



Judikatūras krājums

TIESAS SPRIEDUMS (virspalāta)

2015. gada 6. oktobrī *

Lūgums sniegt prejudiciālu nolēmumu — Personas dati — Fizisku personu aizsardzība attiecībā uz šo datu apstrādi — Eiropas Savienības Pamattiesību harta — 7., 8. un 47. pants — Direktīva 95/46/EK — 25. un 28. pants — Personas datu pārsūtīšana uz trešajām valstīm — Lēmums 2000/520/EK — Personas datu pārsūtīšana uz ASV — Nepienācīgs aizsardzības līmenis — Spēkā esamība — Fiziskas personas sūdzība, kuras dati ir tikuši pārsūtīti no Eiropas Savienības uz ASV — Valsts uzraudzības iestāžu kontroles pilnvaras

Lieta C-362/14

par lūgumu sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *High Court* (Augstā Tiesa, Īrija) iesniedza ar lēmumu, kas pieņemts 2014. gada 17. jūlijā un kas Tiesā reģistrēts 2014. gada 25. jūlijā, tiesvedībā

Maximillian Schrems

pret

Data Protection Commissioner ,

piedaloties

Digital Rights Ireland Ltd .

TIESA (virspalāta)

šādā sastāvā: priekšsēdētājs V. Skouris [*V. Skouris*], priekšsēdētāja vietnieks K. Lēnartss [*K. Lenaerts*], palātu priekšsēdētāji A. Ticano [*A. Tizzano*], R. Silva de Lapuerta [*R. Silva de Lapuerta*], T. fon Danvics [*T. von Danwitz*] (referents), S. Rodins [*S. Rodin*] un K. Jirimēe [*K. Jürimäe*], tiesneši A. Ross [*A. Rosas*], E. Juhāss [*E. Juhász*], E. Borgs Bartets [*A. Borg Barthet*], J. Malenovskis [*J. Malenovský*], D. Švābi [*D. Šváby*], M. Bergere [*M. Berger*], F. Biltšens [*F. Biltgen*] un K. Likurģs [*C. Lycourgos*],

ģenerālvokāts Ī. Bots [*Y. Bot*],

sekretāre L. Hjūleta [*L. Hewlett*], galvenā administratore,

ņemot vērā rakstveida procesu un 2015. gada 24. marta tiesas sēdi,

* Tiesvedības valoda – angļu.

ņemot vērā apsvērumus, ko sniedza:

- *M. Schrems* vārdā – *N. Travers, SC, P. O’Shea, BL*, un *G. Rudden, solicitor*, kā arī *H. Hofmann, Rechtsanwalt*,
- *Data Protection Commissioner* vārdā – *P. McDermott, BL, S. More O’Ferrall* un *D. Young, solicitors*,
- *Digital Rights Ireland Ltd* vārdā – *F. Crehan, BL*, kā arī *S. McGarr* un *E. McGarr, solicitors*,
- Īrijas vārdā – *A. Joyce* un *B. Counihan*, kā arī *E. Creedon*, pārstāvji, kuriem palīdz *D. Fennelly, BL*,
- Beļģijas valdības vārdā – *J.-C. Halleux* un *C. Pochet*, pārstāvji,
- Čehijas valdības vārdā – *M. Smolek* un *J. Vlácil*, pārstāvji,
- Itālijas valdības vārdā – *G. Palmieri*, pārstāve, kurai palīdz *P. Gentili, avvocato dello Stato*,
- Austrijas valdības vārdā – *G. Hesse* un *G. Kunnert*, pārstāvji,
- Polijas valdības vārdā – *M. Kamejsza* un *M. Pawlicka*, kā arī *B. Majczyna*, pārstāvji,
- Slovēnijas valdības vārdā – *A. Grum* un *V. Klemenc*, pārstāves,
- Apvienotās Karalistes valdības vārdā – *L. Christie* un *J. Beeko*, pārstāvji, kuriem palīdz *J. Holmes, barrister*,
- Eiropas Parlamenta vārdā – *D. Moore* un *A. Caiola*, kā arī *M. Pencheva*, pārstāvji,
- Eiropas Komisijas vārdā – *B. Schima, B. Martenczuk* un *B. Smulders*, kā arī *J. Vondung*, pārstāvji,
- Eiropas datu aizsardzības uzraudzītāja (EDAU) vārdā – *C. Docksey, A. Buchta* un *V. Pérez Asinari*, pārstāvji,

noklausījusies ģenerālvokāta secinājumus 2015. gada 23. septembra tiesas sēdē,

pasludina šo spriedumu.

Spriedums

- 1 Lūgums sniegt prejudiciālu nolēmumu ir par to, kā, raugoties Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – “Harta”) 7., 8. un 47. panta gaismā, interpretēt 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 (OV L 281, 31. lpp.), kurā grozījumi izdarīti ar Eiropas Parlamenta un Padomes 2003. gada 29. septembra Regulu (EK) Nr. 1882/2003 (OV L 284, 1. lpp.; turpmāk tekstā – “Direktīva 95/46”), 25. panta 6. punktu un 28. pantu, kā arī būtībā par Komisijas 2000. gada 26. jūlija Lēmuma 2000/520/EK atbilstīgi Direktīvai 95/46 par pienācīgu aizsardzību, kas noteikta ar privātuma “drošības zonas” principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija (OV L 215, 7. lpp.), spēkā esamību.

- 2 Šis lūgums ir iesniegts saistībā ar strīdu starp *M. Schrems* un *Data Protection Commissioner* (datu aizsardzības komisārs, turpmāk tekstā – “komisārs”) saistībā ar pēdējā minētā atteikšanos izskatīt *M. Schrems* iesniegto sūdzību par to, ka *Facebook Ireland Ltd* (turpmāk tekstā – “*Facebook Ireland*”) savu lietotāju personas datus pārsūta uz Amerikas Savienotajām Valstīm un tos saglabā tur esošajos serveros.

Atbilstošās tiesību normas

Direktīva 95/46

- 3 Direktīvas 95/46 preambulas 2., 10., 56., 57., 60., 62. un 63. apsvērums ir formulēti šādi:

“(2) [...] datu apstrādes sistēmas ir paredzētas tam, lai kalpotu cilvēkam; [...] tām neatkarīgi no fizisku personu pilsonības vai pastāvīgas dzīves vietas jārēķina viņu pamattiesības un brīvības, jo īpaši privātās dzīves neaizskaramības tiesības, un jāveicina [...] personu labklājība;

[..]

(10) [...] valstu likumu par personas datu apstrādi mērķis ir aizsargāt pamattiesības un brīvības, īpaši privātās dzīves neaizskaramības tiesības, ko atzīst gan [1950. gada 4. novembrī Romā parakstītās] Eiropas Konvencijas par cilvēka tiesību un pamatbrīvību aizsardzību 8. pants, gan Kopienas tiesību vispārīgie principi; [...] šā iemesla dēļ valstu likumu tuvināšanas rezultāts nedrīkst būt jebkādas to sniegtās aizsardzības samazinājums, bet gan tieši pretēji, tiem jācenšas nodrošināt Kopienā augstu aizsardzības līmeni;

[..]

(56) [...] personas datu pārrobežu plūsmas ir vajadzīgas starptautiskās tirdzniecības paplašināšanai; [...] šīs direktīvas garantētā personu aizsardzība Kopienā netraucē personas datu pārvedumus uz trešajām valstīm, kuras nodrošina pietiekamu aizsardzības līmeni; [...] trešās valsts sniegtā aizsardzības līmeņa pietiekamību jānovērtē, ievērojot visus pārveduma operācijas vai pārveduma operāciju kopuma apstākļus;

(57) [...] no otras puses, personu datu pārvedumu uz trešo valsti, kura nenodrošina pietiekamu aizsardzības līmeni, jāaizliedz;

[..]

(60) [...] jebkurā gadījumā pārvedumus uz trešajām valstīm var realizēt tikai pilnīgā saskaņā ar noteikumiem, ko pieņēmušas dalībvalstis, ievērojot šo direktīvu un jo sevišķi tās 8. pantu;

[..]

(62) [...] uzraudzības iestāžu, kuras pilda savas funkcijas pilnīgi neatkarīgi, izveide dalībvalstīs ir būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi;

(63) [...] šādu iestāžu rīcībā jābūt nepieciešamajiem līdzekļiem savu pienākumu veikšanai, ieskaitot pilnvaras veikt izmeklēšanu un iejaukties, jo sevišķi personu sūdzību gadījumos, un pilnvarām iesaistīties tiesvedībā; [...].”

4 Direktīvas 95/46 1., 2., 25., 26., 28. un 31. pantā ir noteikts:

“1. pants

Direktīvas mērķis

1. Saskaņā ar šo direktīvu dalībvalstis aizsargā fizisku personu pamattiesības un brīvības un jo īpaši viņu tiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi.

[..]

2. pants

Definīcijas

Šajā direktīvā:

- a) “personas dati” ir jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu (“datu subjektu”); identificējama persona ir tā, kuru var identificēt tieši vai netieši, norādot reģistrācijas numuru vai vienu vai vairākus šai personai raksturīgus fiziskās, fizioloģiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktorus;
- b) “personu datu apstrāde” (“apstrāde”) ir jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem – kā vākšana, reģistrēšana, organizēšana, uzglabāšana, piemērošana vai pārveidošana, labošana, konsultēšana, izmantošana, atklāšana, pielietojot pārsūtīšanu, izplatīšanu vai darot tos pieejamus citādā veidā, grupēšana vai savienošana, piekļuves noslēgšana, dzēšana vai iznīcināšana;

[..]

- d) “personas datu apstrādātājs” ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita institūcija, kura viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus; ja apstrādes nolūkus un līdzekļus nosaka valsts vai Kopienas tiesību akti vai noteikumi, personas datu apstrādātāju vai viņa iecelšanas konkrētos kritērijus var noteikt valsts vai Kopienas tiesību akti;

[..]

25. pants

Principi

1. Dalībvalstis paredz to, 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 šīs direktīvas pārējiem noteikumiem, attiecīgā trešā valsts nodrošina pietiekamu aizsardzības līmeni.

2. Trešās valsts sniegtās aizsardzības līmeņa pietiekamība 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.

3. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad tās uzskata, ka trešā valsts nenodrošina pietiekamu aizsardzības līmeni 2. punkta nozīmē.

4. Ja Komisija saskaņā ar 31. panta 2. punktā paredzēto procedūru konstatē, ka trešā valsts nenodrošina pietiekamu aizsardzības līmeni šā panta 2. punkta nozīmē, dalībvalstis veic vajadzīgos pasākumus, lai aizkavētu jebkādu tāda paša tipa datu pārsūtīšanu uz attiecīgo trešo valsti.

5. Atbilstīgā laikā Komisija sāk sarunas ar nolūku labot situāciju, kura izriet no secinājumiem, kas iegūti saskaņā ar 4. punktu.

6. Saskaņā ar 31. panta 2. punktā minēto procedūru Komisija var konstatēt, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni šā panta 2. punkta nozīmē, pamatojoties uz savas valsts tiesībām vai uz starptautiskajām saistībām, kuras tā noslēgusi [tā uzņēmusies], jo īpaši uz 5. punktā minēto sarunu par personu privātās dzīves un pamatbrīvību un tiesību aizsardzību atzinumu.

Dalībvalstis veic nepieciešamos pasākumus, lai izpildītu Komisijas lēmumu.

26. pants

Atkāpes

1. Atkāpjoties no 25. panta un tad, ja vien konkrētus gadījumus reglamentējošās iekšējās tiesības neparedz citādi, dalībvalstis paredz to, ka personas datu pārsūtīšana vai pārsūtījumu kopums uz trešo valsti, kura nenodrošina pietiekamu aizsardzības līmeni 25. panta 2. punkta nozīmē, var notikt ar noteikumu, ka:

- a) datu subjekts viennozīmīgi ir devis savu piekrišanu ierosinātajai datu pārsūtīšanai;
vai
- b) pārsūtīšana vajadzīga, lai izpildītu līgumu starp datu subjektu un personas datu apstrādātāju vai lai īstenotu pēc datu subjekta pieprasījuma veiktos pasākumus, kuriem seko līguma noslēgšana;
vai
- c) datu pārsūtīšana vajadzīga līguma noslēgšanai starp personas datu apstrādātāju un trešajām personām datu subjekta interesēs vai šāda līguma izpildei;
vai
- d) datu pārsūtīšana vajadzīga vai ir likumīgi prasīta, pamatojoties uz svarīgām sabiedrības interesēm, vai juridisku prasību pamatojumam, realizācijai vai aizstāvībai;
vai
- e) datu pārsūtīšana vajadzīga, lai aizsargātu datu subjekta būtiskas intereses;
vai
- f) pārsūtīšanu izdara no reģistra, kurš saskaņā ar likumiem vai regulējumiem ir paredzēts, lai sniegtu informāciju sabiedrībai, un kurš ir pieejams, lai gūtu informāciju, gan plaša[i] sabiedrība[i], gan jebkura[i] persona[i], kura var pierādīt likumīgu ieinteresētību, ciktāl likumā par informācijas pieejamību izvirzītie nosacījumi konkrētajā gadījumā tiek izpildīti.

