ĢENERĀLADVOKĀTA ĪVA BOTA [*YVES BOT*]
SECINĀJUMI,
sniegti 2015. gada 23. septembrī[1]

Lieta C-362/14

Maximillian Schrems
pret
Data Protection Commissioner

(Augstās tiesas (High Court, Īrija) lūgums sniegt prejudiciālu nolēmumu)

Lūgums sniegt prejudiciālu nolēmumu — Personas dati — Fizisko personu aizsardzība attiecībā uz šo datu apstrādi — Eiropas Savienības Pamattiesību harta — 7., 8. un 47. pants — Direktīva 95/46/EK — 25. pants — Lēmums 2000/520/EK — Personas datu pārsūtīšana uz Amerikas Savienotajām Valstīm — Aizsardzības līmeņa pienācīguma novērtēšana — Fiziskas personas, kuras personas dati tikuši pārsūtīti uz trešo valsti, sūdzība — Valsts uzraudzības iestāde — Pilnvaras

I – **Ievads**

1. Kā Eiropas Komisija ir konstatējusi savā 2013. gada 27. novembra paziņojumā[2], "personas datu pārsūtīšana ir svarīgs un nepieciešams transatlantisko attiecību elements. Tā ir neatņemama daļa savstarpējā tirdzniecībā pāri Atlantijas okeānam, tostarp tādās jaunās, augošās digitālās uzņēmējdarbības jomās kā, piemēram, sociālie plašsaziņas līdzekļi vai mākoņdatošana, kā ietvaros no Eiropas Savienības uz Amerikas Savienotajām Valstīm tiek pārsūtīts liels datu apjoms"[3].

2. Komisijas 2000. gada 26. jūlija lēmums atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi Amerikas Savienoto Valstu Tirdzniecības ministrija[4], attiecas uz komerctirdzniecību. Minētais lēmums nodrošina juridisko pamatu personas datu pārsūtīšanai no Savienības Amerikas Savienotajās Valstīs reģistrētajiem uzņēmumiem, kuri ir apņēmušies ievērot "drošības zonas" principus.

3. Pašlaik minētā lēmuma izaicinājums ir atļaut datu plūsmu starp Savienību un Amerikas Savienotajām Valstīm, garantējot augstu šo datu aizsardzības līmeni atbilstoši Savienības tiesībās izvirzītajām prasībām.

4. Nesen vairākos paziņojumos tika norādīts, ka ASV ir izveidotas plaša mēroga informācijas vākšanas programmas. Šie paziņojumi izraisīja bažas par Savienības tiesību ievērošanu, Amerikas Savienotajās Valstīs reģistrētajiem uzņēmumiem pārsūtot personas datus, un par "drošības zonas" režīma trūkumiem.

1 — Oriģinālvaloda – franču.

2 — Komisijas Paziņojums Eiropas Parlamentam un Padomei "Uzticēšanās atjaunošana datu plūsmām starp Eiropas Savienību un Amerikas Savienotajām Valstīm" (COM(2013) 846 *final*).

3 — 2. lpp.

4 — OV L 215, 7. lpp., un labojums – OV 2001, L 115, 14. lpp.

5. Ar šo lūgumu sniegt prejudiciālu nolēmumu Tiesa ir aicināta precizēt, kā ir jārīkojas valsts uzraudzības iestādēm un Komisijai, kad tās saskaras ar traucējumiem Lēmuma 2000/520 piemērošanā.

6. Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [5] IV nodaļā ir paredzētas tiesību normas par personas datu pārsūtīšanu uz trešajām valstīm.

7. Šajā nodaļā, šīs direktīvas 25. panta 1. punktā, ir noteikts princips, saskaņā ar kuru tādu personas datu pārsūtīšana, kuri atrodas apstrādē vai ir paredzēti apstrādei pēc pārsūtīšanas, var notikt tikai tad, ja attiecīgā trešā valsts nodrošina pienācīgu šo datu aizsardzības līmeni.

8. Un otrādi –, kā minētās direktīvas preambulas 57. apsvērumā ir norādījis Savienības likumdevējs, personu datu pārsūtīšana uz trešo valsti, kas nenodrošina pienācīgu aizsardzības līmeni, ir jāaizliedz.

9. Saskaņā ar Direktīvas 95/46 25. panta 2. punktu "trešās valsts sniegtās aizsardzības līmeņa pienācīgums ir jānovērtē, paturot prātā visus ar datu pārsūtīšanas darbību vai datu pārsūtīšanas darbību kopumu cieši saistītos apstākļus; jo īpaši jāapsver datu raksturs, ierosinātās apstrādes darbības vai darbību nolūks un ilgums, izcelsmes valsts un valsts, kura ir galamērķis, attiecīgajā trešajā valstī spēkā esošās gan vispārējo, gan nozaru tiesību normas un šajā valstī ievērotie profesionālie noteikumi un drošības pasākumi".

10. Saskaņā ar šīs direktīvas 25. panta 6. punktu Komisija, ņemot vērā trešās valsts tiesību aktus un tās starptautiskās saistības var konstatēt, ka tā nodrošina pienācīgu personas datu aizsardzības līmeni. Ja Komisija šajā ziņā pieņem lēmumu, personas datus uz attiecīgo trešo valsti drīkst pārsūtīt.

11. Piemērojot šo tiesību normu, Komisija ir pieņēmusi Lēmumu 2000/520. No šī lēmuma 1. panta 1. punkta izriet, ka "privātuma "drošības zonas" principi", kas tiek īstenoti atbilstīgi "visbiežāk uzdotajos jautājumos" [6] sniegtajiem norādījumiem, tiek uzskatīti par tādiem, kas nodrošina pienācīgu to personas datu aizsardzības līmeni, kas no Savienības tiek pārsūtīti Amerikas Savienotajās Valstīs reģistrētajiem uzņēmumiem.

12. Tādējādi ar Lēmumu 2000/520 ir atļauta personas datu pārsūtīšana no dalībvalstīm tādiem uzņēmumiem Amerikas Savienotajās Valstīs, kas ir apņēmušies ievērot "drošības zonas" principus.

13. Lēmuma 2000/520 I pielikumā ir norādīts, ka dažiem principiem, kurus uzņēmumi var pieņemt labprātīgi, piemīt ierobežojumi, un ir paredzēta īpaša uzraudzības sistēma. 2013. gadā tā saukto "uzvedības kodeksu" bija pieņēmuši vairāk nekā 3200 uzņēmumu.

14. "Drošības zonas" režīma pamatā ir risinājums, kurā ir apvienota privāto uzņēmumu pašsertifikācija, kā arī pašnovērtējums un valsts varas iejaukšanās.

15. "Drošības zonas" principi tika izstrādāti, "apspriežoties ar nozares uzņēmumiem un plašu sabiedrību, lai veicinātu tirdzniecību starp Amerikas Savienotajām Valstīm un [..] Savienību. Ir paredzēts, ka tos izmantos tikai tās ASV organizācijas, kas personas datus saņem no [..] Savienības un kuras izpilda "drošības zonas" nosacījumus, un uz kurām tādējādi var attiecināt no tās izrietošo pieņēmumu par "atbilstību"" [7].

5 — OV L 281, 31. lpp. Direktīva, kurā grozījumi izdarīti ar Eiropas Parlamenta un Padomes 2003. gada 29. septembra Regulu (EEK) Nr. 1882/2003 (OV L 284, 1. lpp.; turpmāk tekstā – "Direktīva 95/46").

6 — *Frequently asked questions* [visbiežāk uzdotie jautājumi] (turpmāk tekstā – "*FAQ*").

7 — Lēmuma 2000/520 I pielikuma otrā daļa.

16. Lēmuma 2000/520 I pielikumā noteiktajos "drošības zonas" principos it īpaši ir paredzēts:

— informēšanas pienākums, saskaņā ar kuru "[katrai] organizācijai jāinformē indivīdi par to, kādiem mērķiem tā vāc un izmanto informāciju par viņiem, kādā veidā var vērsties pie organizācijas ar jautājumiem vai sūdzībām, kāda veida trešām personām tā izpauž informāciju un kādas ir izvēles iespējas un līdzekļi, ko organizācija indivīdiem piedāvā, lai ierobežotu informācijas izmantošanu un izpaušanu. Paziņojumu [..] nosūta indivīdiem, pirmo reizi lūdzot tos sniegt personisko informāciju organizācijai, vai, cik drīz vien iespējams, pēc tam, bet jebkurā gadījumā, pirms organizācija šādu informāciju izmanto citiem mērķiem, izņemot tos, kuriem nosūtītāja organizācija to sākotnēji ievākusi vai apstrādājusi, vai to pirmo reizi izpaudusi trešai personai" [8];

— organizācijai indivīdiem jāpiedāvā iespēja izvēlēties, vai viņu personas dati var tikt izpausti trešai personai vai izmantoti mērķim, kas ir nesavienojams ar mērķiem, kuriem tā sākotnēji ievākta vai indivīds pēc tam atļāvis to izmantot. Attiecībā uz sensitīvu informāciju "ir vajadzīga personas piekrītoša vai skaidra (atļaujoša) izvēle, ja informāciju izpaudīs trešai personai vai izmantos citam mērķim izņemot tos, kuriem tā sākotnēji ievākta vai indivīds pēc tam atļāvis [to] izmantot, izdarot izvēli" [9];

— normas attiecībā uz personas datu pārsūtīšanu. Tādējādi, "izpaužot informāciju trešai personai, organizācijām jāpiemēro informēšanas un izvēles principi" [10];

— attiecībā uz datu drošību "organizācijām, kas izveido, uztur, izmanto vai izplata personisko informāciju, jāveic [..] drošības pasākumi, lai to aizsargātu no pazaudēšanas, ļaunprātīgas izmantošanas, neatļautas piekļuves, izpaušanas, izmainīšanas un iznīcināšanas" [11];

— attiecībā uz datu integritāti, "ciktāl tas ir vajadzīgs šiem mērķiem [..], organizācijai jāveic samērīgi pasākumi, lai nodrošinātu, ka dati saistībā ar paredzētajiem mērķiem ir ticami, precīzi, pilnīgi un aktuāli" [12];

— personai ir "jābūt piekļuvei personiskajai informācijai par [viņu], kas ir organizācijas rīcībā, un iespējai šo informāciju labot, mainīt vai dzēst, ja tā ir neprecīza" [13];

— pienākums paredzēt "mehānismus, lai nodrošinātu ["drošības zonas"] principu ievērošanu, to indivīdu tiesību aizsardzību, uz kuriem dati attiecas un kurus ir ietekmējusi principu neievērošana, un sekas organizācijai, ja principi nav ievēroti" [14].

17. ASV organizācijai, kas vēlas ievērot "drošības zonas" principus, savā privātās dzīves aizsardzības politikā ir jānorāda, ka tā ievēro un faktiski piemēro šos principus, kā arī ir jāveic pašsertifikācija, t.i., jāpaziņo Amerikas Savienoto Valstu Tirdzniecības ministrijai, ka tā ievēro minētos principus [15].

8 — Skat. I pielikuma sadaļu "Informēšana".

9 — Skat. I pielikuma sadaļu "Izvēle".

10 — Skat. I pielikuma sadaļu "Tālāka pārsūtīšana".

11 — Skat. I pielikuma sadaļu "Drošība".

12 — Skat. I pielikuma sadaļu "Datu integritāte".

13 — Skat. I pielikuma sadaļu "Piekļuve".

14 — Skat. I pielikuma sadaļu "Piemērošana".

15 — Lēmuma 2000/520 1. panta 2. un 3. punkts. Skat. arī II pielikumu, *FAQ* 6.

18. Organizācijas par "drošības zonas" principu ievērošana var tikt paziņota dažādos veidos. Tādējādi, piemēram, tās var "pievieno[tie]s kādai privātā sektora noteiktai pašregulatīvai slepenības [konfidencialitātes aizsardzības] programmai", kurā ir ievēroti šie principi, vai arī iekļaut "drošības zonas" [principus], "izstrādājot savus [noteikumus datu aizsardzības jomā], ja [tie] atbilst [minētajiem] principiem. [..] Turklāt organizācijas, uz ko attiecas tādi normatīvie akti, administratīvie akti vai citi tiesību akti vai noteikumi, kuri efektīvi aizsargā personu privāto dzīvi [nodrošina efektīvu personas datu aizsardzību], arī var pretendēt uz "drošības zonas" priekšrocībām" [16].

19. Lai pārbaudītu, vai tiek ievēroti "drošības zonas" principi, ir izveidoti vairāki mehānismi, kas ietver strīdu izšķiršanu privātā kārtā un valsts iestāžu uzraudzību. Tādējādi uzraudzību var nodrošināt neatkarīgas trešās personas, izmantojot strīdu izšķiršanas ārpustiesas kārtībā sistēmu. Turklāt uzņēmumi var apņemties sadarboties ar Savienības grupu, kas darbojas datu aizsardzības jomā. Visbeidzot, kompetence izskatīt sūdzības ir Federālajai tirdzniecības komisijai (*Federal Trade Commission*, turpmāk tekstā – "*FTC*"), pamatojoties uz pilnvarām, kas tai piešķirtas saskaņā ar Federālās tirdzniecības komisijas likuma (*Federal Trade Commission Act*) 5. pantu, kā arī Transporta ministrijai (*Department of Transportation*), pamatojoties uz pilnvarām, kas tai piešķirtas saskaņā ar Amerikas Savienoto Valstu kodeksa (*United States Code*) 41712. sadaļas 49. nodaļu.

20. Saskaņā ar Lēmuma 2000/520 I pielikuma ceturto daļu apņemšanos ievērot "drošības zonas" principi var tikt ierobežoti, it īpaši, "lai ievērotu [Amerikas Savienoto Valstu] valsts drošību, sabiedrības intereses un likumus", un "ar likumu, valdības noteikumiem vai tiesu praksi, kas rada pretrunīgus pienākumus vai paredz skaidras atļaujas, ja, izmantojot šādu atļauju, organizācija var pierādīt, ka principu neievērošana ir tikai tiktāl, ciktāl ir vajadzīgs, lai ievērotu sevišķi svarīgas likumīgās intereses, kuras izriet no šādas atļaujas" [17].

21. Turklāt, lai dalībvalstu kompetentās iestādes varētu apturēt datu plūsmu, ir jāievēro vairāki Lēmuma 2000/520 3. panta 1. punktā paredzētie nosacījumi.

22. Šis lūgums sniegt prejudiciālu nolēmumu ir pamats jautājumam par Lēmuma 2000/520 tvērumu, ņemot vērā Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 7., 8. un 47. pantu, kā arī Direktīvas 95/46 25. panta 6. punktu un 28. pantu. Šis lūgums tika iesniegts saistībā ar strīdu starp *M. Schrems* un *Data Protection Commissioner* (Datu aizsardzības komisārs, turpmāk tekstā – "komisārs") attiecībā uz pēdējā minētā atteikumu izskatīt *M. Schrems* sūdzību par to, ka *Facebook Ireland Ltd*. (turpmāk tekstā – "*Facebook Ireland*") uzglabā lietotāju personas datus serveros, kas atrodas Amerikas Savienotajās Valstīs.

23. *M. Schrems* ir Austrijas pilsonis un dzīvo Austrijā. Viņš ir sociālā tīkla *Facebook* lietotājs kopš 2008. gada.

24. Visiem *Facebook* lietotājiem, kas dzīvo Savienības teritorijā, tiek lūgts parakstīt līgumu ar *Facebook Ireland* – mātesuzņēmuma *Facebook Inc*., kura mītne ir Amerikas Savienotajās Valstīs (turpmāk tekstā – "*Facebook USA*"), meitasuzņēmumu. Visi *Facebook Ireland* lietotāju, kas dzīvo Savienības teritorijā, dati vai daļa no tiem tiek pārsūtīti uz *Facebook USA* serveriem, kas atrodas Amerikas Savienoto Valstu teritorijā, kur tie tiek uzglabāti.

25. 2013. gada 25. jūnijā *M. Schrems* iesniedza sūdzību komisāram, būtībā apgalvojot, ka Amerikas Savienoto Valstu tiesības un prakse nenodrošina nekādu faktisku Amerikas Savienoto Valstu teritorijā uzglabāto datu aizsardzību pret valsts uzraudzību. Tas izrietot no *E. Snowden* 2013. gadā atklātās informācijas par Amerikas Savienoto Valstu izlūkdienestu un, it īpaši, Valsts Drošības aģentūras (*National Security Agency*, turpmāk tekstā – "*NSA*") darbību.

16 — I pielikuma trešā daļa.

17 — Skat. arī IV pielikuma B punktu.

26. No šīs atklātās informācijas it īpaši izrietot, ka *NSA* esot izveidojusi programmu ar nosaukumu "PRISM", kuras īstenošanai šī aģentūra esot ieguvusi brīvu piekļuvi datiem, kas tiek uzglabāti Amerikas Savienotajās Valstīs, serveros, kuri pieder vai kurus uzrauga virkne tādu sabiedrību, kas darbojas Interneta un tehnoloģiju jomā, kā *Facebook USA*.

27. Komisārs uzskatīja, ka tam nav jāizskata sūdzība, jo tai neesot juridiskā pamata. Viņš uzskatīja, ka nav nekādu pierādījumu, ka *NSA* būtu piekļuvusi *M. Schrems* datiem. Turklāt, viņaprāt, sūdzība bijusi jānoraida, pamatojoties uz Lēmumu 2000/520, ar kuru Komisija ir konstatējusi, ka Amerikas Savienotās Valstis, īstenojot "drošības zonas" režīmu, nodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni. Visi jautājumi par šo datu aizsardzības pienācīgumu Amerikas Savienotajās Valstīs esot jārisina saskaņā ar šo lēmumu, kas tam liedzot izskatīt sūdzībā norādīto problēmu.

