Eiropas Savienības
Padome

Briselē, 2025. gada 13. martā
(OR. en)

15941/2/24
REV 2

COSI 214
ENFOPOL 463
IXIM 234
CATS 109
COPEN 500
CYBER 342
DATAPROTECT 332

PIEZĪME

Sūtītājs:	prezidentvalsts
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	11281/24
Temats:	Augsta līmeņa grupas jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos noslēguma ziņojums

Augsta līmeņa grupas jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos līdzpriekšsēdētāju vārdā prezidentvalsts pielikumā delegācijām sniedz augsta līmeņa grupas noslēguma ziņojumu.

Šajā pārskatītajā redakcijā ir atspoguļotas lingvistiskās pārskatīšanas laikā izdarītās redakcionālās izmaiņas.

PIELIKUMS

Augsta līmeņa grupas jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos noslēguma ziņojums

2024. gada 15. novembris

Izteiktie viedokļi ir tikai augsta līmeņa grupas ekspertu viedokļi, un tos nevajadzētu uzskatīt par Eiropas Komisijas vai Padomes oficiālo nostāju atspoguļojumu.

Ieteikumi, ko sniegusi Augsta līmeņa grupa jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos, ir jāīsteno, pilnībā ievērojot dalībvalstu kompetenci. Tos piemēro tikai attiecībā uz tiesībaizsardzības darbībām un komerciāliem rīkiem, ko izmanto tiesiskuma nodrošināšanas nolūkos, un tie neskar dalībvalstu ekskluzīvo atbildību par valsts drošību. Tāpēc suverēni rīki un rīki, ko izmanto un/vai izstrādā tikai valsts drošības nolūkos, ir izslēgti no šo ieteikumu darbības jomas.

Saturs

Kopsavilkums

Eiropas Savienība veido brīvības, drošības un tiesiskuma telpu, kur tiek respektētas pamattiesības un dalībvalstu atšķirīgās tiesību sistēmas un tradīcijas. Tā cenšas nodrošināt augstu drošības [1] līmeni, veicot noziedzības novēršanas un apkarošanas pasākumus un sekmējot koordināciju un sadarbību starp tiesībaizsardzības, tiesu un citām kompetentajām iestādēm.

Tehnoloģiju attīstība un mūsu sabiedrības digitalizācija ir izraisījusi gan būtiskas izmaiņas iedzīvotāju ikdienas dzīvē, gan jaunus izaicinājumus tiesībaizsardzības un tiesu iestādēm attiecībā uz augsta drošības līmeņa nodrošināšanu gan nacionālā, gan ES līmenī. Mūsdienu digitālajā laikmetā gandrīz katrā kriminālizmeklēšanā ir kāds digitāls komponents. Šis jautājums tika aplūkots 2023. gada aprīlī Augsta līmeņa ekspertu grupas jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos darbības jomas izpētes dokumentā:

> Tehnoloģijas un rīkus [...] arī ļaunprātīgi izmanto noziedzīgiem nolūkiem. Šāda notikumu attīstība rada arvien lielākas grūtības nodrošināt efektīvu tiesībaizsardzību visā ES, lai garantētu sabiedrisko drošību un novērstu, atklātu, izmeklētu noziegumus un sauktu pie atbildības par tiem, un attaisnotu cietušo tiesisko paļāvību attiecībā uz taisnīgumu un kompensāciju. Ja tam netiks pievērsta pienācīga uzmanība, pastāv reāls risks, ka šī pašreizējā tendence ļaus noziedzniekiem "nozust" […]. Tas nopietni apdraud indivīdu un sabiedrības drošību un var galu galā radīt šķēršļus valsts pozitīvajam pienākumam arī turpmāk nodrošināt tiesiskumu un demokrātisku sabiedrību [2].

[1] Šajā dokumentā termins "drošība" nozīmē noziedzības apkarošanu vai sabiedriskās drošības apdraudējumu novēršanu.

[2] dok 8281/23, 2023. gada 13. aprīlis.

Tiesības uz privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību, kā arī tiesības uz personas datu aizsardzību ir garantētas ES Pamattiesību hartā. Saziņas – gan rakstiski, gan pa tālruni – konfidencialitāte ir viens no galvenajiem demokrātiskas sabiedrības sasniegumiem, kas nodrošina, ka ne valsts, ne privātie aktori nevar iejaukties cilvēku vārda brīvībā, un ļauj veidot plaukstošu pilsonisko sabiedrību. Minēto tiesību izmantošanai var piemērot tiesību aktos paredzētus ierobežojumus, jo īpaši attiecībā uz pasākumiem, kas paredzēti valsts drošības, aizsardzības vai sabiedriskās drošības nodrošināšanai un noziedzīgu nodarījumu vai elektronisko sakaru sistēmu neatļautas izmantošanas novēršanai, izmeklēšanai, atklāšanai un saukšanai pie atbildības par to, ar noteikumu, ka šie pasākumi ir nepieciešami, piemēroti un samērīgi demokrātiskā sabiedrībā. Tāpēc tiesībaizsardzības un tiesu iestādes var atvērt un lasīt rakstisku saziņu, pārtvert telefona zvanus un noklausīties sarunas, ja to uzskata par nepieciešamu, samērīgu un pamatotu un ja šādi pasākumi atbilst piemērojamajām tiesību normām un tiek veikti, pienācīgi ievērojot pamattiesības. Šai iespējai vajadzētu būt pieejamai visām kompetentajām iestādēm neatkarīgi no tehnoloģiju attīstības. Pēdējos gados vērojamā jaunu starppersonu saziņas veidu izplatīšanās nozīmē, ka visai sabiedrībai ir jāpielāgojas jaunajai realitātei. Mums ir jānodrošina, ka saziņa starp iedzīvotājiem joprojām ir aizsargāta un ka tajā pašā laikā tiesībaizsardzības un tiesu iestādes arī turpmāk spēj pildīt savu pienākumu aizsargāt iedzīvotājus, novēršot un apkarojot smago un organizēto noziedzību un terorismu. Nepieciešamība pielāgoties ir steidzama, un eksperti aicina politikas veidotājus rīkoties nekavējoties, jo tiesībaizsardzības iestādes jau tagad atpaliek no tehnoloģiju attīstības tempa, kas tieši ietekmē to spēju aizstāvēt pilsoņu tiesības.

Tieslietu un iekšlietu ministru neformālajā sanāksmē 2023. gada 26. janvārī iekšlietu ministri apsprieda izaicinājumus, ko tiesībaizsardzības jomā digitālajā laikmetā rada tehnoloģiju attīstība. Viņi arī pauda bažas par to, ka piemērojamie noteikumi un to interpretācija judikatūrā, kā arī praktiskie un operatīvie šķēršļi rada arvien lielākas grūtības tiesībaizsardzības iestādēm veikt savu darbu, jo īpaši attiecībā uz tādu datu saglabāšanu un piekļuvi tiem, kas nepieciešami noziedzīgu nodarījumu izmeklēšanai un saukšanai pie atbildības par tiem [3].

[3] Sk. dalībvalstu komentāru apkopojumu dokumentā 7184/1/23 REV 1, 2023. gada 23. marts.

Pēc šīm diskusijām Padome apstiprināja to, ka tiek izveidota grupa ar mērķi izstrādāt stratēģisku, uz nākotni vērstu redzējumu par tiesu un tiesībaizsardzības iestāžu efektīvu un likumīgu piekļuvi datiem, elektroniskajiem pierādījumiem un informācijai digitālajā laikmetā – **Augsta līmeņa grupa jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos** [4].

Augsta līmeņa grupas mērķis bija rast risinājumus problēmai, kas raksturīga likumīgas piekļuves datiem atļaušanai, lai nodrošinātu augstu drošības līmeni visiem ES iedzīvotājiem, vienlaikus nodrošinot pamattiesību, tostarp tiesību uz privātumu un datu aizsardzību, ievērošanu, kā arī augstu kiberdrošības līmeni, izmantojot efektīvus un nākotnes prasībām atbilstošus risinājumus.

42 ieteikumi [5], kas ir galvenais Augsta līmeņa grupas darba rezultāts, ir izstrādāti laikā, kad pieaug aicinājumi nodrošināt pārskatatbildību tiešsaistē. Ieteikumos risinātas pašreizējās un gaidāmās problēmas, ņemot vērā tehnoloģiju attīstību, un to mērķis ir ļaut īstenot visaptverošu ES pieeju nolūkā īstenot efektīvu kriminālizmeklēšanu un krimināltvajāšanu. Ieteikumi ir sagrupēti trīs blokos: **spēju veidošana, sadarbība ar nozari un standartizācija un likumdošanas pasākumi.** Tajos uzsvērtas problēmas, ar kurām saskaras tiesībaizsardzības iestādes, piekļūstot datiem lasāmā formātā kriminālizmeklēšanas vajadzībām, jo trūkst saskaņotu datu saglabāšanas pienākumu un stingru ES judikatūras prasību, aizvien plašāk tiek izmantota pilnīga (*end-to-end*) šifrēšana un daži netradicionālie telesakaru pakalpojumi nesadarbojas. Lai gan ieteikumos atzinīgi vērtēti e-pierādījumu noteikumi, tajos ir uzsvērti to ierobežojumi šifrēšanas radīto problēmu risināšanā un aicināts veidot ciešāku sadarbību starp tiesībaizsardzības un tiesu iestādēm un pakalpojumu sniedzējiem, lai veicinātu pastāvīgu dialogu un savstarpēju izpratni par operatīvajām, tehniskajām un uzņēmējdarbības vajadzībām un pārvarētu grūtības piekļūt šifrētiem datiem. Eksperti uzskata, ka ciešāka sadarbība starp tiesībaizsardzības iestādēm un pakalpojumu sniedzējiem zināmā mērā uzlabos situāciju, taču, lai rastu nākotnes prasībām atbilstošu risinājumu, ir nepieciešams, lai pakalpojumu sniedzēju pienākumi sadarboties tiktu īstenoti ar tiesību aktiem, vispārējā vai sistemātiskā veidā nevājinot šifrēšanu pakalpojuma lietotājiem.

---

4 Augsta līmeņa grupa jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos – Eiropas Komisija (europa.eu).

5 Augsta līmeņa grupas ieteikumi.

2024. gada 13. jūnijā **Padome rīkoja viedokļu apmaiņu** par Augsta līmeņa grupas ieteikumiem, kopumā atzinīgi novērtēja augsta līmeņa grupas ekspertu paveikto darbu un uzsvēra, ka ir ātri jāturpina darbs pie piekļuves datiem efektīvas tiesībaizsardzības nolūkos [6]. Iekšlietu ministri noteica šādas prioritātes: 1) izveidot saskaņotu ES tiesisko regulējumu datu saglabāšanai tiesībaizsardzības nolūkos, 2) izveidot noteikumus par efektīvu piekļuvi datiem, kas attiecas uz starppersonu elektronisko saziņu, un 3) izveidot juridiski un tehniski pamatotus risinājumus piekļuvei šifrētai elektroniskajai saziņai atsevišķos gadījumos un saskaņā ar tiesas rīkojumu, lai novērstu un izmeklētu smagus noziegumus un organizētās noziedzības gadījumus, kā arī terorismu un sauktu pie atbildības par tiem.

Turklāt ministri iestājās par to, ka tiek pastiprināta ES ietekme uz protokolu un tehnoloģiju standartizāciju, un par koordinētu pieeju digitālās kriminālistikas rīku un procedūru sertifikācijai. Visbeidzot, viņi uzstāja, ka attiecībā uz ieteikumu īstenošanu ir nepieciešams izstrādāt ceļvedi, kas ietver īsu grafiku un īstenojamības novērtējumu, un pietiekamus finanšu resursus. Par svarīgu tika uzskatīta arī atsevišķu ieteikumu īstenošanas koordinēšana.

