



Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
YVESA BOTA,
predstavljeni 23. septembra 2015¹

Zadeva C-362/14

Maximillian Schrems
proti
Data Protection Commissioner
(Predlog za sprejetje predhodne odločbe,

ki ga je vložilo High Court of Justice (Irska))

„Predhodno odločanje — Osební podatki — Varstvo posameznikov pri obdelavi teh podatkov —
Listina Evropske unije o temeljnih pravicah — Členi 7, 8 in 47 — Direktiva 95/46/ES — Člen 25 —
Odločba 2000/520/ES — Prenos osebnih podatkov v ZDA — Presoja ustreznosti ali neustreznosti ravni
varstva — Pritožba posameznika, katerega podatki so bili preneseni v tretjo državo —
Nacionalni nadzorni organ — Pooblastila“

I – Uvod

1. Kot je Evropska komisija ugotovila v Sporočilu z dne 27. novembra 2013², „[je p]retok osebnih podatkov [...] pomemben in nujen del čezatlantskega partnerstva ter sestavni del trgovinske menjave, ki poteka čez Atlantik, vključno z novimi in hitro rastočimi digitalnimi podjetji, kot so socialna omrežja ter računalništvo v oblaku, pri katerih se med EU in ZDA pretakajo velike količine podatkov“³.
2. Trgovinske menjave so predmet Odločbe Komisije 2000/520 z dne 26. julija 2000 po Direktivi Evropskega parlamenta in Sveta 95/46/ES o primernosti zaščite, ki jo zagotavljajo načela zasebnosti varnega pristana in s tem povezana najpogostejše zastavljena vprašanja, ki jih je izdalo Ministrstvo za trgovino ZDA.⁴ Navedena odločba je pravna podlaga za prenos osebnih podatkov Unije podjetjem s sedežem v ZDA, zavezanim načelom varnega pristana.
3. Navedena odločba je danes postavljena pred izziv, saj mora omogočati prenos podatkov med Unijo in ZDA, hkrati pa zagotavljati visoko raven varstva teh podatkov, kot to določa pravo Unije.
4. Pred kratkim je bil namreč v več primerih razkrit obstoj ameriških programov obsežnega zbiranja obveščevalnih podatkov. Ta razkritja so zbudila negotovost glede spoštovanja predpisov prava Unije pri prenosu osebnih podatkov podjetjem v ZDA in glede šibkosti ureditve varnega pristana.

1 — Jezik izvirnika: francoščina.

2 — Sporočilo Komisije Evropskemu parlamentu in Svetu z naslovom „Obnovitev zaupanja v pretok podatkov med EU in ZDA“ (COM(2013) 846 final).

3 — Stran 2.

4 — UL, posebna izdaja v slovenščini, poglavje 16, zvezek 1, str. 119.

5. Sodišče mora v okviru tega predloga za sprejetje predhodne odločbe pojasniti, kakšen pristop naj uporabijo nacionalni nadzorni organi in Komisija, kadar se spopadajo z nepravilnostmi pri izvajanju Odločbe 2000/520.

6. Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov⁵ v poglavju IV določa pravila za prenos osebnih podatkov v tretje države.

7. V tem poglavju navedene direktive člen 25(1) določa načelo, da se lahko prenos osebnih podatkov, ki so v obdelavi ali so namenjeni obdelavi po prenosu, v tretjo državo izvede le, če ta tretja država zagotovi ustrezno raven varstva teh podatkov.

8. Če pa, kot je navedel zakonodajalec Unije v uvodni izjavi 57 navedene direktive, tretja država ne zagotavlja ustrezne ravni varstva, je treba prenos osebnih podatkov v to državo prepovedati.

9. Člen 25(2) Direktive 95/46 določa: „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.“

10. Komisija lahko v skladu s členom 25(6) navedene direktive ugotovi, da tretja država zagotavlja ustrezno raven varstva osebnih podatkov zaradi svoje domače zakonodaje ali mednarodnih obveznosti, ki jih je prevzela. Če Komisija sprejme tako odločitev, je mogoče osebne podatke prenesti v zadevno tretjo državo.

11. Komisija je na podlagi navedene določbe sprejela Odločbo 2000/520. Iz člena 1(1) navedene odločbe izhaja, da se „načela zasebnosti varnega pristana“ za zaščito podatkov“, ki se uporabijo v skladu s smernicami iz „najpogostejše zastavljenih vprašanj“⁶, obravnavajo kot načela, ki zagotavljajo ustrezno raven varstva osebnih podatkov, prenesenih iz Unije podjetjem s sedežem v ZDA.

12. Odločba 2000/520 torej dopušča prenos osebnih podatkov iz držav članic v podjetja s sedežem v ZDA, ki so se zavezala k spoštovanju načel varnega pristana.

13. V Prilogi I k Odločbi 2000/520 so navedena nekatera načela, ki se jim lahko podjetja prostovoljno zavežejo, zanje pa veljajo tudi omejitve in poseben sistem nadzora. Leta 2013 je že več kot 3200 podjetij podpisalo to, kar bi bilo mogoče opredeliti kot „kodeks ravnanja“.

14. Sistem varnega pristana temelji na rešitvi, ki združuje samocertificiranje in samoocenjevanje zasebnih podjetij ter posredovanje javne oblasti.

15. Načela varnega pristana so bila izoblikovana „v posvetovanju s predstavniki industrije [podjetji] in širše javnosti [širšo javnostjo] zaradi lajšanja trgovskih in gospodarskih stikov med Združenimi državami in [...] [U]nijo. Načela so namenjena izključno organizacijam ZDA, ki prejemajo osebne podatke iz [U]nije, da izpolnijo pogoje varnega pristana in iz njega izhajajoče domneve o ‚primernosti [primerni ravni varstva]‘“⁷.

5 — UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355. Direktiva, 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).

6 — Frequently asked questions, v nadaljevanju: FAQ.

7 — Drugi odstavek Priloge I.

16. Načela varnega pristana, navedena v Prilogi I k Odločbi 2000/520, določajo zlasti:

- obveznost obveščanja, v skladu s katero „mora [organizacija] posameznike obvestiti o namenih zbiranja in uporabe njihovih osebnih podatkov, kako se s kakršnimi koli vprašanji in pritožbami obrnejo na organizacijo, kategorije strank, katerim razkrije informacije, ter kakšne možnosti in sredstva za omejevanje uporabe ali razkritja organizacija ponuja posameznikom. To obvestilo [...] mora biti jasno in nedvoumno, ko posameznika prvič prosi za zagotovitev osebnih podatkov ali kakor hitro je izvedljivo za tem, v vsakem primeru pa pred uporabo teh podatkov za namene, ki niso tisti, za katere jih je prvotno zbrala in obdelala pošiljajoča organizacija, ali pred prvim razkritjem tretji stranki“⁸;
- obveznost navedenih organizacij, da posameznikom ponudi[jo] možnost izbire o tem, ali se lahko njihovi osebni podatki razkrijejo tretji osebi ali se bodo uporabili za namen, ki ni združljiv z namenom(-i), za katerega so bili prvotno zbrani ali ga (jih) je posameznik pozneje odobril. Pri občutljivih podatkih „morajo imeti posamezniki možnost izrecne pozitivne izbire (privolitve), kadar je te podatke treba razkriti tretji stranki ali jih uporabiti za namen, ki ni tisti, za katerega so bili prvotno zbrani ali ga je posameznik pozneje odobril s svojo izbiro privolitve“⁹;
- pravila za prenos podatkov tretjemu. „Pri razkrivanju podatkov tretji stranki [osebi] morajo tako organizacije uporabiti načeli obvestila in možnosti izbire“¹⁰;
- glede varnosti podatkov, obveznost za „[o]rganizacije, ki pripravljajo, vzdržujejo, uporabljajo ali razširijo osebne podatke, [da] sprej[mejo] ustrezne preventivne ukrepe, da jih zavarujejo pred izgubo, zlorabo in nepooblaščenim dostopom, razkritjem, spreminjanjem ali uničenjem“¹¹;
- glede neokrnjenosti podatkov, obveznost za organizacije, da „[...] z ustreznimi ukrepi zagotovi[...], da so podatki zanesljivi za nameravano uporabo, točni [pravilni], popolni in trenutni [aktualni]“¹²;
- da imajo osebe, katerih podatke hrani organizacija, načeloma „dostop do [teh] podatkov [...] in možnost, da te podatke popravijo, spremenijo ali izbrišejo, kadar niso točni [pravilni]“¹³;
- obveznost, da določi „mehanizme, ki zagotavljajo skladnost z načeli [varnega pristana], pritožbene mehanizme za posameznike, na katere se podatki nanašajo in jih neizpolnjevanje načel prizadene, in posledice za organizacije, kadar ne spoštujejo načel“¹⁴.

17. Ameriška organizacija, ki se želi zavezati k načelom varnega pristana, se mora v svoji politiki varstva zasebnosti zavezati, da bo objavila, da je zavezana navedenim načelom in da jih dejansko spoštuje, in se mora samocertificirati, tako da pri ministrstvu ZDA za trgovino poda izjavo, da spoštuje navedena načela.¹⁵

8 — Glej Prilogo I, naslov „Obvestilo“.

9 — Glej Prilogo I, naslov „Možnost izbire“.

10 — Glej Prilogo I, naslov „Prenos tretjemu“.

11 — Glej Prilogo I, naslov „Varnost“.

12 — Glej Prilogo I, naslov „Neokrnjenost podatkov“.

13 — Glej Prilogo I, naslov „Dostop“.

14 — Glej Prilogo I, naslov „Izvajanje“.

15 — Člen 1(2) in (3) Odločbe 2000/520. Glej tudi Prilogo II, FAQ 6.

18. Organizacije imajo na voljo več načinov za upoštevanje načel varnega pristana. Tako lahko na primer „pristopi[jo] k samourejevalnemu programu varstva zasebnosti, ki vsebujejo načela [je v skladu s temi načeli] [ali] vključijo načelo varnega pristana tako, da oblikujejo svoje samourejevalne politike varstva zasebnosti, če so v skladu z [navedenimi] načeli. [...] Poleg tega lahko pogoje za ugodnosti varnega pristana izpolnjuje tudi organizacija, ki je podvržena zakonom in drugim predpisom (ali pravilom), ki učinkovito varujejo zasebnost posameznikov“¹⁶.

19. Za preverjanje spoštovanja načel varnega pristana obstaja več mehanizmov, ki združujejo zasebno arbitražo in nadzor javnih organov. Nadzor je tako mogoče zagotoviti s sistemom zunajsodnega reševanja sporov po neodvisni tretji osebi. Poleg tega se lahko podjetja zavežejo k sodelovanju s forumom Unije za varstvo podatkov. Nazadnje, za obravnavo pritožb sta pristojna zvezna komisija za trgovino (Federal Trade Commission, v nadaljevanju: FTC) na podlagi pristojnosti, podeljenih v skladu z oddelkom 5 zakona o zvezni komisiji za trgovino (Federal Trade Commission Act), in ministrstvo za promet (Department of Transportation) na podlagi pristojnosti v skladu z oddelkom 41712 zakonika ZDA (United States Code) iz naslova 49.

20. V skladu s četrtem odstavkom Priloge I k Odločbi 2000/520 je lahko zavezanost načelom varnega pristana omejena, zlasti „če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa [in za spoštovanje zakonov]“ in „z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil“.¹⁷

21. Da bi poleg tega pristojni organi držav članic lahko prekinili prenos podatkov, mora biti izpolnjenih več pogojev iz člena 3(1) Odločbe 2000/520.

22. Obravnavani predlog za sprejetje predhodne odločbe se nanaša na razlago Odločbe 2000/520 glede na člene 7, 8 in 47 Listine Evropske unije o temeljnih pravicah (v nadaljevanju: Listina) ter glede na člena 25(6) in 28 Direktive 95/46. Ta predlog je bil vložen v okviru spora med M. Schremsom in Data Protection Commissioner (komisar za varstvo podatkov; v nadaljevanju: komisar), saj je ta zavrnil preiskavo pritožbe, ki jo je vložil M. Schrems, ker Facebook Ireland Ltd. (v nadaljevanju: Facebook Ireland) hrani osebne podatke svojih uporabnikov na strežnikih v ZDA.

23. M. Schrems je avstrijski državljani in prebiva v Avstriji. Od leta 2008 uporablja družabno omrežje Facebook.

24. Vsi uporabniki Facebooka, ki prebivajo na ozemlju Unije, morajo podpisati pogodbo z družbo Facebook Ireland, ki je hčerinska družba matične družbe Facebook Inc. s sedežem v ZDA (v nadaljevanju: Facebook USA). Podatki uporabnikov Facebook Ireland, ki prebivajo na ozemlju Unije, se v celoti ali delno prenesejo na strežnike družbe Facebook USA, ki so na ozemlju ZDA in kjer se hranijo.

25. M. Schrems je 25. junija 2013 pri komisarju vložil pritožbo, pri čemer je v bistvu trdil, da v ameriški zakonodaji in praksi ni nobene dejanske zaščite podatkov, ki se hranijo na ozemlju ZDA, pred državnim nadzorom. To naj bi izhajalo iz razkritij, ki jih je Edward Snowden od maja 2013 posredoval v zvezi z dejavnostmi ameriških obveščevalnih služb, zlasti ameriške Agencije za nacionalno varnost (National Security Agency; v nadaljevanju: NSA).

¹⁶ — Tretji odstavek Priloge I.

¹⁷ — Glej tudi Prilogo IV, točka B.

26. Iz teh razkritij naj bi bilo zlasti razvidno, da je NSA vzpostavil program PRISM, v okviru katerega naj bi navedena agencija dobila prost dostop do množice podatkov, shranjenih na strežnikih v ZDA, ki so v lasti ali pod nadzorom številnih družb, dejavnih na področju interneta in tehnologije, kakršna je družba Facebook USA.

27. Komisar je menil, da mu ni bilo treba preiskati pritožbe, ker naj ne bi imela pravne podlage. Menil je, da ni dokazov, da je NSA dostopala do podatkov M. Schremsa. Poleg tega bi bilo treba pritožbo po njegovih navedbah zavreči na podlagi Odločbe 2000/520, s katero naj bi Komisija ugotovila, da ZDA v okviru ureditve varnega pristana zagotavljajo ustrezno raven varstva prenesenih osebnih podatkov. O vsakem vprašanju glede ustreznosti varstva teh podatkov v ZDA naj bi bilo treba odločiti v skladu z navedeno odločbo, ki naj bi mu preprečevala preučitev vprašanja, navedenega v pritožbi.

