Pamatnostādnes

Pamatnostādnes 2/2023 par E-privātuma direktīvas 5. panta 3. punkta tehnisko piemērošanas jomu

Versija 2.0

Pieņemts 2024. gada 7. oktobrī

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Versiju vēsture

Versija 1.0	2023. gada 14. novembrī	Pamatnostādņu pieņemšana sabiedriskai apspriešanai
Versija 2.0	2024. gada 7. oktobrī	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas

Kopsavilkums

Šajās pamatnostādnēs EDAK aplūko E-privātuma direktīvas 5. panta 3. punkta piemērojamību dažādiem tehniskiem risinājumiem. Šīs pamatnostādnes papildina 29. panta darba grupas atzinumu 9/2014 par E-privātuma direktīvas piemērošanu pirkstu nospiedumu ņemšanas ierīcēm, un to mērķis ir sniegt skaidru izpratni par tehniskajām darbībām, uz kurām attiecas E-privātuma direktīvas 5. panta 3. punkts.

Jaunu izsekošanas metožu parādīšanās, lai aizstātu esošos izsekošanas rīkus (piemēram, sīkfailus, jo daži pārlūkprogrammu pārdevēji ir pārtraukuši trešo pušu sīkfailu atbalstu) un radītu jaunus uzņēmējdarbības modeļus, ir kļuvusi par būtisku datu aizsardzības problēmu. Lai gan E-privātuma direktīvas 5. panta 3. punkta piemērojamība ir labi paredzēta un īstenota attiecībā uz dažām izsekošanas tehnoloģijām, piemēram, sīkdatnēm, ir jānovērš neskaidrības, kas saistītas ar minētā noteikuma piemērošanu jauniem izsekošanas rīkiem.

Pamatnostādnēs ir noteikti trīs galvenie E-privātuma direktīvas 5. panta 3. punkta piemērojamības elementi (2.1. iedaļa), proti, "informācija", "abonenta vai lietotāja termināliekārta" un "pieejas nodrošināšana" un "informācijas uzglabāšana un uzglabātā informācija". Pamatnostādnēs ir sniegta arī katra elementa detalizēta katra (2.2.–2.6. iedaļa).

Pamatnostādņu 3. iedaļā šī analīze tiek piemērota nepilnīgam lietošanas gadījumu sarakstam, kas atspoguļo izplatītākās metodes, proti:

- URL un pikseļu izsekošana
- Vietējā apstrāde
- Izsekošana, pamatojoties tikai uz IP
- periodiska un mediēta lietiskā interneta (IoT) ziņošana
- Unikālais identifikators

Satura rādītājs

Eiropas Datu aizsardzības kolēģija

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk — "VDAR"),

ņemot vērā EEZ līgumu un jo īpaši tā XI. pielikumu un 37. protokolu, ko groza ar EEZ apvienotās komitejas 2018. gada 6. jūlija lēmumu Nr. 154/2018[1];

ņemot vērā 15. panta 3. punktu Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvā 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē, kas grozīta ar Direktīvu 2009/136/EK (turpmāk — "E-privātuma direktīva" vai "ePD"),

ņemot vērā Reglamenta 12. un 22. pantu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES:

1 IEVADS

1. Saskaņā ar ePD 5. panta 3. punktu "*informācijas uzglabāšanai vai pieejas nodrošināšanai abonenta vai lietotāja termināliekārtā uzglabātai informācijai*" ir atļauta tikai pamatojoties uz piekrišanu vai nepieciešamību konkrētiem minētajā pantā noteiktiem mērķiem. Kā atgādināts ePD 24. apsvērumā[2], šā noteikuma mērķis ir aizsargāt lietotāju termināliekārtas, jo tās ir daļa no lietotāju privātās jomas. No panta formulējuma izriet, ka ePD 5. panta 3. punkts neattiecas tikai uz sīkdatnēm, bet arī uz "līdzīgām tehnoloģijām". Tomēr pašlaik nav visaptveroša to tehnisko darbību saraksta, uz kurām attiecas ePD 5. panta 3. punkts.

2. Saskaņā ar direktīvas 29. pantu izveidotā Darba grupas (turpmāk — "DG29") Atzinumā 9/2014 par e-privātuma direktīvas piemērošanu pirkstu nospiedumu ņemšanas ierīcēm (turpmāk — "DG29 Atzinums 9/2014") jau ir precizēts, ka pirkstu nospiedumu ņemšana ietilpst ePD 5. panta 3. punkta tehniskajā darbības jomā[3], taču, ņemot vērā jauno tehnoloģiju attīstību, ir nepieciešami turpmāki norādījumi attiecībā uz pašlaik izmantotajām izsekošanas metodēm. Pēdējo desmit gadu laikā tehniskā vide ir attīstījusies, arvien vairāk izmantojot operētājsistēmās iestrādātos identifikatorus, kā arī radot jaunus rīkus, kas ļauj uzglabāt informāciju termināliekārtās.

3. Neskaidrības attiecībā uz 5. panta 3. punkta ePD piemērošanas jomu ir radījušas stimulu ieviest alternatīvus risinājumus interneta lietotāju izsekošanai un veicina tendenci apiet 5. panta 3. punktā

[1] Šajā dokumentā atsauces uz "dalībvalstīm" būtu jāsaprot kā atsauces uz "EEZ dalībvalstīm".

[2] "Elektronisko komunikāciju tīklu lietotāju termināliekārtas un jebkāda uzglabātā informācija par šādām terminaiekārtām ir to lietotāju privātās jomas daļa, kam nepieciešama aizsardzība saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju. Tā sauktās spiegprogrammas, neredzamie pikseļi, slēptie identifikatori un citi instrumenti, lietotājam to nezinot, var iekļūt lietotāja termināliekārtā, lai iegūtu pieeju informācijai, lai uzglabātu apslēptu informāciju vai izsekotu lietotāja darbības, un var nopietni pārkāpt šo lietotāju privātās dzīves neaizskaramību. Šādu instrumentu izmantošanu var ļaut tikai likumīgos nolūkos, par šo instrumentu izmantošanu informējot attiecīgajos lietotājus."