Šā noslēguma ziņojuma mērķis ir detalizēti aprakstīt ekspertu konstatētās problēmas un izklāstīt iespējas darba turpināšanai un **ieteikumu īstenošanai**. Tajā ir izklāstītas vairākas galvenās ekspertu konstatētās problēmas, kas ir trīs darba virzienu pamatā saskaņā ar Augsta līmeņa grupas pilnvarām.

Pirmkārt, piekļuve datiem ir būtiska **digitālās kriminālistikas** vajadzībām, lai tiesībaizsardzības iestādes varētu vākt un analizēt pierādījumus no elektroniskajām ierīcēm. Šie dati sniedz ticamu informāciju par noziedzīgām darbībām un identificē tos, kas ir atbildīgi par noziedzīgiem nodarījumiem. Ņemot vērā dažu tehnoloģiju, piemēram, šifrēšanas, straujo attīstību un plašo izmantošanu, tiesībaizsardzības iestādēm ir jāpalielina savi resursi, prasmes un tehniskie risinājumi attiecībā uz piekļuvi šifrētiem datiem. Šajā sakarā un attiecībā uz komerciālu risinājumu izmantošanu – efektīva pārrobežu sadarbība var sniegt atbalstu, nodrošinot to, ka notiek dalīšanās pieredzē, tiek izstrādāti standartizēti rīki un procedūras un apvienoti resursi. Tomēr eksperti bija vienisprātis, ka spēju veidošana vien neuzlabos tiesībaizsardzības spējas. Daži eksperti uzskatīja, ka iespēja piekļūt datiem lasāmā formātā skaidri regulētos apstākļos ir ilgtspējīgāks ilgtermiņa risinājums.

[6] dok 11281/24, 2024. gada 21. jūnijs.

Otrkārt, lai tiesībaizsardzība varētu efektīvi izmeklēt noziegumus un saukt pie atbildības par tiem, ir vajadzīgi saskaņoti un konsekventi tiesību akti **datu saglabāšanas** jomā, kas pilnībā atbilst pamattiesībām. Tehnoloģiju straujā attīstība padara arvien vērtīgāku tiesībaizsardzības iestāžu savlaicīgu piekļuvi attiecīgajiem datiem, ko glabā pakalpojumu sniedzēji. Konkrētāk, piekļuve pakalpojumu sniedzēju glabātajiem sakaru metadatiem ir būtiska, lai identificētu aizdomās turētos un izprastu viņu darbības, un ir pierādīta tās nozīme izmeklēšanas virzībā.

Treškārt, **likumīga pārtveršana** ir būtiska, lai efektīvi izmeklētu teroristu organizācijas un organizēto noziedzību un sauktu pie atbildības par to. Tā ļauj iestādēm – saskaņā ar tiesas rīkojumiem un pilnībā ievērojot pamattiesības – pieprasīt, lai pakalpojumu sniedzēji sniedz saziņas saturu, un minētais saturs sniedz vērtīgu informāciju par noziedzīgām darbībām. Ņemot vērā pāreju no tradicionālajiem sakaru nodrošinātājiem uz *OTT* (*over-the-top*) pakalpojumiem, kā definēts Eiropas Elektronisko sakaru kodeksā (*EECC*) [7], un to, ka noziedznieki arvien vairāk pāriet uz pilnīgi šifrētām platformām [8], likumīga piekļuve sakariem reāllaikā prasa izvērtēt vajadzību pēc skaidriem noteikumiem attiecībā uz sadarbību starp tiesībaizsardzības iestādēm un tehnoloģiju uzņēmumiem, kā arī ciešāku sadarbību ES līmenī, lai atvieglotu pārrobežu pieprasījumus.

Šā noslēguma ziņojuma ieteikumi un saturs atspoguļo **tikai Augsta līmeņa grupas ekspertu gaidas un prasības**.

Sniedzot šo ziņojumu, **Augsta līmeņa grupa ir noslēgusi savu darbu** un aicina Komisiju, dalībvalstis, Eiropas Parlamentu un visas attiecīgās ieinteresētās personas, iedvesmoties no ieteikumiem un ziņojuma, izstrādājot pasākumus, lai risinātu jautājumu par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos. Šādi pasākumi būtu jāpapildina ar spēcīgu vēstījumu, kas apliecina, ka ir steidzami jāveic nozīmīgi pasākumi, lai nodrošinātu efektīvu likumīgu piekļuvi datiem. Eksperti mudina visas ES iestādes un struktūras nekavējoties spert vēl vienu soli uz priekšu, īstenojot konkrētas iniciatīvas, kas iekļautas īpašā ceļvedī.

---

[7] Direktīva (ES) 2018/1972 (2018. gada 11. decembris) par Eiropas Elektronisko sakaru kodeksa izveidi to tiesiskā regulējuma daļu, kas attiecas uz tradicionālajiem telesakariem, attiecina arī uz uzņēmumiem, kuri piedāvā interneta pakalpojumus telesakaru infrastruktūrā, kas tiem nepieder vai ko tie nepārvalda, tostarp numurneatkarīgus starppersonu sakaru pakalpojumus *(NI-ICS*).

[8] Eiropola Interneta organizētās noziedzības draudu novērtējums (*IOCTA*), 2024. gads.

Likumīga piekļuve: galvenie izaicinājumi

Mūsu spēja apkarot noziedzību un nosargāt ES drošību pēdējos gados daudzās jomās ir uzlabojusies. Tiesībaizsardzības un tiesu iestāžu sadarbība ir kļuvusi efektīvāka, ir ieviesti jauni tiesību akti un instrumenti cīņai pret smago un organizēto noziedzību un ir pastiprināti kopīgi centieni apkarot migrantu kontrabandu, cilvēku, šaujamieroču un narkotiku tirdzniecību, korupciju un citus smagus noziegumus.

Tomēr, nodrošinot mūsu pilsoņu drošību, tiesībaizsardzības iestādes katru dienu saskaras ar jaunām problēmām, jo īpaši tādām, ko rada mūsu sabiedrības digitalizācija.

Digitālās tehnoloģijas maina mūsu dzīvi, sākot no veida, kādā mēs sazināmies, un beidzot ar to, kā mēs dzīvojam un strādājam, un šīs pārmaiņas raksturo tālejoši sociālie aspekti. Digitalizācija var sniegt risinājumus daudzām problēmām, ar kurām saskaras Eiropa un eiropieši, un tā piedāvā daudz iespēju – iespējas radīt darbvietas, veicināt izglītību, uzlabot konkurētspēju un inovāciju, cīnīties pret klimata pārmaiņām, veicināt zaļo pārkārtošanos u.t.t.

Tomēr digitalizācija arī rada apstākļus noziedzniekiem, lai tie tehnoloģisko progresu izmantotu noziegumu izdarīšanai gan tiešsaistē, gan bezsaistē. Šifrētas ierīces un lietotnes, jauni sakaru operatori, virtuālie privātie tīkli (*VPN*) u.c.. ir paredzēti, lai aizsargātu likumīgu lietotāju privātumu. Taču tie arī nodrošina noziedzniekiem efektīvus līdzekļus, ar ko slēpt savu identitāti, tirgot savus noziedzīgos produktus un pakalpojumus, novirzīt maksājumus un slēpt savu darbību un saziņu, efektīvi izvairoties no atklāšanas, izmeklēšanas un kriminālvajāšanas. Pastāv rīki un pakalpojumi, kuri mērķtiecīgi izveidoti un galvenokārt tiek izmantoti nelikumīgu darbību veikšanai, taču ir pierādījumi, ka noziedznieki arvien vairāk izmanto arī privātuma aizsardzības pasākumus, kurus dara pieejamus likumīgi elektronisko sakaru pakalpojumi (*ECS*). ***Tiesībaizsardzības iestādes šajā ziņā bieži atpaliek no noziedzniekiem, jo tām trūkst atbilstošu darbinieku, instrumentu un līdzekļu, lai efektīvi risinātu šo problēmu***. Šo norišu rezultātā piekļuve datiem tiesībaizsardzības nolūkos pēdējos gados ir kļuvusi par vienu no galvenajiem izaicinājumiem krimināllizmeklēšanā un kriminālvajāšanā. Tomēr ir gūti arī ievērojami panākumi, piemēram, tiesībaizsardzības iestādēm ir izdevies sagraut noziedzīga rakstura šifrētus sakaru tīklus, piemēram, *EncroChat* un *SkyECC*, un tās turpina īstenot tādas operācijas kā *"Desert Light"*, kuras laikā 2022. gada novembrī tika likvidēts kokaīna tirgotāju "superkartelis". Eiropola Atšifrēšanas platforma dažu pēdējo gadu laikā ir atbalstījusi vairākas augsta līmeņa izmeklēšanas, veicinot sekmīgas pret terorismu un smago un organizēto noziedzību vērstas tiesībaizsardzības darbības.

Tomēr aiz minētajiem veiksmes stāstiem nepamanītas paliek daudzas aizkavētas un neveiksmīgas izmeklēšanas – nozares praktiķi ir ziņojuši par pastāvīgām problēmām saistībā ar operatīvo vajadzību savlaicīgu apmierināšanu.

Sniedzot iestādēm iespēju mērķtiecīgi uzraudzīt un pārtvert noziedzīgu saziņu un traucēt noziedznieku darbības, likumīga piekļuve apgrūtina tehnoloģiju izmantošanu noziedzīgiem mērķiem. Turpretī bez stabila tiesiskā regulējuma un pienācīgiem resursiem tiesībaizsardzības iestādes turpinās cīnīties ar nepārvaramām grūtībām, un pastāv risks, ka dažādu iemeslu dēļ kritiski pierādījumi joprojām nebūs pieejami.

- **Dati ne vienmēr ir pieejami** jo īpaši tad, ja tie ir dzēsti, jo datu saglabāšanas noteikumi tiesībaizsardzības nolūkos ir nekonsekventi un neatbilstīgi. Šī nepilnība būtiski kavē smagās un organizētās noziedzības izmeklēšanas. Aptaujā, kas 2023. gadā tika veikta *SIRIUS* projekta ietvaros [9], gandrīz puse aptaujāto izmeklētāju kā galveno šķērsli faktiski minēja saskaņota datu saglabāšanas režīma trūkumu. Bez saskaņotiem noteikumiem pastāv risks, ka būtiski dati joprojām nebūs pieejami, un tas apdraud centienus efektīvi apkarot noziedzību.

- **Datus nevar izgūt**, jo īpaši, ja neizdodas to iegūšana no kādas ierīces. Nepieciešamo prasmju, piemērotu rīku un pietiekamas sadarbības ar ierīču ražotājiem trūkums padara digitālo kriminālistiku sarežģītu, dārgu un laikietilpīgu, ja ne pilnībā praktiski neīstenojamu. Šis būtiskais trūkums kavē efektīvas izmeklēšanas. Bez padziļinātām kriminālistikas spējām un prasmēm un uzlabotas sadarbības ar nozari un starp valsts iestādēm būtiski digitālie pierādījumi joprojām nav pieejami, un tas nopietni ietekmē tiesībaizsardzības centienus.

- **Datus ne vienmēr var lasīt** šifrēšanas dēļ. Daudzos pakalpojumos tagad tiek izmantota galšifrēšana, lai aizsargātu saziņas konfidencialitāti, privātumu un kiberdrošību, taču tas var ārkārtīgi apgrūtināt tiesībaizsardzības piekļuvi saziņas datiem. Tas nozīmē – pat ja dati tiek likumīgi pārtverti, bieži vien nav iespējams tos atkodēt. Bez spējas lasīt šos datus svarīgi pierādījumi paliek slēpti, un tas ievērojami apgrūtina noziegumu izmeklēšanu.