28. Komisārs sūdzību noraidīja, pamatojoties uz šādiem turpinājumā minētiem valsts tiesību aktiem.

29. Ar 1988. gada Likuma par datu aizsardzību (*Data Protection Act 1988*), kas ticis grozīts ar 2003. gada Likumu par datu aizsardzību (*Data Protection (Amendment) Act 2003*, turpmāk tekstā – "Likums par datu aizsardzību"), 10. panta 1. punktu tam esot piešķirtas pilnvaras izskatīt sūdzības, un tajā esot noteikts:

"a) Komisārs var pārbaudīt vai uzdot pārbaudīt, vai šī likuma tiesību normas par personas datiem tikušas, ir vai var tikt pārkāptas, ja šī persona iesniedz tam sūdzību par kādas no šīm tiesību normām pārkāpumu vai ja komisārs uzskata, ka šāds pārkāpums varētu pastāvēt.

b) Ja šī persona iesniedz komisāram sūdzību saskaņā ar šī punkta a) apakšpunktu, komisārs:

i) izskata vai uzdod izskatīt sūdzību, ja vien viņš nesecina, ka tā ir nepamatota vai ļaunprātīga, un,

ii) ja viņš vai viņa saprātīgā termiņā nevar nodrošināt, ka attiecīgie lietas dalībnieki panāk izlīgumu saistībā ar sūdzības priekšmetu, viņš rakstveidā paziņo sūdzības iesniedzējam attiecībā uz sūdzību pieņemto lēmumu, norādot, ka, ja sūdzības iesniedzējam ir iebildumi pret šo lēmumu, viņš var celt pret to prasību tiesā saskaņā ar šī likuma 26. pantu 21 dienas laikā no šī paziņojuma saņemšanas brīža."

30. Izskatāmajā lietā komisārs secināja, ka *M. Schrems* sūdzība ir "nepamatota vai ļaunprātīga" tādējādi, ka tā nav pieņemama, jo tai nav juridiska pamata. Tāpēc tas atteicās izskatīt šo sūdzību.

31. Likuma par datu aizsardzību 11. pantā ir reglamentēta personas datu pārsūtīšana ārpus valsts teritorijas. Tā 11. panta 2. punkta a) apakšpunktā ir paredzēts:

"Kad jebkurā procedūrā, kuru reglamentē šis likums, rodas jautājums:

i) lai noteiktu, vai valstī vai teritorijā, kas atrodas ārpus Eiropas Ekonomikas zonas [(EEZ)], uz kuru šie personas dati tiks pārsūtīti, ir nodrošināts šī panta 1. punktā noteiktais pienācīgais aizsardzības līmenis, un

ii) attiecībā uz šāda veida pārsūtīšanu ir sniegts Savienības atzinums,

jautājumu atrisina saskaņā ar šo atzinumu."

32. Likuma par datu aizsardzību 11. panta 2. punkta b) apakšpunktā Savienības atzinuma jēdziens ir definēts šādi:

"Šī punkta a) apakšpunktā minētais "Savienības atzinums" nozīmē Komisijas atzinumu saskaņā ar Direktīvas [95/46] 25. panta 4. vai 6. punktu [šīs direktīvas] 31. panta 2. pantā paredzētajā procedūrā, kas veikta, lai noteiktu, vai valstī vai teritorijā ārpus EEZ šī panta 1. punktā noteiktais pienācīgais līmenis ir nodrošināts."

33. Komisārs norādīja, ka Lēmums 2000/520 ir "Savienības atzinums" Likuma par datu aizsardzību 11. panta 2. punkta a) apakšpunkta izpratnē, tādējādi saskaņā ar šo likumu jebkurš jautājums par aizsardzības līmeņa pienācīgumu trešajā valstī, uz kuru dati ir pārsūtīti, ir jārisina saskaņā ar šo konstatējumu. Ciktāl runa bija *M. Schrems* sūdzības būtību, proti, par to, ka personas dati tikuši pārsūtīti uz trešo valsti, kas praksē nenodrošinot atbilstīgu aizsardzības līmeni, komisārs uzskatīja, ka, ņemot vērā paša Lēmuma 2000/520 būtību un esamību, viņš nevar izskatīt šo jautājumu.

34. *M. Schrems* par šo komisāra lēmumu noraidīt viņa sūdzību cēla prasību Augstajā tiesā (*High Court*). Izskatījusi pamatlietā sniegtos pierādījumus, šī tiesa konstatēja, ka personas datu elektroniskā uzraudzība un pārtveršana atbilst nepieciešamiem un būtiskiem sabiedrības interešu mērķiem, proti, uzturēt valsts drošību un novērst smagus noziegumus. Augstā tiesa šajā ziņā norāda, ka no Savienības uz Amerikas Savienotajām Valstīm pārsūtīto datu uzraudzība un pārtveršana tiek veikta, lai īstenotu objektīvus leģitīmus mērķus, kas ir saistīti ar terorisma apkarošanu.

35. Saskaņā ar šīs tiesas viedokli *E. Snowden* atklātā informācija tomēr pierādīja, ka *NSA* un citas līdzīgas iestādes ir pieļāvušas būtiskas pārmērības. Lai arī *Foreign Intelligence Surveillance Court* (turpmāk tekstā – "*FISC*"), kas iesaistās saskaņā ar 1978. gada Likumu par ārvalstu izlūkošanas uzraudzību (*Foreign Intelligence Surveillance Act of 1978*) [18], veic uzraudzību, tomēr tiesvedība tajā norisinoties slepeni un, neievērojot sacīkstes principu. Turklāt papildus tam, ka lēmumi par piekļuvi personas datiem esot pieņemti saskaņā ar Amerikas Savienoto Valstu tiesībām, Savienības pilsoņiem neesot nekādu efektīvu tiesību tikt uzklausītiem jautājumā par viņu datu uzraudzību un pārtveršanu.

36. No šī apjomīgā dokumenta, kas ir pievienots oficiālajiem paziņojumiem izskatāmajā lietā, izrietot, ka liela daudzuma *E. Snowden* atklātās informācijas precizitāte nav tikusi apstrīdēta. Tāpēc Augstā tiesa secināja, ka tad, kad personas dati ir pārsūtīti uz Amerikas Savienotajām Valstīm, *NSA*, kā arī citas ASV drošības aģentūras, tādas kā Federālais izmeklēšanas birojs (*Federal Bureau of Investigation (FBI)*), tiem var piekļūt, veicot plašu un nediferencētu datu uzraudzību un pārtveršanu.

37. Augstā tiesa konstatēja, ka Īrijas tiesībās, ņemot vērā konstitucionālo tiesību uz privātās dzīves un dzīvesvietas neaizskaramību nozīmīgumu, tiek prasīts, lai jebkura iejaukšanās šajās tiesībās atbilstu tiesību aktos paredzētajām prasībām. Plaša un nediferencēta piekļuve personas datiem pilnībā neatbilstu samērīguma prasībai un tātad būtu jāuzskata par nesaderīgu ar Īrijas konstitūciju [19].

38. Augstā tiesa norādīja, ka, lai elektronisko komunikāciju pārtveršana varētu tikt uzskatīta par konstitucionālu, esot jāpierāda, ka konkrētu personu vai konkrētu personu grupu komunikāciju pārtveršana un uzraudzība ir objektīvi pamatota ar valsts drošības interesēm un noziedzības apkarošanu un ka tam ir pienācīgas un pārbaudāmas garantijas.

18 — Skat. šī likuma, kas ir grozīts ar 2008. gada likumu (*Foreign Intelligence Surveillance Act of 2008*), 702. sadaļu. Piemērojot šo sadaļu, *NSA* uztur datu bāzi, kas ir pazīstama ar nosaukumu "PRISM" (skat. 2013. gada 27. novembra *Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection*.

19 — Augstā tiesa it īpaši atsaucas uz cilvēka cieņas un personas brīvības ievērošanu (preambula), personisko autonomiju (40. panta 3. punkta 1. un 2. apakšpunkts), dzīvesvietas neaizskaramību (40. panta 5. punkts) un ģimenes dzīves aizsardzību (41. pants).

39. Tādējādi Augstā tiesa norādīja, ka, ja izskatāmā lieta būtu jāizskata tikai saskaņā ar Īrijas tiesībām, rastos būtisks jautājums par to, vai Amerikas Savienotās Valstis "nodrošina pienācīgu privātās dzīves, kā arī pamattiesību un pamatbrīvību aizsardzības līmeni" Likuma par datu aizsardzību 11. panta 1. punkta izpratnē. No tā izriet, ka saskaņā ar Īrijas tiesībām un, it īpaši, tās konstitucionālajām prasībām komisārs neesot varējis noraidīt *M. Schrems* sūdzību, bet tam esot bijis jāizskata šis jautājums.

40. Katrā ziņā Augstā tiesa konstatēja, ka lieta, kuru tā izskata, attiecas uz Savienības tiesību īstenošanu Hartas 51. panta 1. punkta izpratnē, jo komisāra lēmuma tiesiskums esot jāizvērtē saskaņā ar Savienības tiesībām.

41. Problēmu, ar kuru saskārās komisārs, Augstā tiesa ir izskaidrojusi šādi. Saskaņā ar Likuma par datu aizsardzību 11. panta 2. punkta a) apakšpunktu jautājums par atbilstīgu aizsardzību trešajā valstī komisāram ir jāizskata "saskaņā" ar Savienības atzinumu, ko veikusi Komisija saskaņā ar Direktīvas 95/46 25. panta 6. punktu. No tā izrietot, ka komisārs nevarot neņemt vērā šo atzinumu. Tā kā Komisija Lēmumā 2000/520 ir konstatējusi, ka Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni attiecībā uz uzņēmumu, kas apņēmušies ievērot "drošības zonas" principus, veikto datu apstrādi, sūdzība par šādas aizsardzības nepienācīgumu komisāram obligāti esot jānoraida.

42. Konstatējusi, ka komisārs tādējādi skrupulozi ir ievērojis Direktīvu 95/46 un Lēmumu 2000/520, Augstā tiesa norāda, ka *M. Schrems* faktiski drīzāk iebilst pret "drošības zonas" režīma noteikumiem, nevis pret veidu, kādā komisārs tos piemērojis, un uzsver, ka viņš tieši nav apstrīdējis nedz Direktīvas 95/46, nedz Lēmuma 2000/520 spēkā esamību.

43. Tātad Augstās tiesas ieskatā būtiski būtu noskaidrot, vai, ņemot vērā Savienības tiesības un, it īpaši, to, ka vēlāk stājās spēkā Hartas 7. un 8. pants, komisāram obligāti ir jāievēro Komisijas atzinums Lēmumā 2000/520 attiecībā uz Amerikas Savienoto Valstu tiesību un prakses atbilstību personas datu aizsardzības jomā.

44. Augstā tiesa arī precizē, ka prasībā, kuru tā izskata, nav neviena iebilduma pret *Facebook Ireland* un *Facebook USA* darbību kā tādu. Tomēr saskaņā ar šīs tiesas viedokli Lēmuma 2000/520 3. panta 1. punkta b) apakšpunkts, ar kuru kompetentajām valsts iestādēm ir atļauts likt uzņēmumam apturēt datu plūsmu uz trešo valsti, esot piemērojams tikai tad, kad ir iesniegta sūdzība par attiecīgā uzņēmuma rīcību, – bet tā tas nav izskatāmajā lietā.

45. Tāpēc Augstā tiesa uzsver, ka īstais iebildums ir nevis pret *Facebook USA* rīcību kā tādu, bet drīzāk pret to, ka Komisija ir uzskatījusi, ka Amerikas Savienoto Valstu tiesības un prakse datu aizsardzības jomā nodrošina pienācīgu aizsardzību, lai arī *E. Snowden* atklātā informācija skaidri atspoguļo, ka Amerikas Savienoto Valstu iestādēm ir iespējama plaša un nediferencēta piekļuve Savienības iedzīvotāju personas datiem [20].

46. Šajā jautājumā Augstā tiesa uzskata, ka ir grūti iztēloties, kā Lēmums 2000/520 praksē varētu būt saderīgs ar Hartas 7. un 8. pantu, it īpaši, ja tiek ņemti vērā principi, kurus Tiesa ir formulējusi savā spriedumā *Digital Rights Ireland* u.c. [21]. Ja valsts iestādēm tiktu atļauts vispārēji un izlases veidā piekļūt elektroniskajām komunikācijām, nenorādot objektīvu pamatojumu, kas ir balstīts uz valsts drošības vai noziedzības novēršanas apsvērumiem, kas savukārt it īpaši ir saistīti ar attiecīgajiem indivīdiem, un nesniegt nekādas pienācīgas vai pārbaudāmas garantijas, tiktu apdraudēta Hartas 7. pantā paredzētā garantija un dalībvalstu tradīciju būtiskās kopējās vērtības. Tā kā *M. Schrems* prasībā esot norādīts, ka

20 — Augstā tiesa šajā ziņā norāda, ka *M. Schrems* galvenais pamats attiecas uz to, ka, ņemot vērā informāciju, kuru nesen atklāja *E. Snowden*, un to, ka plaša mēroga personas dati tikuši nodoti Amerikas Savienoto Valstu izlūkdienestu rīcībā, komisārs nevarēja lietderīgi secināt, ka trešajā valstī ir pienācīgs šo datu aizsardzības līmenis.

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

Lēmums 2000/520 *in abstracto* varētu nebūt saderīgs ar Hartas 7. un 8. pantu, Tiesa varētu uzskatīt, ka Direktīvu 95/46 un, it īpaši, tās 25. panta 6. punktu, kā arī Lēmumu 2000/520 ir iespējams interpretēt tādējādi, ka valsts iestādēm ar tiem ir atļauts veikt savu izmeklēšanu, lai konstatētu, vai personas datu pārsūtīšana uz trešo valsti un to uzglabāšana atbilst Hartas 7. un 8. pantā izvirzītajām prasībām.

47. Šādos apstākļos Augstā tiesa nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

"Vai, izskatot sūdzību, kas ir iesniegta komisāram, par to, ka personas dati tiek nosūtīti uz trešo valsti (šajā gadījumā – uz Amerikas Savienotajām Valstīm), kuras tiesību akti un prakse, kā tiek apgalvots, nenodrošina pienācīgu datu subjekta aizsardzību, šai amatpersonai tomēr ir pilnībā saistošs Komisijas atzinums par pretējo, kas ir pausts Lēmumā 2000/520, ņemot vērā Hartas 7., 8. un 47. pantu un Direktīvas 95/46 25. panta 6. punktu?

Vai pretējā gadījumā tam ir pienākums pašam veikt izmeklēšanu par šo jautājumu, ņemot vērā faktu attīstību kopš Lēmuma 2000/520 publicēšanas?"

II – **Mana analīze**

48. Ar diviem Augstās tiesas uzdotajiem jautājumiem Tiesa ir aicināta precizēt valstu uzraudzības iestāžu pilnvaras gadījumos, kad tām ir iesniegta sūdzība par personas datu pārsūtīšanu uzņēmumam, kas atrodas trešajā valstī, un kad šīs sūdzības atbalstam ir apgalvots, ka šī valsts nenodrošina pienācīgu pārsūtīto datu aizsardzības līmeni, lai arī Komisija saskaņā ar Direktīvas 95/46 25. panta 6. punktu ir pieņēmusi lēmumu par to, ka šajā trešajā valstī ir nodrošināts pienācīgs aizsardzības līmenis.

49. Norādīšu, ka sūdzībā, kuru *M. Schrems* ir iesniedzis komisāram, ir skarts divkāršs aspekts. Tajā ir apstrīdēts, ka *Facebook Ireland* pārsūta personas datus *Facebook USA*. *M. Schrems* lūdz pārtraukt šo pārsūtīšanu, jo, viņaprāt, Amerikas Savienotās Valstis, īstenojot "drošības zonas" režīmu, nenodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni. Precīzāk, viņš pārmet šai trešajai valstij programmas *PRISM* izveidi, kas ļauj *NSA* brīvi piekļūt ļoti lielam daudzumam datu, kas ir uzglabāti serveros Amerikas Savienotajās Valstīs. Tādējādi sūdzība it īpaši attiecas uz personas datu pārsūtīšanu no *Facebook Ireland* uz *Facebook USA*, un vispārēji apstrīd šo datu aizsardzības līmeni, kas tiek nodrošināts, īstenojot "drošības zonas" režīmu.

50. Komisārs uzskatīja, ka šāda Komisijas lēmuma, kurā ir atzīts, ka Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni, īstenojot "drošības zonas" režīmu, esamība ir šķērslis, lai tas izskatītu sūdzību.

51. Tāpēc ir jāizskata kopā abi jautājumi, ar kuriem būtībā ir vēlme noskaidrot, vai Direktīvas 95/46 28. pants, skatot to kopsakarā ar Hartas 7. un 8. pantu, ir jāinterpretē tādējādi, ka lēmuma, kuru Komisija ir pieņēmusi saskaņā ar šīs direktīvas 25. panta 6. punktu, esamība valsts uzraudzības iestādei liedz izskatīt sūdzību par to, ka trešā valsts nenodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni, un vajadzības gadījumā apturēt šo datu pārsūtīšanu.

52. Ar Hartas 7. pantu ir garantētas tiesības uz privātās dzīves neaizskaramību, savukārt tās 8. pantā skaidri ir noteiktas tiesības uz personas datu aizsardzību. Šī pēdējā minētā panta 2. un 3. punktā ir precizēts, ka šie dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu leģitīmu likumā noteiktu pamatojumu, ka ikvienam ir piekļuves tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos un ka atbilstību šiem noteikumiem kontrolē neatkarīga iestāde.

