16/LV
WP 238

Atzinums Nr. 1/2016 par ES un ASV privātuma vairoga pietiekamības lēmuma projektu

Pieņemts 2016. gada 13. aprīlī

Šī darba grupa tika izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas konsultatīvā organizācija datu aizsardzības un privātuma jautājumos. Tās uzdevumi ir izklāstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā.

Sekretariātu nodrošina Eiropas Komisijas Tiesiskuma un patērētāju ģenerāldirektorāta C direktorāts (Pamattiesības un Savienības pilsonība), B-1049 Brisele, Beļģija, birojs Nr. MO-59 02/013.

Tīmekļa vietne: http://ec.europa.eu/justice/data-protection/index_en.htm

KOPSAVILKUMS

2016. gada 29. februārī Eiropas Komisija publicēja paziņojumu — pietiekamības lēmuma projektu un tam pievienotos tekstus, kas veido jaunu regulējumu attiecībā uz personas datu transatlantisko apmaiņu komerciālos nolūkos: ES un ASV privātuma vairogu (turpmāk tekstā — privātuma vairogs), kura mērķis ir aizstāt iepriekšējo ASV drošības zonu, ko 2015. gada 6. oktobrī atcēlusi Eiropas Savienības Tiesa (turpmāk tekstā — EST) *Schrems* lietā.

Saskaņā ar Direktīvas 95/46/EK 30. panta 1. punkta c) apakšpunktu 29. panta darba grupa (turpmāk tekstā — DG29) izvērtēja šos dokumentus, lai sniegtu savu atzinumu par pietiekamības lēmuma projektu. DG29 vērtēja gan privātuma vairoga komerciālos aspektus, gan iespējamās atkāpes no tā principiem nacionālās drošības, tiesībaizsardzības un sabiedrības interešu nolūkos.

DG29 ņēma vērā piemērojamo ES datu aizsardzības tiesisko regulējumu, kas noteikts Direktīvā 95/46/EK, kā arī pamattiesības uz privāto dzīvi un datu aizsardzību, kas noteiktas Eiropas Cilvēktiesību konvencijas 8. pantā un Eiropas Savienības Pamattiesību hartas 7. un 8. pantā. Darba grupa ņēma vērā arī hartas 47. pantā noteiktās tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu, kā arī tiesu praksi, kas saistīta ar dažādām pamattiesībām.

Turklāt analīze atspoguļo EST argumentāciju *Schrems* lietā par Komisijas rīcības brīvību attiecībā uz pietiekamības novērtēšanu. Ir jāveic pietiekamības prasību strikta pārbaude un kontrole, ņemot vērā pamattiesības uz privātumu un datu aizsardzību un to personu skaitu, ko nosūtīšana varētu ietekmēt.

Privātuma vairogs ir jāskata pašreizējā starptautiskajā kontekstā, saistībā ar lielo datu parādīšanos un pieaugošajām drošības vajadzībām. Personas datu vākšanas un izmantošanas sfēra ir ievērojami paplašinājusies, un apjoms ir krasi pieaudzis, kopš 2000. gadā tika izdots sākotnējais lēmums par drošības zonu. Eiropas datu aizsardzības iestādes stingri aizstāv savu aizsargāto principu nozīmi.

DG29 vispirms atzinīgi vērtē lielos uzlabojumus, ko privātuma vairogs piedāvā salīdzinājumā ar lēmumu par drošības zonu. Darba grupa norāda, ka sarunu dalībnieki ir pievērsuši uzmanību daudziem drošības zonas trūkumiem, ko grupa bija uzsvērusi 2014. gada 10. aprīļa vēstulē priekšsēdētāja vietniecei Redingai.

Fakts, ka privātuma vairoga principi un sniegtās garantijas ir izklāstītas gan pietiekamības lēmumā, gan tā pielikumos, padara informāciju grūti atrodamu un dažkārt arī pretrunīgu. Tāpēc trūkst skaidrības par jauno regulējumu, un pieejamība datu subjektiem, organizācijām un datu aizsardzības iestādēm ir apgrūtināta. Skaidrības trūkst arī izmantotajā valodā. Tāpēc DG29 mudina Komisiju padarīt minētās lietas skaidras un saprotamas abām Atlantijas okeāna pusēm.

Attiecībā uz piemērojamiem tiesību aktiem DG29 uzsver, ka gadījumā, ja privātuma vairoga pietiekamības lēmums tiek pieņemts, pamatojoties uz Direktīvu 95/46/EK, tam ir jāatbilst ES

datu aizsardzības tiesiskajam regulējumam gan darbības jomas, gan terminoloģijas ziņā. DG29 uzskata, ka neilgi pēc tam, kad sāk piemērot Vispārīgo datu aizsardzības regulu, lēmums būtu jāpārskata, lai nodrošinātu, ka pietiekamības lēmumā un tā pielikumos tiek ievērots regulā piedāvātais augstākais datu aizsardzības līmenis.

Par privātuma vairoga komerciālajiem aspektiem

DG29 galvenais mērķis ir pārliecināties, ka personām tiek nodrošināts pēc būtības līdzvērtīgs aizsardzības līmenis, kad personas dati tiek apstrādāti saskaņā ar privātuma vairoga noteikumiem. Lai gan DG29 negaida, ka privātuma vairogs būs ES tiesiskā regulējuma precīza un izsmeļoša kopija, darba grupa uzskata, ka tam būtu jāietver pamatprincipu būtība un attiecīgi jānodrošina „pēc būtības līdzvērtīgs" aizsardzības līmenis.

Par spīti privātuma vairoga piedāvātajiem uzlabojumiem, DG29 uzskata, ka daži galvenie datu aizsardzības principi, kas noteikti Eiropas tiesībās, nav atspoguļoti pietiekamības lēmuma projektā un tā pielikumos vai ir nepietiekami aizstāti ar alternatīviem jēdzieniem.

Piemēram, datu saglabāšanas princips nav skaidri minēts, un to nevar skaidri interpretēt no datu integritātes un nolūka ierobežojuma principa pašreizējā formulējuma. Turklāt, nav formulēta aizsardzība, kas būtu jānodrošina pret automatizētiem individuāliem lēmumiem, pamatojoties tikai un vienīgi uz automatizētu apstrādi. Arī nolūka ierobežojuma principa piemērošana datu apstrādei nav skaidra. Lai ieviestu lielāku skaidrību vairāku svarīgu jēdzienu lietojumā, DG29 ierosina ES un ASV vienoties par skaidrām definīcijām, kas būtu iekļautas privātuma vairoga BUJ terminu glosārijā.

Privātuma vairogs tiks izmantots datu nosūtīšanai arī ārpus ASV, tāpēc DG29 uzstāj, ka tālākai nosūtīšanai no privātuma vairoga subjekta trešo valstu saņēmējiem būtu jānodrošina tāds pats aizsardzības līmenis visos vairoga aspektos (tostarp nacionālās drošības aspektā) un nosūtīšana nedrīkst vājināt vai apiet ES datu aizsardzības principus. Gadījumā, ja ir paredzēta tālāka nosūtīšana uz trešo valsti saskaņā ar privātuma vairogu, ikvienai privātuma vairoga organizācijai ir pienākums pirms nosūtīšanas izvērtēt konkrētās trešās valsts tiesību aktos ietvertās obligātās prasības, kas piemērojamas datu saņēmējam. Kopumā DG29 secina, ka ES personas datu tālāka nosūtīšana nav pietiekami regulēta, jo īpaši attiecībā uz tās piemērošanas jomu, nolūka ierobežošanu un garantijām, kas attiecas uz nosūtīšanu pārstāvjiem.

Visbeidzot, lai gan DG29 norāda uz papildu iespējām, kas personām sniegtas, lai tās varētu izmantot savas tiesības, darba grupai ir bažas, ka jaunais tiesiskās aizsardzības mehānisms praksē var izrādīties pārāk sarežģīts, ES iedzīvotājiem būtu grūti to izmantot, un tāpēc tas būtu neefektīvs. Tāpēc ir jāprecizē dažādās tiesībaizsardzības procedūras; jo īpaši, ES datu aizsardzības iestādes varētu uzskatīt par kontaktpunktiem, kur ES iedzīvotāji var vērsties saistībā ar dažādām procedūrām un kuras var rīkoties šo personu vārdā, ja iestādes ir gatavas to darīt.

Atkāpes nacionālās drošības nolūkos

Attiecībā uz valsts iestāžu piekļuvi datiem gan ES, gan trešajās valstīs DG29 atsaucas uz tās sagatavoto pamattiesību analīzi, kas ietverta darba dokumentā par pamattiesību uz privātumu un datu aizsardzību ierobežošanas, izmantojot uzraudzības pasākumus personas datu nosūtīšanas procesā, pamatotību (Eiropas pamatgarantijas) (DG237).

Liels progress salīdzinājumā ar lēmumu par drošības zonu ir tas, ka pietiekamības lēmuma projektā tiek plaši aplūkota iespējamā piekļuve datiem, kas saskaņā ar privātuma vairogu tiek apstrādāti nacionālās drošības un tiesībaizsardzības nolūkā. DG29 atzīst šo ievērojamo progresu un izlūkošanas datu vākšanai piemērojamo tiesību aktu labāku pārredzamību (VI pielikums), ko nodrošina ASV valdība.

Tomēr DG29 norāda, ka ASV Nacionālās izlūkošanas direktora biroja (NIDB) pārstāvniecības neizslēdz ES izcelsmes personas datu masveida un nekritisku vākšanu. DG29 norāda uz savu ilgstošo nostāju, ka personu masveida un nekritisku novērošanu nevar uzskatīt par samērīgu un noteikti nepieciešamu demokrātiskā sabiedrībā, kā to pieprasa piemērojamo pamattiesību piedāvātā aizsardzība. Turklāt ļoti būtiska ir visu novērošanas programmu visaptveroša uzraudzība. DG29 ņem vērā, ka saistībā ar cīņu pret terorismu pastāv tendence vākt arvien vairāk datu masveidā un nekritiski. Ņemot vērā bažas, kas tās dēļ rodas par privātuma un datu aizsardzības pamattiesību aizsardzību, DG29 gaida EST izskatīšanā esošos nolēmumus lietās par datu masveida un nekritisku vākšanu.

Attiecībā uz tiesisko aizsardzību DG29 atzinīgi vērtē ombuda kā jauna tiesiskās aizsardzības mehānisma izveidi. Tas var ievērojami uzlabot ES iedzīvotāju tiesību stāvokli attiecībā pret ASV izlūkošanas darbībām. Tomēr DG29 bažījas, ka šī jaunā iestāde nav pietiekami neatkarīga un tai nav piešķirtas atbilstošas pilnvaras, lai efektīvi īstenotu tās pienākumus, un tā negarantē apmierinošu tiesiskās aizsardzības līdzekli domstarpību gadījumā.

Kopīga pārskatīšana

Pietiekamības lēmuma projektā minētais ikgadējais kopīgās pārskatīšanas mehānisms ir privātuma vairoga vispārējās uzticamības galvenais faktors, un DG29 ļoti atzinīgi vērtē tā sniegto iespēju pārskatīt pietiekamības lēmumu. Šajā sakarā DG29 saprot, ka DG29 iesaistīto valstu pārstāvji varēs pilnībā piedalīties pārskatīšanas procesā, bet lūdz paskaidrot precīzu kārtību. Par kārtību (tostarp par izrietošo ziņojumu, tā publicitāti un iespējamām sekām, kā arī finansējumu) ir jāvienojas krietnu laiku pirms pirmā pārskata.

Secinājumi

DG29 atzīmē galvenos uzlabojumus, ko privātuma vairogs piedāvā, salīdzinot ar lēmumu par drošības zonu, kas atzīts par spēkā neesošu. Ņemot vērā izteiktās bažas un lūgtos paskaidrojumus, DG29 aicina Komisiju risināt šos jautājumus, noteikt piemērotus risinājumus un sniegt pieprasītos paskaidrojumus, lai uzlabotu pietiekamības lēmuma projektu un nodrošinātu, ka privātuma vairoga sniegtā aizsardzība pēc būtības ir līdzvērtīga ES sniegtajai aizsardzībai.

SATURA RĀDĪTĀJS

1. IEVADS

Pamatojoties uz Eiropas Savienības Tiesas (turpmāk tekstā — EST) 2015. gada 6. oktobra spriedumu *Schrems* lietā[1], 29. panta darba grupa (turpmāk tekstā — DG29, darba grupa) aicināja Eiropas Savienības dalībvalstis (turpmāk tekstā — ES) un pārējās Eiropas iestādes uzsākt sarunas ar Amerikas Savienoto Valstu (turpmāk tekstā — ASV) iestādēm, lai rastu politiskos, juridiskos un tehniskos risinājumus, kas ļautu nosūtīt datus uz ASV teritoriju, ievērojot pamattiesības.

2016. gada 2. februārī, pēc vairāk nekā divus gadus ilgām sarunām, Eiropas Komisija un ASV Tirdzniecības ministrija panāca politisku vienošanos par *jaunu regulējumu attiecībā uz personas datu transatlantisko apmaiņu komerciālos nolūkos: ES un ASV privātuma vairogu* (turpmāk tekstā — privātuma vairogs), kura mērķis ir aizstāt iepriekšējo ASV drošības zonu.

2016. gada 29. februārī Komisija publicēja paziņojumu[2] — pietiekamības lēmuma projektu un tam pievienotos tekstus, kas veidos privātuma vairogu. Saskaņā ar Direktīvas 95/46/EK (turpmāk tekstā — Direktīva) 30. panta 1. punkta c) apakšpunktu DG29 izvērtēja šos dokumentus, lai sniegtu savu pašreizējo viedokli par Komisijas sagatavoto pietiekamības lēmuma projektu, ieskaitot saistītos privātuma vairoga dokumentus. Vērtējuma ietvaros DG29 ir sadalījusi savu darbu starp privātuma vairoga komerciālo aspektu vērtējumu un to drošības pasākumu analīzi, kas veikti attiecībā uz atkāpēm no privātuma vairoga principiem nacionālās drošības, tiesībaizsardzības un sabiedrības interešu nolūkos.

Pēc sprieduma *Schrems* lietā DG29 ir vairākas reizes tikusies ar ASV valdības delegācijām, ES un ASV pilsoniskās sabiedrības organizāciju pārstāvjiem, kā arī zinātniekiem, lai sagatavotu *Schrems* spriedumu seku novērtējumu. Privātuma vairoga vērtēšanas laikā ir organizētas arī citas tikšanās ar Eiropas Komisiju un ASV valdības pārstāvjiem. Šajās tikšanās reizēs tika sniegti daži precizējumi, kas arī ir ņemti vērā šajā atzinumā. DG29 uzsver, ka šajā posmā šie paskaidrojumi ir tikai neformāli un tos nevar uzskatīt par pietiekamības lēmuma projekta neatņemamu daļu, jo tie vēl nav sagatavoti rakstiski.

Tomēr DG29 īpaši atzinīgi vērtē minētajās tikšanās reizēs ASV Tirdzniecības ministrijas izrādīto apņemšanos sadarboties ar ES dalībvalstu datu aizsardzības iestādēm attiecībā uz privātuma vairoga piemērošanu un nodrošināt privātuma vairoga piemērošanas instrukcijas un juridisko interpretāciju, ko tās publicēs savās tīmekļa vietnēs.

1.1. Vispārīgas piezīmes

1.1.1. DG29 vērtējuma apjoms

DG29 vispirms ņēma vērā Eiropas Savienības dalībvalstīs piemērojamo datu aizsardzības regulējumu, tostarp Eiropas Cilvēktiesību konvencijas (turpmāk tekstā — ECK) 8. pantu, kas sargā tiesības uz privāto un ģimenes dzīvi, un Eiropas Savienības Pamattiesību hartas

[1] 2015. gada 6. oktobra spriedums lietā C-362/14 Maximillian *Schrems*/Data Protection Commissioner (turpmāk tekstā — *Schrems*).
[2] COM(2016)117 galīgā redakcija, 29.02.2016.

(turpmāk tekstā — harta) 7., 8. un 47. pantu, kas sargā attiecīgi tiesības uz privāto un ģimenes dzīvi, tiesības uz personas datu aizsardzību un tiesības uz tiesību aizsardzību un taisnīgu tiesu. Darba grupa ņēma vērā arī attiecīgo tiesu praksi, kā arī Direktīvas prasības.

EST *Schrems* lietā sīkāk definēja prasību trešajām valstīm nodrošināt pietiekamu datu aizsardzības līmeni. Tiesa paskaidroja, ka Direktīvas noteikumi ir jāinterpretē, „ņemot vērā hartas garantētās pamattiesības"[3] un jo īpaši tās 7. un 8. pantu. Tā arī norādīja, ka formulējums „pietiekams aizsardzības līmenis" ir jāsaprot kā „prasība trešajai valstij, pamatojoties uz tās tiesību aktiem vai starptautiskām saistībām, faktiski nodrošināt pamattiesību un brīvību aizsardzības līmeni, kas ir pēc būtības līdzvērtīgs tam, ko garantē Eiropas Savienībā atbilstoši Direktīvai, ņemot vērā hartu"[4]. Attiecībā uz agrāko lēmumu par drošības zonu nebija veikts pietiekami detalizēts šāda veida novērtējums. Tāpēc DG29 izvērtēja pietiekamības lēmuma projektu, ņemot vērā prasību sniegt analīzi par pamattiesību un brīvību aizsardzības līmeni, kas ir *pēc būtības līdzvērtīgs* ES garantētajam. DG29 uzsver, ka šajā atzinumā ir paudusi savas galvenās bažas, bet, ņemot vērā īso laiku, kas ir pagājis kopš pietiekamības lēmuma projekta publicēšanas, vēlāk var tikt atklātas arī citas problēmas.

DG29 atzīst, ka, definējot vārdu "pietiekams" Direktīvas 25. panta 6. punktā kā "pēc būtības līdzvērtīgs", EST sīkāk izklāstīja pietiekamību *Schrems* lietā. Tiesa ir uzsvērusi, ka termins „pietiekams aizsardzības līmenis", lai gan tas nepieprasa trešajai valstij nodrošināt aizsardzības līmeni, kas ir identisks ES tiesību sistēmā garantētajam, ir jāsaprot kā prasība trešajai valstij, pamatojoties uz to tiesību aktiem vai starptautiskām saistībām, faktiski nodrošināt pamattiesību un brīvību aizsardzības līmeni, kas ir *pēc būtības līdzvērtīgs* tam, ko garantē Eiropas Savienībā atbilstoši Direktīvai, ņemot vērā hartu.

1.1.2. Pietiekamības lēmuma projekta komerciālās daļas vērtējums

DG29 jau ir izskaidrojusi, kā tā piemēroja ES galvenos datu aizsardzības principus personas datu nosūtīšanai uz trešām valstīm, 12. darba dokumentā „Personas datu nosūtīšana uz trešām valstīm: ES datu aizsardzības direktīvas 25. un 26. panta piemērošana"[5]. DG29 centās atrast līdzvērtīgos drošības pasākumus, kas nodrošina Direktīvā garantētajiem principiem līdzvērtīgu aizsardzības līmeni, jo īpaši attiecībā uz nolūka ierobežojumu, datu kvalitāti un proporcionalitāti, pārredzamību, drošību, piekļuves tiesībām, izlabošanu un iebildumiem, datu saglabāšanu un tālākas nosūtīšanas ierobežojumiem. Līdzīga metode ir izmantota atzinumos, ko DG29 sagatavoja, vērtējot sākotnējo pietiekamības lēmumu par drošības zonu,[6] un 2014. gada 10. aprīlī publicētajos ieteikumos, ko darba grupa vēstulē nosūtīja bijušajai priekšsēdētāja vietniecei un ES tieslietu komisārei Vivjenai Redingai (*Viviane Reding*)[7].

[3] *Schrems*, 38. punkts
[4] *Schrems*, 73. punkts
[5] DG29 pieņēma 1998. gada 24. jūlijā, skatīt lēmuma 6. lapu
[6] Skatīt WP62, WP32, WP27, WP23, WP21, WP19, WP15 un WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

1.1.3. Attiecībā uz valsts iestāžu piekļuvi veikto atkāpju un drošības pasākumu vērtējums

To atkāpju novērtējums, kas veiktas attiecībā uz valsts iestāžu piekļuvi personas datiem, uz ko attiecas privātuma vairogs, ir sarežģīts, jo īpaši ņemot vērā datu aizsardzības iestāžu un sabiedrības pieaugošo izpratni par ASV novērošanas programmām pēc Snoudena (*Snowden*) atklājumiem. Darba grupa atzīst un atzinīgi vērtē ASV valdības centienus palielināt novērošanas programmu pārredzamību un tās vēlmi iekļaut privātuma vairogā papildu drošības pasākumus. Tai pašā laikā DG29 uzsver, ka jebkuram pamattiesību uz privātumu un datu aizsardzību ierobežojumam ir jābūt attaisnojamam demokrātiskā sabiedrībā. EST kritizēja faktu, ka lēmumā par drošības zonu nebija neviena konstatējuma par tādu noteikumu esamību ASV, kurus valsts pieņēmusi, lai mazinātu jebkāda veida ierobežojumus. Tāpat lēmumā nav minēts, ka pastāvētu efektīva tiesiskā aizsardzība pret šāda veida ierobežojumiem.[8]

Tāpēc DG29 analizēja ASV pašreizējo tiesisko regulējumu un ASV izlūkošanas aģentūru praksi, jo tie ir aprakstīti lēmuma projekta pielikumos, kā arī nosacījumus, ar kādiem tie pieļauj Eiropas tiesiskā regulējuma aizsargāto pamattiesību uz privātās dzīves un datu aizsardzību ierobežojumus.

Lai novērtētu to, vai kāds ierobežojums būtu attaisnojams demokrātiskā sabiedrībā, novērtējums tika veikts, ņemot vērā Eiropas tiesu praksi attiecībā uz pamattiesībām, kas nosaka izlūkošanas darbību četras galvenās garantijas[9]:

A. Apstrādei ir jābūt atbilstošai likumdošanai un balstītai uz skaidriem, precīziem un pieejamiem noteikumiem: tas nozīmē, ka ikvienam, kas ir pietiekami informēts, jāspēj paredzēt, kas varētu notikt ar viņa/viņas datiem, ja tie tiek nosūtīti;
B. Nepieciešamība un samērīgums attiecībā uz likumīgiem mērķiem jāpierāda: ir jārod līdzsvars starp mērķi, kuram dati tiek vākti un kura dēļ datiem piekļūst, un personas tiesībām;
C. Ir vajadzīgs neatkarīgs uzraudzības mehānisms, kas ir gan efektīvs, gan objektīvs: tas var būt tiesnesis vai cita neatkarīga struktūra, ja vien tai ir pietiekama spēja veikt nepieciešamās pārbaudes;
D. Personai ir jābūt pieejamiem efektīviem tiesiskās aizsardzības līdzekļiem: ikvienam ir jābūt tiesībām aizstāvēt savas tiesības neatkarīgā iestādē.

1.2. Pietiekamības lēmuma projekts

DG29 vispirms atzinīgi vērtē to, ka jaunu pietiekamības procedūru var uzsākt mazāk nekā sešus mēnešu laikā pēc tam, kad EST pasludināja lēmumu par drošības zonu spēkā neesošu. Ņemot vērā datu apjomu, kas ik dienas tiek nosūtīts starp ES un ASV, ko DG29 atzīst par svarīgu ekonomikas daļu abās Atlantijas okeāna pusēs, juridiskā skaidrība ir nepieciešama iespējami ātri.

[8] *Schrems*, 87., 88. punkts
[9] Eiropas pamatgarantijas balstās uz EST un ECT praksi un ir sīkāk izklāstītas DG29 darba dokumentā WP237, kas publicēts 2016. gada 13. aprīlī.

Tomēr DG29 pauž nožēlu, ka Komisijas publicētajā pietiekamības lēmuma projektā nav ASV iekšējo tiesību aktu un starptautisko saistību visaptveroša novērtējuma pietiekamības ziņojuma veidā, kas iepriekš bijusi regulāra prakse līdzīgās procedūrās un saskaņā ar Direktīvas 25. pantu. Tas neļāva DG29 veikt pilnīgu analīzi par tiesisko kontekstu, kurā privātuma vairogs darbosies. Tā norāda, piemēram, ka pašreizējā pietiekamības lēmuma projektā nav konstatējumu ne par privātuma un datu aizsardzības tiesību aktiem, kas pastāv ASV, federālā un valsts līmenī, tai skaitā nozaru tiesību aktiem, ne par tiesību aktiem, kas pieļauj publisku piekļuvi bez novērošanas. Nav definēta arī saistība starp datu nosūtīšanu saskaņā ar privātuma vairogu un saskaņā ar citiem spēkā esošajiem pietiekamības konstatējumiem, piemēram, ES un ASV Pasažieru datu reģistra (PDR) nolīgumu un Teroristu finansēšanas izsekošanas programmas (TFIP) nolīgumu.