[3] DG29 Atzinums 9/2014, 11. lpp.

noteiktos juridiskos pienākumus. Visas šīs situācijas rada bažas un prasa papildu analīzi, lai papildinātu iepriekšējās EDAK vadlīnijas.

4. Šo pamatnostādņu mērķis ir veikt tehnisko analīzi par ePD 5. panta 3. punkta piemērošanas jomu, proti, precizēt, ko tehniski aptver frāze "*informācijas uzglabāšanai vai pieejas iegūšanai abonenta vai lietotāja termināliekārtā uzglabātai informācijai*". Šajās pamatnostādnēs nav aplūkoti apstākļi, kādos uz apstrādes darbību var attiekties ePD paredzētie atbrīvojumi no piekrišanas prasības[4], jo šie apstākļi būtu jāanalizē katrā gadījumā atsevišķi, ņemot vērā attiecīgo(-ās) dalībvalsts transponēšanu(-as) un valstu kompetento iestāžu sniegtos norādījumus.

5. Šo pamatnostādņu pēdējā daļā tiks analizēts nepilnīgs saraksts ar konkrētiem lietošanas gadījumiem.

2 ANALĪZE

2.1 ePD 5. panta 3. punkta piemērošanas galvenie elementi

6. ePD 5. panta 3. punktu piemēro, ja:

   a. **A KRITĒRIJS:** veiktās darbības attiecas uz "*informāciju*". Jāatzīmē, ka izmantotais termins nav "personas dati", bet gan "informācija".

   b. **B KRITĒRIJS:** veiktās darbības ir saistītas ar abonenta vai lietotāja "*termināliekārtu*" (B.1), kas nozīmē nepieciešamību novērtēt "*publisko komunikāciju tīkla*" (B.2) jēdzienu .

   c. **C KRITĒRIJS** veiktās darbības patiešām ir "*uzglabāšana*" (C.1) vai "*pieejas iegūšana*" (C.2). Šos divus jēdzienus var pētīt neatkarīgi, kā atgādināts DG29 Atzinumā 9/2014: *"Vārda "uzglabāts vai piekļūts" lietojums norāda, ka uzglabāšanai un pieejai nav jānotiek vienā un tajā pašā saziņā un tā nav jāveic vienai un tai pašai pusei*[5]*."*

   Skaidrības labad struktūra, kas iegūst pieeju lietotāja termināliekārtā glabātajai informācijai, turpmāk tiks saukta par "pieejas struktūru".

2.2 Jēdziens "informācija" - A kritērijs

7. Kā norādīts A KRITĒRIJĀ, šajā iedaļā tiks sīkāk aprakstīts, ko ietver jēdziens "informācija". Termina "informācija" izvēle, kas ietver plašāku kategoriju nekā tikai personas datu jēdziens, ir saistīta ar e-privātuma direktīvas darbības jomu.

8. ePD 5. panta 3. punkta mērķis ir aizsargāt lietotāju privāto jomu, kā norādīts tās 24. apsvērumā: "*Elektronisko komunikāciju tīklu lietotāju termināliekārtas un jebkāda uzglabātā informācija par šādām termināliekārtām ir to lietotāju privātās jomas daļa, kam nepieciešama aizsardzība saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju*". To aizsargā arī ES Pamattiesību hartas 7. pants.

9. Faktiski scenāriji, kas iejaucas šajā privātajā sfērā, pat neietverot nekādus personas datus, ir skaidri ietverti ePD 5. panta 3. punkta un 24. apsvēruma formulējumā, piemēram, vīrusu glabāšana lietotāja

[4] Kā noteikts ePD 5. panta 3. punkta e) apakšpunktā. "*Tas neliedz jebkādu tehnisku uzglabāšanu vai vienīgi pieeju, lai veiktu vai veicinātu komunikāciju pārraidīšanu elektronisko komunikāciju tīklā, vai kas nepieciešama, lai sniegtu informācijas sabiedrības pakalpojumu, ko skaidri pieprasa abonents vai lietotājs.*"

[5] DG29 Atzinums 9/2014, 8. lpp.

termināliekārtā. Tas liecina, ka jēdziena "informācija" definīcijai nevajadzētu aprobežoties ar īpašību, ka tā ir saistīta ar identificētu vai identificējamu fizisku personu.

10. To ir apstiprinājusi Eiropas Savienības Tiesa: "*Šāda veida aizsardzība attiecas uz jebkādu informāciju, kas glabājas šādās termināliekārtās, neatkarīgi no tā, vai tā ir vai nav personas dati, un tās mērķis ir jo īpaši, kā tas izriet no minētā apsvēruma, aizsargāt lietotājus no riska, ka slēptie identifikatori un citas līdzīgas ierīces iekļūst šo lietotāju termināliekārtās bez viņu ziņas*"[6].

11. Jautājumi par to, vai šīs informācijas izcelsme un iemesli, kādēļ tā tiek glabāta termināliekārtā, ir jāņem vērā, novērtējot ePD 5. panta 3. punkta piemērojamību, ir iepriekš precizēti. Piemēram, DG29 Atzinumā 9/2014: "*Interpretējot to tā, ka trešai personai nav vajadzīga piekrišana, lai piekļūtu šai informācijai vienkārši tāpēc, ka tā to neglabāja, ir nepareizi. Piekrišanas prasība attiecas arī uz gadījumiem, kad tiek piekļūts tikai lasāmai vērtībai (piemēram, pieprasot tīkla interfeisa MAC adresi, izmantojot OS API)*"[7].

12. Visbeidzot, informācijas jēdziens ietver gan datus, kas nav personas dati, gan personas datus neatkarīgi no tā, kā šie dati tiek glabāti un kurš to ir veicis, t. i., vai tos ir glabājusi ārēja struktūra (tostarp arī citas struktūras, kurām nav piekļuves), lietotājs, ražotājs vai jebkurš cits gadījums.