---

[9] *SIRIUS*, pārrobežu piekļuve elektroniskajiem pierādījumiem (*SIRIUS* projekts), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Datus ne vienmēr var izanalizēt**, piemēram, ne vienmēr ir pieejamas tehnoloģijas un/vai cilvēkresursi, lai veiktu liela datu apjoma skrīningu vai izņemtos datus filtrētu un analizētuefektīvā veidā, kas ir saderīgs ar ES pamatvērtībām un ES un dalībvalstu tiesisko regulējumu.

- **Datus nevar iegūt** tiesību normu kolīziju starp jurisdikcijām dēļ. Dati bieži vien šķērso starptautiskās robežas, radot sarežģītas jurisdikcijas problēmas. Dažādās valstīs ir atšķirīgi normatīvie akti par piekļuvi datiem, un tas apgrūtina ārvalstīs glabātu datu iegūšanu. Jaunā ES E-pierādījumu regula un direktīva ir svarīgi soļi, lai to atvieglotu, taču vēl ir daudz darāmā, lai pilnībā īstenotu šos pasākumus, un bez pilnīgas īstenošanas piekļuve būtiskiem datiem no citām valstīm joprojām rada būtiskas problēmas tiesībaizsardzības jomā.

Tie ir daži no izaicinājumiem, ar ko pašlaik ikdienā saskaras tiesībaizsardzības iestādes.

Noziedznieki pastāvīgi pielāgo savu rīcību, lai izvairītos no atklāšanas. Pieejamā statistika [10] liecina, ka noziedznieki arvien vairāk pāriet uz likumīgām galšifrētām platformām. Tomēr, tiklīdz būs atrasti efektīvi pretpasākumi, ļoti iespējams, ka tie atkal pāries uz citiem saziņas kanāliem. Šā iemesla dēļ ir ārkārtīgi svarīgi, lai tiesībaizsardzības iestādes, kurām palīdz eksperti no visām attiecīgajām kopienām, spētu uzraudzīt tehnoloģiju attīstību un paredzēt izmaiņas noziedznieku rīcībā, piemēram, saistībā ar 6G, lietu internetu (*IoT*) un satelītsakariem. Turklāt, lai risinātu līdzīgas problēmas nākotnē, ir jāsaglabā un jāpielāgo spējas, kas ir darījušas iespējamas sekmīgas operācijas pret noziedzīgiem mērķiem paredzētiem sakaru pakalpojumiem (piemēram, *EncroChat*, *Ghost ECC*).

[10] Eiropola 2024. gada *IOCTA*.

Aizvien aktuālāka kļūst tiesībaizsardzības spēja likumīgi piekļūt digitālai informācijai. Tā kā noziedznieki arvien vairāk paļaujas uz tiešsaistes pakalpojumiem, datu pieprasījumu tiešsaistes pakalpojumu sniedzējiem kļūst aizvien vairāk; laikposmā no 2017. līdz 2022. gadam šādu pieprasījumu skaits ir trīskāršojies [11]. Saziņas datiem (gan metadatiem, gan satura datiem) ir izšķiroša nozīme daudzās kriminālizmeklēšanās. Tiek uzskatīts, ka piekļuvei digitāliem pierādījumiem ir būtiska loma 85 % izmeklēšanu [12]. Jaunais noteikumu kopums par pārrobežu piekļuvi elektroniskiem pierādījumiem palielinās kompetento iestāžu spēju piekļūt minētajiem datiem. Tomēr šie noteikumi var darboties tikai tad, ja dati ir pieejami lasāmā formātā. Tāpat arī piekļuve izņemtajās ierīcēs glabātiem datiem un saziņas likumīga pārtveršana joprojām ir ļoti sarežģīta gan juridiski, gan praktiski. Attiecībā uz tranzītā esošu datu efektīvu pārtveršanu pārrobežu lietās dalībvalstis var pieprasīt tiesu iestāžu sadarbību, izmantojot Konvenciju par savstarpēju tiesisko palīdzību [13] un Eiropas izmeklēšanas rīkojumu [14]; tomēr šie instrumenti galvenokārt tika izstrādāti, domājot par lietisko pierādījumu apmaiņu, un to efektivitāte varētu būt ierobežota tehnoloģiju attīstības kontekstā.

Likumīgai piekļuvei ir jābūt pakļautai stingriem nosacījumiem, kas noteikti valsts, ES un starptautiskajos tiesību aktos, un ir jāievieš pārredzami un atbildīgi procesi, kā regulēt šādu piekļuvi, tostarp, novēršot komercnoslēpumu nelikumīgu izpaušanu un likumīgas izpaušanas gadījumā nodrošinot, ka tiek veikti atbilstīgi pasākumi, lai saglabātu to konfidencialitāti.

Likumīgai piekļuvei ir pilnībā jāatbilst nepieciešamības un samērīguma principiem, un vajadzības gadījumā tā jāapstiprina tiesai vai neatkarīgai iestādei. Piekļuvei datiem ir jābūt līdzsvarā ar stingriem privātuma aizsardzības un kiberdrošības pasākumiem (piemēram, šifrēšana, ugunsmūri un pretvīrusu un pretļaunprogrammatūras programmas). Garantijas tam, ka piekļuve datiem aprobežojas tikai ar to, kas ir nepieciešams izmeklēšanas nolūkā, palīdz aizsargāt individuālu lietotāju privātumu.

---

11 *SIRIUS* projekts.

12 Komisijas ietekmes novērtējums par priekšlikumiem E-pierādījumu regulai un E-pierādījumu direktīvai (2018. gada 17. aprīlis).

13 STP – Eiropas Padomes standarti – *PC-OC* (coe.int).

14 https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=celex:32014L0041.

Likumīga piekļuve datiem tiesībaizsardzības nolūkos ir pamats tam, lai mūsu pilsoņiem nodrošinātu augstāko iespējamo drošības līmeni, taču to nedrīkst īstenot uz pamattiesību vai sistēmu un produktu kiberdrošības rēķina. Nav pieļaujams, ka tiktu vājināta cilvēku personas neaizskaramības un drošības aizsardzība par labu viņu tiesībām un otrādi; ir jārod līdzsvars, kas nodrošina, ka šie aspekti nekaitē viens otram. Gan ES, gan dalībvalstīm ir pienākums nodrošināt, ka pilsoņi var baudīt augstu pamattiesību aizsardzības līmeni un ka viņi jūtas droši ikdienas dzīvē. Tehnoloģiju attīstība nedrīkst radīt droša patvēruma iespējas noziedzniekiem – ja ir pamatotas aizdomas, ka ir izdarīts vai var tikt izdarīts noziegums, tiesībaizsardzībai ir jābūt piekļuvei rīkiem, kas tām ļauj piekļūt attiecīgajiem datiem.

Gan Eiropas Cilvēktiesību konvencijā, gan valstu konstitūcijās, gan ES Pamattiesību hartā ir atzīts, ka ikvienam ir tiesības uz privāto dzīvi, kas ietver arī personas saziņu. ES Pamattiesību hartā ir noteiktas arī tiesības uz datu aizsardzību. Tiesības uz privātumu un personas datu aizsardzību nav absolūtas tiesības, bet gan jāaplūko saistībā ar to funkciju sabiedrībā [15]. Publiskās iestādes nedrīkst iejaukties šo tiesību īstenošanā, ***izņemot gadījumus, kad šāda iejaukšanās ir saskaņā ar likumu, respektē tiesību būtību un ir nepieciešama un samērīga demokrātiskā sabiedrībā.*** Ievērojot minētos nosacījumus, tiesības uz privātumu un personas datu aizsardzību var ierobežot, tostarp valsts un sabiedriskās drošības interesēs un lai novērstu, izmeklētu un atklātu noziegumus un sauktu pie atbildības par tiem.

Izšķiroša nozīme ir stingrai pārskatatbildībai. Mūsu demokrātiskajā sabiedrībā likumdevēju pienākums ir radīt apstākļus šādai pārskatatbildībai, nodrošinot augstu privātuma un drošības līmeni. ***Privātums un drošība nav savstarpēji izslēdzoši***.

Lai veicinātu inovāciju un spēcīgu kiberdrošību, sadarbībā ar visām attiecīgajām ieinteresētajām personām, tostarp nozari, ir jāizstrādā risinājumi likumīgas piekļuves nodrošināšanai pamatotos gadījumos. ***Šie risinājumi jāizstrādā, pienācīgi ņemot vērā visas attiecīgās vajadzības un prasības, un tos nevar atstāt tikai tehnoloģiju uzņēmumu ziņā***.

---

15 2024. gada 30. aprīļa spriedums lietā C-470/21 *La Quadrature du Net u.c.*, EU:C:2024:370, 70. punkts.

Pirms turpmāku pasākumu īstenošanas ir jāveic tehniski novērtējumi, lai kliedētu dažu kiberdrošības ekspertu bažas par to, ka ir sarežģīti nodrošināt likumīgu piekļuvi, vienlaikus saglabājot spēcīgu kiberdrošību. ***Produktu un pakalpojumu kiberdrošība un likumīga piekļuve datiem izriet no juridiskiem pienākumiem, un abiem aspektiem ir jāspēj pastāvēt līdzās vienam otram***. Likumīgas piekļuves prasības ir jāīsteno uz tādu skaidru standartu pamata, ko izstrādājušas visas attiecīgās ieinteresētās personas (tostarp nozares pārstāvji, datu aizsardzības un kiberdrošības eksperti un tiesībaizsardzības praktiķi), atspoguļojot attiecīgās juridiskās prasības, un uz pienācīgi izvērtētu iespējamo risinājumu pamata, tādējādi nodrošinot, ka likumīga piekļuve neapdraud produktu un pakalpojumu drošību.

Daudzi uzņēmumi un pakalpojumu sniedzēji vilcinās sadarboties ar tiesībaizsardzību, jo pastāv juridiskā nenoteiktība, kas saistīta ar brīvprātīgiem pasākumiem, un risks, ka to pakalpojumu lietotāji varētu reaģēt negatīvi. Šāda nevēlēšanās kavē izmeklēšanas. Turklāt uzskats, ka lietotāji augstāk par sabiedrisko drošību vērtē privātumu, var rosināt nozares pārstāvju nevēlēšanos atvērt saziņas kanālus ar tiesībaizsardzības iestādēm un izveidot pielāgotus mehānismus, kas garantē likumīgu piekļuvi. Lai risinātu šo jautājumu, ir vajadzīgs skaidrs likumīgas piekļuves datiem tiesiskais regulējums. Pašlaik spēkā esošajos tiesību aktos pastāv būtiski šķēršļi, kas sarežģī šādas piekļuves nodrošināšanu, jo īpaši, uz brīvprātības pamata.

Sadarbība starp uzņēmumiem un tiesībaizsardzību ir nepietiekama un nepilnīga, un tā jāpapildina ar skaidriem noteikumiem. ***Bez skaidriem un izpildāmiem juridiskiem pienākumiem uzņēmumi bieži vien nespēj palīdzēt tiesībaizsardzībai piekļūt datiem***.

Tā kā nav efektīvu risinājumu likumīgas piekļuves nodrošināšanai, ***uz neaizsargātību balstīti risinājumi bieži vien tiek uzskatīti par vienīgo iespēju***.