1.2.1. ES datu aizsardzības regulējuma, jo īpaši Direktīvas 95/46/EK principu, piemērošanas joma

DG29 atgādina, ka saskaņā ar ES datu aizsardzības tiesisko regulējumu un jo īpaši saskaņā ar Direktīvu (4. panta 1. punktu), dalībvalstu tiesību aktus piemēro ne tikai apstrādes darbībām, ko veic valstu teritorijā reģistrētie datu pārziņi, bet arī tad, ja datu pārziņi (lai gan tie nav reģistrēti ES) izmanto iekārtas, kas atrodas ES teritorijā, jo īpaši attiecībā uz personas datu vākšanu. Tā rezultātā ES dalībvalstu tiesību akti attiecas uz jebkuru apstrādi, kas notiek pirms nosūtīšanas uz ASV, vai nu saistībā ar Eiropas Savienībā reģistrētas organizācijas darbību, vai ar tādu Eiropas Savienībā esošu iekārtu izmantošanu, ko izmanto organizācija, kas nav reģistrēta Eiropas Savienībā. DG29 pieprasa, lai tas būtu skaidri izteikts pietiekamības lēmuma projektā.

Ir jābūt skaidram, ka privātumu vairoga principi būs spēkā no datu nosūtīšanas brīža. Turklāt DG29 atgādina, ka uz datu pārziņiem, kas ir reģistrēti ES un datus nosūta datu apstrādātājiem ASV, attiecas ES datu aizsardzības tiesību akti.

1.2.2. Skaidrības trūkums par privātuma vairoga dokumentiem

Fakts, ka privātuma vairoga principi un sniegtās garantijas ir izklāstītas gan pietiekamības lēmumā, gan tā pielikumos, padara informāciju grūti atrodamu un dažkārt arī pretrunīgu. Tāpēc trūkst skaidrības par jauno regulējumu, un pieejamība datu subjektiem, organizācijām un datu aizsardzības iestādēm ir apgrūtināta. Skaidrības trūkst arī izmantotajā valodā. Tāpēc DG29 mudina Komisiju padarīt minētās lietas skaidras un saprotamas abām Atlantijas okeāna pusēm.

DG29 ierosina iekļaut atsevišķu pielikumu, kurā definēti galvenie termini, kas izmantoti privātuma vairoga dokumentos. Privātuma vairoga pietiekamības lēmuma uzlikto pienākumu vienota un nepārprotama izpratne ir ļoti svarīga tā efektīvai darbībai abās Atlantijas okeāna pusēs, un DG29 ir nobažījusies, ka saistībā ar daudzajām mijnorādēm un nesaskaņotajiem formulējumiem, kā arī pamatdokumentu sarežģītību radīsies grūtības ar privātuma vairoga īstenošanas konsekvenci, saprotamību un skaidrību.

Vēl būtiskāks ir fakts, ka privātuma vairoga dokumentos ir izmantota terminoloģija, kas neatbilst vārdu krājumam, ko ES parasti izmanto saistībā ar datu aizsardzību. Tas nesagādātu problēmas, ja vien ir skaidrs, kāda ir atbilstošā terminoloģija ES tiesību aktos (un ASV tiesību aktos). Taču DG29 norāda, ka tas nav skaidrs, tostarp arī pietiekamības lēmuma projektā. Piemēram, vārds „piekļuve" pietiekamības lēmuma projekta 3. nodaļā ir lietots ar nozīmi, kas liecina par personas datu vākšanu, nevis atļauju kādam apskatīt jau savāktos datus. Uzņēmumu piekļuve datiem un indivīda tiesības uz piekļuvi ir divi atsevišķi jēdzieni, ko nedrīkst sajaukt.

DG29 uzsver, ka terminoloģija jāizmanto arī konsekventi visos dokumentos, tostarp pietiekamības lēmuma projektā. Šobrīd tas nav nodrošināts, piemēram, attiecībā uz jēdzieniem „apstrāde" un „personas dati". Abi ir principā labi definēti II pielikumā, bet ne konsekventi piemēroti visos dokumentos, tādējādi radot nepilnības aizsardzībā[10].[11]

DG29 atzinīgi vērtē, ka dažu lietoto terminu definīcijas ir iekļautas dokumentos, kas veido privātuma vairogu. Tomēr tas nav nodrošināts vairāku citu būtisku terminu, tostarp „pārstāvis" vai „apstrādātājs", „ar šifru kodēti dati", „anonimizēti dati" un „ES indivīds", gadījumā, kam, pēc DG29 uzskatiem, būtu vajadzīga skaidra definīcija, par kuru ASV un ES ir vienisprātis, lai vēlāk gan datu pārziņi un apstrādātāji, kas izmanto privātuma vairogu, gan uzraudzības iestādes un sabiedrība izvairītos no pārpratumiem. Vienkāršs risinājums būtu privātuma vairoga BUJ pievienot terminu glosāriju.

DG29 arī norāda uz 1. papildu principā noteikto likumīgo pamatojumu apstrādāt sensitīvus datus (II pielikuma III daļas 1. punkts) gadījumos, kad organizācijai nav jāiegūst nepārprotama piekrišana (atļauja). Šo 1. papildu principu var saprast kā skaidrojumu likumīgajam pamatojumam vākt datus ES, jo šis saraksts ir līdzīgs direktīvas 8. pantam. DG29 vēlas atgādināt, ka jebkura sensitīvu datu apstrāde (ieskaitot vākšanu un nosūtīšanu) saskaņā ar ES tiesību aktiem ir jāveic ar likumīgu pamatojumu saskaņā ar direktīvas 8. pantu. Privātuma vairogu nevar interpretēt kā šādas apstrādes alternatīva pamatojuma piedāvājumu. Piemēram, DG29 uzskata, ka ASV organizācijai nav iespējams vākt datus saskaņā ar ES tiesību aktiem, pamatojoties uz ASV darba tiesībām (skatīt II pielikuma III daļas 1. punkta a. apakšpunkta v. punktu). Tāpēc DG29 uzsver, ka 1. papildu principa interpretācija var

[10] Dažas klauzulas tikai uzskaita dažus datu apstrādes darbību veidus, nevis izmanto terminu „apstrāde". Tā rezultātā rodas nepilnības aizsardzībā. Piemēram, saskaņā ar II pielikuma III daļas 6. punkta f. apakšpunktu formulējumu privātuma vairoga principi būtu jāpiemēro tikai tad, ja organizācija „uzglabā, izmanto vai izpauž" saņemtos datus (t.i., ne attiecībā uz citām darbībām, uz kurām attiecas termins „apstrāde", piemēram, vākšanu, ierakstīšanu, pārveidošanu, atgūšanu, konsultēšanos un dzēšanu). Datu drošība tiktu attiecināta tikai uz personiskās informācijas „izveidi, uzturēšanu, izmantošanu vai izplatīšanu" (II pielikuma II daļas 4. punkts). Personas datu definīcija attiecas tikai uz „saņemtiem" un „ierakstītiem" datiem. Kā papildu piemēru var minēt informēšanas principu (II pielikuma II daļas 1. punkta a. apakšpunkta iv. punktā), kas nosaka, ka sertificētajai organizācijai jāinformē indivīdi par nolūkiem, kuriem tā „vāc un izmanto" datus par tiem. II pielikuma III daļas 9. punkta a. apakšpunkta 11. punkts min tikai datus, ko „nosūta" vai kam „piekļūst". Pat ja šķiet, ka lielākajā daļā šādu gadījumu mērķis nav ierobežot principu darbības jomu vai radīt aizsardzības nepilnības, šāda nekonsekventa terminoloģija rada šādu nepilnību rašanās risku. Termins „apstrāde" ir definēts principos, tāpēc ir ļoti svarīgi izmantot to konsekventi, lai izvairītos no pastāvošajām nepilnībām. Pretējā gadījumā pastāv pārāk liela neplānotas interpretācijas iespēja, kas citādi varētu radīt nepareizu lēmuma formulējuma interpretāciju.

[11] II pielikuma I daļas 8. punkta a. apakšpunktā iekļautā „personas datu" definīcija attiecas uz „datiem par identificētu vai identificējamu indivīdu". Taču papildu princips norāda, ka saistībā ar cilvēkresursu datiem principi ir piemērojami, tikai „nosūtot identificētus datus vai piekļūstot tiem". DG29 uzskata, ka tas paver iespēju apstrādāt personas datus tādā veidā, kas nav saderīgs ne ar ES tiesību aktos noteiktajiem datu aizsardzības principiem, ne ar personas datu vispārējo definīciju saskaņā ar privātuma vairogu.

novest tikai pie tā piemērošanas sensitīviem datiem, kas jau ir nosūtīti pēc tam, kad tie ir savākti ES ar likumīgu pamatojumu, kas minēts Direktīvas 8. pantā.

Visbeidzot, DG29 min skaidrības trūkumu attiecībā uz jautājumu, ko var uzskatīt par ES indivīdu, kurš tādējādi gūst labumu no privātuma vairoga sniegtās aizsardzības: visi ES pilsoņi vai visas personas, kas dzīvo ES. Tas ir īpaši svarīgi attiecībā uz tiesībām uz tiesisko aizsardzību, tostarp piekļuvi ombuda mehānismam. Turklāt pietiekamības lēmumam būtu jārisina jautājums, cik lielā mērā privātuma vairogs attieksies arī uz EEZ un Šveices pilsoņiem / pastāvīgajiem iedzīvotājiem, uz ko iepriekš attiecās drošības zonas shēma.

1.2.3. Kopīga pārskatīšana un apturēšana

DG29 atzinīgi vērtē to, ka Eiropas Komisija un ASV valdība ir vienojušās regulāri pārskatīt privātuma vairoga praktisko piemērošanu. Šī kopīgā pārskatīšana jau vairākus gadus ir ES datu aizsardzības kopienā zināma prakse, jo īpaši attiecībā uz nolīgumiem par Pasažieru datu reģistra (PDR) datu apmaiņu ar trešajām valstīm un TFTP (Teroristu finansēšanas izsekošanas programmas) nolīgumu. DG29 arī atzinīgi vērtē to, ka kopīgajā pārskatīšanā var piedalīties nenoteikts skaits datu aizsardzības iestāžu pārstāvju.

Ņemot vērā savu pieredzi ar kopīgajiem pārskatiem pēdējo gadu laikā, DG29 vēlētos paskaidrot, ka tā sagaida, ka privātuma vairoga kopīgā pārskatīšana būs plašāka nekā PDR un TFTP kopīgie pārskati. Jo īpaši ir vēlams, lai kopīgā pārskatīšana ietvertu ne tikai tikšanās ar ASV aģentūru, organizāciju un uzņēmumu pārstāvjiem, bet arī atsevišķu privātuma vairoga elementu pārbaudes uz vietas. Datu aizsardzības iestāžu pārstāvjiem kopīgās pārskatīšanas ietvaros būtu jāspēj sniegt ieteikumus šādām pārbaudēm uz vietas.

DG29 uzskata, ka kopīgai pārskatīšanai ir nepieciešams konstatējumu kopīgs novērtējums. Līdz šim kopīgu pārskatu rezultāti ir atspoguļoti Komisijas dienestu darba dokumentā, kam nebija nepieciešams to kopīgās pārskatīšanas komandas locekļu apstiprinājums, kas nepārstāv Komisiju. DG29 augstu novērtētu, ja privātuma vairoga kopīgās pārskatīšanas gadījumā konstatējumu ziņojums tiešām būtu kopēja darba rezultāts. Varētu apsvērt arī iespēju publicēt datu aizsardzības iestāžu atsevišķu kopīgās pārskatīšanas ziņojumu.

Visbeidzot, attiecībā uz kopīgu pārskatīšanu DG29 atgādina Komisijas solījumu, ka tā atlīdzina izmaksas, kas DG29 pārstāvjiem radušās kopīgas pārskatīšanas laikā. Darba grupa pieņem, ka tas attieksies arī uz privātuma vairoga kopīgo pārskatīšanu datu aizsardzības iestāžu pārstāvju saprātīga skaita gadījumā.

DG29 iesaka, ka Komisijai, ASV valdībai un DG29 ne vēlāk kā trīs mēnešus pirms privātuma vairoga pirmās kopīgās pārskatīšanas būtu jāvienojas par kopīgās pārskatīšanas kārtību un vienošanās rezultāts jāfiksē rakstveidā.

1.2.4. ES tiesiskais regulējums, kas tiek pārskatīts

Privātuma vairoga pietiekamības lēmums ir pirmais pietiekamības lēmums, kas ir izstrādāts saskaņā ar principiālo vienošanos par Vispārīgās datu aizsardzības regulas tekstu. Tomēr

DG29 ir konstatējusi, ka privātuma vairogs vēl neatspoguļo turpmāko situāciju. Piemēram, privātuma vairogā nav iekļauti tādi nozīmīgi jauni jēdzieni kā tiesības uz datu pārnešanu un datu pārziņu papildu pienākumi, tostarp nepieciešamība veikt datu aizsardzības ietekmes novērtējumus un ievērot integrētas privātuma aizsardzības un privātuma noklusējuma principus. Tāpēc DG29 vēlētos ieteikt, ka privātuma vairogs, kā jebkurš esošais pietiekamības lēmums, tiek pārskatīts neilgi pēc VDAR (Vispārīgo datu aizsardzības regulas) stāšanās spēkā. Galīgajā pietiekamības lēmumā būtu vēlama skaidra norāde uz šo pārskatīšanas procesu.

2. PIETIEKAMĪBAS LĒMUMA PROJEKTA KOMERCIĀLĀS DAĻAS VĒRTĒJUMS

2.1. Vispārīgas piezīmes

2.1.1. Uzlabojumi

DG29 atzinīgi vērtē privātuma vairoga ieviestos uzlabojumus un sarunu dalībnieku vēlēšanos mēģināt risināt drošības zonas nepilnības, kuras darba grupa bija norādījusi. Salīdzinot ar drošības zonu, uzlabojumi jo īpaši vērojami saistībā ar šādiem elementiem: dažu galveno definīciju, piemēram, „personas dati", „apstrāde" un „pārzinis", iekļaušana, mehānismi, kas izveidoti, lai nodrošinātu privātuma vairoga saraksta uzraudzību, un ārējās vai iekšējās atbilstības pārbaudes, kas tagad ir obligātas. Uzlabojumi veikti arī piekļuves principā, un DG29 atzīmē, ka labošanas un dzēšanas tiesības tagad tiek nodrošinātas gadījumā, ja dati tiek izmantoti tādā veidā, kas neatbilst privātuma vairoga principiem. Turklāt tagad ir skaidrs, ka indivīdam ir jāsaņem gan apstiprinājums, ka dati par viņu tiek apstrādāti, gan informācija par apstrādātajiem datiem.

DG29 atzinīgi vērtē arī pastiprinātās tiesiskās garantijas tālākas nosūtīšanas gadījumos un ASV Tirdzniecības ministrijas un Federālā tirdzniecības komisijas (FTK) apņemšanos izpildīt privātuma vairoga noteiktās saistības.

2.1.2. Privātuma vairoga piemērošana organizācijām, kas darbojas kā apstrādātājs (pārstāvis)

Diemžēl joprojām nav skaidrs, kādā mērā privātuma vairoga principi ir piemērojami sertificētām organizācijām, kas saņem personas datus no ES tikai apstrādes nolūkiem („pārstāvji" vai „apstrādātāji"). Lai gan II pielikuma III daļas 10. punkta a. apakšpunkta noteikumos ir minēta datu nosūtīšana sertificētām organizācijām šādiem nolūkiem — proti, minot prasību noslēgt līgumu —, noteikumos trūkst norādes par to, kā privātuma vairoga principi attiecas uz apstrādātājiem (pārstāvjiem). Tas rada neskaidrības gan sertificētajām ASV organizācijām, kas saņem datus apstrādes nolūkiem, gan ES uzņēmumiem, kas nosūta datus sertificētām organizācijām, kas darbojas kā datu apstrādātāji, gan indivīdiem, kuru dati tiek apstrādāti. Līdz ar to būs grūti noteikt, kuri pienākumi faktiski attiecas uz vairoga organizācijām, kas apstrādā no ES saņemtos personas datus, kā apstrādātājiem. Tāpēc noteikti ir nepieciešams skaidrojums.

Jāņem vērā, ka vairākas principos iekļautās saistības nav piemērotas datu apstrādātājiem, jo datu apstrādes veidus un nolūkus vienmēr nosaka datu pārzinis (sk. definīciju „pārzinis" II pielikuma I daļas 8. punkta c. apakšpunktā). Tieši šī iemesla dēļ dažas principos iekļautās saistības, ja tās piemēro organizācijai, kas rīkojas kā pārstāvis, var būt pretrunā ar datu apstrādes līgumu, ko pieprasa ES tiesību akti (līgumu, kas minēts II pielikuma III daļas 10. punkta a. apakšpunktā). Piemēram, datu apstrādes līgums parasti neatļauj datu apstrādātājam (pārstāvim) tālāk nosūtīt datus pārzinim, kas ir trešā persona, pat II pielikuma II daļas 3. punkta a. apakšpunktā minētajos apstākļos. Tālāku nosūtīšanu pārstāvjiem, kas ir trešās personas, vajadzētu atļaut tikai pēc tam, kad saņemts apstiprinājums no datu pārziņa. Turklāt saskaņā ar ES tiesību aktu prasībām apstrādātājs (pārstāvis) nespēs pilnībā informēt indivīdus, kā to paredz informēšanas princips (II pielikuma II daļas 1. punkts), piemēram, tāpēc, ka šī organizācija nenosaka apstrādes nolūkus.

Tāpēc ir ļoti svarīgi principos precizēt, ka šādu pretrunu gadījumā noteicošie ir datu apstrādes līguma noteikumi un jo īpaši tās organizācijas norādījumi, kas sūta datus no ES. Bez šāda skaidrojuma principus varētu interpretēt un piemērot tādā veidā, kas vairoga pārstāvim sniedz pārāk daudz kontroles spējas, un tas radītu ES datu nosūtītājam risku pārkāpt savas saistības kā datu pārzinim saskaņā ar ES datu aizsardzības tiesību aktiem, kuriem tas ir pakļauts, kā pārstāvis nosūtot datus vairoga organizācijai. Turklāt šāds skaidrības trūkums rada iespaidu, ka apstrādātājs var atkārtoti izmantot datus, kā vien vēlas.

Turklāt jāparedz īpaši noteikumi gadījumam, ja organizācija darbojas kā datu apstrādātājs (pārstāvis), lai nodrošinātu, ka šī organizācija ievēro datu pārziņa norādījumus. Būtu skaidri jānosaka, ka ASV organizācijas, kas saņem datus tikai apstrādes nolūkiem, nevar izlemt apstrādāt datus savā vārdā. Ja nav īpašu noteikumu, kas piemērojami organizācijām, kas darbojas kā apstrādātāji, ir grūti noteikt, saskaņā ar kādiem noteikumiem apstrādātājs (pārstāvji) var pašsertificēties.

2.1.3. Ierobežojumi attiecībā uz pienākumu ievērot principus

II pielikuma I daļas 5. punkts, cita starpā, paredz atbrīvojumus no principiem, ja datus, uz kuriem attiecas privātuma vairogs, izmanto nacionālās drošības[12], sabiedrības interešu, tiesībaizsardzības interesēs vai saskaņā ar likumu, valdības noteikumiem vai tiesu praksi, kas rada pretrunīgas saistības vai skaidras atļaujas. Nepārzinot ASV federālā un štata līmeņa likumus pilnībā, DG29 ir grūti novērtēt šā atbrīvojuma darbības jomu un noteikt, vai šie ierobežojumi ir attaisnojami demokrātiskā sabiedrībā. Būtu svarīgi, lai Eiropas Komisija savā pietiekamības lēmuma projektā ietver analīzi par aizsardzības līmeni gadījumā, ja tiek piemēroti šie atbrīvojumi. DG29 aicina Komisiju nodrošināt, ka ES tiek informēta par jebkuru likumu vai valdības noteikumiem, kas ietekmē principu ievērošanu un tiek piemēroti tobrīd vai brīdī, kad jaunie likumi vai noteikumi stājas spēkā ASV.

[12] Trešajā nodaļā ir pieejams detalizētāks komentārs par privātuma vairoga aizsargāto personas datu izmantošanu nacionālās drošības nolūkos, savukārt ceturtajā nodaļā — par šādu datu izmantošanu tiesībaizsardzības nolūkos.

2.1.4. Datu saglabāšanas ierobežojuma principa neesamība

Datu saglabāšanas ierobežojuma princips (Direktīvas 6. panta 1. punkta e) apakšpunkts) ir ES datu aizsardzības tiesību aktu pamatprincips, kas nosaka, ka personas dati ir jāglabā tikai tik ilgi, cik nepieciešams, lai sasniegtu mērķi, kuram šie dati ir savākti vai kuram tos tālāk apstrādā.

Tomēr dokumentos, kas veido privātuma vairogu, DG29 nevar atrast nekādas atsauces uz nepieciešamību datu pārziņiem nodrošināt, ka dati tiek izdzēsti, kad nolūks, kuram tie tika vākti vai tālāk apstrādāti, ir novecojis. Līdz ar to šķiet, ka principi nerada sertificētajām organizācijām ierobežojumu attiecībā uz datu saglabāšanas periodu, kas būtu pielīdzināms tam, ko rada datu saglabāšanas ierobežojuma princips ES tiesību aktos.

Nekādā gadījumā nevar uzskatīt, ka datu integritātes un nolūka ierobežojuma principa formulējums (II pielikuma II daļas 5. punkts) rada pienākumu organizācijai, kas darbojas kā pārzinis, dzēst datus, kad tie vairs nav nepieciešami nolūkiem, kuriem dati tika savākti vai tālāk apstrādāti, vai organizācijai, kas darbojas kā apstrādātājs, dzēst datus pēc pakalpojuma nolīguma izbeigšanas.

Darba grupa uzsver, ka tādu noteikumu neesamība, kas ievieš ierobežojumu attiecībā uz datu saglabāšanu saskaņā ar privātuma vairogu, dod organizācijām iespēju uzglabāt informāciju, cik vien ilgi tās vēlas, pat pēc izstāšanās no privātuma vairoga, kas nesaskan ar būtisko datu saglabāšanas ierobežojuma principu.

2.1.5. Garantiju trūkums attiecībā uz automatizētiem lēmumiem, kas rada tiesiskas sekas vai būtiski ietekmē indivīdu

Privātuma vairogs nesniedz tiesiskās garantijas gadījumos, kad indivīdi ir pakļauti lēmumam, kas rada tiesiskas sekas attiecībā uz šiem indivīdiem vai nozīmīgi iespaido tos un kas balstās tikai un vienīgi uz datu automatizētu apstrādi, kas paredzēta uz šo indivīdu attiecināmu zināmu personisku aspektu, tādu kā darba izpildes, kredītspējas, uzticamības, uzvedības, utt. novērtējumam.

DG29 savā 12. darba dokumentā jau ir uzsvērusi nepieciešamību nodrošināt tiesiskās garantijas attiecībā uz automatizētiem lēmumiem (kas rada tiesiskas sekas vai būtiski ietekmē indivīdu**),** lai nodrošinātu atbilstošu aizsardzības līmeni.

Šī nepieciešamība kļūst arvien svarīgāka, jo jaunās tehnoloģijas nepārtraukti attīstās, ļaujot lielākam skaitam uzņēmumu apsvērt automatizētu lēmumu pieņemšanas sistēmu ieviešanu, kas var pasliktināt indivīdu pozīciju, atstājot tos bez tiesiskās aizsardzības pret datoru pieņemtajiem lēmumiem. Situācijās, kad automatizēto sistēmu pieņemtie lēmumi ietekmē indivīdu tiesisko situāciju vai būtiski ietekmē tos (piemēram, pievienojot tos melnajam sarakstam un tādējādi liedzot indivīdiem viņu tiesības), ir ļoti svarīgi nodrošināt pietiekamas garantijas, tostarp tiesības iepazīties ar iesaistīto loģiku un pieprasīt lēmuma pārskatīšanu neautomatizētā veidā.

2.1.6. Pārejas periods esošajām komercattiecībām

Privātuma vairogs paredz, ka principi jāpiemēro uzreiz pēc sertifikācijas. Tomēr organizācijām, kas sertificēsies pirmajos divos mēnešos pēc privātuma vairoga regulējuma spēkā stāšanās dienas, būs iespējami drīz jānodrošina, lai visas esošās komercattiecības ar trešajām personām atbilstu atbildības par tālāku nosūtīšanu principam. Jebkurā gadījumā tas ir jāizdara ne vēlāk kā deviņu mēnešu laikā no datuma, kurā tās sertificēja privātuma vairoga ievērošanu.

Tas nozīmē, ka esošie līgumi, ciktāl tas vajadzīgs, ir jāsaskaņo ar principiem 2–9 mēnešu laikā pēc sertifikācijas. Šajā pārejas periodā pietiek ar informēšanas un izvēles principu. DG29 uzstāj, ka datus var nosūtīt, pamatojoties uz privātuma vairogu, tikai no brīža, kad organizācija pilnībā atbilst visām vairoga prasībām. Iespēju nosūtīt datus pārejas periodā, kad saņēmējs pilnībā neatbilst vairoga principiem, nevar uzskatīt par atbilstošu likumīgas nosūtīšanas nosacījumiem, tāpēc šāda iespēja nav pieņemama.

2.2. Īpašas piezīmes

2.2.1. Pārredzamība

a) Vispārīgas piezīmes par informēšanas principu

DG29 atzinīgi vērtē visaptverošākas un detalizētākas prasības, kas noteiktas informēšanas principā, jo īpaši to, ka paziņojumā būs jāiekļauj saite uz privātuma vairoga sarakstu vai tā tīmekļa adrese un jāsniedz informācija par indivīdu piekļuves tiesībām un alternatīviem strīdu izšķiršanas mehānismiem[13]. Tomēr DG29 iesaka sīkāk paskaidrot citas tiesības (labot, dzēst, ja dati ir neprecīzi vai apstrādāti, neievērojot principus).