A – *Par valsts uzraudzības iestāžu pilnvarām gadījumā, kad Komisija ir pieņēmusi lēmumu par atbilstību*

53. Kā savos apsvērumos attiecībā uz sūdzību pamatlietā norāda *M. Schrems*, galvenais jautājums attiecas uz to, ka *Facebook Ireland* pārsūta personas datus *Facebook USA*, ņemot vērā *NSA* un citu Amerikas Savienoto Valstu drošības aģentūru vispārējo piekļuvi *Facebook USA* uzglabātajiem datiem saskaņā ar pilnvarām, kuras tām ir piešķirtas ASV tiesību aktos.

54. *M. Schrems* ieskatā valsts uzraudzības iestāde, kurai ir iesniegta sūdzība, ar ko tiek apstrīdēts atzinums, ka trešā valsts nodrošina pienācīgu pārsūtīto datu aizsardzības līmeni, ir pilnvarota aizliegt sūdzībā minētajam uzņēmumam pārsūtīt datus, ja tās rīcībā ir pierādījumi par šajā sūdzībā minēto apgalvojumu pamatotību.

55. Ņemot vērā komisāra pienākumus aizsargāt *M. Schrems* pamattiesības, pēdējais minētais apgalvo, ka komisāram ne tikai ir pienākums veikt izmeklēšanu, bet arī, ja sūdzība ir pieņemama, izmantot savas pilnvaras apturēt datu plūsmu starp *Facebook Ireland* un *Facebook USA*.

56. Tomēr komisārs sūdzību noraidīja saskaņā ar Likuma par datu aizsardzību tiesību normām attiecībā uz tā pilnvarām. Šis secinājums tika balstīts uz komisāra viedokli par to, ka viņam bija saistošs Lēmums 2000/520.

57. No tā izriet, ka galvenā problēma izskatāmajā lietā ir tā, vai Komisijas vērtējums par pienācīgu aizsardzības līmeni Lēmumā 2000/520 ir absolūti saistošs valsts datu aizsardzības iestādei un tai liedz izskatīt apgalvojumus, ar kuriem ir apstrīdēts šis atzinums. Tātad prejudiciālie jautājumi attiecas uz valsts datu aizsardzības iestāžu pilnvaru apjomu gadījumā, kad Komisija ir pieņēmusi lēmumu par atbilstību.

58. Komisijas skatījumā ir svarīgi ņemt vērā saistību starp attiecīgajām Komisijas pilnvarām un valsts datu aizsardzības iestāžu pilnvarām. Pēdējo minēto kompetencē esot piemērot šajā jomā pieņemtos tiesību aktus konkrētiem gadījumiem, savukārt Komisijas kompetencē esot vispārēji pārskatīt Lēmuma 2000/520, tostarp jebkura lēmuma par tā apturēšanu vai atcelšanu, piemērošanu.

59. Komisija apgalvo, ka *M. Schrems* neesot izvirzījis īpašus argumentus, kas ļautu uzskatīt, ka viņam varētu rasties būtisks kaitējums tāpēc, ka *Facebook Ireland* pārsūta datus *Facebook USA*. Gluži otrādi, *M. Schrems* bažas attiecībā uz ASV drošības aģentūru īstenotajām uzraudzības programmām, ņemot vērā to abstrakto un vispārējo raksturu, esot identiskas tām, kas Komisijai lika uzsākt Lēmuma 2000/520 pārskatīšanu.

60. Komisijas skatījumā valsts uzraudzības iestādes uzņemtos tai piešķirtās pilnvaras atkārtoti pārrunāt ar Amerikas Savienotajām Valstīm šī lēmuma nosacījumus vai vajadzības gadījumā to apturēt, ja tās veiktu pasākumus, pamatojoties uz sūdzībām, kurās ir pausti tikai abstrakti un strukturāli apsvērumi.

61. Es nepiekrītu Komisijas viedoklim. Manuprāt, tas, ka Komisija ir pieņēmusi lēmumu saskaņā ar Direktīvas 95/46 25. panta 6. punktu, nevar nedz liegt, nedz arī mazināt valsts uzraudzības iestāžu pilnvaras, kas tām ir piešķirtas saskaņā ar šīs direktīvas 28. pantu. Pretēji Komisijas apgalvotajam, lai arī valsts uzraudzības iestādēs ir iesniegtas individuālas sūdzības, tas, manuprāt, ņemot vērā to pilnvaras veikt izmeklēšanu un to neatkarību, neliedz tām paust savu viedokli par vispārējo aizsardzības līmeni, kāds tiek nodrošināts trešajā valstī, un izdarīt secinājumus, lemjot par individuālu gadījumu.

62. No Tiesas pastāvīgās judikatūras izriet, ka, interpretējot Savienības tiesību normas, ir jāņem vērā ne tikai to formulējums, bet arī to konteksts un ar tiesisko regulējumu, kurā tās ir iekļautas, izvirzītie mērķi [22].

63. No Direktīvas 95/46 preambulas 62. apsvēruma izriet, ka "uzraudzības iestāžu, kuras pilda savas funkcijas pilnīgi neatkarīgi, izveide dalībvalstīs ir būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi".

64. Saskaņā ar šīs direktīvas 28. panta 1. punkta pirmo daļu "katra dalībvalsts paredz to, ka viena vai vairākas valsts iestādes ir atbildīgas par noteikumu, ko dalībvalstis pieņēmušas saskaņā ar šo direktīvu, piemērošanas pastāvīgu kontroli tās teritorijā". Minētās direktīvas 28. panta 1. punkta otrajā daļā ir noteikts, ka "šīs iestādes tām uzticēto pienākumu izpildē darbojas pilnīgi neatkarīgi".

65. Direktīvas 95/46 28. panta 3. punktā ir uzskaitītas katrai uzraudzības iestādei piešķirtās pilnvaras, proti, izmeklēšanas pilnvaras, efektīvas iejaukšanās pilnvaras, kas tai ļauj noteikt pagaidu vai galīgu aizliegumu datu apstrādei, kā arī pilnvaras uzsākt procesuālas darbības, ja ir pārkāpti saskaņā ar šo direktīvu pieņemtie attiecīgās valsts noteikumi, vai darīt zināmus šos pārkāpumus tiesu iestādēm.

66. Turklāt saskaņā ar Direktīvas 95/46 28. panta 4. punkta pirmo daļu "jebkura persona jebkurai uzraudzības iestādei var iesniegt prasību, kas saistīta ar šīs personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi". Šīs direktīvas 28. panta 4. punkta otrajā daļā ir precizēts, ka "katra uzraudzības iestāde uzklausa jebkuras personas iesniegtās prasības par datu apstrādes likumības pārbaudēm, ja piemērojami saskaņā ar [minētās] direktīvas 13. pantu pieņemtie attiecīgās valsts noteikumi". Precizēšu, ka ar šo pēdējo minēto tiesību normu dalībvalstīm ir atļauts veikt likumdošanas pasākumus, lai ierobežotu vairāku Direktīvā 95/46 paredzēto tiesību un pienākumu piemērojamību gadījumā, kad šāds ierobežojums ir pasākums, kas ir vajadzīgs it īpaši valsts drošības, aizsardzības, sabiedrības drošības, kā arī noziegumu novēršanas, atklāšanas, izmeklēšanas un kriminālvajāšanas mērķiem.

67. Kā ir norādījusi Tiesa, prasība, lai neatkarīga iestāde uzraudzītu Savienības tiesību saistībā ar personu aizsardzību attiecībā uz personas datu apstrādi ievērošanu, izriet arī no Savienības primārajām tiesībām, it īpaši no Hartas 8. panta 3. punkta un LESD 16. panta 2. punkta [23]. Tā arī ir atgādinājusi, ka "uzraudzības iestāžu, kuras pilda savas funkcijas pilnīgi neatkarīgi, izveide dalībvalstīs ir būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi" [24].

68. Tiesa jau ir nospriedusi, ka "Direktīvas 95/46 28. panta 1. punkta otrā daļa ir jāinterpretē tādējādi, ka uzraudzības iestādēm, kuras atbild par personas datu apstrādes uzraudzību, ir jābūt neatkarīgām tādā mērā, ka savus pienākumus tās var veikt bez ārējas ietekmes. Šī neatkarība izslēdz it īpaši jebkādu rīkojumu došanu un jebkādu citu ārēju ietekmi – vai tā būtu tieša vai netieša –, kas varētu iespaidot to lēmumus un kas tādējādi varētu apdraudēt minēto iestāžu pienākumu izpildi, kas ietver taisnīga līdzsvara starp tiesību uz privāto dzīvi aizsardzību un personas datu brīvu apriti izveidi" [25].

69. Tiesa arī ir precizējusi, ka "valsts uzraudzības iestāžu neatkarības garantijas mērķis ir nodrošināt efektīvu un uzticamu kontroli pār tiesību normu ievērošanu saistībā ar fizisko personu aizsardzību attiecībā uz personas datu apstrādi" [26]. Šī neatkarības garantija tika noteikta, "lai pastiprinātu personu un struktūru, kuras skar to lēmumi, aizsardzību" [27].

22 — Skat. it īpaši spriedumu *Koushkaki* (C-84/12, EU:C:2013:862, 34. punkts un tajā minētā judikatūra).

23 — Skat. spriedumus Komisija/Austrija (C-614/10, EU:C:2012:631, 36. punkts) un Komisija/Ungārija (C-288/12, EU:C:2014:237, 47. punkts).

24 — Skat. it īpaši spriedumu Komisija/Ungārija (C-288/12, EU:C:2014:237, 48. punkts un tajā minētā judikatūra). Šajā ziņā skat. arī spriedumu *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238, 68. punkts, kā arī tajā minētā judikatūra).

25 — Skat. it īpaši spriedumu Komisija/Ungārija (C-288/12, EU:C:2014:237, 51. punkts un tajā minētā judikatūra).

26 — Spriedums Komisija/Vācija (C-518/07, EU:C:2010:125, 25. punkts).

27 — Turpat.

70. Kā it īpaši izriet no Direktīvas 95/46 preambulas 10. apsvēruma un 1. panta, tās mērķis ir "garantēt [Savienībā] augsta līmeņa pamattiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi" [28]. Tiesa uzskata, ka "tādējādi Direktīvas 95/46 28. pantā paredzētās uzraudzības iestādes ir minēto pamattiesību un brīvību garanti" [29].

71. Ņemot vērā svarīgo nozīmi, kāda ir valsts uzraudzības iestādēm fizisko personu datu aizsardzībā attiecībā uz personas datu apstrādi, to iejaukšanās pilnvarām ir jābūt visaptverošām, pat ja Komisija ir pieņēmusi lēmumu saskaņā ar Direktīvas 95/46 25. panta 6. punktu.

72. Šajā ziņā uzsvēršu, ka nekas nenorāda uz to, ka personas datu pārsūtīšanas uz trešām valstīm režīmi būtu izslēgti no Hartas 8. panta 3. punkta materiālās piemērošanas jomas, kurā Savienības tiesību normu visaugstākajā hierarhijas līmenī ir noteikts, ka neatkarīgas iestādes veiktajai uzraudzībai attiecībā uz tiesību normu personas datu aizsardzības jomā ievērošanu ir svarīga nozīme.

73. Ja valsts uzraudzības iestādēm Komisijas lēmumi būtu absolūti saistoši, tas neizbēgami ierobežotu to pilnīgo neatkarību. Ņemot vērā, ka valsts uzraudzības iestādes ir pamattiesību garanti, tām ir jāspēj pilnīgi neatkarīgi izskatīt tām iesniegtās sūdzības, lai nodrošinātu indivīdu aizsardzības prioritārās intereses attiecībā uz personas datu apstrādi.

74. Turklāt, kā tiesas sēdē pamatoti ir norādījuši Beļģijas valdība un Eiropas Parlaments, nav nekādas hierarhiskas saiknes starp Direktīvas 95/46 IV nodaļu par personas datu pārsūtīšanu uz trešajām valstīm un tās VI nodaļu, kas it īpaši attiecas uz valsts uzraudzības iestāžu nozīmi. Šajā VI nodaļā nav nevienas norādes, ka noteikumi attiecībā uz valsts uzraudzības iestādēm kaut kādā veidā būtu pakārtoti Direktīvas 95/46 IV nodaļā paredzētajiem dažādajiem noteikumiem attiecībā uz pārsūtīšanu.

75. Gluži otrādi, no šīs direktīvas 25. panta 1. punkta, kas atrodas šīs direktīvas IV nodaļā, skaidri izriet, ka personas datu pārsūtīšana uz trešo valsti, kas nodrošina pienācīgu aizsardzības līmeni, var notikt tikai tad, ja tiek ievērotas valsts tiesību normas, kas ir pieņemtas saskaņā ar pārējiem minētās direktīvas noteikumiem.

76. Šajā ziņā atgādināšu, ka saskaņā ar šo tiesību normu dalībvalstīm savos valsts tiesību aktos ir jāparedz, ka personas datu, kuri atrodas apstrādē vai ir paredzēti apstrādei pēc pārsūtīšanas, pārsūtīšana var notikt tikai tad, ja, neierobežojot atbilstību attiecīgās valsts noteikumiem, kuri pieņemti saskaņā ar pārējiem Direktīvas 95/46 noteikumiem, attiecīgā trešā valsts nodrošina pienācīgu aizsardzības līmeni.

77. Saskaņā ar šīs direktīvas 28. panta 1. punktu valsts uzraudzības iestāžu pienākums ir katrā dalībvalstī uzraudzīt noteikumu, ko dalībvalstis pieņēmušas saskaņā ar šo direktīvu, piemērošanu.

78. Šo divu tiesību normu salīdzinājums ļauj uzskatīt, ka Direktīvas 95/46 25. panta 1. punktā paredzētā tiesību norma, saskaņā ar kuru personas datus var pārsūtīt tikai tad, ja trešās valsts adresāts nodrošina tiem pienācīgu aizsardzības līmeni, pieder tiesību normām, kuru piemērošana ir jāuzrauga valsts uzraudzības iestādēm.

79. Valsts uzraudzības iestāžu pilnvaras pilnīgi neatkarīgi izmeklēt tām saskaņā ar Direktīvas 95/46 28. pantu iesniegtās sūdzības ir jāinterpretē plaši atbilstoši Hartas 8. panta 3. punktam. Tātad šīs pilnvaras nevar ierobežot pilnvaras konstatēt aizsardzības līmeņa trešajā valstī pienācīgumu, kuras saskaņā ar minētās direktīvas 25. panta 6. punktu Komisijai ir piešķīris Savienības likumdevējs.

28 — Turpat (22. punkts un tajā minētā judikatūra).

29 — Turpat (23. punkts). Šajā ziņā skat. arī spriedumus Komisija/Austrija (C-614/10, EU:C:2012:631, 52. punkts) un Komisija/Ungārija (C-288/12, EU:C:2014:237, 53. punkts).

80. Valsts uzraudzības iestādēm, ņemot vērā to būtisko nozīmi personas datu aizsardzības jomā, ir jāspēj veikt izmeklēšanu gadījumos, kad tām ir iesniegta sūdzība par faktiem, ar kuriem varētu tikt apstrīdēts trešajā valstī nodrošinātais aizsardzības līmenis, tostarp arī tad, kad Komisija saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemtā lēmumā ir konstatējusi, ka attiecīgā trešā valsts nodrošina pienācīgu aizsardzības līmeni.

81. Ja valsts uzraudzības iestāde savas izmeklēšanas beigās uzskata, ka, pārsūtot apstrīdētos datus, netiek nodrošināta aizsardzība, kāda ir jāgarantē Savienības pilsoņiem attiecībā uz viņu datu apstrādi, tā ir tiesīga apturēt attiecīgo datu pārsūtīšanu neatkarīgi no tā, kāds būtu Komisijas veiktais vispārējais novērtējums tās lēmumā.

82. Ir skaidrs, ka saskaņā ar Direktīvas 95/46 25. panta 2. punktu trešajā valstī nodrošinātā aizsardzības līmeņa pienācīgums tiek novērtēts, ņemot vērā gan faktisko, gan tiesisko apstākļu kopumu. Ja viens no šiem apstākļiem mainās un ar to tiek apšaubīts trešajā valstī nodrošinātā aizsardzības līmeņa pienācīgums, valsts uzraudzības iestādei, kurai ir iesniegta sūdzība, ir jāspēj izdarīt secinājumus attiecībā uz apstrīdēto pārsūtīšanu.

83. Kā ir norādījusi Īrija, komisāram, tāpat kā citām valsts iestādēm, Lēmums 2000/520 ir saistošs. No LESD 288. panta ceturtās daļas izriet, ka Savienības iestādes pieņemts lēmums uzliek saistības kopumā. Tādējādi Lēmums 2000/520 ir saistošs dalībvalstīm, kurām tas ir adresēts.

84. Šajā ziņā norādīšu, ka Lēmuma 2000/520 5. pantā ir noteikts, ka "dalībvalstis veic visus vajadzīgos pasākumus, lai šo lēmumu izpildītu, vēlākais, deviņdesmit dienas pēc tā paziņošanas dalībvalstīm". Turklāt šī lēmuma 6. pantā ir apstiprināts, ka "[tas] ir adresēts dalībvalstīm".

85. Tomēr es uzskatu, ka, ņemot vērā iepriekš minētās Direktīvas 95/46 un Hartas noteikumus, ar Lēmuma 2000/520 saistošo iedarbību nav izslēgta jebkāda komisāra izmeklēšana attiecībā uz sūdzībām, kurās ir apgalvots, ka, pārsūtot personas datus uz Amerikas Savienotajām Valstīm saskaņā ar šo lēmumu, netiek sniegtas nepieciešamās garantijas, kas ir jānodrošina atbilstoši Savienības tiesībām. Citiem vārdiem sakot, šādas saistošas iedarbības dēļ nav noteikts, ka jebkāda šāda veida sūdzība ir jānoraida kopumā, proti, nekavējoties un neveicot tās pamatotības pārbaudi.