2. Neierobežojot 1. punktu, dalībvalsts var atļaut personas datu pārsūtīšanu vai pārsūtījumu kopumu uz trešo valsti, kura nenodrošina pietiekamu aizsardzības līmeni 25. panta 2. punkta nozīmē, ja personas datu apstrādātājs sniedz atbilstošas garantijas attiecībā uz personu privātās dzīves un pamattiesību un brīvību aizsardzību un attiecībā uz atbilstošo tiesību izmantošanu; šādas garantijas jo īpaši var izrietēt no attiecīgajiem līguma punktiem.

3. Dalībvalsts informē Komisiju un pārējās dalībvalstis par atļaujām, kuras tā piešķir saskaņā ar 2. punktu.

Ja dalībvalsts vai Komisija pamatoti iebilst saistībā ar personu privātās dzīves neaizskaramības un pamattiesību un brīvību aizsardzību, Komisija veic atbilstošus pasākumus saskaņā ar 31. panta 2. punktā noteikto procedūru.

Dalībvalstis veic nepieciešamos pasākumus, lai izpildītu Komisijas lēmumu.

[..]

28. pants

Uzraudzības iestāde

1. 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.

Šīs iestādes tām uzticēto pienākumu izpildē darbojas pilnīgi neatkarīgi.

2. Katra dalībvalsts paredz to, ka, izstrādājot administratīva rakstura pasākumus vai regulējumus attiecībā uz personas tiesību un brīvību aizsardzību, kas saistīta ar personas datu apstrādi, apspriežas ar uzraudzības iestādēm.

3. Katrai iestādei ir piešķirtas:

- izmeklēšanas pilnvaras, tādas kā datu, kuri veido apstrādes darbību priekšmetu, piekļuves pilnvaras un pilnvaras ievākt tās uzraudzības pienākumu izpildei visu vajadzīgo informāciju,
- efektīvas iejaukšanās pilnvaras, tādas kā, piemēram, saskaņā ar 20. pantu atzinumu sniegšana pirms datu apstrādes darbību veikšanas un pilnvaras nodrošināt šādu atzinumu atbilstīgu nodošanu atklātībai, likt noslēgt piekļuvi, dzēst vai iznīcināt datus, noteikt pagaidu vai galīgu aizliegumu datu apstrādei, brīdināt vai izteikt aizrādījumu personas datu apstrādātājam vai nodot jautājumu izskatīšanai valstu parlamentiem vai citām politiskām institūcijām,
- pilnvaras uzsākt procesuālas darbības, ja pārkāpti saskaņā ar šo direktīvu pieņemtie attiecīgās valsts noteikumi vai darīt zināmus šos pārkāpumus tiesu iestādēm.

Uzraudzības iestādes lēmumus, kuri dod tiesības uz sūdzību procedūru, var pārsūdzēt tiesā.

4. Katra uzraudzības iestāde uzklausa jebkuras personas vai šo personu pārstāvošas apvienības iesniegtu prasību, kas saistīta ar šīs personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi. Ieinteresēt[ā] person[a] jāinformē par prasības rezultātu.

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. Attiecīg[ā] person[a] katrā ziņā jāinformē, ka pārbaude ir notikusi.

[..]

6. Katra uzraudzības iestāde ir kompetenta, lai kādas valsts tiesības tiktu piemērotas konkrētajai datu apstrādei, pati savas dalībvalsts teritorijā realizēt tai saskaņā ar 3. punktu piešķirtās pilnvaras. Katru uzraudzības iestādi var lūgt citas dalībvalsts iestāde realizēt tās pilnvaras.

[..]

31. pants

[..]

2. Ja ir atsauce uz šo pantu, piemēro [Padomes 1999. gada 28. jūnija] Lēmuma 1999/468/EK [ar ko nosaka Komisijai piešķirto ieviešanas pilnvaru īstenošanas kārtību (OV L 184, 23. lpp.)] 4. un 7. pantu, ņemot vērā minētā lēmuma 8. panta noteikumus.

[..]”

Lēmums 2000/520

5 Lēmumu 2000/520 pieņēma Komisija, pamatojoties uz Direktīvas 95/46 25. panta 6. punktu.

6 Šī lēmuma preambulas 2., 5. un 8. apsvērums ir izteikti šādā redakcijā:

“(2) Komisija var atzīt, ka trešā valsts nodrošina atbilstīgu aizsardzības līmeni. Šādā gadījumā personas datus no dalībvalsts drīkst nosūtīt bez papildu garantijām.

[..]

(5) Nosūtot datus no Kopienas uz Amerikas Savienotajām Valstīm, ir jāpanāk pienācīgs datu aizsardzības līmenis, kas atzīts ar šo lēmumu, ja organizācijas ievēro privātuma “drošības zonas” principus to personas datu aizsardzībai, kurus nosūta no kādas dalībvalsts uz Amerikas Savienotajām Valstīm (še turpmāk – “principi”), un ņem vērā visbiežāk uzdotos jautājumus (“frequently asked questions”, še turpmāk – “FAQ”), kas sniedz norādījumus par Amerikas Savienoto Valstu valdības 2000. gada 21. jūlijā izdoto principu īstenošanu. Turklāt organizācijām jāpublisko sava slepenības politika un jāpakļaujas Federālās tirdzniecības komisijas [*Federal Trade Commission (FTC)*] jurisdikcijai saskaņā ar *Federal Trade Commission Act* 5. paragrāfu, kas aizliedz negodīgu vai maldinošu rīcību vai praksi, kuru veic tirdzniecībā vai kura to ietekmē, vai arī citas oficiālas iestādes jurisdikcijai, kas efektīvi nodrošina atbilstību principiem, kuri noteikti saskaņā ar *FAQ*.

[..]

(8) Pārredzamības labad un lai panāktu dalībvalstu 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.”

7 Saskaņā ar Lēmuma 2000/520 1.–4. pantu:

“1. *pants*

1. Direktīvas 95/46/EK 25. pantā attiecībā uz visām darbībām, uz kurām attiecas minētā direktīva, uzskata, ka “privātuma “drošības zonas” principi (še turpmāk – “principi, kas izklāstīti šā lēmuma I pielikumā”), kas [piemēroti] atbilstīgi norādījumiem, kuri sniegti ASV Tirdzniecības ministrijas 2000. gada 21. jūlijā izdotajos visbiežāk uzdotajos jautājumos (še turpmāk – “FAQ”), kas izklāstīti šā lēmuma II pielikumā, nodrošina pienācīgu to personas datu aizsardzības līmeni, ko no Kopienas nosūta Amerikas Savienoto Valstu organizācijām, ņemot vērā šādus ASV Tirdzniecības ministrijas izdotus dokumentus:

- a) III pielikumā izklāstīto pārskatu par “drošības zonas” piemērošanu;
- b) Lēmuma IV pielikumā izklāstīto memorandu par kaitējuma atlīdzināšanu par privātās dzīves aizskārumiem un ASV likumos noteiktām skaidrām atļaujām;
- c) Lēmuma V pielikumā doto vēstuli no *Federal Trade Commission* [Federālās tirdzniecības komisijas];
- d) VI pielikumā doto vēstuli no ASV Transporta ministrijas.

2. Attiecībā uz katru datu nosūtīšanu jābūt izpildītiem šādiem nosacījumiem:

- a) organizācija, kas saņem datus, ir skaidri un publiski darījusi zināmu savu apņemšanos ievērot principus, kas īstenoti atbilstīgi FAQ; un
- b) organizācija pakļaujas Amerikas Savienoto Valstu to valdības iestāžu tiesību aktos noteiktajām pilnvarām, kas uzskaitītas šā lēmuma VII pielikumā un kas ir pilnvarotas izmeklēt sūdzības un saņemt palīdzību negodīgas vai maldinošas rīcības novēršanai, kā arī zaudējumu atlīdzību indivīdiem neatkarīgi no viņu mītnes valsts vai valstiskās piederības, ja nav ievēroti atbilstīgi FAQ īstenotie principi.

3. Uzskata, ka organizācijas, kas pašas apliecina, ka tās stingri ievēro atbilstīgi FAQ īstenotos principus, ir izpildījušas 2. punktā noteiktos nosacījumus no dienas, kad organizācija paziņo ASV Tirdzniecības ministrijai (vai tās pārstāvim) par 2. punkta a) apakšpunktā minēto saistību publiskošanu un norāda 2. punkta b) apakšpunktā minētās valdības iestādes nosaukumu.

2. *pants*

Šis lēmums attiecas tikai uz pienācīgu aizsardzību, ko Amerikas Savienotās Valstis nodrošina saskaņā ar principiem, kas īstenoti atbilstīgi FAQ, lai izpildītu Direktīvas 95/46/EK 25. panta 1. punkta prasības, un tas neietekmē citu minētās direktīvas noteikumu piemērošanu, kuri neļauj personas datus apstrādāt dalībvalstīs, jo īpaši tās 4. pantu.

3. pants

1. Neskarot dalībvalstu kompetento iestāžu pilnvaras rīkoties, lai nodrošinātu to valsts tiesību aktu ievērošanu, kuri ir pieņemti atbilstīgi noteikumiem, izņemot Direktīvas 95/46/EK 25. pantu, tās var īstenot savas pašreizējās pilnvaras, lai aizliegtu vai pārtrauktu datu plūsmu uz organizāciju, kas pati ir apliecinājusi, ka tā stingri ievēro atbilstīgi FAQ īstenotos principus, lai individuus aizsargātu attiecībā uz viņu personas datu apstrādi, ja:

- a) šā lēmuma VII pielikumā minētā Amerikas Savienoto Valstu valdības iestāde vai neatkarīgs tiesību aizsardzības mehānisms šā lēmuma I pielikumā izklāstītā piemērošanas principa a) punkta nozīmē ir noteicis, ka organizācija neievēro atbilstīgi FAQ īstenotos principus; vai
- b) 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.

Pārtraukšanu atceļ, tiklīdz ir nodrošināta atbilstīgi FAQ īstenoto principu ievērošana un attiecīgajām kompetentajām iestādēm Kopienā ir par to paziņots.

2. Ja pieņem pasākumus, pamatojoties uz 1. punktu, tad dalībvalstis par to nekavējoties informē Komisiju.

3. Dalībvalstis un Komisija arī informē viena otru par gadījumiem, kad ar to institūciju darbībām, kas Amerikas Savienotajās Valstīs ir atbildīgas par atbilstīgi FAQ īstenoto principu ievērošanu, šāda ievērošana nav panākta.

4. 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 saskaņā ar Direktīvas 95/46/EK 31. pantā noteikto procedūru nolūkā panākt, lai šo lēmumu atceltu vai apturētu vai lai ierobežotu tā darbības jomu.

4. pants

1. Šo lēmumu 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 jebkurā gadījumā 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/EK 31. pantu, tostarp par pierādījumiem, kuri varētu ietekmēt novērtējumu, ka šā lēmuma 1. pantā paredzētie noteikumi nodrošina pienācīgu aizsardzību Direktīvas 95/46/EK 25. panta nozīmē, un par pierādījumiem, ka šo lēmumu īsteno diskriminējošā veidā.

2. Komisija, vajadzības gadījumā, saskaņā ar Direktīvas 95/46/EK 31. pantā norādīto procedūru iesniedz pasākumu projektu.”

- 8 Lēmuma 2000/520 I pielikums ir formulēts šādi:

“Privātuma “drošības zonas” principi izdevusi ASV Tirdzniecības ministrija 2000. gada 21. jūlijā [...] [...] Tirdzniecības ministrija saskaņā ar likumā noteiktajām pilnvarām izdod šo dokumentu (“principi”) un visbiežāk uzdotos jautājumus (FAQ), lai veicinātu, sekmētu un attīstītu starptautisko tirdzniecību.