Dokumenti, kas veido privātuma vairogu, rada bažas par laiku, kad privātuma vairoga organizācijai ir jānosūta paziņojums indivīdam. II pielikuma II daļas 1. punkta b. apakšpunkts nosaka, ka „paziņojums jāsniedz (...), kad indivīdus pirmo reizi lūdz sniegt personisko informāciju organizācijai vai cik drīz vien iespējams pēc tam, bet jebkurā gadījumā pirms organizācija šādu informāciju izmanto citiem nolūkiem, izņemot tos, kuriem nosūtītāja organizācija to sākotnēji ievākusi vai apstrādājusi, vai to pirmo reizi izpaudusi trešajai personai". DG29 uzskata, ka daudzās situācijas ASV vairoga organizācijas neievāks datus tieši no datu subjekta, tāpēc paziņojums ir jānosūta brīdī, kad vairoga organizācija reģistrē datus.

DG29 norāda, ka informēšanas principa un privātuma politikas prasību faktiskā īstenošana ir jānovērtē privātuma vairoga pirmajā gada pārskatā.

b) Privātuma politikas publiskā pieejamība

[13] II pielikums, II daļas 1. punkts; DG29 arī atsaucas uz Komisijas otro ieteikumu Paziņojumā COM(2103)847, kā arī DG29 2041. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), jo īpaši sadaļas „Pārredzamība" 4. punktu.

DG29 atzinīgi vērtē to, ka tagad ir skaidrs, ka ASV Tirdzniecības ministrija pārbaudīs, vai uzņēmumi, kam ir publiskas tīmekļa vietnes, tajās ir publicējuši savu privātuma politiku, vai kā sabiedrība tiek informēta par privātuma politiku gadījumā, ja uzņēmumiem nav publisku tīmekļa vietņu[14].

c) Ar apstrādātājiem noslēgto līgumu privātuma nosacījumu publicēšana

Nosacījumos, saskaņā ar kuriem privātuma vairoga organizācijas var nosūtīt datus apstrādātājam (pārstāvim), privātuma vairogs nosaka pašsertificētu organizāciju pienākumu „pēc ministrijas pieprasījuma iesniegt tai ar konkrēto pārstāvi noslēgtā līguma attiecīgo privātuma noteikumu kopsavilkumu vai reprezentatīvu kopiju" (skatīt II pielikuma II daļas 3. punkta b. apakšpunkta v. punktu). Darba grupa atzinīgi vērtē šo pārredzamības prasību attiecībā uz ASV Tirdzniecības ministriju.

2.2.2. Izvēle

Privātuma vairogs paredz tiesības atteikties no personiskās informācijas izpaušanas trešajai personai vai personiskās informācijas izmantošanas būtiski atšķirīgam nolūkam[15] (II pielikuma III daļas 2. punkts). Turklāt indivīdiem ir tiesības jebkurā laikā atteikties no personiskās informācijas izmantošanas tiešā mārketinga nolūkos (II pielikuma III daļas 12. punkta a. apakšpunkts)[16].

Izņemot tiešā mārketinga nolūka kontekstu, nav sniegta detalizēta informācija par veidu, kādā šo atteikumu var īstenot, un brīdi, kad to var darīt. DG29 uzskata, ka vienkārša atsauce uz šādu tiesību esamību privātuma politikā var nebūt pietiekama, bet *pirms* personiskās informācijas izpaušanas vai atkalizmantošanas būtu jāsniedz *individualizēta* iespēja izmantot šīs tiesības.

Turklāt DG29 uzsver, ka privātuma vairoga ietvaros būtu jāpiedāvā vispārējas tiesības iebilst (ar pārliecinošu pamatojumu, kas saistīts ar datu subjekta konkrēto situāciju), izprotot tās kā tiesības lūgt izbeigt savu datu apstrādi, kad indivīdam ir pārliecinošs, likumīgs pamatojums, kas saistīts ar viņa konkrēto situāciju[17]. DG29 iesaka pietiekamības lēmuma projektā precizēt, ka tiesībām iebilst vajadzētu pastāvēt jebkurā brīdī un ka šis iebildums nav attiecināms tikai uz datu izmantošanu tiešajam mārketingam[18].

DG29 pauž bažas, ka definīcijas neesamība par to, kas ir uzskatāms par "būtiski atšķirīgu" nolūku, radīs apjukumu un tiesisko nenoteiktību. Jāprecizē, ka izvēles principu nekādā gadījumā nevar izmantot, lai apietu nolūka ierobežojuma principu[19]. Izvēles princips būtu jāpiemēro tikai tad, ja nolūks ir būtiski atšķirīgs, bet atbilstīgs, jo apstrāde neatbilstīgā nolūkā

[14] Skatīt Eiropas Komisija pirmo ieteikumu Paziņojumā COM(2013)847 un DG29 2014. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), jo īpaši sadaļas „Pārredzamība" 3. punktu.

[15] Papildu principa 14. punkta c. apakšpunkta I. punkts paredz tiesības pārtraukt dalību klīniskajā izpētē, ko varētu uzskatīt par tiesībām iebilst vai atsaukt piekrišanu.

[16] Tās ir identiskas drošības zonas shēmā sniegtajām (BUJ 12. punkts), un šajā sakarā nav veiktas izmaiņas.

[18] Skatīt DG29 vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), sadaļu "Izvēle".

[19] Konkrēts piemērs par neatbilstīgu tālāku apstrādi, kas atļauta saskaņā ar izvēles principu, ir sniegts papildu principa 9. punkta b. apakšpunkta i. punktā (skatīt DG29 komentāru par to punktā, kas saistīts ar „personāla datiem").

ir aizliegta (II pielikuma II daļas 5. punkta a. apakšpunkts). Jāprecizē, ka atteikšanās tiesības nevar ļaut organizācijai izmantot datus neatbilstīgiem mērķiem. Tāpēc darba grupa iesaka saskaņot saistīto formulējumu, izmantojot vienu definētu formulējumu (piemēram, „būtiski atšķirīgs, tomēr atbilstīgs nolūks").

Noderētu skaidrojums, kādā gadījumā uz lēmumu, kas pieņemts, lai apstrādātu datus citā nolūkā vai izpaustu informāciju, attiecas ES tiesību akti. Šādā situācijā ES parastie juridiskie nosacījumi attiecībā uz šo apstrādi (piemēram, aizliegums apstrādāt datus neatbilstīgiem mērķiem, nosacījums nodrošināt apstrādes likumīgu pamatojumu un nepieciešamība informēt indivīdu) būs tieši piemērojami arī ASV organizācijai, uz kuru attiecas ES tiesību akti. Praksē tas nozīmē, ka apstrādes pārredzamība un likumība saskaņā ar ES tiesību aktiem būs jānodrošina ES datu nosūtītājam, kas pieņem šādu lēmumu. Tāpēc izvēles principu piemēros tikai tad, ja lēmumu pieņem tikai ASV vairoga organizācija, uz kuru neattiecas ES tiesību akti.

2.2.3. Tālāka nosūtīšana

a) Darbības joma

DG29 pauž bažas par situāciju, kad privātuma vairoga sertificēta organizācija, kas atrodas ASV, nosūta personas datus saņēmējam trešajā valstī.

Vairogu nevajadzētu uztvert tikai kā rīku ES datu nosūtīšanai no ES uz ASV, bet arī kā rīku, ko izmantot datu nosūtīšanai no ASV uz trešajām valstīm. Tāpēc noteikumi par tālāku nosūtīšanu ir svarīgs vairoga elements, kam būtu jāsniedz pietiekamas garantijas un atbilstošs aizsardzības līmenis, ja dati tiek tālāk nosūtīti ārpus ASV. Viens problēmjautājums ir saistīts ar nacionālo drošību un tiesībaizsardzību.

Privātuma vairoga princips par atbildību par tālāku nosūtīšanu attiecas ne tikai uz datu pārziņiem-saņēmējiem, apstrādātājiem un pārstāvjiem, kas reģistrēti ASV. Tāpēc datus var tālāk nosūtīt uz trešo valsti, pamatojoties uz privātuma vairogu, pat tad ja šīs trešās valsts likumi paredz publisku piekļuvi personas datiem, piemēram, uzraudzības nolūkos. Tas rada risku, ka attiecībā uz ES datiem var notikt nepamatota iejaukšanās pamattiesību aizsardzībā.

Ja dati tiek tālāk nosūtīti uz trešo valsti, ikvienai privātuma vairoga organizācijai jābūt pienākumam pirms nosūtīšanas izvērtēt konkrētās trešās valsts tiesību aktos ietvertās obligātās prasības, kas piemērojamas datu saņēmējam. Ja tiek identificēts risks, ka pastāv būtiska negatīva ietekme uz privātuma vairoga noteiktajām garantijām, saistībām un aizsardzības līmeni, ASV privātuma vairoga organizācija, kas darbojas kā apstrādātājs (pārstāvis), pirms jebkuras tālākas nosūtīšanas nekavējoties informē ES datu pārzini. Šajos gadījumos datu nosūtītājs ir tiesīgs apturēt datu nosūtīšanu un/vai izbeigt līgumu. Ja pastāv šāds būtiskas negatīvas ietekmes risks, vairoga organizācijai, kas darbojas kā pārzinis, nevajadzētu ļaut tālāk nosūtīt datus, jo tas apdraudētu tās pienākumu nodrošināt tādu pašu aizsardzības līmeni kāds noteikts saskaņā ar principiem tālākas nosūtīšanas gadījumā (skatīt II pielikuma II daļas 3. punkta a. apakšpunktu).

Tāpat, ja trešās valsts tiesību aktos tiek ieviestas izmaiņas, kam varētu būt būtiska negatīva ietekme uz privātuma vairoga noteiktajām garantijām, saistībām un aizsardzības līmeni, ASV privātuma vairoga organizācijai, kas darbojas kā apstrādātājs (pārstāvis), ir jānosaka pienākums (privātuma vairogā) nekavējoties paziņot par šīm izmaiņām datu nosūtītājam, tiklīdz organizācija uzzina par izmaiņām, un šādā gadījumā datu nosūtītājam ir tiesības apturēt datu nosūtīšanu un/vai izbeigt līgumu. Attiecīgi šādā gadījumā vairoga organizācijai, kas darbojas kā pārzinis, nevajadzētu ļaut tālāk nosūtīt datus, jo tai ir pienākums nodrošināt tādu pašu aizsardzības līmeni kāds noteikts saskaņā ar principiem (skatīt II pielikuma II daļas 3. punkta a. apakšpunktu).

DG29 atgādina savu viedokli, ka gadījumā, ja ES datu pārzinis zina par tālāku nosūtīšanu trešajai personai ārpus ASV vēl pirms datu nosūtīšanas uz ASV, vai gadījumā, ja ES datu pārzinis ir līdzatbildīgs par lēmumu atļaut tālāku nosūtīšanu, datu nosūtīšana ir jāuzskata par tiešu nosūtīšanu no ES uz trešo valsti ārpus ASV. Tas nozīmē, ka nosūtīšanai ir piemērojams Direktīvas 25. un 26. pants, nevis privātuma vairoga tālākas nosūtīšanas princips.

b) Datu nosūtīšana no privātuma vairoga organizācijas pārzinim, kas ir trešā persona

DG29 atzinīgi vērtē pienākumu ieviest līgumus (II pielikuma II daļas 3. punkta a. apakšpunkts), lai nodrošinātu, ka pārzinis, kurš ir trešā persona, sniegs vismaz tāda paša līmeņa privātuma aizsardzību, kā to pieprasa privātuma vairoga principi. Tā mērķis ir nodrošināt, ka personas dati arī turpmāk tiek pienācīgi aizsargāti pat pēc to nosūtīšanas tālāk. Tomēr DG29 ir dažas piezīmes par ierosinātajiem nosacījumiem.

Atsauču uz nolūka ierobežojuma principu trūkums

DG29 iesaka ietvert skaidru atsauci uz nolūka ierobežojuma principu (II pielikuma II daļas 5. punkts) nosacījumos par tālāku nosūtīšanu pārzinim, kurš ir trešā persona (II pielikuma II daļas 3. punkta a. apakšpunkts). Tādā gadījumā būtu skaidrs, ka tālāka nosūtīšana nevar notikt, ja pārzinis, kurš ir trešā persona, apstrādās datus neatbilstīgam nolūkam.

Atbrīvojums no prasības slēgt līgumu, ja dati tiek pārsūtīti pārziņu starpā grupas līmenī

Atbrīvojums no prasības slēgt līgumu tiek piešķirts, ja dati tiek pārsūtīti pārziņu starpā grupas līmenī. Šādā gadījumā principi paredz, ka aizsardzības nepārtrauktību varētu piedāvāt saistoši uzņēmuma noteikumi (BCR) vai „citi grupas līmeņa instrumenti (piemēram, atbilstības un kontroles programmas)" (II pielikuma III daļas 10. punkta b. apakšpunkts). DG29 uzskata, ka atsauce uz „citiem grupas līmeņa instrumentiem" negarantē citu grupas dalībnieku juridiski saistošas saistības. DG29 un ES tiesību akti[20] grupas līmeņa nosūtīšanas regulēšanai kopumā dod priekšroku saistošām saistībām, tāpēc ir svarīgi novērst privātuma vairoga izmantošanu tādā veidā, kas apietu šo prasību. DG29 atgādina, ka jebkurā gadījumā tālāka nosūtīšana no ASV uz trešajām valstīm, kas ieplānota pirms datu nosūtīšanas uz ASV, un tālāka nosūtīšana,

[20] Saistošu un izpildāmu saistību nepieciešamība ir uzsvērta arī Vispārīgo datu aizsardzības regulā (VDAR), neatkarīgi no izmantotā instrumenta (BCR, līguma klauzulām, rīcības kodeksiem vai sertifikācijas).

ko pārzina kopā ar ES datu pārzini[21], ir jāuzskata par tiešu nosūtīšanu no ES uz trešo valsti ārpus ASV. Tāpēc nosūtīšanai ir piemērojams Direktīvas 25. un 26. pants.

c) Datu nosūtīšana no privātuma vairoga organizācijas apstrādātājam (pārstāvim), kas ir trešā persona

DG29 atzinīgi vērtē to, ka līgums par tālāku nosūtīšanu tagad ir obligāta prasība saņēmējiem, kas darbojas kā apstrādātāji (pārstāvji), neatkarīgi no to līdzdalības privātuma vairogā un tā, vai saņēmēji gūst labumu no cita risinājuma atbilstības konstatēšanai. DG29 atzinīgi vērtē arī papildu drošības pasākumus, kas regulē tālāku nosūtīšanu (II pielikuma II daļas 3. punkta a. apakšpunkta i. punkts; II daļas 3. punkta a. apakšpunkta iii. punkts; II daļas 3. punkta a. apakšpunkta iv. punkts; II daļas 3. punkta a. apakšpunkta v. punkts; II daļas 7. punkta d. apakšpunkts). Pēdējais apakšpunkts (II pielikuma II daļas 7. punkta d. apakšpunkts) attiecas uz pienākumu saglabāt atbildību, kad dati tiek izpausti pārstāvim. Tomēr šķiet, ka šī garantija neattieksies uz gadījumu, ja organizācija ir izvēlējusies sadarboties ar datu aizsardzības iestādi (skatīt II pielikuma III daļas 5. punkta a. apakšpunkta beigas). DG29 nesaprot šāda izņēmuma pamatojumu un uzskata, ka atbildība būtu jāpiemēro arī šajā gadījumā.

Atsauču uz nolūka ierobežojuma principu trūkums

DG29 norāda, ka atbildības par tālāku nosūtīšanu princips (II pielikuma II daļas 3. punkts) skaidro, ka personas datus var nodot trešajai personai, kas rīkojas kā pārstāvis, tikai ierobežotiem un noteiktiem nolūkiem, bet skaidri nenosaka, ka šiem ierobežotajiem un noteiktajiem nolūkiem ir jāatbilst sākotnējiem nolūkiem, kuriem dati tika vākti, un pārziņa norādījumiem. Šajā jautājumā ir nepieciešams skaidrāks formulējums. Tāpēc DG29 iesaka nodrošināt, ka pietiekamības lēmumā ir sniegta sīkāka informācija, piemēram, ietverot skaidru atsauci uz nolūka ierobežojuma principu (II pielikuma II daļas 5. punktu), saskaņā ar kuru datus nedrīkst apstrādāt (tostarp izpaustos) nolūkiem, kas neatbilst tālākas nosūtīšanas principā (papildus atteikšanās principam) noteiktajiem nolūkiem.

Nepieciešamība noteikt vairāk papildu saistību privātuma vairoga organizācijām, kas darbojas kā tādu datu apstrādātājs (pārstāvis), kad dati tiek tālāk nosūtīti citam apstrādātājam (pārstāvim)

Skaidru noteikumu neesamība gadījumiem, kad vairoga organizācija, kas darbojas kā pārstāvis (proti, ES pārziņa vārdā), ir nepilnība, kas varētu neļaut ES pārzinim saglabāt kontroli. Vairoga organizācijai, kas saņem datus kā ES pārziņa pārstāvis, ir jāievēro ES pārziņa norādījumi. Tas būtu skaidri jānorāda principos, lai nodrošinātu, ka šo norādījumu neievērošana novedīs ne tikai pie līguma laušanas (II pielikuma III daļas 10. punkta a. apakšpunkta ii. punkts), bet arī pie privātuma vairoga principu pārkāpšanas.

Ir jānodrošina, lai vairoga organizācijas-pārstāvja iespēja nosūtīt datus pārstāvim, kas ir trešā persona, būtu pārzinim pārredzama un lai pārzinim šāda nosūtīšana būtu jāapstiprina pirms tās veikšanas. Tāpēc būtu skaidri jānorāda, ka to, vai tālāku nosūtīšanu drīkst veikt, nosaka

[21] Piemēram, personāla datiem.

līgums, ko pārstāvis parakstījis ar ES pārzini (BUJ 10. punktā minēts kā „17. panta līgums")[22].

Pašreizējie nosacījumi, ko piemēro tālākai nosūtīšanai pārstāvim, balstās uz pieņēmumu, ka vairoga organizācija darbojas kā pārzinis, un tāpēc tā pati var lemt par pārstāvja, kas ir trešā persona, iespējamo iejaukšanos. Tomēr to nevajadzētu pieļaut situācijā, kad vairoga organizācija darbojas kā pārstāvis. Pretējā gadījumā ES pārzinim tiks atņemtas tā kontroles spējas.

Attiecīgajiem privātuma noteikumiem, kas ietveri līgumā, kas noslēgts ar pārstāvi, kas ir trešā persona, ir jābūt pieejamiem pārzinim, un tiem ir jānodrošina vismaz tāds pats aizsardzības līmenis, kādu nodrošina līgums, kas parakstīts ar pārzini.

2.2.4. Datu integritāte un nolūka ierobežojums

a) Samērīgums

Mazāk būtiskā aspektā DG29 atsaucas uz savu vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), kurā grupa rakstīja, ka „personas datu apstrāde, pat strikti ievērojot informēšanas un izvēles principus, var nebūt samērīga attiecībā uz datu subjekta vai sabiedrības interesēm, tiesībām un brīvībām. Samērīguma un saprātīguma princips ir jāievēro visos apstrādes posmos un jāpiemēro papildus informēšanas un izvēles principiem."[23]

Privātuma vairogs (II pielikuma II daļas 5. punkta a. apakšpunkts) nosaka, ka informācijai ir jāaprobežojas ar to, kas ir būtiski apstrādei. DG29 atzītu par labāku, ja šis formulējums tiktu labots galīgajā atbilstības lēmumā, jo fakts, ka šiem datiem jābūt saistītiem ar apstrādi, nav pietiekams, lai padarītu apstrādi samērīgu. Lai nodrošinātu atbilstību proporcionalitātes principam, apstrādei būtu jāaprobežojas ar datiem, kas nepieciešami konkrētajai apstrādei.

b) Pareizība

Datu integritātes un nolūka ierobežojuma princips (II pielikuma II daļas 5. punkts) arī nosaka: „Ciktāl tas ir vajadzīgs šiem mērķiem, organizācijai jāveic samērīgi pasākumi, lai nodrošinātu, ka personas dati saistībā ar paredzēto mērķi ir ticami, precīzi, pilnīgi un aktuāli." DG29 norāda, ka šis ir tieši tāds pats formulējums, kāds izmantots drošības zonas shēmā. DG29 šaubās par to, vai formulējums „ciktāl tas ir vajadzīgs šiem mērķiem" ir jāiekļauj, jo datu precizitātei, pēc grupas domām, nevajadzētu būt atkarīgai no apstrādes nolūka. DG29 atzītu par labāku, ja galīgajā pietiekamības lēmumā nebūtu šādas sakarības.

c) Nolūka ierobežojums

Ja personas datus ASV organizācijai nosūta datu pārzinis, kas reģistrēts ES, datu nosūtītājam ir skaidri jāinformē ASV organizācija par nolūkiem, kuriem dati tika sākotnēji savākti. Tas ir

[22] Skatīt DG29 2014. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), sadaļas „Tālāka nosūtīšana" 4. punktu.
[23] Skatīt DG29 2014. gada 10. aprīļa vēstules priekšsēdētāja vietniecei Redingai (*Reding*) 8. punktu.

būtiski, lai noteiktu, vai pēc nosūtīšanas nolūks mainās, tādējādi uzsākot informēšanas un izvēles principa piemērošanu un veicinātu risku un atbildību sadali.

Datu integritātes un nolūka ierobežojuma princips (II pielikuma II daļas 5. punkts) nosaka, ka organizācija nevar apstrādāt personisko informāciju tādā veidā, kas neatbilst nolūkiem, kuriem tā ir savākta vai ko indivīds vēlāk apstiprinājis. Taču izvēles princips (II pielikuma II daļas 2. punkts) paredz atļauju sensitīvas informācijas (proti, personiskās informācijas par veselības stāvokli, rasi vai etnisko izcelsmi, politiskajiem uzskatiem, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās vai informācija par indivīda dzimumdzīvi, kā arī datu par sodāmību) lietošanai nolūkos, kas būtiski atšķiras no tiem nolūkiem, kuriem dati sākotnēji tika savākti vai ko indivīds vēlāk apstiprinājis. Šāda atļauja nav nepieciešama situācijās, kas minēta papildu principa 1. punkta a. apakšpunktā (II pielikuma III daļas 1. punkta a. apakšpunktā). Attiecībā uz nesensitīvu personisko informāciju ir noteikts atteikšanās režīms.

DG29 norāda, ka nolūka ierobežojuma principa darbības joma atšķiras informēšanas, izvēles un datu integritātes un nolūka ierobežojuma principu ietvaros. Faktiski termini „neatbilstīgs nolūks" un „būtiski atšķirīgs nolūks" tiek izmantoti vienā un tajā pašā tekstā bez abu šo jēdzienu skaidras definīcijas[24].

DG29 ir nopietnas bažas par to, ka šāda nekonsekvence var ļoti apgrūtināt datu integritātes un nolūka ierobežojuma principa (II pielikuma II daļas 5. punkts) saskaņošanu ar izvēles principu (II pielikuma II daļas 2. punkts), jo viens nosaka, ka datus nevar apstrādāt tādā veidā, kas neatbilst nolūkiem, kuriem tie tika savākti, savukārt otrs paredz atteikšanās mehānismu gadījumā, ja dati tiek apstrādāti nolūkam, kas būtiski atšķiras no sākotnējā nolūka.

Tādējādi var interpretēt, ka izvēles princips atļauj turpmāku neatbilstīgu apstrādi[25]. Saskaņā ar DG29 viedokli ir skaidri jānorāda, ka organizācijai nav atļauts apstrādāt datus būtiski atšķirīgā nolūkā, ja tas nav atbilstīgs saskaņā ar nolūka ierobežojuma principu. Citiem vārdiem sakot, skaidri jānosaka, ka izvēles princips nav nolūka ierobežojuma principa izņēmums.

Jebkurā gadījumā, ja turpmāku apstrādi var uzskatīt par atbilstīgu, būtu jāpiemēro arī informēšanas un izvēles principi.

2.2.5. Izņēmumi attiecībā uz žurnālistiku

Personas datu apstrādes izņēmumi attiecībā uz žurnālistiku ir noteikti 2. papildu principā (II pielikuma III. daļas 2. punkts). Jāsaprot, ka šie noteikumi atspoguļo vārda brīvības konstitucionālo aizsardzību ASV. Tāpēc privātuma vairoga dokumentos ir norādīts, ka

[24] DG29 atzīmēja, ka ir izmantotas arī dažas citas frāzes: „izmantošana, kas neatbilst" (II pielikuma III daļas 14. punkta b. apakšpunkta ii. punkts), „izmantošana citos nolūkos" (II pielikuma III daļas 9. punkta B. apakšpunkta i. punkts), „izmantošana citos nolūkos, izņemot tos, kuriem tā sākotnēji savākta" (II pielikuma II daļas 1. punkta b. apakšpunkts). Šāda neskaidrība varētu izraisīt situāciju, kad attiecībā uz nolūka ierobežojuma principu nav pietiekamu garantiju.

[25] Skatīt arī komentāru sadaļā par izvēles principu. DG29 uzskata, ka fakts, ka tālākas nosūtīšanas noteikumi (II pielikuma II daļas 3. punkts) attiecas tikai uz izvēles principu, nevis uz nolūka ierobežojuma principu, palielina šādas interpretācijas risku.