2.3 Jēdziens "abonenta vai lietotāja termināliekārta" - B.1. kritērijs

13. Šīs iedaļas pamatā ir definīcija, kas izmantota Direktīvā 2008/63/EK un uz kuru ir atsauce 2. pantā Direktīvā (ES) 2018/1972, kur "termināliekārta" ir definēta kā: "*iekārta, ko tieši vai netieši pieslēdz pie publiskā telekomunikāciju tīkla saskarpunkta, lai nosūtītu, apstrādātu vai saņemtu informāciju; abos gadījumos (tieši vai netieši) pieslēgumu var izveidot ar vadiem, optisko šķiedru vai elektromagnētiski; pieslēgums ir netiešs, ja iekārta ir starp termināliekārtu un publiskā telekomunikāciju tīkla saskarpunktu*"[8].

14. ePD 24. apsvērumā ir sniegta skaidra izpratne par termināliekārtu lomu saistībā ar aizsardzību, ko piedāvā ePD 5. panta 3. punkts. ePD aizsargā lietotāju privātumu ne tikai attiecībā uz viņu informācijas konfidencialitāti, bet arī aizsargājot lietotāja termināliekārtas integritāti. Šī izpratne palīdzēs interpretēt jēdzienu "termināliekārtas" šajās pamatnostādnēs.

15. ePD 3. pantā noteikts, ka, lai piemērotu ePD, personas datu apstrāde jāveic saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos. Tas nozīmē, ka ierīcei jābūt izmantojamai saistībā ar šādu pakalpojumu un ka, lai to kvalificētu kā termināliekārtu, tai jābūt savienotai vai savienojamai[9] ar publiskā komunikāciju tīkla saskarpunktu. EDAK norāda, ka ar 2009. gadā[10] izdarītajiem grozījumiem e-PD 5. panta 3. punkta tekstā tika paplašināta termināliekārtu aizsardzība, svītrojot atsauci uz "elektronisko komunikāciju tīkla izmantošanu" kā līdzekli, lai uzglabātu informāciju vai iegūtu piekļuvi termināliekārtā uzglabātajai

[6] Tiesas 2019. gada 1. oktobra spriedums Planet 49, lieta C-673/17, ECLI:EU:C:2019:801, 70. punkts.
[7] DG29 Atzinums 9/2014, 8. lpp.
[8] Komisijas Direktīva 2008/63/EK (2008. gada 20. jūnijs) par konkurenci telekomunikāciju termināliekārtu tirgos (Kodificēta versija), 1. Panta 1. punkts.
[9] Tas nozīmē, ka ir tehniskas iespējas pieslēgties tīklam pat tad, ja šis pieslēgums pašlaik nav izveidots.
[10] Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīva 2009/136/EK, ar ko groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem, Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē un Regulu (EK) Nr. 2006/2004 par sadarbību starp valstu iestādēm, kas atbildīgas par tiesību aktu īstenošanu patērētāju tiesību aizsardzības jomā (Teksts attiecas uz EEZ),OV L 337, 18.12.2009., 2. panta 5. punkts un 65. apsvērums.

informācijai. Tāpēc, kamēr ierīcei ir tīkla saskarpunkts, kas to padara par atbilstīgu pieslēgumam (pat tad, ja šāds pieslēgums nav izveidots), ePD 5. panta 3. punkts attiecas uz katru vienību, kas glabātu termināliekārtā jau uzglabāto informāciju un iegūtu piekļuvi tai neatkarīgi no piekļuves termināliekārtai veida un neatkarīgi no tā, vai tā ir pieslēgta vai atvienota no tīkla.

16. Iekārtas, kas ir daļa no paša publiskā elektronisko sakaru tīkla, netiktu uzskatītas par termināliekārtām saskaņā ar ePD 5. panta 3. punktu[11].

17. Termināliekārta var sastāvēt no jebkura skaita atsevišķu aparatūras daļu, kas kopā veido termināliekārtu. Tā var būt vai nebūt fiziski slēgta ierīce, kurā atrodas visa displeja, apstrādes, glabāšanas un perifērijas aparatūra (piemēram, viedtālruņi, klēpjdatori, pie tīkla pieslēgta glabāšanas ierīce, savienoti automobiļi vai savienoti televizori, viedās brilles).

18. ePD atzīst, ka lietotāja termināliekārtā uzglabātās informācijas konfidencialitātes aizsardzība un lietotāja termināliekārtas integritāte attiecas ne tikai uz fizisku personu privātās sfēras aizsardzību, bet arī uz viņu tiesībām uz korespondences neaizskaramību vai juridisko personu likumīgajām interesēm[12]. Tādējādi termināliekārtas, kas ļauj veikt šo korespondenci un juridisko personu likumīgās intereses, ir aizsargātas saskaņā ar e-PD 5. panta 3. punktu.

19. Lietotājam vai abonentam var piederēt, viņš var nomāt vai citādi tikt nodrošināts ar termināliekārtu. Vairāki lietotāji vai abonenti var izmantot vienu un to pašu termināliekārtu.

20. Šo aizsardzību nodrošina ePD attiecībā uz termināliekārtām, kas saistītas ar lietotāju vai abonentu, un tas nav atkarīgs no tā, vai lietotājs ir iestatījis piekļuves līdzekļus (piemēram, ja tas ir uzsācis elektronisko saziņu), vai pat no tā, vai lietotājs ir informēts par minētajiem piekļuves līdzekļiem).

2.4 Jēdziens "publiskais komunikāciju tīkls" — B.2. kritērijs

21. Tā kā situācija, ko regulē ePD, ir saistīta ar "*publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Kopienā*"[13] un termināliekārtas definīcijā ir īpaši minēts jēdziens "*publisks komunikāciju tīkls*", ir būtiski precizēt šo jēdzienu, lai noteiktu kontekstu, kurā piemēro ePD 5. panta 3. punktu.