Ja pārtvertos datus (un, iespējams, citus no ierīces iegūtus datus) apstrādā ar rīkiem, ko izstrādājuši privāti uzņēmumi, neatkarīgi no tā, kādas garantijas minētie uzņēmumi var sniegt, valsts iestādēm nav reālas pārskatāmības par to, kādi dati ir pakļauti skrīningam un kādā veidā tas notiek, un tām nākas paļauties tikai uz sertifikātiem, ko sniedz tās valsts valdība, kurā bāzēti pārtveršanas pakalpojumus sniedzošie uzņēmumi. Nepieciešamība paturēt slepenībā izmantoto ievainojamību, lai saglabātu rīku/pakalpojumu efektivitāti, saasina šo problēmu vēl vairāk. Šis jautājums jo īpaši rada bažas tad, ja pakalpojumu sniedzējs atrodas ārpus ES.

Visbeidzot – un tas ir ne mazāk svarīgi – jāmin tas, ka privātiem uzņēmumiem, kas sniedz pakalpojumus saistībā ar invazīvām izmeklēšanas metodēm, ir stimuls maksimāli palielināt savu peļņu, un tāpēc tie var nolemt savus rīkus pārdot režīmiem, kas nav demokrātiski (kā tas bija *Hacking Team* skandālā [16]).

Vēl viena iespēja – problēmas saistībā ar piekļuvi datiem var ***mudināt tiesībaizsardzību pieņemt invazīvākus izmeklēšanas pasākumus***. Šādos gadījumos tiesībaizsardzības iestādes ir spiestas izmantot pasākumus, kas vairāk iejaucas privātumā, piemēram, fizisku novērošanu, nevis piekļuvi ģeolokācijas datiem, un kratīšanu mājvietā, nevis likumīgu pārtveršanu.

Tiesībaizsardzības iestāžu nespēja piekļūt datiem var ievērojami mazināt sabiedrības uzticēšanos justīcijas sistēmai. Ja izmeklēšanas kavējas vai tiek traucētas, pilsoņi sistēmu var uztvert kā neefektīvu. Šāda uzticēšanās samazināšanās var apdraudēt likumību un kārtību un mazināt sabiedrības vēlmi dot ieguldījumu tiesībaizsardzības centienos.

Galu galā ***likumīga piekļuve ļauj tiesībaizsardzībai vākt pierādījumus, lai panāktu taisnīgumu cietušajiem un pasargātu viņus no turpmāka kaitējuma***. Dati var būt svarīgs uzvedinošs elements visu veidu noziegumu – gan bezsaistē, gan tiešsaistē izdarītu – atklāšanai un saukšanai pie atbildības par tiem. Personas var tikt pakļautas smagām kiberbulinga, identitātes zādzības, krāpšanas u. c. formām, kas izriet no digitālo tehnoloģiju, pakalpojumu un sakaru ļaunprātīgas izmantošanas noziedzīgos nolūkos. Šādai pieredzei var būt smagas emocionālas un psiholoģiskas sekas cietušajiem, saasinot pastāvošo nevienlīdzību un neaizsargātību.

---

[16] Sk. https://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/.

Ikvienā kriminālizmeklēšanā ir vajadzīgi pierādījumi, lai identificētu noziedzīgā nodarījuma izdarītāju vai pierādītu viņa vainu tiesneša priekšā. Tie var arī palīdzēt atbrīvot no atbildības pilsoņus, ja viņi ir nepamatoti apsūdzēti. Ja izmeklētāji un prokurori nevar piekļūt nepieciešamajai informācijai, viņi var nespēt virzīt izmeklēšanu un identificēt noziedzīgā nodarījuma izdarītāju, radot papildu ciešanas un finansiālus zaudējumus cietušajam un mazinot uzticēšanos justīcijas sistēmai. Ar tradicionāliem lietiskajiem pierādījumiem vien ne vienmēr pietiek, lai konstatētu saiknes un atrastu uzvedinošus elementus. ***Tiesībaizsardzībai un tiesu varai ir jābūt gatavām digitālajam laikmetam. Tikai tad tās spēs pilnībā aizsargāt mūsu sabiedrību un ekonomiku*** no pieaugošajiem draudiem, ko rada kiberuzbrukumi un hibrīddraudi, kā arī organizētās noziedzības darbības.

Visbeidzot, ja tiesībaizsardzības iestādes nevar efektīvi piekļūt datiem, to spēja nodrošināt drošību un aizturēt vissmagāko nodarījumu izdarītājus ir ievērojami vājināta. ***Tiesībaizsardzībai būtu jāsaņem likumīga un stingri kontrolēta efektīva piekļuve datiem, nodrošinot stingru privātuma aizsardzību un kiberdrošības garantijas, lai novērstu, atklātu un izmeklētu noziegumus un sauktu pie atbildības par tiem, tādējādi ļaujot tām garantēt drošību un dodot iespēju ES pilsoņiem dzīvot drošībā un panākt taisnīgumu, ja pret viņiem ir izdarīti noziegumi***.

I nodaļa: Digitālā kriminālistika

PROBLĒMJAUTĀJUMI

Digitālā kriminālistika attiecas uz tādu digitālo pierādījumu (gan saziņas metadatu, gan satura datu) vākšanu, analīzi un saglabāšanu, kas jebkādā digitālā formātā tiek glabāti elektroniskā ierīcē, tostarp tas attiecas uz informāciju no datoru cietajiem diskiem, mobilajiem tālruņiem, viedierīcēm, transportlīdzekļu navigācijas sistēmām, elektroniskajām durvju slēdzenēm, mākonī un citās digitālajās ierīcēs glabātajiem datiem.

Tā kā pieaug grūtības piekļūt saziņas datiem, kriminālizmeklēšanās arvien svarīgāka kļūst informācijas iegūšana no izņemtajām ierīcēm (vai no savienoto ierīču tīkliem). Piekļuve datiem miera stāvoklī ierīcēs var sniegt tiesībaizsardzībai kvalitatīvāku informāciju, piemēram, par organizētās noziedzības grupu dalībnieku identitāti, nekā citas metodes, piemēram, likumīga pārtveršana. Daži eksperti apgalvo, ka nav iespējams iepriekš zināt, kuri dati ir svarīgi konkrētai izmeklēšanai, proti, pat informācija, kas sākotnēji varētu šķist nebūtiska, izmeklēšanas gaitā varētu izrādīties ļoti svarīga. Piekļuve visiem ierīcē ietvertajiem datiem var būt svarīga arī, lai apstiprinātu aizdomās turētā nevainīgumu un aizsargātu apsūdzētā tiesības [17]. Turklāt izmeklēšanas metodēm vienmēr jābūt samērīgām.

Hronisko **resursu** un spēju **trūkumu**, ar ko saskaras tiesībaizsardzības iestādes šajā jomā, saasina jaunu tehnoloģiju (piemēram, jauna veida ierīču, *IoT* un mākoņdatošanas) ieviešana, kam nepieciešamas jaunas prasmes un rīki. Pat ja dalībvalstu aģentūrās un iestādēs jau ir pieejama būtiska zinātība digitālās kriminālistikas jomā, šīs zināšanas ir izkliedētas un nav skaidru mehānismu spēju kopīgošanai un izplatīšanai, kas nozīmē, ka tās joprojām ir izolētas.

[17] Kāds eksperts minēja gadījumu, kad ierīces darbības analīze bija būtiska, lai pierādītu, ka aizdomās turētais nevarēja būt iesaistīts slepkavībā.

Tādu **digitālās kriminālistikas laboratoriju salīdzināmu spēju trūkums** un vispārējs tādu **standartizētu kriminālistikas procedūru** un mehānismu trūkums, kas ļautu **atzīt digitālās kriminālistikas ekspertu prasmes un zinātību**, var kavēt pārrobežu sadarbību.

Augsta līmeņa grupas eksperti ir skaidri apliecinājuši – ierīcēs esošo datu **šifrēšana** pēc noklusējuma ir viena no galvenajām problēmām, ar ko saskaras tiesībaizsardzības iestādes. Tiesībaizsardzības iestādes – pat izmantojot visspēcīgākās atšifrēšanas platformas – nevar piekļūt datiem, kas tiek glabāti dažu veidu modernās ierīcēs, kuras ir aizsargātas ar kriptomikroshēmām [18] vai ar spēcīgiem šifrēšanas algoritmiem un sarežģītām parolēm. Šifrēšana un citi kiberdrošības un privātuma pasākumi ir nepieciešami, lai aizsargātu informācijas sistēmas un saziņu, kā arī personas datus, taču šie pasākumi – un jo īpaši aizvien plašāka šifrēšanas pēc noklusējuma izmantošana – mazina tiesībaizsardzības spēju vākt pierādījumus.

Dalībvalstīm ir ierobežota **zinātība un spējas** šajā jomā – gandrīz visas dalībvalstis norāda, ka tām trūkst tehnisku risinājumu, lai apmierinātu nozares praktiķu vajadzības, un lielākā daļa uzskata, ka to prasmes un finanšu līdzekļi nav pietiekami. Tiesībaizsardzības iestāžu spējas atšifrēt izņemtajās ierīcēs glabāto informāciju dažādās dalībvalstīs ievērojami atšķiras, proti, sekmīga rezultāta īpatsvars ir no 15–20 % dažos gadījumos līdz vairāk nekā divām trešdaļām citos. Ja spējas ir, tās parasti ir neefektīvas attiecībā uz tādu datu atšifrēšanu, kuri ir aizsargāti ar spēcīgām parolēm, un datnēm, kuras tiek glabātas speciālos šifrētos konteineros. Pat gadījumos, kad atšifrēšana ir sekmīga, tā bieži vien nenotiek savlaicīgi. Atšifrēšanas aprīkojums ir dārgs un ļoti specializēts, un aparatūra patērē jaudu.

Lielākā daļa tiesībaizsardzības iestāžu digitālās kriminālistikas departamentu paļaujas uz komerciāliem risinājumiem, lai piekļūtu datiem ierīcēs, un tas rada papildu izaicinājumus, jo šiem risinājumiem ir sarežģīti neatpalikt no tehnoloģiju attīstības un tie ātri noveco; licenču augstās izmaksas ievērojami samazina pilnvaroto lietotāju skaitu; un šādi risinājumi bieži vien tiek izstrādāti ārpus Eiropas un var būt slikti pielāgoti ES tiesībaizsardzības iestāžu vajadzībām vai neatbilst ES digitālās kriminālistikas pārskatatbildības standartiem.

[18] Piemēram, T2 drošības mikroshēma nesenajos *Apple* klēpjdatoros.

Bieži vien tiesībaizsardzības iestādēm nav citas iespējas kā vien izmantot **ievainojamības**, lai piekļūtu atšifrēšanas atslēgām ierīcēs. Tomēr izmeklēšanas metodēm, kuru pamatā ir šī pieeja, ir jābūt saskaņotām ar mērķi nodrošināt drošāku aparatūru un programmatūru, kā tas noteikts Kibernoturības aktā; ievainojamību pārvaldība un informācijas atklāšanas shēmas mazinātu šādu metožu neparedzētās sekas. Eksperti ir apsvēruši alternatīvus risinājumus, piemēram, noteikt aizdomās turētajiem pienākumu nodot izmeklēšanas iestādēm tos elementus (piemēram, paroles), kas nepieciešami, lai piekļūtu attiecīgajām ierīcēm. Valstu tiesiskais regulējums, ko piemēro šādos gadījumos, ievērojami atšķiras, un tikai trīs dalībvalstis ir norādījušas, ka to tiesību aktos ir īpašas normas, kas aizdomās turētajam uzliek pienākumu nodrošināt piekļuvi šifrēšanas atslēgām vai atšifrētiem datiem [19]. Dažas dalībvalstis aizdomās turētajiem uzliek pienākumu darīt pieejamus noteiktus biometriskos datus (piemēram, pirkstu nospiedumus) un tādējādi nodrošināt piekļuvi ierīcei; citos gadījumos aizdomās turētajiem ir jāizpauž sava parole. Kopumā tā joprojām ir joma, kurā vajadzīgs papildus novērtējums.