„privātuma vairoga principu prasības neattiecas uz personisko informāciju, kas atrodama agrāk publicētos materiālos no plašsaziņas līdzekļu arhīviem" (II pielikuma III daļas 2. punkta b. apakšpunkts). Šķiet, ka šis atbrīvojums ietver jebkuru tālāku apstrādi, ko veic kāds datu pārzinis vai apstrādātājs, proti, ne tikai tālāku apstrādi žurnālistikas nolūkiem. Kā jau norādīts 2014. gada 10. aprīļa vēstulē priekšsēdētāja vietniecei Redingai (*Reding*), DG29 labprātāk redzētu ierobežotāku pieeju izņēmumiem attiecībā uz žurnālistiku, kas labāk atbilstu ES piemērotajam principam, kā arī tiesības uz svītrošanu no sarakstiem atbilstoši Google Spain lietai[26].

2.2.5. Datu subjektu piekļuves, labošanas un dzēšanas tiesības

Saskaņā ar privātuma vairogu indivīdiem ir tiesības saņemt *apstiprinājumu* par to, vai viņu datus apstrādā organizācija, un būt *informētiem* par šādiem datiem (II pielikuma III daļas 8. punkta a. apakšpunkta i. punkts). Taču organizāciju pienākums atbildēt uz indivīdu pieprasījumiem par apstrādes nolūkiem, attiecīgajām personas datu kategorijām, un saņēmējiem vai saņēmēju kategorijām, kam personas dati tiek atklāti, ir diezgan vājš. DG29 uzskata, ka informācija, kas tiks sniegta datu subjektam, būtu jāmin pamattekstā, nevis tikai zemsvītras piezīmē, un tas ir jānosaka kā skaidrs pienākums (saistībā ar II pielikuma III daļas 8. punkta a. apakšpunkta i. punkta 1. apakšpunktu).

Saskaņā ar 8. papildu principu „piekļuve jāsniedz tikai tādā mērā, kādā organizācija uzglabā personisko informāciju" (II pielikuma III daļas 8. punkta d. apakšpunkta ii. punkts). Šis noteikums nebūtu jāinterpretē šaurā nozīmē, proti, ka piekļuve, principā, ir jāsniedz datiem, ko organizācija apstrādā jebkādā veidā, ne tikai uzglabātiem datiem. Tāpēc piekļuves tiesību efektivitātes nolūkā ir svarīgi paskaidrot, ka „uzglabā" nozīmē „apstrādā" II pielikuma I daļas 8. punkta b. apakšpunktā sniegtās definīcijas nozīmē. Šā noteikuma piemērošana būtu rūpīgi jāizskata privātuma vairoga kopīgās pārskatīšanas laikā.

Pastāv bažas attiecībā uz izņēmumu sarakstu, kas sniegts II pielikuma III daļas 8. punkta e. apakšpunkta i) punktā un ir līdzīgs drošības zonas BUJ 8. punktā sniegtajam, un kam ir tendence mainīt līdzsvaru par labu organizāciju interesēm. Šajā nozīmē piekļuve personas datiem netiks sniegta indivīdiem šādu iemeslu dēļ: „profesionālas priekšrocības neievērošana vai pienākuma neizpilde" (II pielikuma III daļas 8. punkta e. apakšpunkta 3. punkts), „kaitējums darbinieku drošības izmeklēšanai vai šķīrējtiesas procesiem, vai saistībā ar plāniem par jaunu darbinieku pieņemšanu un uzņēmuma reorganizāciju" (II pielikuma III daļas 8. punkta e. apakšpunkta 4. punkts), un „"apdraudējums konfidencialitātei, kas jāievēro saistībā ar pareizas pārvaldības uzraudzības, pārbaudes vai regulatīvajām funkcijām, vai turpmākās vai jau notiekošās sarunās, kurās ir iesaistīta organizācija" (II pielikuma III daļas 8. punkta e. apakšpunkta 5. punkts). Šie iemesli būtu jāskata papildus vispārējam atbrīvojumam attiecībā uz konfidenciālu komercinformāciju, kas iekļauts II pielikuma III daļas 8. punkta c. apakšpunktā. Tāpēc indivīds minētajās situācijās nevarēs piekļūt saviem

[26] Lieta C-131/12 — Google Spain v. Agencia Española de Protección de Datos and Mario Costeja González, 2014. gada 13. maijs.

datiem, un līdzsvars starp indivīda un organizācijas tiesībām un interesēm netiks mainīts, lai rastu piekļuves pieprasījuma risinājumu.

DG29 atgādina, ka hartas 8. panta 2. punkts piešķir indivīdiem tiesības piekļūt viņu datiem. Lai gan tās nav absolūtas tiesības, tās ir būtiskas tiesībām uz personas datu aizsardzību, jo atvieglo datu subjekta pārējo tiesību, piemēram, labošanas un dzēšanas tiesību, īstenošanu.

Attiecībā uz labošanas un dzēšanas tiesībām DG29 atzinīgi vērtē būtisku uzlabojumu, ko privātuma vairoga principi nodrošina salīdzinājumā ar drošības zonas principiem, paredzot, ka šīs tiesības tiek piešķirtas ne tikai situācijās, kad dati ir neprecīzi, bet arī tad, ja dati ir apstrādāti, pārkāpjot principus (II pielikuma II daļas 6. punkts).

2.2.6. Tiesību aizsardzība, izpilde un atbildība (tiesiskās aizsardzības mehānismi)

a) ES indivīdu tiesību uz tiesisko aizsardzību efektīva īstenošana

DG29 atzīst ASV iestāžu saistības attiecībā uz tiesiskās aizsardzības mehānisma dažādām iedaļām. Tomēr, ņemot vērā mehānisma vispārējās uzbūves sarežģītību un skaidrības trūkumu, DG29 bažījas, ka praksē datu subjekta tiesību efektīva īstenošana varētu tikt apdraudēta. DG29 norāda, ka tiesiskās aizsardzības mehānisma kvalitātei vajadzētu būt noteicošajai pār ES indivīdiem pieejamo mehānismu skaitu. Pastāv arī bažas, ka lielākā daļa tiesiskās aizsardzības mehānismu (ja ne visi) paredz procedūru Amerikas Savienotajās Valstīs, tādējādi sarežģījot procedūras uzraudzību, ko veic ES datu aizsardzības iestādes.

Faktiski tiesiskās aizsardzības mehānisms, kas paredzēts privātuma vairogā, primāri koncentrējas uz datu subjekta iespēju „nosargāt savas tiesības un turpināt lietu par neatbilstību privātuma principiem, tieši kontaktējoties ar ASV pašsertificēto uzņēmumu”[27]. Turklāt organizācijām ir jānorīko neatkarīga strīdu izšķiršanas iestāde, kas izmeklētu un risinātu individuālas sūdzības. DG29 atzinīgi vērtē, ka tas tiks organizēts, neradot izmaksas indivīdam.

Alternatīva varētu būt iespēja iesniegt sūdzības tieši Federālajai tirdzniecības komisijai, pat ja tai nav pienākuma tās risināt. Arī datu aizsardzības iestāde varētu iesniegt sūdzību, un ASV Tirdzniecības ministrija ir apņēmusies izskatīt sūdzības un darīt visu iespējamo, lai veicinātu to sūdzību izskatīšanu (I pielikums), kas Federālajai tirdzniecības komisijai būs jāizskata „prioritārā kārtā” (II pielikuma III daļas 7. punkta e. apakšpunkts). Tomēr Federālās tirdzniecības komisijas prioritāšu noteikšana sūdzību izskatīšanā nesniedz datu subjektam pārliecību, ka tā sūdzības tiks izskatītas.

Indivīdu galējais risinājums būs iespēja pieprasīt saistošu šķīrējtiesu. Šķīrējtiesas komisija atradīsies ASV, un tās darbu pārskatīs ASV tiesas.

Privātuma vairogs piedāvā arī iespēju organizācijai izvēlēties sadarboties ar ES datu aizsardzības iestādēm (II pielikuma III daļas 5. punkta a. apakšpunkts). Tas pat ir obligāti

[27] Eiropas Komisija, pietiekamības lēmuma projekts, 30. punkts

attiecībā uz cilvēkresursu datiem, kas savākti saistībā ar darba attiecībām (II pielikuma III daļas 9. punkta d. apakšpunkta ii. punkts). Šādā gadījumā alternatīvā strīdu izšķiršana nebūs piemērojama (II pielikuma III daļas 5. punkta a. apakšpunkts). Privātuma vairogs skaidri nenosaka, kā sadarbība ar ES datu aizsardzības iestādēm tiks īstenota praksē. Jo īpaši nav skaidrs, vai komisija risinās visus gadījumus vai katru atšķirīgu gadījumu izskatīs cita komisija.

DG29 uzskata, ka pietiekamības lēmumā būtu jāsniedz sīkāka informācija par datu aizsardzības iestāžu kompetenci izskatīt sūdzības. Tas acīmredzot ir atkarīgs no organizācijas kvalifikācijas, bet nav skaidrs, kādā veidā.

Ja organizācija darbojas kā pārstāvis ES pārziņā vārdā, indivīdiem jebkurā gadījumā būs iespēja iesniegt sūdzību kompetentajai ES datu aizsardzības iestādei. Situācija būs līdzīga arī cilvēkresursu un citu komerciālo datu apstrādes jomā.

Ja privātuma vairoga organizācija darbojas kā datu pārzinis, datu aizsardzības iestādes kompetence izskatīt sūdzību aprobežosies ar apstrādi atbilstoši ES tiesību aktiem (apstrāde, par ko atbild ES pārzinis, — tostarp kopīgā pārziņā ar ASV organizāciju — vai situācijā, kad privātuma vairoga organizācija būtu tieši pakļauta ES tiesību aktiem, piemēram, izmantojot aprīkojumu, kas atrodas ES). Tomēr uz datu apstrādi, ko veic saskaņā ar ASV tiesību aktiem, attieksies tikai privātuma vairoga mehānismi. Lai pārvarētu valodas barjeras un nepietiekamās zināšanas par ASV tiesību sistēmu, būtu noderīgi, ja ES datu aizsardzības iestādes būtu tiesīgas darboties kā starpnieki indivīdu sūdzībām vai palīdzēt viņiem alternatīvās strīdu izšķiršanas procesā ar ASV organizācijām vai indivīdu kontaktēšanās laikā ar ASV iestādēm, ja datu aizsardzības iestāde uzskata to par lietderīgu.

DG29 uzsver, ka privātuma vairogā skaidrotais mehānisms neatbilst agrākajam ieteikumam, saskaņā ar kuru ES indivīdiem būtu jānodrošina „iespēja celt prasību par zaudējumu atlīdzību Eiropas Savienībā" un „jāpiešķir tiesības iesniegt prasību kompetentai ES valsts tiesai."[28] Būtu vēlams, lai privātuma vairoga organizācijas iekļautu šādu iespēju savā privātuma politikā.

Lai nodrošinātu efektivitāti, DG29 iesaka, ka sistēmai būtu vēlams ļaut ES datu aizsardzības iestādēm pārstāvēt datu subjektu un rīkoties viņa vārdā vai darboties kā starpniekam. Alternatīva iespēja ir paredzēt īpašas jurisdikcijas noteikšanas klauzulas, kas dod tiesības datu subjektiem izmantot savas tiesības Eiropā.

b) Šķīrējtiesa

Noslēguma šķīrējtiesas procedūras vēl nav pabeigtas, kas sarežģī DG29 veikto vērtējumu. Šķiet, ka šķīrējtiesas process notiks saskaņā ar ASV tiesību aktiem un vienīgā procedūras valoda būs angļu valoda, tāpēc ES datu aizsardzības iestādes varētu vēlēties tiesības palīdzēt indivīdiem šajā procesā.

[28] Skatīt DG29 2014. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*).

Turklāt šķīrējtiesas procedūra tika ieviesta sakarā ar to, ka nebija nekādas garantijas, ka sūdzība tiks izskatīta, jo Federālajai tirdzniecības komisijai nav pienākuma izskatīt visas sūdzības. Ja ES indivīds jūt nepieciešamību pēc advokāta palīdzības, DG29 atzīmē, ka šai personai būs pašai jāmaksā par advokāta pakalpojumiem, kas varētu atturēt indivīdus no sūdzību iesniegšanas šķīrējtiesas procedūrā.

c) Tiesiskās aizsardzības mehānismu uzraudzība, ieviešana un efektivitāte

Nosacījumi uzņemšanai vairogā

Saskaņā ar EST „pašsertifikācijas sistēmas ticamība [...] būtībā balstās uz efektīvu atklāšanas un kontroles mehānismu ieviešanu, praksē ļaujot noteikt tādu normu iespējamus pārkāpumus, kas nodrošina pamattiesību aizsardzību [...].”[29]

DG29 norāda, ka ASV Tirdzniecības ministrijas privātuma vairoga loma sertifikācijas procesā šķietami aprobežojas tikai ar dokumentu pabeigtības pārbaudi. Lai gan DG29 atzīst, ka pašsertifikācija nenozīmē privātuma politikas ieviešanas sistemātisku *a priori* pārbaudi, ASV Tirdzniecības ministrijai būtu vismaz jāapņemas sistemātiski pārbaudīt, vai privātuma politika ietver visus privātuma vairoga principus. Šāda apņemšanās ir minēta pietiekamības lēmuma projektā, bet tā nav uzskatāma ASV Tirdzniecības ministrijas apliecinājuma vēstulē.[30]

Privātuma vairoga principu pārkāpums var ilgu laiku palikt neievērots un, iespējams, tiek konstatēts tikai pēc tam, kad datu subjekta pamattiesībām ir nodarīts nopietns kaitējums, ko, iespējams, vairs nevar novērst. Tādējādi šī pieeja varētu būt pretrunā ar Eiropas piesardzības principu.

Pārredzamība, izmantojot privātuma vairoga sarakstu un no saraksta svītroto organizāciju reģistru

Ievērojami uzlabojumi ir veikti saistībā ar pārredzamību attiecībā uz datu subjektu. Papildus visām ASV organizācijām, kas ir sertificējušās ASV Tirdzniecības ministrijai, jaunajā privātuma vairoga sarakstā būs arī visu to organizāciju saraksts, kas ir dzēstas no privātuma vairoga saraksta, norādot arī iemeslu, kāpēc organizācija tika dzēsta[31]. ASV Tirdzniecības ministrijas privātuma vairoga tīmekļa vietne vēl vairāk koncentrēsies uz mērķauditorijām, sekmējot tās informācijas veida pārbaudi, uz kuru attiecas organizācijas pašsertifikācija, kā arī privātuma politikas, kas attiecas uz minēto informāciju, un tās metodes pārbaudi, ko organizācija izmanto, lai apliecinātu principu ievērošanu[32]. DG29 atzinīgi vērtē to, ka tagad ir skaidrs, ka ASV Tirdzniecības ministrija pārbaudīs, vai uzņēmumi, kam ir publiskas tīmekļa vietnes, tajās ir publicējuši savu privātuma politiku, vai kā sabiedrība tiek informēta par

[29] EST, *Schrems*, 81. punkts
[30] Eiropas Komisija, pietiekamības lēmuma projekts, 34. punkts
[31] I pielikuma 5. punkts un II pielikuma II daļas 1. punkts; DG29 arī atsaucas uz Komisijas ceturto ieteikumu Paziņojumā COM(2103)847, kā arī DG29 2014. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), jo īpaši sadaļas „Pārredzamība” 5. punktu.
[32] I pielikuma 8. punkts; DG29 arī atsaucas uz savu 2014. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), jo īpaši sadaļas „Pārredzamība” 2. punktu.

privātuma politiku gadījumā, ja uzņēmumiem nav publisku tīmekļa vietņu[33]. Dokumenti sniedz vairāk informācijas arī par privātuma politikas saturu[34].

DG29 uzskata, ka varētu rasties problēma, ja organizācija, kas jau ir iekļauta privātuma vairoga sarakstā, vēlāk paplašina savu sertifikāciju attiecībā uz citām datu kategorijām. Šādos gadījumos saraksts neatspoguļos dažādos periodus, kad principi ir piemērojami dažādām datu kategorijām. Tas rada risku, ka ES indivīdi un uzņēmumi nevar pilnībā izvērtēt, vai konkrēta datu kopa patiešām ir pakļauta privātuma vairoga principiem, un, ja tā, kopš kura laika. Lai novērstu šo trūkumu, darba grupa iesaka organizācijas ierakstā privātuma vairoga sarakstā norādīt pašsertifikācijas spēkā stāšanās datumu atsevišķi katrai personas datu kategorijai.

DG29 atzinīgi vērtē to, ka ASV Tirdzniecības ministrija uzturēs to organizāciju reģistru, kas dzēstas no privātuma vairoga saraksta, un šajā reģistrā būs ietverts skaidrojums, ka šīm organizācijām vairs netiek nodrošinātas privātuma vairoga sniegtās priekšrocības, bet tām ir jāturpina piemērot principus personas datiem, kas saņemti, kamēr tās bija privātuma vairoga sertificētas organizācijas, kamēr vien šādi dati ir organizāciju rīcībā (I pielikuma 3. punkts). Tomēr, ņemot vērā, ka dažas organizācijas, kas ir dzēstas no privātuma vairoga saraksta, var pieņemt lēmumu atgriezt vai dzēst datus, kas saņemti privātuma vairoga ietvaros, bet citas organizācijas paturēs datus, ko tās ir saņēmušas vairoga ietvaros, ir svarīgi indivīdiem nodrošināt šī jautājuma labāku pārredzamību. Tāpēc ASV Tirdzniecības ministrijas uzturētajā uzņēmumu reģistrā jānorāda, vai konkrētās organizācijas rīcībā joprojām ir personas dati, kas saņemti privātuma vairoga ietvaros, vai tā ir atgriezusi vai dzēsusi šādus datus. Ja organizācijas rīcībā joprojām ir šādi dati, reģistrā būtu skaidri jānorāda, ka organizācijai ir jāturpina piemērot principus šādiem datiem.

Turklāt ASV Tirdzniecības ministrijas uzturētajā reģistrā būtu jāmin, ka šīm organizācijām vairs netiek nodrošinātas privātuma vairoga sniegtās priekšrocības attiecībā uz jaunu datu nosūtīšanu, kas nozīmē, ka organizācijai vairs nav atļauts saņemt personas datus no ES saskaņā ar principiem.

[33] I pielikuma 3. un 4. punkts; DG29 arī atsaucas uz Komisijas pirmo ieteikumu Paziņojumā COM(2103)847, kā arī DG29 2014. gada 10. aprīļa vēstuli priekšsēdētāja vietniecei Redingai (*Reding*), jo īpaši sadaļas „Pārredzamība" 3. punktu.
[34] I pielikuma 5. un 6. punkts un II pielikuma III daļas 6. punkts

Pārbaudes procedūras

Lai pārbaudītu, vai pašsertifikācija darbojas praksē, organizācijas var veikt pašnovērtējumu vai ārējās atbilstības pārbaudes. DG29 pauž nožēlu, ka darbinieku apmācība tiek pieprasīta tikai tad, ja organizācija izvēlas pārbaudes nolūkā veikt pašnovērtējumu (II pielikuma III daļas 7. punkta c. apakšpunkts). Šķiet arī, ka nepieciešamība pārbaudīt, vai politika ir precīza, visaptveroša, redzama, īstenota un pieejama, tiek pieprasīta tikai tad, ja organizācija izvēlas iekšēju pārbaudi (pašnovērtējumu), un ka ārēja mehānisma veikta pārbaude aprobežojas ar atbilstību organizācijas privātuma politikai.

A posteriori

DG29 atzinīgi vērtē, ka Federālajai tirdzniecības komisijai un ASV Tirdzniecības ministrija ir piešķirtas izmeklēšanas pilnvaras sūdzību gadījumos. Turklāt DG29 atzīmē, ka ASV Tirdzniecības ministrijai būs iespēja veikt *ex officio* pārbaudes, jo īpaši, nosūtot anketas. Tomēr DG29 vēlētos pārliecināties, ka šāda pieeja ir pietiekama, lai izpildītu EST prasības attiecībā uz pārkāpumu efektīvas atklāšanas un kontroles mehānismiem. Faktiski, DG29 vēl ir jautājumi par ASV varas iestāžu precīzām pilnvarām veikt pārbaudes uz vietas pašsertificēto organizāciju telpās, izmeklējot privātuma vairoga pārkāpumus, par to, kā ASV teritorijā varētu iegūt ES iestādes lēmuma eksekvatūru, un par to, vai sankcijas privātuma vairoga ietvaros ir preventīvas praksē.

2.2.7. Personāla datu apstrāde

Darbības joma

9. papildu princips (II pielikuma III daļas 9. punkts) attiecas uz personisko informāciju par darbinieku (esošu vai bijušu), kas savākta darba attiecību kontekstā. Saskaņā ar papildu principa 9. punkta a. apakšpunkta ii. punkta formulējumu privātumu vairoga principi attiecas tikai uz gadījumiem, kad „tiek nosūtīti identificēti dati vai tiem piekļūst". Termins „identificēti dati" neatbilst jēdziena „personas dati" definīcijai saskaņā ar II pielikuma I daļas 8. punkta a. apakšpunktu, kas ietver „datus par identificētu vai identificējamu indivīdu", un tāpēc neatbilst Direktīvā izmantotajai definīcijai[35].

Papildu principa 9. punkta a. apakšpunkta ii. punktā ir teikts, ka "statistikas ziņojumi, kuros izmantoti apkopoti nodarbinātības dati un kuros nav personas datu, un anonimizētu datu izmantošana nerada bažas par privātumu". Šis apgalvojums ir pretrunā ar vairākiem DG29 sniegtajiem atzinumiem. DG29 vēlas uzsvērt, ka apkopotos datus var atkārtoti identificēt, un tāpēc tie būtu jāuzskata par personas datiem[36].

[35] Kā jau uzsvērts, aprobežošanās ar datiem, „kas tiek nosūtīti vai kam piekļūst", neatbilst terminam „apstrāde" (II pielikuma I daļas 8. punkta b. apakšpunkts).
[36] Skatīt Atzinumu 4/2007 par personas datu jēdzienu un Atzinumu 05/2014 par anonimizācijas metodēm

Informēšana, izvēle un nolūka ierobežojums

Papildu principa 9. punkta b. apakšpunkta i. punkts sniedz piemēru, kā informēšanas un izvēles principus piemēro gadījumā, kad personāla dati tiek izmantoti citam nolūkam. Piemērs attiecas uz ASV organizāciju, kas „ir paredzējusi personisko informāciju, kas ir savākta darba attiecību laikā, izmantot mērķiem, kuri nav saistīti ar nodarbinātību, piemēram, tirdzniecības paziņojumiem". Šādā gadījumā nolūka maiņa ir atļauta ar nosacījumu ievērot informēšanas un izvēles principus. Saskaņā ar DG29 viedokli personāla datu turpmāka apstrāde tiešā mārketinga nolūkos vairumā gadījumu būs jāuzskata par neatbilstīgu nolūku un tādējādi būs pretrunā ar nolūka ierobežojuma principu (II pielikuma II daļas 5. punkta a. apakšpunkts). Turklāt DG29 uzskata, ka izvēle nevar būt pietiekams pamatojums, lai darbinieks sniegtu „piekrišanu" (atteiktos) nolūka maiņai darba attiecību kontekstā, kurā šāda piekrišana varētu nebūt pilnīgi brīva.

DG29 stipri apšauba, vai privātuma vairoga galvenās uzmanības vēršana uz izvēles principu kā nosacījumu turpmākai datu apstrādei citam nolūkam atbilst ESAO privātuma vadlīnijām, jo nepastāv pietiekamas garantijas, kas atturētu no atteikšanās mehānisma izmantošanas turpmākai neatbilstīgai apstrādei. Papildu principa 9. panta b) punkta iv. apakšpunkts paredz plašu un skaidru atbrīvojumu no informēšanas un izvēles principiem „ciktāl un tādu laikposmu, kas ir vajadzīgs, lai nekaitētu organizācijas likumīgajām interesēm, paaugstinot amatā, pieņemot darbā vai attiecībā uz citiem līdzīgiem lēmumiem par nodarbinātību". Pirmkārt, personāla datu izmantošanai šādiem nolūkiem būtu jābūt skaidri norādītai, jau vācot šādus datus. Turklāt formulējums „citi līdzīgi lēmumi par nodarbinātību" ir pārāk neskaidrs un pārāk plašs. Tā rezultātā personāla dati tiks pilnībā atbrīvoti no informēšanas un izvēles principiem, tos apstrādājot darba attiecību kontekstā. Termins ir pārāk plašs un neļauj izvērtēt, vai turpmāka izmantošana ir savietojama ar sākotnējo nolūku. DG29 iesaka šo izņēmumu svītrot.

Piekļuves tiesības

Papildu principa 9. panta e) punkta i. apakšpunktā paredzēts arī piekļuves principa piemērošanas atbrīvojums vai arī atbrīvojums no līguma slēgšanas ar trešās puses personāla datu pārzini gadījumos, kas saistīti ar neregulāru un ar darba attiecībām saistītu neliela skaita darbinieku personas datu nosūtīšanu, piemēram, rezervējot lidojumu, viesnīcas numuru vai apdrošināšanas segumam, ar nosacījumu, ka ir ievēroti informēšanas un izvēles principi. DG29 nesaskata saprātīgu pamatojumu šādam atbrīvojumam un iesaka šo punktu svītrot.