22. Elektronisko komunikāciju tīkla jēdziens nav definēts pašā ePD. Sākotnēji šis jēdziens tika minēts Direktīvā 2002/21/EK (Pamatdirektīva) par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem[14], kas vēlāk tika aizstāta ar Direktīvas (ES) 2018/1972 (Eiropas Elektronisko komunikāciju kodekss) 2. panta 1. punktu. Tagad tajā ir rakstīts:

> *"elektronisko sakaru tīkls" ir pārraides sistēmas, kas var būt un var nebūt bāzētas uz patstāvīgā infrastruktūra vai centralizētas administrācijas jaudās, un attiecīgos gadījumos komutācijas vai maršrutēšanas ierīces un citi resursi, tostarp tīkla pasīvie elementi, ar kuriem signālus var pārvadīt pa vadiem, radioviļņiem, optiskiem vai citiem elektromagnētiskiem līdzekļiem, tostarp satelītsakaru tīkliem, fiksētiem (ķēžu un pakešu komutācijas, ieskaitot internetu) un mobiliem zemes tīkliem, elektrokabeļu sistēmām, ciktāl tās izmanto signālu pārraides nolūkā, radio un*

[11] Lai noteiktu tīkla robežas dažādos kontekstos, skatiet *BEREC* vadlīnijas par vienotu pieeju tīkla beigu punkta noteikšanai dažādās tīkla topoloģijās (BoR (20) 46).
[12] Patiešām, 2. panta 13. punktā Eiropas Parlamenta un Padomes 2018. gada 11. decembra Direktīvā (ES) 2018/1972 par Eiropas Elektronisko sakaru kodeksa izveidi minētais atgādinājums norāda, ka lietotājs var būt fiziska vai juridiska persona.
[13] ePD 3. pants.
[14] Eiropas Parlamenta un Padomes 2002. gada 7. marta Direktīva 2002/21/EK par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva)

televīzijas apraides nolūkā izmantotajiem tīkliem un kabeļtelevīzijas tīkliem neatkarīgi no pārvadītās informācijas veida.[15]

23. Šī definīcija ir neitrāla attiecībā uz pārraides tehnoloģijām. Elektronisko sakaru tīkls saskaņā ar šo definīciju ir jebkura tīkla sistēma, kas ļauj pārraidīt elektroniskos signālus starp tās mezgliem neatkarīgi no izmantotās iekārtas un protokoliem.

24. Jēdziens "elektronisko sakaru tīkls" saskaņā ar Direktīvu 2018/1972 nav atkarīgs ne no infrastruktūras publiskā vai privātā rakstura, ne no tā, kā tīkls tiek izvērsts vai pārvaldīts ("*kas var būt un var nebūt bāzētas pastāvīgā infrastruktūrā vai centralizētas administrācijas jaudās*"[16].) Līdz ar to elektronisko sakaru tīkla definīcija saskaņā ar Direktīvas 2018/1972 2. pantu ir pietiekami plaša, lai aptvertu jebkura veida infrastruktūru. Tas ietver tīklus, ko pārvalda vai nepārvalda operators, tīklus, ko kopīgi pārvalda operatoru grupa, vai pat *ad hoc* tīklus, kuros termināliekārta var dinamiski pievienoties vai pamest citu termināliekārtu tīklu, izmantojot šaura diapazona pārraides protokolus.

25. Šī tīkla definīcija neparedz nekādus ierobežojumus attiecībā uz termināliekārtu skaitu, kas jebkurā brīdī atrodas tīklā. Atsevišķas tīkla shēmas balstās uz mezgliem, kas pārsūta informāciju ad-hoc veidā uz jau savienotiem mezgliem[17], un kādā brīdī var būt tikai divi vienādranga mezgli, kas sazinās savā starpā. Šādi gadījumi būtu ePD direktīvas vispārējā darbības jomā, ja vien tīkla protokols ļauj turpmāk iekļaut vienādranga lietotājus.

26. Sakaru tīkla publiska pieejamība ir nepieciešama, lai ierīci varētu uzskatīt par termināliekārtu un līdz ar to — lai piemērotu ePD 5. panta 3. punktu. Jāatzīmē, ka tas, ka tīkls ir pieejams ierobežotai sabiedrības daļai (piemēram, abonentiem, neatkarīgi no tā, vai viņi maksā vai ne, saskaņā ar atbilstības nosacījumiem), nepadara šādu tīklu par privātu[18].

2.5 Jēdziens "pieejas nodrošināšana" – C.1. kritērijs

27. Lai pareizi formulētu jēdzienu "pieejas nodrošināšana", ir svarīgi ņemt vērā ePD darbības jomu, kas noteikta tās 1. pantā: "*ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis, un jo īpaši attiecībā uz tiesībām uz privāto dzīvi saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, kā arī jānodrošina šo datu un elektronisko komunikāciju iekārtu un pakalpojumu brīva aprite Kopienā*."

28. Īsumā, ePD ir privātuma saglabāšanas juridiskais instruments, kura mērķis ir aizsargāt sakaru konfidencialitāti un ierīču integritāti. ePD 24. apsvērumā ir precizēts, ka fizisku personu gadījumā lietotāja termināliekārta ir daļa no viņa privātās sfēras un ka piekļuve tajā glabātai informācijai bez lietotāja ziņas var nopietni aizskart viņa privātumu.

29. Arī juridiskās personas ir aizsargātas ar ePD[19]. Līdz ar to jēdziens "pieejas nodrošināšana" saskaņā ar e-PD 5. panta 3. punktu ir jāinterpretē tādā veidā, kas aizsargā šīs tiesības pret trešo personu pārkāpumiem.

---

[15] Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1972 (2018. gada 11. decembris) par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija), dokuments attiecas uz EEZ, 2. panta 1. punkts.