Dažas no iepriekš minētajām problēmām var mazināt, **savstarpēji izmantojot dalībvalstu spējas**, bet vienlaikus arī respektējot to ekskluzīvo kompetenci valsts drošības jautājumos. Tomēr šis risinājums joprojām netiek ņemts vērā – dažkārt juridisku ierobežojumu dēļ (septiņās dalībvalstīs ir ierobežojumi attiecībā uz rīku koplietošanu, savukārt piecās no tām ir konstatēti ierobežojumi attiecībā uz citu dalībvalstu kopīgotu rīku izmantošanu), bet lielākoties tādēļ, ka trūkst izveidotu mehānismu rīku koplietošanai vai kopīgai licenču iegādei.

Agrāk tiesībaizsardzības iestādēm bija skaidri **saziņas kanāli ar ražotājiem, pakalpojumu sniedzējiem un piegādātājiem**. Tas ļāva tām izveidot sadarbības protokolus, kas tām sniedza labāku izpratni par jaunieviesto tehnoloģiju attīstību un līdz ar to atviegloja tiesībaizsardzības darbības, vienlaikus nodrošinot arī kiberdrošību. Ņemot vērā jauno tehnoloģiju izvēršanas tempu un jaunu uzņēmumu ienākšanu tirgū, ir mainījušies apstākļi un sadarbība ar nozari vairs nepastāv.

Atbilstīgu standartu pieņemšana varētu ļaut produktu protokolus un tehnisko arhitektūru veidot tā, lai nodrošinātu, ka jau agrīnā posmā tiek ņemti vērā tiesībaizsardzības apsvērumi un tehniskās prasības. Tomēr **tiesībaizsardzības dalība attiecīgajās standartizācijas struktūrās** nav pietiekama, un tas ietekmē to spēju efektīvi piedalīties nākotnes tehnoloģisko standartu izstrādē.

---

[19] *Eurojust*, *"Cybercrime Judicial Monitor"* (Tiesu iestāžu pārskats par kibernoziedzību) (4. izdevums), 2018. gada decembris, 34. lpp., https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

IESPĒJAMIE RISINĀJUMI

I. Palielināt un racionalizēt centienus uzlabot spējas digitālo kriminālistikas rīku jomā

Dalībvalstīm jau ir zinātība un spēja veikt digitālās kriminālistikas darbības; tomēr, kopīgojot savus tehniskos risinājumus un daloties ar tiem, attiecīgās valsts iestādes un struktūras var gūt labumu no citu aģentūru pieredzes un panākt ievērojamus apjomradītus ietaupījumus, tādējādi samazinot nepieciešamos finanšu resursus. Dalībvalstis šajā nolūkā var turpināt pētīt risinājumus gan digitālās kriminālistikas rīku jomā, gan attiecībā uz apmācību un prasmju pilnveidošanu.

1. ieteikumu kopa

Lai uzlabotu sadarbību un veidotu spēcīgākas kolektīvās spējas digitālās kriminālistikas jomā, eksperti iesaka:

1. *kartēt un savienot esošos digitālās kriminālistikas tīklus un izveidot sekretariātu [1. ieteikums];*
2. *padarīt zināšanas pieejamākas un izplatīt tās ekspertu vidū [1. ieteikums];*
3. *apsvērt zināšanu apkopošanas mehānismus [2. ieteikums];*
4. *palielināt finansējumu pētniecībai un izstrādei ar skaidri noteiktiem sasniedzamajiem rezultātiem [4. ieteikums];*
5. *veicināt Eiropola rīku repozitoriju kā galveno centru rīku kopīgošanai [4. ieteikums];*
6. *atvieglot risinājumu un digitālās kriminālistikas rīku kopīgošanu starp dalībvalstīm uzticēšanās vidē (vienlaikus ņemot vērā valstu noteikumus) [2. ieteikums];*
7. *izstrādāt ES līmeņa mehānismu digitālās kriminālistikas rīku licenču kopīgam iepirkumam, lai tās kopīgotu starp dalībvalstīm [3. ieteikums];*
8. *veicināt sadarbību ar digitālās kriminālistikas rīku ražotājiem un izstrādātājiem, lai ar minētajiem rīkiem racionalizētu tiesībaizsardzības iestāžu iegūto datu struktūru un formātu, ideālā gadījumā ievērojot saskaņotus standartus [12. ieteikums];*
9. *izveidot mehānismu/shēmu komerciālo digitālās kriminālistikas rīku izvērtēšanai un – attiecīgā gadījumā – sertifikācijai ES līmenī, ņemot vērā jebkādu iespējamu negatīvu ietekmi, piemēram, nevajadzīgu papildu slogu, uz izmeklēšanas un kriminālvajāšanas procesiem [5. ieteikums].*

Vairākas organizācijas, tīkli, apvienības un projekti apvieno nozares praktiķus un dažādas partneru kategorijas, lai uzlabotu ES tiesībaizsardzības spējas digitālo izmeklēšanu jomā:

- *Eiropas Tiesu ekspertīzes institūtu tīkls* (*ENFSI*) [20] ir galvenais Eiropas tīkls, kas aptver (cita starpā) digitālo kriminālistiku; tajā ir 73 locekļi no 39 valstīm, un šie locekļi piedalās darba grupās, piemēram, par kriminālistikas informācijas tehnoloģiju un digitālo attēlveidošanu;

- *Eiropas Kibernoziedzības apkarošanas tehnoloģiju attīstības asociācija* (*EACTDA*) [21] apvieno daudzu dalībvalstu tiesībaizsardzības iestādes, pētniecības un tehnoloģiju organizācijas, nozares partnerus un akadēmiskās aprindas, lai veicinātu drošības pētniecības projektu rezultātu ieviešanu un nodrošinātu pilnībā testētus un darbībai gatavus programmatūras rīkus bez licences izmaksām un ES sabiedriskās drošības organizāciju piekļuvi pirmkodam;

- Eiropas Birojs krāpšanas apkarošanai (*OLAF*) kopš 2007. gada valstu tiesībaizsardzības iestādēm piedāvā specializētu *digitālās kriminālistikas un analītiķu apmācību (DFAT*), īpašu uzmanību pievēršot krāpšanai, korupcijai un citām nelikumīgām darbībām, kas ietekmē Eiropas Savienības finanšu intereses; gadā tiek apmācīti aptuveni 175 digitālās kriminālistikas eksperti, tādējādi veidojot stabilu kopienu šajā noziedzības jomā;

- citi projekti, piemēram, *CYCLOPES* [22] un *I-LEAD* [23], nav pastāvīgas struktūras, bet gan apvieno ekspertus un sniedz attiecīgu trūkumu analīzi.

Tomēr esošie pastāvīgie tīkli nespēj apvienot digitālās kriminālistikas vienības no ES tiesībaizsardzības iestādēm, kā arī organizācijas, kas ar tām cieši sadarbojas (piemēram, Dublinas Universitātes koledžas Kiberdrošības un kibernoziedzības izmeklēšanas centrs (*UCD*) vai Lietuvas Kibernoziedzības izcilības centrs apmācības, pētniecības un izglītības jomā).

---

20 https://enfsi.eu/.
21 https://www.eactda.eu/index.html.
22 https://www.cyclopes-project.eu/.
23 https://cordis.europa.eu/project/id/740685/en

Eiropols (jo īpaši Eiropola Inovācijas laboratorija kopā ar Eiropas Kibernoziedzības centru) jau – zināmā mērā – sadarbojas ar visiem iepriekš uzskaitītajiem tīkliem un ir apliecinājis spēju pulcēt kopā ievērojamu skaitu nozares praktiķu, piemēram, Eiropas Koordinācijas padomes inovācijai (*EuCB*) pamatgrupās, organizējot *Kriminālistikas ekspertu forumu* [24] un dodot ekspertiem iespēju sazināties ar attiecīgajiem partneriem, piemēram, ar *Kiberinovācijas foruma* [25] starpniecību.

Eiropols arī piedāvā gatavu infrastruktūru – Eiropola ekspertu platformu (*EPE*) –, kas nodrošina sadarbību un zināšanu apmaiņu starp ekspertiem par konkrētiem tematiem.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina uzlabot Eiropola digitālās kriminālistikas spējas

Aktori: Eiropols, Eiropas Komisija, dalībvalstis	*Laiks: 2028. gads*	*Budžets: tiks apspriests vēlāk atkarībā no diskusijās par nākamo DFS panāktajiem rezultātiem*

- Ievērojamās Eiropola stiprināšanas satvarā, par ko paziņots Eiropas Komisijas politiskajās pamatnostādnēs 2024.–2029. gadam, Augsta līmeņa grupas eksperti aicina stiprināt Eiropola spēju palīdzēt dalībvalstīm **apvienot resursus, zināšanas un zinātību un koplietot risinājumus un digitālās kriminālistikas rīkus** uzticēšanās vidē. Suverēni rīki un rīki, ko izmanto un/vai izstrādā vienīgi valsts drošības nolūkos, būtu jāizslēdz.

- Augsta līmeņa grupas eksperti aicina Eiropolu **uzņemties centra lomu**, lai piekļūtu attiecīgajai operatīvajai zinātībai šajā jomā, un, iespējams, **izveidot *SIRIUS* līdzīgu projektu digitālās kriminālistikas jomā**, lai veicinātu dalīšanos ar zinātību un pieredzi un paraugprakses apmaiņu.

- Augsta līmeņa grupas eksperti aicina Eiropolu pastiprināt savu lomu tādu **organizāciju un projektu koordinēšanā** – *EuCB* vadībā un ņemot vērā citu attiecīgo aģentūru ieguldījumu –, kas veicina zināšanu radīšanu digitālās kriminālistikas jomā ES līmenī.

[24] https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference

[25] https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2024

Pastāv vairāki finanšu instrumenti, ar ko atbalstīt pētniecību un rīku izstrādi digitālās kriminālistikas jomā.

- *Iekšējās drošības fonda (IDF)* ietvaros Eiropas Komisija periodiski publicē atklātus uzaicinājumus iesniegt priekšlikumus kibernoziedzības un digitālo izmeklēšanu jomā. Lai arī budžets ir diezgan ierobežots (šīm darbībām no pašreizējās DFS ir piešķirti aptuveni 15 miljoni EUR), šajos uzaicinājumos atlasītie projekti ir izrādījušies mērķtiecīgi un sekmīgi.

  Aptuveni divas trešdaļas IDF budžeta tiek piešķirtas, izmantojot dalītu pārvaldību, kad dalībvalstis izvēlas, kurus projektus finansēt, un uzņemas atbildību par ikdienas pārvaldību. Tādējādi dalībvalstīm ir iespēja atbalstīt digitālās kriminālistikas projektus savu attiecīgo valsts programmu ietvaros.

- *Pamatprogrammas "Apvārsnis Eiropa" kopas "Civilā drošība sabiedrībai"* kopējais budžets septiņu gadu laikā ir 1,596 miljardi EUR, un tās mērķis ir veicināt drošu Eiropas sabiedrību nepieredzētu pārmaiņu un pieaugošās globālās savstarpējās atkarības un draudu kontekstā, vienlaikus stiprinot Eiropas brīvības un tiesiskuma kultūru. Pēdējos gados no tās ir atbalstīti vairāki attiecīgi pētniecības projekti, piemēram, *FORMOBILE* [26] un *EXFILES* [27], kuru ietvaros sniegts atbalsts nozares praktiķiem viņu ikdienas darbībās.