Principus izstrādāja, apspriežoties ar nozares uzņēmumiem un plašu sabiedrību, lai veicinātu tirdzniecību starp Amerikas Savienotajām Valstīm un Eiropas Savienību. Ir paredzēts, ka tos izmantos tikai tās ASV organizācijas, kas personas datus saņem no Eiropas Savienības un kuras izpilda “drošības zonas” nosacījumus, un uz kurām tādējādi var attiecināt no tās izrietošo pieņemumu par “atbilstību”. Tā kā principi ir izstrādāti tikai šim īpašajam mērķim, to pieņemšana citiem mērķiem var būt nepiemērota. [...] Organizāciju lēmumi pretendēt uz “drošības zonu” ir pilnībā brīvprātīgi, un organizācijas var to paziņot dažādos veidos. [...] Šo principu ievērošanu var ierobežot: a) ciktāl tas ir vajadzīgs, lai ievērotu valsts drošību, sabiedrības intereses un/vai [ievērotu Amerikas Savienoto Valstu tiesību likumus]; 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; vai c) ja direktīva vai dalībvalsts tiesību akti pieļauj izņēmumus vai atkāpes, ar nosacījumu, ka šādus izņēmumus vai atkāpes piemēro pielīdzināmās situācijās. Saskaņā ar mērķi uzlabot privātās dzīves aizsardzību organizācijām jācenšas šos principus īstenot pilnībā un pārredzamā veidā, tostarp savā slepenības politikā norādot to, vai ar b) punktu atļautos izņēmumus attiecībā uz principiem piemēros regulāri. Tā paša iemesla dēļ organizācijām, ja iespējams, jāizvēlas labāka aizsardzība, ja izvēli atļauj principi un/vai ASV tiesību akti. [...]”

- 9 Lēmuma 2000/520 II pielikums ir izteikts šādā redakcijā:

“Visbiežāk uzdotie jautājumi (FAQ)

[..] FAQ 6 – Pašsertifikācija

Jaut.:

Kā organizācija pati apliecina, ka tā stingri ievēro “drošības zonas” principus?

Atb.:

“Drošības zonas” priekšrocības nodrošina no dienas, kad organizācija pati apliecina Tirdzniecības ministrijai (vai tās pārstāvim), ka tā stingri ievēro principus atbilstīgi turpmāk minētajiem norādījumiem.

Lai organizācija pati apliecinātu “drošības zonu”, tā var Tirdzniecības ministrijai (vai tās pārstāvim) nosūtīt vēstuli, kuru parakstījusi tās amatpersona organizācijas vārdā, kas pievienojas “drošības zonai”, un kurā ir vismaz šāda informācija:

- 1) organizācijas nosaukums, pasta adrese, e-pasta adrese, telefona un faksa numuri;
- 2) organizācijas darbību apraksts attiecībā uz personisko informāciju, kas saņemta no ES; un
- 3) organizācijas slepenības politikas apraksts attiecībā uz šādu personisko informāciju, tostarp norādot: a) vai slepenības politika ir pieejama publiski, b) dienu, kurā ir sākusies tās īstenošana, c) kontaktbiroju, kas izskata sūdzības, piekļuves pieprasījumus un visus citus jautājumus, kuri rodas saistībā ar “drošības zonu”, d) konkrētu oficiālu iestādi, kuras jurisdikcijā ir izskatīt prasības pret organizāciju attiecībā uz negodīgu vai maldinošu rīcību un privātās dzīves aizsardzību reglamentējošu likumu vai noteikumu pārkāpšanu (un kuras ir uzskaitītas principu pielikumā), e) to slepenības programmu nosaukumus, kurās organizācija piedalās, f) pārbaudes metodi (piem., iekšēja, trešās personas) [...] un g) neatkarīgu tiesību aizsardzības mehānismu, kas ir pieejams neatrisināto sūdzību izmeklēšanai.

Ja organizācija vēlas, lai “drošības zonas” priekšrocības attiektos uz informāciju par cilvēkresursiem, kas nosūtīta no ES izmantošanai saistībā ar darba attiecībām, tā var to darīt, ja ir oficiāla iestāde, kuras jurisdikcijā ir izskatīt tās prasības pret organizāciju, kas rodas saistībā ar principu pielikumā uzskaitīto informāciju par cilvēkresursiem.” [..]

Ministrija (vai tās pārstāvis) uzturēs visu to organizāciju sarakstu, kas šādas vēstules ir atsūtījušas, tā nodrošinot “drošības zonas” priekšrocību pieejamību, un šādu sarakstu atjauninās, pamatojoties uz ikgadējām vēstulēm un paziņojumiem, kuri saņemti atbilstīgi FAQ 11. [..]

[..] FAQ 11 – Strīdu izšķiršana un izpilde

Jaut.:

Kā jāīsteno piemērošanas principa strīdu izšķiršanas prasības, un kas notiek, ja organizācija principus pastāvīgi neievēro?

Atb.:

Piemērošanas princips nosaka prasības “drošības zonas” piemērošanai. Tas, kā izpildīt šā principa b) punkta prasības, ir izklāstīts jautājumā par pārbaudi (FAQ 7). Šis FAQ 11 attiecas uz a) un c) punktu, kuros noteikta prasība pēc neatkarīgiem tiesību aizsardzības mehānismiem. Šie mehānismi var būt dažādi, bet tiem jāatbilst piemērošanas principa prasībām. Organizācijas šīs prasības var izpildīt šādi: 1) ievērojot privātajā sektorā izstrādātas slepenības programmas, kuru noteikumos iekļauti “drošības zonas” principi un kas ietver efektīvus tāda veida izpildes mehānismus, kā aprakstīts jautājumā par piemērošanas principu; 2) pakļaujoties juridiskām vai reglamentējošām uzraudzības iestādēm, kas nosaka indivīdu sūdzību izskatīšanu un strīdu izšķiršanu; vai 3) apņemoties sadarboties ar datu aizsardzības iestādēm, kas atrodas Eiropas Savienībā, vai to pilnvarotajiem pārstāvjiem. Šis saraksts ir aptuvenš un nerada ierobežojumus. Privātais sektors var izstrādāt citus mehānismus, lai nodrošinātu piemērošanu, ciktāl tie atbilst piemērošanas principa prasībām un FAQ. Lūdsu ievērojiēt, ka piemērošanas principa prasības papildina prasības, kas noteiktas principu ievada 3. punktā, ka pašregulējums var būt tiesiski apstrīdams saskaņā ar 5. paragrāfu *Federal Trade Commission Act* vai līdzīgiem likumiem.

Tiesību aizsardzības mehānismi

Pirms izmanto neatkarīgus tiesību aizsardzības mehānismus, patērētāji jārosina iesniegt sūdzības, kas viņiem var rasties par attiecīgo organizāciju. [..]

[..]

FTC darbība

FTC ir apņēmusies, pirmkārt, pārskatīt pieprasījumus, kas saņemti no organizācijām, kuras pašas reglamentē privātās dzīves aizsardzību, kā, piemēram, “BBBOnline” un “TRUSTe”, un ES dalībvalstīm, par kurām apgalvo, ka tās neievēro “drošības zonas” principus, lai noteiktu, vai ir pārkāpts *FTC Act* 5. paragrāfs, kurš tirdzniecībā aizliedz negodīgu vai maldinošu rīcību. [..]”

¹⁰ Saskaņā ar Lēmuma 2000/520 IV pielikumu:

“Kaitējuma atlīdzināšana par privātās dzīves aizskārumiem, tiesiskas atļaujas, apvienošanās un pārņemšana ASV tiesību aktos

Šī ir atbilde uz Eiropas Komisijas pieprasījumu izskaidrot ASV tiesību aktus attiecībā uz a) prasībām atlīdzināt zaudējumus par privātās dzīves aizskārumiem, b) ASV tiesību aktos dotām “skaidrām atļaujām” izmantot personisko informāciju tādā veidā, kas ir pretrunā “drošības zonas” principiem, un c) to, kā apvienošanās un pārņemšana ietekmē atbilstīgi “drošības zonai” uzņemtās saistības.

[..]

B. Likumā skaidri noteiktas atļaujas “Drošības zonas” principos ir iekļauts izņēmums, ja likums, noteikumi vai tiesu prakse rada “pretrunīgus pienākumus vai skaidri izteiktas atļaujas, ja, izmantojot šādu atļauju, organizācija var pierādīt, ka principu neievērošana ir ierobežota, ciktāl tas vajadzīgs, lai ievērotu primārās likumīgās intereses, kuras izriet no šādas atļaujas”. Ir skaidrs, ka, ja ASV tiesību akti uzliek pretrunīgas saistības, ASV organizācijām, neatkarīgi no tā, vai tās ir “drošības zona” vai nē, tie ir jāievēro. Lai gan “drošības zonas” principi ir paredzēti, lai pārvarētu ASV un Eiropas sistēmu atšķirības attiecībā uz privātās dzīves aizsardzību, attiecībā uz skaidrām atļaujām mēs pievērsīsimies mūsu ievēlēto likumdevēju likumdošanas prerogatīvām. Ierobežotais izņēmumu skaits, kad var atkāpties no “drošības zonas” principu stingras ievērošanas, ir noteikts, lai ievērotu abu pušu likumīgās intereses. Izņēmums attiecas tikai uz tiem gadījumiem, kad ir skaidra atļauja. Tādēļ neskaidrās situācijās attiecīgajam likumam, noteikumiem vai tiesas lēmumam ir skaidri jāatļauj “drošības zonas” organizācijām konkrēta rīcība. Citiem vārdiem, izņēmumu nepiemēro, ja tas nav noteikts likumā. Turklāt izņēmumu piemēro tikai tad, ja skaidra atļauja ir pretrunā “drošības zonas” principu ievērošan[ai]. Pat tad izņēmums “ir ierobežots, ciktāl tas ir vajadzīgs, lai ievērotu primārās likumīgās intereses, kuras izriet no šādas atļaujas”. Piemēram, ja likums vienkārši atļauj uzņēmumam sniegt personisko informāciju valdības iestādēm, izņēmumu nepiemēro. Turpretim, ja likums īpaši atļauj uzņēmumam sniegt personisko informāciju valdības iestādēm bez indivīda piekrišanas, tā ir “skaidra atļauja” rīkoties tādā veidā, kas ir pretrunā “drošības zonas” principiem. Arī īpaši izņēmumi no prasībām par informēšanu un piekrišanu attiektos uz izņēmumu (jo tas būtu līdzvērtīgs īpaši atļaujai izpaust informāciju bez informēšanas un piekrišanas). Piemēram, saskaņā ar likumu, kas ļauj ārstiem sniegt viņu pacientu medicīnas datus veselības iestāžu ierēdņiem bez pacienta iepriekšējas piekrišanas, var atļaut izņēmumu no informēšanas un izvēles principiem. Šī atļauja neļautu ārstam šos pašus medicīnas datus sniegt veselības aprūpes organizācijām vai komerciālām farmācijas pētījumu laboratorijām, jo tas neatbilstu ar likumu atļautajiem mērķiem un nebūtu izņēmums. Attiecīgais likumīgais pamats var būt vienreizēja atļauja veikt noteiktas darbības ar personisko informāciju, bet, kā rāda turpmākie piemēri, tas drīzāk būs izņēmums no plašāka likuma, kas reglamentē personiskās informācijas vākšanu, izmantošanu vai izpaušanu. [..]”

Paziņojums COM(2013) 846 final

- 11 2013. gada 27. novembrī Komisija pieņēma paziņojumu Eiropas Parlamentam un Padomei ar nosaukumu “Uzticēšanās atjaunošana datu plūsmām starp ES un ASV” [COM(2013) 846 *final*, turpmāk tekstā – “Paziņojums COM(2013) 846 *final*”). Šim paziņojumam bija pievienots ziņojums, arī datēts ar 2013. gada 27. novembri, kurā bija ietverti “ES un ASV Datu aizsardzības jautājumu *ad hoc* darba grupas ES līdzpriekšsēdētāju konstatējumi” (“Report on the Findings by the EU Co-chairs of the *ad hoc* EU-US Working Group on Data Protection”). Kā norādīts šī ziņojuma 1. punktā, tas tika izstrādāts sadarbībā ar Amerikas Savienotajām Valstīm, jo atklājās, ka šajā valstī ir vairākas uzraudzības programmas, ieskaitot liela apmēra personas datu vākšanu un apstrādi. Minētajā ziņojumā tostarp ir ietverta detalizēta Amerikas Savienoto Valstu tiesību sistēmas analīze, it īpaši attiecībā uz tiesisko pamatojumu, kas pieļauj šādu uzraudzības programmu esamību, kā arī Amerikas Savienoto Valstu iestāžu veiktu personas datu vākšanu un apstrādi.
- 12 Paziņojuma COM(2013) 846 *final* 1. punktā Komisija precizē, ka “savstarpējā tirdzniecība ir aplūkota Lēmumā [2000/520], piebilstot, ka “šis lēmums nodrošina juridisko pamatu personas datu pārsūtīšanai no ES uz ASV nodibinātiem uzņēmumiem, kuri ievēro privātuma “drošības zonas” principus”. Turklāt šajā pašā 1. punktā Komisija ir izcēlusi, ka personas datu plūsmas kļūst aizvien nozīmīgākas un tas tostarp ir saistīts ar digitālās ekonomikas attīstību, kura ir veicinājusi to, ka “eksponenciāli pieaug datu apstrādes darbību apjoms, kvalitāte, daudzveidība un veids”.