[16] Eiropas Parlamenta un Padomes Direktīva (ES) 2018/1972 (2018. gada 11. decembris) par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija), dokuments attiecas uz EEZ, 2. panta 1. punkts.

[17] Piemēram, tīkla shēma, kas ir iecietīga pret aizkavēšanos un kas īsteno "uzglabāšanas un pārsūtīšanas metodes", piemēram, Briar atvērtā pirmkoda projekts.

[18] Sīkāku analīzi par publisko komunikāciju tīklu identificēšanu skatīt *BEREC* pamatnostādnēs par atvērtā interneta regulas īstenošanu (BoR (20) 112).

[19] ePD 26. apsvērums, sk. iepriekš 17. punktu.

30. Informācijas glabāšana vai pieejas nodrošināšana var būt neatkarīgas darbības, un tās var veikt neatkarīgas struktūras. Lai piemērotu ePD 5. panta 3. punktu, nav nepieciešams, lai vienlaikus būtu gan informācijas glabāšana, gan pieeja jau saglabātai informācijai.

31. Kā norādīts DG29 Atzinumā 9/2014: "*Vārdu "glabāšana vai pieeja" lietojums norāda, ka glabāšanai un pieejai nav jānotiek vienā un tajā pašā saziņā un tā nav jāveic vienai un tai pašai pusei. Tāpēc informācija, ko glabā viena puse (tostarp informācija, ko glabā lietotājs vai ierīces ražotājs), kurai vēlāk piekļūst cita persona, ietilpst 5. panta 3. punkta darbības*jomā."[20] Līdz ar to nav noteikti ierobežojumi attiecībā uz informācijas par termināliekārtām izcelsmi, lai varētu piemērot pieejas jēdzienu.

32. Ikreiz, kad vienība veic pasākumus, lai iegūtu piekļuvi termināliekārtā glabātajai informācijai, piemērojams e-PD 5. panta 3. punkts. Parasti tas nozīmē, ka piekļuves struktūrai proaktīvi jānosūta konkrēti norādījumi termināliekārtai, lai saņemtu atpakaļ paredzēto informāciju. Piemēram, tas attiecas uz sīkdatnēm, kur piekļuves struktūra uzdod termināliekārtai proaktīvi nosūtīt informāciju par katru turpmāko hiperteksta pārneses protokola (HTTP) izsaukumu.

33. Tas attiecas arī uz gadījumiem, kad piekļuves struktūra lietotāja termināliekārtā izplata programmatūru, kas tiek saglabāta un pēc tam proaktīvi tīklā izsauc lietojumprogrammu saskarnes (API) galapunktu. Papildu piemēri varētu būt JavaScript kods, kurā piekļuves struktūra uzdod lietotāja pārlūkprogrammai nosūtīt asinhronus pieprasījumus kopā ar mērķorientēto informāciju. Šāda piekļuve nepārprotami ietilpst ePD 5. panta 3. punkta darbības jomā, jo piekļuves struktūra skaidri uzdod gal iekārtām nosūtīt informāciju.

34. Atsevišķos gadījumos struktūra, kas dod norādījumus termināliekārtām nosūtīt atpakaļ mērķdatus, un struktūra, kas saņem informāciju, var nebūt viens un tas pats. Tas var izrietēt no abu struktūru kopīga mehānisma nodrošināšanas un/vai izmantošanas. Uzdodot ierīcei nosūtīt jau uzglabātu informāciju (piemēram, izmantojot protokolu vai SDK, kas nozīmē,[21] ka termināliekārta proaktīvi nosūta informāciju) padara iespējamu ielaušanos termināliekārtā, tāpēc šāda piekļuve izraisa ePD 5. panta 3. punkta piemērojamību. Kā norādīts DG29 Atzinumā 09/2014, tas var notikt, ja tīmekļa vietne uzdod termināliekārtai nosūtīt informāciju trešās puses reklāmas dienestiem, iekļaujot izsekošanas pikseli[22]. Šis izmantošanas gadījums ir sīkāk aprakstīts 3.1. iedaļā.

2.6 Jēdzieni "informācijas glabāšana" un "uzglabātā informācija" – C.2. kritērijs

35. Informācijas glabāšana ePD 5. panta 3. punkta nozīmē attiecas uz informācijas ievietošanu fiziskā elektroniskā datu nesējā, kas ir lietotāja vai abonenta termināliekārtas daļa[23].

36. Parasti informāciju lietotāja vai abonenta termināliekārtā nesaglabā, citai personai tieši piekļūstot ierīces atmiņai, bet gan uzdodot termināliekārtas programmatūrai ģenerēt konkrētu informāciju. Uzskata, ka uzglabāšanu, kas notiek, izmantojot šādas instrukcijas, tieši iniciē otra puse. Tas ietver tādu jau izveidotu protokolu izmantošanu kā pārlūkprogrammas sīkfailu glabāšana, kā arī pielāgotas programmatūras izmantošanu neatkarīgi no tā, kurš ir izveidojis vai instalējis protokolus vai programmatūru termināliekārtā.

[20] DG29 Atzinums 9/2014, 8. lpp.
[21] SDK ("programmatūras izstrādes komplekts") ir programmatūras izstrādes rīku kopums, kas pieejams, lai atvieglotu lietojumprogrammatūras izveidi.
[22] DG29 Atzinums 9/2014, 9. lpp.
[23] Kā noteikts šo pamatnostādņu 2.3. iedaļā.

37. ePD nenosaka nekādu maksimālo vai minimālo ierobežojumu attiecībā uz laiku, cik ilgi informācijai jāpaliek uz datu nesēja, lai to uzskatītu par uzglabātu, un nenosaka arī maksimālo vai minimālo ierobežojumu attiecībā uz uzglabājamās informācijas apjomu.