2.2.8. Farmaceitiskie preparāti un medicīnas produkti

Darbības joma

Saskaņā ar privātuma vairogu ar šifru kodētu datu nosūtīšana no Eiropas Savienības uz ASV farmaceitisko preparātu un medicīnas produktu kontekstā nav uzskatāma par tāda veida nosūtīšanu, uz kuru attiektos privātuma vairogs (II pielikuma III daļas 14. punkta g) apakšpunkta i. punkts). Tomēr ar šifru kodētu datu nosūtīšanu aizsargā Eiropas datu

aizsardzības tiesību akti. Tādējādi praksē uz šādiem nosūtīšanas gadījumiem nevar attiekties privātuma vairogs. DG29 aicina Eiropas Komisiju skaidri noteikt, ka pietiekamības lēmuma projekts neattieksies uz ar šifru kodētu datu nosūtīšanu farmaceitiskiem vai medicīnas nolūkiem, un tādēļ uz šādiem nosūtīšanas gadījumiem ir jāattiecina citi aizsardzības pasākumu, piemēram, līguma standartklauzulas (turpmāk tekstā — SCC) vai BCR. DG29 ierosina šo jautājumu precizēt galīgajā pietiekamības lēmumā.

Nosūtīšana reglamentējošiem un uzraudzības mērķiem (II pielikuma III daļas 14. punkta d) apakšpunkts)

DG29 ir bažas, ka saskaņā ar šiem nosacījumiem personas dati, kas dēļ medicīnas konteksta pamatā ir sensitīvas dabas, var tikt nosūtīti regulatoriem ASV. Tā kā privātuma vairogs ir paredzēts datu nosūtīšanas aizsardzībai starp privātiem subjektiem, šķiet, publisks subjekts, piemēram, ASV regulators, nevar veikt pašsertifikāciju privātuma vairoga ietvaros, kas savukārt rada jautājumu par pietiekamu datu aizsardzību šādos nosūtīšanas gadījumos. Ja šāda nosūtīšana ir jāizpilda reglamentējošiem nolūkiem, ir jāveic atbilstoši pasākumi, lai nodrošinātu nepārtrauktu ES datu subjektu pamattiesību aizsardzību. DG29 uzsver, ka pietiekamības lēmuma projektā šajā jautājumā nav sniegti nekādi konstatējumi. Tādēļ DG29 nav nekādu garantiju, ka ES datu subjektu sensitīvie dati šajā kontekstā tiks pienācīgi aizsargāti.

Turklāt DG29 neizprot, kādēļ „mārketinga" nolūks ir uzskaitīts apstrādes turpmākās zinātniskās pētniecības nolūkiem piemēru sarakstā. Nav skaidrs arī iemesls, kādēļ tālāka nosūtīšana uzņēmumiem un citiem pētniekiem (II pielikuma III daļas 14. punkta d) apakšpunkts) iekļauta sadaļā „Nosūtīšana reglamentējošiem un uzraudzības mērķiem". Šie jautājumi ir jāprecizē galīgajā pietiekamības lēmumā.

Produktu drošība, iedarbīguma uzraudzība (tostarp ziņojot valdības iestādēm) un sekošana līdzi tādiem pacientiem, kas izmanto konkrētas zāles vai medicīnas ierīces

Privātuma vairogs paredz atbrīvojumu no informēšanas, izvēles, tālākas nosūtīšanas un piekļuves principiem, ciktāl sekošana šiem principiem kavē atbilstību normatīvajām prasībām. Pietiekamības lēmuma projektā nav iekļauti nekādi konstatējumi attiecībā uz situācijām, kurās privātuma principi kavē atbilstību normatīvajām prasībām. DG29 pauž sapratni, ka valdības izmeklēšana var kalpot kā attaisnojums informēšanas principa un piekļuves tiesību ierobežošanai, lai pasargātu izmeklēšanu, DG29 nesaskata iemeslus, kas varētu attaisnot tik plašus atbrīvojumus gadījumos, kad apstrādi veic privātā sektora organizācija vai trešā persona. Piemēram, tā kā pacientu ārstēšana kļūst arvien personalizētāka, šāds plašs atbrīvojums no privātuma principiem, sekojot līdzi pacientiem, kas izmanto konkrētas zāles vai medicīnas ierīces, ir nepieņemams, šāda veida aprūpei kļūstot arvien izplatītākai. Tas attiecas arī uz gadījumiem, kad farmācijas uzņēmumi izmanto datus produktu drošuma un iedarbīguma uzraudzībai (jaunu medikamentu testēšanai vai pārdošanai).

2.2.9. Publiski pieejama informācija

Piekļuves tiesību izņēmums publiski pieejamai informācijai un publisko reģistru informācijai (II pielikuma III daļas 15. punkta d) un e) apakšpunkts) raisa bažas tiktāl, cik indivīds, īstenojot savas piekļuves tiesības, vēlas uzzināt, vai konkrētais pārzinis apstrādā viņa datus, kā arī kādus datus, lai varētu kontrolēt savu datu apstrādi. DG29 ir vairākkārt norādījusi, ka saskaņā ar ES tiesību aktiem datu subjektiem vienmēr ir tiesības piekļūt saviem datiem un nepieciešamības gadījumā pieprasīt to labojumu vai dzēšanu, ja datu apstrāde nav bijusi likumīga vai dati ir nepilnīgi vai neprecīzi, neatkarīgi no tā, vai personas dati ir tikuši publiskoti[37]. Ja indivīda piekļuves pieprasījums tiek noraidīts, pamatojot to, ka dati iegūti no publiski pieejamiem avotiem vai publiskā reģistra, indivīds zaudētu tiesības kontrolēt datu precizitāti un pirmkārt to, vai datu publiskošana ir bijusi likumīga.

Privātuma vairogs savukārt atbrīvo publiskos reģistrus un publiski pieejamu informāciju no informēšanas, izvēles, piekļuves un atbildības par tālāka nosūtīšanu principiem (II pielikuma II daļas 15. punkta b) apakšpunkts). Šie atbrīvojumi šķiet pārāk plaši, salīdzinot ar Direktīvu, un rada bažas, jo tie mazina, cita starpā, indivīdu iespējas kontrolēt savu datu precizitāti un ierobežot savu datu izplatīšanu.

2.3. Secinājumi

DG29 atzīst ASV iestāžu un Eiropas Komisijas panāktos būtiskos uzlabojumus datu nosūtīšanas jautājuma starp abiem kontinentiem komerciālajos aspektos. Tomēr, ņemot vērā iepriekš veikto analīzi, DG29 uzskata, ka privātuma vairoga komerciālajā daļā nepieciešami vairāki precizējumi. Piemēram, skaidra datu saglabāšanas principa trūkums rada bažas. Tādēļ DG29 ir nopietnas bažas, vai privātuma vairogs var nodrošināt tāda līmeņa aizsardzību, kas pēc būtības ir līdzvērtīga ES pastāvošajai.

Pietiekamības lēmumā nepieciešams papildus precizēt nolūka ierobežojuma un izvēles principus. Vairākos jautājumos, jo īpaši attiecībā uz tālāku nosūtīšanu, sūdzību apstrādes mehānismu un personāla vai farmaceitisko datu pārstrādi, saglabājas vājo vietu risks. Turklāt nepieciešams sīkāk izstrādāt privātuma vairoga principu piemērošanu datu apstrādātājiem (pārstāvjiem), un jāpievērš īpaša uzmanība skaidras un viennozīmīgas terminoloģijas izmantošanai.

3. PIETIEKAMĪBAS LĒMUMA PROJEKTA NACIONĀLĀS DROŠĪBAS GARANTIJU IZVĒRTĒJUMS

3.1. ASV nacionālās drošības iestādēm piemērojamie aizsardzības pasākumi un ierobežojumi

Ir iespējams ierobežot pamattiesības uz privāto dzīvi un datu aizsardzību ar nosacījumu, ka šāds ierobežojums ir attaisnojams demokrātiskā sabiedrībā. Tas nozīmē, ka privātuma principi nav absolūti un ir iespējamas atkāpes, tomēr tikai tad, ja tiek ievērotas piemērojamās

[37] Skatīt WP20, 4. lpp.

(būtiskās) garantijas. Atbilstīgi privātuma aizsardzības uzlabošanas mērķim organizācijām būtu jācenšas pilnībā un pārredzami īstenot šos principus, tostarp norādot, kuriem privātuma noteikumiem regulāri tiks piemēroti ASV tiesiskajā regulējumā pieļaujamie izņēmumi. Tā paša iemesla dēļ organizācijām, ja iespējams, jāizvēlas labāka aizsardzība, ja izvēli atļauj principi un/vai ASV tiesību akti.

II pielikuma I daļas 5. punktā noteikts, ka „privātuma principu ievērošanu var ierobežot: a) ciktāl tas ir vajadzīgs lai ievērotu valsts drošību, sabiedrības intereses vai izpildītu tiesībaizsardzības prasības; b) ar likumu, valdības noteikumiem vai tiesu praksi, kas 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; vai c) ja direktīva vai dalībvalsts tiesību akti pieļauj izņēmumus vai atkāpes, ar nosacījumu, ka šādus izņēmumus vai atkāpes piemēro pielīdzināmās situācijās.

Jautājums, vai II pielikumā minētās atkāpes ir attaisnojamas demokrātiskā sabiedrībā. Saskaņā ar privātuma vairoga pietiekamības lēmuma projektu Komisija konstatēja, ka „Amerikas Savienotajās Valstīs pastāv noteikumi, kas izstrādāti, kas ierobežo jebkādu iejaukšanos nacionālās drošības nolūkos to personu pamattiesībās, kuru dati tiek nosūtīti no Savienības uz Savienotajām Valstīm privātuma vairoga ietvaros, līdz attiecīgā likumīgā mērķa sasniegšanai absolūti nepieciešamajam.”[38]

Izmantojot šī atzinuma 1.2. sadaļā izklāstīto satvaru un ņemot vērā ASV iestāžu apgalvojumus un Komisijas konstatējumus, DG29 ir izvērtējusi ASV pastāvošo tiesisko regulējumu un ASV izlūkošanas aģentūru praksi, un noteikumus, uz kādiem tiek pieļauta Eiropas tiesiskajā regulējumā aizsargāto pamattiesību uz privātās dzīves ievērošanu un datu aizsardzību ierobežošana. Izvērtējums ir balstīts Prezidenta politikas direktīvas Nr. 28 (PPD-28), Izpildrīkojuma Nr. 12333 (EO12333) analīzē un Ārvalstu izlūkošanas likuma (ĀIUL — 104., 402., 215., 501. un 702. pants) izveidotajos vairākos juridiskajos pamatos. DG29 paļāvās uz privātuma vairoga VI pielikumu, kas sastāv no Nacionālās izlūkošanas direktora biroja (NIDB) sagatavotas vēstules par ASV drošības iestādēm piemērojamajiem aizsardzības līdzekļiem un ierobežojumiem, un kurā apkopota Eiropas Komisijai sniegtā informācija par ASV sakaru izlūkošanas veiktajām vākšanas darbībām.

3.2. A garantija — apstrādei jānoris saskaņā ar tiesību aktiem un balstoties uz skaidriem, precīziem un pieejamiem noteikumiem

Saskaņā ar Eiropas tiesību aktiem iejaukšanās ir jāatbilst tiesību aktiem, noteiktajai politikai un procedūrai un tai jābūt pietiekami skaidrai un pieejamai (katrai valstij piešķirtās izvēles brīvības robežās), sniedzot iedzīvotājiem pietiekamu norādi, kādos apstākļos un pie kādiem nosacījumiem valsts iestādes var izmantot uzraudzības pasākumus.[39]

[38] Komisijas lēmuma projekta saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par ES-ASV privātuma vairoga sniegtās aizsardzības pietiekamību 75. punkts.

[39] ECT *Zakharov,* 247. punkts: „Tiesa jau agrāk ir konstatējusi, ka likumu „paredzamības” prasība neliek valstīm īstenot tiesību normas, kurās sīki aprakstīta visa veida uzvedība, kas var izraisīt lēmumu pakļaut indivīdu slepenai uzraudzībai,

DG29 atzīmē, ka sakaru izlūkošanas darbības tiek veiktas, balstoties uz pieejamu tiesisko regulējumu. Visi VI pielikumā minētie tiesību akti (PPD-28, ĀIUL, ASV Brīvības likums, LIB) ir pieejami tiešsaistē plašākai sabiedrībai (gan ASV, gan ārpus tām). VI pielikumā ir sniegts pastāvošā tiesiskā regulējuma, vākšanas ierobežojumu, saglabāšanas un izplatīšanas ierobežojumu, atbilstības un uzraudzības, pārredzamības un tiesiskās aizsardzības līdzekļu apkopojums. ASV izlūkošanas darbību tiesību sistēmu veido virkne dažādu dokumentu, tostarp atsevišķu aģentūru ziņojumi, noteikumi un procedūras, kuras jāanalizē, lai gūtu labāku izpratni par darbību norisi gan teorijā, gan praksē. Ņemot to vērā, DG29 koncentrējās uz ierobežotu jautājumu skaitu, kuriem tās ieskatā ir būtiska nozīme.

3.2.1. Izpildrīkojums Nr. 12333 un Prezidenta politikas direktīva Nr. 28

EO12333 piemērošanas joma ir plaša; principā jebkura ārzemju izlūkošanas datu vākšana var notikt pēc ASV prezidenta lēmuma, pamatojoties uz rīkojumu. Tomēr tiek apgalvots, ka kopš ĀIUL ieviešanas EO12333 var tikt izmantots tikai datu vākšanai ārpus ASV teritorijas. DG29 atzīmē, ka EO12333 nesniedz daudz informācijas ne par tā ģeogrāfisko tvērumu, to, cik lielā mērā dati var tikt vākti, saglabāti un tālāk izplatīti, nedz arī pārkāpumiem, kuri var novest pie uzraudzības, vai to, kāda informācija var tikt vākta vai izmantota.

DG29 izpratnē galvenais Prezidenta politikas direktīvas Nr. 28 (PPD-28) mērķis ir noteikt personas datu vākšanas un apstrādes ierobežojumus neatkarīgi no izmantotās uzraudzības programmas un datu iegūšanas vietas.

PPD-28 ir Amerikas Savienoto Valstu prezidenta direktīva, kurā noteikti saskaņotības principi, atbilstīgi kuriem sakaru izlūkošanas vākšana tiek atļauta un izveikta, tomēr PPD-28 nav vākšanas juridiskais pamats. PPD-28 ir efektīva, liekot izlūkdienestu iestādēm šos principus ieviest savos noteikumos un procedūrās. Direktīva attiecas uz sakaru izlūkošanas darbībām neatkarīgi no datu atrašanās vietas, ASV vai ārpus tās, datu vākšanas brīdī. Tādēļ tā attiecas arī uz datiem, kas vākti sakaru izlūkošanas nolūkos, kad tie tiek nosūtīti no ES uz ASV.

Jo īpaši PPD-28 nosaka, ka sakaru izlūkošanas darbībām jābūt pēc iespējas pielāgotām[40]. Attiecībā uz datu izmantošanu direktīvā ir noteiktas datu minimizācijas (tostarp datu saglabāšanas un izplatīšanas nosacījumi), datu drošības un attiecīgā personāla piekļuves [t.i., noteikumi, kuri satur aizsardzības pasākumus, ierobežojot ļaunprātīgas un neatbilstošas izmantošanas riskus], datu kvalitātes un uzraudzības procedūras. Šīs garantijas tiek piemērotas neatkarīgi no datu subjektu valstiskās piederības, t.i., gan ASV, gan citu valstu iedzīvotājiem.

---

pamatojoties uz „nacionālo drošību". Pēc savas būtības draudi nacionālajai drošībai var būt dažādi un var būt negaidīti, un grūti definējami iepriekš (skatīt iepriekš minēto spriedumu lietā *Kennedy*, 159. punkts). Tajā pašā laikā Tiesa ir arī uzsvērusi, ka lietās, kas skar pamattiesības, būtu prettiesiski un pret Konvencijā nostiprināto vienu no demokrātiskas sabiedrības pamatprincipiem nacionālās drošības jomas vadītāja rīcības brīvību izteikt kā neierobežotu varu. Sekojoši tiesību aktos jābūt pietiekami skaidri noteiktam šādas kompetentajām iestādēm sniegtas rīcības brīvības tvērumam un īstenošanas veidam, ņemot vērā attiecīgo pasākumu likumīgo mērķi, lai nodrošinātu indivīdam pienācīgu aizsardzību pret patvaļīgu iejaukšanos."

[40] „Sakaru izlūkošanas darbības ir pēc iespējas pielāgotas. Nosakot, vai vākt sakaru izlūkdatus, Amerikas Savienotās Valstis ņem vērā citas informācijas, arī diplomātisko vai publisko avotu, pieejamību. Šādas atbilstošas un iespējamas alternatīvas sakaru izlūkdienestiem ir jāuzskata par prioritāti." (1. sadaļas d) punkts)

Nododot datus ASV, ir piemērojami arī PPD-28 izveidotie aizsardzības līdzekļi. VI pielikumā pausta NIDB apņemšanās, ka gadījumos, ja ASV izlūkdienests vāktu datus no transatlantiskajiem kabeļiem, kamēr tie tiek pārsūtīti uz ASV, „tas to darītu, ievērojot noteiktos ierobežojumus un aizsardzības pasākumus, tostarp PPD-28 prasības”[41]. DG29 atzīmē, ka joprojām trūkst iedibinātas tiesu prakses, nosakot kabeļu pārtveršanas likumību, ja to veic jebkura valsts. Jebkurā gadījumā ASV nedz apstiprina, nedz arī noliedz kabeļu pārtveršanas izmantošanu izlūkdienestu datu vākšanai.

Nedz PPD-28, nedz arī citos piemērojamos tekstos nav definēts „sakaru izlūkošanas” jēdziens.

3.2.2. Ārējās izlūkošanas uzraudzības likums

Kopumā ĀIUL teksts šķiet skaidrāks un precīzāks. Tomēr tik daudzu normu interpretēšana saskaņā ar PPD-28 un tādējādi to praktiskā piemērošana ir lielā mērā atkarīga no dažādu aģentūru veiktās īstenošanas. Lai arī pagaidām nav pieejams pilns ziņojums par jauno aizsardzības pasākumu īstenošanu, ASV delegāti ir informējuši DG29 pārstāvjus, ka PPD-28 aizsardzības pasākumu īstenošana ir pabeigta un tā īstenota līdzīgi visos ASV izlūkdienestos.

Precīzāk izsakoties, 501. pantā relatīvi skaidri noteikts, kāda veida izlūkošanas darbības var tikt atļautas: „jebkādu taustāmu lietu (tostarp grāmatu, ierakstu, papīru, dokumentu un citu priekšmetu) uzrādīšana”. Tomēr jāatzīmē, ka, iekļaujot „taustāmu lietu” definīcijā „citus priekšmetus”, šo pilnvaru tvērums ir samērā plašs.

702. pantā, kas paredz datu vākšanu ārējās izlūkošanas informācijas iegūšanai no citu valstu personām, par kurām var pamatoti uzskatīt, ka tās atrodas ārpus Amerikas Savienotajām valstīm,[42] nav sniegtas tikpat detalizētas norādes kā 501. pantā. 702. pants attiecas uz elektronisko sakaru pakalpojumu sniedzējiem, kas reģistrēti ASV, lai vāktu ārpus ASV robežām esošu indivīdu ārējās izlūkošanas informāciju. „Ārējās izlūkošanas informācijas” definīcija ir plaša. Tajā, cita starpā, ietilpst „informācija par ārvalstu varu vai ārvalstu teritoriju, kas saistīta ar Amerikas Savienoto Valstu ārlietām”[43], kas rada zināmu neskaidrību par to, kāda veida informācija praksē var tikt vākta.

Par spīti dokumentu, Kongresam iesniegto ziņojumu un Privātuma un pilsonisko brīvību pārraudzības padomes (turpmāk tekstā — PPBPP) uzraudzības ziņojumu atslepenošanai, ĀIUL piemērošana, tostarp tā tvērums un noteikto izraudzīšanas noteikumu izmantošana, joprojām ir neskaidra un mulsinoša. Noteikto izraudzīšanas noteikumu („izraudzītāju”) izmantošana ir minēta PPBPP ziņojumā[44], tomēr DG29 izpratnē tie neatbilst no 702. punkta izrietošajiem mērķtiecīgajiem noteikumiem[45]. Ciktāl DG29 var apstiprināt, tie nav minēti vispārpieejamos noteikumos.

[41] Privātuma vairoga VI pielikums, Nacionālās izlūkošanas direktora biroja (NIDB) vēstule par ASV drošības iestādēm piemērojamajiem aizsardzības līdzekļiem un ierobežojumiem, 2. lpp.
[42] ASV Kodeksa 50. sadaļas 1881.a punkta D) apakšpunkta 1. punkts
[43] ASV Kodeksa 50. sadaļas 1801 punkta e) apakšpunkta 2. punkts
[44] PPBPP ziņojums par uzraudzības programmu, kas tiek veikta saskaņā ar ĀIUL 702. pantu, 32. lpp.
[45] ASV Kodeksa 50. sadaļas 1881.a punkta D) apakšpunkts

3.2.3. Secinājumi

Kopumā DG29 atzīmē, ka ar izlūkošanas darbībām saistītie piemērojamie teksti ir pieejami tiešsaistē un ka ASV iestādes ir spērušas nopietnus soļus pārredzamības virzienā.

DG29 atzīst, ka kopš 2013. gada liels skaits dokumentu, piemēram, noteikumi, procedūras, ĀIAT lēmumi un citi atslepenoti dokumenti ir tikuši publicēti. Turklāt PPBPP ir publicējusi svarīgus ziņojumus par darbībām, kas veiktas, balstoties uz 702. punktu un ASV Brīvības likumu. Tiek gaidīts līdzīgs ziņojums par darbībām, kas veiktas saskaņā ar EO12333.

Vairāki tiesību aktu pielikumi, kas varētu sniegt informāciju par izpildraksta sekām indivīdiem, kas atrodas ārpus ASV, un jebkādiem piemērojamajiem aizsardzības līdzekļiem, ir klasificēti un tādējādi nav pieejami sabiedrībai vai indivīdiem, kurus to piemērošana, iespējams, skar. Atslepenotajiem tekstiem ir tikai ierobežota vērtība, un tie sniedz ierobežotu ieskatu izlūkošanas darbībās.

Par spīti pēc Snoudena atklātajiem dokumentiem pieliktajām pūlēm izskaidrot EO12333 darbības principus, jo īpaši pieņemot PPD-28, pašreizējā praktiskā EO12333 piemērošana joprojām ir neskaidra. DG29 atzīmē, ka privātuma vairoga VI pielikumā nav sniegta izsmeļoša informācija par EO12333 darbību.

Lai arī DG29 atzinīgi novērtē ar PPD-28 ieviestos ierobežojumus, ir grūti izsecināt, vai ASV tiesiskais regulējums uzraudzības jomā ir pietiekami paredzams, t.i., vai tajā ir „pietiekama(s) norāde(s) par apstākļiem un nosacījumiem, kādos valsts iestādēm ir tiesības izmantot šādus pasākumus", un tiek gaidīts turpmāks precizējums, tostarp PPBPP ziņojuma par EO12333 publicēšana.

3.3. B garantija — ir jāpierāda vajadzība un samērīgums attiecībā uz sasniedzamajiem likumīgajiem mērķiem

3.3.1. Prezidenta politikas direktīva Nr. 28

PPD-28 ievieš ierobežojumus nolūkiem, kādos var izmantot personas datus, un nosacījumiem, ar kādiem tos var izplatīt, un ietekmē sakaru izlūkošanas datu vākšanu neatkarīgi no izmantotā juridiskā pamatojuma.

Jo īpaši PPD-28 1. sadaļa nosaka, ka ASV sakaru izlūkošanas darbībām jābūt „pēc iespējas pielāgotām". Pat atzīstot šo ierobežojumu, ir grūti noteikt, vai „pēc iespējas pielāgotas" nozīmē, ka jebkāda datu vākšana ir vajadzīga un samērīga.

PPD-28 atzīst, ka lielapjoma vākšana joprojām ir atļauta, lai „noteiktu jaunus vai topošos apdraudējumus un citu būtisku informāciju par valsts drošību, kas nereti ir apslēpta plašajā un komplicētajā mūsdienu globālo sakaru sistēmā".[46] DG29 atzīmē, ka PPD-28 nosaka, ka „lielapjomā savāktie sakaru izlūkdati ir autorizēts liela daudzuma sakaru izlūkdatu

[46] PPD-28 2. sadaļa un privātuma vairoga VI pielikums, Nacionālās izlūkošanas direktora biroja (NIDB) vēstule par ASV drošības iestādēm piemērojamajiem aizsardzības līdzekļiem un ierobežojumiem, 3. lpp.

apkopojums, kas tehnisku vai ar ekspluatāciju saistītu apsvērumu dēļ ir iegūts, neizmantojot diskriminantus (piemēram, konkrētus identifikatorus, izraudzīšanas noteikumus, utt.)".

PPD-28 paredz lielapjomā savāktu sakaru izlūkdatu izmantošanas nolūku ierobežojumus. Datus var vākt lielapjomā sešiem mērķiem, tostarp terorisma apkarošanai un cita veida smagu (transnacionālu) noziegumu apkarošanai. DG29 analīze liecina, ka nolūka ierobežojums ir samērā plašs (iespējams, pārāk plašs), lai būtu uzskatāms par mērķtiecīgu.

