajo osebni podatki, ki se prenesejo v [Združene države] v skladu s Sklepom [2010/87], ki je skladno s členom 47 Listine?

11. Ali Sklep [2010/87] krši člene 7, 8 in/ali 47 Listine?“

77. Pisna stališča so pri Sodišču vložili DPC, družba Facebook Ireland, M. Schrems, vlada Združenih držav, organizacije EPIC, BSA in Digitaleurope, Irska ter belgijska, češka, nemška, nizozemska, avstrijska, poljska in portugalska vlada ter vlada Združenega kraljestva, Evropski parlament in Komisija. DPC, družba Facebook Ireland, M. Schrems, vlada Združenih držav, organizacije EPIC, BSA in Digitaleurope, Irska ter nemška, francoska, nizozemska in avstrijska vlada ter vlada Združenega kraljestva, Parlament, Komisija in Evropski odbor za varstvo podatkov (EOVP) so bili zastopani na obravnavi 9. julija 2019.

IV. Analiza

A. Uvodne ugotovitve

78. Potem ko je Sodišče v sodbi Schrems Odločbo o varnem pristanu razglasilo za neveljavno, so se prenosi osebnih podatkov v Združene države nadaljevali na drugih pravnih podlagah. Natančneje, družbe, ki izvažajo podatke, so lahko uporabile pogodbe z uvozniki podatkov, ki vključujejo standardne klavzule, ki jih je oblikovala Komisija. Te klavzule so tudi pravna podlaga za prenose v številne druge

tretje države, v zvezi s katerimi Komisija ni sprejela sklepa o ustreznosti.[25] Sklep o zasebnostnem ščitu zdaj podjetjem, ki so s samocertificiranjem potrdila svoje spoštovanje načel, določenih v njem, omogoča, da prenašajo osebne podatke v Združene države brez drugih formalnosti.

79. Kot je izrecno navedeno v predložitvenem sklepu in kot so poudarili BSA, Digitaleurope, Irska, avstrijska in francoska vlada, Parlament in Komisija, gre v sporu o glavni stvari pred High Court (višje sodišče) le za ugotavljanje, ali je sklep, s katerim je Komisija določila standardne pogodbene klavzule, ki se navajajo v podporo prenosom iz pritožbe M. Schremsa, to je Sklep 2010/87,[26] veljaven.

80. Ta spor izvira iz pritožbe, s katero je DPC predložitvenemu sodišču predlagal, naj Sodišču predloži vprašanje za predhodno odločanje glede veljavnosti Sklepa 2010/87. Po besedah predložitvenega sodišča spor o glavni stvari tako zadeva uveljavljanje pravnega sredstva, katerega uvedbo je Sodišče državam članicam naložilo v točki 65 sodbe Schrems.

81. Naj spomnim, da je Sodišče v točki 63 te sodbe presodilo, da mora nadzorni organ z vso potrebno skrbnostjo obravnavati pritožbo, v okviru katere posameznik, čigar osebni podatki so bili ali bi lahko bili preneseni v tretjo državo, na katero se nanaša sklep o ustreznosti, izpodbija skladnost tega sklepa s temeljnimi pravicami, določenimi v Listini. V skladu s točko 65 navedene sodbe mora ta organ, če meni, da so očitki iz te pritožbe utemeljeni, v skladu s členom 28(3), prvi pododstavek, tretja alinea, Direktive 95/46 (ki mu ustreza člen 58(5) GDPR) ob upoštevanju člena 8(3) Listine imeti možnost sodelovati v sodnih postopkih. V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki omogočajo predložitev teh očitkov nacionalnim sodiščem, da bi ta, če bi se strinjala z dvomi navedenega organa, sprožila postopek predhodnega odločanja glede veljavnosti zadevnega sklepa.

82. Enako kot predložitveno sodišče menim, da se te ugotovitve po analogiji uporabljajo, kadar nadzorni organ pri obravnavi pritožbe, vložene pri njem, ne dvomi o veljavnosti sklepa o ustreznosti, temveč sklepa, kot je Sklep 2010/87, ki določa standardne pogodbene klavzule za prenos osebnih podatkov v tretjo državo. V nasprotju s trditvami nemške vlade ni pomembno, ali ti dvomi ustrezajo očitkom, na katere ga je opozoril pritožnik, ali pa ta organ sam podvomi o veljavnosti zadevnega sklepa. Zahteve, ki izhajajo iz člena 58(5) GDPR in člena 8(3) Listine ter na katerih temelji obrazložitev Sodišča, se namreč uporabljajo ne glede na pravno podlago za prenos, na katerega se nanaša pritožba, vložena pri nadzornem organu, in ne glede na razloge, iz katerih je ta organ pri obravnavi te pritožbe podvomil o veljavnosti zadevnega sklepa.

83. Ob upoštevanju tega je razlog, da je DPC zaprosil predložitveno sodišče, naj Sodišče povpraša o veljavnosti Sklepa 2010/87, ta, da se mu zdi pojasnilo Sodišča v zvezi s tem nujno za obravnavo pritožbe, s katero M. Schrems od DPC zahteva, naj izvrši pooblastilo, ki ga je imel na podlagi člena 28(3), druga alinea, Direktive 95/46 – in ki mu je zdaj podeljeno s členom 58(2)(f) GDPR – da prekine prenos njegovih osebnih podatkov, ki jih družba Facebook Ireland posreduje družbi Facebook Inc.

84. Medtem ko se spor o glavni stvari torej nanaša samo na veljavnost *in abstracto* Sklepa 2010/87, pa se temeljni postopek, ki poteka pred DPC, nanaša na njegovo izvrševanje njegovega pooblastila za sprejetje popravljalnih ukrepov *v konkretnem primeru*. Sodišču bom predlagal, naj postavljena vprašanja preuči le v obsegu, potrebnem za to, da odloči o veljavnosti Sklepa 2010/87, ker bo taka preučitev zadostovala, da predložitvenemu sodišče reši spor, o katerem odloča.[27]

25 BSA zatrjuje, da je 70 % podjetij, ki so člani te zveze in so odgovorila na anketo v zvezi s tem, izjavilo, da uporabljajo standardne pogodbene klavzule kot glavno podlago za prenose osebnih podatkov v tretje države. Digitaleurope prav tako meni, da so standardne pogodbene klavzule glavni pravni instrument, ki se navaja v podporo tem prenosom.

26 Čeprav predložitveno sodišče navaja, da se njegov predlog za sprejetje predhodne odločbe nanaša na veljavnost vseh treh sklepov SPK, saj so bili ti preučeni v osnutku odločbe DPC in v sodbi z dne 3. oktobra 2017, se vprašanja za predhodno odločanje nanašajo izključno na Sklep 2010/87. To je zato, ker je družba Facebook Ireland pred tem sodiščem ta sklep opredelila kot pravno podlago za prenose podatkov evropskih uporabnikov družabnega omrežja Facebook v Združene države. Moja analiza se bo torej nanašala samo na navedeni sklep.

27 Glej točke od 167 do 186 teh sklepnih predlogov.

85. Pred presojo veljavnosti tega sklepa je treba zavrniti nekatere ugovore, podane zoper dopustnost predloga za sprejetje predhodne odločbe.

B. Dopustnost predloga za sprejetje predhodne odločbe

86. Dopustnost predloga za sprejetje predhodne odločbe je bila izpodbijana iz različnih razlogov, ki se v bistvu nanašajo na neuporabo *ratione temporis* Direktive 95/46, omenjene v vprašanjih za predhodno odločanje (razdelek 1), na okoliščino, da postopek pred DPC ni dosegel dovolj napredne faze, da bi bilo mogoče utemeljiti njegovo korist (razdelek 2), in na nadaljnji obstoj negotovosti v zvezi z dejanskim okvirom, ki ga opisuje predložitveno sodišče (razdelek 3).

87. Na te ugovore nedopustnosti bom odgovoril z mislijo na domnevo upoštevnosti, ki velja za vprašanja, predložena Sodišču na podlagi člena 267 PDEU. V skladu z ustaljeno sodno prakso lahko Sodišče odločanje o predlogu za sprejete predhodne odločbe zavrne le, če zahtevana razlaga prava Unije očitno nima nobene zveze z dejanskim stanjem ali predmetom spora o glavni stvari, če gre za hipotetičen problem ali če Sodišče nima na voljo potrebnih dejanskih in pravnih elementov, da bi lahko koristno odgovorilo na postavljena vprašanja.[28]

1. Uporaba ratione temporis *Direktive 95/46*

88. Družba Facebook Ireland trdi, da vprašanja za predhodno odločbe niso dopustna, ker se sklicujejo na Direktivo 95/46, čeprav je bila ta direktiva razveljavljena in nadomeščena z GDPR z učinkom od 25. maja 2018.[29]

89. Strinjam se s stališčem, da je treba veljavnost Sklepa 2010/87 preizkusiti z vidika določb GDPR.

90. V skladu s členom 94(2) te uredbe se „[s]klicevanja na razveljavljeno direktivo […] štejejo kot sklicevanja na [navedeno] uredbo“. Zdi se mi, da iz tega izhaja, da je treba Sklep 2010/87 v delu, v katerem je kot pravna podlaga omenjen člen 26(4) Direktive 95/46, razumeti tako, kot da se sklicuje na člen 46(2)(c) GDPR, v katerem je v bistvu povzeta vsebina prvo navedenega člena.[30] Zato je treba izvedbene sklepe, ki jih je Komisija sprejela na podlagi člena 26(4) Direktive 95/46 pred začetkom veljavnosti GDPR, razlagati z vidika te uredbe. Z vidika navedene uredbe je treba po potrebi presojati tudi njihovo veljavnost.

91. Te ugotovitve ne ovrže sodna praksa, v skladu s katero je treba zakonitost akta Unije presojati glede na dejanske in pravne okoliščine, ki so obstajale na dan sprejetja tega akta. Ta sodna praksa namreč zadeva preizkus veljavnosti akta Unije glede na upoštevne dejanske okoliščine ob njegovem sprejetju[31] ali glede na postopkovna pravila, ki urejajo njegovo sprejetje.[32] Nasprotno pa je Sodišče veljavnost aktov sekundarne zakonodaje večkrat preizkusilo z vidika hierarhično višjih materialnih pravil, ki so začela veljati po sprejetju teh aktov.[33]

28 Glej med drugim sodbo z dne 10. decembra 2018, Wightman in drugi (C-621/18, EU:C:2018:999, točka 27) in z dne 19. novembra 2019, A. K. in drugi (Neodvisnost disciplinskega senata vrhovnega sodišča) (C-585/18, C-624/18 in C-625/18, EU:C:2019:982, točka 98).

29 Glej člen 94(1) in člen 99(1) GDPR.

30 Poudarjam, da v skladu s členom 46(5) GDPR odločitve, ki jih je Komisija sprejela na podlagi člena 26(4) Direktive 95/46, ostanejo veljavne do njihove spremembe, nadomestitve ali razveljavitve.

31 Glej zlasti sodbe z dne 7. februarja 1979, Francija/Komisija (15/76 in 16/76, EU:C:1979:29, točka 7); z dne 17. maja 2001, IECC/Komisija (C-449/98 P, EU:C:2001:275, točka 87), in z dne 17. oktobra 2013, Schaible (C-101/12, EU:C:2013:661, točka 50).

32 Glej zlasti sodbe z dne 16. aprila 2015, Parlament/Svet (C-540/13, EU:C:2015:224, točka 35); z dne 16. aprila 2015, Parlament/Svet (C-317/13 in C-679/13, EU:C:2015:223, točka 45), in z dne 22. septembra 2016, Parlament/Svet (C-14/15 in C-116/15, EU:C:2016:715, točka 48).

33 Zlasti v sodbi Schrems je Sodišče veljavnost Odločbe o varnem pristanu preizkusilo z vidika določb Listine, ki je bila sprejeta po sprejetju te odločbe. Glej tudi sodbi z dne 17. marca 2011, AJD Tuna (C-221/09, EU:C:2011:153, točka 48), in z dne 11. junija 2015, Pfeifer & Langen (C-51/14, EU:C:2015:380, točka 42).

92. Vendar to, da je v besedilu vprašanj za predhodno odločanje imenovan akt, ki se *ratione temporis* ne uporablja več, čeprav utemeljuje preoblikovanje teh vprašanj, ne more povzročiti njihove nedopustnosti.[34] Kot sta navedla DPC in M. Schrems, je sklicevanja na Direktivo 95/46 v besedilu vprašanj za predhodno odločanje poleg tega mogoče pojasniti glede na postopkovni časovni okvir obravnavane zadeve, saj so bila ta vprašanja Sodišču predložena pred začetkom veljavnosti GDPR.

93. Vsekakor je v določbah GDPR, ki bodo obravnavane za analizo vprašanj za predhodno odločanje, to so zlasti njeni členi 45, 46 in 58, v bistvu povzeta – ob sočasni razširitvi in z nekaj manjšimi razlikami – vsebina členov 25, 26 in 28 Direktive 95/46. Glede njihovih vidikov, ki so upoštevni za odločanje o veljavnosti Sklepa 2010/87, ne vidim nobenega razloga za to, da bi se tem določbam GDPR pripisoval drugačen obseg od obsega ustreznih določb Direktive 95/46.[35]

2. Začasnost dvomov, ki jih je izrazil DPC

94. Po mnenju nemške vlade predlog za sprejetje predhodne odločbe ni dopusten, ker je postopek s pravnim sredstvom, omenjen v točki 65 sodbe Schrems, pogojen s tem, da si je nadzorni organ ustvaril dokončno mnenje glede utemeljenosti očitkov, ki jih pritožnik navaja zoper veljavnost zadevnega sklepa. V obravnavanem primeru naj ne bi bilo tako, ker je DPC svoje dvome glede veljavnosti Sklepa 2010/87 – ki je M. Schrems sicer ne izpodbija – izrazil v osnutku odločbe, ki je bil izdan začasno, brez poseganja v to, da bi družba Facebook Ireland in M. Schrems morebiti predložila dodatne pripombe.

95. Po mojem mnenju začasnost dvomov, ki jih je izrazil DPC, ne vpliva na dopustnost predloga za sprejetje predhodne odločbe. Merila dopustnosti vprašanja za predhodno odločanje je treba namreč presojati glede na predmet spora, kot ga opredeli predložitveno sodišče.[36] Ni pa sporno, da se ta nanaša na veljavnost Sklepa 2010/87. Glede na predložitveni sklep in sodbo, ki mu je priložena, je to sodišče presodilo, da so dvomi, ki jih je izrazil DPC – ne da bi bilo pomembno, ali so bili ti dvomi začasni ali dokončni – utemeljeni, in je zato Sodišče povprašalo o veljavnosti tega sklepa. V teh okoliščinah so pojasnila Sodišča v zvezi s tem brez najmanjšega dvoma upoštevna za to, da se predložitvenemu sodišču omogoči rešitev spora, o katerem odloča.

3. Negotovosti v zvezi z opredelitvijo dejanskega okvira

96. Vlada Združenega kraljestva navaja, da dejanski okvir, ki ga opisuje predložitveno sodišče, vsebuje več vrzeli, ki ogrožajo dopustnost vprašanj za predhodno odločanje. To sodišče naj ne bi razjasnilo, ali so bili osebni podatki v zvezi z M. Schremsom dejansko preneseni v Združene države in, če so bili, ali so jih ameriški organi zbirali. Pravna podlaga za te morebitne prenose naj prav tako ne bi bila zanesljivo opredeljena, saj naj bi bilo v predložitvenem sklepu omenjeno le, da se podatki evropskih uporabnikov družabnega omrežja Facebook prenašajo „v veliki meri“ na podlagi standardnih pogodbenih klavzul iz Sklepa 2010/87. Vsekakor naj ne bi bilo ugotovljeno, da so te klavzule dosledno vključene v pogodbo med družbama Facebook Ireland in Facebook Inc., ki se navaja v podporo spornemu prenosu. Nemška vlada dopustnost predloga za sprejetje predhodne odločbe izpodbija tudi zato, ker predložitveno sodišče ni preučilo, ali je M. Schrems nedvoumno dal privolitev v zadevne prenose, pri čemer naj bi v tem primeru ti veljavno temeljili na členu 26(1) Direktive 95/46 (katerega vsebina je v bistvu povzeta v členu 49(1)(a) GDPR).

34 Glej zlasti sodbe z dne 15. julija 2010, Pannon Gép Centrum (C-368/09, EU:C:2010:441, točke od 30 do 35); z dne 10. februarja 2011, Andersson (C-30/10, EU:C:2011:66, točki 20 in 21), in z dne 25. oktobra 2018, Roche Lietuva (C-413/17, EU:C:2018:865, točke od 17 do 20).

35 Glej v zvezi s tem sklepne predloge generalnega pravobranilca M. Bobka v zadevi Fashion ID (C-40/17, EU:C:2018:1039, točka 87).

36 Glej točko 87 teh sklepnih predlogov.

97. Te trditve nikakor ne omajejo upoštevnosti predloga za sprejetje za predhodne odločbe glede na predmet spora o glavni stvari. Ker ta spor izvira iz tega, da je DPC uveljavljal pravno sredstvo iz točke 65 sodbe Schrems, je njegov predmet to, da nacionalno sodišče predloži predlog za sprejetje predhodne odločbe glede veljavnosti Sklepa 2010/87. Nemška vlada in vlada Združenega kraljestva v resnici ne prerekata potrebnosti vprašanj za predhodno odločanje zaradi ugotavljanja, ali je ta sklep veljaven, temveč zaradi omogočanja, da DPC *in concreto* odloči o pritožbi M. Schremsa.

98. Vsekakor se mi tudi z vidika tega postopka, na katerem temelji spor o glavni stvari, vprašanja za predhodno odločanje glede veljavnosti Sklepa 2010/87 ne zdijo neupoštevna. Predložitveno sodišče je namreč ugotovilo, da je družba Facebook Ireland po razglasitvi neveljavnosti Odločbe o varnem pristanu podatke svojih uporabnikov še naprej prenašala v Združene države in da ti prenosi vsaj delno temeljijo na Sklepu 2010/87. Poleg tega, čeprav je lahko koristno, da se vsa upoštevna dejstva ugotovijo, preden predložitveno sodišče uporabi svojo pristojnost na podlagi člena 267 PDEU, je to sodišče edino, ki presoja, v kateri fazi postopka potrebuje predhodno odločbo Sodišča. [37]

99. Ob upoštevanju vsega navedenega menim, da je predlog za sprejetje predhodne odločbe dopusten.

C. Uporaba prava Unije za prenose osebnih podatkov za komercialne namene v tretjo državo, ki jih lahko obdeluje zaradi nacionalne varnosti (prvo vprašanje)

100. Predložitveno sodišče želi s prvim vprašanjem izvedeti, ali se pravo Unije uporablja za prenos osebnih podatkov, ki ga izvede družba v državi članici družbi s sedežem v tretji državi za komercialne namene, če je mogoče, da bodo po začetku tega prenosa podatke obdelovali javni organi te tretje države z nameni, ki vključujejo varovanje nacionalne varnosti.

101. Pomen tega vprašanja za rešitev spora o glavni stvari je v tem, da če tak prenos ne bi spadal na področje uporabe prava Unije, bi vsi ugovori, podani zoper veljavnost Sklepa 2010/87 v obravnavani zadevi, ostali brez podlage.

102. Kot je opozorilo predložitveno sodišče, je bila obdelava osebnih podatkov v zvezi z nacionalno varnostjo izključena iz področja uporabe Direktive 95/46 na podlagi člena 3(2) te direktive. Člen 2(2) GDPR zdaj določa, da se ta uredba med drugim ne uporablja za obdelavo podatkov v okviru dejavnosti zunaj področja uporabe prava Unije ali s strani pristojnih organov zaradi varovanja javne varnosti. Te določbe odražajo pridržano pristojnost, ki se s členom 4(2) PEU priznava državam članicam na področju varovanja nacionalne varnosti.

103. DPC, M. Schrems, Irska ter nemška, avstrijska, belgijska, češka, nizozemska, poljska in portugalska vlada ter Parlament in Komisija trdijo, da prenosi, kot so ti, na katere se nanaša pritožba M. Schremsa, niso zajeti s temi določbami in zato spadajo na področje uporabe prava Unije. Družba Facebook Ireland trdi nasprotno. Sam se pridružujem stališču prvih.

37 Glej v tem smislu sodbi z dne 1. aprila 1982, Holdijk in drugi (od 141/81 do 143/81, EU:C:1982:122, točka 5), in z dne 9. decembra 2003, Gasser (C-116/02, EU:C:2003:657, točka 27).

104. V zvezi s tem je treba poudariti, da prenos osebnih podatkov iz države članice v tretjo državo sam po sebi pomeni „obdelavo“ v smislu člena 4, točka 2, GDPR, izvedeno na ozemlju države članice.[38] Namen prvega vprašanja za predhodno odločanje je ugotoviti ravno to, ali se pravo Unije uporablja *za obdelavo, ki jo pomeni prenos sam po sebi*. To vprašanje se ne nanaša na uporabo prava Unije za morebitno nadaljnjo obdelavo osebnih podatkov, prenesenih v Združene države, ki bi jo ameriški organi izvajali zaradi nacionalne varnosti, to je obdelavo, ki ne spada na ozemeljsko področje uporabe GDPR.[39]

105. S tega vidika je treba za ugotavljanje, ali se pravo Unije uporablja za prenos zadevnih podatkov, upoštevati le dejavnost, v okvir katere se ta prenos umešča, pri čemer ni pomemben namen morebitne nadaljnje obdelave prenesenih podatkov, ki jo bodo izvedli javni organi namembne tretje države.[40]

106. Iz predložitvenega sklepa pa je razvidno, da je prenos, na katerega se nanaša pritožba M. Schremsa, del komercialne dejavnosti. Ta prenos tudi ni imel namena omogočiti nadaljnjo obdelavo zadevnih podatkov, ki bi jo ameriški organi izvajali zaradi nacionalne varnosti.

107. Poleg tega bi bil s pristopom, ki ga predlaga družba Facebook Ireland, določbam GDPR o prenosih v tretje države odvzet polni učinek, ker nikoli ni mogoče izključiti, da se bodo podatki, preneseni v okviru komercialne dejavnosti, po prenosu obdelovali zaradi nacionalne varnosti.

108. Razlago, ki jo zagovarjam, potrjuje besedilo člena 45(2)(a) GDPR. V tej določbi je navedeno, da ko Komisija sprejme sklep o ustreznosti, upošteva med drugim zakonodajo zadevne tretje države *na področju nacionalne varnosti*. Iz tega je mogoče sklepati, da možnost, da bodo organi namembne tretje države podatke obdelovali zaradi varovanja nacionalne varnosti, ne povzroči, da se pravo Unije ne uporablja za obdelavo, ki jo pomeni prenos podatkov v to tretjo državo.

109. Razlogovanje in ugotovitve, ki jih je Sodišče sprejelo v sodbi Schrems, prav tako temeljijo na tej premisi. Natančneje, Sodišče je v njej – glede na člen 25(6) Direkitve 95/46, razlagan ob upoštevanju Listine – preizkusilo veljavnost Odločbe o varnem pristanu v delu, v katerem se je nanašala na prenose osebnih podatkov v Združene države, kjer je obstajala možnost, da se bodo zbirali in obdelovali zaradi varovanja nacionalne varnosti.[41]

110. Glede na te preudarke menim, da se pravo Unije uporablja za prenos osebnih podatkov iz države članice v tretjo državo, kadar se ta prenos umešča v okvir komercialne dejavnosti, ne da bi bilo pomembno, da lahko javni organi te tretje države prenesene podatke obdelujejo zaradi njene nacionalne varnosti.

38 Glej v tem smislu sodbo z dne 30. maja 2006, Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346, točka 56; v nadaljevanju: sodba PNR), in sodbo Schrems (točka 45). V členu 4, točka 2, GDPR je v bistvu povzeta opredelitev pojma „obdelava“, kakor je bil opredeljen v členu 2, točka (b), Direktive 95/46.

39 V skladu s členom 3(1) GDPR se ta uredba uporablja za vsako obdelavo osebnih podatkov v okviru dejavnosti ustanovitve upravljavca ali obdelovalca v Uniji, ne glede na to, ali obdelava poteka v Uniji ali ne. Vprašanje uporabe prava Unije za obdelavo, ki jo obveščevalne službe tretje države izvajajo zunaj Unije, je treba razlikovati od vprašanja upoštevnosti pravil in praks v zvezi s to obdelavo v zadevni tretji državi za ugotavljanje, ali je v njej zagotovljena ustrezna raven varstva. Zadnjenavedena tema je predmet drugega vprašanja za predhodno odločanje in se bo obravnavala v točkah od 201 do 229 teh sklepnih predlogov.

40 V sklepnih predlogih v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300, točka 47) sem poudaril razliko med neposredno obdelavo osebnih podatkov v okviru oblastnih dejavnosti države na eni strani in komercialno obdelavo, ki ji sledi uporaba javnih organov, na drugi.

41 Enako je Sodišče v mnenju 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017 (EU:C:2017:592; v nadaljevanju: mnenje 1/15) preverilo, ali je osnutek mednarodnega sporazuma med Kanado in Unijo v zvezi s podatki, ki so bili po prenosu v Kanado namenjeni obdelavi organov zaradi varovanja nacionalne varnosti, v skladu s členi 7, 8 in 47 Listine.

D. Raven varstva, zahtevana v okviru prenosa, ki temelji na standardnih pogodbenih klavzulah (prvi del šestega vprašanja)

111. V skladu s prvim delom šestega vprašanja želi predložitveno sodišče izvedeti, kakšna raven varstva temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, mora biti zagotovljena, da je osebne podatke mogoče prenesti v tretjo državo na podlagi standardnih pogodbenih klavzul iz Sklepa 2010/87.

112. To sodišče poudarja, da je Sodišče v sodbi Schrems člen 25(6) Direktive 95/46 (katerega vsebina je v bistvu povzeta v členu 45(3) GDPR) v delu, v katerem je določal, da lahko Komisija sprejme sklep o ustreznosti šele po tem, ko se je prepričala, da zadevna tretja država zagotavlja *ustrezno* raven varstva, razložilo tako, da se z njim zahteva, da ta institucija ugotovi, da ta država zagotavlja raven varstva temeljnih svoboščin in pravic, ki je *v bistvenem enaka* ravni, zagotovljeni v Uniji na podlagi te direktive, razlagane ob upoštevanju Listine.[42]

113. V teh okoliščinah se s prvim delom šestega vprašanja za predhodno odločanje Sodišču predlaga, naj ugotovi, ali mora uporaba „standardnih pogodbenih klavzul“, ki jih je Komisija sprejela na podlagi člena 26(4) Direktive 95/46 – ki ustrezajo „standardnim določilom o varstvu“, zdaj omenjenim v členu 46(2)(c) GDPR – omogočati doseganje ravni varstva, ki ustreza istemu standardu „bistvene enakosti“.