86. Piebildīšu, ka arī no Direktīvas 95/46 25. panta vispārējās struktūras izriet, ka konstatējumu, saskaņā ar kuru trešā valsts nodrošina vai nenodrošina pienācīgu aizsardzības līmeni, var veikt vai nu dalībvalstis, vai Komisija. Tātad runa ir par dalītu kompetenci.

87. Saskaņā ar šīs direktīvas 25. panta 6. punktu, ja Komisija konstatē, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni minētās direktīvas 25. panta 2. punkta izpratnē, dalībvalstīm ir jāveic pasākumi, kas ir vajadzīgi, lai izpildītu Komisijas lēmumu.

88. Tā kā ar šādu lēmumu tiek atļauts pārsūtīt personas datus uz trešo valsti, kurā nodrošināto aizsardzības līmeni Komisija ir atzinusi par pienācīgu, dalībvalstīm principā ir jāatļauj tās teritorijā reģistrētajiem uzņēmumiem veikt šāda veida pārsūtīšanu.

89. Tomēr ar Direktīvas 95/46 25. pantu Komisijai nav piešķirtas ekskluzīvas [pilnvaras] konstatēt pārsūtīto personas datu aizsardzības līmeņa pienācīgumu vai nepienācīgumu. Šī panta vispārējā struktūra liecina par to, ka dalībvalstīm šajā jomā arī ir nozīme. Komisijas lēmumam, neapšaubāmi, ir svarīga nozīme, nosakot vienveidīgus pārsūtīšanas nosacījumus, kas ir spēkā dalībvalstīs. Tomēr šis vienveidīgums var tikt nodrošināts tik ilgi, kamēr minētais secinājums netiek apstrīdēts.

90. Argumentu attiecībā uz nepieciešamību noteikt vienotus nosacījumus personas datu pārsūtīšanai uz trešo valsti, manuprāt, ierobežo tāda situācija kā pamatlietā, kurā Komisija ne tikai ir informēta par to, ka šis secinājums ir pamats kritikai, bet arī tā pati pauž šādu kritiku un risina sarunas, lai to labotu.

91. Dalībvalstis un Komisija var arī sadarboties, veicot trešajā valstī nodrošinātās aizsardzības līmeņa pienācīguma vai nepienācīguma novērtējumu. Direktīvas 95/46 25. panta 3. punktā šajā ziņā ir paredzēts, ka "dalībvalstis un Komisija informē viena otru par gadījumiem, kad tās uzskata, ka trešā valsts nenodrošina pienācīgu aizsardzības līmeni 2. punkta nozīmē". Kā norāda Parlaments, tas labi atspoguļo, ka dalībvalstīm un Komisijai ir līdzvērtīga nozīme, lai konstatētu gadījumus, kad trešā valsts nenodrošina pienācīgu aizsardzības līmeni.

92. Lēmuma par atbilstību mērķis ir atļaut pārsūtīt personas datus uz attiecīgo valsti. Tas nenozīmē, ka Savienības pilsoņi nevar iesniegt uzraudzības iestādēm prasību par personas datu aizsardzību. Šajā ziņā norādīšu, ka Direktīvas 95/46 28. panta 4. punkta pirmajā daļā, saskaņā ar kuru "jebkura persona jebkurai uzraudzības iestādei var iesniegt prasību, kas saistīta ar šīs personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi", nav paredzēts izņēmums no šī principa, ja Komisija ir pieņēmusi lēmumu saskaņā ar šīs direktīvas 25. panta 6. punktu.

93. Tādējādi, lai arī Komisija ir pieņēmusi lēmumu, īstenojot izpildes pilnvaras, kas šai pēdējai minētajai ir piešķirtas ar šo tiesību normu, lai atļautu pārsūtīt personas datus uz trešo valsti, tomēr ar šādu lēmumu dalībvalstīm, it īpaši to valsts uzraudzības iestādēm, nevar tikt atņemtas piešķirtās pilnvaras vai arī tikai ierobežota to kompetence gadījumā, kad tām ir jāizvērtē apgalvojumi par pamattiesību pārkāpumiem.

94. Valsts uzraudzības iestādei ir jāspēj īstenot tai ar Direktīvas 95/46 28. panta 3. punktu piešķirtās pilnvaras, tostarp pilnvaras noteikt pagaidu vai galīgu aizliegumu apstrādāt personas datus. Lai arī šajā tiesību normā noteikto pilnvaru uzskaitījumā skaidri nav paredzētas pilnvaras attiecībā uz pārsūtīšanu no dalībvalsts uz trešo valsti, šāda pārsūtīšana, manuprāt, ir jāuzskata par datu apstrādes sastāvdaļu [30]. Kā izriet no minētās tiesību normas formulējuma, uzskaitījums arī nav izsmeļošs. Katrā ziņā, ņemot vērā valsts uzraudzības iestāžu būtisko nozīmi ar Direktīvu 95/46 izveidotajā sistēmā, tām ir jābūt apveltītām ar pilnvarām apturēt datu pārsūtīšanu, ja tiek pierādīts pamattiesību pārkāpums vai arī pastāv pamattiesību neievērošanas iespēja.

95. Piebildīšu, ka atņemt valsts uzraudzības iestādei tās pilnvaras veikt izmeklēšanu tādos apstākļos kā izskatāmajā lietā būtu pretrunā ne tikai neatkarības principam, bet arī Direktīvas 95/46 mērķim, kas izriet no tās 1. panta 1. punkta.

96. Kā ir norādījusi Tiesa, "no Direktīvas 95/46 preambulas 3., 8. un 10. apsvēruma izriet, ka Savienības likumdevējs ir paredzējis atvieglot personas datu brīvu plūsmu, tuvinot dalībvalstu likumus, saglabājot personu pamattiesības, tostarp tiesības uz privātās dzīves neaizskaramību, un nodrošinot augstu aizsardzības līmeni Savienībā. Šīs direktīvas 1. pantā ir paredzēts, ka dalībvalstu pienākums ir aizsargāt fizisku personu pamattiesības un brīvības un, it īpaši, viņu tiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi [31].

97. Tāpēc Direktīvas 95/46 noteikumi ir jāinterpretē saskaņā ar tās mērķi nodrošināt fizisko personu pamattiesību un brīvību, it īpaši viņu tiesību uz privātās dzīves neaizskaramību, saistībā ar personas datu apstrādi augstu aizsardzības līmeni.

98. Šī mērķa svarīgums un uzdevums, kas dalībvalstīm ir jāveic, lai to sasniegtu, nozīmē, ka tad, kad īpaši apstākļi pamato nopietnas šaubas par Hartā noteikto pamattiesību attiecībā uz personas datu pārsūtīšanu uz trešajām valstīm ievērošanu, Komisijas lēmums par atbilstību dalībvalstīm un, tātad, tajās izveidotajām valsts uzraudzības iestādēm nevar būt absolūti saistošs.

30 — Šajā ziņā skat. ģenerāladvokāta F. Ležē [*Ph. Léger*] secinājumus lietā Parlaments/Padome un Komisija (C-317/04, EU:C:2005:710, 92.–95. punkts). Skat. arī spriedumu Parlaments/Padome un Komisija (C-317/04 P un C-318/04, EU:C:2006:346, 56. punkts).

31 — Skat. it īpaši spriedumu *IPI* (C-473/12, EU:C:2013:715, 28. punkts un tajā minētā judikatūra).

99. Tiesa ir nospriedusi, ka "Direktīvas 95/46 normas attiecībā uz personas datu apstrādi, kas var skart pamattiesības, it īpaši tiesības uz privātās dzīves neaizskaramību, ir jāinterpretē, ievērojot pamattiesības, kas saskaņā ar pastāvīgo judikatūru pieder pie vispārējiem tiesību principiem, kuru aizsardzība ir jānodrošina Tiesai, un kas ir ierakstītas Hartā" [32].

100. Turklāt es atsaucos uz judikatūru, saskaņā ar kuru "dalībvalstīm savas valsts tiesības ir jāinterpretē ne tikai tā, lai tās atbilstu Savienības tiesībām, bet arī jārūpējas, lai to pamatā nebūtu tādas sekundāro tiesību normu interpretācijas, kas būtu konfliktā ar Savienības tiesību sistēmā aizsargātajām pamattiesībām vai ar citiem Savienības tiesību vispārīgajiem principiem" [33].

101. Tiesa savā spriedumā *N. S.* u.c. [34] ir nospriedusi, ka "Regulas [(EK)] Nr. 343/2003 [[35]] piemērošana, pamatojoties uz neapstrīdamu pieņēmumu, ka par patvēruma pieteikuma izskatīšanu parasti atbildīgajā dalībvalstī tiks ievērotas patvēruma meklētāja pamattiesības, [..] nav saderīga ar dalībvalsts pienākumu interpretēt un piemērot Regulu Nr. 343/2003 atbilstoši pamattiesībām" [36].

102. Šajā ziņā Tiesa ir atzinusi, ka, tā kā dalībvalstis ir uzskatāmas par drošām mītneszemēm viena attiecībā pret otru visos juridiskajos un praktiskajos jautājumos, kas saistīti ar patvēruma tiesībām, tad ir jāprezumē, ka attieksme pret patvēruma meklētājiem katrā dalībvalstī atbilst Hartas, 1951. gada 28. jūlijā Ženēvā parakstītās konvencijas [37], kā arī 1950. gada 4. novembrī Romā parakstītās Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas [38] prasībām. Tai pat laikā Tiesa ir nospriedusi, ka "nevar tikt izslēgts, ka šī sistēma noteiktā dalībvalstī praksē var sastapties ar lielām operacionālām grūtībām, kas nozīmē, ka pastāv nopietns risks, ka pret patvēruma meklētājiem to nosūtīšanas uz šo dalībvalsti gadījumā izrādītā attieksme nebūs saderīga ar viņu pamattiesībām" [39].

103. Tādējādi Tiesa ir nospriedusi, ka "dalībvalstīm, ieskaitot valsts tiesas, ir pienākums nenosūtīt patvēruma meklētāju uz "atbildīgo dalībvalsti" Regulas Nr. 343/2003 izpratnē gadījumos, kad tās nevar nezināt, ka sistēmiski trūkumi patvēruma piešķiršanas procesā un patvēruma meklētāju uzņemšanas apstākļos šajā dalībvalstī [ir pietiekams pamats] uzskatīt, ka patvēruma meklētājam radīsies [faktisks] risks tikt pakļautam necilvēciskai vai pazemojošai attieksmei Hartas 4. panta izpratnē" [40].

104. Spriedumā *N. S.* u.c. [41] noteiktais, manuprāt, var tikt attiecināts arī uz tādu situāciju kā pamatlietā aplūkotā. Tādējādi Savienības atvasināto tiesību interpretācija, kas būtu balstīta uz neapstrīdamu pieņēmumu, ka gan dalībvalsts, gan Komisija, gan trešā valsts ievēros pamattiesības, ir jāuzskata par nesaderīgu ar dalībvalstu pienākumu interpretēt un piemērot Savienības atvasinātās tiesības saskaņā ar pamattiesībām. Ar šo tiesību normu nav uzlikts pienākums balstīties uz šādu neapstrīdamu pieņēmumu par pamattiesību ievērošanu, ciktāl tas attiecas uz Komisijas vērtējumu par trešā valstī nodrošinātā aizsardzības līmeņa pienācīgumu. Gluži otrādi, šajā tiesību normā paredzētais pieņēmums, ka ar datu pārsūtīšanu uz trešo valsti tiek ievērotas pamattiesības, ir jāuzskata par atspēkojamu [42]. Tādējādi šī tiesību norma nebūtu jāinterpretē tādējādi, ka ar to ir apstrīdētas it īpaši Direktīvas 95/46 28. panta 3. punktā un Hartas 8. panta 3. punktā paredzētās garantijas, lai nodrošinātu personas datu aizsardzību un tiesību uz personas datu aizsardzību ievērošanu.

32 — Skat. it īpaši spriedumu *Google Spain* un *Google* (C-131/12, EU:C:2014:317, 68. punkts un tajā minētā judikatūra).

33 — Skat. it īpaši spriedumu *N. S.* u.c. (C-411/10 un C-493/10, EU:C:2011:865, 77. punkts, kā arī tajā minētā judikatūra).

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

35 — Padomes 2003. gada 18. februāra Regula, ar ko paredz kritērijus un mehānismus, lai noteiktu dalībvalsti, kura ir atbildīga par trešās valsts pilsoņa patvēruma pieteikuma izskatīšanu, kas iesniegts kādā no dalībvalstīm (OV L 50, 1. lpp.).

36 — Šī sprieduma 99. punkts.

37 — *Recueil des traités des Nations unies* [Apvienoto Nāciju Organizācijas līgumu krājums], 189. sēj., 150. lpp., Nr. 2545 (1954).

38 — Skat. spriedumu *N. S.* u.c. (C-411/10 un C-493/10, EU:C:2011:865, 80. punkts).

39 — Turpat (81. punkts).

40 — Turpat (94. punkts).

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

42 — Šī sprieduma 104. punkts.

105. Tāpēc no minētā sprieduma es secinu, ka, ņemot vērā konstatētos sistēmiskos trūkumus trešajā valstī, uz kuru tiek pārsūtīti personas dati, dalībvalstīm ir jāspēj veikt pasākumus, kas ir vajadzīgi, lai īstenotu ar Hartas 7. un 8. pantu aizsargātās pamattiesības.

106. Turklāt, kā savos apsvērumos ir norādījusi Itālijas valdība, Komisijas pieņemtais lēmums par atbilstību nevar mazināt Savienības pilsoņu aizsardzību attiecībā uz viņu datu apstrādi, kad tie tiek pārsūtīti uz trešo valsti, salīdzinājumā ar aizsardzības līmeni, kāds šīm personām tiktu nodrošināts, ja viņu dati tiktu apstrādāti Savienībā. Tādēļ valsts uzraudzības iestādēm ir jāspēj iejaukties un īstenot savas pilnvaras attiecībā uz datu pārsūtīšanu uz trešām valstīm, par kurām ir pieņemts lēmums par atbilstību. Pretējā gadījumā Savienības pilsoņi būtu neaizsargātāki nekā tad, ja viņu dati tiktu apstrādāti Savienībā.

107. Tādējādi ar Komisijas lēmumu, kas ir pieņemts saskaņā ar Direktīvas 95/46 25. panta 6. punktu, tikai tiek atcelts vispārējs aizliegums eksportēt personas datus uz trešajām valstīm, kas garantētu tādu pašu aizsardzības līmeni, kāds tiek nodrošināts ar šo direktīvu. Citiem vārdiem sakot, ar to netiek izveidota īpaša izņēmuma sistēma, ar kuru Savienības pilsoņiem tiktu nodrošināta mazāka aizsardzība salīdzinājumā ar vispārējo sistēmu, kas minētajā direktīvā ir paredzēta attiecībā uz datu apstrādi Savienībā.

108. Protams, Tiesa sava sprieduma *Lindqvist*[43] 63. punktā ir norādījusi, ka "Direktīvas 95/46 IV nodaļā, kurā atrodas 25. pants, ir izveidota īpaša sistēma ar speciāliem noteikumiem". Tomēr, manuprāt, tas nenozīmē, ka šāda sistēmai būtu jānodrošina mazāka aizsardzība. Gluži otrādi, lai sasniegtu Direktīvas 95/46 1. panta 1. punktā izvirzīto datu aizsardzības mērķi, dalībvalstīm un Komisijai[44] ar šīs direktīvas 25. pantu ir noteikta virkne pienākumu un šajā 25. pantā ir noteikts princips, saskaņā ar kuru tad, kad trešā valsts nenodrošina pienācīgu aizsardzības līmeni, personas datu pārsūtīšana uz šo trešo valsti ir jāaizliedz[45].

109. It īpaši attiecībā uz "drošības zonas" režīmu Komisija paredz valsts uzraudzības iestāžu iejaukšanos un datu plūsmas apturēšanu, tikai piemērojot Lēmuma 2000/520 3. panta 1. punkta b) apakšpunktu.

110. Saskaņā ar šī lēmuma preambulas 8. apsvērumu "pārredzamības labad un lai panāktu dalībvalsts kompetento iestāžu spēju nodrošināt indivīdu aizsardzību attiecībā uz viņu personas datu apstrādi, šajā lēmumā jānosaka izņēmuma apstākļi, kuros konkrētu datu plūsmas apturēšana ir attaisnojama, neatkarīgi no pienācīgas aizsardzības konstatācijas".

111. Izskatāmajā lietā it īpaši tiek apstrīdēta minētā lēmuma 3. panta 1. punkta b) apakšpunkta piemērošana. Tādējādi saskaņā ar šo tiesību normu par datu plūsmas apturēšanu var lemt valsts uzraudzības iestādes, kas būtu "gadījumos, kad ir liela iespējamība, ka principi nav ievēroti; ir pamats uzskatīt, ka attiecīgais piemērošanas mehānisms neietver vai neietvers piemērotus un savlaicīgus pasākumus, lai attiecīgo gadījumu atrisinātu; nosūtīšanas turpināšana datu subjektiem radītu būtiska kaitējuma draudus, un dalībvalsts kompetentās iestādes šajos apstākļos ir darījušas visu iespējamo, lai organizācijai to paziņotu un dotu iespēju atbildēt".