PPD-28 nav likvidēta iespēja nekritiskai personas datu lielapjoma vākšanai, un šādas vākšanas iespējas mērogs joprojām ir neskaidrs un, iespējams, plašs. Šajā sakarā DG29 atzīmē, ka NIDB VI pielikumā apstiprina, ka „visas ar interneta sakariem saistītās informācijas lielapjoma vākšanas darbības, ko ASV izlūkdienests veic, īstenojot sakaru izlūkošanu, notiek nelielā interneta daļā[47] un tādēļ augsti novērtētu turpmāku pierādījumu sniegšanu, izmantojot pārredzamības pasākumus.

3.3.2. Ārējās izlūkošanas uzraudzības likums

ĀIUL 215. un 702. panta minimizācijas procedūras tika ieviestas, lai aizsargātu ASV iedzīvotājus no plašas valdības pieejas viņu datiem. Šie ierobežojumu oficiāli neattiecas uz ārvalstniekiem, lai arī ASV valdības amatpersonas vairākkārt gan publiskās, gan privātās sanāksmēs ar DG29 pārstāvjiem ir atkārtojušas, ka minimizācijas procedūru piemērošanas joma praksē tiek attiecināta uz visiem neatkarīgi no personu valstiskās piederības vai pastāvīgās dzīvesvietas.

702. pantā precizēts, ka autorizētā ieguve „veicama saskaņā ar Amerikas Savienoto Valstu Konstitūcijas ceturto labojumu, ierobežojot datu vākšanu tādā mērā, kas tiek uzskatīts par atbilstīgu pamatotas kratīšanas principam. Šajā sakarā nav atšķirības starp ASV un ārvalstu uzņēmumiem". Citiem vārdiem sakot, ar nosacījumu, ka ceturtais labojums tiek piemērots visiem ASV vāktajiem datiem, ASV veikta lielapjoma vākšana būtu „nepamatota" un tādējādi antikonstitucionāla.

DG29 atzinīgi novērtē PPBPP ziņojuma konstatējumus, ka „praksē ārvalstnieki arī iegūst no piekļuves un saglabāšanas ierobežojumiem, kurus pieprasa dažādu aģentūru minimizācijas un/vai mērķatlases procedūras, dēļ ASV iedzīvotāju informācijas identificēšanas un izņemšanas izmaksām un grūtībām lielam datu apjomam, kas parasti nozīmē, ka viss datu kopums tiek apstrādāts atbilstīgi augstākajiem ASV datu standartiem".

Tālāk DG29 atzīmē, ka saskaņā ar PPBPP konstatējumiem „programma nedarbojas, vācot lielapjoma saziņas datus". NIDB 2014. gada Statistiskais pārredzamības ziņojums apstiprina

[47] Privātuma vairoga VI pielikums, Nacionālās izlūkošanas direktora biroja (NIDB) vēstule par ASV drošības iestādēm piemērojamajiem aizsardzības līdzekļiem un ierobežojumiem, 4. lpp; šajā sakarā DG29 atgādina ziņojumu par ES un ASV Datu aizsardzības jautājumu darba grupas ES līdzpriekšsēdētāju konstatējumiem, kurā apgalvots, ka „Saziņas dati ir ļoti neliela globālās interneta datplūsmas daļa", ņemot vērā, ka „lielāko daļu globālās interneta datplūsmas veido liela apjoma, piemēram, televīzijas seriālu, filmu un sporta pārraižu, straumēšana un lejupielāde" (ziņojuma 3.1.2. punkts).44

šo konstatējumu. Turklāt saskaņā ar PPBPP ziņojumu uzraudzības mērķatlasei tiek izmantoti „norīkotie izraudzītāji", piemēram, e-pasta adrese vai tālruņa numurs[48].

Atbilstošie pieejamie sabiedriskie noteikumi, kas skar mērķatlasi, tomēr neparedz šādus mērķtiecīgus noteikumus un paredz tikai izvairīties no ASV iedzīvotāju vai ASV bāzētu personu mērķatlases. Turklāt labums, ko saskaņā ar PPBPP pausto praksē gūst ārvalstnieki, nav juridiski saistošs vai tiesību aktos noteikts, jo pieejamajos likumdošanas aktos, kas skar mērķatlasi, nav sniegti šādi mērķtiecīgi noteikumi un paredz tikai izvairīties no ASV iedzīvotāju vai ASV bāzētu personu mērķatlases.

DG29 arī atgādina, ka 702. panta nolūkiem personas ir ne tikai indivīdi, bet arī grupas, vienības, asociācijas, korporācijas un ārvalstu varas. Turklāt fakts, ka vākšana ir attaisnojama, jo „būtisks iegūšanas nolūks ir iegūt ārējo izlūkošanas informāciju", padara tās nolūku un vajadzību mazliet neskaidru. Tomēr DG29 atzinīgi novērtē VI pielikumā sniegto informāciju, ka 2014. gadā kopējais mērķatlasei pakļauto indivīdu skaits saskaņā ar 702. sadaļu bija apmēram 90 000 indivīdu[49]. Pirmajā privātuma vairoga pārskatīšanā būs iespēja sniegt papildu mērķatlases noteikumu pierādījumus.

Tiktāl nav pārliecinošas tiesu prakses par masveida un nekritiskas datu vākšanas likumīgumu un turpmāko personas datu izmantošanu noziedzības apkarošanas nolūkos, tostarp par jautājumu, kādos apstākļos šāda personas datu vākšana un izmantošana var notikt. Tiek sagaidīts, ka EST vismaz daļēji pievērsīsies šim jautājumam 2016. gada laikā apvienotajās lietās *Tele2 Sverige AB* pret *Post- och telestyrelsen* un *Secretary of State for the Home Department* pret *Davis and Others*[50] un ieteikumā, kas sniedzams par Kanādas PDR nolīguma spēkā esamību.[51] Tikmēr DG29 atgādina, ka tā konsekventi uzskata, ka masveida un nekritiska datu vākšana nekādā gadījumā nevar tikt uzskatīta par samērīgu.[52]

3.3.3. Secinājumi

Par spīti PPD-28 īstenošanai sekojošajiem ierobežojumiem, DG29 joprojām ir bažas, jo īpaši attiecībā uz datu vākšanas samērīgumu. Pirmkārt, ir pazīmes, ka ASV turpina masveidā un nekritiski vākt datus vai vismaz neizslēdz šādas vākšanas iespēju nākotnē. DG29 ir konsekventi uzsvērusi, ka šāda datu vākšana neatbilst ES tiesību aktiem un tādēļ nav pieņemama.

Otrkārt, DG29 atzīmē, ka arī mērķtiecīga datu apstrāde vai „pēc iespējas pielāgota" apstrāde joprojām var tikt uzskatīta par masveida. Šobrīd, vai šāda masveida datu vākšana būtu jāatļauj, ir atkarīgs no EST tiesvedības. Šī iemesla dēļ DG29 nesniedz gala novērtējumu par mērķtiecīgas, tomēr masveida datu apstrādes likumību. Tomēr tā uzsver, ka gadījumā, ja mērķtiecīga, tomēr masveida datu apstrāde tiktu atļauta, mērķatlases principi būtu jāpiemēro

[48] PPBPP ziņojums par uzraudzības programmu, kas tiek veikta saskaņā ar ĀIUL 702. pantu, 32. lpp.
[49] VI pielikums, 11. lpp.
[50] EST, apvienotās lietas C-203/15 un C-698/15
[51] EST, lieta A-1/15.
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_lv.pdf

gan datu vākšanai, gan to turpmākai izmantošanai, un tie nevar tikt piemēroti tikai izmantošanai. Jebkurā gadījumā pietiekamības lēmuma projektā ir nepieciešams PPD-28 minēto sešu lielapjoma datu vākšanas nolūku precizējums. Šajā posmā DG29 nav pārliecināta, ka šie nolūki ir pietiekami ierobežoti, lai nodrošinātu, ka datu vākšana patiesi ir ierobežota līdz tādam apjomam, kas ir vajadzīgs un samērīgs.

3.4. C garantija — ir jābūt neatkarīgam pārraudzības mehānismam

ASV nepastāv viena federālā līmeņa pārraudzības iestāde, kuras uzdevums būtu pārraudzīt izlūkošanas un uzraudzības programmu ietekmi uz privātumu un datu aizsardzību. ASV izlūkošanas darbības ir drīzāk pakļautas daudzslāņainai pārraudzības procedūrai: iespējams izdalīt iekšējo un ārējo pārraudzību. DG29 atzīst, ka ASV pārraudzības iestāžu ziņošanas prakse ir ļoti detalizēta un lielā mērā publiska.

3.4.1. Iekšējā pārraudzība

Visās izlūkošanas un drošības aģentūrās ir darbinieki, kas ir atbildīgi par atbilstības tiesiskajam regulējumam nodrošināšanu, tostarp ģenerālinspektori, kuru pamata uzdevums ir izvērtēt vispārējo aģentūru darba atbilstību tiesību aktiem, tostarp, bet ne tikai likumiem, kas skar privātumu un datu aizsardzību. Ģenerālinspektoru amats ir paredzēts tiesību aktos, un viņus ieceļ (vai drīz iecels) prezidents un apstiprina Senāts, cenšoties nodrošināt, ka viņi būs organizatoriski neatkarīgi un ziņos Kongresam. Tādēļ DG29 uzskata, ka ģenerālinspektori visticamāk atbildīs EST un Eiropas Cilvēktiesību tiesas (ECT) definētajam organizatoriskās neatkarības kritērijam, vismaz sākot ar brīdi, kad jaunais nominēšanas process tiks piemērots visiem. Tikmēr saglabājas zināmas bažas par ģenerālinspektoriem, kurus joprojām ieceļ viņu pārraudzītās aģentūras direktors.

Ģenerālinspektori var sniegt ieteikumus, kas var tikt tālāk nodoti Tieslietu ministrijai un PPBPP vai pat Kongresa komitejai, kas var panākt šo ieteikumu izpildi. Ja ģenerālinspektors konstatē pārkāpumu, to iespējams novērst, izmantojot iekšējos un politikas pasākumus, un par to var informēt Kongresu. Ģenerālinspektoram ir pilnvaras, piemēram, veikt auditus vai pārbaudes.

DG29 atzīmē, ka ģenerāldirektora ziņojumi var tikt neatklāti sabiedrībai un ka ģenerālinspektoram var tikt liegts sniegt ziņojumu, ja pārbaudītā informācija ir klasificēta. Tomēr ziņojumi vienmēr ir pakļauti Kongresa pārraudzībai, nodrošinot būtisku aizsardzības pasākumu, pat ja tas neparedz individuālu tiesību aizsardzību.

Visās aģentūrās ir privātuma un pilsoniskās brīvības amatpersona, kas palīdz darbā ar obligāto patstāvīgas ziņošanas sistēmu Kongresa pārraudzībai.

Kopumā pastāvošie iekšējās pārraudzības mehānismi var tikt uzskatīti par samērā stabiliem; tomēr, lai pamatotu pamattiesību uz privātumu un datu aizsardzību ierobežošanu, pārraudzībai ir jābūt pilnīgi neatkarīgai. Lai arī DG29 ciena un novērtē dažādo privātuma un pilsoniskās brīvības amatpersonu darbu, grupa nevar izdarīt secinājumu, ka tie atbilst nepieciešamajam neatkarības līmenim, lai darbotos kā neatkarīgi pārraugi.

3.4.2. Ārējā pārraudzība

Ārējo pārraudzību veido vairāki atšķirīgi mehānismi: tiesas pārraudzība saskaņā ar 501. un 702. pantu, kuru nodrošina Ārvalstu izlūkošanas uzraudzības tiesa (turpmāk tekstā — ĀIUT), Kongresa sakaru izlūkošanas komiteju pārraudzība un PPBPP veiktie uzdevumi.

DG29 atgādina, ka ideālā gadījumā, kā to arī norādījušas EST un ECT, pārraudzībai jābūt tiesneša rokās, lai garantētu procedūras neatkarību un objektivitāti. Līdz nesenam laikam ĀIUT procedūra bija *ex parte* procedūra, nesniedzot iesaistītajiem indivīdiem iespēju tikt uzklausītiem vai pat informētiem par lietu. Arī šobrīd ĀIUT procedūra joprojām ir *ex parte,* tomēr pēc ASV Brīvības likuma pieņemšanas ĀIUT tika ieviesti *amici curiae. Amici curiae* darbojas neatkarīgi, tomēr viņi nav iecelti, lai aizstāvētu konkrētus indivīdus, kas var būt iesaistīti lietā.

Ar ASV Brīvības likumu ir izveidota *amici curiae* grupa, kas sniedz ĀIUT rezumējumus par svarīgām lietām. Tiesa ir izvēlējusies piecus juristus, kuri ieguvuši attiecīgo drošības pielaidi un sniedz tehniskus ieteikumus, apmeklē ĀIUT sēdes, sniedz rezumējumus un apspriež lietu pēc būtības no privātuma un pilsonisko tiesību perspektīvas. Tomēr viņi to dara tikai svarīgās lietās vai gadījumos, ja uzrodas jauni juridiski jautājumi.[53]

215. punkts ir gandrīz pilnībā pakļauts *ex ante* (bet ne *ex post*) tiesu pārraudzībai, jo visas programmas, kas 215. punktu izmanto par vākšanas pamatu, vispirms jāapstiprina ĀIUT. PPBPP ziņojumā precizēts, ka „702. pants atšķiras no tradicionālā ĀIUL elektroniskās uzraudzības regulējuma gan piemēroto standartu ziņā, gan ĀIUT individualizēto pieteikumu ziņā. Saskaņā ar likumu ģenerālprokurors un Nacionālās izlūkošanas biroja direktors katru gadu sertificē citu valstu iedzīvotāju, kuri atrodas ārpus Amerikas Savienotajām Valstīm, novērošanu, lai iegūtu ārējās izlūkošanas informāciju, neprecizējot ĀIUT, kurš citas valsts iedzīvotājs tiks novērots. (...) Tāpat nepastāv arī prasība valdībai norādīt pamatotu iemeslu uzskatam, ka atbilstīgi 702. pantam izvēlētais novērojumu mērķis ir ārvalstu vara vai ārvalstu varas pārstāvis, kā to pieprasa tradicionālais ĀIUL regulējums."[54]

Kongresā Sakaru izlūkošanas komitejas pārrauga izlūkošanas darbību apstiprināšanu, jo īpaši budžeta balsojumos. Senāta un Parlamenta izlūkošanas komitejas saņem klasificētus ziņojumus par izlūkošanas darbībām. Ģenerālprokurors ik pēc sešiem mēnešiem atskaitās šīm komitejām par ĀIUL elektronisko pārraudzību. DG29 joprojām nav skaidrs, kādā mērā viņi var apspriest indivīdu, jo īpaši citu valstu iedzīvotāju, personas datu apstrādi.

PPBPP ir neatkarīga ASV valdības izpildvaras daļa, kurai ir divas pamata pilnvaras: 1) pārskatīt un analizēt izpildvaras veiktās darbības [ASV] nācijas aizsargāšanai pret terorismu, nodrošinot, ka šādu darbību nepieciešamība tiek līdzsvarota ar nepieciešamību aizsargāt privātumu un pilsoniskās brīvības, un 2) nodrošināt, ka brīvības apsvērumi tiek pienācīgi ņemti vērā, izstrādājot un īstenojot normatīvos aktus un politiku, kas saistās ar centieniem

[53] Brīvības likuma IV SADAĻA--ĀRVALSTU IZLŪKOŠANAS UZRAUDZĪBAS TIESAS REFORMAS, 401. pants *Amici curiae* iecelšana
[54] PPBPP ziņojums par uzraudzības programmu, kas tiek veikta saskaņā ar ĀIUL 702. pantu, 24., 25. lpp.

aizsargāt nāciju no terorisma. DG29 atzīmē, ka PPBPP ir tiesības izsniegt pavēstes un ir piekļuve klasificētai informācijai. Veicot šos pienākumus, PPBPP pārbauda arī programmu efektivitāti. Pārraudzība tiek veikta pēc, nevis pirms notikušā fakta. PPBPP ir parādījusi savu neatkarību, nepiekrītot Amerikas Savienoto Valstu prezidentam juridiskos jautājumos. Jo īpaši padome konstatēja, ka 215. punkta tālruņu metadatu programma nav likumīgi atļauta, un secināja, ka tā ir neefektīva, jo nav pierādījumu, ka ar to būtu izdevies novērst uzbrukumus. PPBPP arī gada garumā veica 702. punkta programmas izpēti un konstatēja, ka tā ir likumīga un to skaidri atļauj likums, kā arī 702. punkts ir izrādījies ļoti efektīvs, tostarp terorisma jautājumos. Visbeidzot tā ir pievērsusies pārredzamības prasībai un konstatējusi, ka virknei klasificētu faktu nav jābūt klasificētiem. Tiek saprasts, ka PPBPP drīz sniegs ziņojumu par PPD-28 īstenošanu. Šajā sakarā padome uzskata, ka informācijas par ārvalstnieku saglabāšanas pamatojumam nepietiek tikai ar vienkāršo faktu, ka viņš ir ārvalstnieks.

Visbeidzot DG29 atzīmē, ka EO12333 neparedz izskatīšanu tiesā, pārraudzību vai tiesiskās aizsardzības mehānismu uz tā bāzes īstenotajām uzraudzības programmām.

3.4.3. Secinājumi

Pietiekamības lēmuma projektā redzama daudzslāņaina pieeja gan iekšējās, gan ārējās pārraudzības mehānismam, kas pastāv ASV. Lai arī pārraudzības mehānismu darbības principi var šķist mulsinoši, DG29 ir apmierināta, ka kopumā pastāv pietiekami iekšējās pārraudzības mehānismi. Tomēr DG29 māc bažas par nepietiekamu uz EO12333 bāzes īstenoto uzraudzības programmu pārraudzību.

DG29 atzīmē, ka tās iepriekš izteikto kritiku, ka ĀIUT procedūras neatbilst sacīkstes principam, tikai daļēji mazina *amici curiae* ieviešana, kuru uzdevums ir „veicināt individuālās privātās dzīves un pilsonisko brīvību aizsardzību". Par spīti tam, ĀIUT nenodrošina efektīvu citu valstu iedzīvotāju mērķatlases pārraudzību. Joprojām saglabājas zināmas šaubas par ĀIUT spēju efektīvi izvērtēt mērķatlases un minimizācijas procedūras, ko uzsvēra arī PPBPP[55].

3.5. D garantija — indivīdam ir jābūt pieejamiem efektīviem tiesiskās aizsardzības līdzekļiem

3.5.1. Tiesiskās aizsardzības līdzekļi

3.5.1.1. Tiesībspējas prasība

ASV tiesiskās aizsardzības līdzekļu sistēmā ir svarīgs ierobežojums: ASV Konstitūcija pieprasa indivīdam pierādīt savu tiesībspēju: „prasītājam ir jābūt nodarītam vai tiks nodarīts tiešs bojājums vai kaitējums, un šim kaitējumam ir jābūt ar tiesiskiem līdzekļiem novēršamam. Federālās pārvaldes līmenī tiesvedība nevar vienkārši tikt uzsākta, pamatojoties

[55] PPBPP ziņojums par uzraudzības programmu, kas tiek veikta saskaņā ar ĀIUL 702. pantu, 11. lpp.

uz indivīda vai grupas neapmierinātību ar valdības rīcību vai tiesību aktu."[56] Šo prasību, šķiet, anulē uzraudzībai pakļauto indivīdu neinformēšana pat pēc pasākumu beigām. EST un ECT ir atkārtoti uzsvērušas, ka indivīdiem ir jābūt pieejamai administratīvai vai tiesiskai aizsardzībai. ECT savā spriedumā lietā *Zakharov* apstiprināja, ka, pamatojoties uz tiesu praksi, ikviens var vērsties tiesā, ja viņam/viņai ir likumīgs pamats uzskatīt, ka ir ierobežotas viņa/viņas pamattiesības.[57]

Turklāt saskaņā ar Amerikas Savienoto Valstu Augstākās tiesas judikatūru ārzemniekiem, kuri atrodas ārpus ASV, netiek sniegta pilna apjoma konstitucionālā aizsardzība ASV teritorijā[58]. Tas jo īpaši attiecas uz ceturto labojumu, kas aizsargā ASV pilsoņus, bet ne citu valstu pilsoņus, pret nepamatotu kratīšanu vai mantas arestu, un no kā izriet liela daļa ASV tiesību uz privāto dzīvi. Uz Eiropas pilsoņiem un citiem eiropiešiem, kas dzīvo ārpus ASV, gluži vienkārši neattiecas ceturtā labojuma aizsardzība.[59]

Ierobežotā Likuma par tiesisko aizsardzību piemērošana (gan pēc būtības, jo tas neskar nacionālo drošību, gan arī attiecībā uz personām, kas var paļauties uz likumu), daudzie atbrīvojumi un tiesiskā nenoteiktība, attiecībā uz kurām aģentūrām šis likums par tiesisko aizsardzību attieksies, neatbilst prasībai nodrošināt efektīvu tiesiskās aizsardzības mehānismu visiem indivīdiem, kurus skar nacionālās drošības izlūkošanas uzraudzības lietas.

3.5.1.2. Prezidenta politikas direktīva Nr. 28

DG29 atzīmē, ka PPD-28 ir tikai direktīva un tādējādi nerada nekādas tiesības indivīdiem. Tas ir izdarāms tikai ar tiesību aktu palīdzību. Tādēļ indivīdi nevar vērsties tiesā, balstoties uz iespējamu PPD-28 aizsardzības līdzekļu pārkāpumu.

3.5.1.3. Ārējās izlūkošanas uzraudzības likums

Saskaņā ar ĀIUL nelikumīgas uzraudzības gadījumā indivīdiem pastāv daži tiesiskās aizsardzības līdzekļi. Atbilstīgi ĀIUL „cietušai personai, kas nav ārvalstu vara vai ārvalstu varas pārstāvis [...] attiecīgi, kam veikta elektroniska uzraudzība vai par kuru ir atklāta informācija, kas ievākta ar elektroniskās uzraudzības palīdzību, vai kas izmantota, pārkāpjot šīs sadaļas 1809. punktu, ir pamats celt tiesvedību pret jebkuru citu personu, kas ir izdarījusi šādu pārkāpumu". Tomēr šeit skaidri tiek izslēgta ārvalstu vara vai ārvalstu varas pārstāvis, kam piemērots šāds pasākums. Par spīti iepriekšminētajam, prasītājam jāpierāda sava tiesībspēja, kas praksē nebūs iespējams.

Ar ASV Brīvības likumu ir izveidota *Amicus curiae* padomdevēja padome, kas sniedz (pēc izvēles) ĀIUL tiesai ieteikumus būtiski jaunas juridiskās interpretācijas gadījumā. Padomes uzdevums ir sniegt objektīvu ieteikumu, neaizstāvot konkrēta indivīda intereses viņa/viņas prasījumā.

---

[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; *Clapper* pret *Amnesty International USA*

[57] ECT, *Zakharov*, 171. punkts

[58] ASV pret *Verdugo — Urquidez* , 264.-266. lpp.

[59] ES līdzpriekšsēdētāju ziņojums, 2. sadaļa

3.5.2. Administratīvie aizsardzības līdzekļi

3.5.2.1. Ģenerālinspektori

Vēl vienu tiesiskās aizsardzības līdzekļu iespēju nodrošina ģenerālinspektoru institūts, kam var iesniegt sūdzību. Tomēr ģenerālinspektoriem nav pienākuma izskatīt katru sūdzību: nepastāv tiesības tikt uzklausītam, drīzāk izvēles kārtībā. Ģenerālinspektors var izsniegt ziņojumus par pārkāpumu konstatējumiem atslepenotas informācijas gadījumos. Ja indivīds uzskata, ka ziņojums skar viņu, viņš/viņa var vērsties tiesā, pamatojoties uz likuma pārkāpuma konstatējumu.

3.5.2.2. Likums par informācijas brīvību

Visām personām pieejams tiesiskās aizsardzības līdzeklis ir informācijas atklātības pieprasījuma iesniegšana, pamatojoties uz Likumu par informācijas brīvību (LIB). Saskaņā ar ASV valdības pausto LIB pieprasījumu var principā iesniegt jebkura persona — gan ASV, gan citas valsts pilsonis, vienkārši pieprasot jebkuru aģentūras ierakstu. Tostarp iespējams pieprasīt ierakstus par indivīdu, lai arī šādā gadījumā ir nepieciešams uzrādīt personas identitātes apliecinājumu. Tomēr gadījumos, ja informācija ir klasificēta nacionālās drošības aizsardzības nolūkos, LIB pieprasījums visticamāk nebūs sekmīgs, jo tiek piemērots atbrīvojums: aģentūrām nav pienākuma sniegt piekļuvi klasificētai informācijai, tostarp arī gadījumos, ja šī informācija attiecas uz indivīdu, kurš iesniedzis pieprasījumu. Informācija no tobrīd notiekošas tiesībaizsardzības izmeklēšanas ir pilnībā izslēgta no LIB pieprasījumiem. Visbeidzot DG29 izpratnē LIB pieprasījums nesniedz tiesības neatkarīgai iestādei pārbaudīt apstrādes likumību.