114. V zvezi s tem člen 46(1) GDPR določa, da lahko upravljavec, kadar sklep o ustreznosti ni sprejet, osebne podatke prenese v tretjo državo „le, če je […] predvidel *ustrezne zaščitne ukrepe*, in pod pogojem, da imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva“ (moj poudarek).[43] V skladu s členom 46(2)(c) GDPR lahko ti zaščitni ukrepi izhajajo med drugim iz „standardnih določil o varstvu“, ki jih pripravi Komisija.

115. Enako kot DPC, M. Schrems in Irska menim, da morajo „ustrezni zaščitni ukrepi“, ki jih zagotovi upravljavec, na katere se sklicuje člen 46(1) GDPR, zagotavljati, da so pravice oseb, katerih podatki se prenašajo, tako kot v okviru prenosa na podlagi sklepa o ustreznosti deležne ravni varstva, ki je v bistvenem enaka ravni, ki izhaja iz GDPR, razlagane ob upoštevanju Listine.

116. Ta sklep izhaja iz cilja te določbe in instrumenta, katere del je.

117. Cilj členov 45 in 46 GDPR je zagotoviti kontinuiteto visoke ravni varstva osebnih podatkov, zagotovljene s to uredbo, kadar se prenašajo iz Unije. S členom 44 GDPR, naslovljenim „Splošno načelo za prenose“, se namreč začne poglavje V v zvezi s prenosom v tretje države, pri čemer ta člen določa, da se vse določbe tega poglavja uporabljajo za zagotovitev, da ni ogrožena raven varstva posameznikov, ki jo zagotavlja GDPR.[44] S tem pravilom se želi preprečiti, da bi se standardi varstva, ki izhajajo iz prava Unije, zaobšli s prenašanjem osebnih podatkov v tretjo državo, da bi se tam obdelovali.[45] Glede na ta cilj ni pomembno, ali prenos temelji na sklepu o ustreznosti ali na zaščitnih ukrepih, ki jih upravljavec zagotovi zlasti z uporabo pogodbenih klavzul. Zahteve po varstvu temeljnih pravic, zagotovljenih z Listino, ne vsebujejo razlikovanja glede na pravno podlago, na kateri temelji določen prenos.[46]

42 Sodba Schrems (točka 73). Sodišče je to ugotovitev potrdilo v mnenju 1/15 (točka 134).

43 Člen 26(2) Direktive 95/46 je določal, da lahko država članica dovoli tak prenos, „kadar upravljavec navede *ustrezne zaščitne ukrepe* glede varstva zasebnosti ter temeljnih pravic in svoboščin posameznikov in glede uresničevanja ustreznih pravic“ (moj poudarek). Pojem „ustrezni zaščitni ukrepi“ ima po mojem mnenju v tej določbi in v členu 46(1) GDPR isto vsebino.

44 V zvezi s tem je v uvodni izjavi 6 GDPR navedeno, da je treba „visoko raven“ varstva podatkov zagotoviti tako v Uniji kot v primeru prenosa iz Unije. Glej tudi uvodno izjavo 101 GDPR.

45 Glej sodbo Schrems (točka 73) in mnenje 1/15 (točka 214).

46 To velja brez poseganja v možnost, da se osebni podatki prenašajo tudi ob neobstoju ustreznih zaščitnih ukrepov na podlagi razlogov za odstopanje, ki jih določa člen 49(1) GDPR.

118. Nasprotno pa se to, kako se ohranja kontinuiteta visoke ravni varstva, razlikuje glede na pravno podlago za prenos.

119. Po eni strani je namen sklepa o ustreznosti ugotoviti, da zadevna tretja država sama zagotavlja raven varstva, ki je v bistvenem enaka ravni, ki jo treba doseči v Uniji. Sprejetje sklepa o ustreznosti je pogojeno s tem, da Komisija za dano tretjo državo prej oceni raven varstva, zagotovljeno z zakonom, in prakse v tej tretji državi z vidika dejavnikov, določenih v členu 45(3) GDPR. Osebni podatki se lahko potem prenesejo v navedeno tretjo državo, ne da bi upravljavec moral pridobiti posebno dovoljenje.

120. Po drugi strani so, kot je podrobneje predstavljeno v naslednjem oddelku, ustrezni zaščitni ukrepi, ki jih zagotovi upravljavec, namenjeni zagotavljanju visoke ravni varstva v primeru nezadostnosti zaščitnih ukrepov, ki so na voljo v namembni tretji državi. Čeprav torej člen 46(1) GDPR omogoča, da se osebni podatki prenašajo v tretje države, ki ne zagotavljajo ustrezne ravni varstva, so s to določbo taki prenosi dovoljeni, le če se ustrezni zaščitni ukrepi zagotovijo z drugimi sredstvi. Standardne pogodbene klavzule, ki jih sprejme Komisija, v zvezi s tem predstavljajo splošen mehanizem, ki se uporablja za prenose ne glede na to, za katero namembno tretjo državo gre, in ne glede na raven varstva, ki je zagotovljena v njej.

E. Veljavnost Sklepa 2010/87 glede na člene 7, 8 in 47 Listine (sedmo, osmo in enajsto vprašanje)

121. Predložitveno sodišče s sedmim vprašanjem v bistvu sprašuje, ali Sklep 2010/87 ni veljaven, ker za organe tretjih držav, v katere se podatki prenašajo na podlagi standardnih pogodbenih klavzul iz Priloge k temu sklepu, ni zavezujoč in zlasti ker tem organom ne preprečuje, da od uvoznika zahtevajo, da jim da te podatke na razpolago. Tako se s tem vprašanjem dvomi o možnosti, da se ustrezna raven varstva takih podatkov zagotovi z izključno pogodbenimi mehanizmi. Enajsto vprašanje se splošneje nanaša na veljavnost Sklepa 2010/87 glede na člene 7, 8 in 47 Listine.

122. Z osmim vprašanjem je Sodišče pozvano, naj ugotovi, ali je nadzorni organ dolžan uporabiti pooblastila, ki so mu podeljena s členom 58(2)(f) in (j) GDPR, za prekinitev prenosa v tretjo državo, ki temelji na standardnih pogodbenih klavzulah iz Sklepa 2010/87, če meni, da v njej za uvoznika podatkov veljajo obveznosti, ki mu preprečujejo spoštovanje teh klavzul in pripeljejo do tega, da ni zagotovljeno ustrezno varstvo prenesenih podatkov. Ker odgovor na to vprašanje po mojem mnenju vpliva na veljavnost Sklepa 2010/87,[47] ga obravnavam skupaj s sedmim in enajstim vprašanjem.

123. V besedilu člena 46(1) GDPR je v delu, v katerem je določeno, da *„[k]adar sklep v skladu s členom 45(3) ni sprejet*, lahko upravljavec ali obdelovalec osebne podatke prenese v tretjo državo […] le, *če je* upravljavec ali obdelovalec *predvidel* ustrezne zaščitne ukrepe […]“ (moj poudarek), poudarjena logika, iz katere izhajajo pogodbeni mehanizmi, kot je ta iz Sklepa 2010/87. Kot je poudarjeno v uvodnih izjavah 108 in 114 GDPR, je namen teh mehanizmov omogočiti prenose v tretje države, za katere Komisija ni sprejela sklepa o ustreznosti, pri čemer se v tem primeru morebitno pomanjkanje varstva, zagotovljenega v pravnem redu te tretje države, *nadomesti* z zaščitnimi ukrepi, h katerih spoštovanju se pogodbeno zavežeta izvoznik in uvoznik podatkov.

124. Ker je razlog za obstoj pogodbenih zaščitnih ukrepov prav odpraviti možne vrzeli v varstvu, ki ga zagotavljajo namembne tretje države, katere koli že so, veljavnost sklepa, s katerim Komisija ugotovi, da nekatere standardne klavzule ustrezno zapolnjujejo te vrzeli, ne more biti odvisna od ravni varstva, zagotovljene v vsaki od posameznih tretjih držav, v katere bi bili podatki lahko preneseni. Veljavnost takega sklepa je odvisna samo od čvrstosti zaščitnih ukrepov, ki jih določajo te klavzule, da bi se nadomestilo morebitno pomanjkanje varstva v namembni tretji državi. Učinkovitost teh zaščitnih ukrepov je treba oceniti upoštevajoč tudi varovala, ki jih pomenijo pooblastila nadzornih organov na podlagi člena 58(2) GDPR.

47 Glej točko 128 teh sklepnih predlogov.

125. Kot so v zvezi s tem v bistvu poudarili DPC, M. Schrems, BSA, Irska ter avstrijska, francoska, poljska in portugalska vlada ter Komisija, se zaščitni ukrepi, ki jih vsebujejo standardne pogodbene klavzule, lahko zmanjšajo ali celo izničijo, če pravo namembne tretje države za uvoznika določa obveznosti, nasprotne temu, kar se zahteva s temi klavzulami. Tako lahko veljavni pravni okvir v namembni tretji državi glede na konkretne okoliščine prenosa [48] onemogoči izpolnjevanje obveznosti, ki jih določajo te klavzule.

126. V teh okoliščinah, kot sta poudarila M. Schrems in Komisija, pogodbeni mehanizem iz člena 46(2)(c) GDPR temelji na nalaganju odgovornosti izvozniku in, podredno, nadzornim organom. Upravljavec oziroma, če ne on, nadzorni organ *v vsakem primeru posebej* za vsak posamezen prenos preveri, ali pravo namembne tretje države pomeni oviro za izvajanje standardnih klavzul in torej za ustrezno varstvo prenesenih podatkov, tako da je treba prenose prepovedati ali prekiniti.

127. Ob upoštevanju teh ugotovitev menim, da okoliščina, da Sklep 2010/87 in standardne pogodbene klavzule, ki jih določa, za organe namembne tretje države niso zavezujoči, sama po sebi ne povzroči neveljavnosti tega sklepa. Skladnost Sklepa 2010/87 s členi 7, 8 in 47 Listine je po mojem mnenju odvisna od vprašanja, ali obstajajo dovolj čvrsti mehanizmi, s katerimi je mogoče zagotoviti, da se prenosi, ki temeljijo na standardih pogodbenih klavzulah, prekinejo ali prepovejo v primeru kršitve teh klavzul ali nezmožnosti njihovega spoštovanja.

128. V zvezi s tem člen 46(1) GDPR določa, da do prenosa, ki temelji na ustreznih zaščitnih ukrepih, lahko pride le, če „imajo posamezniki, na katere se nanašajo osebni podatki, na voljo izvršljive pravice in učinkovita pravna sredstva“. Preveriti bo treba, ali zaščitni ukrepi, ki jih določajo klavzule iz Priloge k Sklepu 2010/87, skupaj s pooblastili nadzornih organov omogočajo, da se zagotovi izpolnjevanje tega pogoja. Odgovor bo po mojem mnenju pritrdilen, le če obstaja *obveznost* – naložena upravljavcem (razdelek 1) in, v primeru njihovega neukrepanja, nadzornim organom (razdelek 2) – prekiniti ali prepovedati prenos, kadar zaradi navzkrižja med obveznostmi, ki izhajajo iz standardnih klavzul, in obveznostmi, predpisanimi s pravom namembne tretje države, teh klavzul ni mogoče spoštovati.

1. Obveznosti, ki jih imajo upravljavci

129. Prvič, s standardnimi pogodbenimi klavzulami iz Priloge k Sklepu 2010/87 se zahteva, da se v primeru navzkrižja med obveznostmi, ki jih določajo, in zahtevami, ki izhajajo iz prava namembne tretje države, te klavzule ne navajajo v podporo prenosu v to tretjo državo ali da je, če se je prenos na podlagi navedenih klavzul že začel, izvoznik obveščen o tem navzkrižju in lahko ta prenos prekine.

130. Tako se v skladu s klavzulo 5(a) uvoznik zaveže, da obdeluje prenesene osebne podatke samo v imenu izvoznika ter v skladu z njegovimi navodili in standardnimi pogodbenimi klavzulami. Če uvoznik teh klavzul ne more upoštevati, soglaša, da o tem nemudoma obvesti izvoznika, ki je v tem primeru upravičen prekiniti prenos in/ali odstopiti od pogodbe. [49]

48 Predstavljati si je treba, na primer, da tretja država določi obveznost za ponudnike telekomunikacijskih storitev, da javnim organom dopustijo dostop do prenesenih podatkov, brez kakršnih koli omejitev in zaščitnih ukrepov. Čeprav taki ponudniki ne bi mogli spoštovati standardnih pogodbenih klavzul, pa to ne bi bilo preprečeno podjetjem, za katera ta obveznost ne velja.

49 Poleg tega opozarjam, da je s klavzulo 5(d)(i) uvoznik oproščen obveznosti obvestiti izvoznika o pravno zavezujočih zahtevah organa kazenskega pregona tretje države za posredovanje podatkov, če pravo te tretje države nasprotuje takemu obveščanju. V takem primeru izvoznik ne bo imel možnosti prekiniti prenosa, če bo to posredovanje podatkov, s katerim ne bo seznanjen, v nasprotju s standardnimi klavzulami. Vendar uvoznik v skladu s klavzulo 5(a) ostaja dolžan po potrebi obvestiti izvoznika, da meni, da mu zakonodaja te tretje države preprečuje izpolnitev njegovih obveznosti na podlagi dogovorjenih pogodbenih klavzul.

131. V opombi 5 h klavzuli 5 je pojasnjeno, da standardne klavzule niso kršene, kadar uvoznik spoštuje obvezne zahteve nacionalne zakonodaje, ki se zanj uporablja v tretji državi, če te zahteve ne presegajo tega, kar je potrebno v demokratični družbi za zaščito enega od interesov iz člena 13(1) Direktive 95/46 (katerega vsebina je v bistvu povzeta v členu 23(1) GDPR), med katerimi sta javna in državna varnost. In obratno, neupoštevanje teh klavzul zaradi uskladitve z nezdružljivo obveznostjo, ki izhaja iz prava namembne tretje države in presega to, kar je sorazmerno z zaščito legitimnega interesa, ki ga priznava Unija, se obravnava kot kršitev navedenih klavzul.

132. Po mojem mnenju klavzule 5(a) – kot sta navedla M. Schrems in Komisija – ni mogoče razlagati tako, da pomeni, da je prekinitev prenosa ali odstop od pogodbe zgolj možnost, če uvoznik ne more spoštovati standardnih klavzul. Čeprav je v tej klavzuli omenjena zgolj upravičenost v tem smislu v korist izvoznika, je treba to besedilo razumeti v povezavi s pogodbenim okvirom, v katerega se umešča. Dejstvo, da je izvoznik *v svojih dvostranskih razmerjih z uvoznikom* upravičen prekiniti prenos ali odstopiti od pogodbe, če uvoznik ne more spoštovati standardnih klavzul, ne vpliva na obveznost, ki jo ima izvoznik, da ravna tako *glede na zahteve po varstvu pravic posameznikov, na katere se nanašajo osebni podatki, izhajajoče iz GDPR*. Vsaka druga razlaga bi povzročila neveljavnost Sklepa 2010/87, ker standardne pogodbene klavzule, ki jih določa, ne bi omogočale, da bi prenos spremljali „ustrezni zaščitni ukrepi“, kot se zahteva s členom 46(1) GDPR, razlaganim ob upoštevanju določb Listine. [50]

133. Poleg tega v skladu s klavzulo 5(b) uvoznik potrdi, da nima razloga za domnevo, da mu zakonodaja, ki velja zanj, preprečuje izpolnjevanje navodil izvoznika in obveznosti iz pogodbe. V primeru spremembe te zakonodaje, ki bo verjetno imela znaten negativen učinek na jamstva in obveznosti iz standardnih klavzul, mora to spremembo sporočiti izvozniku takoj, ko zanjo izve, izvoznik pa je v tem primeru upravičen prekiniti prenos podatkov in/ali odstopiti od pogodbe. V skladu s klavzulo 4(g) mora izvoznik obvestilo, prejeto od uvoznika, posredovati pristojnemu nadzornemu organu, če se odloči nadaljevati prenos.

134. Tu se mi zdi potrebno zagotoviti nekaj pojasnil glede vsebine preučitve, ki jo morata opraviti stranki pogodbe, da z vidika opombe h klavzuli 5 ugotovita, ali obveznosti, ki so s pravom tretje države naložene uvozniku, pripeljejo do kršitve standardnih klavzul in torej preprečujejo, da bi prenos spremljali ustrezni zaščitni ukrepi. Ta problematika je bila v bistvu izpostavljena v okviru drugega dela šestega vprašanja za predhodno odločanje.

135. Taka preučitev po mojem mnenju vključuje upoštevanje vseh okoliščin, ki opredeljujejo vsak prenos ter ki lahko zajemajo naravo podatkov in njihovo morebitno občutljivost, mehanizme, ki jih izvoznik in/ali uvoznik izvajata za zagotovitev njihove varnosti, [51] naravo in namen obdelave, katere predmet bodo podatki, s strani javnih organov tretje države, podrobnosti te obdelave ter omejitve in zaščitne ukrepe, ki jih zagotavlja ta tretja država. Elementi, značilni za dejavnosti obdelave, ki jih izvajajo javni organi, in za zaščitne ukrepe, ki se uporabljajo v pravnem redu navedene tretje države, se lahko po mojem mnenju prekrivajo s tistimi, ki jih določa člen 45(2) GDPR.

136. Drugič, standardne pogodbene klavzule iz Priloge k Sklepu 2010/87 v korist posameznikov, na katere se nanašajo osebni podatki, določajo izvršljive pravice in pravna sredstva proti izvozniku in, podredno, uvozniku.

50 Iz sodne prakse izhaja, da je treba določbe izvedbenega akta razlagati v skladu z določbami temeljnega akta, s katerim je zakonodajalec dovolil njegovo sprejetje (glej v tem smislu zlasti sodbe z dne 26. julija 2017, Češka republika/Komisija (C-696/15 P, EU:C:2017:595, točka 51); z dne 17. maja 2018, Evonik Degussa (C-229/17, EU:C:2018:323, točka 29), in z dne 20. junija 2019, ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518, točka 112)). Poleg tega je treba akt Unije, če je le mogoče, razlagati tako, da se ne vzbuja dvom o njegovi veljavnosti, in v skladu s celotnim primarnim pravom ter med drugim z določbami Listine (glej zlasti sodbo z dne 14. maja 2019, M in drugi (Preklic statusa begunca) (C-391/16, C-77/17 in C-78/17, EU:C:2019:403, točka 77 in navedena sodna praksa)).

51 V zvezi s tem sta v uvodni izjavi 109 GDPR izvoznik in uvoznik spodbujena, naj standardnim določilom o varstvu dodata dodatne zaščitne ukrepe, zlasti s pogodbenimi sredstvi.

137. Tako klavzula 3, naslovljena „Korist tretjega“, v odstavku 1 določa pravno sredstvo posameznika, na katerega se nanašajo osebni podatki, proti izvozniku v primeru kršitve med drugim klavzule 5(a) ali (b). V skladu s klavzulo 3(2) lahko posameznik, na katerega se nanašajo osebni podatki, proti uvozniku uveljavlja to klavzulo, če izvoznik dejansko izgine ali pravno preneha obstajati.

138. Na podlagi klavzule 6(1) je vsak posameznik, na katerega se nanašajo osebni podatki, ki je zaradi kršitve obveznosti iz klavzule 3 utrpel škodo, upravičen od izvoznika prejeti odškodnino za utrpelo škodo. V skladu s klavzulo 7(1) uvoznik soglaša, da bo – če posameznik, na katerega se nanašajo osebni podatki, zoper uvoznika uveljavlja pravice kot upravičena tretja stranka in/ali odškodninski zahtevek – sprejel odločitev tega posameznika, da bodisi spor predloži v mediacijo, ki jo izvede neodvisna oseba ali, če je primerno, nadzorni organ, bodisi spor predloži sodiščem v državi članici, v kateri je sedež izvoznika.

139. Poleg pravnih sredstev, ki jih imajo posamezniki, na katere se nanašajo osebni podatki, na voljo na podlagi standardnih pogodbenih klavzul iz Priloge k Sklepu 2010/87, lahko ti posamezniki, če menijo, da so bile te klavzule kršene, od nadzornih organov zahtevajo sprejetje popravljalnih ukrepov na podlagi člena 58(2) GDPR, na katerega se sklicuje člen 4 Sklepa 2010/87.[52]

2. Obveznosti, ki jih imajo nadzorni organi

140. Iz v nadaljevanju navedenih razlogov menim – enako kot M. Schrems, Irska ter nemška, avstrijska, belgijska, nizozemska in portugalska vlada ter EOVP – da so na podlagi člena 58(2) GDPR nadzorni organi, ko ob koncu skrbne preučitve ocenijo, da podatki, preneseni v tretjo državo, niso predmet ustreznega varstva zaradi nespoštovanja dogovorjenih pogodbenih klavzul, dolžni sprejeti primerne ukrepe za odpravo te nezakonitosti, po potrebi tako, da odredijo prekinitev prenosa.

141. Prvič, v nasprotju s tem, kar trdi DPC, ugotavljam, da izvrševanje pooblastil, ki jih imajo nadzorni organi na podlagi člena 58(2)(f) in (j) GDPR, da „uvede[jo] začasno ali dokončno omejitev obdelave, vključno s prepovedjo obdelave“, in da „odredi[jo] prekinitev prenosov podatkov uporabniku v tretji državi“, z nobeno določbo Sklepa 2010/87 ni omejeno na izjemne primere.

142. V prvotni različici člena 4 Sklepa 2010/87 je bilo v njegovem odstavku 1 izvrševanje pooblastil nadzornih organov, da prekinejo ali prepovejo čezmejni pretok podatkov, resda omejeno na nekatere primere, v katerih je bila ugotovljena verjetnost, da bi lahko imel prenos na pogodbeni podlagi precej škodljivih posledic za jamstva, namenjena varstvu posameznika, na katerega se nanašajo osebni podatki. Vendar se člen 4 tega sklepa, kot ga je Komisija spremenila leta 2016 zaradi uskladitve s sodbo Schrems,[53] zdaj zgolj sklicuje na zadevna pooblastila, ne da bi bila ta kakor koli omejena. Vsekakor z izvedbenim sklepom Komisije, kot je Sklep 2010/87, ni mogoče veljavno omejevati pooblastil, podeljenih nadzornim organom na podlagi GDPR.[54]

143. Te ugotovitve ne ovrže točka 11 obrazložitve Sklepa 2010/87, v kateri je navedeno, da lahko nadzorni organi pooblastila za prekinitev in prepoved prenosov izvršujejo le v „izjemnih primerih“. Ta točka obrazložitve, navzoča že v prvotni različici tega sklepa, se je navezovala na nekdanji člen 4(1) navedenega sklepa, s katerim so bila pooblastila nadzornih organov omejena. Ob reviziji Sklepa 2010/87 s Sklepom 2016/2297 Komisija navedene točke obrazložitve ni črtala ali spremenila, da bi njeno vsebino prilagodila vsebini določb novega člena 4. Vendar je bilo v točki 5 obrazložitve Sklepa

52 Čeprav se člen 4(1) Sklepa 2010/87 sklicuje na člen 28(3) Direktive 95/46, naj spomnim, da je treba v skladu s členom 94(2) GDPR sklicevanja na to direktivo šteti za sklicevanja na ustrezne določbe GDPR.

53 Glej točki 6 in 7 obrazložitve Sklepa 2016/2297. V točkah od 101 do 104 sodbe Schrems je Sodišče odločilo, da določba Odločbe o varnem pristanu, s katero so bila pooblastila, podeljena nadzornim organom s členom 28 Direktive 95/46, omejena na „izjemne primere“, ni veljavna, ker Komisija ni imela pristojnosti za zožitev teh pooblastil.

54 Glej sodbo Schrems (točka 103).

2016/2297 znova potrjeno pooblastilo nadzornih organov za prekinitev ali prepoved vsakega prenosa, kadar menijo, da je ta v nasprotju s pravom Unije zlasti zaradi uvoznikovega nespoštovanja standardnih pogodbenih klavzul. Točko 11 obrazložitve Sklepa 2010/87 v delu, v katerem je zdaj v nasprotju z besedilom in ciljem njegove pravno zavezujoče določbe, je treba opredeliti kot zastarelo. [55]

144. Drugič, v nasprotju s tem, kar tudi trdi DPC, izvrševanje pooblastil za prekinitev in prepoved, ki so določena v členu 58(2)(f) in (j) GDPR, prav tako ne pomeni zgolj možnosti, ki je prepuščena diskreciji nadzornih organov. Ta ugotovitev po mojem mnenju izhaja iz razlage člena 58(2) GDPR z vidika drugih določb te uredbe in Listine, pa tudi iz splošne sistematike in ciljev Sklepa 2010/87.

145. Zlasti je treba člen 58(2) GDPR razlagati glede na člen 8(3) Listine in člen 16(2) PDEU. V skladu s tema določbama upoštevanje zahtev, ki jih vključuje temeljna pravica do varstva osebnih podatkov, nadzirajo neodvisni organi. Ta naloga nadzora upoštevanja zahtev v zvezi z varstvom osebnih podatkov, ki je omenjena tudi v členu 57(1)(a) GDPR, vključuje obveznost nadzornih organov ravnati tako, da zagotovijo pravilno uporabo te uredbe.

146. Tako mora nadzorni organ z vso potrebno skrbnostjo preučiti pritožbo, ki jo vloži oseba, katere podatki se domnevno prenašajo v tretjo državo v nasprotju s standardnimi pogodbenimi klavzulami, ki se uporabljajo za prenos. [56] S členom 58(1) GDPR so nadzornim organom zato podeljena precejšnja preiskovalna pooblastila. [57]

147. Pristojni nadzorni organ se mora tudi primerno odzvati na morebitne kršitve pravic posameznika, na katerega se nanašajo osebni podatki, ki bi jih ugotovil ob koncu svoje preiskave. V zvezi s tem vsak nadzorni organ na podlagi člena 58(2) GDPR razpolaga s širokim naborom sredstev – raznih pooblastil za sprejetje popravljalnih ukrepov, ki so našteta v tej določbi – za izpolnitev naloge, ki mu je bila zaupana. [58]

148. Čeprav izbira najbolj učinkovitega sredstva spada v diskrecijo pristojnega nadzornega organa glede na vse okoliščine zadevnega prenosa, mora ta organ v celoti izpolniti nalogo nadzora, ki mu je bila zaupana. Po potrebi mora navedeni organ prekiniti prenos, če ugotovi, da se standardne pogodbene klavzule ne spoštujejo in da ustreznega varstva prenesenih podatkov ni mogoče zagotoviti z drugimi sredstvi, kadar izvoznik ni sam končal prenosa.