- *Programma "Digitālā Eiropa"* ir galvenais ES finansēšanas instruments, kura mērķis ir uzlabot ES digitālo infrastruktūru, izmantojot dažādas iniciatīvas. No programmas, kuras kopējais budžets laikposmam no 2021. līdz 2027. gadam ir 7,5 miljardi EUR, ievērojamus resursus piešķir tieši kiberdrošībai, un tā aptver arī digitālo kriminālistiku.

---

[26] *FORMOBILE – From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices* (No mobilajiem tālruņiem līdz tiesai – pilnīga kriminālistiskās izmeklēšanas ķēde, kā priekšmets ir mobilās ierīces): https://cordis.europa.eu/project/id/832800.

[27] *EXFILES – Europe fights against crime and terrorism* (Eiropas cīņa pret noziedzību un terorismu): https://exfiles.eu/.

Eiropola atšifrēšanas platforma ir pamatprojekts IDF ietvaros. Šī platforma, ko 2020. gadā ciešā sadarbībā ar Eiropas Komisijas Kopīgo pētniecības centru (*JRC*) izveidoja Eiropols, sniedz atbalstu valstu tiesībaizsardzības iestādēm, atšifrējot to digitālos pierādījumus. Tās mērķis ir nodrošināt ilgtspējīgu risinājumu tiesībaizsardzības iestādēm, lai tās varētu piekļūt vajadzīgajiem tehniskajiem un IT resursiem. Dažu pēdējo gadu laikā platforma ir izmantota daudzās nozīmīgās lietās, un gandrīz pusē no tām ir gūti būtiski rezultāti, līdz ar ko vairākas lietas ir izdevies veiksmīgi noslēgt. 2023. gadā platforma sekmīgi atbalstīja 37 izmeklēšanas (attiecībā uz bērnu seksuālu izmantošanu, terorismu, kibernoziedzību, organizēto noziedzību, narkotiku kontrabandu un krāpšanu, kā arī augsta līmeņa finanšu izmeklēšanas), tostarp augstas prioritātes izmeklēšanas, piemēram, par *SkyECC* un *Encrochat*. Platforma ir kļuvusi par būtisku rīku tiesībaizsardzības iestādēm, taču ar to nepietiek, lai risinātu visus jautājumus, ar ko saskaras ES iestādes saistībā ar atšifrēšanu.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina turpināt pilnveidot un veicināt ES atšifrēšanas spēju izmantošanu

Aktori: Eiropas Komisija, Eiropols	*Laiks: 2028. gads*	*Budžets: noteiks dalībvalstis (piemēram, saskaņā ar IDF valsts programmām)*

- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju ar specializētu finansējumu (piemēram, IDF valstu programmās paredzētu) un paraugprakses apmaiņas palīdzību atbalstīt valstu iestāžu spēju vākt kvalitatīvu kontekstuālu informāciju, vienlaikus respektējot dalībvalstu ekskluzīvo kompetenci valsts drošības jautājumos, lai tās varētu palīdzēt palielināt Eiropola atšifrēšanas platformas efektivitāti.
- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju atbalstīt Eiropola investīcijas tehnisko spēju uzturēšanā un atšifrēšanas spēju uzlabošanā, ejot kopsolī ar tehnoloģiju attīstību un ņemot vērā pētniecību kvantu kriptogrāfijas jomā.
- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju finansiāli atbalstīt dalībvalstis **valsts un reģionālo atšifrēšanas spēju** attīstīšanā, lai papildinātu Eiropola centienus.

Pašreizējās ES finansēšanas programmas piedāvā ievērojamu atbalstu tiesībaizsardzībai. Šo iespēju turpmāka racionalizēšana palielinātu to ieguldījumu digitālās kriminālistikas departamentu spēju uzlabošanā un mazinātu atkarību no viena pārdevēja un tiesībaizsardzības paļaušanos uz "melnās kastes" rīkiem (t. i., rīkiem, kas apstrādā datus, un uzticamības iestādēm nav iespējas pārbaudīt, kā tie darbojas), kas izstrādāti ārpus ES.

Pasākumus to darbību (pētniecība, izstrāde, ieviešana) ciklā, kas būtu jāveic, lai tiesībaizsardzības iestādēm sniegtu reālu pievienoto vērtību, atbalsta dažādas shēmas. Lai pilnībā izmantotu ES līmenī pieejamās iespējas, valstu pārvaldes iestādēm, tiesībaizsardzības iestādēm un nozares praktiķiem būtu jāapzinās katras konkrētās programmas un mehānisma funkcijas un mērķi.

Ar pamatprogrammu "Apvārsnis Eiropa" ir atbalstīti dažādi veiksmīgi projekti, kuros ir aktīvi piedalījušies tiesībaizsardzības praktiķi. Tomēr pamatprogramma "Apvārsnis Eiropa" ir pētniecības programma, un būtu jāpielāgo gaidas attiecībā uz to, cik tuvu izstrādātie instrumenti ir tam, lai tos varētu praktiski izmantot.

Projekta *Tools4LEAs*, ko finansē IDF un vada *EACTDA*, mērķis ir veicināt drošības pētniecības projektu rezultātu ieviešanu un nodrošināt pilnībā testētus un ekspluatācijai gatavus programmatūras rīkus bez licences izmaksām un ar ES sabiedriskās drošības organizāciju piekļuvi pirmkodam. *Tools4LEAs* ir vislabākās iespējas, balstoties uz pētniecības projektu rezultātiem, palīdzēt nodrošināt izmantojamus rīkus. Eiropols piedalās projektā *Tools4LEAs* un kopā ar visiem galalietotājiem, kas ir *EACTDA* dalībnieki, vada tā darbu.

EuCB ir izveidojusi vairāk nekā 15 dalībvalstu pamatgrupas, lai kopīgi izmantotu jaunās tehnoloģijas un līdzradītu inovatīvus rīkus. Dalībvalstis ir izmantojušas *EuCB* pamatgrupas, lai koordinētu daļu no inovatīvo rīku, kas finansēti ar IDF dotācijām, piemēram, *MARIT-D, ProfID* un tīmekļa pārmeklētāju, izstrādes. Pamatgrupas ir ideāls satvars, kurā dalībvalstis var koordinēt digitālo izmeklēšanas rīku līdzradīšanu.

Izmantojot mērķtiecīgus *uzaicinājumus iesniegt priekšlikumus IDF ietvaros*, Eiropas Komisija turpina finansēt projektus, kas ir ievērojami veicinājuši operatīvo darbību panākumus. Piemēram, projektā *CERBERUS* tika konstatētas *EncroChat* sistēmas ievainojamības, kas ļaus Francijas žandarmērijai – ar Nīderlandes Valsts kriminālistikas institūta un *UCD* atbalstu – to likvidēt. Savukārt projekts *FREETOOL* [28], ko vada *UCD* Kiberdrošības un kibernoziedzības izmeklēšanas centrs, ļāva izstrādāt virkni bezmaksas kibernoziedzības izmeklēšanas rīku [29], kas pielāgoti konkrētām tiesībaizsardzības prasībām digitālo izmeklēšanu un analīzes jomā. Šie rīki tika izstrādāti sadarbībā ar tiesībaizsardzību un ir brīvi pieejami tiesībaizsardzības kopienai. 3000 lietotāji no vairāk nekā 100 tiesībaizsardzības iestādēm, kas pārstāv desmitiem jurisdikciju, ir pieteikušies uz piekļuvi rīkiem, kurus arī organizācijas līmenī ir pieņēmušas vairākas tiesībaizsardzības iestādes un kurus izmanto augsta līmeņa izmeklēšanās. *Programma "Tiesiskums"* attiecas arī uz tiesu iestāžu sadarbību krimināllietās un varētu veicināt pārrobežu sadarbību digitālo izmeklēšanas rīku izmantošanā.

---

28 https://www.ucd.ie/cci/projects/freetool/.

29 Rīki aptver dažādus izmeklēšanas posmus: publiskos avotos pieejamu datu ieguve (*OSINT*) pirmsmeklēšanas posmā; tiešraides datu kriminālistika; atmiņas analīze; *OSINT* pēcmeklēšanas posmā un tiešsaistes resursu saglabāšana; automatizēta datņu/artefaktu izgūšana; kriminālistikas ziņojumi; mediju apstrāde; un artefaktu ģeolokācija.

Eiropola rīku repozitorijs (ERR) kopš izveides ir attīstījies un patlaban aptvert vairāk nekā 40 progresīvus rīkus, kas nodrošina tiešu piekļuvi progresīvām tehnoloģijām Eiropas tiesībaizsardzības vajadzībām. Katru mēnesi tiek pievienoti jauni rīki, un repozitorijs ir kļuvis par galveno avotu nozares praktiķiem Eiropas Savienībā, kuri meklē programmatūru, kas palīdzētu veikt izmeklēšanas. Pašlaik ERR ir vairāk nekā 2,7 tūkstoši lietotāju, un dažādie tā rīki ir lejupielādēti vairāk nekā 7,8 tūkstošus reižu. Valstu izmeklēšanas vienības šos rīkus ir plaši izmantojušas, lai atbalstītu daudzveidīgas darbības, tostarp attiecībā uz dažādām noziedzības jomām, piemēram, cilvēku tirdzniecību, smago un organizēto noziedzību, kibernoziedzību un seksuālu vardarbību pret bērniem tiešsaistē. ERR piedāvā tādu ES finansētu projektu tiešas izmantošanas iespēju, kuri piedāvā konkrētus un galīgus rezultātus un kuru radītāji vēlas tos licencēt Eiropolam izplatīšanai visās Eiropas tiesībaizsardzības iestādēs. Izraudzītie partneri no projektiem *INSPECTr, Tools4LEAs* un *FORMOBILE* jau ir kopīgojuši rīkus repozitorijā. Eiropols sadarbojas ar ES Tiesībaizsardzības apmācības aģentūru (*CEPOL*) nolūkā piedāvāt lietotājiem apmācību par ERR rīkiem.

Turklāt programmai "Digitālā Eiropa" būtu aizvien plašāk jāveicina sinerģija un papildināmība starp kiberdrošību un kibernoziedzības apkarošanu – jomām, kas bieži vien balstās uz vieniem un tiem pašiem digitālās kriminālistikas rīkiem un metodēm.

Pašlaik nav mehānisma, kas nodrošinātu, ka digitālās kriminālistikas rīki atbilst pārskatatbildības un kriminālistikas standartiem ES. Šādam mehānismam būtu jānodrošina tehnisks izvērtējums, kas nodrošina, ka tiek pilnībā ievērots samērīgums (t. i., tiek sniegts apliecinājums, ka rīks ļauj piekļūt mērķorientētai informācijai un līdz ar to analīze aprobežojas tikai ar to, kas ir nepieciešams), pārredzamība un atbildētāja tiesības (t. i., tiek sniegts apliecinājums, ka rīks izgūst informāciju, kas ir autentiska un precīza, tādējādi sniedzot garantijas advokātiem un neatkarīgiem kriminālistikas ekspertiem, kas sniedz liecības tiesā) un citas juridiskās prasības (piemēram, atbilstība MI aktam). Tas palielinātu pierādījumu uzticamību tiesā – valstu, kā arī pārrobežu līmenī – un līdz ar to stiprinātu pārrobežu sadarbību.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina mērķtiecīgi finansēt projektus digitālās kriminālistikas rīku izpētei, izstrādei un ieviešanai

Aktori: Eiropas Komisija, Eiropols, dalībvalstis, EACTDA, ENFSI | *Laiks: sākot ar 2024. gadu* | *Budžets:*

- Augsta līmeņa grupas eksperti aicina dalībvalstis **digitālās kriminālistikas projektus, ko finansē no to attiecīgajām IDF valsts programmām, integrēt esošajos mehānismos** (piemēram, *EMPACT*) vai tīklos (piemēram, *ECTEG, EACTDA*), lai varētu izmantot citu dalībvalstu nozares praktiķu pieredzi un vienlaikus veicinātu rezultātu izplatīšanu un izmantošanu citās tiesībaizsardzības iestādēs.