3.5.3. Privātuma vairoga ombuds

3.5.3.1. Ombuda izveide

Privātuma vairogs izveido jaunu mehānismu „ES indivīdiem", ļaujot iesniegt prasījumus pret „ASV sakaru izlūkošanu" nule izveidotajam privātuma vairoga ombudam. Kā paskaidrots valsts sekretāra Džona Kerija (*John Kerry*) 2016. gada 22. februāra vēstulei pievienotajā memorandā, par ombudu tiks iecelta valsts sekretāra vietniece K.Novelli kundze (*C. Novelli*). Viņa pildīs šīs funkcijas papildus PPD-28 4. punkta d) apakšpunktā izveidotās vecākās koordinatores starptautiskās informāciju tehnoloģijas diplomātijas jautājumos pienākumiem. Vēstulē un memorandā tiek uzsvērts, ka „valsts sekretāra vietniece ir tieši pakļauta valsts sekretāram un neatkarīga no izlūkdienestiem".

Neatkarīgi no nosaukuma memorandā tiek paskaidrots, ka privātuma vairoga ombuds apstrādās ne tikai pieprasījumus saistībā ar nacionālās drošības piekļuvi datiem, kas privātuma vairoga ietvaros nodoti no ES uz ASV, bet arī pieprasījumus saistībā ar datiem, kas nodoti saskaņā ar līguma standartklauzulām, saistošiem uzņēmumu noteikumiem, atkāpēm (saskaņā ar Direktīvas 95/46/EK 26. pantu) vai „iespējamām atkāpēm nākotnē", kas definētas memoranda otrajā zemsvītras piezīmē.

Mehānisma paredzētais darbības princips var tikt apkopots šādi: ES indivīds iesniedz prasījumu par nacionālās drošības pakalpojumiem kompetentajai dalībvalsts iestādei vai centralizētai „ES individuālo sūdzību izskatīšanas struktūrai", ja tāda tiks izveidota vai nozīmēta. Iestāde, kura nosūta pieprasījumu ombudam, pārbaudīs vispirms, vai pieprasījums ir pilnīgs saskaņā ar vēstules 3. punkta b) apakšpunktā noteikto.[60] Tiklīdz pieprasījums ir nodots privātuma vairoga ombudam un ir konstatēta tā atbilstība 3. punkta b) apakšpunktam, privātuma vairoga ombuds sniedz atbildi, kurā apstiprina, ka „i) ka sūdzība ir pienācīgi izmeklēta un ii) ka ir ievēroti ASV tiesību akti, statūti, izpildrīkojumi, prezidenta direktīvas un aģentūras politikas virzieni, kas paredz Nacionālā Izlūkošanas direktora biroja (NIDB) vēstulē aprakstītos ierobežojumus un aizsardzības pasākumus, vai — neatbilstības gadījumā —, ka šāda neatbilstība ir novērsta."[61] Atbilde „neapstiprinās un nenoliegs, vai indivīds ir ticis novērots; ombuds arī neapstiprinās konkrēto piemēroto tiesiskās aizsardzības līdzekli."[62] Attiecībā uz jautājumu, kā ombuds veic izmeklēšanu, tiek paskaidrots, ka privātuma vairoga ombuds „cieši sadarbosies ar citām Amerikas Savienoto Valstu valdības amatpersonām, tostarp atbilstošām neatkarīgām pārraudzības struktūrām"[63], un konkrētāk „varēs cieši koordinēt darbību ar NIDB, Tieslietu ministriju un citām ministrijām un aģentūrām, kas ir attiecīgi iesaistītas Amerikas Savienoto Valstu nacionālās drošības garantēšanā, kā arī ģenerālinspektoriem, Likuma par informācijas brīvību īstenošanas amatpersonām un pilsonisko brīvību un privātuma aizsardzības amatpersonām"[64]. Koordinēšana būs tāda, lai nodrošinātu, ka privātuma vairoga ombuds var nosūtīt atbildi, iekļaujot iepriekš aprakstītos apstiprinājumus.

3.5.3.2. Jaunā ombuda mehānisma izvērtējums

Darba grupa novērtē Eiropas Komisijas un ASV valdības pieliktās pūles, lai ieviestu jaunu mehānismu tiesiskās aizsardzības līdzekļu iespēju uzlabošanai ASV uzraudzības darbību jomā. Darba grupa saprot, ka šī mehānisma kā starptautisko attiecību jaunuma sakaru izlūkošanas vai nacionālās drošības jomā izvērtējumam ir īpaša nozīme.

Šajā sadaļā DG29 izvērtēs, kā privātuma vairoga ombuds ir saistīts ar indivīdiem obligātajām prasībām, pieprasot tiesisko aizsardzību, kā to nosaka harta, ECTK un Eiropas tiesu prakse.

---

[60] b. ES individuālo sūdzību izskatīšanas struktūra, veicot turpmāk aprakstītās darbības, nodrošinās, ka pieprasījums ir pilnīgs:
i) pārbaudīs indivīda identitāti un to, vai viņš/viņa rīkojas savā vārdā, nevis kā valdības vai starpvaldību organizācijas pārstāvis;
ii) nodrošinās, ka pieprasījums ir sagatavots rakstiski un tajā ir iekļauta šāda pamatinformācija:
* visa pieprasījuma pamatinformācija,
* prasītās informācijas vai tiesiskās aizsardzības līdzekļa veids,
* iespējami iesaistītās Amerikas Savienoto Valstu struktūras, ja tādas ir, un
* citi pasākumi, kas veikti, lai iegūtu prasīto informāciju vai tiesiskās aizsardzības līdzekli, un ar šiem pasākumiem saistītā reakcija.
iii) pārbaudīs, vai pieprasījums attiecas uz datiem, par kuriem ir pamatoti uzskatīt, ka tie ir pārsūtīti no ES un Amerikas Savienotajām Valstīm saskaņā ar privātuma vairogu, *SCC, BCR*, atkāpēm vai iespējamām turpmākām atkāpēm;
iv) sākotnēji konstatēs, vai pieprasījums nav maznozīmīgs, apgrūtinošs vai iesniegts ļaunticīgi.

[61] Privātuma vairoga III pielikums, 4.e punkts

[62] Privātuma vairoga III pielikums, 4.e punkts

[63] Privātuma vairoga III pielikums, 2.a punkts

[64] Privātuma vairoga III pielikums, 2.a punkts

3.5.3.3. Vai ombuda izveidošana pati par sevi var būt pietiekama?

Iesākumā ir jāuzdod jautājums, vai ombuda izveidošana vispār var tikt uzskatīta par atbilstīgu hartas 47. pantam, kurā minētas tiesības uz efektīvu tiesisko aizsardzību un taisnīgu tiesu[65], vismaz gadījumos, kad nav citas iespējas gūt efektīvu tiesisko aizsardzību. Tas ir svarīgi, jo EST *Schrems* lietā, svarīgajā 95. apsvērumā, atsaucas uz hartas 47. pantu, nesniedzot norādi, ka 47. pants būtu jāsaprot atšķirīgi uzraudzības pasākumu kontekstā. Gluži otrādi, EST jau ir piemērojusi hartas 47. pantu attiecīgi nacionālās un starptautiskās drošības[66] uzraudzības pasākumiem *Kadi II* lietā[67].

Tomēr ECT judikatūrā skaidri noteikts, ka tiesiskās aizsardzības līdzekļi parastajās tiesās nav priekšnoteikums, lai apsvērtu uzraudzības shēmu atbilstību 8. pantam (un ECTK 13. pantam).[68] Drīzāk Tiesa saskaņā ar 8. pantu kā nepieciešamo uzraudzības darbību aizsardzības līdzekli ir noteikusi tiesiskās aizsardzības iespēju citās iestādēs. Tomēr ECT ir augstas prasības attiecībā uz citām iestādēm, kuras nodrošina efektīvu tiesisko aizsardzību, nosakot, ka šādai iestādei ir jābūt „neatkarīgai no uzraudzību veicošajām iestādēm, un tai ir jābūt pietiekamām pilnvarām un kompetencei, lai īstenotu efektīvu un nepārtrauktu kontroli"[69].

Lietās *Klass* un *Kennedy* ECT sniedz ieskatu, ko šīs prasības varētu nozīmēt slepenas uzraudzības kontekstā, kad datu subjekts nav informēts par viņa/viņas datu apstrādi. Abos spriedumos ECT iestādes uzskata par neatkarīgām, jo īpaši no iestādēm, kuras veic uzraudzību, kā arī no jebkuras citas iestādes sniegtajām norādēm[70]. Konkrētāk lietā *Kennedy* tiesa atzina par neatkarīgu un objektīvu iestādi, kas bija pieņēmusi savu reglamentu un ko veidoja dalībnieki, kuri ieņem vai ieņēma augstu tiesu varas amatu vai arī bija pieredzējuši juristi[71].

Veicot indivīdu iesniegto sūdzību pārbaudi, iestādēm abos spriedumos bija piekļuve visai būtiskajai informācijai, tostarp slēgtiem materiāliem. Visbeidzot abām iestādēm bija pilnvaras novērst neatbilstības.[72]

Papildus jautājumam, vai ombudu vai uzskatīt par „tiesu", hartas 47. panta 2. punkta piemērošana norāda uz vēl vienu sarežģījumu, nosakot, ka tiesai ir jābūt „likumā noteiktai".

[65] Pamattiesību hartas skaidrojumos turklāt ir noteikts, ka 47. pants ir jāinterpretē kā garantija tiesībām uz efektīvu lietas izskatīšanu tiesā (Pamattiesību hartas skaidrojums, Paskaidrojums par 47. pantu ((2007/C 303/02)).
[66] *Kadi* II, 97. un 100. punkts: visu Savienības tiesību aktu, tostarp to, kuri izstrādāti, lai īstenotu Drošības padomes saskaņā ar Apvienoto Nāciju hartas VII sadaļu pieņemtās rezolūcijas, tiesiskumu pārbauda Eiropas Savienības tiesas (VII sadaļa attiecas uz pasākumiem saistībā ar miera apdraudējumu, miera pārkāpumiem un agresijas aktiem).
[67] Apvienotās lietas C-584/10 P, C-593/10 P un C-595/10 P, Eiropas Komisija un Apvienotā Karaliste pret *Kadi,* 2013. gada 18. jūlijs
[68] ECTK 13. pants uzliek dalībvalstīm par pienākumu nodrošināt, ka „ikvienam, kura tiesības un brīvības (..) tikušas pārkāptas, ir nodrošināta efektīva lietas izskatīšana valsts iestādē". ECT lietas *Klass* 56. un 67. punktā precizējusi, ka šai iestādei nav obligāti jābūt tiesu iestādei.
69 *Klass,* 56. un 67. punkts.
[70] ECT, *Klass,* 21. un 53. punkts.
[71] G10 Komisija (sprieduma izdarīšanas laikā) sastāv no trim locekļiem, un tās priekšsēdētājam jābūt kvalificētam ieņemt tiesu varas amatu, *Klass,* 21. un 53. punkts).
[72] ECT, *Kennedy* 167. punkts; *Klass,* 21. un 53. punkts.

Tomēr ir apšaubāms, vai memorands, kurā izklāstīti jaunā mehānisma darbības principi, ir uzskatāms par „likumu".

Rezultātā, ņemot vērā pēc būtības līdzvērtīgas aizsardzības principu, tā vietā, lai izvērtētu, vai ombudu oficiāli var uzskatīt par likumā noteiktu tiesu, darba grupa nolēma padziļināti pievērsties judikatūras niansēm attiecībā uz konkrētām prasībām, kas jāizpilda, lai „tiesiskās aizsardzības līdzekļus" vai „tiesisko aizsardzību" varētu uzskatīt par atbilstīgu hartas 7., 8.un 47. pantā un ECTK 8. (un 13.) pantā noteiktajām pamattiesībām. Turpmākajā analīzē, apspriežot jaunā mehānisma piemērošanas jomu, darba grupa pievērsīsies šādiem kritērijiem: prasībai iesniegt pieprasījumu ombudam un saņemt atbildi (tiesībspēja), ombuda neatkarība, tā izmeklēšanas pilnvaras piekļūt nepieciešamajiem materiāliem, tostarp klasificētiem dokumentiem, un pieprasīt palīdzību citām aģentūrām un, visbeidzot, tiesības novērst neatbilstības.

3.5.3.4. Ombuda mehānisma piemērošanas joma

Attiecībā uz piekļuvi ombuda mehānismam DG29 uzskata, ka uz visām ES tiesību aktiem pakļautajām personām ir jāattiecina privātuma vairoga ietvaros noteiktie aizsardzības līdzekļi. Nebūtu pieņemama diferencēšana, balstoties uz tautību, jo īpaši ņemot vērā, ka ES pamattiesības attiecas uz visiem, ne tikai uz ES pases turētajiem. III pielikumā ir minēts „ES indivīds", tālāk nedefinējot, kas tas ir. Darba grupa pauž nožēlu par šo neskaidrību un ierosina precizēt to tādā izpratnē, ka visām personām, kas pakļautas ES tiesību aktiem, ir tiesības panākt, ka ombuds izskata viņu pieprasījumu atbilstoši memorandā izklāstītajiem nosacījumiem. Turklāt Komisijai un ASV būtu jāpievēršas jautājumam, kādā mērā privātuma vairogs attieksies arī uz EEZ un Šveices pilsoņiem/iedzīvotājiem, uz kuriem agrāk attiecās drošības zonas shēma.

Turklāt DG29 atzīmē zināmas neskaidrības par ombuda mehānisma piemērošanas jomu. Lai arī memorandā ir noteikts, ka ombuds izskata pieprasījumu saistībā ar no ES uz ASV nosūtīto datu nacionālo drošību saskaņā ar visiem nosūtīšanas rīkiem, kas pieejami ES tiesību aktos, memorandā arī vienlīdz skaidri ir noteikts mehānisms „saistībā ar sakaru izlūkošanu". Pēdējais termins vedina domāt, ka tas attiecas tikai uz tādiem datu nosūtīšanas gadījumiem, kad dati vākti, izmantojot sakaru izlūkošanas rīkus, kas savukārt noved pie jautājuma, vai, piemēram, ĀIUL ietvaros vāktie dati ir „sakaru izlūkdati". Tā tas, šķiet, ir attiecībā uz 702. pantu, kā paskaidrots NIDB apsvērumos, 10. lpp.[73]. Tomēr DG29 izsaka nožēlu, ka termina „sakaru izlūkošana" izmantošana rada nevajadzīgas neskaidrības šajā kontekstā.

Darba grupas izpratnē ombuda mehānisms arī neattiecas uz tiesībaizsardzības aģentūru pieprasījumiem, kas saistīti ar piekļuvi.[74] Ja tā ir, nav skaidrs, vai šis mehānisms attiektos uz pieprasījumiem, kurus iesniedz dažas aģentūras, jo īpaši CIP.

[73] Privātuma vairoga VI pielikums, 10. punkts
[74] Memorands par ombuda izveidi, 1. lpp.

3.5.3.5. Tiesībspēja un pieprasījuma procedūra

Sākt tiesvedību parastajās Amerikas Savienoto Valstu tiesās pret ASV valdības veiktiem uzraudzības pasākumiem ir ļoti grūti. Darba grupa ir informēta, ka Augstākā tiesa noraidījusi tiesībspēju izlūkošanas jautājumu lietās, kad pieteicējs nav spējis pierādīt individuālu, „konkrētu, precīzu un faktisku vai nenovēršamu kaitējumu".[75] Šajā sakarā ombuda izveide ir svarīgs solis, radot papildu tiesiskās aizsardzības iespēju veidus, kas savādāk nepastāvētu. Tādēļ darba grupa atzinīgi novērtē 3. punkta c) apakšpunktā iekļauto precizējumu. Balstoties uz šo sadaļu, lai iesniegtu pieprasījumu jaunā mehānisma ietvaros, vairs nav nepieciešams pierādīt, ka pieprasītāja datiem ir piekļūts, izmantojot sakaru izlūkošanas darbības.

Darba grupa lielā mērā atbalsta sūdzības iesniedzēja identifikācijas procedūru ombuda mehānismā. Ir loģiski veikt identifikāciju ES teritorijā, jo šāda procedūra tiek piemērota arī piekļuves mehānismam saskaņā ar ES-ASV TFIP2 līgumu. Tomēr darba grupa neizprot, kādēļ pārbaudi ES teritorijā jāveic „dalībvalstu iestādēm, kuru kompetencē ir nacionālo drošības dienestu pārraudzība". Pirmkārt, maz ticams, ka saskaņā ar Līguma par Eiropas Savienību 4. panta 2. punktu Eiropas Komisijai būtu iespēja uzdot šādu uzdevumu iestādēm, jo skaidri zināms, ka tas ir dalībvalstu kompetencē.

Turklāt, ņemot vērā dalībvalstīs pastāvošo nacionālās drošības dienestu uzraudzības mehānismu daudzveidību, attiecīgo iestāžu iesaiste var nopietni ietekmēt šīs sistēmas efektivitāti dalībvalstu pilsoņiem. Piemēram, gadījumos, ja vairākas iestādes ir atbildīgas par nacionālās drošības dienestu pārraudzību un indivīdam ir grūti identificēt attiecīgo, ja piemērojamie valstu tiesību akti nesniedz indivīdiem iespēju sazināties ar attiecīgo pārraudzības iestādi vai ja šīs iestādes nav izveidotas tā, lai tās varētu veikt pietiekamības lēmuma projektā tām uzticētos uzdevumus[76]. Ņemot vērā DAI iesaisti privātuma vairoga piemērošanā un pārraudzībā, kā arī to līdzīgās funkcijas TFIP2 līguma ietvaros, ir loģiskāk šo uzdevumu uzticēt dalībvalstu nacionālajām datu aizsardzības iestādēm. Darba grupa uzsver, ka tā neuzskata par ticamu situāciju, ka privātuma vairoga ombuds apstrādā klasificētu informāciju, jo viņa atbilde norāda tikai „atbilstību vai neatbilstību, kas tikusi novērsta".

3.5.3.6. Neatkarība

Valsts sekretāra apsvērumos skaidri norādīts, ka ombuda funkcijas pildīs valsts sekretāra vietniece. Viņu ieceļ prezidents un apstiprina Senāts. Ombuda funkcijām nav nepieciešams papildu apstiprinājums; pietiek piešķirt ombuda funkcijas. Sekretāra vietnieci pēc valsts sekretāra pieprasījuma ombuda amatā ieceļ ASV prezidents, un sekretāra vietnieces amatā viņu apstiprina ASV Senāts. Kā uzsvērts vēstulē un memorandā, ombuds ir „neatkarīgs no ASV izlūkdienestiem". Tomēr DG29 apšauba, vai ombuds ir izveidots tam vispiemērotākajā ministrijā. Šķiet, ir nepieciešamas noteiktas zināšanas un izpratne par izlūkdienestu darbības principiem, lai efektīvi pildītu ombuda funkcijas, un tai pašā laikā nepieciešams būt pietiekamā attālumā no izlūkdienestiem, lai varētu strādāt neatkarīgi.

[75] *Clapper v. Amnesty International USA*, 568 U.S. ___ (2013) II., 10. lpp.
[76] Piemēram, dažās ES dalībvalstīs indivīdi var piekļūt nacionālās drošības dienestu īpašumā esošai informācijai tikai, iesniedzot pieprasījumu Augstākās tiesas tiesnesim.

Privātuma vairogā nav paredzēti konkrēti kritēriji ombuda atlaišanai. Tādējādi darba grupas izpratnē ombudu var atlaist tieši tāpat kā šo personu var atbrīvot no valsts sekretāra vietnieka pienākumiem, kas, iespējams, var apdraudēt ombuda neatkarību.

Acīmredzami valsts sekretāra vietnieka nozīmēšanas ombuda amatā neatkarība atšķiras no parastas tiesas jurisdikcijas noteikšanas indivīda tiesiskajai aizsardzībai. Tādējādi rodas jautājums, vai ombudu neatkarības izteiksmē var uzskatīt par vienlīdzīgu citām neatkarīgām pārraudzības struktūrām, kuras atzītas par atbilstošām. Uzraudzības kontekstā par tādām jo īpaši uzskatītu Apvienotās Karalistes Izmeklēšanas pilnvaru tiesu (IPT) un Vācijas G10 Komisiju.

Lai to izvērtētu, nepieciešama papildu „neatkarīgajam" piešķirto pilnvaru analīze.

3.5.3.7. Izmeklēšanas pilnvaras

Lietā *Kadi* II attiecībā uz hartas 47. pantu EST lēma, ka „attiecīgajai personai jāvar uzzināt attiecībā uz to pieņemtā lēmuma pamatojumu vai nu pašā lēmumā, vai vēlākā paziņojumā pēc šīs personas pieprasījuma, neskarot kompetentās tiesas tiesības lūgt attiecīgajai iestādei iesniegt tai šo informāciju, tā, lai viņa vislabākajā veidā varētu aizstāvēt savas tiesības".[77] Eiropas Savienības tiesām ir jāpārliecinās, ka šis lēmums ir pieņemts, balstoties uz pietiekami drošu faktisko pamatu[78]. Tiesa arī skaidri nosaka, ka „[...] informācijas vai pierādījumu slepenība vai konfidencialitāte nav derīga iebilde", vismaz ne Eiropas Savienības tiesās[79]. Tādēļ darba grupa secina, ka ombudam ir jāsniedz informācija un pierādījumi, uz kuriem balstīti veiktie pasākumi, lai atbilstu EST izvirzītajām prasībām[80].

Pagaidām nav skaidrs ombuda izmeklēšanas pilnvaru apjoms. Ne Komisijas lēmuma projekts, ne Valsts departamenta sniegtais III pielikums nevieš skaidrību šajā jautājumā. Ciktāl tas saprotams darba grupai, ombudam būtu jāsaņem pietiekama informācija, lai tas varētu noteikt, vai drošības dienestu veiktā datu apstrādes operācija noris saskaņā ar likumu, un ja ne, lai varētu novērst neatbilstību. Ne Valsts departamenta vēstulē, ne Komisijas lēmuma projektā nav precizēts, vai ombudam būtu tieša piekļuve par attiecīgo personu iegūtajai informācijai, ļaujot veikt savu izmeklēšanu, vai arī viņam/viņai būs jāpaļaujas tikai uz citu ASV valdības amatpersonu sniegto informāciju.

3.5.3.8. Korektīvās pilnvaras

Memorands nevieš skaidrību, kādā veidā ombuds varēs panākt neatbilstības novēršanu. Apvienojumā ar skaidrības trūkumu par izmeklēšanas pilnvarām, vēl jo vairāk nav skaidrs, kādā mērā ombuds varēs efektīvi uzdot neatbilstības novēršanu un kāds būtu šādas īstenošanas rezultāts. Vai tas varētu nozīmēt, ka dati, kas iegūti neatbilstīgā veidā (t.i., nelikumīgi) vairs nekādā procedūrā nedrīkst tikt izmantoti un ir dzēšami?

---

[77] *Kadi* II 100. punkts.
78 *Kadi* II 119. punkts.
79 *Kadi* II 125. punkts.
[80] *Kadi* II 122. punkts. lai gan attiecīgajai iestādei nav jāsniedz visa informācija un pierādījumi, uz kuriem balstīts pasākums.

Turklāt darba grupas izpratnē privātuma vairogs nesniedz nekādas pārsūdzības vai ombuda „lēmuma" pārskatīšanas iespējas.

Visbeidzot, attiecībā uz ombuda un sūdzības iesniedzēja saziņu — pēc sūdzības izskatīšanas ombuds nedrīkst atklāt, vai izlūkdienesti ir rīkojušies prettiesiski. Sniegtā atbilde vienmēr būs viena un tā pati, un tā būs vispārīga. Lietā *Kadi* II EST lēma, ka kompetentai iestādei (kā pārraudzības struktūrai) ir pienākums sniegt jebkādu apstākļus ietverošu pamatojumu, lai arī LESD 296. pants nepieprasa detalizētu atbildi[81].

3.5.4. Secinājumi

Iedarbīgu tiesiskās aizsardzības līdzekļu pastāvēšana indivīdiem joprojām rada bažas DG29. Pirmkārt, pietiekamības lēmuma projektā nav sniegta skaidra atbilde uz jautājumu, kādās situācijās un ar kādiem priekšnoteikumiem indivīdi var celt prasību, lai noteiktu savas tiesības.

DG29 atzīst un novērtē alternatīva tiesiskās aizsardzības mehānisma jeb ombuda ieviešanu, kas iezīmē unikālu attīstību ES un trešās valsts attiecībās. Neskarot iepriekšminēto nepieciešamību precizēt terminu „ES indivīdi", mehānisms sniedz papildu iespējas tiem, kuri vēlas saņemt ASV administrācija tiesisko aizsardzību, lai pārliecinātos, ka pieteicēja personas dati tiek apstrādāti atbilstīgi ASV tiesību aktiem.

Vienlaikus, izvērtējot ombuda atbilstību neatkarīgas tiesas standartiem hartas 47. panta izpratnē un saskaņā ar EST un ECT uzraudzības lietu judikatūrā noteiktajām prasībām, DG29 atzīmē būtiskas nepilnības. Pirmkārt, pastāv bažas, vai ombudu var uzskatīt par (oficiāli un pilnībā) neatkarīgu, jo īpaši, pateicoties salīdzinoši vienkāršajai pēc politiskajiem kritērijiem iecelto amatpersonu nomaiņai. Otrkārt, saglabājas bažas par ombuda pilnvarām īstenot efektīvu un nepārtrauktu kontroli. Balstoties uz III pielikumā pieejamo informāciju, DG29 nevar izdarīt secinājumu, ka ombudam vienmēr būs tieša piekļuve jebkādai informācijai, datnēm un IT sistēmām, kas nepieciešama, lai izdarītu savu izvērtējumu, ne arī, ka ombuds varēs uzdot atbildīgajām izlūkošanas aģentūrām izbeigt neatbilstīgu datu apstrādi, jo īpaši domstarpību gadījumā par to, vai datu apstrāde atbilst likumam. Iespējams, turpmāks ombuda stāvokļa un pilnvaru precizējums varētu kliedēt DG29 bažas.