149. To razlago potrjuje člen 58(4) GDPR, ki določa, da nadzorni organ izvršuje pooblastila, ki so mu dodeljena v skladu s tem členom, na podlagi ustreznih zaščitnih ukrepov, vključno z učinkovitim pravnim sredstvom v skladu s členom 47 Listine. V členu 78(1) in (2) GDPR se poleg tega priznava pravica vsake osebe do učinkovitega pravnega sredstva zoper pravno zavezujočo odločitev, ki jo nadzorni organ sprejme v zvezi z njo, ali kadar ta organ ne obravnava njene pritožbe. [59]

150. Kot v bistvu zatrjujejo M. Schrems, BSA, Irska ter poljska vlada in vlada Združenega kraljestva ter Komisija, te določbe pomenijo, da se zoper odločitev, s katero nadzorni organ ne prepove ali ne prekine prenosa v tretjo državo na zahtevo osebe, ki zatrjuje tveganje, da se v tej državi podatki, ki se nanašajo nanjo, obdelujejo v nasprotju z njenimi temeljnimi pravicami, lahko vloži pravno sredstvo. Priznavanje pravice do pravnega sredstva pa predpostavlja obstoj vezane, in ne povsem diskrecijske

55 Vsekakor preambula akta Unije nima pravno zavezujoče veljave in se nanjo ni mogoče sklicevati zato, da se odstopi od samih določb tega akta. Glej sodbe z dne 19. novembra 1998, Nilsson in drugi (C-162/97, EU:C:1998:554, točka 54); z dne 12. maja 2005, Meta Fackler (C-444/03, EU:C:2005:288, točka 25), in z dne 10. januarja 2006, IATA in ELFAA (C-344/04, EU:C:2006:10, točka 76).

56 Glej po analogiji sodbo Schrems (točka 63).

57 Dodati moram, da v skladu s klavzulo 8(2) iz Priloge k Sklepu 2010/87 stranki pogodbe soglašata, da nadzornemu organu podelita pooblastilo za izvedbo pregleda uvoznika pod enakimi pogoji, ki bi veljali za pregled izvoznika v skladu z veljavnim pravom.

58 Glej v tem smislu sodbo Schrems (točka 43).

59 V skladu z uvodno izjavo 141 GDPR mora vsak posameznik imeti pravico do učinkovitega pravnega sredstva v skladu s členom 47 Listine, če nadzorni organ „ne ukrepa, kadar je tak ukrep potreben za zaščito pravic [tega] posameznika“. Glej tudi uvodni izjavi 129 in 143 GDPR.

pristojnosti nadzornih organov. Poleg tega sta M. Schrems in Komisija pravilno poudarila, da izvajanje učinkovitega sodnega nadzora pomeni, da organ, ki je avtor izpodbijanega akta, ta akt ustrezno obrazloži.[60] Ta obveznost obrazložitve po mojem mnenju pokriva izbiro nadzornih organov, da uporabijo eno ali drugo izmed pooblastil, ki so jim podeljena s členom 58(2) GDPR.

151. Vendar je treba odgovoriti še na trditve, s katerimi DPC zatrjuje, da tudi če bi nadzorni organi morali prekiniti ali prepovedati prenos, kadar to zahteva varstvo pravic posameznika, na katerega se nanašajo osebni podatki, veljavnost Sklepa 2010/87 vseeno ne bi bila zagotovljena.

152. Prvič, DPC meni, da taka obveznost ne bi odpravila sistemskih problemov v zvezi z neobstojem ustreznih zaščitnih ukrepov v tretji državi, kot so Združene države. Nadzorni organi lahko namreč svoja pooblastila izvršujejo le v vsakem primeru posebej, medtem ko naj bi bile vrzeli, ki so značilne za ameriško pravo, splošne in strukturne. Zaradi tega naj bi obstajalo tveganje, da različni nadzorni organi sprejmejo razhajajoče se odločitve za primerljive prenose.

153. V zvezi s tem ne morem prezreti praktičnih težav, povezanih z zakonodajno izbiro, da se nadzornim organom naloži odgovornost za zagotavljanje spoštovanja temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, v okviru posameznih prenosov ali pretoka podatkov k določenemu uporabniku. Vendar se mi ne zdi, da te težave povzročijo neveljavnost Sklepa 2010/87.

154. Zdi se mi namreč, da pravo Unije ne zahteva, da se za vse prenose v dano tretjo državo, ki bi lahko vključevali ista tveganja kršitve temeljnih pravic, uporabi splošna in preventivna rešitev.

155. Poleg tega je tveganje razdrobljenosti pristopov, ki jim sledijo različni nadzorni organi, sestavni del zasnove decentraliziranega nadzora, ki ga je želel zakonodajalec.[61] Vrh tega se, kot je poudarila nemška vlada, s poglavjem VII GDPR, naslovljenim „Sodelovanje in skladnost“, uvajajo mehanizmi, ki so namenjeni preprečevanju tega tveganja. Člen 60 te uredbe v primeru čezmejne obdelave podatkov določa postopek za sodelovanje med zadevnimi nadzorni organi in nadzornim organom ustanovitve upravljavca, imenovanim „vodilni nadzorni organ“.[62] V primeru nasprotujočih si stališč mora nesoglasje rešiti EOVP.[63] Ta ima tudi pristojnost, da na zahtevo nadzornega organa izdaja mnenja o vsaki zadevi, ki ima pomen za več držav članic.[64]

156. Drugič, DPC se sklicuje na neveljavnost Sklepa 2010/87 glede na člen 47 Listine, ker lahko nadzorni organi pravice posameznikov, na katere se nanašajo osebni podatki, varujejo le za naprej, ne da bi ponujali rešitev tistim, katerih podatki so bili že preneseni. DPC zlasti poudarja, da člen 58(2) GDPR ne določa niti pravice do dostopa do podatkov, ki jih zberejo javni organi tretje države, ter do njihovega popravka in izbrisa niti možnosti za posameznike, na katere se nanašajo osebni podatki, da pridobijo odškodnino za nastalo škodo.

157. V zvezi z zatrjevanim neobstojem pravice do dostopa do zbranih podatkov ter do njihovega popravka in izbrisa je treba ugotoviti, da kadar v namembni tretji državi ni nobenega učinkovitega pravnega sredstva, pravna sredstva, ki so zoper upravljavca na voljo v Uniji, ne omogočajo, da bi se pri javnih organih te tretje države dosegel dostop do teh podatkov ali njihov popravek ali izbris.

60 Glej med drugim sodbi z dne 28. julija 2011, Samba Diouf (C-69/10, EU:C:2011:524, točka 57), in z dne 17. novembra 2011, Gaydarov (C-430/10, EU:C:2011:749, točka 41).

61 Glej v zvezi s tem sodbo z dne 5. junija 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, točke od 69 do 73).

62 Glej člen 56(1) GDPR. V skladu s členom 61 te uredbe so nadzorni organi dolžni drug drugemu zagotavljati medsebojno pomoč. S členom 62 navedene uredbe jim je dovoljeno skupno ukrepanje.

63 Glej člen 65 GDPR.

64 Glej člen 64(2) GDPR.

158. Vendar po mojem mnenju ta ugovor ne utemeljuje nezdružljivosti Sklepa 2010/87 s členom 47 Listine. Veljavnost tega sklepa namreč ni odvisna od ravni varstva v vsaki tretji državi, v katero bi se lahko podatki prenašali na podlagi standardnih pogodbenih klavzul, ki jih navedeni sklep določa. Če pravo namembne tretje države uvozniku preprečuje spoštovanje teh klavzul, ker zahteva, da javnim organom dopusti dostop do podatkov, zoper ta dostop pa ni mogoče vložiti primernih pravnih sredstev, morajo nadzorni organi, če upravljavec ni prekinil prenosa na podlagi klavzule 5(a) ali (b) iz Priloge k Sklepu 2010/87, sprejeti popravljalne ukrepe.

159. Poleg tega, kot je poudaril M. Schrems, imajo osebe, katerih pravice so bile kršene, zdaj na podlagi člena 82 GDPR pravico do odškodnine za premoženjsko ali nepremoženjsko škodo, nastalo zaradi kršitve te uredbe, ki jo plača upravljavec ali obdelovalec.[65]

160. Kot izhaja iz vseh teh preudarkov, moja analiza ni razkrila nobenega elementa, ki bi lahko vplival na veljavnost Sklepa 2010/87 glede na člene 7, 8 in 47 Listine.

F. Neobstoj nujnosti odgovoriti na preostala vprašanja za predhodno odločanje in preizkusiti veljavnost Sklepa o zasebnostnem ščitu

161. V tem oddelku predstavljam razloge, povezane predvsem z omejenostjo predmeta spora o glavni stvari na veljavnost Sklepa 2010/87, iz katerih menim, da ni treba odgovoriti na drugo, tretje, četrto, peto, deveto in deseto vprašanje za predhodno odločanje niti odločiti o veljavnosti Sklepa o zasebnostnem ščitu.

162. Drugo vprašanje za predhodno odločanje se nanaša na določitev standardov varstva, ki jih morajo tretje države upoštevati, da se lahko podatki zakonito prenašajo vanje na podlagi standardnih pogodbenih klavzul, če je za te podatke mogoče, da jih po prenosu organi te tretje države obdelujejo zaradi nacionalne varnosti. Tretje vprašanje, predloženo Sodišču, zadeva določitev elementov, ki opredeljujejo ureditev varstva, veljavno v namembni tretji državi, in ki jih je treba upoštevati pri preverjanju, ali ta ureditev ustreza tem standardom.

163. S četrtim, petim in desetim vprašanjem želi predložitveno sodišče v bistvu izvedeti, ali so glede na dejstva, ki jih je ugotovilo v zvezi s pravom Združenih držav, v tej državi določeni ustrezni zaščitni ukrepi pred posegi ameriških obveščevalnih organov v uresničevanje temeljnih pravic do spoštovanja zasebnega življenja, varstva osebnih podatkov in učinkovitega sodnega varstva.

164. Deveto vprašanje za predhodno odločanje se nanaša na posledice, ki jih ima v okviru preučitve, s katero nadzorni organ preveri, ali prenos v Združene države na podlagi standardnih pogodbenih klavzul iz Sklepa 2010/87 spremljajo ustrezni zaščitni ukrepi, okoliščina, da je Komisija v Sklepu o zasebnostnem ščitu ugotovila, da Združene države zagotavljajo ustrezno raven varstva temeljih pravic posameznikov, na katere se nanašajo osebni podatki, pred takimi posegi.

165. Predložitveno sodišče ni izrecno postavilo vprašanja veljavnosti Sklepa o zasebnostnem ščitu, čeprav se, kot je pojasnjeno v nadaljevanju,[66] s četrtim, petim in desetim vprašanjem za predhodno odločanje posredno dvomi o utemeljenosti ugotovitve o ustreznosti, do katere je Komisija prišla v tem sklepu.

65 Člen 83(5)(c) GDPR določa tudi globe, ki se naložijo upravljavcu v primeru kršitve členov od 44 do 49 te uredbe.

66 Glej točko 175 teh sklepnih predlogov.

166. Po mojem mnenju glede na elemente, ki izhajajo iz zgornje analize, pojasnila Sodišča glede teh vprašanj ne bi mogla vplivati na njegovo ugotovitev v zvezi z veljavnostjo *in abstracto* Sklepa 2010/87 in torej niti na rešitev spora o glavni stvari (razdelek 1). Poleg tega, čeprav bi se odgovori Sodišča na navedena vprašanja v poznejši fazi lahko izkazali kot koristni za to, da bi DPC v okviru postopka, na katerem temelji ta spor, ugotovil, ali je treba *in concreto* zadevne prenose prekiniti zaradi domnevnega neobstoja ustreznih zaščitnih ukrepov, bi bilo po mojem mnenju prezgodaj zadevna vprašanja obravnavati v okviru te zadeve (razdelek 2).

1. Neobstoj nujnosti odgovorov Sodišča glede na predmet spora o glavni stvari

167. Spor o glavni stvari izvira, naj spomnim, iz tega, da je DPC uveljavljal pravno sredstvo, opisano v točki 65 sodbe Schrems, v skladu s katero mora vsaka država članica nadzornemu organu omogočiti, da – kadar meni, da je to potrebno za odločitev o pritožbi o kateri odloča – nacionalnemu sodišču predlaga, naj Sodišču predloži vprašanje za predhodno odločanje glede veljavnosti sklepa o ustreznosti ali, po analogiji, sklepa o določitvi standardnih pogodbenih klavzul.

168. V zvezi s tem je High Court (višje sodišče) poudarilo, da sta bili edini možnosti, ki ju je imelo po tem, ko se je nanj obrnil DPC, ti, da bodisi sproži postopek predhodnega odločanja glede veljavnosti Sklepa 2010/87, kot je predlagal DPC, če bi se strinjalo z njegovimi dvomi o veljavnosti tega sklepa, bodisi v nasprotnem primeru zavrne ta predlog. To sodišče meni, da če bi uporabilo drugo navedeno pot, bi moralo končati postopek, ker pritožba DPC ne bi imela drugega predmeta.[67]

169. V istem smislu je Supreme Court (vrhovno sodišče), pri katerem je družba Facebook Ireland vložila pritožbo zoper predložitveni sklep, spor o glavni stvari opisalo kot ugotovitveni postopek, s katerim je DPC predložitvenemu sodišču predlagal, naj Sodišču postavi vprašanje za predhodno odločanje glede veljavnosti Sklepa 2010/87. Po besedah irskega vrhovnega sodišča se zato edino bistveno vprašanje, ki se postavlja pred predložitvenim sodiščem in pred Sodiščem, nanaša na veljavnost tega sklepa.[68]

170. Ob upoštevanju tako opredeljenega predmeta spora o glavni stvari je predložitveno sodišče Sodišču predložilo svojih prvih deset vprašanj, ker je menilo, da bo njihova preučitev del celovite presoje, ki bo potrebna, da bi Sodišče v odgovor na enajsto vprašanje odločilo o veljavnosti Sklepa 2010/87 glede na člene 7, 8 in 47 Listine. Kot je navedeno v predložitvenem sklepu, je to vprašanje logični rezultat predhodnih vprašanj.

171. S tega vidika se mi drugo, tretje, četrto, peto, deveto in deseto vprašanje za predhodno odločanje zdijo podprta s premiso, da bo veljavnost Sklepa 2010/87 odvisna od ravni varstva temeljnih pravic, določenega v vsaki tretji državi, v katero se lahko podatki prenašajo na podlagi standardnih pogodbenih klavzul, ki jih ta sklep določa. Kot pa izhaja iz moje analize sedmega vprašanja,[69] je ta premisa po mojem mnenju napačna. Preučitev prava namembne tretje države je upoštevna šele takrat, ko Komisija sprejme sklep o ustreznosti ali ko upravljavec – ali, če ne on, pristojni nadzorni organ – preveri, ali v okviru prenosa, ki temelji na ustreznih zaščitnih ukrepih v smislu člena 46(1) GDPR, obveznosti, ki so s pravom te tretje države naložene uvozniku, ne ogrožajo učinkovitosti varstva, zagotovljenega s temi zaščitnimi ukrepi.

67 Sodba High Court (višje sodišče) z dne 3. oktobra 2017 (točka 337).

68 V skladu s sodbo Supreme Court (vrhovno sodišče) z dne 31. maja 2019 (točka 2.7) „[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [PDEU]“. V točki 2.9 te sodbe je dalje navedeno: „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*“ (moj poudarek).

69 Glej točko 124 teh sklepnih predlogov.

172. Zato odgovori Sodišča na zgoraj omenjena vprašanja ne morejo vplivati na njegovo ugotovitev v zvezi z enajstim vprašanjem.[70] Tako tudi z vidika predmeta spora o glavni stvari ni treba odgovoriti nanje.

173. Sodišču predlagam, naj se omeji na obravnavo te zadeve le z vidika predmeta tega spora. Po mojem mnenju Sodišče ne bi smelo preseči tega, kar je potrebno za rešitev navedenega spora, tako da bi se vprašanj za predhodno odločanje lotevalo z vidika temeljnega postopka, ki poteka pred DPC. Kot je pojasnjeno v nadaljevanju, ta poziv k zadržanosti izhaja po eni strani iz skrbi, da se ne bi oviral normalen potek postopka, ki se bo moral nadaljevati pred DPC, ko bo Sodišče odločilo o veljavnosti Sklepa 2010/87. Po drugi strani bi se mi glede na dejstva obravnavane zadeve zdelo nekoliko prenagljeno, tudi z vidika pomena tega postopka, da bi Sodišče obravnavalo probleme, ki se postavljajo z drugim, tretjim, četrtim, petim, devetim in desetim vprašanjem.

2. Razlogi proti preučitvi, ki bi jo Sodišče opravilo z vidika predmeta postopka, ki poteka pred DPC

174. M. Schrems v svoji pritožbi pred DPC od tega nadzornega organa zahteva, naj izvrši pooblastilo, ki ga ima na podlagi člena 58(2)(f) GDPR, in družbi Facebook Ireland odredi prekinitev prenosa njegovih osebnih podatkov v Združene države na podlagi pogodbenih klavzul. V utemeljitev te zahteve se M. Schrems v bistvu sklicuje na neustreznost teh pogodbenih zaščitnih ukrepov zaradi posegov v uresničevanje njegovih temeljnih pravic, ki so posledica dejavnosti ameriških obveščevalnih služb.

175. M. Schrems s svojimi trditvami dvomi o ugotovitvi, do katere je Komisija prišla v Sklepu o zasebnostnem ščitu in v skladu s katero Združene države zagotavljajo ustrezno raven varstva podatkov, prenesenih na podlagi tega sklepa, ob upoštevanju omejitev, uvedenih za dostop do teh podatkov in njihovo uporabo od ameriških obveščevalnih organov ter za pravno varstvo, zagotovljeno posameznikom, na katere se nanašajo osebni podatki.[71] Pomisleki, ki jih začasno izraža DPC,[72] izraža pa jih tudi predložitveno sodišče v okviru četrtega, petega in desetega vprašanja, prav tako posredno vzbujajo dvom o utemeljenosti te ugotovitve.

176. Seveda je Sklep o zasebnostnem ščitu omejen na ugotavljanje ustreznosti ravni varstva osebnih podatkov, prenesenih v skladu z načeli, ki jih določa, podjetju s sedežem v Združenih državah, ki je s samocertificiranjem potrdilo svoje spoštovanje teh načel.[73] Vendar preudarki, navedeni v njem, presegajo okvir prenosov, zajetih s tem sklepom, ker se nanašajo na veljavno pravo in prakse v tej tretji državi v zvezi z obdelavo prenesenih podatkov zaradi varovanja nacionalne varnosti. Kot so

70 Iz istega razloga je Supreme Court (vrhovno sodišče) v sodbi z dne 31. maja 2019 (točke od 8.1 do 8.5), čeprav je priznalo, da ni pristojno, da bi podvomilo o sklepu predložitvenega sodišča, s katerim je to Sodišču predložilo vprašanja za predhodno odločanje, in da bi spreminjalo njegovo besedilo, izrazilo dvome o nujnosti nekaterih od teh vprašanj. Natančneje, v točki 8.5 te sodbe je navedeno: „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 Glej točke od 64 do 141 obrazložitve Sklepa o zasebnostnem ščitu. Naj spomnim, kot izhaja iz člena 1(2) tega sklepa, da zasebnostni ščit ne sestavljajo le načela, ki jih morajo spoštovati podjetja, ki želijo prenašati podatke na podlagi navedenega sklepa, temveč tudi uradna zagotovila in zaveze, ki jih je dala vlada Združenih držav in so navedeni v dokumentih, priloženih zadevnemu sklepu.

72 Osnutek odločbe DPC je nastal pred sprejetjem Sklepa o zasebnostnem ščitu. DPC je v tem osnutku pojasnil, da v njem začasno sicer ugotavlja, da zaščitni ukrepi, določeni s pravom Združenih držav, ne omogočajo vsaj tega, da bi se zagotovila skladnost prenosov v to tretjo državo s členom 47 Listine, vendar *v tej fazi ne preučuje ali upošteva novih ureditev, načrtovanih v osnutku sporazuma o zasebnostnem ščitu, ker ta še ni bil sprejet*. Ob tem High Court (višje sodišče) v točki 307 sodbe z dne 3. oktobra 2017 meni: „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 Glej člen 1(1) in (3) ter točke od 14 do 16 obrazložitve Sklepa o zasebnostnem ščitu.

v bistvu opozorili družba Facebook Ireland, M. Schrems, vlada Združenih držav in Komisija, se nadzor, ki ga izvajajo ameriški obveščevalni organi, pa tudi zaščitni ukrepi pred tveganji zlorabe, ki jih vključuje, in mehanizmi za nadzor njihovega spoštovanja uporabljajo ne glede na to, katera je z vidika prava Unije pravna podlaga, ki se navaja v podporo prenosu.

177. S tega vidika bi se vprašanje, ali so ugotovitve, podane na to temo v Sklepu o zasebnostnem ščitu, zavezujoče za nadzorne organe, ko preučujejo zakonitost prenosa, izvedenega na podlagi standardnih pogodbenih klavzul, lahko izkazalo za upoštevno za obravnavo pritožbe M. Schremsa pred DPC. V primeru pritrdilnega odgovora na to vprašanje bi se postavljalo vprašanje, ali je ta sklep res veljaven.

178. Vendar Sodišču odsvetujem, da odloči o teh vprašanjih zgolj zato, da bi pomagalo DPC pri obravnavi te pritožbe, medtem ko nanje ni treba odgovoriti, da bi se predložitvenemu sodišču omogočila rešitev spora o glavni stvari. Ker se s postopkom iz člena 267 PDEU uvaja dialog med sodišči, Sodišču ni treba podajati pojasnil le z namenom pomagati upravnemu organu v okviru postopka, na katerem temelji ta spor.

179. Zadržanost je po mojem mnenju še toliko bolj potrebna, ker mu vprašanje veljavnosti Sklepa o zasebnostnem ščitu ni bilo izrecno postavljeno, pri čemer je ta sklep poleg tega že predmet ničnostne tožbe v postopku, ki poteka pred Splošnim sodiščem Evropske unije.[74]

180. Poleg tega bi Sodišče z odločitvijo o zgoraj opisanih problemih po mojem mnenju zmotilo normalen potek postopka, ki ga bo treba izpeljati po tem, ko bo izreklo svojo sodbo v obravnavani zadevi. V okviru navedenega postopka bo moral DPC obravnavati pritožbo M. Schremsa ob upoštevanju odgovora, ki ga bo Sodišče dalo na enajsto vprašanje za predhodno odločanje. Če bi Sodišče, tako kot mu predlagam, in v nasprotju s tem, kar je pred njim trdil DPC, presodilo, da Sklep 2010/87 ni neveljaven glede na člene 7, 8 in 47 Listine, bi moral DPC po mojem mnenju dobiti možnost ponovno preučiti spis v postopku, ki poteka pred njim. Če bi DPC menil, da ne more odločiti o pritožbi M. Schremsa, ne da bi Sodišče prej ugotovilo, ali Sklep o zasebnostnem ščitu pomeni oviro za izvrševanje njegovih pooblastil za prekinitev zadevnega prenosa, in bi potrdil, da ima dvome o veljavnosti tega sklepa, bi se lahko svobodno znova obrnil na nacionalna sodišča, da bi ta Sodišču predložila vprašanja glede tega.[75]

181. Nato bi se sprožil postopek, v katerem bi lahko vse stranke in zainteresirani subjekti iz člena 23, drugi odstavek, Statuta Sodišča Sodišču predložili stališča posebej v zvezi z veljavnostjo Sklepa o zasebnostnem ščitu, pri čemer bi po potrebi navedli posamezne presoje, ki jih izpodbijajo, in razloge, iz katerih menijo, da je Komisija v njem prekoračila zmanjšano polje proste presoje, s katerim je razpolagala.[76] V okviru takega postopka bi Komisija imela priložnost natančno in podrobno odgovoriti na vsakega od morebitnih očitkov zoper navedeni sklep. Čeprav so v obravnavni zadevi stranke in zainteresirani subjekti, ki so Sodišču predložili stališča, dobili priložnost razpravljati o nekaterih upoštevnih vidikih za presojo skladnosti Sklepa o zasebnostnem ščitu s členi 7, 8 in 47 Listine, je temu vprašanju glede na njegov pomen vredno nameniti izčrpno in poglobljeno razpravo.

182. Po mojem mnenju previdnost narekuje, da se počaka, da se te postopkovne faze zaključijo, preden Sodišče preuči učinke Sklepa o zasebnostnem ščitu na obravnavo, ki jo nadzorni organ nameni zahtevi za prekinitev prenosa, izvedenega v Združene države na podlagi člena 46(1) GDPR, in preden odloči o veljavnosti tega sklepa.

74 Še nerešena zadeva T-738/16, La Quadrature du Net in drugi/Komisija (UL 2017, C 6, str. 39).

75 Poleg tega ugotavljam, da se DPC v pisnem stališču ni opredelil do učinkov Sklepa o zasebnostnem ščitu na obravnavo pritožbe, o kateri odloča.

76 Glej v zvezi s tem sodbo Schrems (točka 78).

183. To velja še toliko bolj, ker na podlagi spisa, predloženega Sodišču, ni mogoče sklepati, da bo obravnava pritožbe M. Schremsa pred DPC nujno odvisna od vprašanja, ali Sklep o zasebnostnem ščitu nasprotuje temu, da nadzorni organi izvršujejo svoje pooblastilo za prekinitev prenosa, ki temelji na standardnih pogodbenih klavzulah.

184. V zvezi s tem, prvič, ni izključeno, da bo moral DPC prekiniti zadevni prenos iz drugih razlogov od tistih, ki se nanašajo na domnevno neustreznost ravni varstva, ki se v Združenih državah zagotavlja pred posegi v temeljne pravice posameznikov, na katere se nanašajo osebni podatki, kot posledico dejavnosti ameriških obveščevalnih služb. Predložitveno sodišče je zlasti pojasnilo, da M. Schrems v pritožbi pred DPC zatrjuje, da pogodbene klavzule, na katere se družba Facebook Ireland sklicuje v podporo temu prenosu, niso dosleden izraz tistih, ki jih določa Priloga k Sklepu 2010/87. Poleg tega M. Schrems trdi, da navedeni prenos ne spada na področje uporabe tega sklepa, temveč na področje uporabe drugih sklepov SPK.[77]

185. Drugič, DPC in predložitveno sodišče sta poudarila, da se družba Facebook Ireland v podporo prenosu iz pritožbe M. Schremsa ni sklicevala na Sklep o zasebnostnem ščitu,[78] kar je ta družba potrdila na obravnavi. Čeprav je družba Facebook Inc. s samocertificiranjem potrdila svoje spoštovanje načel zasebnostnega ščita od 30. septembra 2016,[79] družba Facebook Ireland zatrjuje, da se to spoštovanje nanaša le na prenos nekaterih kategorij podatkov, in sicer tistih v zvezi s poslovnimi partnerji družbe Facebook Inc. Po mojem mnenju ne bi bilo primerno, da Sodišče predvideva vprašanja, ki bi se lahko pojavila v zvezi s tem, tako da preučuje, ali bi bil – ob predpostavki, da se družba Facebook Ireland ne more sklicevati na Sklep 2010/87 v podporo zadevnemu prenosu – ta prenos vseeno zajet s Sklepom o zasebnostnem ščitu, medtem ko zadnjenavedena družba ni podala te trditve ne pred predložitvenim sodiščem ne pred DPC.

186. Na podlagi tega ugotavljam, da na drugo, tretje, četrto, peto, deveto in deseto vprašanje za predhodno odločanje ni treba odgovoriti niti ni treba preizkusiti veljavnosti Sklepa o zasebnostnem ščitu.