28. Komisar je pritožbo zavrgel na podlagi spodaj navedene nacionalne zakonodaje.

29. Člen 10(1) zakona o varstvu podatkov iz leta 1988 (Data Protection (Amendment) Act 1988), kakor je bil spremenjen z zakonom o varstvu podatkov iz leta 2003 (Data Protection Act 2003, v nadaljevanju: zakon o varstvu podatkov), mu daje pristojnost za preučitev pritožb in določa:

- „(a) Komisar lahko preuči ali odredi preučitev, ali so bile, so ali so lahko določbe tega zakona kršene v zvezi z določeno osebo, če ta oseba pri njem vloži pritožbo zaradi kršitve katere koli od teh določb, ali če komisar meni, da bi lahko taka kršitev obstajala.
- (b) Če oseba vloži pritožbo pri komisarju na podlagi točke (a) tega odstavka, komisar:
 - (i) preišče ali odredi preiskavo pritožbe, razen če ugotovi, da je neresna ali vložena iz nagajivosti, in
 - (ii) če v razumnem roku med zadevnimi strankami ne more doseči mirne rešitve spora glede predmeta pritožbe, pritožnika pisno obvesti o odločitvi v zvezi s pritožbo in navede, da lahko, če ta odločitev posega v njegov položaj, na podlagi člena 26 tega zakona v 21 dneh od vročitve zoper njo vloži pravno sredstvo.“

30. Komisar je v obravnavanem primeru ugotovil, da je bila pritožba M. Schremsa „neresna ali vložena iz nagajivosti“, ker naj bi bilo že takoj jasno, da ji zaradi neobstoja pravne podlage ne bo mogoče ugoditi. Zato je preučitev navedene pritožbe zavrnil.

31. Člen 11 zakona o varstvu podatkov ureja prenos osebnih podatkov zunaj nacionalnega ozemlja. Njegov člen 11(2)(a) določa:

„Kadar se pri katerem koli postopku, ki ga ureja ta zakon, pojavi vprašanje:

- (i) v zvezi z ugotovitvijo, ali je v državi ali na ozemlju zunaj Evropskega gospodarskega prostora [(EGP)], kamor bodo preneseni osebni podatki, zagotovljena ustrezna raven varstva, opredeljena v odstavku 1 tega člena, in
- (ii) ali je Unija sprejela ugotovitev glede zadevnih vrst prenosov,

se o vprašanju odloči v skladu s to ugotovitvijo.“

32. V členu 11(2)(b) zakona o varstvu podatkov je opredeljen pojem ugotovitve Unije:

„V točki (a) tega odstavka ‚ugotovitev Unije‘ pomeni ugotovitev, ki jo je Komisija [...] sprejela v skladu z odstavkoma 4 ali 6 člena 25 Direktive [95/46] v okviru postopka iz [njenega] člena 31(2), da bi določila, ali je v državi ali na ozemlju zunaj [EGS] zagotovljena ustrezna raven varstva, opredeljena v odstavku 1 tega člena.“

33. Komisar je navedel, da je bila Odločba 2000/520 „ugotovitev Unije“ v smislu člena 11(2)(a) zakona o varstvu podatkov, zato naj bi bilo treba na podlagi tega zakona o vsakem vprašanju glede ustreznosti varstva podatkov v tretji državi, v katero so ti preneseni, odločiti v skladu z navedeno ugotovitvijo. Komisar je v delu, ki je zadeval bistveni del pritožbe M. Schremsa – to je okoliščino, da so bili podatki preneseni v tretjo državo, ki naj v praksi ne bi zagotavljala ustrezne ravni varstva – menil, da zaradi narave in samega obstoja Odločbe 2000/520 ni mogel preučiti navedenega vprašanja.

34. M. Schrems je pri High Court of Justice vložil tožbo zoper odločbo komisarja, da zavrže njegovo pritožbo. Potem ko je navedeno sodišče preučilo dokaze, predložene v postopku v glavni stvari, je ugotovilo, da se elektronski nadzor in prestrežanje osebnih podatkov uporabljata v obveznih in nujnih primerih, ki so v javnem interesu, in sicer za zagotavljanje nacionalne varnosti in preprečevanje hudih kaznivih dejanj. High Court of Justice v zvezi s tem navaja, da sta nadzor in prestrežanje osebnih podatkov, ki so preneseni iz Unije v ZDA, namenjena legitimnim protiterorističnim ciljem.

35. Vendar so po navedbah istega sodišča razkritja E. Snowdena pokazala, da so NSA in drugi podobni organi znatno presegle pooblastila. Čeprav naj bi v ZDA obstajal nadzor, ki naj bi ga na podlagi zakona o nadzoru tujih obveščevalnih služb iz leta 1978 (Foreign Intelligence Surveillance Act of 1978) izvajalo Foreign Intelligence Services Court (sodišče za nadzor tujih obveščevalnih podatkov, v nadaljevanju: FISC)¹⁸, naj bi ta potekal tajno in ne bi bil kontradiktoren. Po njegovih navedbah državljani Unije poleg tega nimajo dejanske pravice do izjave o vprašanju nadzora in prestrežanja podatkov, pa tudi odločanje o dostopu do takih podatkov naj bi potekalo na podlagi ameriške zakonodaje.

36. Iz obsežnih dokazil, ki so bila priložena k pisnim izjavam pod prisego, danim v postopku v glavni stvari, naj bi bilo jasno razvidno, da pravilnost številnih Snowdenovih razkritij očitno ni sporna. High Court of Justice je zato ugotovilo, da lahko NSA in druge ameriške agencije za varnost, kakršna je Federal Bureau of Investigation (zvezni preiskovalni urad, FBI), pri množičnem in vsesplošnem nadzoru in prestrežanju takih podatkov dostopajo do osebnih podatkov po njihovem prenosu v ZDA.

37. High Court of Justice ugotavlja, da sta v irskem pravu ustavni pravici do zasebnega življenja in nedotakljivosti stanovanja tako pomembni, da mora biti vsako poseganje skladno z zakonsko določenimi zahtevami in sorazmerno. Množičen in vsesplošen dostop do osebnih podatkov naj nikakor ne bi bil skladen z zahtevo po sorazmernosti, zato naj bi bilo zanj treba šteti, da nasprotuje irski ustavi.¹⁹

38. High Court of Justice poudarja, da je mogoče prestrežanje elektronskih komunikacij šteti za ustavno, če se dokaže, da je posamezno prestrežanje komunikacij in nadzor nekaterih posameznikov ali skupin posameznikov objektivno utemeljeno z interesom zatiranja kriminala in nacionalne varnosti ter da so pri vsakem takem prestrežanju vzpostavljena ustrezna in preverljiva jamstva.

18 — Glej oddelek 702 navedenega zakona, kakor je bil spremenjen z zakonom iz leta 2008 (Foreign Intelligence Surveillance Act of 2008). NSA ima na podlagi tega oddelka podatkovno zbirko, znano pod imenom „PRISM“ (glej Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection z dne 27. novembra 2013).

19 — High Court of Justice se sklicuje zlasti na spoštovanje človekovega dostojanstva in svobode posameznika (preambula), osebne avtonomije (člen 40(3), točki 1 in 2), nedotakljivosti stanovanja (člen 40(5)) in spoštovanje družinskega življenja (člen 41).

39. High Court of Justice zato navaja, da bi se, če bi za obravnavano zadevo v celoti veljalo irsko pravo, odprlo precej pomembno vprašanje, ali ZDA „zagotavljajo ustrezno raven varstva zasebnega življenja ter temeljnih pravic in svoboščin“ v smislu člena 11(1) zakona o varstvu podatkov. Komisar naj torej na podlagi irskega prava, zlasti njegovih ustavnih zahtev, ne bi smel zavreči pritožbe M. Schremsa, temveč bi moral navedeno vprašanje preučiti.

40. Vendar High Court of Justice ugotavlja, da se zadeva, o kateri odloča, nanaša na izvajanje prava Unije v smislu člena 51(1) Listine, zato naj bi bilo treba zakonitost komisarjeve odločitve presojati glede na pravo Unije.

41. High Court of Justice težavo, na katero je naletel komisar, pojasnjuje tako. Komisar naj bi moral na podlagi člena 11(2)(a) zakona o varstvu podatkov o vprašanju ustreznosti varstva v tretji državi odločiti „v skladu“ z ugotovitvijo Unije, ki naj bi jo Komisija sprejela v skladu s členom 25(6) Direktive 95/46. Zato naj komisar ne bi mogel prezreti navedene ugotovitve. Ker naj bi Komisija v Odločbi 2000/520 ugotovila, da ZDA zagotavljajo ustrezno raven varstva pri obdelavi podatkov družb, zavezanih načelom varnega pristana, naj bi moral komisar pritožbo, s katero se izpodbija ustreznost navedenega varstva, nujno zavreči.

42. Čeprav High Court of Justice ugotavlja, da je komisar s tem izkazal zvesto dobesedno upoštevanje Direktive 95/46 in Odločbe 2000/520, navaja, da M. Schrems v resnici ugovarja določbam ureditve varnega pristana samega in ne toliko načinu, kako ga je komisar uporabil, hkrati pa poudarja, da ni neposredno izpodbijal veljavnosti Direktive 95/46 niti veljavnosti Odločbe 2000/520.

43. Po navedbah High Court of Justice je torej bistveno vprašanje, ali komisarja v skladu s pravom Unije in zlasti ob upoštevanju poznejšega začetka veljavnosti členov 7 in 8 Listine v celoti zavezuje ugotovitev Komisije, kot je navedena v Odločbi 2000/520 v zvezi z ustreznostjo varstva podatkov v zakonodaji in praksi v ZDA.

44. High Court of Justice poleg tega pojasnjuje, da v tožbi, o kateri odloča, ni bil naveden noben očitek zoper samo delovanje družb Facebook Ireland in Facebook USA. Člen 3(1)(b) Odločbe 2000/520, na podlagi katerega lahko nacionalni pristojni organi podjetju odredijo prekinitev prenosa podatkov v tretjo državo, pa se po navedbah tega sodišča uporablja samo, kadar je pritožba vložena zoper ravnanje zadevnega podjetja, kar naj ne bi veljalo v obravnavanem primeru.

45. High Court of Justice zato poudarja, da se ugovor dejansko ne nanaša na samo ravnanje družbe Facebook USA, temveč bolj na mnenje Komisije, da zakonodaja in praksa na področju varstva podatkov v ZDA zagotavljata ustrezno varstvo, čeprav naj bi bilo iz razkritij E. Snowdena jasno razvidno, da lahko ameriški organi množično in nerazlikovalno dostopajo do osebnih podatkov prebivalcev na ozemlju Unije.²⁰

46. High Court of Justice v zvezi s tem meni, da je težko razumeti, kako bi lahko Odločba 2000/520 v praksi zadostila zahtevam iz členov 7 in 8 Listine, zlasti ob upoštevanju načel, ki naj bi jih Sodišče navedlo v sodbi Digital Rights Ireland in drugi.²¹ Poseglo naj bi se zlasti v jamstvo, zagotovljeno na podlagi člena 7 Listine in temeljih vrednot, ki naj bi bile skupne tradicijam držav članic, če bi lahko javni organi naključno in vsesplošno dostopali do elektronskih komunikacij brez potrebe po objektivni utemeljitvi iz razlogov v zvezi z državno varnostjo ali preprečevanjem kaznivih dejanj, ki se nanaša konkretno na zadevne posameznike, in brez ustreznih in preverljivih jamstev. Ker naj bi bila iz tožbe

20 — High Court of Justice v zvezi s tem navaja, da je glavni tožbeni razlog, ki ga je pred njim navedel M. Schrems, ta, da komisar glede na nedavna razkritja E. Snowdena in obsežno dajanje zasebnih podatkov na voljo ameriškim obveščevalnim službam ni mogel pravilno ugotoviti, da je v tej tretji državi vzpostavljena ustrezna raven varstva navedenih podatkov.

21 — C-293/12 in C-594/12, EU:C:2014:238, točke od 65 do 69.

M. Schremsa razvidna domneva, da bi lahko bila Odločba 2000/520 abstraktno nezdružljiva s členoma 7 in 8 Listine, naj bi lahko Sodišče razsodilo, da je mogoče Direktivo 95/46, zlasti njen člen 25(6), in Odločbo 2000/520 razlagati tako, da nacionalni organi lahko opravijo lastne preiskave in ugotovijo, ali prenos osebnih podatkov v tretjo državo tam izpolnjuje zahteve iz členov 7 in 8 Listine.

47. V teh okoliščinah je High Court of Justice prekinilo odločanje in Sodišču v predhodno odločanje predložilo ti vprašanji za predhodno odločanje:

„Ali je komisar pri odločanju o pritožbi, da se osebni podatki prenašajo v tretjo državo (v tem primeru Združene države Amerike), katere zakonodaja in praksa domnevno ne vsebujeta ustreznega varstva za subjekte podatkov, absolutno zavezan upoštevati nasprotno ugotovitev Skupnosti [Unije] iz Odločbe 2000/520, ob upoštevanju členov 7, 8 in 47 Listine, ne glede na določbe člena 25(6) Direktive 95/46?

Ali pa lahko komisar opravi in/ali mora opraviti lastno preiskavo zadeve glede na dejanski razvoj dogodkov v času od prvotne objave Odločbe 2000/520?“

II – Analiza

48. Sodišče mora na podlagi vprašanj, ki ju je navedlo High Court of Justice, pojasniti pooblastila, ki jih imajo nacionalni nadzorni organi, kadar odločajo o pritožbi v zvezi s prenosom osebnih podatkov podjetju s sedežem v tretji državi in če je navedena pritožba podprta s trditvijo, da ta tretja država ne zagotavlja ustreznih ravni varstva prenesenih podatkov, čeprav je Komisija na podlagi člena 25(6) Direktive 95/46 sprejela odločbo, s katero je ugotovila, da navedena tretja država zagotavlja ustrezno raven varstva.

49. Ugotavljam, da ima pritožba, ki jo je M. Schrems vložil pri komisarju, dva vidika. Njen namen je izpodbijati prenos osebnih podatkov prek družbe Facebook Ireland družbi Facebook USA. M. Schrems predlaga, naj se ta prenos preneha, ker naj ZDA ne bi zagotavljale ustreznih ravni varstva osebnih podatkov, ki so preneseni v okviru ureditve varnega pristana. Natančneje, navedeni tretji državi očita, da je vzpostavila program PRISM, ki naj bi NSA omogočal prost dostop do množice podatkov, shranjenih na strežnikih v ZDA. Pritožba se tako posebej nanaša na prenose osebnih podatkov prek družbe Facebook Ireland družbi Facebook USA, hkrati pa se z njo splošneje izpodbija raven varstva teh podatkov v okviru ureditve varnega pristana.

50. Komisar je menil, da že zaradi samega obstoja odločbe Komisije, s katero naj bi ta priznala, da ZDA v okviru ureditve varnega pristana zagotavljajo ustrezno raven varstva, ne more preiskati pritožbe.

51. Skupaj je torej treba preučiti navedeni vprašanji, ki se v bistvu nanašata na to, ali je treba člen 28 Direktive 95/46 v povezavi s členoma 7 in 8 Listine razlagati tako, da obstoj odločbe, ki jo je sprejela Komisija na podlagi člena 25(6) navedene direktive, učinkuje tako, da nacionalnemu nadzornemu organu preprečuje, da preišče pritožbo, s katero se očita, da tretja država ne zagotavlja ustreznih ravni varstva prenesenih osebnih podatkov, in po potrebi prekine prenos teh podatkov.

52. Člen 7 Listine zagotavlja pravico do spoštovanja zasebnega življenja, njen člen 8 pa izrecno določa pravico do varstva osebnih podatkov. V odstavkih 2 in 3 člena 8 je pojasnjeno, da je treba te podatke obdelovati pošteno, za določene namene in na podlagi privolitve zadevne osebe ali na drugi legitimni podlagi, določeni z zakonom, da ima vsakdo pravico dostopa do podatkov, zbranih o njem, in pravico zahtevati, da se ti podatki popravijo, ter da spoštovanje teh pravil nadzira neodvisen organ.