- 13 Šī paziņojuma 2. punktā Komisija norāda, ka “ir palielinājušās bažas par [Savienības] pilsoņu to personas datu aizsardzību, kuri tiek nosūtīti ASV saskaņā ar “drošības zonas” shēmu” un ka, “ņemot vērā, ka šī shēma ir brīvprātīga un deklaratīva, tiek pievērsta pastiprināta uzmanība tās pārredzamībai un piemērošanas nodrošināšanai”.
- 14 Turklāt Komisija tajā pašā 2. punktā norāda, ka “ASV iestādes var piekļūt [Savienības] pilsoņu personas datiem, kas ir pārsūtīti uz ASV saskaņā ar “drošības zonas” shēmu, un veikt to turpmāku apstrādi tādā veidā, kas nav saderīgs ar pamatojumu, ar kādu tie sākotnēji savākti [Savienībā], un mērķi, kādēļ tie tika nosūtīti uz ASV”, un ka “lielākā daļa ASV interneta uzņēmumu, ko šīs [uzraudzības] programmas, šķiet, ietekmē tiešāk, ir sertificēti atbilstoši “drošības zonas” shēmai”.
- 15 Paziņojuma COM(2013) 846 *final* 3.2. punktā Komisija norāda uz vairākiem trūkumiem saistībā ar Lēmuma 2000/520 īstenošanu. Tā min, pirmkārt, ka ASV sertificētie uzņēmumi neievēro Lēmuma 2000/520 1. panta 1. punktā minētos principus (turpmāk tekstā – ““drošības zonas” principi”) un ka minētajā lēmumā būtu jāveic uzlabojumi saistībā ar “strukturālie[m] trūkumi[em], kas saistīti ar pārredzamību un piemērošanas nodrošināšanu un [..]attiecas uz “drošības zonas” materiāltiesiskajiem principiem un valsts drošības izņēmuma darbību”. Otrkārt, tā norāda, ka ““drošības zona” arī darbojas kā kanāls ES pilsoņu personas datu pārsūtīšanai no Savienības uz ASV, ko veic uzņēmumi, kam ir pienākums sniegt datus ASV izlūkdienestiem saskaņā ar ASV izlūkdatu vākšanas programmām”.
- 16 Šajā 3.2. punktā Komisija secina, ka, lai arī, “ņemot vērā apzinātos trūkumus, “drošības zonas” pašreizējo īstenošanu nevar turpināt, tomēr tās atcelšana nelabvēlīgi ietekmētu shēmā iesaistīto ES un ASV uzņēmumu intereses”. Visbeidzot, minētajā 3.2. punktā Komisija piebilst, ka tā “sadarbosies ar ASV iestādēm, lai apspriestu apzinātos trūkumus”.

Paziņojums COM(2013) 847 final

- 17 Šai pašā datumā – 2013. gada 27. novembrī – Komisija pieņēma paziņojumu Eiropas Parlamentam un Padomei par drošības zonas darbību no ES pilsoņu un uzņēmumu, kas veic uzņēmējdarbību ES, viedokļa (COM(2013) 847 *final*, turpmāk tekstā – “Paziņojums COM(2013) 847 *final*”). Kā izriet no šī paziņojuma 1. punkta, tas ir balstīts uz Eiropas Savienības un ASV *ad-hoc* darba grupas saņemto informāciju un tajā ir ievēroti divi Komisijas novērtējuma ziņojumi, kas sniegti “drošības zonas” shēmas darbības sākumposmā – attiecīgi 2002. un 2004. gadā.
- 18 Šī paziņojuma 1. punktā ir precizēts, ka Lēmuma 2000/520 darbība “paļaujas uz iesaistīto uzņēmumu apņemšanos un pašsertifikāciju”, un piebilsts, ka “pieteikšanās šai shēmai ir brīvprātīga, bet uzņēmumiem, kuri piesakās, noteikumi ir saistoši”.
- 19 Turklāt no Paziņojuma COM(2013) 847 *final* 2.2. punkta izriet, ka 2013. gada 26. septembrī tika sertificēti 3246 uzņēmumi, kas ietilpst vairākās ekonomikas un pakalpojumu nozarēs. Šie uzņēmumi galvenokārt sniedz pakalpojumus Savienības iekšējā tirgū, it īpaši interneta jomā, un daļa no tiem ir Savienības uzņēmumi ar meitasuzņēmumiem Amerikas Savienotajās Valstīs. Daļa no šiem uzņēmumiem apstrādāja savu Eiropā nodarbināto darbinieku datus, kas uz šo valsti tika pārsūtīti cilvēkresursu pārvaldes vajadzībām.
- 20 Tai pašā 2.2. punktā Komisija uzsver, ka “jebkādi ASV puses trūkumi pārredzamības vai piemērošanas nodrošināšanas jomā noved[a] pie tā, ka atbildība tiek novirzīta uz Eiropas datu aizsardzības iestādēm un uzņēmumiem, kas izmanto shēmu”.
- 21 Tostarp no Paziņojuma COM(2013) 847 *final* 3.–5. un 8. punkta izriet, ka praksē liels skaits sertificēto uzņēmumu neievēroja vai daļēji neievēroja drošības zonas principus.

- 22 Turklāt šī paziņojuma 7. punktā Komisija min, ka “visi uzņēmumi, kas iesaistīti *PRISM* programmā (plaša mēroga izlūkdatu vākšanas programma), kas piešķir ASV iestādēm piekļuvi ASV uzglabātiem un apstrādātiem datiem, ir sertificēti “drošības zonas” dalībnieki” un ka tādējādi ““drošības zonas” shēma ir kļuvusi par vienu no kanāliem, pa kuriem ASV izlūkdienesti iegūst piekļuvi to personas datu vākšanai, kas sākotnēji ir apstrādāti [Savienībā]”. Šai sakarā Komisija minētā paziņojuma 7.1. punktā ir konstatējusi, ka “ASV tiesību akti rada vairākus juridiskos pamatus, ļaujot veikt tādu personas datu plaša mēroga vākšanu un apstrādi, kurus uzglabā vai citādi apstrādā uzņēmumi, kas atrodas ASV” un ka “šo programmu plašais mērogs var radīt situāciju, ka saskaņā ar “drošības zonu” pārsūtītiem datiem piekļūst un to turpmāku apstrādi veic ASV iestādes, pārsniedzot to, kas ir samērīgs un nepieciešams tikai valsts drošības aizsardzībai, kā to paredz Lēmumā 2000/520 noteiktais izņēmums”.
- 23 Paziņojuma COM(2013) 847 *final* 7.2. punktā ar nosaukumu “Ierobežojumi un tiesiskās aizsardzības iespējas” Komisija uzsver, ka “aizsardzības pasākumi, kas noteikti ASV tiesību aktos, ir pieejami pārsvarā ASV pilsoņiem vai personām, kuras likumīgi uzturas valstī” un ka “turklāt ne ES, ne ASV datu subjektiem nav iespēju 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, kas notiek saskaņā ar ASV novērošanas programmām”.
- 24 Atbilstoši Paziņojuma COM(2013) 847 *final* 8. punktam sertificēto uzņēmumu vidū ir “tīmekļa uzņēmumi *Google, Facebook, Microsoft, Apple* [un] *Yahoo*”, kuriem ir “simtiem miljonu klientu Eiropā” un tie pārsūta uz ASV personas datus apstrādei.
- 25 Komisija šai pašā 8. punktā ir secinājusi, ka “izlūkdienestu plaša mēroga piekļuve datiem, ko sertificēti “drošības zonas” uzņēmumi pārsūta uz ASV, liek uzdot nopietnus papildu jautājumus par eiropiešu datu aizsardzības tiesību nepārtrauktību, kad viņu dati tiek pārsūtīti uz ASV”.

Pamatlieta un prejudiciālie jautājumi

- 26 *M. Schrems*, Austrijā dzīvojošais tās pašas valsts pilsonis, ir sociālā tīkla *Facebook* (turpmāk tekstā – “*Facebook*”) lietotājs kopš 2008. gada.
- 27 Visiem *Facebook* lietotājiem, kas dzīvo Savienības teritorijā, reģistrējoties tiek lūgts parakstīt līgumu ar *Facebook Ireland* – mātesuzņēmuma *Facebook Inc.*, kura mītne ir Amerikas Savienotajās Valstīs, meitasuzņēmumu. Visi *Facebook* lietotāju, kas dzīvo Savienības teritorijā, dati vai daļa no tiem tiek pārsūtīti uz *Facebook Inc.* serveriem, kas atrodas Amerikas Savienoto Valstu teritorijā, kur tie tiek apstrādāti.
- 28 2013. gada 25. jūnijā *M. Schrems* iesniedza sūdzību komisāram, būtībā viņam prasot īstenot savas likumiskās pilnvaras un aizliegt *Facebook Ireland* pārsūtīt šos personas datus uz ASV. Sūdzībā viņš norādīja, ka šajā valstī spēkā esošās tiesības un prakse nenodrošina pietiekamu Amerikas Savienoto Valstu teritorijā uzglabāto personas datu aizsardzību pret valsts iestāžu īstenoto uzraudzību. Šai sakarā *M. Schrems* atsaucās uz *Edward Snowden* atklāto informāciju par Amerikas Savienoto Valstu izlūkdienestu, it īpaši *National Security Agency* (turpmāk tekstā – “*NSA*”) darbību.
- 29 Komisārs, uzskatīdams, ka viņam par *M. Schrems* sūdzībā minētajiem faktiem izmeklēšana nav jāveic, to noraidīja kā nepamatotu. Viņš faktiski uzskatīja, ka nav pierādījumu tam, ka *NSA* būtu bijusi piekļuve ieinteresētās personas datiem. Komisārs piebilda, ka *M. Schrems* sūdzībā izvirzītajiem iebildumiem nevar piekrist, jo ikviens ar personas datu pienācīgu aizsardzības līmeni ASV saistīts jautājums esot jāizskata saskaņā ar Lēmumu 2000/520 un ka šajā lēmumā Komisija esot konstatējusi, ka Amerikas Savienotās Valstis nodrošinot pienācīgu aizsardzības līmeni.