G. Podredni preudarki glede učinkov in veljavnosti Sklepa o zasebnostnem ščitu

187. Čeprav na podlagi zgornje analize Sodišču primarno predlagam, naj se vzdrži odločanja o učinkih Sklepa o zasebnostnem ščitu na obravnavo pritožbe, kot je ta, ki jo je M. Schrems vložil pri DPC, in o veljavnosti tega sklepa, se mi zdi koristno podredno in s pridržki podati nekaj neizčrpnih preudarkov na to temo.

1. Učinki Sklepa o zasebnostnem ščitu v okviru obravnave, ki jo nadzorni organ nameni pritožbi v zvezi z zakonitostjo prenosa, temelječega na pogodbenih zaščitnih ukrepih

188. Z devetim vprašanjem za predhodno odločanje se sprašuje, ali ugotovitev, ki je podana v Sklepu o zasebnostnem ščitu in se nanaša na ustreznost ravni varstva, zagotovljene v Združenih državah, glede na omejitve, uvedene za dostop do prenesenih podatkov in njihovo uporabo od ameriških organov zaradi nacionalne varnosti ter za pravno varstvo posameznikov, na katere se nanašajo osebni podatki, pomeni oviro za to, da nadzorni organ prekine prenos v to tretjo državo, izveden na podlagi standardnih pogodbenih klavzul.

77 M. Schrems v utemeljitev te trditve navaja, da je treba družbo Facebook Inc. glede obdelave osebnih podatkov uporabnikov družabnega omrežja Facebook šteti ne le za obdelovalca, temveč tudi za „upravljavca“ v smislu člena 4, točka 7, GDPR. Glej v zvezi s tem sodbo z dne 5. junija 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, točka 30).

78 Glej sodbo High Court (višje sodišče) z dne 3. oktobra 2017 (točka 66).

79 Glej spletišče zasebnostnega ščita (https://www.privacyshield.gov/participant_search).

189. Zdi se mi, da je treba ta problem razumeti z vidika točk 51 in 52 sodbe Schrems, iz katerih izhaja, da je sklep o ustreznosti za nadzorne organe zavezujoč, dokler ni razglašen za neveljavnega. Nadzorni organ, ki odloča o pritožbi osebe, katere podatki se prenašajo v tretjo državo, ki jo zadeva sklep o ustreznosti, torej ne more prekiniti prenosa zato, ker raven varstva v njej ni ustrezna, če Sodišče prej ne razglasi neveljavnosti tega sklepa.[80]

190. Predložitveno sodišče želi v bistvu izvedeti, ali v zvezi s sklepom o ustreznosti – kot je Sklep o zasebnostnem ščitu ali pred njim Odločba o varnem pristanu – ki temelji na tem, da podjetja prostovoljno spoštujejo načela, določena v njem, ta ugotovitev velja le, če je prenos v zadevno tretjo državo zajet s tem sklepom, ali pa velja tudi, če prenos temelji na drugi pravni podlagi.

191. Po mnenju M. Schremsa ter nemške, nizozemske, poljske in portugalske vlade ter Komisije zaradi ugotovitve o ustreznosti v Sklepu o zasebnostnem ščitu nadzornim organom ni odvzeto njihovo pooblastilo za prekinitev ali prepoved prenosa v Združene države, izvedenega na podlagi standardnih pogodbenih klavzul. Kadar prenos v Združene države ne temelji na Sklepu o zasebnostnem ščitu, naj ta za nadzorne organe formalno ne bi bil zavezujoč v okviru izvrševanja pooblastil, ki so jim podeljena s členom 58(2) GDPR. Ti organi naj bi se, drugače povedano, lahko odmaknili od ugotovitev, do katerih je Komisija prišla v zvezi z ustreznostjo ravni varstva pred posegi ameriških javnih organov v uresničevanje temeljnih pravic posameznikov, na katere se nanašajo osebni podatki. Nizozemska vlada in Komisija natančneje navajata, da jih morajo nadzorni organi vseeno upoštevati, kadar uporabijo ta pooblastila. Po mnenju nemške vlade lahko ti organi drugače presodijo šele po vsebinski preučitvi, ki vključuje ustrezne preiskave ugotovitev, do katerih je prišla Komisija.

192. Nasprotno pa družba Facebook Ireland in vlada Združenih držav v bistvu trdita, da zavezujoči učinek sklepa o ustreznosti ob upoštevanju zahtev po pravni varnosti in enotni uporabi prava Unije pomeni, da nadzornim organom ni dovoljeno podvomiti o ugotovitvah iz tega sklepa niti v okviru obravnave pritožbe, s katero se želi doseči prekinitev prenosov v zadevno tretjo državo, izvedenih na drugi podlagi, in ne na navedenem sklepu.

193. Sam se strinjam s prvim od teh dveh pristopov. Ker je področje uporabe Sklepa o zasebnostnem ščitu omejeno na prenose podjetju, samocertificiranemu na podlagi tega sklepa, ta za nadzorne organe formalno ne more biti zavezujoč v zvezi s prenosi, ki ne spadajo na to področje uporabe. V skladu s tem je namen Sklepa o zasebnostnem ščitu zagotoviti pravno varnost le izvoznikom, ki prenašajo podatke v okviru, ki ga določa. Po mojem mnenju neodvisnost, ki se s členom 52 GDPR priznava nadzornim organom, nasprotuje tudi temu, da bi bile ugotovitve, do katerih je Komisija prišla v sklepu o ustreznosti, za te organe zavezujoče zunaj njegovega področja uporabe.

194. Seveda ugotovitve, navedene v Sklepu o zasebnostnem ščitu v zvezi z ustreznostjo ravni varstva, ki se v Združenih državah zagotavlja pred posegi, povezanimi z dejavnostmi obveščevalnih služb te države, pomenijo izhodišče za analizo, s katero nadzorni organ v vsakem primeru posebej oceni, ali je treba prenos, ki temelji na standardnih pogodbenih klavzulah, zaradi takih posegov prekiniti. Vendar če pristojni nadzorni organ po temeljiti preiskavi oceni, da se ne more strinjati s temi ugotovitvami glede prenosa, na katerega je bil opozorjen, po mojem mnenju ohrani možnost izvrševanja pooblastil, ki so mu podeljena s členom 58(2)(f) in (j) GDPR.

195. Ob tem bi bilo treba preučiti – če bi Sodišče tu obravnavanem vprašanju namenilo odgovor, nasproten tistemu, ki ga zagovarjam – ali ne bi bilo treba teh pooblastil vseeno ponovno vzpostaviti zaradi neveljavnosti Sklepa o zasebnostnem ščitu.

80 Glej v tem smislu sodbo Schrems (točka 59).

2. Veljavnost Sklepa o zasebnostnem ščitu

196. V preudarkih, ki sledijo, bom izpostavil nekatera vprašanja v zvezi z utemeljenostjo presoj v Sklepu o zasebnostnem ščitu v zvezi z ustreznostjo – v smislu člena 45(1) GDPR – ravni varstva, zagotovljene v Združenih državah, glede na dejavnosti nadzora elektronskih komunikacij, ki jih izvajajo ameriški obveščevalni organi. Namen teh preudarkov ni predstaviti dokončno ali celovito stališče glede veljavnosti tega sklepa. Omejeni bodo na nekatere premisleke, ki bi se lahko izkazali za koristne, če bi Sodišče želelo v nasprotju z mojim predlogom odločiti o tej točki.

197. V zvezi s tem je iz točke 64 obrazložitve Sklepa o zasebnostnem ščitu in točke I.5 Priloge II k temu sklepu razvidno, da je to, da podjetja spoštujejo načela, določena v navedenem sklepu, lahko med drugim omejeno z zahtevami nacionalne varnosti, javnega interesa in kazenskega pregona ali z nezdružljivimi obveznostmi, ki izhajajo iz ameriškega prava.

198. Komisija je zato ocenila zaščitne ukrepe, ki so v pravu Združenih držav na voljo glede dostopa do prenesenih podatkov in glede njihove uporabe s strani ameriških javnih organov zlasti zaradi nacionalne varnosti.[81] Od ameriške vlade je pridobila nekatere zaveze, ki se na eni strani nanašajo na omejitve za dostop do prenesenih podatkov in za njihovo uporabo s strani ameriških organov ter na drugi na pravno varstvo, zagotovljeno posameznikom, na katere se nanašajo osebni podatki.[82]

199. M. Schrems pred Sodiščem trdi, da Sklep o zasebnostnem ščitu ni veljaven, ker tako opisani zaščitni ukrepi ne zadostujejo za zagotovitev ustrezne ravni varstva temeljnih pravic oseb, katerih podatki se prenašajo v Združene države. DPC, EPIC ter avstrijska, poljska in portugalska vlada – ne da bi neposredno prerekali veljavnost tega sklepa – izpodbijajo presoje, ki jih je Komisija opravila v navedenem sklepu v zvezi z ustreznostjo ravni varstva pred posegi, ki so posledica dejavnosti ameriških obveščevalnih služb. Ti dvomi odsevajo pomisleke, ki so jih izrazili Parlament,[83] EOVP[84] in ENVP[85].

200. Pred preučitvijo utemeljenosti ugotovitve o ustreznosti v Sklepu o zasebnostnem ščitu je treba pojasniti metodologijo, po kateri se mora ravnati ta preučitev.

a) Pojasnila v zvezi z vsebino preizkusa veljavnosti sklepa o ustreznosti

1) Pogoji primerjave, ki omogočajo ocenjevanje „bistvene enakosti“ ravni varstva

201. V skladu s členom 45(3) GDPR in sodno prakso Sodišča[86] lahko Komisija ugotovi, da tretja država zagotavlja ustrezno raven varstva, le če je ob primerni obrazložitvi ugotovila, da je v tej tretji državi raven varstva temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, „v bistvenem enaka“ ravni, ki se zahteva v Uniji na podlagi te uredbe, razlagane ob upoštevanju Listine.

81 Glej točko 65 obrazložitve Sklepa o zasebnostnem ščitu.

82 Glej priloge od III do VII Sklepa o zasebnostnem ščitu.

83 Resoluciji Parlamenta z dne 6. aprila 2017 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, P8_TA(2017)0131, in z dne 5. julija 2018 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, P8_TA (2018)0315.

84 Glej: Delovna skupina za varstvo podatkov iz člena 29 (v nadaljevanju: WP29), Mnenje št. 1/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA, 13. april 2016, WP 238; WP29, Zasebnostni ščit EU-ZDA – Prvi skupni letni pregled, 28. november 2017, WP 255, in EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019. WP29 je bila ustanovljena v skladu s členom 29(1) Direktive 95/46, ki je določal, da ima ta skupina svetovalni status in deluje samostojno. V skladu s členom 29(2) te direktive so navedeno skupino sestavljali predstavnik vsakega nacionalnega nadzornega organa, predstavnik vsakega organa, ustanovljenega za ustanove ali organe Skupnosti, in predstavnik Komisije. Z začetkom veljavnosti GDPR je bila WP29 nadomeščena z EOVP (glej člen 94(2) te uredbe).

85 Glej ENVP, Mnenje št. 4/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA z dne 30. maja 2016. ENVP je bil ustanovljen s členom 1(2) Uredbe (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 26, str. 102). Njegova naloga je spremljati uporabo določb te uredbe.

86 Glej točko 112 teh sklepnih predlogov.

202. Tako preverjanje ustreznosti ravni varstva, zagotovljene v tretji državi, nujno vključuje primerjavo med veljavnimi pravili in praksami v tej tretji državi na eni strani ter veljavnimi standardi varstva v Uniji na drugi. Predložitveno sodišče z drugim vprašanjem Sodišču predlaga, naj opredeli pogoje te primerjave. [87]

203. Natančneje, to sodišče želi izvedeti, ali pridržana pristojnost, ki se s členom 4(2) PEU in členom 2(2) GDPR priznava državam članicam na področju varovanja nacionalne varnosti, pomeni, da pravni red Unije ne vključuje standardov varstva, s katerimi bi bilo treba primerjati zaščitne ukrepe – ki veljajo v tretji državi za obdelavo tja prenesenih podatkov, ki jo javni organi izvajajo zaradi varovanja nacionalne varnosti – da bi se ocenila ustreznost teh zaščitnih ukrepov. Če je odgovor pritrdilen, navedeno sodišče želi izvedeti, kako je treba določiti upoštevni referenčni okvir.

204. V zvezi s tem se ne sme pozabiti, da se razlog za obstoj omejitev, ki se s pravom Unije uvajajo za mednarodne prenose osebnih podatkov s tem, da se zahteva, da se zagotovi kontinuiteta ravni varstva pravic posameznikov, na katere se nanašajo osebni podatki, navezuje na preprečevanje tveganja, da bi se zaobšli standardi, veljavni v Uniji. [88] Kot je v bistvu navedla družba Facebook Ireland, glede na ta cilj nikakor ne bi bilo upravičeno od tretje države pričakovati, da spoštuje zahteve, ki se ne ujemajo z obveznostmi držav članic.

205. V skladu s členom 51(1) Listine pa se ta uporablja za države članice samo takrat, kadar izvajajo pravo Unije. Zato je veljavnost sklepa o ustreznosti glede na omejitve, ki jih predpisi namembne tretje države določajo za uresničevanje temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, odvisna od primerjave med temi omejitvami in omejitvami, ki bi bile državam članicam dovoljene z določbami Listine *le v primeru, v katerem bi podobni predpisi države članice spadali na področje uporabe prava Unije*.

206. Vendar ustreznosti ravni varstva, zagotovljene v namembni tretji državi, ni mogoče presojati, ne da bi se upoštevali morebitni posegi v uresničevanje temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, izhajajoči iz državnih ukrepov, zlasti na področju nacionalne varnosti, ki – če bi jih sprejela država članica – ne bi spadali na področje uporabe prava Unije. Za to presojo se s členom 45(2)(a) GDPR brez kakršnega koli omejevanja zahteva upoštevanje predpisov s področja nacionalne varnosti, veljavnih v tej tretji državi.

207. Ocenjevanje ustreznosti ravni varstva z vidika takih državnih ukrepov po mojem mnenju vključuje primerjavo zaščitnih ukrepov, ki spremljajo te državne ukrepe, z ravnjo varstva, zahtevano v Uniji na podlagi prava držav članic, vključno z njihovimi zavezami v okviru EKČP. Ker so države članice zaradi pristopa k EKČP zavezane svoje nacionalno pravo uskladiti z določbami te konvencije in ker gre torej, kot so v bistvu poudarile družba Facebook Ireland, nemška in češka vlada ter Komisija, za skupni imenovalec držav članic, bom te določbe štel za upoštevno primerjalno merilo za to ocenjevanje.

208. V obravnavanem primeru, kot je omenjeno zgoraj, [89] zahteve Združenih držav glede nacionalne varnosti prevladajo nad obveznostmi podjetij, samocertificiranih na podlagi Sklepa o zasebnostnem ščitu. Tako je veljavnost tega sklepa odvisna od vprašanja, ali te zahteve spremljajo zaščitni ukrepi, s katerimi se zagotavlja raven varstva, ki je v bistvenem enaka ravni, ki mora biti zagotovljena v Uniji.

87 Spomniti moram, da je treba bistveno enakost ravni varstva, ki jo zagotavlja tretja država, v primerjavi z ravnjo, ki se zahteva v Uniji, oceniti tudi, kadar v okviru posameznega prenosa, ki temelji na standardnih pogodbenih klavzulah iz Sklepa 2010/87, upravljavec ali, če ne on, pristojni nadzorni organ preveri, ali javni organi namembne tretje države uvozniku nalagajo zahteve, ki presegajo meje tega, kar je potrebno v demokratični družbi (glej klavzulo 5 v Prilogi k Sklepu 2010/87 in opombo k tej klavzuli). Glej točke 115, 134 in 135 teh sklepnih predlogov.

88 Glej točko 117 teh sklepnih predlogov.

89 Glej točko 197 teh sklepnih predlogov.

209. Za odgovor na to vprašanje je treba najprej opredeliti standarde – in sicer tiste, ki izhajajo iz Listine ali seveda iz EKČP – ki jim morajo v Uniji ustrezati predpisi s področja nadzora elektronskih komunikacij, podobni tistim, ki jih je Komisija preučila v Sklepu o zasebnostnem ščitu. Opredelitev standardov, ki se uporabljajo, je odvisna od tega, ali bi predpisi, kot sta člen 702 FISA in EO 12333, če bi izvirali iz države članice, spadali ali ne v okvir omejitve, uvedene za področje uporabe GDPR v skladu s členom 2(2) te uredbe, razlaganim ob upoštevanju člena 4(2) PEU.

210. V zvezi s tem iz člena 4(2) PEU in iz ustaljene sodne prakse izhaja, da se pravo Unije in zlasti instrumenti sekundarne zakonodaje o varstvu osebnih podatkov ne uporabljajo za dejavnosti s področja varovanja nacionalne varnosti, ker so to dejavnosti držav ali državnih organov, ki niso povezane s področji dejavnosti posameznikov. [90]

211. To načelo pomeni, *prvič*, da predpisi s področja varovanja nacionalne varnosti ne spadajo na področje uporabe prava Unije, kadar urejajo samo državne dejavnosti, ne urejajo pa nobene dejavnosti, ki jo izvajajo posamezniki. Zato se to pravo po mojem mnenju ne uporablja za nacionalne ukrepe v zvezi z zbiranjem in uporabo osebnih podatkov, ki jih država neposredno izvaja zaradi varovanja nacionalne varnosti in s katerimi se zasebnim subjektom ne nalagajo posebne obveznosti. Kot je Komisija navedla na obravnavi, bi bil iz področja uporabe prava Unije izključen zlasti ukrep, ki bi ga sprejela država članica in s katerim bi se tako kot z EO 12333 dovoljeval neposreden dostop njenih varnostnih služb do podatkov v tranzitu. [91]

212. Veliko bolj zapleteno je vprašanje, *drugič*, ali na področje uporabe prava Unije prav tako ne bi spadale nacionalne določbe, na podlagi katerih so – tako kot s členom 702 FISA – ponudniki elektronskih komunikacijskih storitev zavezani nuditi podporo organom, pristojnim za nacionalno varnost, da bi jim omogočili dostop do nekaterih osebnih podatkov.

213. Medtem ko sodba PNR govori v prid pritrdilnemu odgovoru na to vprašanje, bi razlogovanje, sprejeto v sodbah Tele2 Sverige in Ministerio Fiscal, lahko utemeljevalo, da se nanj odgovori nikalno.

214. V sodbi PNR je Sodišče razglasilo ničnost odločbe, v kateri je Komisija ugotovila ustreznost ravni varstva osebnih podatkov iz evidence imen letalskih potnikov (Passenger Name Records, PNR), posredovane ameriškemu organu, pristojnemu za carinsko in mejno zaščito. [92] Sodišče je odločilo, da obdelava, na katero se nanaša ta odločba, in sicer prenos podatkov PNR s strani letalskih družb zadevnemu organu, *glede na njen predmet* spada v okvir izključitve iz področja uporabe Direktive 95/46, ki jo določa njen člen 3(2). Kot je presodilo Sodišče, ta obdelava ni potrebna za opravljanje

90 Glej zlasti sodbo z dne 6. novembra 2003, Lindqvist (C-101/01, EU:C:2003:596, točki 43 in 44); sodbo PNR (točka 58); sodbo z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia (C-73/07, EU:C:2008:727, točka 41); sodbo z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970, točka 69; v nadaljevanju: sodba Tele2 Sverige), in sodbo z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, točka 32; v nadaljevanju: sodba Ministerio Fiscal).

91 Za izognitev vsakršni zmedi glede tega moram poudariti, da Komisija v Sklepu o zasebnostnem ščitu ni bila zmožna ugotoviti, ali Združene države dejansko prestrezajo komunikacije, ki prehajajo po čezatlantskih kablih, ker ameriški organi niso ne potrdili ne zavrnili te teze (glej točko 75 obrazložitve tega sklepa in dopis Roberta Litta z dne 22. februarja 2016, ki je v Prilogi VI, točka I(a), k navedenemu sklepu). Toda ker vlada Združenih držav ni zanikala zbiranja podatkov v tranzitu na podlagi EO 12333, se mi zdi, da je morala Komisija, preden je podala ugotovitev o ustreznosti, od te vlade dobiti zagotovila, da bi tako zbiranje, če bi se izvajalo, spremljali ustrezni zaščitni ukrepi pred tveganji zlorabe. S tega vidika je Komisija v točkah od 68 do 77 obrazložitve zadevnega sklepa preučila omejitve in zaščitne ukrepe, ki bi se morali uporabljati v takem primeru na podlagi PPD 28.

92 Šlo je za Odločbo Komisije 2004/535/ES z dne 14. maja 2004 o ustreznem varstvu osebnih podatkov, vsebovanih v Evidenci imen letalskih potnikov, posredovani Uradu za carinsko in mejno zaščito Združenih držav Amerike (UL 2004, L 235, str. 11).

storitev, ampak za zaščito javne varnosti in zaradi kazenskega pregona. Ker je zadevni prenos spadal v okvir, ki so ga določili javni organi, in se je nanašal na javno varnost, je bil izključen iz področja uporabe te direktive, čeprav so podatke PNR najprej zbirali zasebni subjekti v okviru komercialne dejavnosti, ki je spadala na to področje uporabe, in čeprav so ta prenos organizirali ti subjekti. [93]

215. V poznejši sodbi Tele2 Sverige [94] je Sodišče presodilo, da nacionalne določbe, ki temeljijo na členu 15(1) Direktive 2002/58/ES [95] ter urejajo, tako hrambo podatkov o prometu in o lokaciji s strani ponudnikov telekomunikacijskih storitev kot dostop javnih organov do hranjenih podatkov v smislu te določbe – ki vključujejo kazenski pregon in varovanje nacionalne varnosti – spadajo na področje uporabe te direktive in posledično Listine. Kot je menilo Sodišče, niti določbe o hrambi podatkov niti določbe o dostopu do hranjenih podatkov niso zajete z izključitvijo iz področja uporabe te direktive, določeno v njenem členu 1(3), ki se sklicuje med drugim na dejavnosti države v zvezi s kazenskim pregonom in varovanjem nacionalne varnosti. [96] Sodišče je to sodno prakso potrdilo v sodbi Ministerio Fiscal. [97]

216. Vendar se člen 702 FISA razlikuje od takih predpisov, ker se s to določbo ponudnikom elektronskih komunikacijskih storitev ne nalaga nobena obveznost hrambe podatkov ali kakršne koli druge obdelave, če obveščevalni organi ne podajo zahteve za dostop.

217. Zato se postavlja vprašanje, ali na področje uporabe GDPR in posledično Listine spadajo nacionalni ukrepi, s katerimi se tem ponudnikom nalaga obveznost dati podatke na razpolago javnim organom zaradi nacionalne varnosti *neodvisno od kakršne koli obveznosti hrambe*. [98]

218. *Prvi pristop* bi lahko bil ta, da bi se zgoraj omenjeni usmeritvi sodne prakse čim bolj uskladili tako, da bi se ugotovitev Sodišča iz sodb Tele2 Sverige in Ministerio Fiscal v zvezi z uporabo prava Unije za ukrepe, ki urejajo dostop nacionalnih organov do podatkov med drugim za namene varovanja nacionalne varnosti, [99] razlagala kot omejena na primere, v katerih se podatki hranijo *v skladu z zakonsko obveznostjo*, uvedeno na podlagi člena 15(1) Direktive 2002/58. Ta ugotovitev se, nasprotno, ne bi uporabljala v drugačnem dejanskem okviru iz sodbe PNR, ki se je nanašala na prenos podatkov, ki so jih letalske družbe na lastno pobudo hranile za komercialne namene, ameriškemu organu, pristojnemu za nacionalno varnost.

93 Sodba PNR (točke od 56 do 58). Poleg tega je Sodišče v sodbi z dne 10. februarja 2009, Irska/Parlament in Svet (C-301/06, EU:C:2009:68, točki 90 in 91), odločilo, da ugotovitev iz sodbe PNR ni mogoče prenesti na obdelavo, na katero se nanaša Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (UL 2006, L 105, str. 54). Sodišče je ta sklep utemeljilo s tem, da Direktiva 2006/24 drugače kot odločba, obravnavana v sodbi PNR, ureja samo dejavnosti ponudnikov storitev na notranjem trgu, ne pa dejavnosti javnih organov z namenom pregona. Zdi se mi, da je Sodišče s tem razlogovanjem potrdilo, da bi bilo, nasprotno, ugotovitev iz sodbe PNR mogoče prenesti na določbe o dostopu do hranjenih podatkov ali njihovi uporabi s strani teh organov.

94 Sodba Tele2 Sverige (točke od 67 do 81).

95 Direktiva Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514).

96 Ker se z Direktivo 2002/58 uresničujejo zahteve iz Direktive 95/46, ki je zdaj razveljavljena na podlagi GDPR, v kateri je obširno povzeta vsebina te direktive, se mi zdi, da se sodna praksa glede razlage člena 1(3) Direktive 2002/58 po analogiji uporablja za razlago člena 2(2) GDPR. Glej v tem smislu sodbi Tele2 Sverige (točka 69) in Ministerio Fiscal (točka 32).

97 Sodba Ministerio Fiscal (točke 34, 35 in 37).

98 Isto vprašanje je bilo postavljeno v okviru treh drugih predlogov za sprejetje predhodne odločbe v še nerešenih zadevah pred Sodiščem. Glej zadevo C-623/17, Privacy International (UL 2018, C 22, str. 29), ter združeni zadevi C-511/18 in C-512/18, La Quadrature du Net in drugi in French Data Network in drugi (UL 2018, C 392, str. 7).

99 Čeprav se je Sodišče v sodbi Tele2 Sverige osredotočilo na preučitev utemeljitve za posege, ki so izhajali iz zadevnih ukrepov v zvezi s hrambo in dostopom, glede na cilj boja proti kaznivim dejanjem, ugotovitev, do katere je prišlo, *mutatis mutandis* velja tudi, kadar taki ukrepi sledijo cilju varovanja nacionalne varnosti. V členu 15(1) Direktive 2002/58 sta namreč med cilji, ki lahko upravičujejo take ukrepe, omenjena tako boj proti kaznivim dejanjem kot varovanje nacionalne varnosti. Poleg tega so s členom 1(3) Direktive 2002/58 in členom 2(2) GDPR iz področja uporabe teh instrumentov izključene dejavnosti države tako na področju nacionalne varnosti kot na kazenskem področju. Ukrepi, obravnavani v zadevi, v kateri je bila izrečena sodba Tele2 Sverige, so sicer sledili tudi cilju, povezanem z nacionalno varnostjo. V točki 119 te sodbe je Sodišče utemeljitev ukrepov v zvezi s hrambo podatkov o prometu in o lokaciji ter dostopom do teh podatkov izrecno obravnavalo z vidika cilja varovanja nacionalne varnosti v delu, v katerem ta cilj zajema boj proti terorizmu.