A – Pooblastila nacionalnih nadzornih organov v primeru odločbe Komisije o ustreznosti

53. Kot navaja M. Schrems v stališčih v zvezi z zadevno pritožbo iz postopka v glavni stvari, je osrednje vprašanje prenos osebnih podatkov prek družbe Facebook Ireland družbi Facebook USA ob upoštevanju splošnega dostopa NSA in drugih ameriških varnostnih agencij do podatkov, ki jih shranjuje družba Facebook USA, na podlagi pooblastil, ki jim jih podeljuje ameriška zakonodaja.

54. Nacionalni nadzorni organ, pri katerem je bila vložena pritožba zaradi izpodbijanja ugotovitve, da tretja država zagotavlja ustrezno raven varstva prenesenih podatkov, ima po navedbah M. Schremsa, če ima na voljo dokaze za utemeljenost navedb v navedeni pritožbi, pooblastilo, da odredi prekinitev prenosa podatkov, ki ga je izvedlo podjetje, na katero se nanaša navedena pritožba.

55. M. Schrems meni, da mora komisar glede na obveznost, da varuje njegove temeljne pravice, ne le preučiti pritožbo, temveč – če se pritožbi ugoti – uporabiti tudi svoje pooblastilo za prekinitev prenosa podatkov med družbama Facebook Ireland in Facebook USA.

56. Vendar je komisar pritožbo zavrgel na podlagi zakonskih določb o varstvu podatkov, v katerih so našteje njegove pristojnosti. Ta ugotovitev naj bi temeljila na stališču komisarja, da ga je zavezovala Odločba 2000/520.

57. Glede na navedeno je v obravnavanem primeru osrednje vprašanje, ali presoja Komisije glede ustreznosti varstva iz Odločbe 2000/520 v celoti zavezuje nacionalni organ za varstvo podatkov in mu preprečuje preiskavo trditev, s katerimi se ta ugotovitev izpodbija. Vprašnji za predhodno odločanje se torej nanašata na obseg preiskovalnih pooblastil nacionalnih organov za varstvo podatkov v primeru odločbe Komisije o ustreznosti.

58. Po navedbah Komisije je pomembno upoštevati povezavo med njenimi pooblastili in pooblastili nacionalnih organov za varstvo podatkov. Navedeni organi naj bi bili pristojni zlasti za uporabo zakonodaje na tem področju v posamičnih primerih, za splošen ponoven pregled izvajanja Odločbe 2000/520, vključno z vsemi odločbami o začasnem zadržanju njenega izvajanja ali njeni razveljavitvi, pa naj bi bila pristojna Komisija.

59. Komisija navaja, da M. Schrems ni navedel posebnih utemeljitev, iz katerih bi bilo razvidno, da zanj zaradi prenosa podatkov med družbama Facebook Ireland in Facebook USA obstaja neposredna nevarnost za nastanek velike škode. Nasprotno, zaradi abstraktnosti in splošnosti naj bi bili pomisleki M. Schremsa v zvezi z nadzornimi programi, ki jih izvajajo ameriške varnostne agencije, enaki tistim, ki so Komisijo pripeljali do ponovnega pregleda Odločbe 2000/520.

60. Nacionalni nadzorni organi bi po navedbah Komisije posegali v njene pristojnosti za ponovno pogajanje o pogojih iz navedene odločbe z ZDA ali po potrebi za začasno zadržanje njenega izvajanja, če bi sprejeli ukrepe na podlagi pritožb, v katerih so navedeni samo strukturni in abstraktni pomisleki.

61. Z mnenjem Komisije se ne strinjam. Menim, da z obstojem odločbe, ki jo je Komisija sprejela na podlagi člena 25(6) Direktive 95/46, ni mogoče izničiti niti zmanjšati obsega pooblastil, ki jih imajo nacionalni nadzorni organi na podlagi člena 28 navedene direktive. Če se pri nacionalnih nadzornih organih vložijo posamične pritožbe, jim to po mojem mnenju in v nasprotju z navedbami Komisije ne preprečuje, da si na podlagi preiskovalnih pooblastil in neodvisnosti izoblikujejo mnenje glede splošne varnosti, ki jo zagotavlja tretja država, in iz tega pri odločanju o posamičnem primeru izpeljejo posledice.

62. Iz ustaljene sodne prakse Sodišča izhaja, da je treba pri razlagi določb prava Unije upoštevati ne le njihovo besedilo, ampak tudi sobesedilo in cilje, ki jih uresničuje ureditev, katere del so.²²

63. Iz uvodne izjave 62 Direktive 95/46 izhaja, da „je v državah članicah ustanovitev nadzornih organov, ki opravljajo svoje naloge popolnoma samostojno, bistvena sestavina varstva posameznikov pri obdelavi osebnih podatkov“.

64. V skladu s členom 28(1), prvi pododstavek, navedene direktive „[v]saka država članica določi, da je eden ali več javnih organov na njenem ozemlju odgovornih za spremljanje uporabe predpisov, ki so jih sprejele države članice v skladu s to direktivo“. Člen 28(1), drugi pododstavek, navedene direktive določa, da „[t]i organi pri izvajanju nalog, ki so jim zaupane, delujejo popolnoma samostojno“.

65. V členu 28(3) Direktive 95/46 so naštetá pooblastila vsakega nadzornega organa, in sicer preiskovalna pooblastila, dejanska pooblastila za posredovanje, ki mu omogočajo naložitev začasne ali dokončne prepovedi obdelave, in pooblastila za sodelovanje v sodnih postopkih, kadar so kršene nacionalne določbe, sprejete v skladu z navedeno direktivo, ali za seznanitev sodnih organov s temi kršitvami.

66. Poleg tega v skladu s členom 28(4), prvi pododstavek, Direktive 95/46, „[v]sak nadzorni organ obravnava zahteve, ki jih je vložila katera koli oseba [...] v zvezi z varstvom svojih pravic in svoboščin glede obdelave osebnih podatkov.“ Člen 28(4), drugi pododstavek, navedene direktive določa, da „[v]sak nadzorni organ obravnava predvsem zahteve za preverjanje zakonitosti obdelave podatkov, ki jih vloži katera koli oseba, kadar se uporabljajo nacionalne določbe, sprejete v skladu s členom 13 navedene direktive.“ Naj še navedem, da lahko države članice v skladu s to zadnjo določbo sprejmejo zakonodajne ukrepe za omejitev obsega več obveznosti in pravic, določenih v Direktivi 95/46, kadar je taka omejitev potreben ukrep za zaščito med drugim državne varnosti, obrambe, javne varnosti ter preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj.

67. Kot je že poudarilo Sodišče, zahteva po nadzoru neodvisnega organa nad spoštovanjem prava Unije o varstvu posameznikov pri obdelavi osebnih podatkov izhaja tudi iz primarnega prava Unije, zlasti iz člena 8(3) Listine Evropske unije o temeljnih pravicah in člena 16(2) PDEU.²³ Opozorilo je tudi, da „je v državah članicah ustanovitev neodvisnih nadzornih organov bistveni element spoštovanja varstva oseb pri obdelavi osebnih podatkov“²⁴.

68. Sodišče je poleg tega razsodilo, da „je treba člen 28(1), drugi pododstavek, Direktive 95/46 razlagati tako, da morajo biti nadzorni organi, pristojni za spremljanje obdelave osebnih podatkov, samostojni, tako da lahko svoje naloge izvajajo brez zunanjega vpliva. Ta samostojnost izključuje zlasti vsakršno navodilo in kakršenkoli drug zunanji vpliv, bodisi neposreden bodisi posreden, ki bi lahko usmerjal odločitve teh nadzornih organov in tako ogrožal njihovo opravljanje naloge ohranjanja pravega ravnotežja med pravnim varstvom zasebnosti in prostim pretokom osebnih podatkov“²⁵.

69. Sodišče je poleg tega navedlo: „Cilj zagotavljanja samostojnosti nacionalnih nadzornih organov je učinkovit in zanesljiv nadzor spoštovanja določb na področju varstva fizičnih oseb pri obdelavi osebnih podatkov“²⁶. Navedeno zagotavljanje samostojnosti je bilo uvedeno „za krepitev varstva oseb in organov, na katere se [...] nanašajo odločbe [teh nacionalnih nadzornih organov]“²⁷.

22 — Glej zlasti sodbo Koushaki (C-84/12, EU:C:2013:862, točka 34 in navedena sodna praksa).

23 — Glej sodbi Komisija/Avstrija (C-614/10, EU:C:2012:631, točka 36) in Komisija/Madžarska (C-288/12, EU:C:2014:237, točka 47).

24 — Glej zlasti sodbo Komisija/Madžarska (C-288/12, EU:C:2014:237, točka 48 in navedena sodna praksa). V tem smislu glej tudi sodbo Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238, točka 68 in navedena sodna praksa).

25 — Glej zlasti sodbo Komisija/Madžarska (C-288/12, EU:C:2014:237, točka 51 in navedena sodna praksa).

26 — Sodba Komisija/Nemčija (C-518/07, EU:C:2010:125, točka 25).

27 — *Idem*.

70. Kot izhaja zlasti iz uvodne izjave 10 in člena 1 Direktive 95/46, je njen cilj v Uniji zagotoviti „visoko raven varstva temeljnih svoboščin in pravic pri obdelavi osebnih podatkov“²⁸. Po navedbah Sodišča so „[n]adzorni organi, določeni v členu 28 Direktive 95/46, [...] torej varuhi teh temeljnih pravic in svoboščin“.²⁹

71. Zaradi pomembne vloge nacionalnih nadzornih organov na področju varstva posameznikov pri obdelavi osebnih podatkov morajo njihova pooblastila za ukrepanje ostati neokrnjena, tudi če je Komisija sprejela odločbo na podlagi člena 25(6) Direktive 95/46.

72. V zvezi s tem naj pripomnim, da nič ne kaže, da bi bile ureditve prenosa osebnih podatkov v tretje države izključene s stvarnega področja uporabe člena 8(3) Listine, v katerem ima na hierarhični lestvici predpisov prava Unije najvišje mesto pomembnost nadzora, ki ga izvaja neodvisni organ v zvezi s spoštovanjem pravil o varstvu osebnih podatkov.

73. Če bi odločbe, ki jih je sprejela Komisija, v celoti zavezovale nacionalne nadzorne organe, bi to neizogibno omejevalo njihovo popolno neodvisnost. Nacionalni nadzorni organi morajo imeti v skladu z vlogo varuhov temeljnih pravic možnost, da povsem neodvisno preiščejo pri njih vložene pritožbe v višjem interesu varstva posameznikov pri obdelavi osebnih podatkov.

74. Poleg tega, kot sta upravičeno poudarila Evropski parlament in belgijska vlada na obravnavi, ni nobene hierarhične povezave med poglavjem IV Direktive 95/46 o prenosu osebnih podatkov v tretje države in njenim poglavjem VI, v katerem je opredeljena zlasti vloga nacionalnih nadzornih organov. Nič v navedenem poglavju VI ne kaže na to, da bi bile določbe o nacionalnih nadzornih organih kakor koli podrejene ločenim določbam o prenosih iz poglavja IV Direktive 95/46.

75. Nasprotno, iz člena 25(1) v poglavju IV navedene direktive je izrecno razvidno, da se prenos osebnih podatkov v tretjo državo, ki zagotavlja ustrezno raven varstva, lahko izvede le, če se upoštevajo zakoni držav članic, s katerimi se izvajajo druge določbe navedene direktive.

76. V zvezi s tem naj opozorim, da morajo države članice v skladu z navedeno določbo v nacionalni zakonodaji določiti, da se lahko prenos osebnih podatkov, ki so v obdelavi ali so namenjeni obdelavi po dovoljenem prenosu, v tretjo državo izvede le, če ta tretja država ob upoštevanju nacionalnih določb, sprejetih na podlagi drugih določb Direktive 95/46, zagotovi ustrezno raven varstva teh podatkov.

77. V skladu s členom 28(1) te direktive so nacionalni nadzorni organi na ozemlju vsake države članice odgovorni za spremljanje uporabe predpisov, ki so jih sprejele države članice v skladu s to direktivo.

78. Če primerjamo navedeni določbi, lahko ugotovimo, da je pravilo iz člena 25(1) Direktive 95/46, v skladu s katerim se lahko osebni podatki prenesejo le, če tretja država prejemnica zagotovi ustrezno raven njihovega varstva, med pravili, katerih uporabo morajo nadzirati nacionalni nadzorni organi.

79. V skladu s členom 8(3) Listine je treba široko razlagati pooblastila nacionalnih nadzornih organov, da povsem neodvisno preiskujejo pri njih v skladu s členom 28 Direktive 95/46 vložene pritožbe. Navedenih pooblastil torej pri ugotavljanju, ali je raven varstva v tretji državi ustrezna, ni mogoče omejiti s pooblastili, ki jih je zakonodajalec Unije v skladu s členom 25(6) navedene direktive podelil Komisiji.

28 — *Ibidem* (točka 22 in navedena sodna praksa).

29 — *Ibidem* (točka 23). Glej v tem smislu tudi sodbi Komisija/Avstrija (C-614/10, EU:C:2012:631, točka 52) in Komisija/Madžarska (C-288/12, EU:C:2014:237, točka 53).

80. Nacionalni nadzorni organi morajo zaradi svoje bistvene vloge pri varstvu osebnih podatkov imeti možnost preiskave, kadar je pri njih vložena pritožba, v kateri so navedeni dokazi, s katerimi bi bilo mogoče izpodbijati raven varstva v tretji državi, tudi če je Komisija v odločbi, sprejeti na podlagi člena 25(6) Direktive 95/46, ugotovila, da zadevna tretja država zagotavlja ustrezno raven varstva.

81. Če nacionalni nadzorni organ na koncu svojih preiskav meni, da sporni prenos podatkov posega v varstvo, ki ga je treba zagotoviti državljanom Unije pri obdelavi njihovih podatkov, ima pooblastilo, da prekine prenos zadevnih podatkov, in to ne glede na splošno presojo Komisije v njeni odločbi.

82. V skladu s členom 25(2) Direktive 95/46 namreč ni sporno, da se ustreznost ravni varstva, ki jo zagotavlja tretja država, presodi glede na vse dejanske in pravne okoliščine. Če se katera od okoliščin spremeni in se zdi, da postavlja pod vprašaj ustreznost ravni varstva v tretji državi, mora nacionalni nadzorni organ, pri katerem je vložena pritožba, imeti možnost, da lahko iz tega izpelje posledice v zvezi s spornim prenosom.

83. Kot je poudarila Irska, Odločba 2000/520 zavezuje komisarja in druge državne organe. Iz člena 288, četrti odstavek, PDEU namreč izhaja, da je odločba, ki jo je sprejela institucija Unije, v celoti zavezujoča. Zato Odločba 2000/520 velja za države članice, na katere je naslovljena.

84. Naj v zvezi s tem poudarim, da člen 5 same Odločbe 2000/520 določa, da „[d]ržave članice sprejmejo vse potrebne ukrepe za uskladitev [z njo] najpozneje v 90 dneh od datuma uradnega obvestila o odločbi državam članicam.“ Člen 6 navedene odločbe poleg tega potrjuje, da je „[t]a [...] naslovljena na države članice“.