38. Tāpat arī glabāšanas jēdziens nav atkarīgs no informācijas nesēja veida, kurā informācija tiek uzglabāta. Tipiski piemēri ir cietie diski ("HDD"), cietvielu diski ("SSD"), elektriski izdzēšama programmējama lasāmatmiņa ("EEPROM") un brīvpiekļuves atmiņa ("RAM"), bet no piemērošanas jomas nav izslēgti arī mazāk tipiski scenāriji, kas ietver tādus datu nesējus kā magnētiskās lentes vai centrālā procesora ("CPU") kešatmiņa. Uzglabāšanas datu nesēju var pieslēgt iekšēji (piemēram, izmantojot SATA savienojumu), ārēji (piemēram, izmantojot USB savienojumu).

39. "Saglabātā informācija" attiecas uz informāciju, kas jau atrodas termināliekārtā, neatkarīgi no šīs informācijas avota vai veida. Tas ietver jebkuru rezultātu, kas izriet no informācijas uzglabāšanas iepriekš minētā ePD 5. panta 3. punkta nozīmē (vai nu tās pašas puses, kas vēlāk iegūtu piekļuvi, vai citas trešās puses). Turklāt tas ietver arī informācijas uzglabāšanas procesu rezultātus, kas neietilpst ePD 5. panta 3. punkta darbības jomā, piemēram: glabāšana termināliekārtā, ko veic pats lietotājs vai abonents, vai aparatūras ražotājs (piemēram, tīkla interfeisa kontrolieru MAC adreses), termināla iekārtā integrēti sensori vai termināla iekārtā izpildīti procesi un programmas, kas var radīt informāciju, kura ir vai nav atkarīga no uzglabātās informācijas vai atvasināta no tās.

3 IZMANTOŠANAS GADĪJUMI

40. Kā norādīts šo pamatnostādņu ievadā,[24]tajās nav analizēts, kā tiek piemēroti ePD 5. panta 3. punktā paredzētie atbrīvojumi no pienākuma saņemt piekrišanu. EDAK atgādina, ka visos gadījumos, kad tiek uzglabāta informācija vai nodrošināta pieeja jau uzglabātajai informācijai, būtu jāizvērtē, vai ir vajadzīga piekrišana un vai varētu piemērot atbrīvojumu saskaņā ar e-PD 5. panta 3. punktu. Tādēļ lasītājam būtu jāapsver atbrīvojumi to lietošanas gadījumā saistībā ar šo tehnisko analīzi.

41. Neskarot konkrēto gadījumu, kādā var izmantot minētās tehniskās kategorijas, kas ir nepieciešamas, lai kvalificētu, vai ir piemērojams ePD 5. panta 3. punkts, ir iespējams neizsmeļošā veidā identificēt plašas identifikatoru un informācijas kategorijas, kas tiek plaši izmantotas un kam var piemērot ePD 5. panta 3. punktu.

42. Tīkla komunikācija parasti balstās uz daudzslāņainu modeli, kas prasa izmantot identifikatorus, lai nodrošinātu pareizu komunikācijas izveidi un veikšanu. Šo identifikatoru paziņošana attālinātiem dalībniekiem tiek veikta, izmantojot programmatūru saskaņā ar apstiprinātiem komunikācijas protokoliem. Kā minēts iepriekš, tas, ka saņēmēja struktūra, iespējams, nav tā struktūra, kas sniedz norādījumus informācijas nosūtīšanai, neizslēdz e-PD 5. panta 3. punkta piemērošanu. Tas var attiekties uz maršrutēšanas identifikatoriem, piemēram, termināliekārtas MAC vai IP adresi, kā arī sesijas identifikatoriem (SSRC, Websocket identifikators) vai autentifikācijas žetoniem.

43. Tāpat lietojumprotokolā var būt vairāki mehānismi, kas nodrošina konteksta datus (piemēram, HTTP galvene, tostarp "pieņemt" lauks vai lietotāja aģents), kešēšanas mehānisms (piemēram, ETag[25]) vai citas funkcijas (viena no tām ir sīkdatnes vai HSTS[26]). Kā arī paļaušanās uz šiem mehānismiem

[24] Sk. 4. punktu iepriekš.
[25] HTTP ETag ir identifikators, kas ļauj iesniegt nosacītu pieprasījumu, pamatojoties uz kešatmiņas klienta datu derīgumu.
[26] HTTP Stingrā transporta drošība (HSTS) ļauj serveriem noteikt, kādi resursi vienmēr jāpieprasa, izmantojot HTTPS savienojumus.

informācijas vākšanai (piemēram, pirkstu nospiedumu noņemšanas[27] vai resursu identifikatoru izsekošanas gadījumā) var novest pie ePD 5. panta 3. punkta piemērošanas.

44. No otras puses, ir daži konteksti, kuros vietējās lietojumprogrammas, kas instalētas termināliekārtā, izmanto kādu informāciju tikai termināla iekšienē, piemēram, viedtālruņa sistēmas API (piekļuve kamerai, mikrofonam, GPS sensoram, paātrinātāja mikroshēmai, radio mikroshēmai, piekļuve vietējiem failiem, kontaktu sarakstam, piekļuve identifikatoriem utt.). Tas varētu attiekties arī uz tīmekļa pārlūkprogrammām, kas apstrādā ierīcē glabātu vai ģenerētu informāciju (piemēram, sīkfailus, vietējo krātuvi, WebSQL vai pat pašu lietotāju sniegto informāciju). Šādas informācijas izmantošana lietojumprogrammā nebūtu uzskatāma par "pieejas nodrošināšanu jau uzglabātai informācijai" ePD 5. panta 3. punkta izpratnē, kamēr informācija netiek iznesta no ierīces, bet, ja šai informācijai vai jebkādiem šīs informācijas atvasinājumiem tiek piekļūts, tiktu piemērots ePD 5. panta 3. punkts.