219. V skladu z *drugim pristopom*, ki ga predlaga Komisija in ki se mi zdi bolj prepričljiv, bi razlogovanje, sprejeto v sodbah Tele2 Sverige in Ministerio Fiscal, utemeljevalo uporabo prava Unije za nacionalna pravila, s katerimi se od ponudnikov elektronskih komunikacijskih storitev zahteva, da nudijo pomoč organom, odgovornim za nacionalno varnost, da bi ti lahko dostopali do nekaterih podatkov, *ne da bi bilo pomembno, ali ta pravila spremljajo predhodno obveznost hrambe podatkov ali ne*.

220. Jedro tega razlogovanja namreč ne temelji na predmetu zadevnih določb, tako kot v sodbi PNR, temveč na dejstvu, da so te določbe urejale dejavnosti ponudnikov, pri čemer jim je bila z njimi naložena obdelava podatkov. Te dejavnosti niso bile dejavnosti države na področjih iz člena 1(3) Direktive 2002/58 in člena 3(2) Direktive 95/46, katerega vsebina je v bistvu povzeta v členu 2(2) GDPR.

221. Tako je Sodišče v sodbi Tele2 Sverige opozorilo, da se „dostop do podatkov, ki jih hranijo […] ponudniki, nanaša na obdelavo osebnih podatkov *s strani teh ponudnikov*, pri čimer gre za obdelavo, ki spada na področje uporabe te direktive“.[100] Enako je v sodbi Ministerio Fiscal presodilo, da zakonski ukrepi, ki ponudnikom nalagajo, da pristojnim organom odobrijo dostop do hranjenih podatkov, „nujno pomenijo obdelavo [teh] podatkov *s strani teh ponudnikov*“.[101]

222. Upravljavčevo dajanje podatkov na razpolago javnemu organu pa ustreza opredelitvi „obdelave“ iz člena 4, točka 2, GDPR.[102] Enako velja za predhodno filtriranje podatkov z uporabo iskalnih meril, da bi se izluščili tisti podatki, do katerih so javni organi zahtevali dostop.[103]

223. Iz tega sklepam, da se na podlagi razlogovanja, ki ga je Sodišče sprejelo v sodbah Tele2 Sverige in Ministerio Fiscal, GDPR in posledično Listina uporabljata za nacionalne predpise, s katerimi je ponudnik elektronskih komunikacijskih storitev zavezan nuditi pomoč organom, odgovornim za nacionalno varnost, tako da jim da podatke na razpolago, po potrebi po tem, ko jih je filtriral, tudi neodvisno od kakršne koli zakonske obveznosti hrambe teh podatkov.

224. Poleg tega se mi zdi, da ta razlaga vsaj implicitno izhaja iz sodbe Schrems. Kot so poudarili DPC, avstrijska in poljska vlada ter Komisija, je Sodišče v njej v okviru preizkusa veljavnosti Odločbe o varnem pristanu presodilo, da mora pravo tretje države, ki jo zadeva sklep o ustreznosti, pred posegi, ki jih njeni javni organi izvajajo v temeljne pravice posameznikov, na katere se nanašajo osebni podatki, zaradi nacionalne varnosti, določati zaščitne ukrepe, ki so v bistvenem enaki zaščitnim ukrepom, ki izhajajo zlasti iz členov 7, 8 in 47 Listine.[104]

225. Iz tega, natančneje, sledi, da nacionalni ukrep, s katerim je ponudnikom elektronskih komunikacijskih storitev naloženo, da se odzovejo na zahtevo organov, pristojnih za nacionalno varnost, za dostop do nekaterih podatkov, ki jih ti ponudniki hranijo v okviru svojih komercialnih dejavnosti, neodvisno od kakršne koli zakonske obveznosti, in da predhodno opredelijo zahtevane podatke z uporabo izbirnikov (tako kot v okviru programa PRISM), ne bi spadal na področje uporabe člena 2(2) GDPR. Enako bi veljalo za nacionalni ukrep, s katerim se od podjetij, ki upravljajo telekomunikacijsko „hrbtenico“, zahteva, da organom, odgovornim za nacionalno varnost, zagotovijo dostop do podatkov, ki prehajajo po infrastrukturi, ki jo ta podjetja upravljajo (tako kot v okviru programa Upstream).

100 Sodba Tele2 Sverige (točka 78, moj poudarek). Kot kaže uporaba izraza „poleg tega“, je Sodišče v točki 79 te sodbe zgolj za potrditev svoje ugotovitve v zvezi z uporabo Direktive 2002/58 poudarilo tesno povezavo med obveznostjo hrambe podatkov, obravnavano v zadevi, v kateri je bila izrečena ta sodba, in določbami o dostopu nacionalnih organov do hranjenih podatkov.

101 Sodba Ministerio Fiscal (točka 37, moj poudarek).

102 Glej v tem smislu sodbo Ministerio Fiscal (točka 38).

103 Glej v tem smislu sodbo z dne 13. maja 2014, Google Spain in Google (C-131/12, EU:C:2014:317, točka 28).

104 Sodba Schrems (točke od 91 do 96). V točkah 90, 124 in 141 obrazložitve Sklepa o zasebnostnem ščitu se Komisija poleg tega sklicuje na določbe Listine, s čimer sprejema načelo, da morajo biti omejitve temeljnih pravic, ki izpolnjujejo cilj varovanja nacionalne varnosti, v skladu z Listino.

226. Ko državni organi pridobijo zadevne podatke, pa sta njihova hramba in nadaljnja uporaba s strani teh organov zaradi nacionalne varnosti po mojem mnenju iz istih razlogov, kot so omenjeni v točki 211 teh sklepnih predlogov, zajeti z odstopanjem, ki ga določa člen 2(2) GDPR, tako da ne spadata na področje uporabe te uredbe in posledično Listine.

227. Glede na vse navedeno menim, da preizkus veljavnosti Sklepa o zasebnostnem ščitu z vidika omejitev načel, določenih v njem, ki bi lahko izhajale iz dejavnosti ameriških obveščevalnih organov, vključuje dvojno preverjanje.

228. *Prvič*, preučiti bo treba, ali je raven varstva, ki jo zagotavljajo Združene države pred omejitvami, ki so posledica uporabe člena 702 FISA v delu, v katerem je s to določbo NSA dovoljeno, da ponudnikom naloži, da ji dajejo na razpolago osebne podatke , v bistvenem enaka ravni, izhajajoči iz določb GDPR in Listine.

229. *Drugič*, določbe EKČP bodo upoštevni referenčni okvir pri ocenjevanju, ali omejitve, do katerih bi lahko pripeljalo izvajanje EO 12333 v delu, v katerem je obveščevalnim organom dovoljeno, da sami, brez pomoči zasebnih subjektov, zbirajo osebne podatke, vzbujajo dvom o ustreznosti ravni varstva, zagotovljene v Združenih državah. Te določbe bodo zagotovile tudi standarde primerjave, ki bodo omogočili presojo ustreznosti te ravni varstva glede na hrambo in uporabo podatkov, ki jih ti organi pridobivajo zaradi nacionalne varnosti.

230. Vendar je treba ugotoviti še, ali je ugotovitev o ustreznosti pogojena s tem, da zbiranje podatkov na podlagi EO 12333 spremlja raven varstva, ki je v bistvenem enaka ravni varstva, ki mora biti zagotovljena v Uniji, *tudi če je to zbiranje potekalo zunaj ozemlja Združenih držav*, v fazi tranzita podatkov iz Unije v to tretjo državo.

2) Nujnost zagotoviti ustrezno raven varstva v fazi tranzita podatkov

231. Pred Sodiščem so bila zastopana tri različna stališča glede tega, ali je nujno ali ne, da Komisija pri ocenjevanju ustreznosti ravni varstva, zagotovljene v tretji državi, upošteva nacionalne ukrepe v zvezi z dostopom organov te tretje države do podatkov zunaj njenega ozemlja, v fazi tranzita podatkov iz Unije na to ozemlje.

232. Prvič, družba Facebook Ireland ter vladi Združenih držav in Združenega kraljestva v bistvu trdijo, da obstoj takih ukrepov nima učinkov v okviru ugotovitve o ustreznosti. V podporo temu pristopu se sklicujejo na nezmožnost tretje države, da nadzira vse komunikacijske poti zunaj svojega ozemlja, po katerih prehajajo podatki iz Unije, tako da naj posledično nikoli ne bi bilo mogoče zagotoviti, da druga tretja država ne bo skrivaj zbirala podatkov med njihovim tranzitom.

233. Drugič, DPC, M. Schrems, EPIC, avstrijska in nizozemska vlada, Parlament in EOVP zatrjujejo, da zahteva po kontinuiteti ravni varstva, določena v členu 44 GDPR, pomeni, da mora biti ta raven ustrezna skozi celoten prenos, tudi ko podatki prehajajo po podmorskih kablih, preden dosežejo ozemlje namembne tretje države.

234. Čeprav priznava to načelo, Komisija trdi, tretjič, da je predmet ugotovitve o ustreznosti omejen na varstvo, ki ga zadevna tretja država zagotavlja *znotraj svojih meja*, tako da okoliščina, da ustrezna raven varstva ni zagotovljena *med tranzitom* v to tretjo državo, ne omaje veljavnosti sklepa o ustreznosti. Vseeno naj bi upravljavec v skladu s členom 32 GDPR moral zagotoviti varnost prenosa tako, da v največji možni meri zavaruje osebne podatke v fazi tranzita v navedeno tretjo državo.

235. V zvezi s tem ugotavljam, da člen 44 GDPR določa, da je treba za prenos v tretjo državo spoštovati pogoje, navedene v določbah poglavja V te uredbe, če so podatki lahko predmet obdelave „po prenosu“. Ta izraz bi bilo mogoče razumeti bodisi tako – kot je vlada Združenih držav zatrdila v pisnem odgovoru na vprašanja Sodišča – da je treba te pogoje spoštovati, *ko podatki enkrat prispejo na cilj*, bodisi tako, da veljajo *po tem, ko se prenos začne* (tudi v fazi tranzita).

236. Ker besedilo člena 44 GDPR ni dovolj jasno, se na podlagi teleološke razlage pridružujem drugi od teh razlag in podpiram drugega izmed zgoraj omenjenih pristopov. Če bi se namreč štelo, da zahteva po kontinuiteti ravni varstva, določena v tej določbi, zajema le ukrepe nadzora, ki se izvajajo na ozemlju namembne tretje države, bi jo bilo mogoče zaobiti, če ta tretja država uporablja take ukrepe zunaj svojega ozemlja, v fazi tranzita podatkov. Za izognitev temu tveganju se mora ocenjevanje ustreznosti ravni varstva, ki jo zagotavlja tretja država, nanašati na vse določbe, zlasti na področju nacionalne varnosti, pravnega reda te tretje države,[105] med katerimi so tako določbe v zvezi z nadzorom, ki se izvaja na njenem ozemlju, kot določbe, ki omogočajo nadzor podatkov v tranzitu na to ozemlje.[106]

237. Ob tem pa nihče ne prereka tega, da se, kot je poudaril EOVP, ocenjevanje ustreznosti ravni varstva – kot je razvidno iz člena 45(1) GDPR – nanaša samo na določbe pravnega reda *tretje države, v katero so namenjeni podatki*. Nezmožnost – na katero se opirajo družba Facebook Ireland ter vladi Združenih držav in Združenega kraljestva – zagotoviti, da druga tretja država ne bo skrivaj zbirala teh podatkov med njihovim tranzitom, ne vpliva na to ocenjevanje. Poleg tega takega tveganja ni mogoče izključiti niti po tem, ko podatki prispejo na ozemlje namembne tretje države.

238. Sicer je res tudi, da bi se Komisija, ko presoja ustreznost ravni varstva, ki jo zagotavlja tretja država, glede na okoliščine lahko srečala s tem, da ji ta tretja država ne bi razkrila obstoja nekaterih tajnih programov nadzora. Vendar iz tega ne izhaja, da lahko Komisija, *kadar je seznanjena s takimi programi*, te prezre v okviru preučitve ustreznosti. Prav tako je Komisija, če po sprejetju sklepa o ustreznosti izve za obstoj nekaterih tajnih programov nadzora, ki jih zadevna tretja država izvaja na svojem ozemlju ali med tranzitom na to ozemlje, dolžna ponovno preučiti svojo ugotovitev o ustreznosti ravni varstva, ki jo zagotavlja ta tretja država, če tako razkritje vzbuja dvom o tem.[107]

3) Upoštevanje dejanskih ugotovitev Komisije in predložitvenega sodišča glede prava Združenih držav

239. Čeprav ni sporno, da Sodišče ni pristojno za podajo razlage prava tretje države, ki bi bila zavezujoča v njenem pravnem redu, je veljavnost Sklepa o zasebnostnem ščitu odvisna od utemeljenosti presoj, ki jih je Komisija opravila v zvezi z ravnjo varstva, zagotovljeno s pravom in prakso Združenih držav za temeljne pravice oseb, katerih podatki se prenašajo v to tretjo državo. Komisija je namreč svojo ugotovitev o ustreznosti morala obrazložiti glede na elemente, ki zadevajo zlasti vsebino prava navedene tretje države in so omenjeni v členu 45(2) GDPR.[108]

105 Glej v tem smislu sodbo Schrems (točki 74 in 75).

106 Glej v tem smislu EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019 (str. 17, točka 86).

107 Glej člen 45(5) GDPR. Glej tudi sodbo Schrems (točka 76).

108 Tako je bila Odločba o varnem pristanu razglašena za neveljavno z obrazložitvijo, da Komisija v tej odločbi ni ugotovila, da Združene države dejansko zagotavljajo ustrezno raven varstva zaradi svoje nacionalne zakonodaje ali mednarodnih obveznosti (sodba Schrems, točka 97). Zlasti Komisija ni ugotovila niti obstoja državnih predpisov, katerih namen bi bil omejiti morebitne posege v temeljne pravice posameznikov, na katere se nanašajo osebni podatki (sodba Schrems, točka 88), niti obstoja učinkovitega sodnega varstva v primeru takih posegov (sodba Schrems, točka 89).

240. High Court (višje sodišče) je v sodbi z dne 3. oktobra 2017, potem ko je presodilo dokaze, ki so jih predložile stranke spora, predstavilo podrobne ugotovitve, v katerih je opisalo upoštevne vidike ameriškega prava.[109] Ta predstavitev se v veliki meri ujema z ugotovitvami Komisije v Sklepu o zasebnostnem ščitu, ki se nanašajo na vsebino pravil v zvezi z zbiranjem prenesenih podatkov in dostopom do njih s strani ameriških obveščevalnih organov ter v zvezi s pravnimi sredstvi in nadzornimi mehanizmi, povezanimi s temi dejavnostmi.

241. Predložitveno sodišče, pa tudi več strank in zainteresiranih subjektov, ki so pri Sodišču vložili stališča, izražajo dvome bolj o pravnih posledicah, ki jih je Komisija izpeljala iz teh ugotovitev – in sicer o sklepanju, da Združene države zagotavljajo ustrezno raven varstva temeljnih pravic oseb, katerih podatki se prenašajo na podlagi tega sklepa – kot o opisu vsebine ameriškega prava, ki ga je predstavila.

242. V teh okoliščinah bom v bistvu presodil veljavnost Sklepa o zasebnostnem ščitu z vidika ugotovitev, ki jih je Komisija podala v zvezi z vsebino ameriškega prava, tako da bom preučil, ali te ugotovitve utemeljujejo sprejetje tega sklepa o ustreznosti.

243. V zvezi s tem se ne strinjam s stališčem, ki ga zagovarjata DPC in M. Schrems ter v skladu s katerim so ugotovitve High Court (višje sodišče) glede prava Združenih držav zavezujoče za Sodišče v okviru preizkusa veljavnosti Sklepa o zasebnostnem ščitu. Ti stranki trdita, da v skladu z irskim procesnim pravom tuje pravo pomeni dejansko vprašanje, zato je le predložitveno sodišče pristojno za ugotavljanje njegove vsebine.

244. V ustaljeni sodni praksi se resda nacionalnemu sodišču priznava izključna pristojnost za ugotavljanje upoštevnih dejstev ter za razlago prava države članice in njegovo uporabo v sporu, o katerem odloča.[110] S to sodno prakso se v okviru postopka, vzpostavljenega s členom 267 PDEU, izraža delitev funkcij med Sodiščem in predložitvenim sodiščem. Čeprav je Sodišče edino pristojno za razlago prava Unije in odločanje o veljavnosti sekundarne zakonodaje, je naloga predložitvenega sodišča, ki mora rešiti dejanski spor, ki mu je predložen, da ugotovi njegov dejanski in pravni okvir, da bi mu Sodišče lahko dalo koristen odgovor.

245. Razlog za obstoj te izključne pristojnosti predložitvenega sodišča se mi ne zdi prenosljiv na ugotavljanje prava tretje države kot elementa, ki lahko vpliva na ugotovitev Sodišča glede veljavnosti akta sekundarne zakonodaje.[111] Ker je razglasitev neveljavnosti takega akta v pravnem redu Unije zavezujoča *erga omnes*,[112] ugotovitev Sodišča ne more biti odvisna od izvora predloga za sprejetje predhodne odločbe. Kot sta poudarili družba Facebook Ireland in vlada Združenega kraljestva, pa bi bila odvisna od tega predloga, če bi bile ugotovitve predložitvenega sodišča v zvezi s pravom tretje države za Sodišče zavezujoče, saj se te ugotovitve lahko razlikujejo glede na nacionalno sodišče, ki jih poda.

109 Te ugotovitve so povzete v točkah od 54 do 73 teh sklepnih predlogov.

110 Glej med drugim sodbe z dne 4. maja 1999, Sürül (C-262/96, EU:C:1999:228, točka 95); z dne 11. septembra 2008, Eckelkamp in drugi (C-11/07, EU:C:2008:489, točka 32), in z dne 26. oktobra 2016, Senior Home (C-195/15, EU:C:2016:804, točka 20).

111 Glej v zvezi s tem sodbo Supreme Court (vrhovno sodišče) z dne 31. maja 2019 (točka 6.18).

112 Glej sodbo z dne 13. maja 1981, International Chemical Corporation (66/80, EU:C:1981:102, točki 12 in 13).

246. Glede na te preudarke menim, da kadar odgovor na vprašanje za predhodno odločanje, ki se nanaša na veljavnost akta Unije, vključuje presojo vsebine prava tretje države, Sodišče sicer lahko upošteva ugotovitve predložitvenega sodišča v zvezi s pravom te tretje države, vendar te ugotovitve zanj niso zavezujoče. Sodišče se lahko po potrebi odmakne od njih ali jih dopolni, tako da ob spoštovanju načela kontradiktornosti upošteva druge vire za ugotavljanje elementov, potrebnih za presojo veljavnosti zadevnega akta.[113]

4) Obseg standarda „bistvene enakosti“

247. Veljavnost Sklepa o zasebnostnem ščitu je odvisna, naj spomnim, od vprašanja, ali pravni red Združenih držav osebam, katerih podatki se prenašajo iz Unije v to tretjo državo, zagotavlja raven varstva, ki je „v bistvenem enaka“ ravni, zagotovljeni v državah članicah na podlagi GDPR in Listine ter – na področjih, izključenih iz področja uporabe prava Unije – njihovih zavez v okviru EKČP.

248. Kot je Sodišče poudarilo v sodbi Schrems,[114] ta standard ne pomeni, da mora biti raven varstva „povsem enaka“ tisti, ki se zahteva v Uniji. Čeprav so lahko sredstva, ki jih tretja država uporabi za varstvo pravic posameznikov, na katere se nanašajo osebni podatki, drugačna od sredstev, ki jih določa GDPR, razlagana ob upoštevanju Listine, „se morajo ta sredstva […] izkazati kot učinkovita za zagotovitev varstva, ki je v bistvenem enakovredno varstvu, zagotovljenemu znotraj Unije“.

249. Iz tega po mojem mnenju tudi izhaja, da pravo namembne tretje države lahko odseva lastno lestvico vrednot, glede na katero se lahko teža vsakega od različnih prisotnih interesov razlikuje od teže, ki je tem interesom pripisana v pravnem redu Unije. Poleg tega varstvo osebnih podatkov, ki prevladuje v Uniji, ustreza posebno visokemu standardu v primerjavi z ravnjo varstva, veljavno drugod po svetu. Zato bi se merilo „bistvene enakosti“ po mojem mnenju moralo uporabljati tako, da se ohrani določena prožnost za upoštevanje različnih pravnih in kulturnih tradicij. Vendar to merilo, če naj mu ne bo odvzeto bistvo, pomeni, da imajo nekateri minimalni zaščitni ukrepi in splošne zahteve za varstvo temeljnih pravic, ki izhajajo iz Listine in EKČP, ekvivalent v pravnem redu namembne tretje države.[115]

250. V zvezi s tem mora v skladu s členom 52(1) Listine kakršno koli omejevanje uresničevanja pravic in svoboščin, določenih v njej, biti predpisano z zakonom, spoštovati njihovo bistveno vsebino ter ob upoštevanju načela sorazmernosti biti potrebno in dejansko ustrezati cilju splošnega interesa, ki ga priznava Unija, ali biti potrebno zaradi zaščite pravic in svoboščin drugih. Te zahteve v bistvu ustrezajo tistim, ki jih določa člen 8(2) EKČP.[116]

251. Člen 52(3) Listine določa, da če pravice, zagotovljene v njenih členih 7, 8 in 47, ustrezajo pravicam, določenim v členih 8 in 13 EKČP, imajo enako vsebino in obseg, pri čemer se jim s pravom Unije vseeno lahko zagotovi širše varstvo. S tega vidika so, kot bo razkrila moja analiza, standardi, ki izhajajo iz členov 7, 8 in 47 Listine, kot jih razlaga Sodišče, v nekaterih pogledih strožji od tistih, ki izhajajo iz člena 8 EKČP, glede na razlago, ki jo je v zvezi s tem podalo Evropsko sodišče za človekove pravice (v nadaljevanju: ESČP).

113 Glej v zvezi s tem sodbo z dne 22. marca 2012, GLS (C-338/10, EU:C:2012:158, točke 15, 33 in 34), v kateri je Sodišče za presojo veljavnosti uredbe o uvedbi protidampinške dajatve upoštevalo statistične podatke Eurostata, ki jih je Komisija predložila na poziv Sodišča. Glej tudi sodbo z dne 22. oktobra 1991, Nölle (C-16/90, EU:C:1991:402, točke 17, 23 in 24). Podobno je Sodišče v sodbi Schrems (točka 90) pri preizkusu veljavnosti Odločbe o varnem pristanu upoštevalo nekatera sporočila Komisije.

114 Sodba Schrems (točki 73 in 74).

115 Glej v tem smislu WP29, „Adequacy Referential (updated)“ (Referenčni dokument o ustreznosti (posodobljen), 28. november 2017, WP 254 (str. 3, 4 in 9).

116 Vendar se člen 8(2) EKČP ne sklicuje na pojem „bistvena vsebina“ pravice do spoštovanja zasebnega življenja. Glej v zvezi s tem opombo 166 teh sklepnih predlogov.

252. Ugotavljam tudi, da je vsako od teh dveh sodišč v okviru še nerešenih zadev pozvano, naj ponovno pretehta nekatere vidike svoje sodne prakse. Tako sta bili, prvič, dve novejši sodbi ESČP v zvezi z nadzorom elektronskih komunikacij – to sta sodbi Centrüm för Rättvisa proti Švedski[117] in Big Brother Watch proti Združenem kraljestvu –[118] predloženi v ponovno obravnavo velikemu senatu. Drugič, tri nacionalna sodišča so Sodišču predložila predloge za sprejetje predhodne odločbe, ki odpirajo razpravo glede tega, ali je treba sodno prakso, ki izhaja iz sodbe Tele2 Sverige, preusmeriti ali ne.[119]

253. Po navedbi teh pojasnil bom zdaj preizkusil veljavnost Sklepa o zasebnostnem ščitu glede na člen 45(1) GDPR, razlagan ob upoštevanju Listine in EKČP v delih, v katerih ta akta na eni strani zagotavljata pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov (razdelek b)) ter na drugi pravico do učinkovitega sodnega varstva (razdelek c)).

b) Veljavnost Sklepa o zasebnostnem ščitu glede na pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov

254. Predložitveno sodišče v okviru četrtega vprašanja v bistvu dvomi o bistveni enakosti med ravnjo varstva, zagotovljeno v Združenih državah, in ravnjo varstva, ki jo imajo posamezniki, na katere se nanašajo osebni podatki, v Uniji na podlagi svojih temeljnih pravic do spoštovanja zasebnega življenja in do varstva osebnih podatkov.

1) Obstoj posegov

255. Komisija v točkah od 67 do 124 obrazložitve Sklepa o zasebnostnem ščitu omenja možnost, da ameriški javni organi dostopajo do podatkov, ki se prenašajo iz Unije, in jih uporabljajo zaradi nacionalne varnosti v okviru programov, ki temeljijo zlasti na členu 702 FISA in na EO 12333.

256. Izvajanje teh programov pripelje do posegov ameriških obveščevalnih služb, ki bi se, če bi jih uporabljali organi države članice, šteli za posege v uresničevanje pravice do spoštovanja zasebnega življenja, zagotovljene v členu 7 Listine in členu 8 EKČP. Poleg tega izvajanje navedenih programov posameznike, na katere se nanašajo osebni podatki, izpostavlja tveganju, da bodo njihovi osebni podatki predmet obdelave, ki ne izpolnjuje zahtev iz člena 8 Listine.[120]

257. Najprej moram pojasniti, da pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov ne obsegata le varstva vsebine komunikacij, ampak tudi podatkov o prometu[121] in o lokaciji (skupaj poimenovanih z izrazom „metapodatki“). Tako Sodišče kot ESČP sta namreč priznali, da lahko metapodatki enako kot podatki o vsebini razkrijejo zelo natančne informacije o zasebnem življenju posameznika.[122]

117 Sodba ESČP z dne 19. junija 2018 (CE:ECHR:2018:0619JUD003525208; v nadaljevanju: sodba Centrüm för Rättvisa).

118 Sodba ESČP z dne 13. septembra 2018 (CE:ECHR:2018:0913JUD005817013; v nadaljevanju: sodba Big Brother Watch).

119 Glej zadeve, navedene v opombi 102 teh sklepnih predlogov, ter zadevo C-520/18, Ordre des barreaux francophones et germanophones in drugi (UL 2018, C 408, str. 39).

120 Čeprav se z obdelavo lahko kršita hkrati člen 7 in člen 8 Listine, je okvir analize, upošteven za uporabo člena 8, strukturno drugačen od okvira analize, povezanega s členom 7. Pravica do varstva osebnih podatkov v skladu s členom 8(2) Listine pomeni, da se morajo „[o]sebni podatki […] obdelovati pošteno, za določene namene in na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom“, ter da ima „[v]sakdo […] pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo“. Kršitev te pravice predpostavlja, da so osebni podatki predmet obdelave, izvedene v nasprotju s temi zahtevami. To se zlasti zgodi, kadar obdelava ne temelji niti na privolitvi prizadete osebe *niti na drugi legitimni podlagi, določeni z zakonom*. Čeprav sta v takem položaju vprašanje obstoja posega in vprašanje njegove upravičenosti konceptualno različni v okviru člena 7, se ti vprašanji prekrivata glede člena 8 Listine.