85. Vseeno menim, da glede na zgoraj navedene določbe Direktive 95/46 in Listine zavezujoč učinek Odločbe 2000/520 ne izključuje kakršne koli preiskave komisarja v zvezi s pritožbami, v katerih se očita, da prenosi osebnih podatkov v ZDA v okviru navedene odločbe ne zagotavljajo potrebnih jamstev, zahtevanih s pravom Unije. Z drugimi besedami, tak zavezujoč učinek ne pomeni, da je treba vsako tako pritožbo takoj in brez preučitve njene utemeljenosti preprosto zavreči.

86. Naj dodam, da poleg tega iz sistematike člena 25 Direktive 95/46 izhaja, da lahko to, ali tretja država zagotavlja ustrezno raven varstva ali ne, ugotovijo države članice ali Komisija. Gre torej za deljeno pristojnost.

87. Iz člena 25(6) navedene direktive izhaja, da morajo države članice sprejeti ukrepe, ki so potrebni za uskladitev z odločitvijo Komisije, če ta ugotovi, da tretja država zagotavlja ustrezno raven varstva v smislu člena 25(2).

88. Ker navedena odločitev učinkuje tako, da se omogoči prenos osebnih podatkov v tretjo državo, za katero Komisija meni, da zagotavlja ustrezno raven varstva, morajo torej države članice načeloma omogočiti, da podjetja s sedežem na njihovem ozemlju tak prenos izvedejo.

89. Vendar Komisija na podlagi člena 25 Direktive 95/46 nima izključne pristojnosti za ugotavljanje, ali je raven varstva prenesenih osebnih podatkov ustrezna ali ne. Iz sistematike navedenega člena je razvidno, da imajo pri tem vlogo tudi države članice. Odločitev Komisije ima seveda pomembno vlogo pri poenotenju pogojev za prenos, veljavnih v državah članicah. Vendar je to poenotenje mogoče le, dokler se navedene ugotovitve ne izpodbija.

90. Utemeljitev, da je treba pogoje za prenos osebnih podatkov v tretjo državo poenotiti, je po mojem mnenju omejena v položaju, kakršen je obravnavani v postopku v glavni stvari in v katerem Komisija ni le obveščena o očitkih zoper njeno ugotovitev, temveč tudi ona sama navaja take očitke in vodi pogajanja, da bi navedeni položaj popravila.

91. Pri presoji ustreznosti ali neustreznosti ravni varstva v tretji državi lahko države članice in Komisija tudi sodelujejo. Člen 25(3) Direktive 95/46 v zvezi s tem določa, da „[se] [d]ržave članice in Komisija [...] medsebojno obveščajo o primerih, za katere menijo, da tretja država ne zagotavlja ustrezne ravni varstva v smislu odstavka 2.“ Kot ugotavlja Parlament, to jasno kaže, da imajo države članice in Komisija enakovredno vlogo pri odkrivanju primerov, v katerih tretja država ne zagotavlja ustrezne ravni varstva.

92. Cilj odločbe o ustreznosti je dovoliti prenos osebnih podatkov v zadevno tretjo državo. To ne pomeni, da državljani Unije pri nadzornih organih ne morejo več vložiti pravnega sredstva za varstvo osebnih podatkov. Naj v zvezi s tem opozorim, da člen 28(4), prvi pododstavek, Direktive 95/46, v skladu s katerim „[lahko] [v]sak nadzorni organ obravnava zahteve, ki jih je vložila katera koli oseba [...] v zvezi z varstvom svojih pravic in svoboščin glede obdelave osebnih podatkov“, ne določa izjeme od navedenega načela, če je Komisija sprejela odločbo v skladu s členom 25(6) navedene direktive.

93. Čeprav torej odločba, ki jo je sprejela Komisija na podlagi izvedbenih pooblastil, podeljenih s to zadnjo določbo, učinkuje tako, da omogoči prenos osebnih podatkov v tretjo državo, pa taka odločba ne more učinkovati tako, da državam članicam, zlasti njenim nacionalnim nadzornim organom, odvzame vsakršno pooblastilo ali da jih samo omeji, če se pred njimi očita, da so bile kršene temeljne pravice.

94. Nacionalni nadzorni organ mora imeti možnost za izvajanje pooblastil iz člena 28(3) Direktive 95/46, med katerimi je ta, da začasno ali dokončno prepove obdelavo osebnih podatkov. Čeprav med naštetimi pooblastili iz navedene določbe niso izrecno določena pooblastila v zvezi s prenosom iz države članice v tretjo državo, je treba tak prenos po mojem mnenju obravnavati kot obdelavo podatkov.³⁰ Kot je poleg tega razvidno iz besedila navedene določbe, seznam naštetih pooblastil ni izčrpen. Vsekakor morajo nacionalni nadzorni organi glede na svojo bistveno vlogo v sistemu, vzpostavljenem z Direktivo 95/46, imeti možnost, da prekinejo prenos podatkov ob morebitnem dokazanem poseganju ali nevarnosti poseganja v temeljne pravice.

95. Naj dodam, da bi bilo odvzete preiskovalnih pooblastil nacionalnemu nadzornemu organu v okoliščinah obravnavane zadeve ne le v nasprotju z načelom neodvisnosti, temveč tudi s ciljem Direktive 95/46, kakršen izhaja iz njenega člena 1(1).

96. Kot je poudarilo Sodišče, je „[i]z uvodnih izjav 3, 8 in 10 Direktive 95/46 [...] razvidno, da je želel zakonodajalec Unije olajšati prosti pretok osebnih podatkov s približevanjem zakonodaj držav članic, vendar ob varstvu temeljnih pravic oseb, zlasti pravice do zasebnosti, in z zagotavljanjem visoke ravni varstva v Uniji. Člen 1 te direktive tako določa, da države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov“³¹.

97. Določbe Direktive 95/46 je torej treba razlagati v skladu z njenim ciljem, ki je v Uniji zagotoviti visoko raven varstva temeljnih svoboščin in pravic fizičnih oseb in predvsem njihovo pravico do zasebnega življenja pri obdelavi osebnih podatkov.

98. Odločba Komisije o ustreznosti ne more v celoti zavezovati držav članic in s tem njihovih nacionalnih nadzornih organov zaradi pomembnosti navedenega cilja in vloge, ki jo morajo izpolnjevati države članice, da bi ta cilj dosegle, kadar je mogoče s posebnimi okoliščinami utemeljiti resen dvom v spoštovanje temeljnih pravic iz Listine pri prenosu osebnih podatkov v tretjo državo.

30 — Glej sklepne predloge generalnega pravobranilca P. Légerja v zadevi Parlament/Svet in Komisija (C-317/04, EU:C:2005:710, točke od 92 do 95). Glej tudi sodbo Parlament/Svet in Komisija (C-317/04 in C-318/04, EU:C:2006:346, točka 56).

31 — Glej zlasti sodbo IPI (C-473/12, EU:C:2013:715, točka 28 in navedena sodna praksa).

99. Sodišče je že razsodilo, da „je treba določbe Direktive 95/46, ki urejajo obdelavo osebnih podatkov in ki lahko ogrožajo temeljne svoboščine ter zlasti pravico do zasebnosti, nujno razlagati ob upoštevanju temeljnih pravic, ki so na podlagi sodne prakse sestavni del splošnih pravnih načel, katerih spoštovanje zagotavlja Sodišče in ki so zdaj vključene v Listino“³².

100. Poleg tega se sklicujem na sodno prakso, v skladu s katero „morajo države članice [...] ne zgolj razlagati nacionalno pravo v skladu s pravom Unije, temveč tudi paziti, da se ne oprejo na tako razlago besedila sekundarne zakonodaje, ki bi bila v nasprotju s temeljnimi pravicami, ki jih varuje pravni red Unije, ali z drugimi splošnimi načeli prava Unije“³³.

101. Sodišče je tako v sodbi N. S in drugi³⁴ razsodilo, da „uporaba Uredbe [(ES)] št. 343/2003³⁵ na podlagi neizpodbojne domneve, da bo država članica, ki je po navadi pristojna za obravnavanje prošnje prosilca za azil, spoštovala njegove temeljne pravice, ni združljiva z obveznostjo držav članic, da Uredbo št. 343/2003 razlagajo in uporabljajo v skladu s temeljnimi pravicami“³⁶.

102. Sodišče je v zvezi s tem v okviru statusa držav članic kot držav, ki se za vse pravne in praktične namene glede azilnih zadev med seboj obravnavajo kot varne izvirne države, potrdilo, da je treba domnevati, da je obravnavanje prosilcev za azil v vsaki državi članici v skladu z zahtevami Listine, Konvencije o statusu beguncev, podpisane v Ženevi 28. julija 1951,³⁷ in Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin, podpisane v Rimu 4. novembra 1950.³⁸ Vendar je Sodišče razsodilo, da „ni mogoče izključiti, da ima ta sistem v praksi večje težave pri delovanju v določeni državi članici, tako da obstaja resna nevarnost, da bi bili prosilci za azil v primeru predaje v navedeno državo članico obravnavani v nasprotju s temeljnimi pravicami“³⁹.

103. Sodišče je zato razsodilo, da „so [...] države članice, vključno z nacionalnimi sodišči, zavezane, da prosilca za azil ne predajo ‚državi članici, ki je odgovorna‘ v smislu Uredbe št. 343/2003, če ni mogoče, da ne bi vedele, da sistematične pomanjkljivosti sistema azilnega postopka in pogojev za sprejem prosilcev za azil v tej državi članici pomenijo utemeljene razloge za prepričanje, da bi bil prosilec izpostavljen resnični nevarnosti, da se bo z njim nečloveško ali ponižujoče ravnovalo v smislu člena 4 Listine“⁴⁰.

104. Zdi se, da je mogoče prispevek sodbe N. S. in drugi⁴¹ razširiti na položaj, kakršen je ta iz postopka v glavni stvari. Za razlago sekundarne zakonodaje Unije, ki bi temeljila na neizpodbojni domnevi, da bodo država članica, Komisija ali tretja država spoštovala temeljne pravice, je tako treba šteti, da ni združljiva z obveznostjo držav članic, da sekundarno zakonodajo Unije razlagajo in uporabljajo v skladu s temeljnimi pravicami. Člen 25(6) Direktive 95/46 torej pri presoji Komisije, ali je v tretji državi zagotovljena ustrezna raven varstva, ne nalaga take neizpodbojne domneve o spoštovanju temeljnih pravic. Nasprotno, domnevo, na kateri temelji ta določba, da se pri prenosu podatkov

32 — Glej zlasti sodbo *Google Spain in Google* (C-131/12, EU:C:2014:317, točka 68 in navedena sodna praksa).

33 — Glej zlasti sodbo N. S. in drugi (C-411/10 in C-493/10, EU:C:2011:865, točka 77 in navedena sodna praksa).

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

35 — Uredba sveta (ES) št. 343/2003 z dne 18. februarja 2003 o vzpostavitvi meril in mehanizmov za določitev države članice, odgovorne za obravnavanje prošnje za azil, ki jo v eni od držav članic vložijo državljani tretje države (UL, posebna izdaja v slovenščini, poglavje 19, zvezek 6, str. 109).

36 — Točka 99 te sodbe.

37 — *Zbirka pogodb Združenih narodov*, zvezek 189, str. 150, št. 2545 (1954).

38 — Glej sodbo N. S. in drugi (C-411/10 in C-493/10, EU:C:2011:865, točka 80).

39 — *Ibidem* (točka 81).

40 — *Ibidem* (točka 94).

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

v tretjo državo spoštujejo temeljne pravice, je treba šteti za izpodbojno.⁴² Zato se navedena določba ne bi smela razlagati tako, da postavlja pod vprašaj jamstva, navedena zlasti v členu 28(3) Direktive 95/46 in v členu 8(3) Listine, katerih namen je varstvo in spoštovanje pravice do varstva osebnih podatkov.

105. Iz te sodbe torej sklepam, da morajo imeti države članice pri ugotovljenih sistematičnih pomanjkljivostih v tretji državi, v katero so preneseni osebni podatki, možnost, da sprejmejo potrebne ukrepe za varstvo temeljnih pravic iz členov 7 in 8 Listine.

106. Če poleg tega, kot je poudarila italijanska vlada v stališčih, Komisija sprejme odločbo o ustreznosti, to ne pomeni, da se zmanjša varstvo državljanov Unije pri obdelavi njihovih podatkov, kadar so ti preneseni v tretjo državo, glede na raven varstva, ki bi bila navedenim osebam zagotovljena, če bi bili njihovi podatki obdelani v Uniji. Nacionalni nadzorni organi morajo zato imeti možnost, da ukrepajo in izvajajo pooblastila v zvezi s prenosom podatkov v tretje države, na katere se nanaša odločba o ustreznosti. V nasprotnem primeru bi bilo državljanom Unije zagotovljeno slabše varstvo, kot če bi bili njihovi podatki obdelani v Uniji.

107. S tem ko je Komisija sprejela odločbo na podlagi člena 25(6) Direktive 95/46, je bila torej samo odpravljena splošna prepoved izvažanja osebnih podatkov v tretje države, ki zagotavljajo raven varstva, primerljivo z ravno, zagotovljeno na podlagi navedene direktive. Z drugimi besedami, ne gre za vzpostavitev posebne ureditve izjem, ki bi državljanom Unije zagotavljal slabše varstvo glede na splošni sistem iz navedene direktive, določen za obdelavo podatkov znotraj Unije.

108. Sodišče je v točki 63 sodba Lindqvist⁴³ res navedlo, da „[je] s [p]oglavjem IV Direktive 95/46, v katero je vključen člen 25, [...] uvedena posebna ureditev“. Vendar to po mojem mnenju ne pomeni, da mora taka ureditev zagotavljati slabše varstvo. Nasprotno, za doseg cilja varstva podatkov iz člena 1(1) Direktive 95/46 njen člen 25 za države članice in Komisijo določa vrsto obveznosti⁴⁴ in načelo, da je treba prepovedati prenos osebnih podatkov v tretjo državo, ki ne zagotavlja primerne ravni varstva.⁴⁵

109. Glede, natančneje, ureditve varnega pristana Komisija meni, da lahko nacionalni nadzorni organi ukrepajo in prekinijo prenos podatkov samo v okviru člena 3(1)(b) Odločbe 2000/520.

110. Uvodna izjava 8 navedene odločbe določa: „Zaradi preglednosti in zaščite zmožnosti pristojnih organov v državah članicah, da zagotovijo varstvo posameznika glede obdelave njegovih osebnih podatkov, je treba s to odločbo določiti izjemne okoliščine, ki lahko upravičijo prekinitev prenosa posebnih podatkov, ne glede na ugotovitve o ustrezni zaščiti.“

111. V obravnavanem primeru se je razpravljalo natančneje o uporabi člena 3(1)(b) navedene odločbe. Tako lahko nacionalni nadzorni organi v skladu z navedeno določbo odločijo, da se prenos podatkov prekine, če „obstaja precejšnja verjetnost, da se načela kršijo; obstaja utemeljena podlaga za prepričanje, da zadevni mehanizem uveljavljanja ne sprejema ali ne bo sprejel ustreznih in pravočasnih ukrepov za rešitev spornega primera; [bi] nadaljnji prenos podatkov [...] povzročil neposredno nevarnost za nastanek velike škode za subjekte podatkov; in so si pristojni organi v državah članicah v danih okoliščinah razumno prizadevali, da bi organizacijo obvestili in ji dali priložnost za odgovor“.