112. Minētajā tiesību normā paredzētos nosacījumus lietas dalībnieki šajā tiesvedībā ir interpretējuši atšķirīgi[46]. Sīki neanalizējot šīs interpretācijas, no tām izriet, ka šie nosacījumi strikti attiecas uz valsts uzraudzības iestāžu pilnvarām apturēt datu plūsmu.

43 — C-101/01, EU:C:2003:596.

44 — 65. punkts.

45 — 64. punkts.

46 — *M. Schrems* skatījumā pirmais nosacījums neesot izpildīts. Runa ir par nosacījumu, saskaņā ar kuru "ir liela iespējamība, ka principi nav ievēroti". Tomēr viņš nav apgalvojis, ka *Facebook USA* kā pašsertificēta iestāde, kurai tiek pārsūtīti dati, būtu pārkāpis "drošības zonas" principus tāpēc, ka ASV iestādēm ir plaša un nediferencēta piekļuve datiem. "Drošības zonas" principu [piemērošanu] acīmredzami ierobežo ASV tiesības, kas Lēmuma 2000/520 I pielikuma ceturtajā daļā ir definētas, atsaucoties uz likumu, valdības noteikumiem un tiesu praksi.

113. Pretēji Komisijas apgalvotajam Lēmuma 2000/520 3. panta 1. punkta b) apakšpunkts ir jāinterpretē saskaņā ar Direktīvā 95/46 izvirzīto mērķi nodrošināt personas datu aizsardzību, kā arī saskaņā ar Hartas 8. pantu. Prasība interpretēt atbilstoši pamattiesībām pamato šīs tiesību normas plašu interpretāciju.

114. No tā izriet, ka Lēmuma 2000/520 3. panta 1. punkta b) apakšpunktā paredzētie nosacījumi, manuprāt, nevar aizkavēt valsts uzraudzības iestādi pilnīgi neatkarīgi īstenot pilnvaras, kas tai ir piešķirtas saskaņā ar Direktīvas 95/46 28. panta 3. punktu.

115. Kā tiesas sēdē būtībā ir norādījušas Beļģijas un Austrijas valdības, Lēmuma 2000/520 3. panta 1. punkta b) apakšpunktā paredzētā "avārijas izeja" ir tik šaura, ka to ir grūti izmantot praksē. Tajā ir noteikti kumulatīvi kritēriji un latiņa ir novietota pārāk augstu. Taču, ņemot vērā Hartas 8. panta 3. punktu, valsts uzraudzības iestāžu rīcības brīvību attiecībā uz Direktīvas 95/46 28. panta 3. punktā noteiktajām prerogatīvām nav iespējams ierobežot tādējādi, ka minētās iestādes tās vairs nevarētu īstenot.

116. Šajā ziņā Parlaments pamatoti norāda, ka Savienības likumdevējs ir tas, kurš nolēmis, kādas pilnvaras būtu jāīsteno valsts uzraudzības iestādēm. Tomēr izpildes pilnvaras, kuras Savienības likumdevējs ar Direktīvas 95/46 25. panta 6. punktu ir piešķīris Komisijai, neietekmē pilnvaras, kuras šis pats likumdevējs ar šīs direktīvas 28. panta 3. punktu ir piešķīris valsts uzraudzības iestādēm. Citiem vārdiem sakot, Komisijas kompetencē nav ierobežot valsts uzraudzības iestāžu pilnvaras.

117. Tādējādi, lai nodrošinātu fizisko personu pamattiesību pienācīgu aizsardzību attiecībā uz personas datu apstrādi, valsts uzraudzības iestādēm ir jābūt tiesīgām veikt izmeklēšanu gadījumos, kad tiek izteikti apgalvojumi par šo tiesību pārkāpumiem. Ja šādu izmeklēšanu noslēgumā šīs iestādes uzskata, ka trešajā valstī, uz kuru attiecas lēmums par atbilstību, zināmas pazīmes liecina par Savienības pilsoņu tiesību uz personas datu aizsardzību neievērošanu, tām ir jāspēj apturēt datu pārsūtīšanu šajā trešajā valstī reģistrētam adresātam.

118. Citiem vārdiem sakot, valsts uzraudzības iestādēm ir jāspēj veikt savu izmeklēšanu un vajadzības gadījumā apturēt datu pārsūtīšanu neatkarīgi no Lēmuma 2000/520 3. panta 1. punkta b) apakšpunktā paredzētajiem ierobežojošajiem nosacījumiem.

119. Turklāt, ņemot vērā to pilnvaras uzsākt procesuālas darbības gadījumā, ja ir pārkāptas valsts tiesību normas, piemērojot Direktīvu 95/46, vai to pilnvaras darīt zināmus šos pārkāpumus tiesas iestādei, kas ir paredzētas šīs direktīvas 28. panta 3. punktā, valsts uzraudzības iestādēm, kad tām ir zināmi fakti, kas pierāda, ka trešā valsts nenodrošina pienācīgu aizsardzības līmeni, ir jābūt apveltītām ar pilnvarām celt prasību valsts tiesā, kas vajadzības gadījumā varēs lemt par lūguma sniegt prejudiciālu nolēmumu iesniegšanu Tiesā, lūdzot izvērtēt Komisijas lēmuma par atbilstību spēkā esamību.

120. No visiem šiem apstākļiem izriet, ka Direktīvas 95/46 28. pants, skatot to kopsakarā ar Hartas 7. un 8. pantu, ir jāinterpretē tādējādi, ka tāda lēmuma esamība, kuru Komisija ir pieņēmusi saskaņā ar šīs direktīvas 25. panta 6. punktu, neliedz valsts uzraudzības iestādei izskatīt sūdzību par to, ka trešā valsts nenodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni, un vajadzības gadījumā apturēt šo datu pārsūtīšanu.

121. Lai arī savā lūgumā sniegt prejudiciālu nolēmumu Augstā tiesa uzsver, ka prasībā pamatlietā *M. Schrems* oficiāli nav apstrīdējis nedz Direktīvas 95/46, nedz Lēmuma 2000/520 spēkā esamību, no šī lūguma sniegt prejudiciālu nolēmumu izriet, ka *M. Schrems* galvenokārt kritizē secinājumu, ka Amerikas Savienotās Valstis, īstenojot "drošības zonas" režīmu, nodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni.

122. Arī no komisāra apsvērumiem izriet, ka *M. Schrems* sūdzības mērķis tieši ir apstrīdēt Lēmumu 2000/520. Iesniedzot šo sūdzību, šis pēdējais minētais apšauba "drošības zonas" režīma kā tāda noteikumus un darbību, pamatojoties uz to, ka personas datu plaša uzraudzība Amerikas Savienotajās Valstīs pierādot, ka šajā trešajā valstī nedz tiesībās, nedz praksē neesot nodrošināta patiesa šo datu aizsardzība.

123. Turklāt pati iesniedzējtiesa norāda, ka ar Hartas 7. pantu nodrošinātā garantija un dalībvalstu konstitucionālo tradīciju būtiskās kopējās vērtības netiktu ievērotas, ja valsts iestādēm tiktu atļauts vispārēji un izlases veidā piekļūt elektroniskajām komunikācijām, nenorādot objektīvu pamatojumu, kas būtu balstīts uz valsts drošības vai noziedzības novēršanas apsvērumiem, kas it īpaši ir saistīti ar attiecīgiem indivīdiem, un nesniedzot nekādas pienācīgas vai pārbaudāmas garantijas [47]. Iesniedzējtiesa arī netieši pauž šaubas par Lēmuma 2000/520 spēkā esamību.

124. Tāpēc, lai izvērtētu, vai Amerikas Savienotās Valstis, īstenojot "drošības zonas" režīmu, nodrošina atbilstīgu pārsūtīto personas datu aizsardzību, obligāti ir jāizskata jautājums par šī lēmuma spēkā esamību.

125. Šajā ziņā ir jānorāda, ka saistībā ar sadarbības starp Tiesu un valsts tiesām instrumentu, kas izveidots ar LESD 267. pantu, Tiesa, kurai ir tikai uzdots jautājums par Savienības tiesību interpretāciju, dažos īpašos gadījumos var pārbaudīt sekundāro tiesību aktu noteikumu spēkā esamību.

126. Tādējādi Tiesa pēc savas ierosmes vairākkārt ir pasludinājusi par spēkā neesošu aktu, kuru tai ir ticis lūgts interpretēt [48]. Tā arī ir nospriedusi, ka, "ja izrādās, ka valsts tiesas uzdoto jautājumu patiesā būtība, visticamāk, attiecas uz spēkā esamības pārbaudi, nevis uz [Savienības] tiesību aktu interpretāciju, tad Tiesai nekavējoties ir jāsniedz atbilde minētajai tiesai, neuzspiežot absolūti novilcinošu formālismu, kas nebūtu saderīgs ar to mehānismu būtību, kas iedibināti ar [LESD 267.] pantu" [49]. Tiesa arī ir nospriedusi, ka iesniedzējtiesas paustās šaubas par atvasināto tiesību akta saderīgumu ar tiesību normām par pamattiesību aizsardzību, ir jāsaprot kā šī tiesību akta spēkā esamības apstrīdēšana Savienības tiesību kontekstā [50].

127. Atgādināšu arī – no Tiesas judikatūras izriet, ka tiek prezumēts, ka Savienības iestāžu un struktūru akti ir spēkā, kas nozīmē, ka tie rada tiesiskas sekas tikmēr, kamēr tie nav atsaukti, atcelti prasībā atcelt tiesību aktu vai pasludināti par spēkā neesošiem lūguma sniegt prejudiciālu nolēmumu vai iebildes par prettiesiskumu rezultātā. Tikai Tiesa ir kompetenta konstatēt Savienības tiesību akta spēkā neesamību – šīs kompetences mērķis ir garantēt tiesisko noteiktību, nodrošinot Savienības tiesību vienveidīgu piemērošanu. Tādējādi, ja Komisija nepasludina lēmumu par spēkā neesošu, grozītu vai atceltu, tas ir pilnībā saistošs un tieši piemērojams visās dalībvalstīs [51].

128. Lai iesniedzējtiesai sniegtu izsmeļošu atbildi un kliedētu šajā tiesvedībā paustās šaubas par Lēmuma 2000/520 spēkā esamību, es uzskatu, ka Tiesai tāpēc būtu jāveic šī lēmuma spēkā esamības novērtējums.

129. Tādējādi ir arī jāprecizē, ka Lēmuma 2000/520 spēkā esamības vai neesamības pārbaude ir jāveic tikai attiecībā uz šajā tiesvedībā notikušajās debatēs izteiktajiem iebildumiem. Šajā tiesvedībā netika apspriesti visi "drošības zonas" režīma darbības aspekti, tāpēc man nešķiet, ka šeit ir iespējams veikt izsmeļošu šī režīma trūkumu pārbaudi.

47 — Lūguma sniegt prejudiciālu nolēmumu 24. punkts.

48 — Skat. it īpaši spriedumus *Strehl* (62/76, EU:C:1977:18, 10.–17. punkts), *Roquette Frères* (145/79, EU:C:1980:234, 6. punkts), kā arī *Schutzverband der Spirituosen-Industrie* (C-457/05, EU:C:2007:576, 32.–39. punkts).

49 — Spriedums *Schwarze* (16/65, EU:C:1965:117, 1094. lpp.).

50 — Skat. spriedumu *Hauer* (44/79, EU:C:1979:290, 16. punkts).

51 — Skat. it īpaši spriedumu *CIVAD* (C-533/10, EU:C:2012:347, 39.–41. punkts un tajos minētā judikatūra).

130. Savukārt šajā tiesvedībā Tiesā tika apspriests jautājums par to, vai vispārēja un nediferencēta ASV izlūkošanas dienestu piekļuve pārsūtītajiem datiem var skart Lēmuma 2000/520 tiesiskumu. Tāpēc šī lēmuma spēkā esamība var tikt izvērtēta šādā aspektā.

B – *Par Lēmuma 2000/520 spēkā esamību*

1) Par apstākļiem, kas ir jāņem vērā, izvērtējot Lēmuma 2000/520 spēkā esamību

131. Ir jāatgādina Tiesas judikatūra, saskaņā ar kuru, "ceļot prasību atcelt tiesību aktu, tiesību akta tiesiskums ir jāizvērtē, ņemot vērā tiesiskos un faktiskos apstākļus, kādi pastāvēja tiesību akta pieņemšanas brīdī; Komisijas vērtējums var tikt apšaubīts tikai tad, ja tas ir acīmredzami kļūdains, ņemot vērā faktus, kas bija tās rīcībā tiesību akta pieņemšanas brīdī" [52].

132. Savā spriedumā *Gaz de France – Berliner Investissement* [53] Tiesa ir atgādinājusi principu, saskaņā ar kuru "akta spēkā esamības vērtējumam, kas ir jāizdara Tiesai prejudiciāla nolēmuma tiesvedībā, parasti ir jābalstās uz situāciju, kāda pastāv akta pieņemšanas brīdī" [54]. Tomēr, šķiet, tā tai pat laikā ir atzinusi, ka "akta spēkā esamība var atsevišķos gadījumos tikt novērtēta atkarībā no jaunajiem faktiem, kas radušies pēc tā pieņemšanas" [55].

133. Šādi ieskicētai Tiesas atvērtībai, manuprāt, ir īpaša nozīme izskatāmajā lietā.

134. Komisijas lēmumiem, kas ir pieņemti saskaņā ar Direktīvas 95/46 25. panta 6. punktu, ir īpašas iezīmes. To mērķis ir novērtēt, vai trešajās valstīs nodrošinātais personas datu aizsardzības līmenis ir vai nav pienācīgs. Runa ir par trešā valstī [nodrošinātā līmeņa] vērtējumu, ņemot vērā faktiskos un tiesiskos apstākļus.

135. Tā kā lēmums par atbilstību ir īpašs lēmumu veids, tad izskatāmajā lietā ir jāprecizē tiesību norma, saskaņā ar kuru tā spēkā esamības novērtējums var tikt veikts, tikai ņemot vērā apstākļus, kas pastāvēja tā pieņemšanas brīdī. Šādas tiesību normas dēļ pēc vairākiem gadiem pēc lēmuma par atbilstību pieņemšanas Tiesa, veicot savu novērtējumu par spēkā esamību, nevarētu ņemt vērā vēlākus notikumus arī tad, ja šāda lūguma sniegt prejudiciālu nolēmumu par spēkā esamību iesniegšana nebūtu ierobežota laikā un ja tā iesniegšanu tieši varētu būt izraisījuši turpmākie fakti, kas atspoguļo attiecīgā tiesību akta trūkumus.

136. Izskatāmajā lietā Lēmuma 2000/520 saglabāšana spēkā jau piecpadsmit gadus liecina par netiešu Komisijas 2000. gadā veiktā vērtējuma apliecinājumu. Ja prejudiciāla nolēmuma tiesvedībā Tiesai ir jāizvērtē šī vērtējuma, kuru Komisija ir saglabājusi laikā, spēkā esamība, tā ne tikai var, bet tai ir jāsalīdzina minētais vērtējums ar jaunajiem apstākļiem, kas ir radušies kopš lēmuma par atbilstību pieņemšanas.

137. Ņemot vērā lēmuma par atbilstību īpašo būtību, Komisijai tas regulāri ir jāpārskata. Ja pēc notikumiem, kas ir norisinājušies starplaikā, Komisija negroza savu lēmumu, tas nozīmē, ka tā netieši, bet noteikti uztur sākotnēji veikto vērtējumu. Tādējādi tā apstiprina savu atzinumu, saskaņā ar kuru attiecīgā trešā valsts nodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni. Tiesai ir jāpārbauda, vai šis atzinums joprojām ir spēkā, neraugoties uz apstākļiem, kas ir radušies vēlāk.

52 — Skat. it īpaši spriedumu *BVGD*/Komisija (T-104/07 un T-339/08, EU:T:2013:366, 291. punkts), atsaucoties uz spriedumu *IECC*/Komisija (C-449/98 P, EU:C:2001:275, 87. punkts).

53 — C-247/08, EU:C:2009:600.

54 — 49. punkts un tajā minētā judikatūra.

55 — 50. punkts un tajā minētā judikatūra. Šajā ziņā skat. Lenaerts, K., Maselis, I., un Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, kurā ir norādīts, ka "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" (10.16. punkts, 471. lpp.).

138. Tāpēc, lai nodrošinātu šāda veida lēmuma efektīvu pārbaudi tiesā, tā spēkā esamības novērtējums, manuprāt, ir jāveic, ņemot vērā pašreizējos faktiskos un tiesiskos apstākļus.

2) Par pienācīga aizsardzības līmeņa jēdzienu

139. Direktīvas 95/46 25. pants pilnībā ir balstīts uz principu, saskaņā ar kuru personas dati var tikt pārsūtīti uz trešo valsti tikai tad, ja šī trešā valsts nodrošina pienācīgu šādu datu aizsardzības līmeni. Šī panta mērķis arī ir nodrošināt ar šo direktīvu paredzētās aizsardzības turpinātību gadījumā, kad personas dati tiek pārsūtīti uz trešo valsti. Šajā ziņā ir jāatgādina, ka ar minēto direktīvu Savienības pilsoņiem tiek nodrošināts augsts aizsardzības līmenis attiecībā uz viņu personas datu apstrādi.

140. Ņemot vērā svarīgo nozīmi, kāda personas datu aizsardzībai ir saistībā ar pamattiesībām uz privātās dzīves neaizskaramību, šāds augsts aizsardzības līmenis ir jānodrošina arī tad, kad personas dati tiek pārsūtīti uz trešo valsti.