121 V členu 2, drugi odstavek, točka (b), Direktive 2002/58 je pojem „podatki o prometu“ opredeljen kot „kater[i] koli podatk[i], obdelan[i] za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila“.

122 Glej sodbo z dne 8. aprila 2014, Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238, točka 27; v nadaljevanju: sodba Digital Rights Ireland), in sodbo Tele2 Sverige (točka 99). Glej tudi sodbi ESČP z dne 2. avgusta 1984, Malone proti Združenemu kraljestvu (CE:ECHR:1984:0802JUD000869179, točka 84), z dne 8. februarja 2018, Ben Faiza proti Franciji (CE:ECHR:2018:0208JUD003144612, točka 66).

258. V skladu s sodno prakso Sodišča za dokaz, da obstaja poseg v uresničevanje temeljne pravice, zagotovljene v členu 7 Listine, ni pomembno, ali so zadevni podatki občutljivi in ali so bile zadevne osebe zaradi zadevnega ukrepa nadzora oškodovane ali ne.[123]

259. Vendar programi nadzora, ki temeljijo na členu 702 FISA, pripeljejo predvsem do posegov v uresničevanje temeljnih pravic oseb, katerih komunikacije ustrezajo izbirnikom, ki jih je izbrala NSA, zaradi česar ponudniki elektronskih komunikacijskih storitev te komunikacije posredujejo tej agenciji.[124] Natančneje, obveznost, ki jo imajo ponudniki, da *dajo* podatke *na razpolago* agenciji NSA, ker ta obveznost odstopa od načela zaupnosti komunikacij,[125] sama po sebi pripelje do posega, tudi če teh podatkov v nadaljevanju ne bi pregledovali in uporabljali obveščevalni organi.[126] *Hramba* in dejanski *dostop* s strani teh organov do metapodatkov in do vsebine komunikacij, ki so jim dani na razpolago, ter *uporaba* teh podatkov pomenijo dodatne posege.[127]

260. Vrh tega glede na ugotovitve predložitvenega sodišča[128] in drugih virov, kot je poročilo PCLOB o programih, izvajanih na podlagi člena 702 FISA, na katero je Sodišče opozorila ameriška vlada,[129] NSA v okviru programa Upstream že ima *dostop, in sicer zaradi filtriranja*, do obsežnih zbirk („paketov“) podatkov iz tokov komunikacij, ki prehajajo po telekomunikacijski „hrbtenici“ in zajemajo komunikacije, ki ne vsebujejo izbirnikov, ki jih je opredelila NSA. NSA naj bi te zbirke podatkov lahko pregledovala le za to, da na hitro in avtomatizirano ugotovi, ali vsebujejo te izbirnike. Le tako filtrirane komunikacije naj bi bilo potem mogoče shranjevati v podatkovnih bazah NSA. Ta dostop do podatkov zaradi njihovega filtriranja bi po mojem mnenju prav tako pomenil poseg v uresničevanje pravice posameznikov, na katere se nanašajo osebni podatki, do spoštovanja zasebnega življenja ne glede na nadaljnjo uporabo hranjenih podatkov.[130]

261. Poleg tega dajanje zadevnih podatkov na razpolago in njihovo filtriranje,[131] dostop obveščevalnih organov do teh podatkov, pa tudi morebitna hramba, analiza in uporaba navedenih podatkov spadajo v okvir pojma „obdelava“ v smislu člena 4, točka 2, GDPR in člena 8(2) Listine. Ta obdelava mora zato izpolnjevati zahteve iz zadnjenavedene določbe.[132]

262. Nadzor na podlagi EO 12333 pa bi lahko vključeval neposredni dostop obveščevalnih organov do podatkov v tranzitu, kar bi pripeljalo do posega v uresničevanje pravice, zagotovljene v členu 8 EKČP. Temu posegu bi se pridruževal še poseg, ki bi ga pomenila morebitna nadaljnja uporaba teh podatkov.

123 Glej sodbo Digital Rights Ireland (točka 33); mnenje 1/15 (točka 124), in sodbo Ministerio Fiscal (točka 51).

124 Glej točke od 78 do 81 obrazložitve Sklepa o zasebnostnem ščitu in Prilogo VI, točka II, k temu sklepu.

125 Glej v zvezi s tem sodbo Digital Rights Ireland (točka 32).

126 Glej v tem smislu mnenje 1/15 (točki 124 in 125), iz katerega izhaja, da sporočanje podatkov tretji osebi pomeni poseg v uresničevanje temeljnih pravic posameznikov, na katere se nanašajo osebni podatki, ne glede na nadaljnjo uporabo teh podatkov.

127 Glej v tem smislu sodbo Digital Rights Ireland (točka 35); sodbo Schrems (točka 87), in mnenje 1/15 (točke od 123 do 126).

128 Glej točko 60 teh sklepnih predlogov.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2. julij 2014 (v nadaljevanju: poročilo PCLOB, str. 84 in 111). Glej tudi WP29, Zasebnostni ščit EU-ZDA – Prvi skupni letni pregled, 28. november 2017, WP 255 (točka B.1.1, str. 15).

130 Glej opombo 131 teh sklepnih predlogov.

131 Glej v zvezi s tem točko 222 teh sklepnih predlogov.

132 Glej mnenje 1/15 (točka 123 in navedena sodna praksa).

2) Zahteva, da so posegi „predpisani z zakonom“

263. V skladu sodno prakso Sodišča [133] in ESČP [134] zahteva, da mora biti vsak poseg v uresničevanje temeljnih pravic „predpisan z zakonom“ v smislu člena 52(1) Listine in člena 8(2) EKČP, ne pomeni le, da mora imeti ukrep, s katerim je poseg določen, pravno podlago v nacionalnem pravu, ampak tudi, da mora ta pravna podlaga imeti določene lastnosti glede dostopnosti in predvidljivosti, tako da se prepreči tveganje samovoljnosti.

264. V zvezi s tem si stranke in zainteresirani subjekti, ki so Sodišču predložili stališča, v bistvu nasprotujejo glede vprašanja, ali člen 702 FISA in EO 12333 izpolnjujeta pogoj glede predvidljivosti zakona.

265. S tem pogojem, kot ga razlagata Sodišče [135] in ESČP [136], se zahteva, da predpisi, ki pomenijo poseg v uresničevanje pravice do spoštovanja zasebnega življenja, določajo jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da se posameznikom, na katere se nanašajo osebni podatki, zagotovijo ustrezni zaščitni ukrepi za varstvo njihovih podatkov pred tveganji zlorabe in vsakršnim nezakonitim dostopom do teh podatkov ali njihovo nezakonito uporabo. Taka pravila morajo zlasti določati, v kakšnih okoliščinah in pod katerimi pogoji lahko javni organi hranijo osebne podatke, do njih dostopajo in jih uporabljajo. [137] Poleg tega mora pravna podlaga, ki omogoča poseg, sama opredeljevati obseg omejitve uresničevanja pravice do spoštovanja zasebnega življenja. [138]

266. Enako kot M. Schrems in EPIC dvomim, da sta EO 12333 in PPD 28 – v slednji so določeni zaščitni ukrepi, ki spremljajo vse obveščevalne dejavnosti SIGINT – [139] dovolj predvidljivi, da bi imeli „status zakona“.

133 Glej zlasti mnenje 1/15 (točka 146).

134 Glej zlasti sodbo ESČP z dne 2. avgusta 1984, Malone proti Združenemu kraljestvu (CE:ECHR:1984:0802JUD000869179, točka 66); sklep z dne 29. junija 2006, Weber in Saravia proti Nemčiji (CE:ECHR:2006:0629DEC005493400, točka 84 in navedena sodna praksa; v nadaljevanju: sklep Weber in Saravia), in sodbo z dne 4. decembra 2015, Zakharov proti Rusiji (CE:ECHR:2015:1204JUD004714306, točka 228, v nadaljevanju: sodba Zakharov).

135 Glej zlasti sodbo Digital Rights Ireland (točki 54 in 65); sodbo Schrems (točka 91); sodbo Tele2 Sverige (točka 109), in mnenje 1/15 (točka 141).

136 Glej zlasti sklep Weber in Saravia (točki 94 in 95); sodbo Zakharov (točka 236), in sodbo ESČP z dne 12. januarja 2016, Szabó in Vissy proti Madžarski (CE:ECHR:2016:0112JUD003713814, točka 59; v nadaljevanju: sodba Szabó in Vissy).

137 Glej sodbo Tele2 Sverige (točka 117) in mnenje 1/15 (točka 190). Prav tako glej zlasti sodbo ESČP z dne 2. avgusta 1984, Malone proti Združenemu kraljestvu (CE:ECHR:1984:0802JUD000869179, točka 67); sodbo Zakharov (točka 229), in sodbo Szabó in Vissy (točka 62). ESČP v njih pojasnjuje, da zahteva po predvidljivosti na področju prestrezanja komunikacij nima enakega obsega kot na drugih področjih. V okviru ukrepov prikritega nadzora „zahteva po predvidljivosti ne more pomeniti, da je treba posamezniku omogočiti, da predvidi, ali in kdaj lahko organi prestrezajo njegove komunikacije, da bi lahko skladno s tem prilagodil svoje ravnanje“.

138 Mnenje 1/15 (točka 139). Glej v tem smislu tudi sodbo ESČP z dne 25. marca 1983, Silver in drugi proti Združenemu kraljestvu (CE:ECHR:1983:0325JUD000594772, točki 88 in 89).

139 Točke od 69 do 77 obrazložitve Sklepa o zasebnostnem ščitu in Priloga VI, točka I, k temu sklepu vsebujejo predstavitev PPD 28. V njih je pojasnjeno, da se ta predsedniška direktiva uporablja za obveščevalne dejavnosti, ki temeljijo na členu 702 FISA, in za tiste, ki se izvajajo zunaj ozemlja Združenih držav.

267. V teh instrumentih je izrecno omenjeno, da se z njima zadevnim osebam ne podeljujejo pravno izvršljive pravice.[140] Te osebe se zato pred sodišči ne morejo sklicevati na zaščitne ukrepe, ki jih določa PPD 28.[141] Komisija je v Sklepu o zasebnostnem ščitu sicer menila, da zaščitni ukrepi, določeni v tej predsedniški direktivi, čeprav so za obveščevalne službe zavezujoči,[142] „niso naveden[i] v […] pravnih izrazih“.[143] EO 12333 in PPD 28 sta bolj podobni internim upravnim navodilom, ki jih predsednik Združenih držav lahko razveljavi ali spremeni. ESČP pa je že odločilo, da interna upravna navodila nimajo statusa „zakona“.[144]

268. M. Schrems v zvezi s členom 702 FISA izpodbija predvidljivost te določbe, ker naj izbire izbirnih meril, ki se uporabljajo za filtriranje podatkov, ne bi omejevala z ustreznimi zaščitnimi ukrepi pred tveganji zlorabe. Ker se ta problem nanaša tudi na nujno potrebnost posegov, ki jih določa člen 702 FISA, ga bom preučil v nadaljevanju svoje analize.[145]

269. Tretje vprašanje za predhodno odločanje se prekriva s temo izpolnjevanja pogoja v zvezi s „statusom zakona“. S tem vprašanjem želi predložitveno sodišče v bistvu izvedeti, ali je treba ustreznost ravni varstva, zagotovljene v tretji državi, preučiti zgolj glede na pravno zavezujoča pravila, veljavna v tej tretji državi, in prakse, katerih namen je zagotoviti njihovo upoštevanje, ali pa tudi glede na razne nezavezujoče instrumente in izvensodne nadzorne mehanizme, ki se uporabljajo v njej.

270. V zvezi s tem člen 45(2)(a) GDPR določa neizčrpen seznam okoliščin, ki jih mora Komisija upoštevati pri ocenjevanju ustreznosti ravni varstva, zagotovljene v tretji državi. Med temi okoliščinami sta veljavna zakonodaja in to, kako se izvaja. V tej določbi je omenjen tudi vpliv drugih vrst pravil, kot so strokovna pravila in varnostni ukrepi. Poleg tega se z njo zahteva, da se upoštevajo „dejanske in izvršljive pravice“ ter „učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo“.[146]

271. Navedena določba, v celoti gledano in ob upoštevanju neizčrpnosti seznama, ki ga vsebuje, po mojem mnenju pomeni, da je prakse ali instrumente, ki nimajo dostopne in predvidljive pravne podlage, mogoče upoštevati v okviru celovitega ocenjevanja ravni varstva, zagotovljene v zadevni tretji državi, tako da se potrdijo zaščitni ukrepi, ki imajo pravno podlago s tema lastnostma. Toda kot v bistvu navajajo DPC, M. Schrems, avstrijska vlada in EOVP, taki instrumenti ali prakse ne morejo nadomestiti takih zaščitnih ukrepov in torej niti sami po sebi zagotoviti zahtevane ravni varstva.

140 Točka 3.7(c) EO 12333 določa: „[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“. Člen 6(d) PPD 28 prav tako določa: „[t]his 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 Glej v tem smislu EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019 (točka 99).

142 Točke od 69 do 77 obrazložitve Sklepa o zasebnostnem ščitu.

143 Točka 76 obrazložitve Sklepa o zasebnostnem ščitu.

144 Glej sodbo ESČP z dne 25. marca 1983, Silver in drugi proti Združenemu kraljestvu (CE:ECHR:1983:0325JUD000594772, točki 26 in 86).

145 Glej točke od 295 do 301 teh sklepnih predlogov. V sodbi Tele2 Sverige (točki 116 in 117) in mnenju 1/15 (točki 140 in 141) je bil pogoj predvidljivosti zakona predstavljen kot tesno povezan s pogojem potrebnosti in sorazmernosti posega. Podobno je v skladu s sodno prakso ESČP obstoj učinkovitih zaščitnih ukrepov pred tveganji zlorabe sestavni del tako pogoja „predvidljivosti“ posega kot tudi pogoja, ki se nanaša na njegovo „potrebnost v demokratični družbi“, pri čemer se izpolnjevanje teh dveh pogojev preizkuša skupaj. Glej zlasti sodbo ESČP z dne 18. maja 2010, Kennedy proti Združenemu kraljestvu (CE:ECHR:2010:0518JUD002683905, točka 155); sodbo Zakharov (točka 236); sodbo Centrüm för Rättvisa (točka 107), in sodbo Big Brother Watch (točka 322).

146 Glej tudi uvodno izjavo 104 GDPR.

3) Neposeganje v bistveno vsebino temeljnih pravic

272. Zahteva iz člena 52(1) Listine, v skladu s katero mora kakršno koli omejevanje pravic ali svoboščin, zagotovljenih z Listino, spoštovati njihovo bistveno vsebino, pomeni, da kadar se s posegom vanje poseže v to bistveno vsebino, tega ni mogoče upravičiti z nobenim legitimnim ciljem. Takrat se šteje, da je ta poseg v nasprotju z Listino, ne da bi bilo treba preučiti ali je primeren in potreben za doseganje uresničevanega cilja.

273. V zvezi s tem je Sodišče odločilo, da nacionalni predpisi, ki javnim organom omogočajo splošen dostop do *vsebine* elektronskih komunikacij, posegajo v bistvo pravice do spoštovanja zasebnega življenja, zagotovljene v členu 7 Listine.[147] Nasprotno pa je, čeprav je poudarilo tveganja, povezana z dostopom do *podatkov o prometu in o lokaciji* ter njihovo analizo,[148] presodilo, da kadar je z nacionalnimi predpisi državnim organom dovoljen splošen dostop do teh podatkov, bistvena vsebina te pravice ni prizadeta.[149]

274. Za člen 702 FISA po mojem mnenju ni mogoče šteti, da je z njim ameriškim obveščevalnim organom dovoljeno splošno dostopati do vsebine elektronskih komunikacij.

275. Po eni strani je namreč dostop obveščevalnih organov do podatkov na podlagi člena 702 FISA *zaradi njihove* morebitne *analize in uporabe* omejen na podatke, ki ustrezajo izbirnim merilom, ki se navezujejo na posamezne cilje.

276. Po drugi strani bi program Upstream sicer lahko vključeval splošen dostop do vsebine elektronskih komunikacij *zaradi njihovega avtomatiziranega filtriranja*, če se izbirniki ne bi uporabili le za polji „od“ in „za“, temveč tudi za celotno vsebino tokov komunikacij (iskanje „v zvezi z“ izbirnikom).[150] Vendar kot trdi Komisija ter v nasprotju s tem, kar zatrjujeta M. Schrems in EPIC, začasnega dostopa obveščevalnih organov do celotne vsebine elektronskih komunikacij zgolj zaradi njihovega filtriranja z uporabo izbirnih meril ni mogoče enačiti s splošnim dostopom do te vsebine.[151] Po mojem mnenju teža posega, ki je posledica tega časovno omejenega dostopa zaradi avtomatiziranega filtriranja, ne dosega teže posega, ki je rezultat splošnega dostopa javnih organov do te vsebine zaradi

147 Glej sodbo Schrems (točka 94). Glej tudi sodbi Digital Rights Ireland (točka 39) in Tele2 Sverige (točka 101). Ob upoštevanju tesne povezave med pravicama do spoštovanja zasebnega življenja in do varstva osebnih podatkov se mi zdi, da bi nacionalni ukrep, s katerim se javnim organom daje splošen dostop do vsebine komunikacij, pomenil tudi kršitev bistvene vsebine pravice, določene v členu 8 Listine.

148 Glej točko 257 teh sklepnih predlogov. V sodbi Tele2 Sverige (točka 99) je Sodišče poudarilo, da so metapodatki zlasti sredstva za ugotavljanje profila zadevnih oseb. V Mnenju št. 4/2014 o nadzoru elektronskih komunikacij v obveščevalne namene in namene nacionalne varnosti z dne 10. aprila 2014, WP 215 (str. 5), je WP29 opozorila, da je metapodatke, ker so strukturirani, lažje povezati in analizirati kot podatke o vsebini.

149 Glej sodbo Tele2 Sverige (točka 99). Nekateri komentatorji so se spraševali o utemeljenosti razlikovanja med splošnim dostopom do vsebine komunikacij in splošnim dostopom do metapodatkov glede na razvoj tehnologij in načinov komuniciranja. Glej Falot, N., in Hijmans, H., „Tele2: de afweging tussen privacy en veiligheid nader omlijnd“, *Nederlands Tijdschrift voor Europees Recht*, št. 3, 2017 (str. 48), in 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 o sodbi Schrems), *European Constitutional Law Review*, 2016 (str. 5).

150 Glej opombo 87 Sklepa o zasebnostnem ščitu. Vendar je v skladu s stališčem EPIC in pisnim odgovorom vlade Združenih držav na vprašanja, ki jih je postavilo Sodišče, FISC leta 2017 zahtevalo prekinitev iskanj „v zvezi z“ izbirnikom zaradi nepravilnosti, ki so se pojavljala pri tovrstnih iskanjih. Kljub temu naj bi kongres v aktu o ponovni odobritvi FISA, sprejetem leta 2018, določil možnost ponovne uvedbe tovrstnih iskanj ob soglasju FISC in kongresa. Glej tudi EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019 (str. 27, točka 55).

151 S tega vidika je predložitveno sodišče v točkah 188 in 189 svoje sodbe z dne 3. oktobra 2017 razlikovalo „množično“ iskanje od „množičnega“ pridobivanja, zbiranja ali hrambe. Navedeno sodišče v bistvu meni, da če program Upstream vključuje „množično“ iskanje po vseh tokovih podatkov, ki prehajajo po telekomunikacijski „hrbtenici“, so pridobivanje, zbiranje in hramba ciljni v tem smislu, da so usmerjeni le v podatke, ki vsebujejo zadevne izbirnike.

njene analize in njene morebitne uporabe.[152] Začasni dostop zaradi filtriranja tem organom ne omogoča, da hranijo metapodatke ali vsebino komunikacij, ki ne ustrezajo izbirnim merilom, in zlasti ne – kot je pripomnila ameriška vlada – da oblikujejo profile v zvezi s posamezniki, ki niso izbrani kot cilji na podlagi teh meril.

277. Ob tem je vprašanje, ali izbira ciljev z uporabo izbirnikov v okviru programov, ki temeljijo na členu 702 FISA, učinkovito omejuje pooblastila obveščevalnih organov, odvisno od okvira za izbiro izbirnikov.[153] M. Schrems v zvezi s tem trdi, da ameriško pravo, ker za to ni zadostnega nadzora, ne določa zaščitnih ukrepov pred splošnih dostopom do vsebine komunikacij že v fazi filtriranja, tako da se s tem pravom posega v bistvo pravice posameznikov, na katere se nanašajo osebni podatki, do spoštovanja zasebnega življenja.

278. Kot bom podrobneje pojasnil v nadaljevanju,[154] se nagibam k strinjanju s temi dvomi glede vprašanja, ali je okvir za izbiro izbirnikov zadosten, da bi izpolnjeval merili predvidljivosti in sorazmernosti posegov. Vendar obstoj tega okvira, čeprav nepopolnega, nasprotuje ugotovitvi, da se s členom 702 FISA javnim organom dovoljuje splošen dostop do vsebine elektronskih komunikacij in da gre torej pri njem za poseganje v bistvo pravice, določene v členu 7 Listine.

279. Poudarjam tudi, da je Sodišče v mnenju 1/15 presodilo, da se bistvena vsebina pravice do varstva osebnih podatkov, zagotovljenega v členu 8 Listine, ohrani, kadar so nameni obdelave omejeni ter obdelavo spremljajo pravila za zagotavljanje, med drugim, varnosti, zaupnosti in celovitosti podatkov ter za njihovo varstvo pred nezakonitima dostopom in obdelavo.[155]

280. V Sklepu o zasebnostnem ščitu je Komisija ugotovila, da člen 702 FISA in PPD 28 oba določata meje v zvezi z nameni, za katere se lahko zbirajo podatki v okviru programov, ki se izvajajo na podlagi člena 702 FISA.[156] Komisija je v njem tudi navedla, da PPD 28 določa pravila, ki omejujejo dostop do podatkov, pa tudi njihovo hrambo in razširjanje, da bi se zagotovila njihova varnost in da bi bili zaščiteni pred nedovoljenimi dostopi.[157] Kot bo prikazano v nadaljevanju moje analize,[158] se mi pojavljajo dvomi zlasti glede vprašanja, ali so nameni zadevne obdelave opredeljeni dovolj jasno in natančno, da se zagotovi raven varstva, ki je v bistvenem enaka ravni, ki obstaja v pravnem redu Unije. Vendar te morebitne slabosti po mojem mnenju ne zadoščajo, da bi bilo mogoče ugotoviti, da bi se s takimi programi, če bi se izvajali v Uniji, kršila bistvena vsebina pravice do varstva osebnih podatkov.

152 Glej v tem smislu sodbo Supreme Court (vrhovno sodišče) z dne 31. maja 2019 (točki 11.2 in 11.3). Navedeno sodišče v njej poudarja: „[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 Glej mnenje 1/15 (točka 122). Glej tudi poročilo Evropske komisije za demokracijo skozi pravo (Beneška komisija) o demokratičnem nadzoru agencij za zbiranje obveščevalnih podatkov SIGINT z dne 15. decembra 2015, študija št. 719/2013 (CDL-AD(2015)011), str. 10: „V praksi gre pri vprašanju, ali ta proces primerno omejuje nepotrebne posege v nedolžne osebne komunikacije, za ugotavljanje, ali je izbirnik dovolj upošteven in specifičen ter ali je kakovost računalniškega algoritma, uporabljenega za prepoznavanje upoštevnih podatkov v okviru izbranih parametrov, zadovoljiva [...]".

154 Glej točke od 297 do 301 teh sklepnih predlogov.

155 Mnenje 1/15 (točka 150).

156 Glej točke 70, 103 in 109 obrazložitve Sklepa o zasebnostnem ščitu.

157 Glej točke od 83 do 87 obrazložitve Sklepa o zasebnostnem ščitu in Prilogo VI, točka I(c), k temu sklepu. Opozarjam, da se glede na poročilo PCLOB (str. od 51 do 66) postopki NSA za zmanjšanje količine podatkov na podlagi člena 702 FISA nanašajo v večini svojih vidikov le na ameriške osebe. Namen PPD 28 je bil veljavne zaščitne ukrepe razširiti na neameriške osebe. Glej PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, na voljo na naslovu: https://www.pclob.gov/reports/report-PPD28/ (str. 2). Ob tem pa hramba in uporaba podatkov za namene nacionalne varnosti, potem ko so jih javni organi pridobili, po mojem mnenju ne spadata na področje uporabe prava Unije (glej točko 226 teh sklepnih predlogov). Ustreznost ravni varstva, zagotovljene v okviru teh dejavnosti, je torej treba presojati glede na člen 8 EKČP.

158 Glej točke od 283 do 289 teh sklepnih predlogov.

281. Poleg tega je treba ustreznost ravni varstva, zagotovljene v okviru dejavnosti nadzora na podlagi EO 12333, naj spomnim, ocenjevati glede na določbe EKČP. V zvezi s tem je iz Sklepa o zasebnostnem ščitu razvidno, da so edine omejitve, uvedene za izvajanje ukrepov na podlagi EO 12333 za zbiranje podatkov o neameriških osebah, tiste, ki jih določa PPD 28.[159] Ta predsedniška direktiva določa, da mora biti uporaba tujih obveščevalnih podatkov „čim bolj prilagojena“. Vendar je v njej izrecno omenjena možnost „množičnega“ zbiranja podatkov zunaj ameriškega ozemlja zaradi uresničevanja nekaterih posebnih ciljev nacionalne varnosti.[160] Po mnenju M. Schremsa se z določbami PPD 28 – s katero se sicer ne ustvarjajo pravice za posameznike – osebam, na katere se nanašajo osebni podatki, ne zagotavlja varstvo pred tveganjem splošnega dostopa do vsebine njihovih elektronskih komunikacij.

282. V zvezi s tem bom opozoril samo, da se ESČP v svoji sodni praksi glede člena 8 EKČP ne zanaša na koncept poseganja v bistveno vsebino ali v bistvo pravice do spoštovanja zasebnega življenja.[161] Vse do danes ni presodilo, da ureditve, ki omogočajo prestrezanje elektronskih komunikacij, tudi množično, *presegajo polje proste presoje držav članic*. ESČP meni, da so take ureditve združljive s členom 8(2) EKČP, če jih spremljajo nekateri minimalni zaščitni ukrepi.[162] V teh okoliščinah se mi ne zdi primerno skleniti, da ureditev nadzora, kot je ta, ki jo določa EO 12333, presega polje proste presoje držav članic, ne da bi se lotil kakršne koli preučitve morebitnih zaščitnih ukrepov, ki jo spremljajo.