- Augsta līmeņa grupas eksperti atzinīgi vērtē Eiropas Komisijas pašreizējos centienus atbalstīt digitālās kriminālistikas rīku izpēti, izstrādi un ieviešanu, izmantojot finansējumu no attiecīgajām finanšu programmām: **"Apvārsnis Eiropa"**, **"Digitālā Eiropa"** un **IDF**. Atkarībā no pieejamajiem resursiem Eiropas Komisija ik pēc diviem gadiem publicēs **atklātus uzaicinājumus iesniegt priekšlikumus** IDF ietvaros kibernoziedzības un digitālo izmeklēšanu jomā.

- Augsta līmeņa grupas eksperti atzinīgi vērtē Eiropas Komisijas pašreizējos centienus IDF ietvaros finansēt ***EACTDA***, lai *EACTDA* varētu ES sabiedriskās drošības organizācijām nodrošināt pilnībā testētus un ekspluatācijai gatavus programmatūras rīkus bez licences izmaksām un ES sabiedriskās drošības organizāciju piekļuvi pirmkodam.

- Augsta līmeņa grupas eksperti atzinīgi vērtē Eiropas Komisijas pašreizējos centienus finansēšanas iespēju ietvaros veicināt **Eiropola rīku repozitorija** izmantošanu kā galveno centru rīku izplatīšanai; tie mudina **Eiropola Inovācijas laboratoriju** turpināt centienus, lai ES tiesībaizsardzībai darītu pieejamus uzticamus, drošus, bezmaksas, viegli instalējamus un mērogojamus izmeklēšanas rīkus.

- Augsta līmeņa grupas eksperti aicina turpināt apsvērt tādu **shēmu izveidi** ES līmenī, kas paredzētas komerciālu digitālās kriminālistikas rīku **izvērtēšanai un – attiecīgā gadījumā – sertifikācijai**. To var darīt, piemēram, **Eiropas Tiesu ekspertīzes institūtu tīkla ietvaros.**

Digitālās kriminālistikas rīku licences ir dārgas, un dažkārt dažas tiesībaizsardzības iestādes tās nevar atļauties. Kopīga licenču iegāde – ar iespēju licences pēc tam kopīgot starp dažādu dalībvalstu iestādēm – var ļaut vienoties par zemākām cenām.

Ar projektu *iProcureNet* [30], ko finansē no pamatprogrammas "Apvārsnis Eiropa", ir izveidota metodika kopīgam iepirkumam drošības jomā, kā arī dalībvalstu iepirkuma iestāžu tīkls. Ņemot vērā *ES Inovācijas centra iekšējai drošībai* sastāvu un darba organizāciju, tas būtu piemērots tam, lai piedalītos dalībvalstu kopīgo vajadzību definēšanā un noteiktu, kuri rīki būtu vislietderīgākie, ar noteikumu, ka tiek izveidots specializēts digitālās kriminālistikas darba virziens.

Bieži vien digitālās kriminālistikas rīki rada papildu problēmas, kas nav saistītas vienīgi ar izmaksām. Piemēram, ar šiem rīkiem izgūtie dati var būt strukturēti vai pasniegti formātā, kas neatbilst esošajām iekšzemes informācijas sistēmām, kuras izmanto turpmākai apstrādei (piemēram, datu analīzei vai kopīgošanai). Tāpēc ir jānoformulē dalībvalstu kopīgo prasību kopums attiecībā uz to datu struktūru un formātu, kas iegūti, izmantojot digitālās kriminālistikas rīkus. Pamatojoties uz to, dalībvalstu iestādes spētu iesaistīties diskusijās ar digitālās kriminālistikas rīku nodrošinātājiem, lai panāktu, ka to prasības varētu pienācīgi ņemt vērā, piemēram, saistībā ar kopīgām iepirkuma procedūrām, kā minēts iepriekš.

Galvenā darbība: Augsta līmeņa grupas eksperti uzsver, ka, iegādājoties digitālās kriminālistikas rīkus, ir vajadzīga labāka cenas un vērtības attiecība

Aktori: dalībvalstis, Eiropas Komisija, ES Inovācijas centrs iekšējai drošībai, Eiropols	*Laiks: sākot ar 2025. gadu (kopīgais iepirkums)*	*Budžets: nav norādīts*

- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju:
  - palīdzēt dalībvalstīm **noteikt digitālās kriminālistikas rīkus**, kas visvairāk nepieciešami efektīvām izmeklēšanām (iespējams, ES Inovācijas centra iekšējai drošībai ietvaros);
  - atbalstīt **sadarbību starp operatīvajām vienībām un kontaktpunktiem iepirkuma iestādēs**, ko apvieno *iProcureNet*;
  - izveidot **digitālās kriminālistikas rīku licenču kopīgas iegādes pilotprojektu**.
- Augsta līmeņa grupas eksperti uzskata, ka **Eiropolam** ir iespēja palīdzēt dalībvalstīm noteikt **kopīgas prasības attiecībā uz tādu datu struktūru un formātu, kas iegūti**, izmantojot digitālās kriminālistikas rīkus, un, pamatojoties uz to, veicināt sadarbību starp attiecīgajām valsts iestādēm un ekspertiem, dodot tiem iespēju iesaistīties sadarbībā ar minēto rīku ražotājiem un izstrādātājiem, lai tie varētu vienoties par standartiem un pienācīgi ņemt vērā dalībvalstu prasības.

[30] https://www.iprocurenet.eu/.

II. Apmaiņīties ar spējām un koplietot sensitīvus rīkus

Ievainojamību izmantošana nolūkā piekļūt atšifrēšanas atslēgām ierīcēm pašlaik joprojām ir galvenā tiesībaizsardzības iespēja, kā piekļūt šifrētam saturam, ņemot vērā atšifrēšanas spēju ierobežoto pieejamību (piemēram, Eiropola atšifrēšanas platforma) un to, ka trūkst efektīvas sadarbības ar nozari vai specializēta tiesiskā regulējuma, ar ko nodrošināt likumīgu piekļuvi digitālajās ierīcēs esošajai informācijai.

Pat ja šie nosacījumi (daži no tiem) zināmā mērā varētu būt izpildīti, noziedznieki, visticamāk, izmantos specializētas šifrētas ierīces, lai slēptu informāciju vai nelikumīgu saturu. Tādējādi tiesībaizsardzībai tuvākajā nākotnē joprojām būs jāizmanto sensitīvi rīki [31] un spējas un, iespējams, tie jākoplieto.

2. ieteikumu kopa

Lai koplietotu sensitīvus rīkus un saistīto spēju atbildīgu pārvaldību, eksperti iesaka:

1. *apsvērt tādu mehānismu izveidi, ar kuriem var nodrošināt, ka sensitīvus rīkus var koplietot tā, lai pilnībā tiktu ievēroti valstu noteikumi [1. ieteikums];*
2. *izveidot procesu, kas paredzēts tādu spēju apmaiņai, kuras potenciāli ietver ievainojamību izmantošanu, kas ļautu apvienot zināšanas un resursus, vienlaikus nodrošinot to, ka tiek ievērota informācijas konfidencialitāte un sensitivitāte [6. ieteikums];*
3. *iespējams, izpētīt Eiropas pieeju tādu ievainojamību pārvaldībai un atklāšanai, ko risina tiesībaizsardzība, pamatojoties uz pašreizējo labo praksi [2. ieteikums].*

Izmantojot pamatprogrammu "Apvārsnis Eiropa" un IDF, Eiropas Komisija ir atbalstījusi projektus (*EXFILES* un *ForRES* [32]), kas veltīti neaizsargātībai un programmatūras izmantošanai, nodrošinot tiesībaizsardzības speciālistiem rīkus un protokolus ātrai un konsekventai datu ieguvei, kas tomēr atbilst visām attiecīgajām tiesību normām.

---

31 Ar "sensitīviem rīkiem" saprotama gan digitālā kriminālistika, gan taktiskās pārtveršanas rīki.

32 https://forres.eu.

Sensitīvu rīku un saistīto spēju koplietošana starp uzticamiem Eiropas partneriem atvieglo operatīvo sadarbību, ļauj savstarpēji izmantot zināšanas un rada apjomradītus ietaupījumus, samazinot nepieciešamos resursus.

Lai gan ievainojamību izmantošana dažkārt joprojām ir ļoti svarīgs faktors izmeklēšanās, rīcībai šajā ziņā ir jābūt ļoti piesardzīgai un ir jāievēro attiecīgais iekšzemes tiesiskais regulējums, jo šāda izmantošana ietekmē aparatūras un programmatūras drošības parametrus.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina atbalstīt sensitīvu rīku koplietošanu un saistīto spēju atbildīgu pārvaldību

Aktori: dalībvalstis, Eiropas Komisija *Laiks: sākot ar 2024. gadu* *Budžets: nav norādīts*

- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju turpināt atbalstīt projektus, kas paredzēti sensitīvu rīku (gan digitālās kriminālistikas, gan taktiskās pārtveršanas rīku) kopīgošanai un resursu apvienošanai, izmantojot attiecīgas finansēšanas programmas; turklāt Komisija varētu atbalstīt **zināšanu strukturēšanai un koplietošanai paredzētas transnacionālas platformas izveidi**.

- Augsta līmeņa grupas eksperti aicina Eiropas Komisijas *JRC* izpētīt, vai ir iespējams izstrādāt **Eiropas pieeju ievainojamību pārvaldībai un atklāšanai**, ar ko nodarbotos tiesībaizsardzība, pamatojoties uz esošo labo praksi.

III. Kolektīvas investīcijas prasmju attīstīšanā un zinātības uzlabošanā digitālās kriminālistikas jomā

Attiecīgie tiesībaizsardzības darbinieki būtu jāapmāca pielietot izmeklēšanas rīkus un metodes, ko izmanto izmeklēšanās, un viņu zinātība būtu jāsertificē. To prasītajām un dokumentētajām kompetencēm būtu jāatbilst to lomai un jāaptver vismaz vispārēja digitālā kriminālistika darbam ar mobilajām ierīcēm (dažādu rīku pratība), temati saistībā ar pārraudzības ķēdi / pierādījumiem un pamatprincipi attiecībā uz dažādiem iegūšanas, analīzes, ziņošanas veidiem un dalību iztiesāšanā. Dokumentācijā vajadzētu būt atspoguļotam, vai šīs prasmes ir iegūtas apmācībā vai darbā.