141. Tāpēc es uzskatu, ka Komisija saskaņā ar Direktīvas 95/46 25. panta 6. punktu var konstatēt, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, tikai tad, ja pēc visu attiecīgās trešās valsts tiesību un prakses novērtējuma tā spēj konstatēt, ka šajā trešajā valstī aizsardzības līmenis būtībā ir līdzvērtīgs līmenim, kāds ir nodrošināts ar šo direktīvu, pat ja noteikumi attiecībā uz šo aizsardzību var atšķirties no tiem, kas parasti tiek piemēroti Savienībā.

142. Lai arī jēdziens "adequate" angļu valodā no lingvistiskā viedokļa var tikt saprasts kā tāds, ar ko apzīmē aizsardzības līmeni, kas ir tik tikko pietiekams vai pietiekams, un tādējādi tam var būt cits semantiskais lauks nekā terminam "adéquat" franču valodā, ir jānorāda, ka vienīgais kritērijs, kas ir jāņem vērā šī jēdziena interpretācijā, ir mērķis sasniegt augstu pamattiesību aizsardzības līmeni, kā tas ir prasīts Direktīvā 95/46.

143. Veicot trešajā valstī nodrošinātā aizsardzības līmeņa pārbaudi, ir jānoskaidro divi pamatelementi, proti, piemērojamo tiesību normu saturs un līdzekļi, lai nodrošinātu šo tiesību normu ievērošanu [56].

144. Manuprāt, lai sasniegtu aizsardzības līmeni, kas būtībā būtu līdzvērtīgs Savienībā spēkā esošajam, "drošības zonas" režīmam, kura pamatā ir uzņēmumu, kas labprātīgi piedalās šajā režīmā, pašnovērtējums un pašsertifikācija, būtu jāparedz atbilstošas garantijas un pietiekams uzraudzības mehānisms. Tādējādi personas datu pārsūtīšanai uz trešajām valstīm nebūtu jānodrošina mazāka aizsardzība nekā Savienībā veiktajai datu apstrādei.

145. Šajā ziņā sākumā norādīšu, ka Savienībā priekšroka ir dota koncepcijai, saskaņā ar kuru noteikums par neatkarīgas iestādes veiktu ārēju uzraudzību ir obligāta visas sistēmas sastāvdaļa, kuras mērķis ir nodrošināt tiesību normu attiecībā uz personas datu aizsardzību ievērošanu.

146. Turklāt, lai nodrošinātu Direktīvas 95/46 25. panta 1.–3. punkta lietderīgo iedarbību, ir jāņem vērā, ka trešajā valstī nodrošinātā aizsardzības līmeņa pienācīgums ir pārmaiņām pakļauta situācija, kas daudzu faktoru ietekmē laika gaitā var mainīties. Tāpēc dalībvalstīm un Komisijai pastāvīgi rūpīgi ir jāseko visām apstākļu izmaiņām, kuru dēļ var rasties nepieciešamība atkārtoti izvērtēt trešajā valstī nodrošinātā aizsardzības līmeņa pienācīgumu. Trešajā valstī nodrošinātā aizsardzības līmeņa pienācīguma novērtējums nevar tikt veikts kādā konkrētā brīdī un vēlāk pastāvīgi saglabāts, neraugoties uz apstākļu izmaiņām, kas liecina par to, ka faktiski aizsardzības līmenis vairs nav pienācīgs.

56 — Skat. 5. lpp. Komisijas darba dokumentā WP 12 "Personas datu pārsūtīšana uz trešām valstīm: ES Datu aizsardzības direktīvas 25. un 26. panta piemērošana", ko 1998. gada 24. jūlijā ir pieņēmusi Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi.

147. Tādējādi trešajai valstij ir pienākums pastāvīgi nodrošināt pienācīgu aizsardzības līmeni. Ja novērtējums ir veikts kādā konkrētā brīdī, tad priekšnosacījums lēmuma par atbilstību saglabāšanai ir tāds, ka kopš tā laika nav radies neviens apstāklis, ar kuru varētu tikt apstrīdēts Komisijas sākotnējais vērtējums.

148. Nedrīkst neņemt vērā, ka joprojām Direktīvas 95/46 25. panta mērķis ir novērst personas datu pārsūtīšanu uz trešo valsti, kas nenodrošina pienācīgu aizsardzības līmeni, pārkāpjot pamattiesības uz personas datu aizsardzību, kas ir garantētas ar Hartas 8. pantu.

149. Jāuzsver, ka pilnvaras konstatēt, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, kuras Komisijai ir piešķīris Savienības likumdevējs ar Direktīvas 95/46 25. panta 6. punktu, tieši ir pakļautas prasībai, ka šī trešā valsts nodrošina pienācīgu aizsardzības līmeni šī panta 2. punkta izpratnē. Tāpēc, ja jaunie apstākļi ir tādi, ka ar tiem var tikt apstrīdēts sākotnējais Komisijas novērtējums, tai tādējādi būtu jāpieņem savs lēmums.

3) Mans vērtējums

150. Atgādināšu, ka atbilstoši Direktīvas 95/46 25. panta 6. punktam "saskaņā ar 31. panta 2. punktā minēto procedūru Komisija var konstatēt, ka trešā valsts nodrošina pietiekamu [pienācīgu] aizsardzības līmeni šā panta 2. punkta nozīmē, pamatojoties uz savas valsts tiesībām vai uz starptautiskajām saistībām, kuras tā noslēgusi [uzņēmusies], jo īpaši uz 5. punktā minēto sarunu par personu privātās dzīves un pamatbrīvību un tiesību aizsardzību atzinumu". Skatot kopsakarā ar šīs direktīvas 25. panta 2. punktu, tās 25. panta 6. punkts nozīmē, ka, lai konstatētu, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, Komisijai ir jāveic visu šajā trešajā valstī spēkā esošo tiesību normu, kā arī to piemērošanas novērtējums.

151. Kā norādīts, tas, ka Komisija paturēja spēkā Lēmumu 2000/520, neņemot vērā jaunos tiesiskos un faktiskos apstākļus, ir jāsaprot tādējādi, ka tā vēlējās apstiprināt tās sākotnējo novērtējumu.

152. Tiesai prejudiciālā nolēmuma tiesvedībā nav jāvērtē pamatlietas rašanās fakti, kuru dēļ valsts tiesa ir nolēmusi iesniegt šo lūgumu sniegt prejudiciālu nolēmumu [57].

153. Tāpēc es balstīšos tikai uz faktiem, kurus iesniedzējtiesa ir norādījusi savā lūgumā sniegt prejudiciālu nolēmumu un kurus arī pati Komisija atzīst par pierādītiem [58].

154. Tiesā norādītie apstākļi, kas lika apstrīdēt Komisijas novērtējumu, saskaņā ar kuru "drošības zonas" režīms nodrošina pienācīgu aizsardzības līmeni no Savienības uz Amerikas Savienotajām Valstīm pārsūtītajiem personas datiem, var tikt aprakstīti šādi.

155. Savā lūgumā sniegt prejudiciālu nolēmumu iesniedzējtiesa min šādus divus faktus. Pirmkārt, personas datus, kurus tādi uzņēmumi kā *Facebook Ireland* pārsūta saviem mātesuzņēmumiem Amerikas Savienotajās Valstīs, vēlāk var izmantot *NSA*, kā arī citas ASV drošības aģentūras, veicot plašu un nediferencētu datu uzraudzību un pārtveršanu. Pēc *E. Snowden* atklātās informācijas no pieejamajiem pierādījumiem pašlaik vēl nevar tikt izdarīts neviens cits ticams secinājums [59]. Otrkārt, Savienības pilsoņiem neesot nekādu efektīvu tiesību tikt uzklausītiem jautājumā par to, ka *NSA* un citas ASV drošības aģentūras veic viņu datu pārtveršanu un uzraudzību [60].

57 — Skat. it īpaši spriedumu *Fallimento Traghetti del Mediterraneo* (C-140/09, EU:C:2010:335, 22. punkts un tajā minētā judikatūra).

58 — Skat. 2. zemsvītras piezīmē minēto Komisijas Paziņojumu Eiropas Parlamentam un Padomei par "drošības zonas" darbību no Savienības pilsoņu un uzņēmumu, kas veic uzņēmējdarbību Savienībā, viedokļa [COM(2013) 847 *final*].

59 — Lūguma sniegt prejudiciālu nolēmumu 7. punkta c) apakšpunkts.

60 — Lūguma sniegt prejudiciālu nolēmumu 7. punkta b) apakšpunkts.

156. Augstās tiesas veiktos faktu konstatējumus arī pamato Komisijas veiktie faktu konstatējumi.

157. Tādējādi savā iepriekš minētajā paziņojumā par "drošības zonas" darbību, no Savienības pilsoņu un tās teritorijā reģistrētu uzņēmumu viedokļa raugoties, Komisija ir konstatējusi, ka 2013. gadā informācija par Amerikas Savienoto Valstu uzraudzības programmu apjomu un tvērumu ir radījusi bažas par to personas datu nepārtrauktu aizsardzību, kuri likumīgi tiek pārsūtīti uz Amerikas Savienotajām Valstīm saskaņā ar "drošības zonas" režīmu. Tā ir norādījusi, ka visi *PRISM* programmā iesaistītie uzņēmumi, kas ASV iestādēm atļauj piekļūt Amerikas Savienotajās Valstīs uzglabātiem un apstrādātiem datiem, šķiet, ir sertificēti "drošības zonas" sakarā. Tādējādi tās ieskatā "drošības zonas" režīms ir kļuvis par vienu no kanāliem, pa kuriem ASV izlūkdienesti iegūst piekļuvi to personas datu vākšanai, kas sākotnēji ir apstrādāti Savienībā [61].

158. No šiem apstākļiem izriet, ka saskaņā ar Amerikas Savienoto Valstu tiesībām un praksi, īstenojot "drošības zonas" režīmu, ir atļauts plašā mērogā vākt Savienības pilsoņu personas datus, nenodrošinot pēdējiem minētajiem efektīvu tiesību aizsardzību tiesā.

159. Šie faktu konstatējumi, manuprāt, pierāda, ka Lēmumā 2000/520 nav pietiekamu garantiju. Ņemot vērā šo garantiju trūkumu, šis lēmums tika īstenots, neievērojot Hartā, kā arī Direktīvā 95/46 izvirzītās prasības.

160. Tomēr lēmuma, kuru Komisija ir pieņēmusi saskaņā ar Direktīvas 95/46 25. panta 6. punktu, mērķis ir konstatēt, ka trešā valsts "nodrošina" pienācīgu aizsardzības līmeni. Jēdziens "nodrošina", kas lietots tagadnes formā, nozīmē, ka, lai šis lēmums varētu tikt saglabāts, tam ir jāattiecas uz trešo valsti, kas pēc minētā lēmuma pieņemšanas turpina nodrošināt pienācīgu aizsardzības līmeni.

161. Faktiski atklātā informācija par *NSA*, kas esot izmantojusi "drošības zonas" režīma ietvaros pārsūtītos datus, darbībām ir izgaismojusi Lēmuma 2000/520 juridiskā pamata trūkumus.

162. Šajā tiesvedībā atklātie trūkumi it īpaši ir konstatēti šī lēmuma I pielikuma ceturtajā daļā.

163. Atgādināšu, ka saskaņā ar šo tiesību normu "šo ["drošības zonas"] principu ievērošanu var ierobežot: a) ciktāl tas ir vajadzīgs, lai ievērotu valsts drošību, sabiedrības intereses vai izpildītu piemērošanas prasības; b) ar likumu, valdības noteikumiem vai tiesu praksi, kas rada pretrunīgus pienākumus, vai paredz skaidras atļaujas, ja, izmantojot šādu atļauju, organizācija var pierādīt, ka principu neievērošana ir tikai tiktāl, ciktāl ir vajadzīgs, lai ievērotu sevišķi svarīgas likumīgās intereses, kuras izriet no šādas atļaujas".

164. Būtībā problēma rodas tāpēc, ka ASV iestādes izmanto minētajā tiesību normā paredzētās atkāpes. Tā kā tās ir formulētas pārāk vispārīgi, iestādes neīsteno šīs atkāpes tikai tiktāl, ciktāl tas ir vajadzīgs.

165. Šim pārmērīgi vispārīgajam formulējumam pievienojas apstāklis, ka Savienības pilsoņiem nav pienācīga tiesību aizsardzības līdzekļa pret viņu personas datu apstrādi, lai īstenotu citus mērķus, nevis tos, kuru dēļ tie sākotnēji tika vākti un vēlāk tika pārsūtīti uz Amerikas Savienotajām Valstīm.

166. Līdztekus Lēmumā 2000/520 paredzētajām atkāpēm no "drošības zonas" principu piemērošanas, lai it īpaši ievērotu valsts drošības prasības, būtu bijis jāizveido neatkarīgs uzraudzības mehānisms, lai novērstu konstatēto tiesību uz privātās dzīves neaizskaramību neievērošanu.

167. Tādējādi informācija par ASV izlūkdienestu praksi vispārīgi uzraudzīt pārsūtītos datus saistībā ar "drošības zonas" režīmu atklāja konkrētus Lēmuma 2000/520 trūkumus.

61 — Paziņojuma 19. lpp.

168. Izskatāmajā lietā minētie apgalvojumi nav *Facebook* "drošības zonas" principu pārkāpums. Lai arī tāds sertificēts uzņēmums kā *Facebook USA* ASV iestādēm nodrošina piekļuvi dalībvalsts pārsūtītajiem datiem, var tikt uzskatīts, ka tas to veic saskaņā ar ASV tiesību aktiem. Tā kā šāda situācija Lēmumā 2000/520, ņemot vērā tajā paredzēto atkāpju pārāk plašo formulējumu, ir skaidri pieļauta, izskatāmajā lietā faktiski rodas jautājums par šādu atkāpju saderīgumu ar Savienības primārajām tiesībām.

169. Šajā ziņā ir jāuzsver, ka no Tiesas pastāvīgās judikatūras izriet, ka pamattiesību ievērošana ir Savienības tiesību aktu tiesiskuma nosacījums un ka Savienībā nav pieļaujami pasākumi, kas nav saderīgi ar to ievērošanu [62].

170. Turklāt no Tiesas judikatūras arī izriet, ka savākto personas datu paziņošana trešajām personām – valsts vai privātām – ir iejaukšanās tiesībās uz privātās dzīves neaizskaramību "neatkarīgi no nodotās informācijas tālākās izmantošanas" [63]. Savā spriedumā *Digital Rights Ireland* u.c. [64] Tiesa ir apstiprinājusi, ka atļaujas sniegšana kompetentajām valsts iestādēm piekļūt šādiem datiem ir papildu un cita veida šo pamattiesību aizskārums [65]. Turklāt Hartas 8. pants attiecas uz jebkāda veida personas datu apstrādi, un tā ir iejaukšanās tiesībās uz šādu datu aizsardzību [66]. Tāpēc, nodrošinot ASV izlūkdienestiem piekļuvi pārsūtītajiem datiem, notiek iejaukšanās ar Hartas 8. pantu garantētajās pamattiesībās uz personas datu aizsardzību neievērošana, jo šāda piekļuve nozīmē šo datu apstrādi.

171. Kā šajā spriedumā ir konstatējusi Tiesa, konstatētā iejaukšanās tāpēc ir ļoti plaša un, ņemot vērā, ka tā ir skārusi lielu lietotāju skaitu un pārsūtīto datu daudzumu, tā ir jāuzskata par īpaši smagu. Šie apstākļi kopā ar ASV iestāžu slepeno piekļuvi personas datiem, kas tika pārsūtīti Amerikas Savienotajās Valstīs reģistrētajiem uzņēmumiem, padara iejaukšanos par īpaši būtisku.

172. Turklāt tam pievienojas apstāklis, ka Savienības pilsoņi, *Facebook* lietotāji, nav informēti par to, ka viņu personas dati būs vispārīgi pieejami ASV drošības aģentūrām.

173. Ir jāuzsver arī iesniedzējtiesas secinājums par to, ka Savienības pilsoņiem Amerikas Savienotajās Valstīs nav efektīvu tiesību tikt uzklausītiem jautājumā par viņu datu uzraudzību un pārtveršanu. *FISC* piekritībā ir veikt uzraudzību, taču tiesvedība tajā norisinās slepeni, un tajā netiek ievērots sacīkstes princips [67]. Uzskatu, ka runa ir par iejaukšanos Savienības pilsoņu tiesībās uz efektīvu tiesību aizsardzību tiesā, kas ir garantētas ar Hartas 47. pantu.

174. Tāpēc ir jākonstatē iejaukšanās, ar ko ir pieļautas Lēmuma 2000/520 I pielikuma ceturtajā daļā paredzētās atkāpes no to pamattiesību ievērošanas, kas ir aizsargātas ar Hartas 7., 8. un 47. pantu.

175. Tālāk ir jāpārbauda, vai šī iejaukšanās ir vai nav pamatota.

176. Atbilstoši Hartas 52. panta 1. punktam visiem tajā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos, tajos jārespektē šo tiesību un brīvību būtība un, ievērojot samērīguma principu, ierobežojumus šīm tiesībām un brīvībām drīkst noteikt tikai tad, ja tie ir vajadzīgi un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai arī vajadzībai aizsargāt citu personu tiesības un brīvības.

62 — Skat. it īpaši spriedumu *Kadi* un *Al Barakaat International Foundation*/Padome un Komisija (C-402/05 P un C-415/05 P, EU:C:2008:461, 284. punkts un tajā minētā judikatūra).

63 — Spriedums *Österreichischer Rundfunk* u.c. (C-465/00, C-138/01 un C-139/01, EU:C:2003:294, 74. punkts).

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

65 — 35. punkts.

66 — 36. punkts.

67 — Lūguma sniegt prejudiciālu nolēmumu 7. punkta b) apakšpunkts.