4) Uresničevanje legitimnega cilja

283. V skladu s členom 52(1) Listine mora kakršno koli omejevanje uresničevanja pravic, določenih v njej, dejansko ustrezati ciljem splošnega interesa, ki jih priznava Unija. Člen 8(2) Listine tudi določa, da mora vsaka obdelava osebnih podatkov, ki ne temelji na privolitvi prizadete osebe, temeljiti na „legitimni podlagi, določeni z zakonom“. V členu 8(2) EKČP so navedeni cilji, ki lahko upravičujejo poseg v uresničevanje pravice do spoštovanja zasebnega življenja.

284. V skladu s Sklepom o zasebnostnem ščitu je spoštovanje načel, ki jih določa, lahko omejeno zaradi izpolnjevanja zahtev nacionalne varnosti, javnega interesa in kazenskega pregona.[163] V točkah od 67 do 124 obrazložitve tega sklepa so natančneje preučene omejitve, ki izhajajo iz dostopa do podatkov in njihove uporabe s strani ameriških javnih organov zaradi nacionalne varnosti.

159 Komisija je v točki 127 obrazložitve Sklepa o zasebnostnem ščitu zlasti ugotovila, da četrti amandma ustave Združenih držav ne zajema neameriških oseb.

160 Glej točki 73 in 74 obrazložitve Sklepa o zasebnostnem ščitu ter Prilogo VI, točka I(b), k temu sklepu. Ti cilji zajemajo boj proti vohunstvu ter drugim grožnjam in dejavnostim, ki jih tuje sile usmerjajo zoper Združene države in njene interese, proti terorističnim grožnjam, proti grožnjam, ki izhajajo iz razvoja, posesti, širjenja ali uporabe orožja za množično uničevanje, proti grožnjam, povezanim s kibernetsko varnostjo, proti grožnjam za oborožene sile Združenih držav ali njenih zaveznikov in proti nadnacionalnim kriminalnim grožnjam. Glede na opombo 5 PPD 28 omejitev ciljev, ki upravičuje uporabo „množično“ zbranih podatkov, ne velja, kadar je tako zbiranje zgolj začasno in namenjeno olajšanju ciljnega zbiranja.

161 Čeprav v določbah EKČP „bistvena vsebina“ temeljnih pravic ni omenjena, je v sodni praksi ESČP glede nekaterih od teh določb mogoče najti pojem, enakovreden „samemu bistvu“ temeljne pravice. V zvezi z bistvom pravice do poštenega sojenja, zagotovljene v členu 6 EKČP, glej zlasti sodbe ESČP z dne 25. maja 1985, Ashingdane proti Združenemu kraljestvu (CE:ECHR:1985:0528JUD000822578, točki 57 in 59); z dne 21. decembra 2000, Heaney in McGuinness proti Irski (CE:ECHR:2000:1221JUD003472097, točki 55 in 58), in z dne 23. junija 2016, Baka proti Madžarski (CE:ECHR:2016:0623JUD002026112, točka 121). V zvezi z bistvom pravice do poroke, določene v členu 12 EKČP, glej sodbo ESČP z dne 11. julija 2002, Christine Goodwin proti Združenemu kraljestvu (CE:ECHR:2002:0711JUD002895795, točki 99 in 101). Glede bistva pravice do izobraževanja, zagotovljene v členu 2 Protokola št. 1 k EKČP, glej sodbo ESČP z dne 23. julija 1968, zadeva „o nekaterih vidikih jezikovnega sistema belgijskega izobraževanja“ (CE:ECHR:1968:0723JUD000147462, točka 5).

162 Glej zlasti sodbi Centrüm för Rättvisa (točke od 112 do 114 in navedena sodna praksa) in Big Brother Watch (točka 337).

163 Glej točko 197 teh sklepnih predlogov.

285. Ni sporno, da je varovanje nacionalne varnosti legitimen cilj, ki lahko upravičuje odstopanja od zahtev, izhajajočih iz GDPR,[164] in od temeljnih pravic, določenih v členih 7 in 8 Listine[165] in členu 8(2) EKČP. Vendar so M. Schrems, avstrijska vlada in EPIC opozorili, da cilji, uresničevani v okviru programov nadzora, ki temeljijo na členu 702 FISA in na EO 12333, presegajo zgolj nacionalno varnost. Cilj teh instrumentov je namrečpridobivanje „tujih obveščevalnih podatkov“, pri čemer ta pojem zajema različne vrste informacij, ki vključujejo informacije, povezane z nacionalno varnostjo, niso pa nujno omejene nanje.[166] S pojmom „tuji obveščevalni podatki“ v smislu člena 702 FISA so tako zajeti podatki, povezani z vodenjem zunanjih zadev.[167] V EO 12333 pa je ta pojem opredeljen tako, da zajema informacije v zvezi z zmogljivostmi, nameni ali dejavnostmi tujih vlad, tujih organizacij in tujih oseb.[168] M. Schrems izpodbija legitimnost tako zastavljenega cilja v delu, v katerem presega nacionalno varnost.

286. Po mojem mnenju področje nacionalne varnosti v določeni meri lahko vključuje zaščito interesov, povezanih z vodenjem zunanjih zadev.[169] Poleg tega ni nemogoče, da nekateri od namenov, razen varovanja nacionalne varnosti, ki jih zajema pojem „tuji obveščevalni podatki“, kot je opredeljen v členu 702 FISA in v EO 12333, ustrezajo pomembnim ciljem v splošnem interesu, ki lahko upravičujejo poseg v temeljni pravici do spoštovanja zasebnega življenja in do varstva osebnih podatkov. Ti cilji bi v okviru tehtanja med temeljnimi pravicami posameznikov, na katere se nanašajo osebni podatki, in ciljem, ki se uresničuje s posegom, vsekakor imeli manjšo težo kot varovanje nacionalne varnosti.[170]

287. Vendar je v skladu s členom 52(1) Listine potrebno še, da se z ukrepi, ki določajo zadevne posege, dejansko uresničuje nacionalna varnost ali drug legitimen cilj.[171] Poleg tega morajo biti nameni posegov opredeljeni na način, ki ustreza zahtevama po jasnosti in natančnosti.[172]

288. Po mnenju M. Schremsa pa namen ukrepov nadzora iz člena 702 FISA in iz EO 12333 ni določen dovolj natančno, da bi se spoštovali jamstvi predvidljivosti in sorazmernosti. To naj bi zlasti veljalo, ker je v teh instrumentih pojem „tuji obveščevalni podatki“ opredeljen posebej široko. Poleg tega je Komisija v točki 109 obrazložitve Sklepa o zasebnostnem ščitu ugotovila, da se s členom 702 FISA zahteva, da je „pomemben namen“ pridobivanja zbrati tuje obveščevalne podatke, pri čemer ta formulacija – na prvi pogled in kot navaja EPIC – ne izključuje uresničevanja drugih, neopredeljenih ciljev.

164 Glej člen 23(1)(a) GDPR.

165 Glej sodbo Schrems (točka 88). Sodišče je sorodni pojem „javna varnost“ v smislu določb PDEU, s katerimi so dovoljena odstopanja od temeljnih svoboščin, zagotovljenih z njo, štelo za samostojen pojem prava Unije, ki pokriva tako notranjo kot zunanjo varnost držav članic (glej zlasti sodbi z dne 26. oktobra 1999, Sirdar (C-273/97, EU:C:1999:523, točka 17), in z dne 13. septembra 2016, CS (C-304/14, EU:C:2016:674, točka 39 in navedena sodna praksa)). Notranja varnost je lahko ogrožena zlasti z neposredno grožnjo za mir in fizično varnost prebivalstva zadevne države članice, zunanja varnost pa je lahko ogrožena zlasti s tveganjem resnih motenj v zunanjih odnosih ali mirnem sožitju med narodi. Ne da bi lahko enostransko določila vsebino teh pojmov, ima vsaka država članica določeno polje proste presoje za opredelitev svojih bistvenih interesov v smislu varnosti. Glej zlasti sodbo z dne 2. maja 2018, K. in H. F. (Pravica do prebivanja in obtožbe o vojnih zločinih) (C-331/16 in C-366/16, EU:C:2018:296, točke od 40 do 42 in navedena sodna praksa). Te preudarke je po mojem mnenju mogoče prenesti na razlago pojma „nacionalna varnost“ kot interesa, katerega zaščita lahko upravičuje omejitve določb GDPR in pravic, zagotovljenih s členoma 7 in 8 Listine.

166 Glej v zvezi s tem točko 89 obrazložitve in opombo 97 Sklepa o zasebnostnem ščitu.

167 Glej točko 55 teh sklepnih predlogov.

168 Glej točko 61 teh sklepnih predlogov.

169 V sodbi Centrüm för Rättvisa (točka 111) je ESČP presodilo, da dejavnosti nadzora, katerih namen je podpreti zunanjo, obrambno in varnostno politiko Švedske ter odkriti zunanje grožnje, organizirane na Švedskem, uresničujejo legitimne cilje v zvezi z nacionalno varnostjo.

170 Glej v zvezi s tem sodbo Tele2 Sverige (točka 115) in sodbo Ministerio Fiscal (točka 55). Sodišče je v teh sodbah poudarilo povezavo med težo posega in težo interesa, ki se navaja, da bi se ta poseg upravičil.

171 WP29 v svojem delovnem dokumentu o nadzoru elektronskih komunikacij v obveščevalne namene in namene nacionalne varnosti z dne 5. decembra 2014,WP 228 (str. 26), poudarja pomen tega, da se kritično presodi, ali se nadzor dejansko izvaja zaradi nacionalne varnosti.

172 Glej mnenje 1/15 (točka 181), v katerem je Sodišče presodilo, da besedilo zakonskih določb, s katerimi so bili določeni posegi, ne izpolnjuje zahtev po jasnosti in natančnosti, tako da ti posegi niso bili omejeni na tisto, kar je bilo nujno potrebno. Z istega vidika je generalni pravobranilec Y. Bot v sklepnih predlogih v zadevi Schrems (C-362/14, EU:C:2015:627, točke od 181 do 184) menil, da so cilji ukrepov nadzora opredeljeni preveč splošno, da bi se lahko šteli za cilje v splošnem interesu, razen v zvezi z nacionalno varnostjo.

289. Iz teh razlogov se je, ne da bi bilo izključeno, da ukrepi nadzora na podlagi člena 702 FISA in EO 12333 ustrezajo legitimnim ciljem, dopustno vprašati, ali so ti cilji opredeljeni dovolj jasno in natančno, da se prepreči tveganje zlorabe in da je mogoč nadzor sorazmernosti posegov, ki so posledica teh ukrepov. [173]

5) Potrebnost in sorazmernost posegov

290. Sodišče je večkrat poudarilo, da pravice, določene v členih 7 in 8 Listine, niso absolutne pravice, temveč jih je treba v skladu z načelom sorazmernosti obravnavati glede na vlogo, ki jo imajo v družbi, in jih uravnotežiti z drugimi temeljnimi pravicami. [174] Kot je izpostavila družba Facebook Ireland, te druge pravice vključujejo pravico do varnosti, zagotovljeno v členu 6 Listine.

291. V zvezi s tem mora biti v skladu s prav tako ustaljeno sodno prakso vsak poseg v uresničevanje pravic, zagotovljenih s členoma 7 in 8 Listine, predmet strogega nadzora sorazmernosti. [175]

292. Iz sodbe Schrems zlasti izhaja, da „ni zgolj na nujno potrebno omejena ureditev, ki splošno dovoljuje hrambo vseh […] podatkov […], ne da bi se uporabljalo kakršno koli razlikovanje, omejitev ali izjema glede na cilj, ki se ga poskuša doseči, in ne da bi bilo predvideno objektivno merilo, ki bi omogočalo dostop javnih organov do podatkov in poznejšo uporabo teh podatkov samo v namene, ki so natančno določeni, strogo omejeni in bi lahko utemeljevali poseg, ki ga pomenita dostop in uporaba teh podatkov“. [176]

293. Sodišče je tudi odločilo, da mora sodišče ali neodvisen upravni organ, razen v nujnih primerih, ki so ustrezno utemeljeni, opraviti predhoden nadzor dostopa, pri čemer je odločitev tega sodišča ali organa namenjena omejevanju dostopa do podatkov in njihove uporabe na tisto, kar je nujno potrebno za doseganje uresničevanega cilja. [177]

294. Člen 23(2) GDPR zdaj določa niz zaščitnih ukrepov, ki jih mora država članica določiti, kadar odstopa od določb te uredbe. Predpisi, ki omogočajo tako odstopanje, morajo vsebovati določbe, ki se med drugim nanašajo na namen obdelave, obseg odstopanja, zaščitne ukrepe za preprečitev zlorab, obdobja hrambe in pravico posameznikov, na katere se nanašajo osebni podatki, da so obveščeni o odstopanju, razen če to ne bi posegalo v namen odstopanja.

295. V obravnavanem primeru M. Schrems trdi, da člena 702 FISA ne spremljajo ustrezni zaščitni ukrepi pred tveganji zlorabe in nezakonitega dostopa do podatkov. Zlasti naj izbira izbirnih meril ne bi bila dovolj omejena, tako da naj ta določba ne bi zagotavljala jamstev proti splošnemu dostopu do vsebine komunikacij.

296. Vlada Združenih držav in Komisija nasprotno zatrjujeta, da je v členu 702 FISA izbira izbirnikov omejena z objektivnimi merili, ker ta določba omogoča le zbiranje podatkov o elektronskih komunikacijah neameriških oseb, ki so zunaj Združenih držav, zaradi pridobivanja tujih obveščevalnih podatkov.

173 Podobne dvome je izrazil ENVP v svojem mnenju z dne 30. maja 2016, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision (str. 8).

174 Glej sodbo z dne 9. novembra 2010, Volker und Markus Schecke in Eifert (C-92/09 in C-93/09, EU:C:2010:662, točka 48); mnenje 1/15 (točka 136), in sodbo z dne 24. septembra 2019, Google (Ozemeljski obseg odstranitve povezav) (C-507/17, EU:C:2019:772, točka 60).

175 Glej zlasti sodbo z dne 16. decembra 2008, Satakunnan Markkinapörssi in Satamedia (C-73/07, EU:C:2008:727, točka 56); sodbo Digital Rights Ireland (točki 48 in 52); sodbo Schrems (točki 78 in 92), in mnenje 1/15 (točki 139 in 140). Glej tudi točko 140 obrazložitve Sklepa o zasebnostnem ščitu.

176 Sodba Schrems (točka 93). Glej v tem smislu tudi sodbo Digital Rights Ireland (točka 60).

177 Glej sodbo Tele2 Sverige (točka 120) in mnenje 1/15 (točka 202).

297. Po mojem mnenju je dopustno dvomiti o zadostni jasnosti in natančnosti teh merilter o obstoju ustreznih zaščitnih ukrepov za preprečitev tveganj zlorabe.

298. Najprej, v točki 109 obrazložitve Sklepa o zasebnostnem ščitu je navedeno, da ne FISC ne drug sodni ali neodvisen upravni organ ne odobri posamično izbirnikov, preden se uporabijo. Komisija je v njej ugotovila, da „FISC […] ne dovoljuje posameznih nadzornih ukrepov, temveč dovoljuje nadzorne programe […] na podlagi letnih potrdil“, kar je vlada Združenih držav potrdila pred Sodiščem. V tej točki obrazložitve je pojasnjeno, da „potrdila, ki ji[h] odobri FISC, ne vsebujejo nobenih informacij o ciljnih posameznikih, temveč so v njih opredeljene kategorije tujih obveščevalnih podatkov“, ki se lahko zbirajo. Komisija v njej tudi ugotavlja, da „FISC ne presoja – na podlagi verjetnega vzroka ali katerega koli drugega standarda – ustreznosti ciljnega osredotočanja na posameznike za pridobivanje tujih obveščevalnih podatkov“, čeprav nadzira izpolnjevanje pogoja, da „je pomemben namen pridobivanja zbrati tuje obveščevalne podatke“.

299. Dalje, v skladu s to točko obrazložitve je s členom 702 FISA agenciji NSA dovoljeno zbirati komunikacije „samo, če je mogoče utemeljeno sklepati, da se zadevno komunikacijsko sredstvo uporablja za sporočanje tujih obveščevalnih podatkov“. V točki 70 obrazložitve Sklepa o zasebnostnem ščitu je dodano, da se izbira izbirnikov izvaja v okviru prednostnih nalog nacionalnih obveščevalnih služb (National Intelligence Priorities Framework, NIPF). Ta sklep ne omenja natančnejših zahtev v zvezi z obrazložitvijo ali utemeljitvijo izbire izbirnikov glede na te upravne prednostne naloge, ki naj bi bile veljale za NSA. [178]

300. Nazadnje, točka 71 obrazložitve Sklepa o zasebnostnem ščitu se sklicuje na zahtevo, ki je določena v PPD 28 in v skladu s katero mora biti zbiranje tujih obveščevalnih podatkov „prilagojeno in izvedljivo [čim bolj prilagojeno]“. Poleg tega, da se s to predsedniško direktivo ne ustvarjajo pravice za posameznike, se mi bistvena enakost med merilom „čim bolj prilagojene“ dejavnosti in merilom „nujno potrebnega“, ki ga določa člen 52(1) Listine za upravičenost posega v uresničevanje pravic, zagotovljenih z njenima členoma 7 in 8, še zdaleč ne zdi očitna. [179]

301. Glede na te preudarke ni gotovo, da na podlagi elementov, predstavljenih v Sklepu o zasebnostnem ščitu, ukrepe nadzora, ki temeljijo na členu 702 FISA, spremljajo zaščitni ukrepi – povezani z omejevanjem oseb, za katere se lahko uporabi ukrep nadzora, in ciljev, za katere se lahko zbirajo podatki – ki bi bili v bistvenem enaki zaščitnim ukrepom, ki se zahtevajo v skladu s GDPR, razlagano ob upoštevanju členov 7 in 8 Listine. [180]

178 V poročilu PCLOB (str. 45) je natančneje navedeno: „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 Glej v tem smislu WP29, Mnenje št. 1/2016 o osnutku sklepa o ustreznosti zasebnostnega ščita EU-ZDA, 13. april 2016, WP 238 (točka 3.3.1, str. 38); Resolucijo Parlamenta z dne 6. aprila 2017 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, P8_TA(2017)0131 (točka 17), in Poročilo Parlamenta o posledicah velepodatkov za temeljne pravice: zasebnost, varstvo podatkov, nediskriminacija, varnost in kazenski pregon, 20. februar 2017, A8-0044/2017 (točka 17).

180 Glej v tem smislu WP29, Zasebnostni ščit EU-ZDA – Prvi skupni letni pregled, 28. november 2017, WP 255 (str. 3); Resolucijo Evropskega parlamenta z dne 5. julija 2018 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, P8_TA (2018)0315 (točka 22), in EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019 (točke od 81 do 83 in 87).

302. Poleg tega je treba v zvezi z ocenjevanjem ustreznosti ravni varstva, zagotovljenega pri nadzoru na podlagi EO 12333, navesti, da ESČP državam članicam priznava široko polje proste presoje pri izbiri sredstev, s katerimi varujejo nacionalno varnost, pri čemer pa je to polje vseeno omejeno z zahtevo, da se določijo ustrezni in zadostni zaščitni ukrepi pred zlorabami.[181] V svoji sodni praksi glede ukrepov prikritega nadzora ESČP preverja, ali nacionalno pravo, na katerem temeljijo ti ukrepi, vsebuje ustrezne in učinkovite zaščitne ukrepe in varovala, s katerimi je mogoče izpolniti zahtevi po „predvidljivosti“ in „potrebnosti v demokratični družbi“.[182]

303. ESČP v zvezi s tem navaja nekatere minimalne zaščitne ukrepe. Ti zaščitni ukrepi zadevajo jasno navedbo narave kršitev, ki lahko pripeljejo do naloga za prestrezanje, opredelitev kategorij oseb, katerih komunikacije se lahko prestrezajo, določitev meje za čas trajanja izvajanja ukrepa, postopek, ki se uporablja za pregledovanje, uporabo in hrambo zbranih podatkov, previdnostne ukrepe, ki se sprejmejo za posredovanje podatkov drugim stranem, in okoliščine, v katerih je mogoče ali treba izbrisati ali uničiti shranjene podatke.[183]

304. Ustreznost in učinkovitost zaščitnih ukrepov, s katerimi je omejen poseg, sta odvisni od vseh okoliščin zadeve, vključno z naravo, obsegom in trajanjem ukrepov, razlogi, ki se zahtevajo za njihovo odreditev, organi, ki so pristojni za njihovo odobritev, izvajanje in nadzor, ter vrsto pravnega sredstva, ki je zagotovljeno v nacionalnem pravu.[184]

305. Pri ocenjevanju utemeljenosti ukrepa prikritega nadzora ESČP zlasti upošteva vse nadzore, ki se opravijo „ob odreditvi“, „med izvajanjem“ in „po prenehanju“ ukrepa.[185] V zvezi s prvo od teh treh faz ESČP zahteva, da tak ukrep odobri neodvisen organ. Čeprav po njegovem mnenju sodna oblast ponazarja najboljša jamstva neodvisnosti, nepristranskosti in pravilnosti postopka, ni nujno, da zadevni organ pripada sodstvu.[186] Poglobljen sodni nadzor v poznejši fazi lahko odtehta morebitne pomanjkljivosti v postopku odobritve.[187]

306. V obravnavanem primeru je iz Sklepa o zasebnostnem ščitu razvidno, da so edini zaščitni ukrepi, ki omejujejo zbiranje in uporabo podatkov zunaj ozemlja Združenih držav, določeni v PPD 28, saj se člen 702 FISA ne uporablja zunaj tega ozemlja. Nisem prepričan, da lahko ti zaščitni ukrepi zadostujejo za izpolnjevanje pogojev „predvidljivosti“ in „potrebnosti v demokratični družbi“.

307. Najprej, navedel sem že, da se s to predsedniško direktivo ne ustvarjajo pravice za posameznike. Dalje, dvomim, da je zahteva po zagotovitvi „čim bolj prilagojenega“ nadzora izražena z dovolj jasnimi in natančnimi izrazi, da bi bili posamezniki, na katere se nanašajo osebni podatki, ustrezno zaščiteni pred tveganji zlorabe.[188] Nazadnje, v Sklepu o zasebnostnem ščitu ni ugotovljeno, da bi v zvezi z nadzorom, ki temelji na EO 12333, neodvisen organ opravil predhodni nadzor ali da bi lahko bil predmet naknadnega sodnega nadzora.[189]

181 Glej zlasti sodbi Zakharov (točka 232) in Szabó in Vissy (točka 57).

182 Glej zlasti sodbe Zakharov (točka 237); Centrüm för Rättvisa (točka 111), in Big Brother Watch (točka 322).

183 Glej zlasti sklep Weber in Saravia (točka 95); sodbo ESČP z dne 28. junija 2007, Association for european integration and human rights in Ekimdjiev (CE:ECHR:2007:0628JUD006254000, točka 76) in sodbo Zakharov (točka 231).

184 Glej zlasti sklep Weber in Saravia (točka 106); sodbo Zakharov (točka 232), in sodbo Centrüm för Rättvisa (točka 104).

185 Glej zlasti sodbo ESČP z dne 6. septembra 1978, Klass in drugi proti Nemčiji (CE:ECHR:1978:0906JUD000502971, točka 55); sodbo Zakharov (točka 233), in sodbo Centrüm för Rättvisa (točka 105).

186 Glej zlasti sodbo Klass (točka 56); sodbo ESČP z dne 18. maja 2010, Kennedy proti Združenemu kraljestvu (CE:ECHR:2010:0518JUD002683905, točka 167), in sodbo Zakharov (točki 233 in 258).

187 Glej sodbi Szabó in Vissy (točka 77) in Centrüm för Rättvisa (točka 133).

188 To velja še toliko bolj glede na preudarke, navedene v točki 281 teh sklepnih predlogov.

189 Glej točki 330 in 331 teh sklepnih predlogov.

308. V teh okoliščinah se sprašujem o utemeljenosti ugotovitve, da Združene države v okviru dejavnosti svojih obveščevalnih služb na podlagi člena 702 FISA in EO 12333 zagotavljajo ustrezno raven varstva v smislu člena 45(1) GDPR, razlaganega ob upoštevanju členov 7 in 8 Listine ter člena 8 EKČP.

c) Veljavnost Sklepa o zasebnostnem ščitu glede na pravico do učinkovitega pravnega sredstva

309. S petim vprašanjem za predhodno odločanje je Sodišče pozvano, naj odloči, ali so osebe, katerih podatki se prenašajo v Združene države, v tej državi deležne sodnega varstva, ki je v bistvenem enako varstvu, ki mora biti zagotovljeno v Uniji v skladu s členom 47 Listine. Z desetim vprašanjem ga predložitveno sodišče v bistvu sprašuje, ali mora biti odgovor na peto vprašanje pritrdilen ob upoštevanju dejstva, da je bil s Sklepom o zasebnostnem ščitu uveden mehanizem varuha človekovih pravic.

310. Najprej ugotavljam, da Komisija v točki 115 obrazložitve tega sklepa priznava, da ameriški pravni sistem vsebuje vrzeli v sodnem varstvu posameznikov.

311. V skladu s to točko obrazložitve, prvič, „vsaj nekatere pravne podlage, ki jih lahko uporabijo obveščevalni organi ZDA (npr. [EO] 12333), niso zajete“ z možnostmi pravnih sredstev. Z EO 12333 in PPD 28 se namreč zadevnim osebam ne podeljujejo pravice in se te nanju ne morejo sklicevati pred sodišči. Učinkovito sodno varstvo pa je pogojeno vsaj s tem, da imajo posamezniki pravice, na katere se lahko sklicujejo pred sodišči.

312. Drugič, „tudi kadar za nedržavljane ZDA [neameriške osebe] načeloma obstajajo možnosti pravnega varstva, kot na primer pri nadzoru v skladu s FISA, [so] razpoložljive možnosti za ukrepanje omejene in zahtevki […] se razglasijo za nedopustne, če ne morejo dokazati pravnega interesa [procesnega upravičenja], kar omejuje dostop do rednih sodišč“.

313. Iz točk 116, 117 in 122 obrazložitve Sklepa o zasebnostnem ščitu je razvidno, da je namen uvedbe varuha človekovih pravic nadomestiti te omejitve. Komisija v točki 139 obrazložitve tega sklepa ugotavlja, da „*nadzorni* in *pritožbeni* mehanizmi, ki jih zagotavlja zasebnostni ščit, *kot celota* […] posamezniku, na katerega se nanašajo osebni podatki, ponujajo pravna sredstva za pridobitev dostopa do osebnih podatkov, povezanih z njim, in, na koncu, popravek ali izbris takih podatkov“ (moj poudarek).

314. Spomnil bom na splošna načela, določena v sodni praksi Sodišča in ESČP glede pravice do pravnega sredstva zoper ukrepe nadzora komunikacij, hkrati pa preveril, ali pravna sredstva, določena v ameriškem pravu, kot so opisana v Sklepu o zasebnostnem ščitu, omogočajo zagotavljanje ustreznega sodnega varstva zadevnih oseb (razdelek 1)). Nato bom presodil, ali uvedba izvensodnega mehanizma varuha človekovih pravic glede na okoliščine omogoča, da se zapolnijo morebitne vrzeli, prisotne v sodnem varstvu teh oseb (razdelek 2)).