42 — Točka 104 te sodbe.

43 — C-101/01, EU:C:2003:596.

44 — Točka 65.

45 — Točka 64.

112. Navedena določba nalaga več pogojev, ki so jih stranke v tem postopku različno razlagale.⁴⁶ Iz navedenih razlag, ne da bi jih podrobno obravnaval, izhaja, da navedeni pogoji ozko določajo pooblastilo nacionalnih nadzornih organov, da prekinijo prenos podatkov.

113. Vendar je treba v nasprotju s trditvijo Komisije člen 3(1)(b) Odločbe 2000/520 razlagati v skladu s ciljem varstva osebnih podatkov, ki ga določa Direktiva 95/46, in glede na člen 8 Listine. Nujnost razlage v skladu s temeljnimi pravicami podpira široko razlago navedene določbe.

114. Glede na navedeno pogoji iz člena 3(1)(b) Odločbe 2000/520 po mojem mnenju ne morejo preprečiti, da nacionalni nadzorni organ povsem neodvisno izvaja pooblastila, ki jih ima na podlagi člena 28(3) Direktive 95/46.

115. Kot sta v bistvu navedli belgijska in avstrijska vlada na obravnavi, je člen 3(1)(b) Odločbe 2000/520 kot zasilni izhod tako ozek, da ga je težko uporabiti v praksi. Navedeni člen določa kumulativna merila, poleg tega pa so ta previsoka. Vendar glede na člen 8(3) Listine ni mogoče, da bi bilo polje proste presoje nacionalnih nadzornih organov v zvezi s posebnimi pravicami, izhajajočimi iz člena 28(3) Direktive 95/46, tako omejeno, da teh ne bi bilo več mogoče izvajati.

116. Parlament je v zvezi s tem upravičeno pripomnil, da je zakonodajalec Unije določil, katera pooblastila morajo imeti nacionalni nadzorni organi. Vendar izvedbeno pooblastilo, ki ga je zakonodajalec Unije podelil Komisiji v členu 25(6) Direktive 95/46, ne posega v pooblastila, ki jih je isti zakonodajalec podelil nacionalnim nadzornim organom v členu 28(3) navedene direktive. Z drugimi besedami, Komisija ne more omejevati pooblastil nacionalnih nadzornih organov.

117. Nacionalni nadzorni organi morajo imeti zato za zagotovitev ustreznega varstva temeljnih pravic posameznikov pri obdelavi osebnih podatkov pooblastilo, da ob očitanih kršitvah navedenih pravic izvedejo preiskave. Če ti organi po takih preiskavah menijo, da v tretji državi, na katero se nanaša odločba o ustreznosti, obstajajo resni indici za poseganje v pravico državljanov Unije do varstva njihovih osebnih podatkov, morajo imeti možnost, da prekinijo prenos podatkov prejemniku s sedežem v tej tretji državi.

118. Z drugimi besedami, nacionalni nadzorni organi morajo imeti možnost, da izvedejo preiskave in po potrebi prekinijo prenos podatkov, ne glede na omejevalne pogoje iz člena 3(1)(b) Odločbe 2000/520.

119. Nacionalni nadzorni organi morajo imeti poleg tega na podlagi pooblastila za sodelovanje v sodnih postopkih, kadar so kršene nacionalne določbe, sprejete v skladu z Direktivo 95/46, ali pooblastila za seznanitev sodnih organov s temi kršitvami, ki sta določeni v členu 28(3) navedene direktive, možnost, da ob seznanjenosti z dokazi, da tretja država ne zagotavlja ustreznih ravni varstva, zadevo predložijo nacionalnemu sodišču, ki lahko po potrebi odloči, ali bo pri Sodišču vložilo predlog za sprejetje predhodne odločbe za presojo veljavnosti odločbe Komisije o ustreznosti.

120. Iz vseh navedenih okoliščin izhaja, da je treba člen 28 Direktive 95/46 v povezavi s členoma 7 in 8 Listine razlagati tako, da obstoj odločbe, ki jo je sprejela Komisija na podlagi člena 25(6) navedene direktive, učinkuje tako, da nacionalnemu nadzornemu organu ne preprečuje, da preišče pritožbo, s katero se očita, da tretja država ne zagotavlja ustreznih ravni varstva osebnih podatkov, in po potrebi prekine sporni prenos podatkov.

46 — Po navedbah M. Schremsa prvi pogoj, da „obstaja precejšnja verjetnost, da se načela kršijo“, ni izpolnjen. Vendar ni navedeno, da je družba Facebook USA kot samocertificiran subjekt, na katerega so bili preneseni podatki, sama kršila načela varnega pristana zaradi množičnega in vsesplošnega dostopa ameriških organov do podatkov, ki jih hrani. Načela varnega pristana so namreč izrecno omejena z ameriško zakonodajo, ki je v Prilogi I, četrti odstavek, k Odločbi 2000/520 opredeljena z naporom na zakone, vladne podzakonske akte in sodno prakso.

121. Čeprav Haute Cour de justice v predložitveni odločbi poudarja, da M. Schrems v tožbi iz postopka v glavni stvari ni formalno izpodbijal niti veljavnosti Direktive 95/46 niti veljavnosti Odločbe 2000/520, je iz navedene predložitvene odločbe razvidno, da se glavni očitke M. Schremsa nanaša na izpodbijanje ugotovitve, da ZDA v okviru ureditve varnega pristana zagotavljajo ustrezno raven varstva prenesenih osebnih podatkov.

122. Iz stališč komisarja poleg tega izhaja, da M. Schrems s pritožbo neposredno izpodbija Odločbo 2000/520. Z njeno vložitvijo je želel izpodbijati pogoje in delovanje ureditve varnega pristana kot takega, ker naj bi nadzor nad množico osebnih podatkov, prenesenih v ZDA, dokazoval, da v veljavni zakonodaji in praksi navedene tretje države ni resničnega varstva teh podatkov.

123. Poleg tega predložitveno sodišče ugotavlja, da bi se poseglo v jamstvo, zagotovljeno na podlagi člena 7 Listine in temeljnih vrednot, ki naj bi bile skupne ustavnim tradicijam držav članic, če bi lahko javni organi naključno in vsesplošno dostopali do elektronskih komunikacij, ne da bi morali to objektivno utemeljiti z razlogi državne varnosti ali preprečevanja kaznivih dejanj, ki se nanašajo konkretno na zadevne posameznike, ter brez ustreznih in preverljivih jamstev.⁴⁷ Predložitveno sodišče tako posredno izraža pomisleke glede veljavnosti Odločbe 2000/520.

124. Za presojo vprašanja, ali ZDA v okviru ureditve varnega pristana zagotavljajo ustrezno raven varstva prenesenih osebnih podatkov, je torej nujno treba preučiti veljavnost navedene odločbe.

125. V zvezi s tem je treba poudariti, da lahko Sodišče v okviru instrumenta sodelovanja med njim in nacionalnimi organi, uvedenega s členom 267 PDEU, čeprav mu je v predhodno odločanje predloženo izključno vprašanje razlage prava Unije, v nekaterih posebnih okoliščinah preizkusi veljavnost določb sekundarnega prava.

126. Zato je Sodišče večkrat po uradni dolžnosti za neveljaven razglasilo akt, glede katerega se je zahtevala le razlaga.⁴⁸ Razsodilo je tudi, da „kadar se zdi, da je resnični predmet vprašanj, ki jih postavi nacionalno sodišče, bolj preizkus veljavnosti kot razlaga aktov [Unije], mora Sodišče navedenemu sodišču nemudoma dati pojasnilo, ne da bi ga zavezalo k formalizmu, ki prinaša zgolj odlašanje in ni združljivo z naravo mehanizmov, uvedenih s členom [267 PDEU]“⁴⁹. Sodišče je poleg tega že razsodilo, da je treba očitne dvome predložitvenega sodišča glede združljivosti akta sekundarnega prava s pravili o varstvu temeljnih pravic razlagati tako, da postavljajo pod vprašaj veljavnost navedenega akta glede na pravo Unije.⁵⁰

127. Naj še spomnim, da iz sodne prakse Sodišča izhaja, da se za akte institucij, organov, uradov in agencij Unije domneva, da so veljavni, kar pomeni, da imajo ti pravne učinke toliko časa, dokler niso preklicani, razglašeni za nične v okviru ničnostne tožbe ali razglašeni za neveljavne v okviru postopka predhodnega odločanja ali ugovora nezakonitosti. Za ugotovitev neveljavnosti akta Unije je pristojno le Sodišče, namen te pristojnosti pa je zagotavljanje pravne varnosti z enotno uporabo prava Unije. Ker Komisija navedene odločbe ni razglasila za neveljavno, spremenila ali razveljavila, je ta še naprej obvezna v vseh elementih in se neposredno uporablja v vseh državah članicah.⁵¹

128. Menim, da bi torej moralo Sodišče, da bi predložitvenemu sodišču dalo celovit odgovor in odpravilo dvome, navedene v tem postopku glede veljavnosti Odločbe 2000/520, presoditi veljavnost te odločbe.

47 — Točka 24 predložitvene odločbe.

48 — Glej zlasti sodbe Strehl (62/76, EU:C:1977:18, točke od 10 do 17), Roquette Frères (145/79, EU:C:1980:234, točka 6) in Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, točke od 32 do 39).

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

50 — Glej sodbo Hauer (44/79, EU:C:1979:290, točka 16).

51 — Glej zlasti sodbo CIVAD (C-533/10, EU:C:2012:347, točke od 39 do 41 in navedena sodna praksa).

129. Zato je treba tudi pojasniti, da se je treba pri preučitvi, ali je Odločba 2000/520 veljavna ali ne, omejiti na očitke, o katerih se je razpravljalo v okviru tega postopka. V navedenem okviru se namreč ni razpravljalo o vseh vidikih, povezanih z delovanjem ureditve varnega pristana, zato menim, da tu ne morem izčrpno preučiti pomanjkljivosti navedene ureditve.

130. Pred Sodiščem se je v okviru tega postopka razpravljalo o vprašanju, ali vsesplošen in neusmerjen dostop ameriških obveščevalnih služb do prenesenih podatkov lahko posega v zakonitost Odločbe 2000/520. Veljavnost navedene odločbe je torej mogoče presoati s tega vidika.

B – Veljavnost Odločbe 2000/520

1. Vidiki, ki jih je treba upoštevati pri presoji veljavnosti Odločbe 2000/520

131. Spomniti je treba na sodno prakso, v skladu s katero „je treba v okviru ničnostne tožbe zakonitost akta presoditi glede na dejanske in pravne elemente, ki obstajajo takrat, ko se akt sprejme, presojo Komisije pa je mogoče preizkusiti le, če je očitno napačna, glede na elemente, ki jih je imela na voljo, ko je sprejela sporni akt“⁵².

132. Sodišče je v sodbi *Gaz de France – Berliner Investissement*⁵³ opozorilo na načelo, v skladu s katerim „mora presoja veljavnosti akta, ki jo opravi Sodišče v okviru predloga za sprejetje predhodne odločbe, običajno temeljiti na položaju, ki je obstajal v trenutku sprejemanja akta“⁵⁴. Vendar se zdi, da je dopustilo, da „bi bilo mogoče veljavnost akta v nekaterih okoliščinah presoati glede na nove elemente, nastale po njegovem sprejetju“⁵⁵.

133. Navedeno izhodišče, kot ga je zastavilo Sodišče, se mi zdi zlasti upoštevno v okviru obravnavane zadeve.

134. Odločbe, ki jih je sprejela Komisija na podlagi člena 25(6) Direktive 95/46, imajo namreč posebne značilnosti. Njihov namen je presoditi, ali je v tretji državi raven varstva osebnih podatkov ustrezna ali ne. Pri tem gre za presojo, ki se lahko spreminja glede na dejanske in pravne okoliščine v tretji državi.

135. Ker je odločba o ustreznosti odločba posebne vrste, je treba pravilo, da je mogoče njeno veljavnost presoati samo glede na elemente, ki so obstajali ob njenem sprejetju, v obravnavanem primeru prilagoditi. Tako pravilo bi sicer povzročilo, da Sodišče več let po sprejetju odločbe o ustreznosti pri presoji, ki jo mora opraviti, ne more upoštevati poznejših dogodkov, čeprav predlog za sprejetje predhodne odločbe za presojo veljavnosti ni časovno omejen in ga je mogoče vložiti prav zaradi poznejših dejstev, ki kažejo na pomanjkljivosti zadevnega akta.

136. V obravnavanem primeru to, da Odločba 2000/520 velja že približno petnajst let, kaže na to, da Komisija implicitno potrjuje svojo presojo iz leta 2000. Če mora Sodišče v okviru predloga za sprejetje predhodne odločbe presoditi veljavnost navedene presoje, ki jo je ves ta čas ohranila Komisija, je torej ne le mogoče, temveč tudi ustrezno, da lahko navedeno presojo ponovno preuči glede na nove okoliščine, ki so nastale po sprejetju odločbe o ustreznosti.

52 — Glej zlasti sodbo *BVG/D/Komisija* (T-104/07 in T-339/08, EU:T:2013:366, točka 291), ki napotuje na sodbo *IECC/Komisija* (C-449/98 P, EU:C:2001:275, točka 87).

53 — C-247/08, EU:C:2009:600.

54 — Točka 49 in navedena sodna praksa.

55 — Točka 50 in navedena sodna praksa. Glej v tem smislu *Lenaerts, K., Maselis, I., in Gutman, K., EU Procedural Law*, Oxford University Press, 2014, kjer je navedeno, da „in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court“ (točka 10.16, str. 471).

137. Komisija mora navedeno odločbo o ustreznosti zaradi njene posebne narave redno ponovno pregledovati. Če Komisija na podlagi novih dogodkov, ki so medtem nastopili, te ne spremeni, pomeni, da implicitno, vendar nujno potrjuje prvotno opravljeno presojo. Tako ponovi svojo ugotovitev, da zadevna tretja država zagotavlja ustrezno raven varstva prenesenih osebnih podatkov. Sodišče mora preučiti, ali navedena ugotovitev ostaja veljavna kljub pozneje nastalim okoliščinam.

138. Za zagotovitev učinkovitega sodnega nadzora nad tako odločbo je torej treba po mojem mnenju pri presoji njene veljavnosti upoštevati trenutne dejanske in pravne okoliščine.

2. Pojem ustrezne ravni varstva

139. Člen 25 Direktive 95/46 v celoti temelji na načelu, da prenos osebnih podatkov v tretjo državo ni mogoč, razen če ta tretja država ne zagotavlja ustrezne ravni varstva takih podatkov. Cilj navedenega člena je tako zagotoviti neprekinjenost varstva, zagotovljenega z navedeno direktivo, pri prenosu osebnih podatkov v tretjo državo. V zvezi s tem je treba opozoriti, da navedena direktiva državljanom Unije pri obdelavi njihovih osebnih podatkov zagotavlja visoko raven varstva.

140. Ker ima varstvo osebnih podatkov v zvezi s temeljno pravico do zasebnega življenja pomembno vlogo, ga je treba zagotoviti tudi pri prenosu osebnih podatkov v tretjo državo.