177. Ņemot vērā šādus nosacījumus attiecībā uz pilnvarām noteikt ar Hartu aizsargāto tiesību un brīvību īstenošanas ierobežojumus, man ir lielas šaubas, vai izskatāmajā lietā aplūkotie ierobežojumi varētu tikt uzskatīti par tādiem, ar kuriem tiek respektēta Hartas 7. un 8. panta būtība. ASV izlūkdienestiem nodrošinātā piekļuve pārsūtītajiem datiem, šķiet, attiecas arī uz elektronisko komunikāciju saturu, kā rezultātā netiek ievērotas ar Hartas 7. pantu garantētās pamattiesības uz privātās dzīves neaizskaramību un citas tiesības. Turklāt, ciktāl Lēmuma 2000/520 I pielikuma ceturtajā daļā paredzēto ierobežojumu plašā formulējuma dēļ, iespējams, varētu tikt noraidīta visu "drošības zonas" principu piemērošana, varētu tikt uzskatīts, ka šie ierobežojumi aizskar pamattiesību uz personas datu aizsardzību būtību [68].

178. Attiecībā uz jautājumu par to, vai konstatētā iejaukšanās atbilst vispārējo interešu mērķiem, sākumā atgādināšu, ka saskaņā ar Lēmuma 2000/520 I pielikuma ceturtās daļas b) punktu apņemšanās ievērot "drošības zonas" principus var tikt ierobežota "ar likumu, valdības noteikumiem vai tiesu praksi, kas rada pretrunīgus pienākumus, vai paredz skaidras atļaujas, ja, izmantojot šādu atļauju, organizācija var pierādīt, ka principu neievērošana ir tikai tiktāl, ciktāl ir vajadzīgs, lai ievērotu sevišķi svarīgas likumīgās intereses, kuras izriet no šādas atļaujas".

179. Jākonstatē, ka šajā tiesību normā minētās "likumīgās intereses" nav precizētas. No tā izriet nenoteiktība attiecībā uz šīs atkāpes no "drošības zonas" principa, kuru ir apņēmušies piemērot uzņēmumi, iespējams, ļoti plašo tvērumu.

180. Lēmuma 2000/520 IV pielikuma B punktā "Likumā skaidri noteiktas atļaujas" ietvertie paskaidrojumi apstiprina šo iespaidu, it īpaši apgalvojumu, saskaņā ar kuru "ir skaidrs, ka, ja ASV tiesību akti uzliek pretrunīgas saistības, ASV organizācijām, neatkarīgi no tā, vai tās ir "drošības zonā" vai nē, tie ir jāievēro". Turklāt attiecībā uz skaidrām atļaujām ir norādīts, ka, "lai gan "drošības zonas" principi ir paredzēti, lai pārvarētu ASV un Eiropas sistēmu atšķirības attiecībā uz privātās dzīves aizsardzību, [..] mēs pievērsīsimies mūsu ievēlēto likumdevēju likumdošanas prerogatīvām".

181. Manuprāt, no tā izriet, ka šī atkāpe ir pretrunā Hartas 7. un 8. pantam un 52. panta 1. punktam, ciktāl ar to netiek īstenoti pietiekami precīzi noteiktie vispārējo interešu mērķi.

182. Katrā ziņā iespēja un vispārīgums, ar kādiem pašā Lēmumā 2000/520, tā I pielikuma ceturtās daļas b) punktā un IV pielikuma B punktā ir paredzēta iespēja neievērot "drošības zonas" principus, piemērojot ASV tiesību normas, nav saderīgi ar nosacījumu, saskaņā ar kuru atkāpes no normām attiecībā uz personas datu aizsardzību ir jāierobežo līdz līmenim, kāds nepieciešams šādu darbību veikšanai. Vajadzības nosacījums, protams, ir minēts, bet, izņemot to, ka šī nosacījuma [izpilde] ir jāpierāda attiecīgajam uzņēmumam, es nesaprotu, kā šis uzņēmums varētu nepildīt pienākumu ievērot "drošības zonas" principus, kas izriet no tam saistošām tiesību normām.

183. Tāpēc es uzskatu, ka Lēmums 2000/520 ir jāpasludina par spēkā neesošu, ciktāl atkāpes, ar kuru vispārīgi un neprecīzi ir atļauts neievērot "drošības zonas" principus, esamība kā tāda neļauj uzskatīt, ka šis režīms nodrošina pienācīgu aizsardzības līmeni personas datiem, kas no Savienības tiek pārsūtīti uz Amerikas Savienotajām Valstīm.

184. Tālāk, runājot par pirmo Lēmuma 2000/520 I pielikuma ceturtās daļas a) punktā paredzēto ierobežojumu kategoriju, lai ievērotu ASV valsts drošību, sabiedriskās intereses un tiesību aktus, tikai pirmais mērķis, manuprāt, ir pietiekami precīzs, lai tas varētu tikt uzskatīts par Savienības atzītu vispārējo interešu mērķi Hartas 52. panta 1. punkta izpratnē.

185. Ir jāpārbauda konstatētās iejaukšanās samērīgums.

68 — Šajā ziņā skat. spriedumu *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238, 39. un 40. punkts).

186. Šajā ziņā ir jāatgādina, ka saskaņā ar pastāvīgo Tiesas judikatūru samērīguma princips prasa, lai Savienības iestāžu akti būtu piemēroti ar attiecīgo tiesisko regulējumu sasniedzamo leģitīmo mērķu īstenošanai un nepārsniegtu šo mērķu sasniegšanai vajadzīgo [69].

187. Attiecībā uz pārbaudi tiesā par šo nosacījumu ievērošanu, ja runa ir par iejaukšanos pamattiesībās, Savienības likumdevēja novērtējuma brīvība var būt ierobežota atkarībā no daudziem faktoriem, tostarp skartās jomas, attiecīgo Hartā garantēto tiesību rakstura, iejaukšanās rakstura un būtiskuma, kā arī tās mērķa [70].

188. Uzskatu, ka Komisijas saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemtie lēmumi ir pakļauti pilnīgai Tiesas pārbaudei attiecībā uz šīs iestādes veiktā novērtējuma samērīgumu ar trešajā valstī nodrošinātās aizsardzības pienācīgumu, "ņemot vērā tās tiesību aktus un tās starptautiskās saistības".

189. Šajā ziņā ir jānorāda, ka savā spriedumā *Digital Rights Ireland* u.c. [71] Tiesa ir nospriedusi, ka, "ņemot vērā, pirmkārt, nozīmīgo lomu, kāda personas datu aizsardzībai ir attiecībā uz pamattiesībām uz privātās dzīves neaizskaramību, un, otrkārt, ar [apstrīdēto] direktīvu [..] radītās iejaukšanās šajās tiesībās apjomu un būtiskumu, Savienības likumdevēja novērtējuma brīvība ir ierobežota un tādējādi jāveic stingra pārbaude" [72].

190. Ar šādu iejaukšanos ir jāspēj īstenot attiecīgajā Savienības tiesību aktā izvirzīto mērķi, un tai ir jābūt vajadzīgai šī mērķa sasniegšanā.

191. Šajā ziņā "attiecībā uz tiesībām uz privātās dzīves neaizskaramību ir jānorāda, ka atbilstoši Tiesas pastāvīgajai judikatūrai to aizsardzība [..] prasa, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti absolūti nepieciešamā ietvaros" [73].

192. Veicot pārbaudi, Tiesa arī ņem vērā apstākli, ka "personas datu aizsardzība, kas izriet no Hartas 8. panta 1. punktā skaidri izteiktā pienākuma, ir īpaši nozīmīga tās 7. pantā nostiprinātajām tiesībām uz privātās dzīves neaizskaramību" [74].

193. Tiesa, kas šajā ziņā atsaucas uz Eiropas Cilvēktiesību tiesas judikatūru, uzskata, ka "attiecīgajā Savienības tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentētu attiecīgā pasākuma apjomu un piemērošanu un noteiktu minimālas prasības tādējādi, lai personām, kuru dati tikuši saglabāti, būtu pietiekamas garantijas, kas ļautu to personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu" [75]. Tiesa norāda, ka "šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka [..] personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves šiem datiem risks" [76].

194. Manuprāt, pastāv analoģija starp Lēmuma 2000/520 I pielikuma ceturtās daļas a) punktu un Direktīvas 95/46 13. panta 1. punktu. Pirmajā minētajā tiesību normā ir norādīts, ka "drošības zonas" principu ievērošana var tikt ierobežota, ciktāl tas ir vajadzīgs, lai ievērotu Amerikas Savienoto Valstu "valsts drošību, sabiedrības intereses vai izpildītu piemērošanas prasības". Otrajā minētajā tiesību normā ir paredzēts, ka dalībvalstis drīkst veikt likumdošanas pasākumus, lai ierobežotu šīs direktīvas

69 — Spriedums *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238, 46. punkts, kā arī tajā minētā judikatūra).

70 — Turpat (47. punkts un tajā minētā judikatūra).

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

72 — 48. punkts.

73 — Spriedums *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238, 52. punkts, kā arī tajā minētā judikatūra).

74 — Turpat (53. punkts).

75 — Turpat (54. punkts un tajā minētā judikatūra).

76 — Turpat (55. punkts un tajā minētā judikatūra).

6. panta 1. pantā, 10. pantā, 11. panta 1. punktā un 12. un 21. pantā paredzēto tiesību un pienākumu piemērojamību gadījumos, kad šāds ierobežojums ir pasākums, kas ir vajadzīgs it īpaši valsts drošības, aizsardzības, sabiedrības drošības, kā arī noziegumu novēršanas, atklāšanas, izmeklēšanas un kriminālvajāšanas mērķiem.

195. Kā Tiesa ir norādījusi savā spriedumā *IPI*[77], no Direktīvas 95/46 13. panta 1. punkta formulējuma izriet, ka dalībvalstis var noteikt šajā tiesību normā paredzētos pasākumus tikai tad, kad tie ir nepieciešami. Pasākumu "nepieciešamība" tādējādi ir nosacījums iespējai, kas dalībvalstīm ir dota ar minēto tiesību normu[78]. Attiecībā uz personas datu apstrādi Savienībā šīs direktīvas 13. pantā paredzētie ierobežojumi ir jāsaprot kā tādi, kas ir obligāti nepieciešami, lai sasniegtu izvirzīto mērķi. Tas pats, manuprāt, ir attiecināms uz Lēmuma 2000/520 I pielikuma ceturtajā daļā paredzētajiem "drošības zonas" principu ierobežojumiem.

196. Tomēr ir jākonstatē, ka ne visās valodu redakcijās Lēmuma 2000/520 I pielikuma ceturtās daļas a) punkta formulējumā ir minēts nepieciešamības kritērijs. Tas it īpaši ir sakāms par franču valodas redakciju, kurā ir norādīts, ka "šo principu ievērošanu var ierobežot [..] prasības attiecībā uz valsts drošību, sabiedrības interesēm vai Amerikas Savienoto Valstu tiesību aktu ievērošanu", lai gan, piemēram, spāņu, vācu un angļu valodu redakcijās ir norādīts, ka noteiktie ierobežojumi ir vajadzīgi, lai sasniegtu iepriekšminētos mērķus.

197. Lai kā arī būtu, faktiskie apstākļi, kurus ir minējušas iesniedzējtiesa, kā arī Komisija savos iepriekš minētajos paziņojumos, skaidri atspoguļo to, ka šī ierobežojuma īstenošanu praksē nenosaka tas, kas ir obligāti vajadzīgs minēto mērķu sasniegšanā.

198. Šajā ziņā norādīšu, ka ASV izlūkdienestiem piešķirtā piekļuve pārsūtītajiem personas datiem vispārīgi aptver visas personas un visus elektroniskās komunikācijas līdzekļus, kā arī visu pārsūtīto datu kopumu, ieskaitot komunikāciju saturu, nešķirojot un bez ierobežojumiem vai izņēmumiem saistībā ar izvirzīto vispārējo interešu mērķi[79].

199. ASV izlūkdienestiem sniegtā piekļuve pārsūtītajiem datiem vispārīgi attiecas uz visām personām, kas izmanto elektronisko komunikāciju pakalpojumus, neprasot, vai attiecīgās personas rada draudus valsts drošībai[80].

200. Šāda plaša un nediferencēta uzraudzība būtībā nav samērīga un ir nepamatota iejaukšanās ar Hartas 7. un 8. pantu nostiprinātajās tiesībās.

201. Kā savos apsvērumos pamatoti ir norādījis Parlaments, tā kā Savienības likumdevējs vai dalībvalstis nevar pieņemt normatīvos aktus, ar kuriem Hartas neievērošanas gadījumā tiktu paredzēta plaša un nediferencēta uzraudzība, no tā noteikti izriet, ka nekādi nevar tikt uzskatīts, ka trešās valstis nodrošina pienācīgu Savienības pilsoņu personas datu aizsardzību, ja to tiesiskajā regulējumā faktiski ir atļauta plaša un nediferencēta šādu datu uzraudzība un pārtveršana.

202. Turklāt ir jāuzsver, ka "drošības zonas" režīmā, kā tas ir definēts Lēmumā 2000/520, nav paredzētas attiecīgās garantijas, lai novērstu plašu un vispārēju piekļuvi pārsūtītajiem datiem.

77 — C-473/12, EU:C:2013:715.

78 — 32. punkts.

79 — Skat. pēc analoģijas spriedumu *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238, 57. punkts un tajā minētā judikatūra).

80 — Turpat (58. un 59. punkts).

203. Šajā ziņā norādīšu, ka Tiesa spriedumā *Digital Rights Ireland* u.c.[81] ir uzsvērusi, ka ir jāparedz "skaidri un precīzi noteikumi, kas reglamentētu iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās apjomu"[82]. Tiesas skatījumā šī iejaukšanās ir precīzi jāreglamentē "ar tiesību normām, kas ļautu nodrošināt, lai tā patiešām būtu ierobežota ar absolūti nepieciešamo"[83]. Tiesa šajā pašā spriedumā arī ir uzsvērusi nepieciešamību paredzēt "pietiekamas garantijas, tādas kā Hartas 8. pantā prasītās, kas ļautu nodrošināt saglabāto [personas] datu efektīvu aizsardzību pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu"[84].

204. Tomēr ir jākonstatē, ka *FTC* un privāti strīdu izšķiršanas mehānismi, ņemot vērā to relatīvo nozīmi komercstrīdos, nav līdzekļi, lai apstrīdētu ASV izlūkdienestiem nodrošināto piekļuvi personas datiem, kas ir pārsūtīti no Savienības.

205. *FTC* jurisdikcijā ir arī lietas par negodīgu vai krāpniecisku darbību vai praksi tirdzniecībā, un tāpēc tai nav jurisdikcijas pār personiskas informācijas vākšanu un izmantošanu nekomerciāliem nolūkiem[85]. *FTC* ierobežotās kompetences joma ierobežo privātpersonu tiesības uz personas datu aizsardzību. *FTC* tika izveidota, nevis lai nodrošinātu individuālās tiesības uz privātās dzīves neaizskaramību, kā tas ir Savienībā valsts uzraudzības iestāžu gadījumā, bet lai nodrošinātu patērētājiem lojālu un ticamu tirdzniecību, kas *de facto* ierobežo tās iejaukšanās spēju personas datu aizsardzības jomā. Tāpēc *FTC* nozīme nav salīdzināma ar Direktīvas 95/46 28. pantā paredzēto valsts uzraudzības iestāžu nozīmi.

206. Savienības pilsoņi, kuru dati tikuši pārsūtīti, var vērsties tādās specializētās Amerikas Savienotajās Valstīs reģistrētās strīdu izšķiršanas iestādēs kā *TRUSTe* un *BBBOnline*, lai lūgtu precizējumus par to, vai uzņēmums, kura rīcībā ir viņu personas dati, nepārkāpj pašsertifikācijas režīma nosacījumus. Tādām iestādēm kā *TRUSTe* izšķirot strīdus privātā kārtā, tās nevar izskatīt tiesību uz personas datu aizsardzību pārkāpumus, kurus ir izdarījušas iestādes vai struktūras, kas nav pašsertificēti uzņēmumi. Šo strīdu izšķiršanas iestāžu kompetencē nav lemt par ASV drošības aģentūru darbību tiesiskumu.

207. Tātad nedz *FTC*, nedz privāto strīdu izšķiršanas iestāžu kompetencē nav pārbaudīt iespējamos personas datu aizsardzības principu pārkāpumus, kurus ir izdarījuši tādi publisko tiesību subjekti kā ASV drošības aģentūras. Tomēr šādai kompetencei var būt būtiska nozīme, lai pilnībā nodrošinātu tiesības uz efektīvu šo datu aizsardzību. Tātad, pieņemot Lēmumu 2000/520 un paturot to spēkā, Komisija nevarēja konstatēt, ka visiem uz Amerikas Savienotajām Valstīm pārsūtītajiem personas datiem tiks nodrošināta pienācīga aizsardzība, kas piešķirta ar Hartas 8. panta 3. punktu, proti, ka neatkarīga iestāde veiks efektīvu kontroli attiecībā uz šo datu drošības un aizsardzības prasību ievērošanu.

208. Tādēļ ir jākonstatē, ka Lēmumā 2000/520 noteiktajā "drošības zonas" režīmā nav paredzētas neatkarīgas iestādes, kas varētu uzraudzīt, vai atkāpju no "drošības zonas" principiem īstenošanā ir darīts tikai obligāti nepieciešamais. Tomēr, kā tika norādīts, šāda neatkarīgas iestādes saskaņā ar Savienības tiesībām veikta uzraudzība ir būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi[86].

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

82 — 65. punkts.

83 — Turpat.

84 — Turpat (66. punkts).