1) Učinkovitost pravnih sredstev, določenih v pravu Združenih držav

315. Prvič, člen 47, prvi odstavek, Listine določa pravico vsakogar, ki so mu kršene pravice in svoboščine, zagotovljene s pravom Unije, do učinkovitega pravnega sredstva pred sodiščem.[190] V skladu z drugim odstavkom tega člena ima vsakdo pravico, da o njegovi zadevi odloča neodvisno in nepristransko sodišče.[191] Dostop do neodvisnega sodišča je bistvena vsebina pravice, zagotovljene v členu 47 Listine.[192]

316. Ta pravica do individualnega sodnega varstva obstaja poleg obveznosti, ki je naložena državam članicam na podlagi členov 7 in 8 Listine, da za vsak ukrep nadzora, razen v nujnih primerih, ki so ustrezno utemeljeni, zagotovijo predhoden nadzor, ki ga opravi sodišče ali neodvisen upravni organ.[193]

317. Res je, da pravica do učinkovitega pravnega sredstva, kot sta zatrdili nemška in francoska vlada, ni absolutno jamstvo,[194] saj je ta pravica lahko omejena iz razlogov v zvezi z nacionalno varnostjo. Vendar so odstopanja dovoljena le, če ne posegajo v njeno bistveno vsebino in so nujno potrebna za doseganje legitimnega cilja.

318. V zvezi s tem je Sodišče v sodbi Schrems odločilo, da ureditev, ki ne določa *nobene možnosti*, da bi posameznik lahko uporabil pravna sredstva za pridobitev dostopa do osebnih podatkov, ki se nanj nanašajo, ali dosegel popravo ali izbris takih podatkov, posega v bistvo temeljne pravice, določene v členu 47 Listine.[195]

319. Poudarjam, da ta pravica do dostopa vključuje možnost, da oseba od javnih organov ob upoštevanju odstopanj, ki so nujno potrebna za uresničevanje legitimnega interesa, dobi *potrditev, ali obdelujejo njene osebne podatke, ali ne*.[196] Tak je po mojem mnenju praktični obseg pravice do dostopa, kadar zadevna oseba ne ve, ali so javni organi zlasti po koncu procesa avtomatiziranega filtriranja tokov elektronskih komunikacij shranili njene osebne podatke.

190 V Pojasnilih k Listini je v zvezi s tem navedeno, da „je varstvo [iz njenega člena 47] v okviru prava Unije širše [od varstva, podeljenega s členom 13 EKČP], saj zagotavlja pravico do učinkovitega pravnega sredstva pred sodiščem“. Glej tudi sklepne predloge generalnega pravobranilca M. Watheleta v zadevi Berlioz Investment Fund (C-682/15, EU:C:2017:2, točka 37).

191 Za presojo, ali ima neki organ v okviru uporabe člena 47 Listine status „sodišča“, je treba upoštevati njegovo zakonsko podlago, njegovo stalnost, obveznost njegove sodne pristojnosti, kontradiktornost njegovega postopka, njegovo uporabo pravnih pravil in njegovo neodvisnost. Glej sodbo z dne 27. februarja 2018, Associação Sindical dos Juízes Portugueses (C-64/16, EU:C:2018:117, točka 38 in navedena sodna praksa).

192 Glej zlasti sodbo z dne 25. julija 2018, Minister for Justice and Equality (Pomanjkljivosti v pravosodnem sistemu) (C-216/18 PPU, EU:C:2018:586, točki 59 in 63); z dne 5. novembra 2019, Komisija/Poljska (Neodvisnost splošnih sodišč) (C-192/18, EU:C:2019:924, točka 106), in z dne 19. novembra 2019, A. K. in drugi (Neodvisnost disciplinskega senata vrhovnega sodišča) (C-585/18, C-624/18 in C-625/18, EU:C:2019:982, točka 120).

193 Glej točko 293 teh sklepnih predlogov. Člen 45(3)(a) GDPR določa, da se pri ocenjevanju ustreznosti ravni varstva, zagotovljene v tretji državi, upošteva učinkovito „upravno *in sodno* varstvo“ posameznikov, na katere se nanašajo osebni podatki (moj poudarek). Podobno bi moralo biti v skladu z uvodno izjavo 104 GDPR sprejetje sklepa o ustreznosti pogojeno s tem, da je posameznikom, na katere se nanašajo osebni podatki, v zadevni tretji državi zagotovljen „dostop do učinkovitega upravnega *in sodnega* varstva“ (moj poudarek). Glej tudi WP29, Zasebnostni ščit EU-ZDA – Prvi skupni letni pregled, 28. november 2017, WP 255 (točka B.3); Resolucijo Parlamenta z dne 5. julija 2018 o ustreznosti varstva, ki ga zagotavlja zasebnostni ščit EU-ZDA, P8_TA (2018)0315 (točki 25 in 30), in EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019 (točke od 94 do 97).

194 Glej v tem smislu sodbo z dne 28. februarja 2013, Preveritev Arango Jaramillo in drugi/EIB (C-334/12 RX-II, EU:C:2013:134, točka 43).

195 Sodba Schrems (točka 95).

196 Člen 15 GDPR, naslovljen „Pravica dostopa posameznika, na katerega se nanašajo osebni podatki“, v odstavku 1 določa, da ima ta posameznik „pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je t[o] tako, dostop do osebnih podatkov“. „Načelo dostopa“, določeno v Prilogi II, točka II.8(a), k Sklepu o zasebnostnem ščitu, ima enak pomen.

320. Poleg tega iz sodne prakse izhaja, da so organi države članice načeloma dolžni obveščati o dostopu do podatkov *takoj, ko to obveščanje ne more več ogroziti preiskav, ki se vodijo*.[197] Tako obveščanje je namreč prvi pogoj za uresničevanje pravice do pravnega sredstva na podlagi člena 47 Listine.[198] Ta obveznost je zdaj povzeta v členu 23(2)(h) GDPR.

321. V točkah od 111 do 135 obrazložitve Sklepa o zasebnostnem ščitu so jedrnato predstavljena vsa pravna sredstva, ki so na voljo osebam, katerih podatki se prenašajo, kadar jih skrbi, da so te podatke po prenosu obdelovale ameriške obveščevalne službe. Ta pravna sredstva so bila opisana tudi v sodbi High Court (višje sodišče) z dne 3. oktobra 2017 in v stališču med drugim vlade Združenih držav.

322. Vsebine teh predstavitev ni treba še enkrat podrobno opisovati. Predložitveno sodišče namreč dvomi o ustreznosti zaščitnih ukrepov, povezanih s pravnim varstvom zadevnih oseb, v bistvu zato, ker posebno stroge zahteve glede procesnega upravičenja (*standing*)[199] v povezavi z neobstojem kakršne koli obveznosti obveščanja oseb, ki so bile predmet ukrepa nadzora, *tudi ko to obveščanje ne bi več ogrozilo ciljev*, v praksi preveč otežujejo uveljavljanje pravnih sredstev, določenih v pravu Združenih držav. DPC, M. Schrems, avstrijska, poljska in portugalska vlada ter EOVP se strinjajo s temi dvomi.[200]

323. V zvezi s tem bom samo spomnil, da pravila v zvezi s procesnim upravičenjem ne morejo posegati v učinkovito sodno varstvo,[201] in ugotovil, da v Sklepu o zasebnostnem ščitu ni omenjena nobena zahteva glede obveščanja zadevnih oseb o tem, da so bile predmet ukrepa nadzora.[202] Ker bi neobstoj obveznosti obveščanja o takem ukrepu, tudi ko obveščanje zadevne osebe ne bi več ogrozilo njegove učinkovitosti, lahko onemogočil uveljavljanje pravnih sredstev, je ta neobstoj očitno problematičen z vidika sodne prakse, omenjene v točki 320 teh sklepnih predlogov.

324. V opombi 169 Sklepa o zasebnostnem ščitu se poleg tega priznava, da razpoložljive možnosti za ukrepanje „bodisi zahtevajo obstoj škode […] ali dokaz, da namerava vlada uporabiti ali razkriti podatke, ki so pridobljeni [z] elektronsk[im] nadzor[om] zadevne osebe, proti tej osebi“. Kot so poudarili predložitveno sodišče, DPC in M. Schrems, je ta zahteva v nasprotju s sodno prakso Sodišča, v skladu s katero za dokaz posega v pravico zadevne osebe do spoštovanja zasebnega življenja ni potrebno, da je bila ta oseba zaradi zatrjevanega posega oškodovana.[203]

325. Poleg tega se mi stališče, ki ga izražata družba Facebook Ireland in vlada Združenih držav ter v skladu s katerim so slabosti, značilne za sodno varstvo oseb, katerih podatki se prenašajo v Združene države, nadomeščene s predhodnimi in naknadnimi nadzori, ki jih opravlja FISC, ter s številnimi nadzornimi mehanizmi, vzpostavljenimi v okviru izvršilne in zakonodajne oblasti,[204] ne zdi prepričljivo.

197 Sodba Tele2 Sverige (točka 121) in mnenje 1/15 (točka 220). Kot je opozorila družba Facebook Ireland, obveščanja o dostopu javnih organov do podatkov torej ni mogoče sistematično zahtevati. V zvezi s tem ESČP meni, da „[v] praksi morda ne bo mogoče zahtevati naknadnega obveščanja“, ker grožnja, ki je predmet ukrepov nadzora, „lahko traja leta, celo desetletja“ po odpravi teh ukrepov, tako da lahko obveščanje „ogrozi dolgoročni cilj, ki je bil prvotno razlog za nadzor“, in „razkrije delovne metode obveščevalnih služb, področja njihove dejavnosti in […] identiteto njihovih agentov“ (sodba Zakharov (točka 287 in navedena sodna praksa)). Ob neobstoju obveščanja, čeprav so individualna pravna sredstva torej nepraktična v primeru kršitve pravnih zahtev, lahko drugi zaščitni ukrepi zadostujejo za varstvo pravice do spoštovanja zasebnega življenja (glej tudi sodbo Centrüm för Rättvisa, točke od 164 do 167 in od 171 do 178). Glej točko 330 teh sklepnih predlogov.

198 Glej v zvezi s tem opombo 216 teh sklepnih predlogov.

199 Glej točko 67 teh sklepnih predlogov.

200 Glej EOVP, Zasebnostni ščit EU-ZDA – Drugi skupni letni pregled, 22. januar 2019 (str. 18, točka 97).

201 Glej zlasti sodbi z dne 11. julija 1991, Verholen in drugi (od C-87/90 do C-89/90, EU:C:1991:314, točka 24 in navedena sodna praksa), in z dne 28. februarja 2013, Réexamen Arango Jaramillo in drugi/EIB (C-334/12 RX-II, EU:C:2013:134, točka 43).

202 Vendar je vlada Združenih držav enako kot predložitveno sodišče pojasnila, da mora biti ciljna oseba obveščena o ukrepu nadzora na podlagi člena 702 FISA, če se zbrani podatki uporabijo zoper njo v okviru sodnega postopka.

203 Sodba z dne 20. maja 2003, Österreichischer Rundfunk in drugi (C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točka 75); sodba Digital Rights Ireland (točka 33); sodba Schrems (točka 87), in mnenje 1/15 (točka 124).

204 Ti mehanizmi so opisani v točkah od 95 do 110 obrazložitve Sklepa o zasebnostnem ščitu. Komisija v njih znotraj kategorije pravil o „učinkovitem pravnem varstvu“ razlikuje nadzorne mehanizme (glej točke od 92 do 110 obrazložitve) od individualnih pravnih sredstev (glej točke od 111 do 124 obrazložitve).

326. Poudaril sem že, da po eni strani v skladu z ugotovitvami, navedenimi v Sklepu o zasebnostnem ščitu, FISC ne nadzira posamičnih ukrepov nadzora pred njihovim izvajanjem.[205] Kot je navedeno v točki 109 obrazložitve tega sklepa in kot je vlada Združenih držav potrdila v pisnem odgovoru na vprašanja, ki jih je postavilo Sodišče, je po drugi strani namen naknadnega nadzora uporabe izbirnikov preveriti – ko obveščevalna agencija opozori FISC na primer, ki se nanaša na morebitno neupoštevanje postopkov za izbiro ciljev in za zmanjšanje količine podatkov –[206] upoštevanje pogojev, ki urejajo izbiro izbirnikov in se določijo v letnem potrjevanju. Za postopek pred FISC se torej ne zdi, da zagotavlja učinkovito individualno pravno sredstvo za osebe, katerih podatki se prenašajo v Združene države.

327. Izvensodni nadzorni mehanizmi, omenjeni v točkah od 95 do 110 obrazložitve Sklepa o zasebnostnem ščitu, čeprav bi glede na okoliščine lahko okrepili pravna sredstva, ki jih je možno vložiti pri sodišču, po mojem mnenju ne morejo zadostovati za zagotovitev ustrezne ravni varstva z vidika pravice zadevnih oseb do pravnega sredstva. Zdi se mi, da zlasti generalni inšpektorji, ki so del notranje strukture vsake agencije, ne pomenijo neodvisnih nadzornih mehanizmov. Nadzor, ki ga opravljajo PCLOB in obveščevalna odbora kongresa, pa ni enakovreden mehanizmu individualnega pravnega sredstva proti ukrepom nadzora.

328. Preučiti bo torej treba, ali uvedba varuha človekovih pravic odpravlja te vrzeli tako, da zadevnim osebam zagotavlja učinkovito pravno sredstvo pred neodvisnim in nepristranskim organom.[207]

329. Drugič, naj spomnim, da upoštevni referenčni okvir pri ocenjevanju utemeljenosti ugotovitve o ustreznosti, podane v Sklepu o zasebnostnem ščitu, z vidika pravnih sredstev, ki so na voljo osebam, ki menijo, da so bile predmet nadzora na podlagi EO 12333, tvorijo določbe EKČP.

330. Kot je bilo že razloženo,[208] ESČP pri ocenjevanju, ali ukrep nadzora izpolnjuje pogoja „predvidljivosti“ in „potrebnosti v demokratični družbi“ v smislu člena 8(2) EKČP,[209] opravi celovit preizkus mehanizmov za nadzor in spremljanje, ki se uporabljajo „pred, med in po“ izvedbi tega ukrepa. Kadar je uveljavljanje individualnega pravnega sredstva onemogočeno, ker obveščanje o ukrepu nadzora ni mogoče, ne da bi bila ogrožena njegova učinkovitost,[210] je to vrzel mogoče odtehtati z opravljanjem neodvisnega nadzora pred uporabo zadevnega ukrepa.[211] Čeprav torej ESČP meni, da je tako obveščanje „zaželeno“, takoj ko ga je mogoče uporabiti brez poslabšanja učinkovitosti ukrepa nadzora, ga ni povzdignilo v zahtevo.[212]

331. V zvezi s tem iz Sklepa o zasebnostnem ščitu ni razvidno, da bi se o ukrepih nadzora, ki temeljijo na EO 12333, obveščalo zadevne posameznike ali da bi bili ti ukrepi v kateri koli fazi njihovega sprejetja ali izvajanja omejeni s sodnimi ali neodvisnimi upravnimi nadzornimi mehanizmi.

205 Glej točko 298 teh sklepnih predlogov.

206 V skladu s točko 109 obrazložitve Sklepa o zasebnostnem ščitu „[g]eneralni državni tožilec in direktor [NSA] preverjata skladnost, agencije pa morajo kakršen koli primer neskladnosti sporočiti FISC, ki lahko na tej podlagi spremeni pooblastilo“.

207 Glej točke od 333 do 340 teh sklepnih predlogov.

208 Glej točko 305 teh sklepnih predlogov.

209 ESČP je v svoji sodni praksi, povezani z ukrepi nadzora telekomunikacij, vprašanje pravnih sredstev obravnavalo v okviru preučitve „statusa zakona“ in potrebnosti posega v uresničevanje pravice, zagotovljene s členom 8 EKČP (glej zlasti sodbi Zakharov (točka 236) in Centrüm för Rättvisa (točka 107)). V sodbi z dne 1. julija 2008, Liberty in drugi proti Združenemu kraljestvu (CE:ECHR:2008:0701JUD005824300, točka 73), in sodbi Zakharov (točka 307)je ESČP, potem ko je ugotovilo kršitev člena 8 EKČP, presodilo, da ni treba ločeno preučiti očitka v zvezi s členom 13 te konvencije.

210 Kot meni ESČP, čeprav neobveščanje v kateri koli fazi ni nujno ovira za to, da ukrep nadzora izpolnjuje pogoj „potrebnosti v demokratični družbi“, to neobveščanje spodkopava dostop do sodišč in s tem učinkovitost pravnih sredstev (glej zlasti sodbo z dne 6. septembra 1978, Klass in drugi proti Nemčiji (CE:ECHR:1978:0906JUD000502971, točki 57 in 58); odločbo Weber in Saravia (točka 135), in sodbo Zakharov (točka 302)).

211 Glej v tem smislu sodbo Centrum för Rättvisa (točka 105).

212 V sodbi Big Brother Watch (točka 317) ESČP minimalnim zaščitnim ukrepom, ki so se uporabljali za ureditev nadzora, za katero je bilo značilno množično prestrezanje elektronskih komunikacij, ni hotelo dodati zahteve po obveščanju zadevnih oseb o nadzoru. Glej tudi sodbo Centrüm för Rättvisa (točka 164). Namen predložitve teh sodb velikemu senatu ESČP je med drugim ponovna preučitev tega sklepa.

332. V teh okoliščinah je treba preučiti, ali uporaba varuha človekovih pravic vseeno omogoča, da se zagotovi neodvisen nadzor ukrepov nadzora, tudi kadar temeljijo na EO 12333.

2) Vpliv mehanizma varuha človekovih pravic na raven varstva pravice do učinkovitega pravnega sredstva

333. V skladu s točko 116 obrazložitve Sklepa o zasebnostnem ščitu je mehanizem varuha človekovih pravic, opisan v Prilogi III A k temu sklepu, namenjen zagotovitvi dodatnih pravnih sredstev vsem osebam, katerih podatki se prenašajo iz Unije v Združene države.

334. Kot je poudarila vlada Združenih držav, dopustnost pritožbe, vložene pri varuhu človekovih pravic, ni pogojena z upoštevanjem pravil v zvezi s procesnim upravičenjem, podobnih tistim, ki urejajo dostop do ameriških sodišč. V točki 119 obrazložitve navedenega sklepa je glede tega pojasnjeno, da uporaba varuha človekovih pravic ne predpostavlja, da zadevna oseba dokaže, da je vlada Združenih držav dostopala do njenih osebnih podatkov.

335. Tako kot DPC, M. Schrems, poljska in portugalska vlada ter EPIC dvomim o zmožnosti tega mehanizma, da nadomesti pomanjkljivosti sodnega varstva, zagotovljenega osebam, katerih podatki se prenašajo iz Unije v Združene države.

336. Najprej, čeprav mehanizem izvensodnega pravnega sredstva lahko pomeni učinkovito pravno sredstvo v smislu člena 47 PDEU, to velja, le če ima zadevni organ zlasti podlago v zakonu in izpolnjuje pogoj neodvisnosti.[213]

337. Iz Sklepa o zasebnostnem ščitu pa je razvidno, da mehanizem varuha človekovih pravic, ki izvira iz PPD 28,[214] nima podlage v zakonu. Varuha človekovih pravic imenuje zunanji minister in je sestavni del zunanjega ministrstva Združenih držav.[215] Ta sklep ne vsebuje nobene informacije, v skladu s katero bi za odpoklic varuha človekovih pravic ali razveljavitev njegovega imenovanja veljala posebna jamstva.[216] Čeprav je varuh človekovih pravic predstavljen kot neodvisen od „obveščevalne skupnosti“, odgovarja zunanjemu ministru in zato ni neodvisen od izvršilne oblasti.[217]

338. Dalje, zdi se mi, da je učinkovitost izvensodnega pravnega sredstva odvisna tudi od zmožnosti zadevnega organa, da sprejema zavezujoče in obrazložene odločbe. V zvezi s tem Sklep o zasebnostnem ščitu ne vsebuje nobene informacije, v skladu s katero bi varuh človekovih pravic sprejemal take odločbe. V njem ni ugotovljeno, da bi uvedba varuha človekovih pravic pritožnikom omogočala, da dostopajo do podatkov, ki se nanašajo nanje, in zagotovijo njihov popravek ali izbris, niti da bi varuh človekovih pravic osebam, oškodovanim zaradi ukrepa nadzora, dodeljeval odškodnino. Kot je razvidno iz Priloge III A, točka 4(e), k temu sklepu, zlasti „[v]aruh človekovih pravic […] ne bo ne potrdil ne zanikal, ali je posameznik tarča nadzora, prav tako pa varuh človekovih pravic

213 Pojem neodvisnosti zajema prvi, zunanji vidik, ki predpostavlja, da je zadevni organ zavarovan pred zunanjim posredovanjem ali pritiski, ki lahko ogrozijo neodvisnost sojenja njegovih članov glede sporov, ki so jim predloženi. Drugi, notranji vidik tega pojma je povezan s pojmom „nepristranskost“ in se nanaša na to, da je zagotovljena enaka distanca v razmerju do strank v sporu in njihovih posameznih interesov glede predmeta spora. Glej zlasti sodbe z dne 19. septembra 2006, Wilson (C-506/04, EU:C:2006:587, točke od 50 do 52); z dne 25. julija 2018, Minister for Justice and Equality (Pomanjkljivosti v pravosodnem sistemu) (C-216/18 PPU, EU:C:2018:586, točki 63 in 65), in z dne 19. novembra 2019, A. K. in drugi (Neodvisnost disciplinskega senata vrhovnega sodišča) (C-585/18, C-624/18 et C-625/18, EU:C:2019:982, točki 121 in 122). V skladu z načelom delitve oblasti mora biti zagotovljena zlasti neodvisnost sodišč od zakonodajne oblasti. Glej sodbo z dne 19. novembra 2019, A. K. in drugi (Neodvisnost disciplinskega senata vrhovnega sodišča) (C-585/18, C-624/18 et C-625/18, EU:C:2019:982, točka 127 in navedena sodna praksa).

214 Priloga III A k Sklepu o zasebnostnem ščitu se v zvezi s tem sklicuje na člen 4(d) PPD 28.

215 Glej točko 116 obrazložitve Sklepa o zasebnostnem ščitu.

216 V sodbi z dne 31. maja 2005, Syfait in drugi (C-53/03, EU:C:2005:333, točka 31), je Sodišče poudarilo pomen takih jamstev za izpolnjevanje pogoja neodvisnosti. V zvezi s tem glej tudi sodbi z dne 24. junija 2019, Komisija/Poljska (Neodvisnost vrhovnega sodišča) (C-619/18, EU:C:2019:531, točka 76) in z dne 5. novembra 2019, Komisija/Poljska (Neodvisnost splošnih sodišč) (C-192/18, EU:C:2019:924, točka 113).

217 Glej točki 65 in 121 obrazložitve Sklepa o zasebnostnem ščitu ter Prilogo III A, točka 1, k temu sklepu.

[…] ne bo potrdil posebnega pravnega sredstva, ki je bil[o] uporabljen[o]“.[218] Čeprav se je ameriška vlada zavezala, da je zadevni organ v sestavi obveščevalnih služb dolžan odpraviti vsako kršitev veljavnih pravil, ki jo odkrije varuh človekovih pravic,[219] navedeni sklep ne omenja zakonskih zaščitnih ukrepov, ki bi spremljali to zavezo in na katere bi se lahko zadevni posamezniki sklicevali.

339. Zato uvedba varuha človekovih pravic po mojem mnenju ne zagotavlja pravnega sredstva pred neodvisnim organom, ki bi osebam, katerih podatki se prenašajo, ponujalo možnost, da uveljavljajo svojo pravico do dostopa do podatkov ali da izpodbijajo morebitne kršitve veljavnih pravil s strani obveščevalnih služb.

340. Nazadnje, v skladu s sodno prakso bi se v tem primeru za spoštovanje pravice, zagotovljene s členom 47 Listine, zahtevalo, da nad odločbo upravnega organa, ki ne izpolnjuje pogoja neodvisnosti, pozneje nadzor opravi sodni organ, pristojen za obravnavo vseh upoštevnih vprašanj.[220] Vendar glede na informacije, zagotovljene v Sklepu o zasebnostnem ščitu, odločbe varuha človekovih pravic niso predmet neodvisnega sodnega nadzora.

341. V teh okoliščinah se mi, kot trdijo DPC, M. Schrems, EPIC ter poljska in portugalska vlada, bistvena enakost med sodnim varstvom, ki se v pravnem redu Združenih držav zagotavlja osebam, katerih podatki se prenašajo v to državo iz Unije, in sodnim varstvom, ki izhaja iz GDPR, razlagane ob upoštevanju člena 47 Listine in člena 8 EKČP, zdi vprašljiva.

342. Glede na vse zgornje preudarke imam določene dvome glede skladnosti Sklepa o zasebnostnem ščitu s členom 45(1) GDPR, razlaganega ob upoštevanju členov 7, 8 in 47 Listine ter člena 8 EKČP.

V. Predlog

343. Sodišču predlagam, naj na vprašanja za predhodno odločanje, ki jih je postavilo High Court (višje sodišče, Irska), odgovori:

Analiza vprašanj za predhodno odločanje ni razkrila elementov, ki bi lahko vplivali na veljavnost Sklepa Komisije 2010/87/EU z dne 5. februarja 2010 o standardnih pogodbenih klavzulah za prenos osebnih podatkov obdelovalcem s sedežem v tretjih državah v skladu z Direktivo Evropskega parlamenta in Sveta 95/46/ES, kakor je bil spremenjen z Izvedbenim sklepom Komisije (EU) 2016/2297 z dne 16. decembra 2016.

218 Poleg tega je v točki 121 obrazložitve Sklepa o zasebnostnem ščitu navedeno, da „bo moral varuh človekovih pravic ‚potrditi', da (i) je bila pritožba ustrezno proučena in da (ii) se je upoštevala ustrezna zakonodaja ZDA, vključno zlasti z omejitvami in zaščitnimi ukrepi iz Priloge VI, ali, v primeru neskladnosti, da je bila taka kršitev odpravljena“.

219 Komisija je v okviru tretjega letnega pregleda zasebnostnega ščita ugotovila, da bi bilo treba glede na izjave vlade Združenih držav v primeru, v katerem bi preiskava varuha človekovih pravic razkrila kršitev postopkov za izbiro ciljev in za zmanjšanje količine podatkov, ki jih je odobrilo FISC, s to kršitvijo seznaniti to sodišče. FISC bi potem opravilo neodvisno preiskavo in, če bi bilo to potrebno, zadevni obveščevalni agenciji odredilo, naj navedeno kršitev odpravi. Glej 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. oktober 2019, SWD(2019) 390 final, str. 28. Komisija se v tem dokumentu sklicuje na dokument z naslovom „Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure“, na voljo na naslovu https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (str. 4 in 5).

220 Glej sodbi z dne 16. maja 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, točka 55), in z dne 13. decembra 2017, El Hassani (C-403/16, EU:C:2017:960, točka 39).