- 30 *M. Schrems* par pamatlietā minēto lēmumu cēla prasību *High Court* (Augstajā Tiesā). Izskatot pamatlīetas pušu iesniegtos pierādījumus, šī tiesa konstatēja, ka no Savienības uz ASV pārsūtīto personas datu elektroniskā pārraudzība un pārtveršana atbilst nepieciešamajiem un neaizstājamajiem mērķiem sabiedrības labā. Tomēr minētā tiesa piebilda, ka *E. Snowden* atklātā informācija pierādot, ka NSA un citi federālie dienesti esot “ievērojami pārsnieguši” savas tiesības.
- 31 Tās pašas tiesas skatījumā Savienības pilsoņiem neesot faktisku tiesību tikt uzklausi. Izlūkdienestu darbību uzraudzība notiekot saskaņā ar slepenu procedūru, nevis balstoties uz sacīkstes principu. Tiklīdz personas dati tiek pārsūtīti uz ASV, NSA un citi federālie dienesti – tādi kā *Federal Bureau of Investigation (FBI)*, šiem datiem var piekļūt, veicot nediferencētu datu uzraudzību un pārtveršanu, ko tie plaši praktizē.
- 32 *High Court* (Augstā Tiesa) konstatēja, ka Īrijas tiesībās ir aizliegta personas datu nosūtīšana ārpus valsts teritorijas, izņemot gadījumu, kad attiecīgā trešā valsts nodrošina pienācīgu privātās dzīves, kā arī pamattiesību un pamatbrīvību aizsardzības līmeni. Tiesību uz privātās dzīves un mājokļa neaizskaramību, kas garantētas Īrijas konstitūcijā, nozīmīguma pamatā esot prasība, lai iejaukšanās šajās tiesībās būtu samērīga un saderīga ar likumā paredzētajām prasībām.
- 33 Liela apmēra un nediferencēta piekļuve personas datiem acīmredzami būtu pretrunā samērīguma principam un pamatvērtībām, kas aizsargātas Īrijas konstitūcijā. Lai elektroniskās saziņas pārtveršana varētu tikt uzskatīta par atbilstošu šai konstitūcijai, esot jāpierāda, ka šī pārtveršana ir mērķtiecīga, ka konkrētu personu vai konkrētu personu grupu komunikāciju pārtveršana un uzraudzība ir objektīvi pamatota ar valsts drošības interesēm vai noziedzības apkarošanu un ka tam ir pienācīgas un pārbaudāmas garantijas. Tā *High Court* (Augstās Tiesas) skatījumā, ja pamatlieta būtu jāizskata, pamatojoties tikai uz Īrijas tiesībām, būtu jākonstatē, ka, ņemot vērā pastāvošas nopietnas šaubas, vai Amerikas Savienotās Valstis nodrošina pienācīgu personas datu aizsardzības līmeni, komisāram būtu bijis pienākums veikt izmeklēšanu par *M. Schrems* sūdzībā minētajiem faktiem un viņš šo sūdzību ir kļūdaini noraidījis.
- 34 Tomēr *High Court* (Augstā Tiesa) uzskata, ka šī lieta attiecas uz Savienības tiesību īstenošanu Hartas 51. panta izpratnē, tādējādi pamatlietā aplūkoto lēmuma tiesiskums esot jāizvērtē saskaņā ar Savienības tiesībām. Šīs tiesas skatījumā Lēmums 2000/520 neatbilst ne no Hartas 7. un 8. panta izrietošajām prasībām, ne arī principiem, ko Tiesa minējusi spriedumā *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238). 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, kuri savukārt it īpaši ir saistīti ar attiecīgajiem indivīdiem, un nesniegt nekādas pienācīgas vai pārbaudāmas garantijas šādām darbībām, tiktu apdraudētas Hartas 7. pantā garantētās tiesības uz privātās dzīves neaizskaramību un dalībvalstu tradīcijām būtiskās kopējās vērtības.
- 35 *High Court* (Augstā Tiesa) turklāt norāda, ka *M. Schrems* savā prasībā faktiski apstrīd tā “drošības zonas” režīma tiesiskumu, kas ieviests ar Lēmumu 2000/520 un tiek turpināts saskaņā ar pamatlietā aplūkoto lēmumu. Tāpat, lai arī *M. Schrems* formāli nav apstrīdējis nedz Direktīvu 95/46, nedz Lēmumu 2000/520, iesniedzējtiesas skatījumā rodas jautājums, vai, ņemot vērā šīs direktīvas 25. panta 6. punktu, komisāram bija saistošs šajā Komisijas lēmumā izdarītais konstatējums, saskaņā ar kuru Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni, vai arī ar Hartas 8. pantu komisāram vajadzības gadījumā tiek ļauts no šāda secinājuma izvairīties.
- 36 Šādos apstākļos *High Court* (Augstā Tiesa) nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:
- 1) Vai, izskatot sūdzību, kas ir iesniegta neatkarīgam komisāram, kura pienākumos ietilpst datu aizsardzības tiesiskā regulējuma piemērošana, par to, ka personas dati tiek nosūtīti uz trešo valsti (šajā gadījumā – uz Amerikas Savienotajām Valstīm), kuras tiesību akti un prakse, kā apgalvo

pieteicējs, nenodrošina pienācīgu attiecīgās personas aizsardzību, šai amatpersonai tomēr ir pilnībā saistošs Savienības 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?

- 2) Vai pretējā gadījumā tam ir pienākums vai tiesības pašam veikt izmeklēšanu par šo jautājumu, ņemot vērā faktu attīstību kopš Komisijas lēmuma pirmās publicēšanas?”

Par prejudiciālajiem jautājumiem

- 37 Uzdodama prejudiciālos jautājumus, kas ir jāizskata kopā, iesniedzējtiesa būtībā jautā, vai un cik lielā mērā Direktīvas 95/46 25. panta 6. punkts, to lasot kopā ar Hartas 7., 8. un 47. pantu, ir jāinterpretē tādējādi, ka saskaņā ar šo tiesību normu pieņemts lēmums – kā Lēmums 2000/520 –, kurā Komisija konstatē, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, rada šķēršļus tam, lai dalībvalsts uzraudzības iestāde šīs direktīvas 28. panta izpratnē varētu izskatīt personas iesniegumu par šīs personas tiesību un brīvību aizsardzību to personas datu apstrādes jomā, kas tikuši pārsūtīti no dalībvalsts uz šo trešo valsti, ja šī persona norāda, ka tās spēkā esošās tiesības un prakse nenodrošina pienācīgu aizsardzības līmeni.

Par valsts uzraudzības iestāžu kontroles pilnvarām Direktīvas 95/46 28. panta izpratnē, esot Komisijas lēmumam, kas pieņemts saskaņā ar šīs direktīvas 25. panta 6. punktu

- 38 Vispirms ir jāatgādina, ka Direktīvas 95/46 normas attiecībā uz personas datu apstrādi, kas var skart pamattiesības un, it īpaši, tiesības uz privātās dzīves neaizskaramību, ir jāinterpretē, ievērojot pamattiesības, kas ir ierakstītas Hartā (skat. spriedumus *Österreichischer Rundfunk* u.c., C-465/00, C-138/01 un C-139/01, EU:C:2003:294, 68. punkts; *Google Spain* un *Google*, C-131/12, EU:C:2014:317, 68. punkts, kā arī *Ryneš*, C-212/13, EU:C:2014:2428, 29. punkts).
- 39 No Direktīvas 95/46 1. panta, kā arī no tās preambulas 2. un 10. apsvēruma izriet, ka tās mērķis ir ne tikai nodrošināt efektīvu un pilnīgu fizisko personu pamattiesību un brīvību, it īpaši viņu tiesību uz privātās dzīves neaizskaramību saistībā ar personas datu apstrādi, aizsardzību, bet arī augstu šo pamattiesību un brīvību aizsardzības līmeni. Gan pamattiesību uz privātās dzīves neaizskaramību, kas garantētas Hartas 7. pantā, gan arī pamattiesību uz personas datu aizsardzību, kas garantētas tās 8. pantā, nozīme ir uzsvērtā arī Tiesas judikatūrā (skat. spriedumus *Rijkeboer*, C-553/07, EU:C:2009:293, 47. punkts; *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 53. punkts, un *Google Spain* un *Google*, C-131/12, EU:C:2014:317, 53., 66. un 74. punkts un tajos minētā judikatūra).
- 40 Attiecībā uz pilnvarām, ar kurām valsts uzraudzības iestādes ir apveltītas saistībā ar personas datu pārsūtīšanu uz trešām valstīm, ir jānorāda, ka Direktīvas 95/46 28. panta 1. punktā dalībvalstīm ir noteikts pienākums noteikt vienu vai vairākas valsts iestādes, kuru atbildībā ir pilnīgi neatkarīgi kontrolēt Savienības tiesību normu par fizisko personu aizsardzību saistībā ar šādu datu apstrādi ievērošanu. Šāda prasība izriet arī no Savienības primārajām tiesībām, proti, Hartas 8. panta 3. punkta un LESD 16. panta 2. punkta (šajā ziņā 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).
- 41 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, un tā ir jāinterpretē šī mērķa kontekstā. Tā ir tikusi ieviesta, lai pastiprinātu to personu un organizāciju aizsardzību, uz kurām šo iestāžu lēmumi attiecas. Neatkarīgas uzraudzības iestādes izveide dalībvalstīs – kā tas norādīts Direktīvas 95/46 preambulas 62. apsvērumā, tādējādi ir būtisks apstāklis

personu aizsardzības nodrošināšanā attiecībā uz personas datu apstrādi (skat. spriedumus Komisija/Vācija, C-518/07, EU:C:2010:125, 25. punkts, kā arī Komisija/Ungārija, C-288/12, EU:C:2014:237, 48. punkts un tajā minētā judikatūra).

- 42 Lai garantētu šo aizsardzību, valsts uzraudzības iestādēm ir īpaši jānodrošina taisnīgs līdzsvars starp pamattiesību uz privātās dzīves neaizskaramību ievērošanu, no vienas puses, un interesēm, kas prasa personas datu brīvu apriti, no otras puses (šajā ziņā skat. spriedumus Komisija/Vācija, C-518/07, EU:C:2010:125, 24. punkts, un Komisija/Ungārija, C-288/12, EU:C:2014:237, 51. punkts).
- 43 Šim nolūkam šīs iestādes ir apveltītas ar virkni pilnvaru, un tām, esot uzskaitītām Direktīvas 95/46 28. panta 3. punktā esošajā sarakstā, kas nav uzskatāms par galīgu, – kā uzsvērts šīs direktīvas preambulas 63. apsvērumā – ir vajadzīgi līdzekļi to uzdevumu izpildē. Tādējādi minētajām iestādēm ir tostarp izmeklēšanas pilnvaras, piemēram, pilnvaras ievākt visu tās uzraudzības pienākumu izpildei vajadzīgo informāciju, efektīvas iejaukšanās pilnvaras, piemēram, noteikt pagaidu vai galīgu aizliegumu datu apstrādei, vai arī pilnvaras iesaistīties tiesvedībā.
- 44 Protams, no Direktīvas 95/46 28. panta 1. un 6. punkta izriet, ka valsts uzraudzības iestāžu pilnvaras attiecas uz personas datu apstrādi dalībvalsts teritorijā, kurā šīs iestādes atrodas, un, pamatojoties uz šo 28. pantu, to pilnvaras nesniedz līdz šādu datu apstrādei, kas veikta trešās valsts teritorijā.
- 45 Tomēr darbība, kurā ietilpst personas datu pārsūtīšana no dalībvalsts uz trešo valsti, kā tāda ir personas datu apstrāde Direktīvas 95/46 2. panta b) punkta izpratnē (šajā ziņā skat. spriedumu Parlaments/Padome un Komisija, C-317/04 un C-318/04, EU:C:2006:346, 56. punkts), kas veikta dalībvalsts teritorijā. Šajā tiesību normā “personu datu apstrāde” ir “jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem”, kā piemēru minot – “atklāšan[u], pielietojot pārsūtīšanu, izplatīšanu vai darot tos pieejamus citādā veidā”.
- 46 Direktīvas 95/46 preambulas 60. apsvērumā ir precizēts, ka personas datu pārsūtīšana uz trešajām valstīm var tikt realizēta tikai pilnīgā saskaņā ar noteikumiem, ko pieņēmušas dalībvalstis, piemērojot šo direktīvu. Šim nolūkam minētās direktīvas IV nodaļā, kurā ir 25. un 26. pants, ir izveidota sistēma, kuras mērķis ir nodrošināt dalībvalstu kontroli pār personas datu pārsūtīšanu uz trešajām valstīm. Ar šo sistēmu tiek papildināta vispārējā sistēma, kura ir ieviesta ar šīs pašas direktīvas II nodaļu, kurā ir paredzēti personas datu apstrādes likumības vispārīgie nosacījumi (šajā ziņā skat. spriedumu *Lindqvist*, C-101/01, EU:C:2003:596, 63. punkts).
- 47 Tā kā valsts uzraudzības iestāžu ziņā saskaņā ar Hartas 8. panta 3. punktu un Direktīvas 95/46 28. pantu ir kontrolēt, vai tiek ievērotas Savienības tiesību normas par fizisku personu aizsardzību saistībā ar personas datu apstrādi, ikviena no tām tātad ir apveltīta ar pilnvarām pārbaudīt, vai personas datu pārsūtīšanā no dalībvalsts, kurā tā darbojas, uz trešo valsti ir ievērotas ar Direktīvu 95/46 izvirzītās prasības.
- 48 Visādā ziņā Direktīvas 95/46 preambulas 56. apsvērumā atzīstot, ka personas datu pārsūtīšana no dalībvalstīm uz trešajām valstīm ir vajadzīga starptautiskās tirdzniecības attīstībai, šīs direktīvas 25. panta 1. punktā kā princips ir izvirzīts fakts, ka šāda pārsūtīšana var notikt tikai tad, ja tiek nodrošināts pienācīgs aizsardzības līmenis.
- 49 Turklāt minētās direktīvas preambulas 57. apsvērumā ir precizēts, ka personas datu pārsūtīšana uz trešajām valstīm, kuras nenodrošina pienācīgu aizsardzības līmeni, ir aizliegta.
- 50 Lai kontrolētu personas datu pārsūtīšanu uz trešajām valstīm atkarībā no katrā no šīm valstīm noteiktā aizsardzības līmeņa, Direktīvas 95/46 25. pantā ir noteikta virkne pienākumu dalībvalstīm un Komisijai. No šī panta tostarp izriet, ka konstatēt, vai trešā valsts nodrošina vai nenodrošina pienācīgu aizsardzības līmeni, – kā to savu secinājumu 86. punktā ir minējis ģenerāladvokāts, – var vai nu dalībvalstis, vai Komisija.