85 — Šajā ziņā skat. Lēmuma 2000/520 II pielikuma "*FTC* darbība" *FAQ* 11 un tā III, V un VII pielikumu.

86 — Spriedums *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238, 68. punkts, kā arī tajā minētā judikatūra).

209. Šajā ziņā ir jāuzsver nozīme, kāda valsts uzraudzības iestādēm ir Savienībā spēkā esošajā personas datu aizsardzības sistēmā attiecībā uz Direktīvas 95/46 13. pantā paredzēto ierobežojumu uzraudzību. Saskaņā ar šīs direktīvas 28. panta 4. punkta otro daļu "katra uzraudzības iestāde uzklausa jebkuras personas iesniegtās prasības par datu apstrādes likumības pārbaudēm, ja piemērojami saskaņā ar šīs direktīvas 13. pantu pieņemtie attiecīgās valsts noteikumi". Pēc analoģijas es uzskatu, ka papildus Lēmuma 2000/520 I pielikuma ceturtajā daļā paredzētajiem "drošības zonas" principu ierobežojumiem būtu jāizveido uzraudzības mehānisms, kura darbību nodrošinātu neatkarīga iestāde, kas specializējusies personas datu aizsardzības jomā.

210. Neatkarīgu uzraudzības iestāžu iejaukšanās ir Eiropas personas datu aizsardzības sistēmas pamatā. Tātad ir pilnīgi dabiski, ka šādas iestādes esamība tiek uzskatīta par vienu no nepieciešamajiem nosacījumiem, lai konstatētu, ka trešajās valstīs ir nodrošināta pienācīga aizsardzība. Tas ir viens nosacījums, lai datu plūsma no dalībvalstu teritorijas uz trešo valsti netiktu aizliegta saskaņā ar Direktīvas 95/46 25. pantu [87]. Kā norādīts diskusiju dokumentā, kuru ir pieņēmusi saskaņā ar šīs direktīvas 29. pantu izveidotā darba grupa, Eiropā pastāv vispārēja vienošanās, saskaņā ar kuru "noteikums par "ārēju uzraudzību", ko veic neatkarīga iestāde, ir nepieciešama tādas sistēmas sastāvdaļa, kuras mērķis ir nodrošināt datu aizsardzības normu ievērošanu" [88].

211. Turklāt norādīšu, ka *FISC* nenodrošina efektīvu tiesību aizsardzību Savienības pilsoņiem, kuru dati tikuši pārsūtīti uz Amerikas Savienotajām Valstīm. Aizsardzība pret valsts dienestu veikto uzraudzību saskaņā ar 1978. gada Likuma par ārvalstu izlūkošanas uzraudzību 702. iedaļu ir nodrošināta tikai ASV pilsoņiem, kā arī ārvalstniekiem, kuri likumīgi un pastāvīgi uzturas Amerikas Savienotajās Valstīs. Kā ir norādījusi Komisija, ASV izlūkdatu vākšanas programmu pārraudzība varētu tikt uzlabota, nostiprinot *FISC* nozīmi un ieviešot tiesiskās aizsardzības līdzekļus privātpersonām. Šie mehānismi varētu mazināt Savienības pilsoņu to personas datu apstrādi, kuri nav būtiski no valsts drošības viedokļa [89].

212. Turklāt pati Komisija ir norādījusi, ka Savienības pilsoņiem nav nekādas iespējas iegūt piekļuvi datiem vai panākt to labošanu vai dzēšanu, vai izmantot administratīvus vai juridiskus tiesiskās aizsardzības līdzekļus attiecībā uz viņu personas datu vākšanu un turpmāku apstrādi saskaņā ar ASV novērošanas programmām [90].

213. Visbeidzot, ir jānorāda, ka ASV normas attiecībā uz privātās dzīves neaizskaramību var tikt piemērotas atšķirīgi ASV pilsoņiem un ārvalstu pilsoņiem [91].

214. No iepriekš minētā izriet, ka Lēmumā 2000/520 nav paredzēti skaidri un precīzi noteikumi, ar kuriem tiktu reglamentēts iejaukšanās Hartas 7. un 8. pantā nostiprinātajās pamattiesībās apjoms. Tādējādi ir jākonstatē, ka šis lēmums un tā piemērošana izraisa plaša apjoma un īpaši būtisku iejaukšanos šajās pamattiesībās un šī iejaukšanās nav precīzi reglamentēta ar tiesību normām, kas ļautu nodrošināt, lai tā patiešām būtu ierobežota ar absolūti nepieciešamo.

215. Pieņemot Lēmumu 2000/520 un paturot to spēkā, Komisija tātad ir pārsniegusi attiecībā uz samērīguma principa ievērošanu noteiktās robežas, ņemot vērā Hartas 7. un 8. pantu un 52. panta 1. punktu. Ir arī jākonstatē nepamatota iejaukšanās Savienības pilsoņu tiesībās uz efektīvu tiesību aizsardzību tiesā, kas ir aizsargātas ar Hartas 47. pantu.

87 — Skat. Poullet, Y., "L'autorité de contrôle: 'vues' de Bruxelles", *Revue française d'administration publique*, Nr. 89, janvāris – marts 1999, 69. lpp., it īpaši 71. lpp.

88 — Skat. 7. lpp. Komisijas darba dokumentā WP 12, kas minēts 56. zemsvītras piezīmē.

89 — Skat. Komisijas paziņojuma, kas minēts 2. zemsvītras piezīmē, 10. un 11. lpp.

90 — Skat. Komisijas paziņojuma, kas minēts 58. zemsvītras piezīmē, 7.2. punktu, 20. lpp.

91 — Attiecībā uz šo jautājumu skat. Kuner, C., "Foreign Nationals and Data Protection Law: A Transatlantic Analysis", *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Kembridža, 2014, 213. lpp., it īpaši 216. un nākamās lpp.

216. Tādējādi lēmums ir jāpasludina par spēkā neesošu, jo, ņemot vērā iepriekš aprakstītos pamattiesību pārkāpumus, nevar tikt uzskatīts, ka ar to izveidotais "drošības zonas" režīms nodrošina atbilstīgu aizsardzības līmeni personas datiem, kas saskaņā ar šo režīmu tiek pārsūtīti no Savienības uz Amerikas Savienotajām Valstīm.

217. Ņemot vērā šo Savienības pilsoņu pamattiesību pārkāpumu konstatējumu, es uzskatu, ka Komisijai būtu bijusi jāaptur Lēmuma 2000/520 piemērošana.

218. Šis lēmums ir pieņemts uz nenoteiktu laiku. Tomēr izskatāmā lieta atspoguļo to, ka trešajā valstī nodrošinātā aizsardzības līmeņa pienācīgums, ņemot vērā izmaiņas gan faktiskajos, gan tiesiskajos apstākļos, kas bijuši minētā lēmuma pamatā, pēc noteikta laika var mainīties.

219. Norādīšu, ka pašā Lēmumā 2000/520 ir tiesību normas, ar kurām Komisijai ir paredzēta iespēja to pielāgot atbilstoši apstākļiem.

220. Tādējādi no šī lēmuma preambulas 9. apsvēruma izriet, ka ""drošības zona", kas ir noteikta ar principiem un *FAQ*, varbūt ir jāpārskata, ņemot vērā pieredzi, attīstību attiecībā uz privātās dzīves aizsardzību apstākļos, kad tehnoloģijas pastāvīgi atvieglo personas datu nosūtīšanu un apstrādi, un ņemot vērā iesaistīto izpildiestāžu ziņojumus par veikto piemērošanu".

221. Tāpat saskaņā ar minētā lēmuma 3. panta 4. punktu, "ja saskaņā ar 1., 2. un 3. punktu apkopotā informācija liecina par to, ka kāda no iestādēm, kas Amerikas Savienotajās Valstīs ir atbildīga par atbilstīgi *FAQ* īstenoto principu ievērošanu, savu uzdevumu pilda neefektīvi, tad Komisija informē ASV Tirdzniecības ministriju un, vajadzības gadījumā, iesniedz pasākumu projektu [..] nolūkā panākt, lai šo lēmumu atceltu vai apturētu vai lai ierobežotu tā darbības jomu".

222. Turklāt saskaņā ar Lēmuma 2000/520 4. panta 1. punktu to "var pielāgot jebkurā laikā, ņemot vērā pieredzi saistībā ar tā īstenošanu un/vai, ja ASV tiesību aktos ietver prasības nodrošināt augstāku aizsardzības līmeni, nekā to nodrošina principi un *FAQ*. Komisija katrā ziņā trīs gadus pēc paziņošanas dalībvalstīm novērtē šā lēmuma īstenošanu, pamatojoties uz pieejamo informāciju, un par visiem atbilstīgajiem atzinumiem ziņo Komitejai, kas izveidota saskaņā ar Direktīvas 95/46[..] 31. pantu, tostarp par pierādījumiem, kuri varētu ietekmēt novērtējumu, ka šā lēmuma 1. pantā paredzētie noteikumi nodrošina pienācīgu aizsardzību Direktīvas 95/46 25. panta nozīmē". Atbilstīgi Lēmuma 2000/520 4. panta 2. punktam "Komisija, vajadzības gadījumā, saskaņā ar Direktīvas 95/46 31. pantā norādīto procedūru iesniedz pasākumu projektu".

223. Savos rakstveida apsvērumos Komisija ir konstatējusi, ka "ir liela varbūtība, ka apņemšanās ievērot "drošības zonas" principus ir tikusi ierobežota veidā, kas vairs neatbilst nosacījumiem, kuri obligāti reglamentē valsts drošības jomā paredzēto atkāpi" [92]. Šajā ziņā tā norāda, ka "attiecīgā atklātā informācija liecina par liela mēroga nediferencētu uzraudzības pakāpi, kas nav saderīga ar šajā atkāpē noteikto nepieciešamības principu, nedz – vispārīgāk – ar Hartas 8. pantā nostiprinātajām tiesībām uz personas datu aizsardzību" [93]. Komisija arī ir konstatējusi, ka "šo uzraudzības programmu tvērums apvienojumā ar nevienlīdzīgo attieksmi pret [Savienības] pilsoņiem liek apšaubīt aizsardzības līmeni, ko nodrošina "drošības zonas" režīms" [94].

92 — 44. punkts.

93 — Turpat.

94 — Skat. Komisijas paziņojuma, kas minēts 2. zemsvītras piezīmē, 5. lpp.

224. Turklāt Komisija tiesas sēdē skaidri atzina, ka, īstenojot Lēmumu 2000/520, kā tas pašlaik tiek piemērots, nav garantijas, ka Savienības pilsoņu tiesības uz šo datu aizsardzību tiks nodrošinātas. Tomēr tās ieskatā šis konstatējums nevar padarīt šo lēmumu par spēkā neesošu. Lai arī Komisija piekrīt apgalvojumam, saskaņā ar kuru tai ir jārīkojas jaunajos apstākļos, tā uzskata, ka tā ir veikusi atbilstīgus un samērīgus pasākumus, uzsākot sarunas ar Amerikas Savienotajām Valstīm, lai grozītu "drošības zonas" režīmu.

225. Es nepiekrītu šim viedoklim. Starplaikā personas datu pārsūtīšanu uz Amerikas Savienotajām Valstīm ir jāspēj apturēt – pēc valsts uzraudzības iestāžu ierosmes vai pamatojoties uz tajās ir iesniegtajām sūdzībām.

226. Turklāt es arī uzskatu, ka, ņemot vērā šādus konstatējumus, Komisijai būtu bijusi jāaptur Lēmuma 2000/520 piemērošana. Lai sasniegtu Direktīvā 95/46, kā arī Hartas 8. pantā izvirzīto personas datu aizsardzības mērķi, pienākumi ir uzlikti ne tikai dalībvalstīm, bet arī, kā tas izriet no Hartas 51. panta 1. punkta, Savienības iestādēm.

227. Vērtējot trešajā valstī nodrošinātās aizsardzības līmeni, Komisijai ir jāpārbauda ne tikai šīs trešās valsts tiesību akti un starptautiskās saistības, bet arī tas, kā personas datu aizsardzība tiek nodrošināta praksē. Ja prakses pārbaudē tiek atklāti traucējumi, Komisijai ir jārīkojas un vajadzības gadījumā tās lēmums ir jāaptur un/vai nekavējoties jāpielāgo.

228. Kā norādīts iepriekš, dalībvalstu pienākums ir galvenokārt nodrošināt Direktīvā 95/46 paredzēto tiesību normu ievērošanu ar to valsts uzraudzības iestāžu starpniecību.

229. Komisijas pienākums ir apturēt lēmuma, kuru tā ir pieņēmusi saskaņā ar šīs direktīvas 25. panta 6. punktu, piemērošanu, ja attiecīgajā trešajā valstī ir konstatēti trūkumi, un laikā, kad tā risina sarunas ar šo trešo valsti par šo trūkumu novēršanu.

230. Atgādināšu, ka lēmuma, kuru Komisija ir pieņēmusi, pamatojoties uz šo tiesību normu, mērķis ir konstatēt, ka trešā valsts "nodrošina" pienācīgu aizsardzības līmeni personas datiem, kas tiek pārsūtīti uz šo valsti. Jēdziens "nodrošina", kas ir lietots tagadnes formā, nozīmē, ka, lai šis lēmums varētu tikt paturēts spēkā, tam ir jāattiecas uz trešo valsti, kas pēc minētā lēmuma pieņemšanas turpina nodrošināt pienācīgu aizsardzības līmeni.

231. Saskaņā ar Direktīvas 95/46 preambulas 57. apsvērumu "personu datu pārvedums uz trešo valsti, kura nenodrošina pietiekamu [pienācīgu] aizsardzības līmeni, jāaizliedz".

232. Saskaņā ar šīs direktīvas 25. panta 4. punktu, "ja Komisija saskaņā ar 31. panta 2. punktā paredzēto procedūru konstatē, ka trešā valsts nenodrošina pienācīgu aizsardzības līmeni šā panta 2. punkta nozīmē, dalībvalstis veic vajadzīgos pasākumus, lai aizkavētu jebkādu tāda paša tipa datu pārsūtīšanu uz attiecīgo trešo valsti". Turklāt minētās direktīvas 25. panta 5. punktā ir noteikts, ka "atbilstīgā laikā Komisija sāk sarunas ar nolūku labot situāciju, kura izriet no secinājumiem, kas iegūti saskaņā ar 4. punktu".

233. No šīs pēdējās minētās tiesību normas izriet, ka ar Direktīvas 95/46 25. pantu izveidotajā sistēmā ar šo trešo valsti sarunas tiek uzsāktas, lai novērstu konstatēto nepienācīgo aizsardzības līmeni saskaņā ar minētās direktīvas 31. panta 2. punktā paredzēto procedūru. Aplūkotajā gadījumā Komisija saskaņā ar šo procedūru nav konstatējusi, ka "drošības zonas" režīms vairs nenodrošina pienācīgu aizsardzības līmeni. Tādējādi, ja Komisija būtu nolēmusi uzsākt sarunas ar Amerikas Savienotajām Valstīm, tā vispirms būtu uzskatījusi, ka šajā valstī nodrošinātais aizsardzības līmenis vairs nav pienācīgs.

234. Lai arī Komisija zināja par traucējumiem Lēmuma 2000/520 piemērošanā, tā to nedz atcēla, nedz arī pielāgoja, tādējādi pieļaujot, ka tiek pārkāptas to personu pamattiesības, kuru personas dati tikuši un tiek pārsūtīti saskaņā ar "drošības zonas" režīmu.

235. Tomēr Tiesa jau ir lēmusi, lai arī citā kontekstā, ka Komisijai ir jāraugās, lai tiesiskais regulējums tiktu pielāgots jaunajiem faktiem [95].

236. Šāds Komisijas rīcības trūkums, kas tieši aizskar ar Hartas 7., 8. un 47. pantu aizsargātās tiesības, manuprāt, ir papildu iemesls, lai šajā prejudiciālā nolēmuma tiesvedībā Lēmums 2000/520 tiktu pasludināts par spēkā neesošu [96].

III – **Secinājumi**

237. Ņemot vērā iepriekš minētos apsvērumus, es ierosinu Tiesai uz Augstās tiesas uzdotajiem prejudiciālajiem jautājumiem atbildēt šādi:

Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti 28. pants, skatot to kopsakarā ar Eiropas Savienības Pamattiesību hartas 7. un 8. pantu, ir jāinterpretē tādējādi, ka tāda lēmuma esamība, kuru Eiropas Komisija ir pieņēmusi saskaņā ar Direktīvas 95/46 25. panta 6. punktu, neliedz valsts uzraudzības iestādei izskatīt sūdzību par to, ka trešā valsts nenodrošina pienācīgu pārsūtīto personas datu aizsardzības līmeni, un vajadzības gadījumā apturēt šo datu pārsūtīšanu.

Komisijas 2000. gada 26. jūlija Lēmums 2000/520/EK atbilstīgi Eiropas Parlamenta un Padomes Direktīvai 95/46/EK par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija, nav spēkā.

95 — Šajā ziņā skat. spriedumu *Agrarproduktion Staebelow* (C-504/04, EU:C:2006:30, 40. punkts).

96 — Lai arī Tiesa savā spriedumā *T. Port* (C-68/95, EU:C:1996:452) ir nospriedusi, ka "Līgumā nav paredzēta iespēja iesniegt lūgumu sniegt prejudiciālu nolēmumu, ar kuru iesniedzējtiesa lūgtu Tiesai prejudiciālā nolēmuma tiesvedībā konstatēt iestādes bezdarbību" (53. punkts), šķiet, tā ir pieņēmusi labvēlīgāku nostāju pret šo iespēju savā spriedumā *Ten Kate Holding Musselkanaal* u.c. (C-511/03, EU:C:2005:625, 29. punkts).