141. Zato menim, da lahko Komisija na podlagi člena 25(6) Direktive 95/46 ugotovi, da tretja država zagotavlja ustrezno raven varstva, samo če po celostni presoji zakonodaje in prakse v zadevni tretji državi lahko dokaže, da ta tretja država zagotavlja bistveno enakovredno raven varstva kot navedena direktiva, čeprav se lahko načini tega varstva razlikujejo od tistih, ki se običajno uporabljajo v Uniji.

142. Čeprav je mogoče angleški izraz „adequate“ z jezikovnega vidika mogoče razumeti tako, da označuje ravno še zadovoljivo ali zadostno raven varstva, in se tako njegovo pomensko polje razlikuje od francoskega izraza „adéquat“, je treba ugotoviti, da je treba pri razlagi navedenega izraza kot edino merilo upoštevati cilj, da se doseže visoka raven varstva temeljnih pravic, kot to določa Direktiva 95/46.

143. Pri preučitvi ravni varstva v tretji državi je treba upoštevati dve temeljni okoliščini, in sicer vsebino pravil, ki se uporabljajo, in sredstva, s katerimi je mogoče doseči spoštovanje teh pravil.⁵⁶

144. Po mojem mnenju bi morala ureditev varnega pristana, ki v veliki meri temelji na samocertificiranju in samoocenjevanju podjetij, ki so prostovoljno del te ureditve, za dosego ravni varstva, ki je bistveno enakovredna tisti v Uniji, vključevati ustrezna jamstva in mehanizem zadostnega nadzora. Varstvo, zagotovljeno pri prenosu osebnih podatkov v tretje države, tako ne bi smelo biti slabše kot pri obdelavi teh podatkov v Uniji.

145. V zvezi s tem naj takoj poudarim, da v Uniji prevladuje pojmovanje, da je mehanizem zunanjega nadzora, ki ga izvaja neodvisni organ, potreben pri vsakem sistemu, katerega namen je zagotoviti spoštovanje pravil o varstvu osebnih podatkov.

⁵⁶ — Glej str. 5 delovnega dokumenta Komisije WP 12 z naslovom „Prenosi podatkov v tretje države: uporaba členov 25 in 26 Direktive o varstvu podatkov“, ki ga je 24. julija 1998 sprejela delovna skupina o varstvu posameznikov pri obdelavi osebnih podatkov.

146. Poleg tega je treba za zagotovitev polnega učinka člena 25, od (1) do (3), Direktive 95/46 upoštevati, da je ustreznost ravni varstva v tretji državi položaj, ki se lahko zaradi številnih dejavnikov skozi čas spreminja. Države članice in Komisija morajo zato biti stalno pozorne na vsako spremembo okoliščin, pri kateri bi bilo treba ponovno presoditi ustreznost ravni varstva v tretji državi. Presoja ustreznosti te ravni varstva ni nikakor mogoče omejiti na določen trenutek in jo nato neomejeno ohranjati, pri tem pa ne upoštevati vseh spremenjenih okoliščin, iz katerih je razvidno, da raven varstva ni več ustrezna.

147. Obveznost tretje države, da zagotovi ustrezno raven varstva, je torej trajna. Če se navedena presoja opravi v določenem trenutku, ohranitev veljavnosti odločbe kaže na domnevo, da z nobeno poznejšo okoliščino ni mogoče izpodbiti prvotne veljavnosti presoje Komisije.

148. Ne sme se namreč spregledati, da je cilj člena 25 Direktive 95/46 preprečiti, da bi se osebni podatki prenesli v tretjo državo, ki ne zagotavlja ustrezne ravni varstva, s čimer bi bila kršena temeljna pravica do varstva osebnih podatkov, zagotovljena s členom 8 Listine.

149. Pomembno je poudariti, da pooblastilo, ki ga je zakonodajalec Unije v členu 25(6) Direktive 95/46 podelil Komisiji, da ugotovi, ali tretja država zagotavlja ustrezno raven varstva, je izrecno pogojeno z zahtevo, da mora ta tretja država v skladu z odstavkom 2 navedenega člena zagotavljati tako raven. Če je mogoče zaradi novih okoliščin podvomiti o prvotni presoji Komisije, mora torej zadnja svojo odločbo prilagoditi.

3. Presoja

150. Naj spomnim, da lahko na podlagi člena 25(6) Direktive 95/46 „Komisija [...]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“. Iz odstavka 6 člena 25 navedene direktive v povezavi z njegovim odstavkom 2 izhaja, da mora Komisija za ugotovitev, da tretja država zagotavlja ustrezno raven varstva, celostno presoditi pravna pravila, ki veljajo v navedeni tretji državi, in njihovo uporabo.

151. Videli smo, da je treba to, da je Komisija ohranila veljavnost svoje Odločbe 2000/520, čeprav so se pojavile nove dejanske in pravne okoliščine, razumeti kot njeno voljo, da potrdi svojo prvotno presajo.

152. Sodišče v okviru predloga za sprejetje predhodne odločbe ni pristojno za presajo okoliščin, zaradi katerih je nastal spor, v zvezi s katerim je nacionalno sodišče vložilo navedeni predlog.⁵⁷

153. Zato se bom oprl na okoliščine, ki jih je navedlo predložitveno sodišče v predlogu za sprejetje predhodne odločbe in jih je poleg tega Komisija splošno priznala kot dokazane.⁵⁸

154. Za izpodbijanje presoje Komisije, da ureditev varnega pristana zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz Unije v Združene države, so bile pred Sodiščem navedene te okoliščine.

155. Predložitveno sodišče v predlogu za sprejetje predhodne odločbe izhaja iz naslednjih dveh dejanskih ugotovitev. Po eni strani naj bi lahko imeli NSA in druge ameriške varnostne agencije vpogled v osebne podatke, ki so jih prenesla podjetja, kakršno je Facebook Ireland, matični družbi s sedežem v ZDA, pri dejavnostih množičnega in neusmerjenega nadzora in prestrezanja podatkov. Po

57 — Glej zlasti sodbo Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, točka 22 in navedena sodna praksa).

58 — Glej sporočilo Komisije, navedeno v opombi 2, in Sporočilo Komisije Evropskemu parlamentu in Svetu o delovanju varnega pristana z vidika državljanov EU in družb, ustanovljenih v EU (COM(2013) 847 final).

razkritjih E. Snowdena naj namreč za zdaj na podlagi razpoložljivih dokazov ne bi bilo mogoče verodostojno ugotavljati drugače.⁵⁹ Po drugi strani naj državljani Unije ne bi imeli dejanske pravice do izjave o vprašanju nadzora in prestrazovanja njihovih podatkov, ki naj bi ju izvajali NSA in ameriške varnostne agencije.⁶⁰

156. Dejanske ugotovitve, ki jih je tako navedlo High Court of Justice, so podprte celo z ugotovitvami Komisije.

157. Komisija je tako v zgoraj navedenem sporočilu o delovanju varnega pristana z vidika državljanov Unije in podjetij s sedežem na njenem ozemlju izhajala iz ugotovitve, da so v letu 2013 informacije o obsegu programov ameriškega nadzora zbudile skrb o kontinuiteti varstva osebnih podatkov, zakonito prenesenih v ZDA v okviru ureditve varnega pristana. Poudarila je, da se zdi, da so vse družbe, ki so vključene v program PRISM in ki organom v ZDA dovoljujejo dostop do podatkov, shranjenih in obdelanih v ZDA, certificirane za varni pristan. S tem je ureditev varnega pristana po njenih navedbah postala eden od kanalov, po katerih je ameriškim obveščevalnim organom omogočen dostop do zbiranja osebnih podatkov, prvotno obdelanih v Uniji.⁶¹

158. Iz navedenih okoliščin izhaja, da zakonodaja in praksa ZDA omogočata obsežno zbiranje osebnih podatkov državljanov Unije, prenesenih v okviru ureditve varnega pristana, ne da bi bilo navedenim državljanom zagotovljeno učinkovito pravno varstvo.

159. Navedene dejanske ugotovitve po mojem mnenju dokazujejo, da Odločba 2000/520 ne vsebuje zadostnih jamstev. Navedena odločba se je zaradi teh pomanjkljivih jamstev izvajala v nasprotju z zahtevami Listine in Direktive 95/46.

160. Namen odločbe, ki jo sprejme Komisija na podlagi člena 25(6) Direktive 95/46, pa je ugotoviti, da tretja država „zagotavlja“ ustrezno raven varstva. Izraz „zagotavlja“ v sedanjiku kaže na to, da se mora navedena odločba za ohranitev veljavnosti nanašati na tretjo državo, ki po sprejetju navedene odločbe še naprej zagotavlja ustrezno raven varstva.

161. Dejansko pa so navedena razkritja glede ravnanja NSA, ki naj bi uporabljala podatke, prenesene v okviru ureditve varnega pristana, osvetlila pomanjkljivosti pravne podlage, ki je Odločba 2000/520.

162. Pomanjkljivosti, ki so bile ugotovljene v tem postopku, so natančneje zajete v Prilogi I, četrtri odstavek, k navedeni odločbi.

163. Naj spomnim, da je v skladu z navedeno določbo „[z]avezanost k načelom [varnega pristana] [...] lahko omejena: (a) če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa [in za spoštovanje zakonov]; (b) z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdržljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil“.

164. Težava izhaja zlasti iz tega, kako so ameriški organi uporabili izjeme, opredeljene v navedeni določbi. Izvajanje navedenih izjem navedenih organov zaradi njihove presplošne opredelitve ni omejeno na tisto, kar je nujno potrebno.

165. Tej presplošni opredelitvi se pridružuje okoliščina, da državljani Unije nimajo na voljo ustreznega pravnega sredstva zoper obdelavo osebnih podatkov za druge namene, kot so tisti, za katere so bili prvotno zbrani in nato preneseni v ZDA.

59 — Točka 7(c) predložitvene odločbe.

60 — Točka 7(b) predložitvene odločbe.

61 — Str. 19 njenega obvestila.

166. Poleg izjem, navedenih v Odločbi 2000/520 za uporabo načel varnega pristana, zlasti za izpolnjevanje zahtev nacionalne varnosti, bi bilo treba vzpostaviti ustrezen mehanizem neodvisnega nadzora, ki bi preprečeval ugotovljene posege v pravico do zasebnega življenja.

167. Razkritja o praksah ameriških obveščevalnih služb pri splošnem nadzoru prenesenih podatkov v okviru varnega pristana so torej osvetlila nekatere pomanjkljivosti Odločbe 2000/520.

168. Navedeni očitki v okviru tega spora se ne nanašajo na to, ali je družba Facebook kršila načela varnega pristana. Če certificirano podjetje, kakršno je Facebook USA, ameriškim organom omogoči dostop do podatkov, ki so bili preneseni iz države članice, je mogoče šteti, da tako ravna v skladu z ameriško zakonodajo. Ker je tak položaj zaradi široke opredelitve izjem v Odločbi 2000/520 s to odločbo izrecno priznan, se v obravnavanem primeru dejansko postavlja vprašanje, ali so take izjeme združljive s primarnim pravom Unije.

169. V zvezi s tem je treba poudariti, da iz ustaljene sodne prakse Sodišča izhaja, da je spoštovanje človekovih pravic pogoj za zakonitost aktov Unije in da v Uniji niso dopustni ukrepi, ki niso združljivi s spoštovanjem človekovih pravic.⁶²

170. Poleg tega iz sodne prakse Sodišča izhaja, da sporočanje zbranih osebnih podatkov tretjim osebam, javnim ali zasebnim, pomeni poseg v pravico do spoštovanja zasebnega življenja, „ne glede na to, kakšna bo poznejša uporaba posredovanih podatkov“⁶³. Sodišče je poleg tega v sodbi Digital Rights Ireland in drugi⁶⁴ potrdilo, da dovolitev pristojnim nacionalnim organom, da dostopajo do takih podatkov, pomeni dodatno kršitev v to temeljno pravico.⁶⁵ Poleg tega je vsaka oblika obdelave osebnih podatkov določena v členu 8 Listine in pomeni poseganje v pravico do varstva teh podatkov.⁶⁶ Dostop ameriških obveščevalnih služb do prenesenih podatkov je torej prav tako poseganje v temeljno pravico do varstva osebnih podatkov, zagotovljeno s členom 8 Listine, saj tak dostop pomeni obdelavo teh podatkov.

171. V skladu z ugotovitvijo Sodišča v navedeni sodbi je tako ugotovljeno poseganje zaradi velikega števila zadevnih uporabnikov in količine prenesenih podatkov zelo obsežno in ga je treba šteti za zelo resno. To poseganje je zaradi navedenih okoliščin in tajnosti dostopa ameriških organov do osebnih podatkov, prenesenih podjetjem s sedežem v ZDA, zelo resno.

172. K temu se pridružuje okoliščina, da državljani Unije, ki uporabljajo Facebook, niso seznanjeni, da bodo njihovi osebni podatki splošno dostopni ameriškim varnostnim agencijam.

173. Poudariti je tudi treba, da je predložitveno sodišče ugotovilo, da državljani Unije v ZDA nimajo dejanske pravice do izjave o vprašanju nadzora in prestrezanja njihovih podatkov. FISC izvaja nadzor, toda postopek pred njim poteka tajno in *ex parte*.⁶⁷ Menim, da gre tu za poseganje v pravico državljanov Unije do učinkovitega pravnega sredstva iz člena 47 Listine.

174. Ugotovljeno je torej poseganje v temeljne pravice iz členov 7, 8 in 47 Listine, ki ga omogočajo izjeme od načel varnega pristana, določene v Prilogi I, četrti odstavek, Odločbe 2000/520.

175. Zdaj je treba preveriti, ali je to poseganje utemeljeno ali ne.

62 — Glej zlasti sodbo Kadi in Al Barakat International Foundation/Svet in Komisija (C-402/05 P in C-415/05 P, EU:C:2008:461, točka 284 in navedena sodna praksa).

63 — Sodba Österreichischer Rundfunk in drugi (C-465/00, C-138/01 in C-139/01, EU:C:2003:294, točka 74).

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

65 — Točka 35.

66 — Točka 36.

67 — Točka 7(b) predložitvene odločbe.

176. V skladu s členom 52(1) Listine mora biti kakršno koli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Ob upoštevanju načela sorazmernosti pa so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.

177. Glede na tako opredeljene pogoje za možnost priznanja omejitev pri izvajanju pravic in svoboščin, ki jih ščiti Listina, močno dvomim, da bi bilo mogoče za zadevne omejitve iz obravnavane zadeve šteti, da so v skladu z bistveno vsebino členov 7 in 8 Listine. Zdi se namreč, da dostop ameriških obveščevalnih služb do prenesenih podatkov zajema vsebino elektronskih komunikacij, kar bi posegalo v bistveno vsebino temeljne pravice do spoštovanja zasebnega življenja in drugih pravic iz člena 7 Listine. Ker je poleg tega zaradi široke opredelitve omejitev iz Priloge I, četrti odstavek, k Odločbi 2000/520 mogoče potencialno izključiti uporabo vseh načel varnega pristana, je mogoče šteti, da te omejitve posegajo v bistveno vsebino temeljne pravice do varstva osebnih podatkov.⁶⁸

178. Glede vprašanja, ali je ugotovljeno poseganje utemeljeno s ciljem v splošnem interesu, naj najprej spomnim, da je mogoče v skladu s točko (b) četrtega odstavka Priloge I k Odločbi 2000/520 zavezanost načelom varnega pristana omejiti „z zakonom, vladnim podzakonskim aktom ali sodno prakso, ki ustvarijo nezdružljivost obveznosti ali izrecnih pooblastil, pod pogojem, da lahko organizacija pri izvajanju takih pooblastil dokaže, da je njeno neizpolnjevanje načel toliko omejeno, kolikor je potrebno za izpolnitev prednostnih zakonitih interesov na podlagi takšnih pooblastil“.