45. Visbeidzot, dažos gadījumos dalībnieki izplata ļaunprātīgus programmatūras elementus, piemēram, kriptoizraces programmatūru vai, vispārīgāk, ļaunprogrammatūru, izmantojot termināliekārtas apstrādes spējas izplatītāja labā. Minētās ļaunprogrammatūras izplatīšana lietotāja termināliekārtā veidotu "glabāšanu" ePD 5. panta 3. punkta nozīmē. Turklāt, ja programmatūra izveidotu tīkla savienojumu, lai vēlāk nosūtītu informāciju, tā būtu "pieejas nodrošināšana" ePD 5. panta 3. punkta nozīmē.

46. Attiecībā uz šo kategoriju apakškopu, kas rada īpašu interesi vai nu to plašas izmantošanas dēļ, vai tāpēc, ka konkrēts pētījums ir pamatots attiecībā uz to izmantošanas apstākļiem, turpmāk ir sniegta īpaša analīze.

3.1 URL un pikseļu izsekošana

47. Izsekošanas pikselis ir hipersaite uz resursu, parasti attēla datni, kas iestrādāta kādā satura daļā, piemēram, interneta vietnē vai e-pastā. Šim pikselim parasti nav nekāda mērķa, kas būtu saistīts ar pašu pieprasīto saturu; tā vienīgais mērķis ir automātiski izveidot klienta komunikāciju ar pikseļa mitinātāju, kas citādi nebūtu notikusi. Tomēr tas nav sistemātiski, un izsekošanas pikseļus var izveidot arī, pievienojot papildu informāciju hipersaites ielādes attēliem, kas attiecas uz lietotājam rādīto saturu. Komunikācijas nodibināšana nosūta dažādu informāciju pikseļa saimniekam atkarībā no konkrētā lietošanas gadījuma.

48. E-pasta gadījumā sūtītājs var iekļaut izsekošanas pikseli, lai noteiktu, kad saņēmējs izlasa e-pastu. Izsekošanas pikseļi tīmekļa vietnēs var būt saistīti ar struktūru, kas apkopo daudzus šādus pieprasījumus un tādējādi var izsekot lietotāju uzvedībai. Šādi izsekošanas pikseļi var saturēt arī papildu identifikatorus, metadatus vai saturu kā daļu no saites. Šos datu punktus var pievienot tīmekļa vietnes īpašnieks, iespējams, saistībā ar lietotāja darbību šajā tīmekļa vietnē, lai varētu sagatavot analītiskus izmantošanas ziņojumus. Tos var arī dinamiski ģenerēt, izmantojot klienta puses lietojumprogrammas loģiku, ko nodrošina struktūra.

49. Izsekošanas saites var darboties tādā pašā veidā, bet identifikators ir pievienots tīmekļa vietnes adresei. Kad lietotājs apmeklē vienoto resursu vietrādi (URL), mērķorientētā tīmekļa vietne ielādē pieprasīto resursu, kā arī vāc identifikatoru, kas nav būtisks resursu identificēšanai. Tos ļoti bieži izmanto e-komercijas tīmekļa vietnēs, lai noteiktu to ienākošā datplūsmas avota izcelsmi. Piemēram, šādas vietnes var nodrošināt partneriem izsekojamas saites, ko izmantot savā domēnā, lai e-komercijas

[27] Kā minēts ievadā, skatīt saskaņā ar direktīvas 29. Pantu izveidotās Darba grupas Atzinumā 9/2014 par E-privātuma direktīvas piemērošanu ierīču pirkstu nospiedumu noņemšanai.

vietne zinātu, kurš no tās partneriem ir atbildīgs par pārdošanu, un samaksātu komisijas maksu – šī prakse ir pazīstama kā partnermārketings.

50. Gan izsekošanas saites, gan izsekošanas pikseļus var izplatīt, izmantojot visdažādākos kanālus, piemēram, e-pastus, vietnes vai pat – izsekošanas saišu gadījumā – jebkāda veida īsziņu sistēmas. Šī izplatīšana attiecībā uz lietotāja termināliekārtu nozīmē uzglabāšanu, vismaz izmantojot klienta puses programmatūras uzglabāšanas mehānismu. ePD 5. panta 3. punkts kā tāds ir piemērojams pat tad, ja šī uzglabāšana nav pastāvīga.

51. Izsekošanas informācijas pievienošana URL vai attēliem (pikseļiem), kas nosūtīti lietotājam, ir norādījums termināliekārtai nosūtīt atpakaļ mērķa informāciju (norādīto identifikatoru). Dinamiski veidotu izsekošanas pikseļu gadījumā instrukcija ir lietojumprogrammas loģikas (parasti JavaScript koda) izplatīšana. Līdz ar to var uzskatīt, ka identifikatoru vākšana, kas nodrošināta, izmantojot šādus izsekošanas mehānismus, ir "pieejas nodrošināšana" ePD 5. panta 3. punkta izpratnē, tādējādi tā attiecas arī uz šo posmu.

3.2 Vietējā apstrāde

52. Dažas tehnoloģijas balstās uz vietējo apstrādi, ko instruējusi programmatūra, kas izplatīta lietotāju termināliekārtā, kur vietējās apstrādes rezultātā iegūtā informācija pēc tam tiek darīta pieejama izvēlētiem dalībniekiem, izmantojot API klienta pusē. Tas var attiekties, piemēram, uz tīmekļa pārlūkprogrammas nodrošināto API, kur attālināti var piekļūt vietēji ģenerētiem rezultātiem.

53. Ja jebkurā brīdī un, piemēram, klienta puses kodeksā apstrādātā informācija ir pieejama trešai personai, piemēram, nosūtīta atpakaļ tīklā uz serveri, šāda darbība (saskaņā ar tās struktūras norādījumiem, kura veido klienta puses kodu, kas tiek izplatīts lietotāja termināliekārtā) būtu "pieejas nodrošināšana jau uzglabātai informācijai". Tas, ka šī informācija tiek sagatavota vietējā līmenī, neizslēdz e-PD 5. panta 3. punkta piemērošanu.