- 51 Komisija uz Direktīvas 95/46 25. panta 6. punkta pamata var pieņemt lēmumu par to, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni. Šāda lēmuma adresātes saskaņā ar šīs tiesību normas otro daļu ir dalībvalstis, kurām ir jāveic vajadzīgie pasākumi, lai atbilstu šī lēmuma prasībām. Saskaņā ar LESD 288. panta ceturto daļu tas ir saistošs visām dalībvalstīm adresātēm, kā arī visām to organizācijām (šajā ziņā skat. spriedumus *Albako Margarinefabrik*, 249/85, EU:C:1987:245, 17. punkts, un *Mediaset*, C-69/13, EU:C:2014:71, 23. punkts), jo tā rezultātā tiek atļauta personas datu pārsūtīšana no dalībvalstīm uz šajā pašā lēmumā minētajām trešajām valstīm.
- 52 Tādējādi tikmēr, kamēr Komisijas lēmumu Tiesa nav atzinusi par spēkā neesošu, dalībvalstis un to organizācijas, pie kurām ir pieskaitāmas neatkarīgas to uzraudzības iestādes, protams, nedrīkst veikt ar šādu lēmumu nesaderīgus pasākumus – piemēram, pieņemt tiesību aktus, kuros ar saistošām sekām būtu noteikts, ka minētajā lēmumā norādītajās trešajās valstīs netiek nodrošināts pienācīgs aizsardzības līmenis. Savienības iestāžu aktiem principā ir likumības prezumpcija, un tie tādējādi rada tiesiskas sekas tik ilgi, kamēr tie nav atsaukti, atcelti prasības atcelt tiesību aktu ietvaros vai pasludināti par spēkā neesošiem pēc prejudiciāla nolēmuma pieņemšanas vai iebildes par prettiesiskumu apmierināšanas (spriedums Komisija/Grieķija, C-475/01, EU:C:2004:585, 18. punkts un tajā minētā judikatūra).
- 53 Tomēr saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemts Komisijas lēmums – kā Lēmums 2000/520 – nevar liegt personām, kuru personas dati ir tikuši vai var tikt pārsūtīti uz trešajām valstīm, vērsties valsts uzraudzības iestādēs šīs direktīvas 28. panta 4. punkta izpratnē ar prasību par viņu tiesību un brīvību aizsardzību saistībā ar šo datu apstrādi. Tāpat šāda veida lēmums – kā to it īpaši savu secinājumu 61., 93. un 116. punktā norāda ģenerāladvokāts – nevar nedz noliegt, nedz arī mazināt valsts uzraudzības iestāžu pilnvaras, kas tām ir skaidri piešķirtas ar Hartas 8. panta 3. punktu un minētās direktīvas 28. pantu.
- 54 Nedz Hartas 8. panta 3. punktā, nedz Direktīvas 95/46 28. pantā no valsts uzraudzības iestāžu kontroles jomas nav izslēgta personas datu pārsūtīšanas uz trešajām valstīm kontrole, kas ir bijusi atbilstoši šīs direktīvas 25. panta 6. punktam pieņemta Komisijas lēmuma priekšmets.
- 55 It īpaši Direktīvas 95/46 28. panta 4. punkta pirmajā daļā, kurā ir paredzēts, ka valsts uzraudzības iestādes uzklaua “jebkuras personas vai šo personu pārstāvošas apvienības iesniegtu prasību, kas saistīta ar šīs personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi”, šai sakarā nav paredzēts nekāds izņēmums gadījumā, ja Komisija saskaņā ar šīs direktīvas 25. panta 6. punktu būtu pieņēmusi lēmumu.
- 56 Turklāt ar sistēmu, kas ieviesta ar Direktīvu 95/46, un tās 25. un 28. panta mērķiem nebūtu saderīgi tas, ka saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemta Komisijas lēmuma rezultātā valsts uzraudzības iestādei būtu liegts izskatīt personas pieteikumu par tās tiesību un brīvību aizsardzību saistībā ar šo personas datu apstrādi, kuri ir tikuši vai var tikt pārsūtīti no dalībvalsts uz šādā lēmumā minēto trešo valsti.
- 57 Tieši otrādi – Direktīvas 95/46 28. pants pēc tā būtības ir piemērojams visa veida personas datu apstrādei. Tādējādi, lai arī Komisija ir pieņēmusi lēmumu saskaņā ar šīs direktīvas 25. panta 6. punktu, valsts uzraudzības iestādēm, kurās persona ir vērsusies ar prasību par tās tiesību un brīvību aizsardzību saistībā ar personas datu apstrādi, kas attiecas uz šo personu, ir jāvar pilnīgi neatkarīgi izvērtēt, vai šo datu pārsūtīšana atbilst šajā direktīvā izvirzītajām prasībām.
- 58 Pretējā gadījumā personām, kuru personas dati ir tikuši vai varētu tikt pārsūtīti uz attiecīgo trešo valsti, tiktu liegtas Hartas 8. panta 1. un 3. punktā garantētās tiesības vērsties valsts uzraudzības iestādēs ar prasību aizsargāt viņu pamattiesības (skat. pēc analogijas spriedumu *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 68. punkts).

- 59 Prasība Direktīvas 95/46 28. panta 4. punkta izpratnē, kurā persona, kuras personas dati ir tikuši vai var tikt pārsūtīti uz trešo valsti – kā pamatlietā –, norāda, ka šīs trešās valsts tiesības un prakse, neraugoties uz to, ko Komisija ir konstatējusi šīs direktīvas 25. panta 6. punktā, nenodrošina pienācīgu aizsardzības līmeni, ir jāsaprot kā tāda, kas būtībā attiecas uz šī lēmuma saderīgumu ar personu privātās dzīves neaizskaramību un pamattiesību un pamatbrīvību aizsardzību.
- 60 Šai sakarā ir jāatgādina Tiesas pastāvīgā judikatūra, saskaņā ar kuru Savienība ir tiesiska Savienība, kurā tiek pārbaudīta tās iestāžu aktu atbilstība, tostarp Līgumiem, vispārējiem tiesību principiem, kā arī pamattiesībām (šajā ziņā skat. spriedumus Komisija u.c./*Kadi*, C-584/10^P, C-593/10^P un C-595/10^P, EU:C:2013:518, 66. punkts; *Inuit Tapiriit Kanatami* u.c./Parlaments un Padome, C-583/11 P, EU:C:2013:625, 91. punkts, kā arī *Telefónica*/Komisija (C-274/12 P, EU:C:2013:852, 56. punkts). Saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemtie Komisijas lēmumi tādēļ nebūtu atstājami ārpus šādas kontroles.
- 61 Tādēļ tikai Tiesas kompetencē ir konstatēt Savienības tiesību akta, kāds ir saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemtais Komisijas lēmums, spēkā neesamību – šīs kompetences ekskluzīvais mērķis ir garantēt tiesisko noteiktību, nodrošinot Savienības tiesību vienveidīgu piemērošanu (skat. spriedumus *Melki* un *Abdeli*, C-188/10 un C-189/10, EU:C:2010:363, 54. punkts, kā arī *CIVAD*, C-533/10, EU:C:2012:347, 40. punkts).
- 62 Lai arī valsts tiesām, protams, ir likumīgas tiesības pārbaudīt Savienības tiesību aktu, kāds ir saskaņā ar Direktīvas 95/46 25. panta 6. punktu pieņemtais Komisijas lēmums, spēkā esamību, tās tomēr nav apveltītas ar pilnvarām, saskaņā ar kurām tās pašas konstatē šāda tiesību akta spēkā neesamību (skat. šajā ziņā spriedumus *Foto-Frost*, 314/85, EU:C:1987:452, 15.–20. punkts, kā arī *IATA* un *ELFAA*, C-344/04, EU:C:2006:10, 27. punkts). Izskatot *a fortiori* prasību šīs direktīvas 28. panta 4. punkta izpratnē par Komisijas lēmuma, kas pieņemts atbilstoši šīs direktīvas 25. panta 6. punktam, saderīgumu ar personu privātās dzīves neaizskaramības un pamatbrīvību un pamattiesību aizsardzību, valsts uzraudzības iestādes pašas nav tiesīgas konstatēt šāda lēmuma spēkā neesamību.
- 63 Ņemot vērā šos apsvērumus, ja persona, kuras personas dati ir tikuši vai var tikt pārsūtīti uz trešo valsti, par kuru Komisija saskaņā ar Direktīvas 95/46 25. panta 6. punktu ir pieņēmusi lēmumu, vēršas valsts uzraudzības iestādē ar prasību par tās tiesību un brīvību aizsardzību saistībā ar šo datu apstrādi un šīs prasības ietvaros, kā tas ir pamatlietā, apstrīd šī lēmuma saderīgumu ar personu privātās dzīves neaizskaramības un pamatbrīvību un pamattiesību aizsardzību, šai iestādei minētā prasība ir jāizskata ar vislielāko rūpību.
- 64 Pieņemot, ka minētā iestāde nonāk pie secinājuma, ka minētais šādas prasības atbalstam nav pamatots, un šī iemesla dēļ prasību noraida, personai, kas iesniegusi minēto prasību, – kā tas izriet no Direktīvas 95/46 28. panta 3. punkta otrās daļas, to lasot kopā ar Hartas 47. pantu, – būtu jāvar piekļūt tiesību aizsardzības līdzekļiem tiesā, radot iespēju šo viņai nelabvēlīgo lēmumu apstrīdēt valstu tiesās. Ņemot vērā šī sprieduma 61. un 62. punktā minēto judikatūru, ja valsts tiesas uzskata, ka viens vai vairāki lietas dalībnieku norādītie Savienības tiesību akta spēkā neesamības pamati vai, ja tāds būtu gadījums, pamati, kas konstatēti pēc tiesas ierosmes, ir pamatoti, tām ir pienākums apturēt tiesvedību un vērsties Tiesā ar lūgumu sniegt prejudiciālu nolēmumu akta spēkā esamības izvērtēšanai (šajā ziņā skat. spriedumu *T & L Sugars* un *Sidul Açúcares*/Komisija, C-456/13 P, EU:C:2015:284, 48. punkts un tajā minētā judikatūra).
- 65 Pretējā gadījumā, ja minētā iestāde par pamatotām atzīst iebildes, ko izvirzījusi persona, kas iesniegusi prasību par tās tiesību un brīvību aizsardzību saistībā ar šo personas datu apstrādi, šai pašai iestādei atbilstoši Direktīvas 95/46 28. panta 3. punkta pirmās daļas trešajam ievilkumam, to lasot kopā ar Hartas 8. panta 3. punktu, ir jāvar iesaistīties tiesvedībā. Šajā ziņā valsts likumdevēja ziņā ir paredzēt tiesiskās aizsardzības līdzekļus, kas valsts uzraudzības iestādei ļauj valstu tiesās izvirzīt iebildes, ko tā

uzskata par pamatotām, lai šīs tiesas – ja arī tās piekrīt šīs iestādes šaubām par Komisijas lēmuma spēkā esamību – iesniegtu lūgumu sniegt prejudiciālu nolēmumu šī lēmuma spēkā esamības izvērtēšanas nolūkos.

- 66 Nemot vērā visus iepriekš minētos apsvērumus, uz uzdotajiem jautājumiem ir jāatbild, ka Direktīvas 95/46 25. panta 6. punkts, to lasot kopā ar Hartas 7., 8. un 47. pantu, ir jāinterpretē tādējādi, ka saskaņā ar šo tiesību normu pieņemts lēmums – kā Lēmums 2000/520 –, kurā Komisija konstatē, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, nerada šķēršļus tam, lai dalībvalsts uzraudzības iestāde šīs direktīvas 28. panta izpratnē izskatītu personas prasību par tās tiesību un brīvību aizsardzību saistībā ar to personas datu apstrādi, kas attiecas uz šo personu un kuri ir tikuši vai var tikt pārsūtīti no dalībvalsts uz šo trešo valsti, ja šī persona norāda, ka tajā spēkā esošās tiesības un prakse nenodrošina pienācīgu aizsardzības līmeni.