179. Ugotoviti je treba, da „zakoniti interesi“, navedeni v tej določbi, niso opredeljeni. Iz navedenega izhaja negotovost glede potencialno zelo širokega področja uporabe navedene izjeme od uporabe načel varnega pristana podjetij, zavezanih tem načelom.

180. Ta vtis je mogoče potrditi z branjem pojasnil v naslovu B Priloge IV k Odločbi 2000/520, naslovljenem „Izrecna zakonska pooblastila“, zlasti trditve, da „[je] povsem jasno [...], da kadar ameriško pravo odreja nasprotno obveznost, morajo ameriške organizacije, ne glede na to, ali so udeleženke varnega pristana ali ne, ravnati v skladu z zakonom“. Poleg tega je v zvezi z izrecnimi pooblastili navedeno, da „je namen načel varnega pristana premostiti razlike med ameriškim in evropskim režimom varstva zasebnosti, dolžni pa smo upoštevati posebne pravice naših izvoljenih predstavnikov zakonodajne oblasti“.

181. Iz navedenega po mojem mnenju izhaja, da navedena izjema nasprotuje členom 7, 8 in 52(1) Listine, ker ne sledi cilju splošnega interesa, ki bi bil dovolj natančno opredeljen.

182. Vsekakor pa enostavnost in splošnost, s katero sama Odločba 2000/520 v točki (b) četrtega odstavka Priloge I in v točki B Priloge IV določa, da je mogoče od načel varnega pristana odstopati v skladu s predpisi ameriškega prava, nista združljivi s pogojem, da je treba izjeme od pravil o varstvu osebnih podatkov omejiti le na tisto, kar je to nujno potrebno. Drži, da je naveden pogoj potrebnosti, vendar razen tega, da je dokazno breme za izpolnjevanje tega pogoja na strani zadevnega podjetja, ne vidim, kako bi se lahko tako podjetje izognilo obveznosti odstopanja od načel varnega pristana, izhajajoči iz pravnih pravil, ki jih mora spoštovati.

183. Zato menim, da je treba Odločbo 2000/520 razglasiti za neveljavno, ker že zaradi samega obstoja izjeme, ki tako splošno in nenatančno omogoča odstopanje od načel ureditve varnega pristana, ni mogoče šteti, da navedena ureditev zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih iz Unije v ZDA.

68 — Glej v zvezi s tem sodbo Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238, točki 39 in 40).

184. Glede prve kategorije omejitev iz točke (a) četrtega odstavka Priloge I k Odločbi 2000/520 zaradi izpolnjevanja zahtev nacionalne varnosti, javnega interesa in spoštovanja ameriških zakonov se mi zdi samo prvi cilj dovolj natančno opredeljen, da bi ga bilo mogoče šteti za cilj v splošnem interesu, ki ga priznava Unija v skladu s členom 52(1) Listine.

185. Zdaj je treba preveriti sorazmernost ugotovljenega poseganja.

186. V zvezi s tem je treba opozoriti, da „načelo sorazmernosti v skladu z ustaljeno prakso Sodišča zahteva, da je z ravnanjem institucij Unije mogoče uresničiti legitimne cilje, ki jim sledi zadevna ureditev, in da to ravnanje ne prestopi meje tega, kar je primerno in potrebno za uresničitev teh ciljev“.⁶⁹

187. Glede sodnega nadzora nad upoštevanjem teh pogojev „se lahko, ker gre za poseganje v temeljne pravice, izkaže, da je obseg polja proste presoje, ki ga ima zakonodajalec Unije, omejen glede na nekatere elemente, med katerimi so zlasti zadevno področje, narava zadevne pravice, zagotovljene z Listino, narava in teža poseganja ter cilj tega poseganja“.⁷⁰

188. Menim, da mora odločbe, ki jih Komisija sprejme na podlagi člena 25(6) Direktive 95/46, v celoti nadzorovati Sodišče, glede sorazmernosti presoje navedene institucije o ustreznosti ravni varstva v tretji državi zaradi „[njene] domače zakonodaje ali mednarodnih obveznosti, ki jih je prevzela“.

189. V zvezi s tem je treba tudi pripomniti, da je Sodišče v sodbi *Digital Rights Ireland in drugi*⁷¹ razsodilo, da „je ob upoštevanju, prvič, pomembne vloge varstva osebnih podatkov z vidika temeljne pravice do spoštovanja zasebnega življenja ter, drugič, obsega in teže poseganja v to pravico, ki jo pomeni [izpodbijana] [d]irektiva [...], polje proste presoje zakonodajalca Unije zmanjšano, tako da je treba izvajati strog nadzor“⁷².

190. To poseganje mora biti mogoče za uresničevanje cilja zadevnega akta Unije in potrebno za doseg tega cilja.

191. Glede tega „[v] zvezi s pravico do spoštovanja zasebnega življenja varstvo te temeljne pravice v skladu z ustaljeno sodno prakso Sodišča [...] zahteva, da se odstopanja od varstva osebnih podatkov in njegove omejitve določijo v mejah tega, kar je nujno potrebno“⁷³.

192. Sodišče pri nadzoru upošteva tudi, „da je varstvo osebnih podatkov, ki izhaja iz izrecne obveznosti, določene v členu 8(1) Listine, posebno pomembno za pravico do spoštovanja zasebnega življenja, potrjeno v členu 7 te listine“⁷⁴.

193. Sodišče se v zvezi s tem sklicuje na sodno prakso Evropskega sodišča za človekove pravice, pri čemer navaja: „Zadevni predpisi Unije morajo [...] določati jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter določajo minimalne zahteve, tako da imajo osebe, katerih podatki so bili hranjeni, zadostna jamstva, ki omogočajo učinkovito varovanje njihovih osebnih podatkov pred tveganji zlorabe in vsakršnim nezakonitim dostopom do teh podatkov ter njihovo nezakonito uporabo.“⁷⁵ Pri tem dodaja: „Potreba po takih jamstvih je toliko pomembnejša, če so osebni podatki [...] predmet avtomatske obdelave in obstaja veliko tveganje nezakonitega dostopa do teh podatkov.“⁷⁶

69 — Sodba *Digital Rights Ireland in drugi* (C-293/12 in C-594/12, EU:C:2014:238, točka 46 in navedena sodna praksa).

70 — *Ibidem* (točka 47 in navedena sodna praksa).

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

72 — Točka 48.

73 — Sodba *Digital Rights Ireland in drugi* (C-293/12 in C-594/12, EU:C:2014:238, točka 52 in navedena sodna praksa).

74 — *Ibidem* (točka 53).

75 — *Ibidem* (točka 54 in navedena sodna praksa).

76 — *Ibidem* (točka 55 in navedena sodna praksa).

194. Menim, da obstaja analogija med točko (a) četrtega odstavka Priloge I k Odločbi 2000/520 in členom 13(1) Direktive 95/46. V prvi določbi je navedeno, da je lahko zavezanost „načelom varnega pristana“ omejena, „če je to potrebno za izpolnjevanje zahtev nacionalne varnosti, javnega interesa [in za spoštovanje zakonov]“. V drugi je navedeno, da lahko države članice sprejmejo zakonodajne ukrepe za omejitev obsega obveznosti in pravic, opredeljenih v členih 6(1), 10, 11(1), 12 in 21 navedene direktive, kadar je taka omejitev potreben ukrep za zaščito, med drugim, državne varnosti, obrambe, javne varnosti ter preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj.

195. Kot je poudarilo Sodišče v sodbi IPI⁷⁷, iz besedila člena 13(1) Direktive 95/46 izhaja, da lahko države članice ukrepe, na katere se nanaša navedena določba, določijo le, če so ti potrebni. Možnost, ki jo navedena določba daje državam članicam, je tako pogojena s „potrebnostjo“ ukrepov.⁷⁸ Za omejitve iz člena 13 navedene direktive pri obdelavi osebnih podatkov znotraj Unije je treba šteti, da se nanašajo na to, kar je nujno potrebno za uresničitev zadevnega cilja. Menim, da mora enako veljati za omejitve načel varnega pristana, ki so opredeljene v četrtem odstavku Priloge I k Odločbi 2000/520.

196. Vendar je treba ugotoviti, da merilo potrebnosti iz točke (a) četrtega odstavka Priloge I k Odločbi 2000/520 ni omenjeno v vseh jezikovnih različicah. To velja zlasti za francosko različico, v kateri je navedeno, da je „«[l]’adhésion aux principes peut être limitée par [...] les exigences relatives à la sécurité nationale, l’intérêt public et le respect des lois aux États-Unis (zavezanost k načelom je lahko omejena z zahtevami nacionalne varnosti, javnega interesa in za spoštovanje zakonov ZDA)“, medtem ko je v španski, nemški in angleški jezikovni različici na primer navedeno, da morajo biti uvedene omejitve potrebne za doseg zgoraj navedenih ciljev.

197. Kakorkoli že, dejanske okoliščine, ki sta jih navedla predložitveno sodišče in Komisija v zgoraj navedenih sporočilih, jasno kažejo, da izvajanje navedene omejitve v praksi ni omejeno samo na to, kar je nujno potrebno za doseg zadevnih ciljev.

198. V zvezi s tem ugotavljam, da dostop do prenesenih osebnih podatkov, ki ga imajo ameriške obveščevalne službe, splošno zajema vse osebe in vsa sredstva elektronske komunikacije ter vse prenesene podatke, vključno z vsebino komunikacij, pri tem pa ni nobenega razlikovanja, omejitve ali izjeme glede na zadevni cilj v splošnem interesu.⁷⁹

199. Dostop ameriških obveščevalnih služb do prenesenih podatkov namreč na splošno zadeva vse osebe, ki uporabljajo elektronske komunikacijske storitve, tudi če zadevne osebe ne ogrožajo nacionalne varnosti.⁸⁰

200. Tak množičen in neusmerjen nadzor sam po sebi ni sorazmeren in neupravičeno posega v pravice, ki jih zagotavljata člena 7 in 8 Listine.

201. Kot je upravičeno poudaril Parlament v stališčih, ni mogoče, da bi zakonodajalec Unije ali države članice sprejeli zakonodajne določbe, ki bi v nasprotju z Listino določale množičen in neusmerjen nadzor, zato nujno sledi, da *a fortiori* za tretje države nikakor ni mogoče šteti, da zagotavljajo ustrezno raven varstva osebnih podatkov državljanov Unije, če njihova zakonodaja dejansko dovoljuje množičen in neusmerjen nadzor in prestrezanje takih podatkov.

202. Poleg tega je treba poudariti, da ureditev varnega pristana, kakor je opredeljena v Odločbi 2000/520, nima jamstev, s katerimi je mogoče preprečiti množičen in vsesplošen dostop do prenesenih podatkov.

⁷⁷ — C-473/12, EU:C:2013:715.

⁷⁸ — Točka 32.

⁷⁹ — Glej po analogiji sodbo Digital Rights Ireland in drugi (C-293/12 in C-594/12, EU:C:2014:238, točka 57 in navedena sodna praksa).

⁸⁰ — *Ibidem* (točki 58 in 59).

203. V zvezi s tem ugotavljam, da je Sodišče v sodbi *Digital Rights Ireland* in drugi⁸¹ poudarilo pomembnost tega, da se določijo „jasn[a] in natančn[a] pravil[a], ki bi urejala obseg poseganja v temeljne pravice, potrjene s členoma 7 in 8 Listine⁸²“. Tako poseganje mora biti po navedbah Sodišča „natančno določeno v predpisih, s katerimi bi bilo zagotovljeno, da je dejansko omejeno na to, kar je nujno potrebno“⁸³. Sodišče je poleg tega v isti sodbi poudarilo potrebo, da se določijo „zadostn[a] jamst[va], kot se zahtevajo v členu 8 Listine, ki bi omogočala zagotovitev učinkovitega varovanja hranjenih [osebnih] podatkov pred tveganji zlorabe ter vsakršnim nezakonitim dostopom do teh podatkov in njihovo nezakonito uporabo“⁸⁴.

204. Vendar je treba ugotoviti, da mehanizma zasebne arbitraže in FTC zaradi njune omejenosti na trgovinske spore nista ustrezni sredstva za ugovarjanje dostopu ameriških obveščevalnih služb do zasebnih podatkov, prenesenih iz Unije.

205. Pristojnost FTC zajema nepoštena in goljufiga dejanja ali prakse v trgovini in torej ne vključuje zbiranja in uporabe osebnih podatkov za netrgovinske namene.⁸⁵ Na področju omejene pristojnosti FTC je pravica posameznikov do varstva osebnih podatkov omejena. Drugače od nacionalnih nadzornih organov v Uniji FTC ni bila vzpostavljena za varstvo pravice posameznika do zasebnega življenja, temveč za zagotovitev poštene in zanesljive trgovine za potrošnike, kar dejansko omejuje njene zmožnosti poseganja na področje varstva osebnih podatkov. Vloga FTC torej ni primerljiva z vlogo nacionalnih nadzornih organov iz člena 28 Direktive 95/46.

206. Državljeni Unije, katerih podatki so bili preneseni, lahko za pojasnilo, ali podjetje, ki ima njihove osebne podatke, krši pogoje sistema samocertificiranja, prosijo specializirane arbitražne organe v ZDA, kot sta TRUSTe in BBBOnline. Organi, kot je TRUSTe, z zasebno arbitražo ne morejo obravnavati kršitev pravice do varstva osebnih podatkov, če so jih storile organizacije ali subjekti, ki niso med samocertificiranimi podjetji. Ti arbitražni organi nimajo nobene pristojnosti za odločanje o zakonitosti dejavnosti ameriških varnostnih agencij.

207. Niti FTC niti zasebni arbitražni organi torej niso pristojni za nadzor nad morebitnimi kršitvami načel varstva osebnih podatkov, ki so jih storili javni subjekti, kot so ameriške varnostne agencije. Vendar bi bila taka pristojnost bistvena za popolno zagotavljanje pravice do učinkovitega varstva navedenih podatkov. Komisija torej s sprejetjem Odločbe 2000/520 in ohranjanjem njene veljavnosti ni mogla ugotoviti, da za vse osebne podatke, ki bi bili preneseni v ZDA, obstaja ustrezno varstvo pravice, zagotovljene s členom 8(3) Listine, to pomeni, da bi neodvisni organ izvajal učinkovit nadzor nad spoštovanjem zahtev po varstvu in varnosti navedenih podatkov.

208. Zato je treba ugotoviti, da v ureditvi varnega pristana iz Odločbe 2000/520 ni določen neodvisni organ, ki bi lahko nadzoroval, da se izjeme od načel varnega pristana izvajajo v okviru tega, kar je nujno potrebno. Vendar, kot je bilo prikazano, je tak nadzor, ki ga izvaja neodvisni organ, glede na pravo Unije bistvena sestavina varstva posameznikov pri obdelavi osebnih podatkov.⁸⁶

209. V zvezi s tem je treba poudariti vlogo, ki jo imajo v sistemu varstva osebnih podatkov, veljavnem v Uniji, nacionalni nadzorni organi pri nadzoru nad omejitvami iz člena 13 Direktive 95/46. V skladu s členom 28(4), drugi pododstavek, navedene direktive „[v]sak nadzorni organ obravnava predvsem zahteve za preverjanje zakonitosti obdelave podatkov, ki jih vloži katera koli oseba, kadar se

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

82 — Točka 65.