3.6. Noslēguma piezīmes par ASV nacionālās drošības iestādēm piemērojamajiem aizsardzības pasākumiem un ierobežojumiem

Vispirms DG29 uzteic Komisiju un ASV iestādes par pieliktajām pūlēm pārredzamības palielināšanai attiecībā uz ASV uzraudzības programmu iespējamajām sekām uz privātuma vairoga ietvaros vai arī ar jebkura cita nosūtīšanas rīka palīdzību nosūtītajiem datiem. Kopš Snoudena (*Snowden*) atklātajiem dokumentiem 2013. gadā ir sperti būtiski soļi. Tomēr DG29 atzīmē, ka bažas saglabājas. Ir nepieciešams sniegt papildu paskaidrojumus un precizējumus vismaz par tiesībām un pienākumiem privātuma vairoga ietvaros.

[81] *Kadi* II 116. punkts.

Divi galvenie DG29 apsvērumi ir fakts, ka ASV iestādes neizslēdz masveida un nekritisku datu vākšanu, un ombuda stāvokļa un pilnvaru detalizēta apraksta trūkums. Turklāt valstu DAI, nevis izlūkošanas aģentūru pārraudzības struktūrām, būtu jābūt kompetentām uzsākt procesu pie ombuda indivīda vārdā. Papildus tam, lai gan DG29 atzinīgi novērtē mēģinājumus novērst DAI celtās iebildes, turpmāku aizsardzības līdzekļu ieviešana būtu apsveicama, lai nodrošinātu, ka ASV uzraudzības programmu radītie ierobežojumi ir nepieciešami demokrātiskā sabiedrībā.

4. PRIVĀTUMA VAIROGA TIESĪBAIZSARDZĪBAS GARANTIJU IZVĒRTĒJUMS

4.1. Ievads

Attiecībā uz publisku piekļuvi personas datiem tiesībaizsardzības nolūkos DG29 atzīmē, ka privātuma vairoga II pielikumā iekļautie privātuma principi satur drošības zonas privātuma principos iekļautajām atkāpēm līdzvērtīgas atkāpes. Tādējādi atkāpju vispārējā būtība tiek saglabāta, kas nozīmē, ka jaunie privātuma vairoga principi ļauj ierobežot to personu, kuru datu tiek nosūtīti no ES uz ASV, pamattiesības, „balstoties uz nacionālās drošības apsvērumiem un sabiedrības interesēm vai Amerikas Savienoto Valstu tiesību aktiem.”[82]

Vienu no galvenajām drošības zonas kritikām *Schrems* lietā tiesa veltīja faktam, ka tajā „nav nekādu konstatējumu par ASV štatu pieņemtu noteikumu pastāvēšanu, kas paredzēti to personu, kuru datu tiek nosūtīti no ES uz ASV, pamattiesību ierobežojumu ierobežošanai”.

Tādēļ DG29 atzinīgi novērtē ASV administrācijas centienus sniegt dziļāku ieskatu tiesiskajā regulējumā attiecībā uz iejaukšanos personas datos, kas tiek nosūtīti privātuma vairoga ietvaros, tiesībaizsardzības nolūkos, tostarp par piemērojamajiem ierobežojumiem un aizsardzības līdzekļiem. Vienlaikus DG29 uzsver, ka tā skata publiskās piekļuves jautājumu, ņemot vērā faktu, ka jebkādi pamattiesību uz privāto dzīvi un datu aizsardzību ierobežojumi demokrātiskā sabiedrībā ir jāpamato. Tādēļ DG29 ir analizējusi privātuma vairoga tiesībaizsardzības garantijas, izmantojot šī atzinuma 1.2. sadaļā sniegto satvaru.

4.2. Eiropas pamatgarantiju piemērošana tiesībaizsardzības iestāžu piekļuvei datiem, kas ir korporāciju valdījumā

4.2.1 Tiesībaizsardzības iestāžu piekļuvei personas datiem jānoris saskaņā ar tiesību aktiem un balstoties uz skaidriem, precīziem un pieejamiem noteikumiem

Privātuma vairoga VII pielikumā ir vēstule no ASV Tieslietu ministrijas, kurā „sniegts īss pārskats par galvenajiem izmeklēšanas instrumentiem, ko izmanto, lai krimināltiesību piemērošanas vai sabiedrības interešu (civiltiesisku un regulatīvu) ievērošanas nolūkos iegūtu no Amerikas Savienoto Valstu uzņēmumiem komercdatus un citu reģistrēto informāciju”.

Visas VII pielikumā minētās procedūras izriet tieši no ASV Konstitūcijas (ceturtā labojuma), no likumiem un procesuālajiem tiesību aktiem vai arī no Tieslietu ministrijas vadlīnijām un

[82] *Schrems*, 87. punkts

noteikumiem. Tomēr VII pielikumā nav konkrēti minēti visi likumi, kuri šīs procedūras paredz, tā vietā sniedzot īsu pašu procedūru aprakstu. VII pielikumā ir arī minēts, ka „uzņēmumi, ņemot vērā savas nozares specifiku un to rīcībā esošo datu veidus, var apstrīdēt no administratīvajām aģentūrām saņemtos datu pieprasījumus, arī atsaucoties uz citiem juridiskajiem pamatiem", sniedzot vairākus neizsmeļošus piemērus, tādus kā Banku slepenības likums, Likums par godīgu kredītinformāciju un Likums par tiesībām uz finansiālo privātumu.

DG29 atzīmē, ka likumu, procedūru un noteikumu satvars ir sadrumstalots un atbilstošā juridiskā bāze attiecīgajam piekļuves pieprasījumam būs atkarīga no tam nepieciešamo datu būtības, uzņēmuma veida, tiesiskā procesa veida (kriminālprocess, administratīvs, saistīts ar sabiedrības interesēm), kā arī no piekļuves pieprasījumu iesniegušā subjekta būtības.

Tā kā visi tiesībaizsardzības iestāžu piekļuvi privātuma vairoga ietvaros nosūtītajiem datiem ierobežojošie noteikumi balstīti Konstitūcijā, likumos vai Tieslietu ministrijas pārredzamajos noteikumos, DG29 ņem vērā šo noteikumu pieejamības pieņēmumu. Tomēr noteikumu skaidrību un precizitāti iespējams izvērtēt tikai katram atsevišķam procesa veidam un piekļuves pieprasījumam. Tādēļ DG29 ar nožēlu atzīmē, ka, balstoties uz privātuma vairoga VII pielikumā pieejamo informāciju un lēmuma projekta konstatējumiem, šādu izvērtējumu šobrīd nav iespējams veikt.

4.2.2. Ir jāpierāda vajadzība un samērīgums attiecībā uz sasniedzamajiem likumīgajiem mērķiem

DG29 atzīmē, ka pieprasījumu piekļuvei datiem tiesībaizsardzības nolūkos var uzskatīt par likumīga mērķa sasniegšanai atbilstošu. Piemēram, ECTK 8. panta 2. punktā paredzēta iespēja valsts iestādēm ierobežot tiesības uz privātās dzīves aizsardzību „lai aizsargātu (..) sabiedrisko drošību, (...) lai nepieļautu nekārtības vai noziedzību". Tomēr šādi ierobežojumi ir pieļaujami tikai tad, ja tie ir vajadzīgi un samērīgi[83].

Saskaņā ar ECT judikatūru samērīguma princips pieprasa, ka juridiskajiem pasākumiem, ar kuriem ierosina tiesību uz privāto dzīvi un personas datu aizsardzību ierobežojumus, ir jābūt „piemērotiem *ar attiecīgo tiesisko regulējumu* sasniedzamo leģitīmo mērķu īstenošanai, un tie nedrīkst pārsniegt šo mērķu sasniegšanai vajadzīgo"[84] (izcēlums mūsu). Tādēļ vajadzības un samērīguma izvērtējums vienmēr veicams saistībā ar tiesību aktos paredzēto konkrēto pasākumu.

ASV iestādes VII pielikumā norāda, ka federālā līmeņa prokurori un izmeklēšanas pārstāvji var piekļūt organizāciju dokumentiem un citai ierakstu informācijai, „īstenojot dažādus obligātos juridiskos procesus, tostarp, iesniedzot zvērināto pavēstes, administratīvās pavēstes un kratīšanas orderus", kā arī iegūt citu sakaru informāciju, „īstenojot federālās kriminālnoziedznieku noklausīšanās un zvanīto tālruņa numuru reģistrētāja izmantošanas

[83] Skatīt Darba dokumentu par Eiropas pamatgarantijām, 7.-9. lpp. Vispārējam vajadzības un samērīguma jēdzienu izvērtējumam skatīt DG29 „Atzinumu Nr. 01/2014 par vajadzīguma un samērīguma jēdziena un datu aizsardzības piemērošanu tiesībaizsardzības nozarē", 2014. gada 27. februāris.
[84] *Digital Rights Ireland Ltd*, 46. punkts, un lietā citētā judikatūra.

pilnvaras”[85]. Turklāt aģentūras, kurām ir civiltiesiska vai regulatīva atbildība, var izsniegt pavēstes organizācijām, pieprasot „uzņēmuma informāciju, elektroniski glabātu informāciju vai citus materiālus vienumus”[86]. VII pielikumā arī precizēts, ka šādus juridisko procesus izmanto galvenokārt, lai iegūtu informāciju no „korporācijām”, kuras atrodas ASV, neskatoties uz to, vai tās ir sertificētas privātuma vairoga ietvaros, vai arī „no datu subjekta valstspiederības”. Citiem vārdiem sakot, šķiet, šīs aizsardzības subjekti ir organizācijas, nevis paši indivīdi.

Papildus VII pielikumam lēmuma projektā, kas balstīts uz privātuma vairoga principiem, ir Komisijas konstatējumi par ASV pastāvošiem noteikumiem, kas paredzēti, lai ierobežotu to personu, kuru dati privātuma vairoga ietvaros tiek nosūtīti no ES un ASV, pamattiesību ierobežojumus.

Jo īpaši lēmuma projekta konstatējumos minēti saskaņā ar ASV Konstitūcijas ceturto labojumu piemērojamie ierobežojumi un aizsardzības līdzekļi, atbilstīgi kuriem tiesībaizsardzības iestādēm principā ir nepieciešams tiesas orderis, kura iegūšanai jāuzrāda pietiekams pamats, lai veiktu kratīšanu vai mantas arestu[87]. Konstatējumos minēts arī fakts, ka izņēmuma gadījumos, uz kuriem neattiecas prasība par orderi, tiesībaizsardzības iestādēm ir jāpiemēro „saprātīguma” kritēriju[88].

Tomēr konstatējumi nevieš skaidrību, kā šie aizsardzības līdzekļi tiks piemēroti ārvalstniekiem. Patiesībā lēmumu projekta apsvērumā ir atzīts, ka „aizsardzība atbilstīgi ceturtajam labojumam neattiecas uz citu valstu pilsoņiem, kuri nedzīvo Amerikas Savienotajās Valstīs”[89]. Tālāk tajos pašos lēmumu projekta punktos ir noteikts, ka citu valstu iedzīvotāji „gūst netiešu labumu no ASV uzņēmumiem, kuri ir personas datu turētāji un pie kuriem tiesībaizsardzības iestādes vēršas ar pieprasījumiem, sniegtās aizsardzības”. Tomēr DG29 ar nožēlu atzīmē, ka šajā konstatējumā nav nevienas atsauces uz juridisku avotu — likumu vai tiesu praksi.

Kopumā DG29 atzīmē, ka komercdatu un citas reģistrētās informācijas iegūšanai no ASV esošām korporācijām krimināltiesību piemērošanas vai sabiedrības interešu (civiltiesisku un regulatīvu) ievērošanas nolūkos (tostarp piekļuves ierobežošanai un aizsardzības līdzekļiem) izmantoto izmeklēšanas rīku sistēma ir sarežģīts pasākumu kopums. Balstoties uz pieejamo informāciju, šobrīd nav iespējams novērtēt sistēmu kopumā. Ir nepieciešams konkrēts atsevišķu gadījumu izvērtējums, lai patiesi varētu novērtēt tiesībaizsardzības izmeklēšanas pasākumu vajadzību un samērīgumu attiecībā pret pamattiesībām uz privāto dzīvi un datu aizsardzību.

[85] VII pielikums, 2. lpp.
[86] VII pielikums, 4. lpp.
[87] Pietiekamības lēmuma projekts, 107. punkts
[88] Privātuma vairogs, 107. punkts
[89] Pietiekamības lēmuma projekts, 108. punkts

4.2.3. Ir jābūt neatkarīgam pārraudzības mehānismam

DG29 atzīmē faktu, ka lielākajai daļa VII pielikumā aprakstīto procedūru ir nepieciešams tiesas lēmums pirms iestādes var uzsākt datu iegūšanu (piemēram, tiesu rīkojumi par zvanīto numuru reģistrētāju un uztveršanas un trasēšanas ierīču izmantošanu, tiesu rīkojumi par novērošanu saskaņā ar Federālo Likumu par telefona sarunu noklausīšanos, kratīšanas orderi —41. noteikums). Tomēr, šķiet, ka ne visiem ir nepieciešama *a priori* tiesas iesaiste. Piemēram, civiltiesiskās un regulatīvās iestādes „var izsniegt pavēstes"[90]. Šādos gadījumos pastāv *ex post* pavēstes saprātīguma tiesu kontroles iespēja, jo „administratīvās pavēstes saņēmējs var apstrīdēt šīs pavēstes izpildi tiesā"[91].

Balstoties uz pieejamo informāciju, DG29 atzīmē, ka saistībā ar tiesībaizsardzības iestāžu piekļuvi datiem, kuru turētāji ir ASV esoši uzņēmumi, pastāv samērā stabils, neatkarīgs pārraudzības mehānisms.

4.2.4. Indivīdam ir jābūt pieejamiem efektīviem tiesiskās aizsardzības līdzekļiem

Kā iepriekš minēts, „aizsardzība atbilstīgi ceturtajam labojumam neattiecas uz citu valstu pilsoņiem, kuri nedzīvo Amerikas Savienotajās Valstīs"[92]. Tas nozīmē, ka citu valstu pilsoņi nevarētu apstrīdēt tiesu orderus vai pavēstes, atsaucoties uz ceturto labojumu. Pietiekamības lēmuma projektā ir noteikts, ka citu valstu iedzīvotāji gūst netiešu labumu no ASV uzņēmumiem, kuri ir personas datu turētāji un pie kuriem tiesībaizsardzības iestādes vēršas ar pieprasījumiem, sniegtās aizsardzības. Tomēr DG29 atzīmē, ka pat, ja šī aizsardzība ir efektīva, tas nenozīmē, ka indivīdiem ir pieejami efektīvi tiesiskās aizsardzības līdzekļi, jo šajā scenārijā efektīvu tiesiskās aizsardzības līdzekļu tiesību subjekts ir uzņēmums, kurš saņem piekļuves pieprasījumu, nevis indivīds, kura datus tas skar.

VII pielikumā nav nekādas papildu informācijas par iespējamajiem, no likumiem izrietošajiem tiesiskās aizsardzības līdzekļiem, kas pieejami citu valstu pilsoņiem, kad iestādes vai uzņēmumi nelikumīgi sniedz vai gūst piekļuvi viņu datu saturam.

DG29 atzinīgi novērtē faktu, ka nesen pieņemtais Likums par tiesisko aizsardzību[93] paredz tiesības uz tiesisko aizsardzību citu valstu pilsoņiem. Šīs tiesības tomēr īstenojamas tikai skaidri definētos prasījumos: tiesības panākt datu labojumus, piekļuvi datiem un advokāta izdevumu segšanu, ja „nozīmētā federālā aģentūra vai komponente" liedz datu labojumu vai piekļuvi šādiem datiem, un tiesības panākt civiltiesisko aizsardzību gadījumos, kad dati izpausti „ar nodomu vai patvaļīgi".

Turklāt lēmuma projekta attiecīgo apsvērumu zemsvītras atsaucēs norādītā ASV judikatūra, jo īpaši *City of Ontario v. Quon*[94], *Maryland v. King*[95] un *Samson v. California*[96], nav būtiska,

[90] VII pielikums, 4. lpp.
[91] VII pielikums, 4. lpp.
[92] Pietiekamības lēmuma projekts, 108. punkts
[93] 2015. gada Likums par tiesisko aizsardzību, H.R. 1428.
[94] *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson v. California*, 547 U.S. 843, 848 (2006).

izvērtējot, vai citu valstu pilsoņi var celt prasību tiesā, lai apstrīdētu viņu privātuma ierobežojuma[97]. Visas lietas skar ASV iedzīvotāju tiesības uz privāto dzīvi, un visās ir iekļauti ASV Augstākās tiesas lēmumi, kas patiesībā ierobežo ceturtā labojuma piemērošanu.

Kopumā DG29 atzīst un atzinīgi novērtē Likuma par tiesisko aizsardzību pieņemšanu, tomēr saglabājas šaubas, vai atsevišķiem datu subjektiem efektīvi tiesiskās aizsardzības līdzekļi ir faktiski pieejami.

4.3. Nobeiguma piezīmes

DG29 apsveic un atzinīgi novērtē ASV administrācijas centienus sniegt dziļāku ieskatu tiesiskajā regulējumā attiecībā uz iejaukšanos personas datos, kas tiek nosūtīti privātuma vairoga ietvaros, tiesībaizsardzības nolūkos, tostarp par piemērojamajiem ierobežojumiem un aizsardzības līdzekļiem.

DG29 atzīmē, ka tiesībaizsardzības iestāžu izmeklēšanas rīku sistēma, tostarp piemērojamie ierobežojumi un aizsardzības līdzekļi, ir plaša un sarežģīta, un privātuma vairogā iekļautā informācija ir īsa. Tādēļ DG29 pauž nožēlu, ka, balstoties uz ierobežoto informāciju (piemēram, privātuma vairoga VII pielikumā un lēmuma projekta konstatējumos), tā šobrīd nevar sniegt piemērojamo noteikumu pieejamības, paredzamības, vajadzības un samērīguma vispārēju izvērtējumu. Neskarot citus DG29 šajā atzinumā izdarītos konstatējumus par privātuma vairogu, šāds izvērtējums varētu būt daļa no privātuma vairoga ikgadējās pārskatīšanas.

Attiecībā uz tiesībaizsardzības iestādēm DG29 atzīmē, ka pastāv samērā stabils un neatkarīgs pārraudzības mehānisms. Turklāt DG29 atzinīgi novērtē Likuma par tiesisko aizsardzību pieņemšanu, sniedzot tiesiskās aizsardzības tiesības citu valstu pilsoņiem. Tomēr DG29 atzīmē, ka šīs tiesības ir ierobežotas. Papildus konstatējumam, ka citu valstu iedzīvotāji nevarētu apstrīdēt tiesā orderus vai pavēstes, atsaucoties uz ceturto labojumu, saglabājas arī bažas, vai tiesībaizsardzības jomā atsevišķiem datu subjektiem būs faktiski pieejami efektīvi tiesiskās aizsardzības līdzekļi.

5. SECINĀJUMI UN IETEIKUMI

DG29 vispirms atzinīgi novērtē faktu, ka piecu mēnešu laikā pēc drošības zonas pasludināšanas par spēkā neesošu, ir sagatavots jauns pietiekamības lēmuma projekts ar vairākiem uzlabojumiem, salīdzinot ar iepriekšējo mehānismu. Darba grupa ir jo īpaši apmierināta ar paaugstināto pārredzamības līmeni, kuru nodrošina ASV Tirdzniecības ministrijas tīmekļa vietnē publicētie divi privātuma vairoga saraksti: vienā sarakstā ir iekļauta

[97] Lietā *Ontario v Quon* tiesa lēma, ka Ontārio pilsētas pašvaldība nepārkāpa savu darbinieku ceturtā labojuma tiesības, jo pašvaldības piekļuve darbinieku attiecīgo privāto ziņojumu saturam bija saprātīga, balstoties uz ar darbu saistītu nolūku un nepārsniedza tvērumu. Lietā *Samson v California* tiesa konstatēja, ka „ceturtais labojums neaizliedz policijas darbiniekam veikt probācijā esošas personas pārmeklēšanu bez aizdomu pamata". Lietā *Maryland v King* tiesa lēma, ka gadījumos, kad darbinieks veic arestu, balstoties uz pamatotām aizdomām, lai aizturētu nopietnā noziegumā aizdomās turamo un viņu nogādātu iecirknī paturēšanai apcietinājumā, aizturētā siekalu uztriepes noņemšana DNS analīzei, pirkstu nospiedumu noņemšana, fotografēšana un likumīgas policijas aizturēšanas procedūras uzskatāmas par saprātīgām atbilstīgi ceturtajam labojumam.

informācija par visām organizācijām, kuras ievēro privātuma vairogu, savukārt otrā sarakstā ir informācija par organizācijām, kas to agrāk ir ievērojušas, taču vairs ne tagad. Tāpat tiek atzinīgi novērtēta paaugstinātais pārredzamības līmenis saistībā ar publisko piekļuvi datiem, kurus nacionālās drošības vai tiesībaizsardzības nolūkiem nosūta privātuma vairoga ietvaros. Visbeidzot DG29 ļoti priecājas uzzināt, ka visiem datu nosūtīšanas uz ASV gadījumiem tiks piemērota vienāda aizsardzība: nepastāv konkrētas likumdošanas normas, kas vienam rīkam piešķirtu priekšrocības, salīdzinot ar citiem.

5.1. Trīs jautājumi, kas vieš bažas

Tomēr saglabājas trīs svarīgi jautājumi, kas vieš bažas un kuri DG29 ieskatā būs jārisina.

Pirmais jautājums — pietiekamības lēmuma projektā izmantotā valoda neuzliek organizācijām par pienākumu izdzēst datus, kad tie vairs nav vajadzīgi. Šis ir būtisks ES datu aizsardzības tiesību aktu elements, lai nodrošinātu, ka dati netiek saglabāti ilgāk nekā tas nepieciešams, lai sasniegtu mērķi, kādam tie tika vākti. Otrkārt, DG29 no VI pielikuma secina, ka ASV administrācija pilnībā neizslēdz turpmāku masveida un nekritisku datu vākšanu. DG29 ir vairākkārt uzsvērusi, ka šāda datu vākšana ir nepamatota indivīdu pamattiesību ierobežošana. Trešais jautājums skar ombuda mehānisma ieviešanu. Lai arī DG29 atzinīgi novērtē šo agrāk nepieredzēto soli, izveidojot papildu tiesiskās aizsardzības un pārraudzības mehānismu indivīdiem, saglabājas bažas par ombuda pilnvaru pietiekamību, lai efektīvi pildītu savus pienākumus. Ir jāprecizē vismaz ombuda pilnvaras un stāvoklis, lai parādītu, ka šis amats ir pilnībā neatkarīgs un var nodrošināt efektīvus tiesiskās aizsardzības līdzekļu neatbilstīgas datu apstrādes gadījumos.

5.2. Ieteicamie precizējumi

Papildus iepriekšminētajiem punktiem DG29 šajā atzinumā ir norādījusi vairākus punktus, kurus pietiekamības lēmumā ir nepieciešams precizēt. Vissvarīgākais attiecas uz nepieciešamību nodrošināt, kā galveno privātuma vairogā izmantoto datu aizsardzības jēdzienu konsekventu definīciju un piemērošanu. Šobrīd tas tā nav. Atzinīgi tiktu novērtēta terminu glosārija ieviešana privātuma vairoga BUJ, iekļaujot definīcijas, par kurām ES un ASV pilnībā vienojušās. DG29 arī secina, ka ES personas datu tālāka nosūtīšana ir nepietiekami regulēta, jo īpaši attiecībā uz tās tvērumu, nolūka ierobežošanu un garantijām, kas piemērojamas nosūtīšanai pārstāvjiem. Attiecībā uz tiesībaizsardzības iestāžu piekļuvi privātuma vairoga datiem, bažas jo īpaši rada tiesību aktu paredzamība, pateicoties plašajai un sarežģītajai ASV tiesībaizsardzības sistēmas būtībai, gan federālā, gan štatu līmenī, un šajā pietiekamības lēmumā ir iekļauta ierobežota informācija.

Privātuma vairogs ir pirmais pietiekamības lēmums, kas ticis izstrādāts kopš konceptuālās vienošanās par Vispārīgās datu aizsardzības regulas tekstu. Tomēr vairāki indivīdiem pieejamā datu aizsardzības līmeņa uzlabojumi nav atspoguļoti privātuma vairogā. Tādēļ DG29 iesaka pārskatīt pietiekamības lēmumu, kā arī pietiekamības lēmumus, kas izdoti citām trešajām valstīm, drīz pēc tam, kad sāk piemērot vispārīgo datu aizsardzības regulu.

DG29 noslēguma ieteikumi attiecas uz kopīgu pārskatīšanu. DG29 atzinīgi novērtē to, ka privātuma vairoga pietiekamības lēmums tiks ik gadu pārskatīts, plaši iesaistot DAI un citas attiecīgās personas. Darba grupa arī novērtētu savlaicīgu vienošanos pirms pirmā pārskata veikšanas par kopīgas pārskatīšanas elementiem, tostarp par visu pušu dalību pārskata ziņojuma izstrādē un prezentācijā.