Par Lēmuma 2000/520 spēkā esamību

- 67 No iesniedzējtiesas paskaidrojumiem saistībā ar uzdotajiem jautājumiem izriet, kā *M. Schrems* pamattiesvedībā norāda, ka ASV tiesības un prakse nenodrošina pienācīgu aizsardzības līmeni Direktīvas 95/46 25. panta izpratnē. Kā to savu secinājumu 123. un 124. punktā norāda ģenerālvokāts, *M. Schrems* pauž šaubas, kuras, šķiet, būtībā ir arī šai tiesai, par Lēmuma 2000/520 spēkā esamību. Šajos apstākļos, ņemot vērā šī sprieduma 60.–63. punktā konstatēto un lai sniegtu pilnīgu atbildi minētajai tiesai, ir jāizvērtē, vai šis lēmums ir saderīgs ar prasībām, kas izriet no šīs direktīvas, to lasot Hartas gaismā.

Par prasībām, kas izriet no Direktīvas 95/46 25. panta 6. punkta

- 68 Kā jau tas norādīts šī sprieduma 48. un 49. punktā, Direktīvas 95/46 25. panta 1. punktā ir noteikts aizliegums pārsūtīt personas datus uz trešajām valstīm, kurās netiek nedrošināts pienācīgs aizsardzības līmenis.
- 69 Tomēr šādas pārsūtīšanas kontroles nolūkos šīs direktīvas 25. panta 6. punkta pirmajā daļā ir noteikts, ka Komisija “var konstatēt, ka trešā valsts nodrošina pietiekamu aizsardzības līmeni šā panta 2. punkta nozīmē, pamatojoties uz savas valsts tiesībām vai uz starptautiskajām saistībām, kuras tā noslēgusi [tā uzņēmusies] [...] par personu privātās dzīves un pamatbrīvību un [pamat]tiesību aizsardzību”.
- 70 Protams, nedz Direktīvas 95/46 25. panta 2. punktā, nedz kādā citā tās normā nav pienācīga aizsardzības līmeņa definīcijas. It īpaši minētās direktīvas 25. panta 2. punktā ir vien minēts, ka trešās valsts piedāvātais pienācīgais aizsardzības līmenis “ir jānovērtē, paturot prātā visus ar datu pārsūtīšanas darbību vai datu pārsūtīšanas darbību kopumu cieši saistītos apstākļus”, un neizsmēļoši ir uzskaitīti apstākļi, kādi šādā vērtējumā būtu jāņem vērā.
- 71 Tomēr, no vienas puses, kā izriet no Direktīvas 95/46 25. panta 6. punkta formulējuma, šajā tiesību normā tiek prasīts, lai trešā valsts “nodrošina” pietiekamu aizsardzības līmeni, pamatojoties uz savas valsts tiesībām vai uz starptautiskajām saistībām. No otras puses, tāpat saskaņā ar šo tiesību normu trešās valsts nodrošinātais pienācīgais aizsardzības līmenis tiek vērtēts, “pamatojoties uz personu privātās dzīves un pamatbrīvību un [pamat]tiesību aizsardzību”.
- 72 Tādējādi ar Direktīvas 95/46 25. panta 6. punktu tiek īstenots skaidrs Hartas 8. panta 1. punktā paredzētais personas datu aizsardzības pienākums un tā mērķis, – kā to savu secinājumu 139. punktā ir norādījis ģenerālvokāts, – ir nodrošināt šīs aizsardzības augsta līmeņa turpinātību, personas datus pārsūtot uz trešo valsti.

- 73 Protams, Direktīvas 95/46 25. panta 6. punktā minētais jēdziens “pietiekams [pienācīgs]” nozīmē, ka nevar tikt prasīts, lai trešā valsts nodrošinātu aizsardzības līmeni, kas būtu identisks Savienības tiesiskajā kārtībā nodrošinātajam. Tomēr, kā to savu secinājumu 141. punktā ir norādījis ģenerālvokāts, “pienācīgs aizsardzības līmenis” būtu jāsaprot kā tāds, kur šī trešā valsts tik tiešām, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tā uzņēmusies, nodrošina būtībā ekvivalentu pamatbrīvību un pamattiesību aizsardzības līmeni, kāds saskaņā ar Direktīvu 95/46, to lasot Hartas gaismā, ir garantēts Savienībā. Faktiski, ja šādas prasības nebūtu, šī sprieduma iepriekšējā punktā minētais mērķis netiktu ievērots. Turklāt ar Direktīvu 95/46, to lasot Hartas gaismā, garantēto augsto aizsardzības līmeni viegli varētu neievērot, personas datus no Savienības pārsūtot uz trešajām valstīm, lai tos apstrādātu šajās valstīs.
- 74 No Direktīvas 95/46 25. panta 6. punkta formulējuma skaidri izriet, ka tieši Komisijas lēmumā minētajai trešās valsts tiesiskajai kārtībai ir jānodrošina pienācīgs aizsardzības līmenis. Pat ja līdzekļi, pie kuriem šī trešā valsts ņemas šādas aizsardzības nodrošināšanai, var atšķirties no tiem, kas tikuši likti lietā Savienībā, lai nodrošinātu no šīs direktīvas, to lasot Hartas gaismā, izrietošo prasību ievērošanu, šiem līdzekļiem tik un tā praksē būtu jābūt efektīviem, lai nodrošinātu būtībā Savienībā esošajai aizsardzībai ekvivalentu aizsardzību.
- 75 Šajos apstākļos vērtējumā par trešās valsts piedāvāto aizsardzības līmeni Komisijai ir jāizvērtē to šajā valstī piemērojamo tiesību normu saturs, kas izriet no iekšējiem tiesību aktiem vai starptautiskām saistībām, ko tā uzņēmusies, kā arī prakse, kuras mērķis ir nodrošināt šo normu ievērošanu, un šai iestādei atbilstoši Direktīvas 95/46 25. panta 2. punktam ir jāņem vērā visi ar personas datu pārsūtīšanu uz trešo valsti saistītie apstākļi.
- 76 Tāpat, ņemot vērā, ka trešās valsts nodrošinātais aizsardzības līmenis, iespējams, var mainīties, Komisijai pēc lēmuma pieņemšanas atbilstīgi Direktīvas 95/46 25. panta 6. punktam periodiski ir jāpārbauda, vai konstatētais saistībā ar aplūkotās trešās valsts nodrošināto pienācīgo aizsardzības līmeni vēl joprojām ir faktiski un juridiski pamatots. Vajadzība pēc šāda vērtējuma katrā ziņā rodas, ja norādes rada šaubas šai sakarā.
- 77 Turklāt savu secinājumu 134. un 135. punktā ģenerālvokāts arī ir norādījis, ka, pārbaudot Komisijas lēmuma, kas pieņemts saskaņā ar Direktīvas 95/46 25. panta 6. punktu, spēkā esamību, ir jāņem vērā arī apstākļi, kas iestājušies pēc šī lēmuma pieņemšanas.
- 78 Šai sakarā ir jākonstatē, ka, ņemot vērā, pirmkārt, nozīmīgo lomu, kāda personas datu aizsardzībai ir attiecībā uz pamattiesībām uz privātās dzīves neaizskaramību, un, otrkārt, lielo skaitu personu, kuru pamattiesības, iespējams, var tikt pārkāptas, personas datus pārsūtot uz trešajām valstīm, kurā nav nodrošināts pienācīgs aizsardzības līmenis, Komisijas pārbaudes pilnvaras saistībā ar trešās valsts nodrošinātu pietiekamu aizsardzības līmeni ir ierobežotas, tādēļ ir jāveic stingra no Direktīvas 95/46 25. panta, to lasot Hartas gaismā, izrietošo prasību pārbaude (pēc analogijas skat. spriedumu *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 47. un 48. punkts).

Par Lēmuma 2000/520 1. pantu

- 79 Lēmuma 2000/520 1. panta 1. punktā Komisija norādīja, ka tā I pielikumā minētie principi, kas piemēroti atbilstīgi norādījumiem, kuri sniegti minētā lēmuma II pielikumā minētajos FAQ, nodrošina pienācīgu to personas datu aizsardzības līmeni, ko no Savienības nosūta Amerikas Savienotajās Valstīs reģistrētām organizācijām. No šīs tiesību normas izriet, ka gan šos principus, gan šos FAQ ir publicējusi ASV Tirdzniecības ministrija.
- 80 No šī lēmuma 1. panta 2. un 3. punkta, tos lasot kopā ar minētā lēmuma II pielikumā atrodamo 6. FAQ, izriet, ka organizācijas piesaistīšana “drošības zonas” principiem norit, pamatojoties uz pašsertifikācijas sistēmu.

- 81 Lai arī tas, ka trešā valsts izmanto pašsertifikācijas sistēmu, pats par sevi nav pretrunā Direktīvas 95/46 25. panta 6. punktā noteiktajai prasībai, saskaņā ar kuru attiecīgajai trešajai valstij ir jānodrošina pienācīgs aizsardzības līmenis, “pamatojoties uz šīs valsts iekšējiem tiesību aktiem vai starptautiskām saistībām, ko tā uzņēmusies”, šādas sistēmas ticamība šīs prasības kontekstā būtībā balstās uz efektīvu atklāšanas un kontroles mehānismu ieviešanu, praksē ļaujot noteikt tādu normu iespējamus pārkāpumus, kas nodrošina pamattiesību aizsardzību, tostarp tiesības uz privāto dzīvi, kā arī tiesības uz personas datu aizsardzību, un piemērot sankcijas par tiem.
- 82 Šajā gadījumā drošības zonas principi saskaņā ar Lēmuma 2000/520 I pielikuma otro daļu ir domāti “tikai tā[m] ASV organizācij[ām], kas personas datus saņem no Eiropas Savienības un kuras izpilda “drošības zonas” nosacījumus, un uz kurām tādējādi var attiecināt no tās izrietošo pieņemumu par “atbilstību””. Tādēļ šos principus piemēro tikai pašsertificētām ASV organizācijām, kas personas datus saņem no Savienības, neizvirzot prasību, lai ASV iestādes minētos principus ievērotu.
- 83 Turklāt saskaņā ar Lēmuma 2000/520 2. pantu tas “attiecas tikai uz pienācīgu aizsardzību, ko Amerikas Savienotās Valstis nodrošina saskaņā ar [drošības zonas] principiem, kas īstenoti atbilstīgi FAQ, lai izpildītu Direktīvas [95/46] 25. panta 1. punkta prasības”, taču tajā nav ietverti pietiekami secinājumi par pasākumiem, ar kuru palīdzību Amerikas Savienotās Valstis nodrošina pienācīgu aizsardzības līmeni šīs direktīvas 25. panta 6. punkta izpratnē, pamatojoties uz to iekšējiem tiesību aktiem vai starptautiskām saistībām, ko tās uzņēmusies.
- 84 Papildinot – saskaņā ar Lēmuma 2000/520 I pielikuma ceturto daļu minēto principu piemērojamība tostarp var tikt ierobežota ar “prasībām par valsts drošību, sabiedrības interes[ēm] un/vai [lai] ievērotu Amerikas Savienoto Valstu [...] likumus”, kā arī “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”.
- 85 Šai sakarā Lēmuma 2000/520 IV pielikuma B daļā saistībā ar ierobežojumiem, kādiem drošības zonas principu piemērojamība ir pakļauta, ir uzsvērts, ka “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”.
- 86 Tā Lēmumā 2000/520 ir iedibināts “valsts drošība[s], sabiedrības intere[šu] un/vai Amerikas Savienoto Valstu [...] likumu” pārkāpums pār “drošības zonas principiem”, saskaņā ar kuru pašsertificētām ASV organizācijām, kas personas datus saņem no Savienības, bez jebkādiem ierobežojumiem no šiem principiem ir jāatkāpjas, ja tie nonāk pretrunā šīm prasībām un tādējādi izrādās ar tām nesaderīgi.
- 87 Ņemot vērā Lēmuma 2000/520 I pielikuma ceturtajā daļā atrodamo vispārīgo atkāpi, ar to ir radīta iespēja, pamatojoties uz prasībām, kas saistītas ar valsts drošību un sabiedrības interesēm vai ASV tiesisko regulējumu, iejaukties to personu pamattiesībās, kuru personas dati ir vai var tikt pārsūtīti no Savienības uz ASV. Lai pierādītu, ka pastāv iejaukšanās pamattiesībās uz privātās dzīves neaizskaramību, nav nozīmes tam, vai attiecīgajai informācijai par privāto dzīvi ir vai nav delikāts raksturs, vai arī tam, vai attiecīgajām personām ir vai nav radītas iespējamās neērtības šīs iejaukšanās dēļ (spriedums *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 33. punkts un tajā minētā judikatūra).
- 88 Turklāt Lēmumā 2000/520 nav ietverts neviens secinājums par to, ka ASV ir spēkā valsts tiesību akti, kuru mērķis ir ierobežot iespējamo iejaukšanos to personu pamattiesībās, kuru dati no Savienības ir pārsūtīti uz ASV, – iejaukšanos, ko šīs valsts struktūras ir tiesīgas praktizēt, ja tā kalpo leģitīmam mērķim – kā valsts drošība.
- 89 Tas ir jāpapildina ar faktu, ka Lēmumā 2000/520 nav runas par efektīvas tiesiskās aizsardzības pret šāda veida iejaukšanos esamību. Kā to savu secinājumu 204.–206. punktā norāda ģenerāladvokāts, privāti strīdu izšķiršanas mehānismi un procedūras Federālajā tirdzniecības komisijā, kuras attiecīgās

pilnvaras, kas tostarp aprakstītas šī lēmuma II pielikumā ietvertajā 11. visbiežāk uzdotajā jautājumā, ir ierobežotas ar komercstrīdiem par to, vai ASV uzņēmumi ievēro drošības zonas principus, un tie nevar tikt īstenoti strīdos par tādas iejaukšanās pamattiesībās likumību, kas izriet no valsts struktūras pasākumiem.