83 — *Idem*.

84 — *Ibidem* (točka 66).

85 — Glej v zvezi s tem Prilogo II, FAQ 11, k Odločbi 2000/520, naslov „Ukrepi Federal Trade Commission“, ter njene Priloge III, V in VII.

86 — Glej sodbo *Digital Rights Ireland* in drugi (C-293/12 in C-594/12, EU:C:2014:238, točka 68 in navedena sodna praksa).

uporabljajo nacionalne določbe, sprejete v skladu s členom 13 navedene direktive“. Po analogiji menim, da bi moral poleg navedbe omejitev pri uporabi načel varnega pristana iz četrtega odstavka Priloge I k Odločbi 2000/520 obstajati mehanizem nadzora, ki bi ga zagotavljal specializiran neodvisen organ na področju varstva osebnih podatkov.

210. Ukrepanje neodvisnih nadzornih organov je namreč v središču evropskega sistema varstva osebnih podatkov. Zato ni nič nenavadnega, da se je obstoj takega organa že na samem začetku štel za enega od nujnih pogojev za ugotavljanje ustreznosti ravni varstva v tretjih državah. Tu gre za pogoj, da prenos podatkov z ozemlja držav članic na ozemlje tretjih držav ni prepovedan v skladu s členom 25 Direktive 95/46.⁸⁷ Kot je navedeno v dokumentu za razpravo, ki ga je sprejela delovna skupina, ustanovljena na podlagi člena 29 navedene direktive, v Evropi obstaja vsesplošno soglasje, da „je mehanizem ‚zunanjega nadzora‘, ki ga izvaja neodvisni organ, potreben pri vsakem sistemu, katerega namen je zagotoviti spoštovanje pravil o varstvu osebnih podatkov“⁸⁸.

211. Poleg tega naj poudarim, da FISC državljanom Unije, katerih osebni podatki so bili preneseni v ZDA, ne omogoča vložitve učinkovitega pravnega sredstva. Varstvo proti nadzoru, ki ga izvajajo vladne službe v okviru oddelka 702 zakona o nadzoru tujih obveščevalnih služb iz leta 1978, se namreč uporablja samo za ameriške državljane in tuje državljane, ki zakonito in stalno prebivajo v ZDA. Kot je poudarila sama Komisija, bi bilo mogoče nadzor nad ameriški programi zbiranja obveščevalnih podatkov izboljšati z okrepitevijo vloge FISC in vzpostavitev pravnih sredstev za posameznike. S temi mehanizmi bi bilo mogoče zmanjšati obseg obdelave osebnih podatkov državljanov Unije, ki niso upoštevni za zaščito nacionalne varnosti.⁸⁹

212. Komisija je poleg tega sama navedla, da državljani Unije ne morejo dostopati do podatkov, jih popravljati ali izbrisati ali imeti dostopa do upravnega ali sodnega varstva zaradi zbiranja in nadaljnje obdelave njihovih osebnih podatkov v okviru ameriških programov nadzora.⁹⁰

213. Nazadnje je treba navesti, da se lahko ameriški predpisi o varstvu zasebnega življenja različno uporabljajo za ameriške in tuje državljane.⁹¹

214. Iz navedenega izhaja, da Odločba 2000/520 ne določa jasnih in natančnih pravil, ki bi urejala obseg poseganja v temeljne pravice, določene s členoma 7 in 8 Listine. Ugotoviti je torej treba, da se z navedeno odločbo in njeno uporabo v velikem obsegu in zelo resno posega v temeljne pravice, ne da bi bilo tako poseganje natančno določeno s predpisi, s katerimi bi bilo zagotovljeno, da je to poseganje dejansko omejeno na to, kar je nujno potrebno.

215. Komisija je torej s sprejetjem Odločbe 2000/520 in nato ohranjanjem njene veljavnosti prestopila meje, ki jih nalaga spoštovanje načela sorazmernosti glede členov 7, 8 in 52(1) Listine. Temu se pridružuje ugotovitev, da gre za neupravičeno poseganje v pravico državljanov Unije do učinkovitega pravnega sredstva iz člena 47 Listine.

216. Zato menim, da je treba navedeno odločbo razglasiti za neveljavno, ker zaradi zgoraj opisanih kršitev temeljnih pravic ni mogoče šteti, da ureditev varnega pristana, ki je bila z njo uvedena, zagotavlja ustrezno raven varstva osebnih podatkov, prenesenih v okviru navedene ureditve iz Unije v Združene države.

87 — Glej Poulet, Y., „L'autorité de contrôle: ‚vues‘ de Bruxelles“, *Revue française d'administration publique*, št. 89, januar–marec 1999, str. 69 in zlasti str. 71.

88 — Glej str. 7 delovnega dokumenta Komisije WP 12, navedenega v opombi 56.

89 — Str. 10 in 11 Sporočila Komisije, navedenega v opombi 2.

90 — Glej točko 7.2, str. 20, Sporočila Komisije, navedenega v opombi 58.

91 — Glej v zvezi s tem vprašanjem Kuner, C., „Foreign Nationals and Data Protection Law: A Transatlantic Analysis“, *Data Protection Anno 2014: How To Restore Trust?* Intersentia, Cambridge, 2014, str. 213 ter zlasti str. 216 in naslednje.

217. Glede na navedeno ugotovitev, da so bile kršene temeljne pravice državljanov Unije, menim, da bi morala Komisija ustaviti izvajanje Odločbe 2000/520.

218. Navedena odločba ni časovno omejena. Vendar je iz obravnavanega primera razvidno, da se lahko ustreznost ravni varstva v tretji državi sčasoma razvija zaradi spremembe dejanskih in pravnih okoliščin, na katerih je temeljila navedena odločba.

219. Naj poudarim, da sama Odločba 2000/520 zajema določbe, v katerih je navedena možnost, da Komisija to odločbo prilagodi glede na okoliščine.

220. Iz uvodne izjave 9 tako izhaja, da „[bo] [v]arni pristan“, vzpostavljen z načeli in FAQ, [...] morda treba preveriti z vidika izkušenj in razvoja v zvezi z varstvom zasebnosti v okoliščinah, ko tehnologija vse bolj lajša prenos in obdelavo osebnih podatkov, ter z vidika poročil o uporabi, ki jih predložijo za uveljavljanje pristojni organi“.

221. V členu 3(4) navedene odločbe je poleg tega navedeno: „Če informacije, zbrane po odstavkih 1, 2 in 3, dokazujejo, da kateri koli organ, ki je v Združenih državah odgovoren za zagotavljanje skladnosti z načeli, uveljavljenimi v skladu s FAQ, njegove naloge ne opravlja učinkovito, Komisija obvesti Ministrstvo za trgovino ZDA ter po potrebi in [...] predloži osnutek ukrepov za razveljavitev ali odložitev te odločbe ali omejitev področja njene uporabe.“

222. Poleg tega člen 4(1) Odločbe 2000/520 določa, da se ta „lahko kadar koli prilagodi glede na izkušnje z njeno uporabo in/ali če zakonodaja ZDA prevzame raven zaščite, ki jo zagotavljajo načela in FAQ. Komisija v vsakem primeru oceni izvajanje sedanje odločbe na podlagi razpoložljivih informacij tri leta po uradnem obvestilu držav članic o odločbi in poroča odboru, ustanovljenemu po členu 31 Direktive 95/46[...], o vseh ustreznih ugotovitvah, vključno z vsemi dokazi, ki bi lahko vplivali na oceno, da določbe iz člena 1 te odločbe zagotavljajo ustrezno zaščito v smislu člena 25 Direktive 95/46“. V skladu s členom 4(2) Odločbe 2000/520 „Komisija po potrebi predloži osnutek ukrepov po postopku iz člena 31 [D]irektive 95/46“.

223. Komisija je v stališčih ugotovila, da „obstaja velika verjetnost, da je bila zavezanost načelom varnega pristana omejena na način, ki ni v skladu s strogo omejenimi pogoji za izjemo, določeno na področju nacionalne varnosti“⁹². V zvezi s tem ugotavlja, da „je iz zadevnih razkritij razvidna raven vsesplošnega obsežnega nadzora, ki ni združljiva z merilom potrebnosti, določenim v okviru te izjeme, niti splošneje s pravico do varstva osebnih podatkov iz člena 8 Listine“⁹³. Komisija je poleg tega sama ugotovila, da „[o]bseg [...] programov nadzora, skupaj z neenako obravnavo državljanov [Unije], postavlja pod vprašaj raven varstva, ki jo zagotavlja dogovor o varnem pristanu“⁹⁴.

224. Komisija je poleg tega na obravnavi izrecno priznala, da v okviru Odločbe 2000/520, kakršna se zdaj uporablja, ni jamstva, da bo zagotovljena pravica državljanov Unije do varstva navedenih podatkov. Vendar po njenih navedbah na podlagi te ugotovitve ni mogoče razveljaviti navedene odločbe. Čeprav se Komisija strinja s trditvijo, da mora v primeru novih okoliščin ukrepati, meni, da je sprejela ustrezne in sorazmerne ukrepe, s tem ko naj bi začela pogajanja z ZDA za spremembo ureditve varnega pristana.

225. S tem se ne strinjam. V vmesnem času bi namreč morala obstajati možnost, da se prenosi osebnih podatkov v ZDA na pobudo nacionalnih nadzornih organov ali na podlagi pri njih vloženi pritožbi prekinijo.

92 — Točka 44

93 — *Idem*.

94 — Glej str. 5 Sporočila Komisije, navedenega v opombi 2.

226. Poleg tega menim, da bi morala Komisija zaradi takih ugotovitev ustaviti izvajanje Odločbe 2000/520. Cilj varstva osebnih podatkov, določen v Direktivi 95/46 in členu 8 Listine, namreč nalaga obveznosti ne le državam članicam, temveč tudi institucijam Unije, kot je to razvidno iz člena 51(1) Listine.

227. Komisija mora pri presoji ravni varstva v tretji državi preučiti ne le notranjo zakonodajo in mednarodne obveznosti te tretje države, temveč tudi način, na katerega se varstvo osebnih podatkov zagotavlja v praksi. Če se pri preučitvi prakse odkrijejo nepravilnosti, mora Komisija ukrepati ter po potrebi nemudoma začasno zadržati izvajanje svoje odločbe in/ali jo prilagoditi.

228. Kot je bilo prikazano v zgornjih premislekih, je obveznost držav članic zlasti ta, da z ukrepi svojih nacionalnih nadzornih organov zagotovijo spoštovanje pravil iz Direktive 95/46.

229. Obveznost Komisije je, da v času pogajanj z zadevno tretjo državo, pri kateri so bile odkrite nepravilnosti, ustavi izvajanje odločbe, ki jo je sprejela na podlagi člena 25(6) navedene direktive, da bi se te pravilnosti odpravile.

230. Naj spomnim, da je namen odločbe, ki jo sprejme Komisija na podlagi navedene določbe, ugotoviti, da tretja država „zagotavlja“ ustrezno raven varstva osebnih podatkov, prenesenih vanjo. Izraz „zagotavlja“ v sedanjiku kaže na to, da se mora navedena odločba za ohranitev veljavnosti nanašati na tretjo državo, ki po sprejetju navedene odločbe še naprej zagotavlja tako ustrezno raven varstva.

231. V skladu z uvodno izjavo 57 Direktive 95/46 „se mora [...] prepovedati prenos osebnih podatkov v tretjo državo, ki ne zagotavlja primerne ravni varstva“.

232. Člen 25(4) navedene direktive določa: „Kadar Komisija na podlagi postopka iz člena 31(2) ugotovi, da tretja država ne zagotavlja ustrezne ravni varstva v smislu odstavka 2 tega člena, države članice sprejmejo ukrepe, ki so potrebni za preprečevanje kakršnih koli prenosov podatkov iste vrste v to tretjo državo.“ Poleg tega člen 25(5) te direktive določa: „Ko je ustrezno, Komisija začne pogajanja glede ureditve položaja, ki izhaja iz ugotovitve po odstavku 4.“

233. Iz te zadnje določbe izhaja, da je v sistemu, vzpostavljenem s členom 25 navedene direktive, namen pogajanj, začeti s tretjo državo, odpraviti neustrezno raven varstva, ugotovljeno v skladu s postopkom iz člena 31(2) Direktive 95/46. Komisija v obravnavanem primeru ni v skladu z navedenim postopkom uradno ugotovila, da navedena ureditev varnega pristana ni več zagotavljala ustrezne ravni varstva. Vendar, če se je Komisija odločila, da bo začela pogajanja z ZDA, je morala najprej meniti, da raven v tej tretji državi ni bila ustrezna.

234. Čeprav je Komisija vedela za nepravilnosti pri izvajanju Odločbe 2000/520, ni začasno zadržala njenega izvajanja niti je ni prilagodila, s čimer je omogočila nadaljnje kršenje temeljnih pravic oseb, katerih osebni podatki so bili preneseni in se še vedno prenašajo v okviru ureditve varnega pristana.

235. Čeprav seveda v drugih okoliščinah, je Sodišče že razsodilo, da mora Komisija poskrbeti za prilagoditev ureditve novim podatkom.⁹⁵

236. Tako neukrepanje Komisije, ki neposredno krši temeljne pravice iz členov 7, 8 in 47 Listine, je po mojem mnenju v okviru tega predloga za sprejetje predhodne odločbe dodaten razlog za razglasitev neveljavnosti Odločbe 2000/520.⁹⁶

95 — Glej v zvezi s tem sodbo Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, točka 40).

96 — Čeprav je Sodišče v sodbi T. Port (C-68/95, EU:C:1996:452) razsodilo, da „Pogodba ni določala možnosti za vložitev predloga za sprejetje predhodne odločbe, s katerim bi nacionalno sodišče prosilo Sodišče, naj predhodno odloči o upravni opustitvi“ (točka 53), se zdi, da je zavzelo bolj naklonjeno stališče do te možnosti v sodbi Ten Kate Holding Musselkanaal in drugi (C-511/03, EU:C:2005:625, točka 29).

III – Predlog

237. Ob upoštevanju navedenih ugotovitev Sodišču predlagam, naj na vprašanja, ki jih je postavilo High Court of Justice, odgovori:

Člen 28 Direktive 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov v povezavi s členoma 7 in 8 Listine Evropske unije o temeljnih pravicah je treba razlagati tako, da obstoj odločbe, ki jo je sprejela Evropska komisija na podlagi člena 25(6) Direktive 95/46, ne učinkuje tako, da nacionalnemu nadzornemu organu preprečuje, da preuči pritožbo, s katero se očita, da tretja država ne zagotavlja ustrezne ravni varstva prenesenih osebnih podatkov, in po potrebi prekine prenos teh podatkov.

Odločba Komisije 2000/520 z dne 26. julija 2000 v skladu z Direktivo 95/46 Evropskega parlamenta in Sveta 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, ni veljavna.