3.3 Izsekošana, pamatojoties tikai uz IP

54. Daži pakalpojumu sniedzēji izstrādā risinājumus, kas balstās tikai uz viena komponenta, proti, IP adreses, apkopošanu, lai izsekotu lietotāja navigāciju[28], atsevišķos gadījumos aptverot vairākas jomas. Šajā gadījumā ePD 5. panta 3. punktu varētu piemērot pat tad, ja norādījumu par IP pieejamības nodrošināšanu ir izteikusi cita struktūra, nevis saņēmēja struktūra.

55. Tomēr pieejas nodrošināšana IP adresēm izraisītu ePD 5. panta 3. punkta piemērošanu tikai gadījumos, kad šīs informācijas avots ir abonenta vai lietotāja termināliekārta. Lai gan tas nav parasts gadījums (piemēram, ja ir aktivizēts CGNAT[29]), statiskās izejošās IPv4 adreses, kas nāk no lietotāja maršrutētāja, ietilpst šajā gadījumā, tāpat kā IPV6 adreses, jo tās daļēji nosaka mitinātājs. Ja vien struktūra nevar nodrošināt, ka IP adrese nenāk no lietotāja vai abonenta termināliekārtas, tam ir jāveic visi pasākumi saskaņā ar ePD 5. panta 3. punktu.

56. Lai gan šajās pamatnostādnēs nav analizēts, kā tiek piemēroti ePD 5. panta 3. punktā paredzētie atbrīvojumi no pienākuma saņemt piekrišanu, ir svarīgi vēlreiz atgādināt, ka šā panta piemērojamība

[28] Tas ir papildus un neatkarīgi no IP adreses izmantošanas un funkcijām, lai izveidotu un nodotu vai pārsūtītu pamatā esošos tehniskos sakarus, vai tas, ka tie var būt vai nebūt personas dati (attiecībā uz E-privātuma analīzi tā ir "informācija").

[29] Pārvadātāja līmeņa NAT jeb CGNAT izmanto interneta pakalpojumu sniedzēji, lai maksimāli izmantotu ierobežoto IP adrešu telpu. Tas grupē vairākus abonentus zem vienas publiskās IP adreses.

vienmēr nenozīmē, ka ir jāsaņem piekrišana. Tādējādi EDAK atgādina, ka katrā gadījumā būtu jāizvērtē, vai ir vajadzīga piekrišana un vai varētu piemērot atbrīvojumu saskaņā ar ePD 5. panta 3. punktu[30].

3.4 Periodiska un ar mediāciju saistīta IoT ziņošana

57. IoT (lietu interneta) ierīces sniedz informāciju nepārtraukti visu laiku, piemēram, izmantojot ierīcē iegultus sensorus, kurus var vai nevar iepriekš apstrādāt lokāli. Daudzos gadījumos informācija tiek padarīta pieejama attālinātam serverim, taču šīs ievākšanas modalitātes var atšķirties.

58. Dažām IoT ierīcēm ir tiešs savienojums ar publisko komunikāciju tīklu, izmantojot mobilo SIM karti. Citam var būt netiešs savienojums ar publisko komunikāciju tīklu, piemēram, izmantojot WIFI vai pārraidot informāciju citai ierīcei, izmantojot punkta-punktu savienojumu (piemēram, ar Bluetooth starpniecību). Otra ierīce var būt, piemēram, viedtālrunis vai īpaša vārteja, kas var vai nevar iepriekš apstrādāt informāciju pirms tās nosūtīšanas serverim.

59. Ražotājs var dot norādījumus IoT ierīcēm vienmēr straumēt savākto informāciju, tomēr vispirms to var saglabāt lokālā kešatmiņā, piemēram, līdz brīdim, kad ir pieejams savienojums.

60. Jebkurā gadījumā IoT ierīce, ja tā ir (tieši vai netieši) pieslēgta publiskajam komunikāciju tīklam, pati par sevi būtu uzskatāma par termināliekārtu. Tas, ka informācija tiek straumēta vai glabāta kešatmiņā periodiskai ziņošanai, nemaina šīs informācijas būtību. Abās situācijās būtu piemērojams ePD 5. panta 3. punkts, jo, izmantojot IoT ierīces kodu, tiek dots norādījums dinamiski uzglabātos datus nosūtīt uz attālo serveri, notiek "pieejas nodrošināšana".

3.5 Unikālais identifikators

61. Kopīgs rīks, ko izmanto uzņēmumi, ir jēdziens “unikālie identifikatori” vai “pastāvīgie identifikatori”. Šādus identifikatorus var atvasināt no pastāvīgiem personas datiem (vārds un uzvārds, e-pasta adrese, tālruņa numurs u. c.), kas tiek šifrēti lietotāja ierīcē, apkopoti un koplietoti starp vairākiem pārziņiem, lai unikāli identificētu personu dažādās datu kopās (lietošanas dati, kas apkopoti, izmantojot tīmekļa vietni vai lietojumprogrammu, klientu attiecību pārvaldības (CRM) dati, kas saistīti ar tiešsaistes vai bezsaistes pirkumiem vai abonēšanu utt.). Tīmekļa vietnēs pastāvīgie personas dati parasti tiek iegūti autentificēšanas vai informatīvo izdevumu abonēšanas nolūkā.

62. Kā minēts iepriekš, fakts, ka lietotājs ievada informāciju, neliedz piemērot e-PD 5. panta 3. punktu attiecībā uz uzglabāšanu, jo pirms ievākšanas šī informācija uz laiku tiek glabāta termināliekārtā.

63. Saistībā ar “unikālā identifikatora” ievākšanu tīmekļa vietnēs vai mobilajās lietotnēs struktūra, kas ievāc informāciju, dod norādījumus pārlūkprogrammai (izplatot klienta puses kodu) nosūtīt šo informāciju. Tādējādi notiek “pieejas nodrošināšana”, un tiek piemērots e-PD 5. panta 3. punkts.

[30] WP29 Atzinumā 9/2014 ir sniegti daži piemēri, kad piekrišana var nebūt nepieciešama.