- 90 Turklāt iepriekš veikto Lēmuma 2000/520 analīzi apstiprina vērtējums, ko Komisija pati ir veikusi par situāciju, kas izriet no šī lēmuma īstenošanas. Faktiski Paziņojuma COM(2013) 846 *final* 2. un 3.2. punktā, kā arī Paziņojuma COM(2013) 847 *final* 7.1., 7.2. un 8. punktā, kuru saturs skaidri ir izklāstīts šī sprieduma 13.–16. punktā, kā arī 22., 23. un 25. punktā, šī iestāde konstatēja, ka ASV iestādes varēja piekļūt personas datiem, kas ir pārsūtīti no dalībvalstīm uz ASV, un tos apstrādāt neatbilstīgi tostarp pārsūtīšanas mērķiem, pārsniedzot to, kas ir absolūti nepieciešams un samērīgs ar valsts drošības aizsardzību. Tāpat Komisija konstatēja, ka attiecīgo personu rīcībā nav administratīvu vai juridisku tiesiskās aizsardzības līdzekļu, lai piekļūtu datiem, kas uz tām attiecas, un vajadzības gadījumā panākt to labošanu vai dzēšanu.
- 91 Attiecībā uz Savienībā garantēto pamatbrīvību un pamattiesību aizsardzības līmeni tās tiesiskajā regulējumā, kurā ir ietverta iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās, saskaņā ar Tiesas pastāvīgo judikatūru ir jāparedz skaidri un precīzi noteikumi, kas reglamentētu attiecīgā pasākuma apjomu un piemērošanu un noteiktu minimālās prasības tādējādi, lai personām, kuru personas dati ir tikuši skarti, 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. Šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves šiem datiem risks (spriedums *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 54. un 55. punkts, kā arī tajos minētā judikatūra).
- 92 Turklāt un vispirmām kārtām, pamattiesību uz privātās dzīves neaizskaramību aizsardzības Savienības līmenī pamatā ir prasība, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti absolūti nepieciešamā ietvaros (spriedums *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 52. punkts un tajā minētā judikatūra).
- 93 Tā līdz absolūti nepieciešamajam nav ierobežots tiesiskais regulējums, saskaņā ar kuru vispārīgi tiek pieļauta visu to personu personas datu saglabāšana, kuru dati no Savienības ir pārsūtīti uz ASV – nešķirojot, bez ierobežojumiem vai izņēmumiem saistībā ar mērķi, kam tie kalpo, vai neparedzot objektīvus kritērijus, kas valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu ļauj ierobežot precīzi, strikti ierobežotiem un tādiem mērķiem, kas pamato gan piekļuvi šiem datiem, gan arī to izmantošanu (šajā ziņā saistībā ar Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīvu 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tiklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK (OV L 105, 54. lpp.) skat. spriedumu *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 57.–61. punkts).
- 94 It īpaši tiesiskais regulējums, saskaņā ar kuru valsts iestādēm vispārīgi tiek ļauts piekļūt elektronisko komunikāciju saturam, ir jāuzskata par tādu, kas apdraud pašu Hartas 7. pantā garantēto pamattiesību uz privātās dzīves neaizskaramību būtību (šajā ziņā skat. spriedumu *Digital Rights Ireland* u.c., C-293/12 un C-594/12, EU:C:2014:238, 39. punkts).
- 95 Tāpat tiesiskajā regulējumā, kurā indivīdiem nav paredzētas nekādas iespējas likt lietā tiesību aizsardzības līdzekļus, lai piekļūtu personas datiem, kas uz tiem attiecas, vai panākt šādu datu labošanu vai dzēšanu, nav ņemta vērā Hartas 47. pantā iedibināto pamattiesību uz efektīvu aizsardzību tiesā būtība. Hartas 47. panta pirmajā daļā ir noteikts, ka ikvienai personai, kuras tiesības un brīvības, kas garantētas Savienības tiesībās, tikušas pārkāptas, ir tiesības uz efektīvu tiesību aizsardzību tiesā, ievērojot nosacījumus, kuri paredzēti šajā pantā. Šai sakarā pārbaude tiesā, kuras mērķis ir nodrošināt Savienības tiesību normu ievērošanu, ir raksturīga tiesiskai valstij (šajā ziņā skat. spriedumus *Les Verts*

/Parlaments, 294/83, EU:C:1986:166, 23. punkts; *Johnston*, 222/84, EU:C:1986:206, 18. un 19. punkts; *Heylens* u.c., 222/86, EU:C:1987:442, 14. punkts, kā arī *UGT-Rioja* u.c., no C-428/06 līdz C-434/06, EU:C:2008:488, 80. punkts).

- 96 Kā tas ticis konstatēts tostarp šī sprieduma 71., 73. un 74. punktā, lēmuma, ko Komisija ir pieņēmusi atbilstīgi Direktīvas 95/46 25. panta 6. punktam, pieņemšanas pamatā ir šīs iestādes pienācīgi pamatots secinājums par to, ka trešā valsts tik tiešām, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tā uzņēmusies, nodrošina būtībā ekvivalentu pamatbrīvību un pamattiesību aizsardzības līmeni tam, kāds tiek garantēts Savienības tiesiskajā kārtībā, kā tas it īpaši izriet no šī sprieduma iepriekšējiem punktiem.
- 97 Jānorāda, ka Komisija Lēmumā 2000/520 nav norādījusi, ka ASV reāli “nodrošina” pienācīgu aizsardzības līmeni, pamatojoties uz savu iekšējo tiesisko kārtību vai starptautiskajām saistībām, ko tās uzņēmušas.
- 98 Tālāk un nepastāvēt vajadzībai izvērtēt drošības zonas principu saturu, ir jāsecina, ka šī lēmuma 1. pantā nav ievērotas Direktīvas 95/46 25. panta 6. punktā, to lasot Hartas gaismā, noteiktās prasības un tādēļ tas nav spēkā.

Par Lēmuma 2000/520 3. pantu

- 99 No šī sprieduma 53., 57. un 63. punktā minētajiem apsvērumiem izriet, ka, ņemot vērā Direktīvas 95/46 28. pantu, to lasot it īpaši Hartas 8. panta gaismā, valsts uzraudzības iestādēm pilnīgi neatkarīgi ir jāvar izvērtēt ikvienu prasību par personas tiesību un brīvību aizsardzību saistībā ar to personas datu apstrādi, kas uz to attiecas. Tā tas it īpaši ir tad, kad šī persona šādā prasībā iebilst pret tāda Komisijas lēmuma saderīgumu ar privātās dzīves aizsardzību un personu pamatbrīvībām un pamattiesībām, kas pieņemts atbilstoši šīs direktīvas 25. panta 6. punktam.
- 100 Tomēr Lēmuma 2000/520 3. panta 1. punkta pirmajā daļā ir paredzēts īpašs tiesiskais regulējums par pilnvarām, ar kurām valsts uzraudzības iestādes ir apveltītas saistībā ar Komisijas konstatēto par pienācīgu aizsardzības līmeni Direktīvas 95/46 25. panta izpratnē.
- 101 Tā saskaņā ar šo tiesību normu šīs iestādes, “neskarot [to] pilnvaras rīkoties, lai nodrošinātu to valsts tiesību aktu ievērošanu, kuri ir pieņemti atbilstīgi noteikumiem, izņemot Direktīvas [95/46] 25. pantu, [var] īstenot savas pašreizējās pilnvaras, lai aizliegtu vai pārtrauktu datu plūsmu uz organizāciju” ierobežojošos apstākļos, radot augstu iejaukšanās sliekšni. Lai gan šajā tiesību normā nav ierobežotas šo iestāžu pilnvaras rīkoties, lai ievērotu valsts tiesību normas, kas pieņemtas saskaņā ar šo direktīvu, tajā tomēr ir izslēgtas minēto iestāžu pilnvaras veikt darbības, lai ņemtu vērā šīs pašas direktīvas 25. pantu.
- 102 Tādēļ Lēmuma 2000/520 3. panta 1. punkta pirmā daļa ir jāsaprot kā tāda, ar kuru valsts uzraudzības iestādēm tiek atņemtas kontroles pilnvaras, ar kurām tās atbilstoši Direktīvas 95/46 28. pantam ir apveltītas gadījumā, kad persona saskaņā ar šo tiesību normu iesniegtā prasībā izvirza apsvērumus, ar kuriem tiek apšaubīts tāda Komisijas lēmuma saderīgums ar privātās dzīves neaizskaramības un personu pamatbrīvību un pamattiesību aizsardzību, kurā, pamatojoties uz šīs direktīvas 25. panta 6. punktu, ir konstatēts, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni.
- 103 Izpildes pilnvaras, ko Savienības likumdevējs Direktīvas 95/46 25. panta 6. punktā ir piešķīris Komisijai, šai iestādei nepiešķir kompetenci ierobežot šī sprieduma iepriekšējā punktā minētās valsts uzraudzības iestāžu pilnvaras.

- 104 Šajos apstākļos ir jākonstatē, ka, pieņemdamā Lēmuma 2000/520 3. pantu, Komisija ir pārsniegusi savas Direktīvas 95/46 25. panta 6. punktā, to lasot Hartas gaismā, piešķirtās kompetences robežas; no tā izriet, ka pants nav spēkā.
- 105 Tā kā Lēmuma 2000/520 1. un 3. pants nav nodalāmi no šī lēmuma 2. un 4. panta, kā arī tā pielikumiem, to spēkā neesamības rezultātā spēku zaudē arī lēmums kopumā.
- 106 Ņemot vērā visus iepriekš minētos apsvērumus, ir jāsecina, ka Lēmums 2000/520 nav spēkā.

Par tiesāšanās izdevumiem

- 107 Attiecībā uz pamatlietas pusēm šī tiesvedība ir stadija procesā, kuru izskata iesniedzējtiesa, un tā lemj par tiesāšanās izdevumiem. Izdevumi, kas radušies, iesniedzot apsvērumus Tiesai, un kas nav minēto pušu izdevumi, nav atlīdzināmi.

Ar šādu pamatojumu Tiesa (virspalāta) nospriež:

- 1) 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, kurā grozījumi izdarīti ar Eiropas Parlamenta un Padomes 2003. gada 29. septembra Regulu (EK) Nr. 1882/2003, 25. panta 6. punkts, to lasot Eiropas Savienības Pamattiesību hartas 7. 8. un 47. panta gaismā, ir jāinterpretē tādējādi, ka saskaņā ar šo tiesību normu pieņemts lēmums – kā Komisijas 2000. gada 26. jūlija Lēmums 2000/520/EK atbilstīgi Direktīvai 95/46 par pienācīgu aizsardzību, kas noteikta ar privātuma “drošības zonas” principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija –, kurā Eiropas Komisija konstatē, ka trešā valsts nodrošina pienācīgu aizsardzības līmeni, nav šķērslis tam, lai dalībvalsts uzraudzības iestāde šīs grozītās direktīvas 28. panta izpratnē izskatītu personas prasību par tās tiesību un brīvību aizsardzību saistībā ar to personas datu apstrādi, kas uz viņu attiecas un kuri ir tikuši no dalībvalsts pārsūtīti uz šo trešo valsti, ja šī persona apgalvo, ka tajā spēkā esošās tiesības un prakse nenodrošina pienācīgu aizsardzības līmeni;
- 2) Lēmums 2000/520 nav spēkā.

[Paraksti]