3. ieteikumu kopa

Lai atbalstītu prasmju un zinātības attīstīšanu digitālās kriminālistikas jomā, tostarp atšifrēšanu un standartizāciju, eksperti iesaka:

1. *palielināt apmācības iespēju skaitu ekspertiem [7. ieteikums];*
2. *izveidot ES līmeņa sertifikācijas shēmu digitālās kriminālistikas ekspertiem nolūkā garantēt sniegtās tehniskās apmācības kvalitāti un vienveidību [7. ieteikums];*
3. *ieguldīt, lai novērstu tehnisko prasmju trūkumu standartizācijas jomā un palielinātu informētību, panākot vienošanās ar akadēmiskajām aprindām un citiem attiecīgiem institūtiem [8. ieteikums].*

CEPOL rīko apmācības kursus par vairākiem būtiskiem tematiem [33]. Eiropas Kibernoziedzības apkarošanas apmācības un izglītības grupa (*ECTEG*) [34] izstrādā kursus par kibernoziedzību un digitālo kriminālistiku un dara tos pieejamus bez maksas *CEPOL* un valstu tiesībaizsardzības iestādēm.

ECTEG ir izstrādājusi *Decrypt* – apmācības resursu, ar ko uzlabot ES dalībvalstu tiesībaizsardzības iestāžu likumīgās atšifrēšanas spējas, izmantojot sarežģītas stratēģijas likumīgai rīcībai ar šifrētiem pierādījumiem. *CEPOL*, kā arī valstu vienības var pielietot *Decrypt*, izmantojot infrastruktūru, ko ir darījis pieejamu *JRC*.

---

[33] Digitālās kriminālistikas izmeklētāju apmācība, mobilā kriminālistika, tiešraides datu kriminālistika un *Mac* kriminālistika.

[34] *ECTEG* ir bezpeļņas organizācija, kas apvieno 30 tiesībaizsardzības iestādes no 20 Eiropas valstīm, starptautiskām struktūrām un akadēmiskajām aprindām. Ar IDF atbalstu *ECTEG* izstrādā, popularizē un kopīgo apmācības resursus, risinājumus un materiālus. Sk. https://www.ecteg.eu/.

Vienlīdz svarīgi ir nodrošināt ātrās reaģēšanas dienestu darbiniekiem pamatprasmes digitālās kriminālistikas jomā. Līdzās citiem projektiem *ECTEG* ir izveidojusi *eFirst* ("Tiesībaizsardzības ātrās reaģēšanas dienestu darbinieku izglītošana par svarīgākajiem kiberjomas aspektiem"). *eFirst* ir tiešsaistes pašpalīdzības apmācības modulis, kas paredzēts policistiem uz vietas (patrulēšana, nozieguma vieta, kratīšana dzīvesvietā) vai amatpersonām, kuru uzdevums ir pieņemt cietušā sākotnējo sūdzību. Tas sniedz pamatzināšanas par kibernoziedzību un digitālo kriminālistiku. To var izmantot arī par pamatu klātienes kursiem policijas akadēmijās.

Ekspertu profilu sertifikācija nodrošina, ka katrai personai ir nepieciešamās zināšanas un prasmes. Tā motivē profesionāļus attīstīt prasmes un sekot līdzi norisēm savā jomā, kā arī atbalsta karjeras izaugsmi un personisku atzinību. Tā rezultāts ir kvalitatīvāks un precīzāk izpildīts darbs. Turklāt personas sertifikācija var:

- sniegt skaidru un pārredzamu aprakstu par digitālās kriminālistikas ekspertu prasmēm un kompetencēm, ļaujot nozares praktiķiem, kā arī struktūrvienību vadītājiem noteikt, kura persona atbilst nepieciešamajām prasībām, kas vajadzīgas attiecīgo uzdevumu efektīvai izpildei;

- veicināt apmācības kursu izstrādi un vadīt to organizēšanu valsts, reģionālā un ES līmenī; salīdzināma policijas apmācība visās ES dalībvalstīs nodrošina, ka visām policijas amatpersonām ir piekļuve konsekventam zināšanu un prasmju līmenim neatkarīgi no valsts, no kuras viņi nāk;

- veicināt pārredzamāku tiesvedību;

- palielināt uzticēšanos starp izmeklētājiem un citiem aktoriem, tādējādi stiprinot starptautisko sadarbību starp valstu tiesībaizsardzības iestādēm.

CEPOL ir sākusi izstrādāt *Nozaru kvalifikācijas ietvarstruktūru* policijas darbībai, galveno uzmanību pievēršot pārrobežu sadarbībai. Šo modeli var operacionalizēt, pamatojoties uz darbu, ko *ECTEG* sava *Globālās ar kibernoziedzības jomu saistītās sertifikācijas projekta* [35] ietvaros ir veikusi digitālās kriminālistikas ekspertu sertifikācijas jomā.

Gan *ECTEG*, gan *EACTDA* daļu no saviem resursiem investē, lai atbalstītu *attiecīgo tiesībaizsardzības praktiķu* efektīvu *dalību standartizācijas procesos*, piemēram, atvieglojot nepieciešamo prasmju apguvi.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina uzlabot tehniskās prasmes un sertificēt profilus

Aktori: CEPOL, ECTEG | *Laiks: darbības notiek; digitālās kriminālistikas ekspertu sertifikācijas shēmu paredzēts izstrādāt līdz 2026. gadam* | *Budžets:*

- Augsta līmeņa grupas eksperti aicina *CEPOL* turpināt **piedāvāt** apmācību kursus (jo īpaši pasniedzēju apmācības kursus).
- Augsta līmeņa grupas eksperti aicina *ECTEG* turpināt **izstrādāt un atjaunināt** apmācības kursus par digitālo kriminālistiku ekspertiem un ātrās reaģēšanas dienestu darbiniekiem, īpašu uzmanību pievēršot atšifrēšanai, **kā arī īstenot pilotprojektus** saistībā ar šādiem kursiem.
- Augsta līmeņa grupas eksperti atzinīgi vērtē Komisijas pastāvīgos centienus (izmantojot atklātus uzaicinājumus iesniegt priekšlikumus IDF ietvaros) atbalstīt *ECTEG*, kā arī apmācības kursu **izvēršanu** reģionālā līmenī.
- Augsta līmeņa grupa aicina *ECTEG* turpināt izskatīt iespēju ES līmenī ieviest digitālās kriminālistikas ekspertu sertifikācijas shēmu un aicina *CEPOL* pēc iespējas vairāk sniegt ieguldījumu šajos centienos, balstoties uz darbu pie **Nozaru kvalifikācijas ietvarstruktūras** policijas darbībai un pie **Globālās ar kibernoziedzības jomu saistītās sertifikācijas**.
- Augsta līmeņa grupa aicina *ECTEG* turpināt atvieglot attiecīgo nozares praktiķu iespējas **iegūt kompetences un zinātību par standartizācijas procesiem**.

[35] https://www.ecteg.eu/running/gcc/.

IV. Atvieglot likumīgu piekļuvi

Bez normām, kas reglamentē integrētu likumīgu piekļuvi, tiesībaizsardzības iestādēm aizvien vairāk jāizmanto ievainojamības, lai piekļūtu izņemtajām ierīcēm, kurās esošā informācija ir aizsargāta ar šifrēšanu. Tomēr, lai gan šī metode var veicināt izmeklēšanas, tā rada lielas finansiālās izmaksas. Tāpēc ir jāapsver iespējamas alternatīvas.

4. ieteikumu kopa

Lai izveidotu mehānismus sadarbībai ar attiecīgajiem nozares partneriem un izpētītu iespēju noteikt saistošus standartus un tuvināt tiesību aktus likumīgas piekļuves jomā atbilstīgi Eiropas Savienības Tiesas (EST) un Eiropas Cilvēktiesību tiesas judikatūrai, eksperti iesaka:

1. *izstrādāt platformu (*SIRIUS *vai tai līdzvērtīgu) nolūkā koplietot rīkus, paraugpraksi un zināšanas par to, kā nodrošināt piekļuvi produktu īpašnieku, ražotāju un aparatūras ražotāju datiem [11. ieteikums];*

2. *kartēt tiesībaizsardzības kontaktpunktus digitālās aparatūras un programmatūras ražotāju satvarā [11. ieteikums];*

3. *veikt visaptverošu kartēšanu un izstrādāt ES rokasgrāmatu par spēkā esošajiem tiesību aktiem dalībvalstīs, lai detalizēti norādītu digitālās aparatūras un programmatūras ražotāju juridiskos pienākumus izpildīt tiesībaizsardzības iestāžu datu pieprasījumus, ņemot vērā konkrētus scenārijus un prasības, kas uzņēmumiem liek piekļūt ierīcēm [25 ieteikums];*

4. *izveidot pētniecības grupu, lai novērtētu integrētas likumīgas piekļuves pienākumu (tostarp attiecībā uz piekļuvi šifrētiem datiem) tehnisko iespējamību digitālajām ierīcēm, vienlaikus saglabājot un neapdraudot ierīču drošību un visu lietotāju informācijas privātumu, kā arī nevājinot vai neapdraudot sakaru drošību [26. ieteikums];*

5. *atkarībā no iepriekš minētās kartēšanas izstrādāt saistošus nozares standartus ierīcēm, kas laistas ES tirgū, nolūkā integrēt likumīgu piekļuvi un veicināt tiesību aktu tuvināšanu šajā jomā [25. ieteikums].*

Tiesībaizsardzības pašreizējā iesaiste ar nozari neveicina konkrētu rezultātu sasniegšanu; ir jāpastiprina sadarbība ar nozari, lai tiesībaizsardzības iestādēm radītu iespējas likumīgi piekļūt ierīcēm un lietojumprogrammām. Piemēram, videonovērošanas ierakstīšanas gadījumā tiesībaizsardzības iestādes aizvien biežāk saskaras ar šifrētām datnēm, kuras nevar analizēt ar automātisku programmatūru, jo īpaši tad, ja videomateriālu apjoms ir liels.

Teorētiski tiesībaizsardzības iestādes var lūgt atbalstu ierīču ražotājiem, kuri savukārt var darīt pieejamu savas programmatūras pirmkodu, lai atvieglotu piekļuvi nešifrētiem satura datiem, vai nodrošināt tāda aprīkojuma tehnisko dokumentāciju, kas ir kriminālizmeklēšanu priekšmets.

Eiropolam būtu labas iespējas apkopot paraugpraksi (piemēram, tiesībaizsardzības kontaktpunktu izveide) un zināšanas par to, kā produktu īpašnieki, ražotāji un aparatūras ražotāji varētu atvieglot piekļuvi un darīt to pieejamu visām tiesībaizsardzības iestādēm ar *SIRIUS* (vai līdzvērtīgas platformas) starpniecību.

Vienlaikus būtu jāapsver pārredzamāki risinājumi, kas ļauj piekļūt nešifrētiem datiem izņemtajās ierīcēs, lai palielinātu izmeklēšanu efektivitāti un vienlaikus nodrošinātu vienlīdzīgus konkurences apstākļus nozares dalībniekiem, saglabājot kiberdrošību un aizsargājot privātumu.

Pamatojoties uz detalizētu analīzi par tiesībaizsardzības prasībām attiecībā uz likumīgu piekļuvi, eksperti mudina Eiropas Komisiju izstrādāt *tehnoloģiju ceļvedi* [36], kurā būtu apvienotas tehnoloģiju, kiberdrošības, privātuma, standartizācijas un drošības ekspertu darbības un nodrošināta pienācīga koordinācija.

Viena no galvenajām darbībām saskaņā ar šo tehnoloģiju ceļvedi būtu izvērtēt, vai ir *tehniski iespējams ieviest integrētas likumīgas piekļuves pienākumus* (tostarp attiecībā uz piekļuvi šifrētiem datiem un šifrētiem videonovērošanas sistēmu (*CCTV*) ierakstiem) attiecībā uz digitālajām datnēm un ierīcēm [37], vienlaikus nodrošinot stingrus kiberdrošības aizsardzības pasākumus un nevājinot vai neapdraudot sakaru drošību. Šis izvērtējums tiktu veikts, iesaistot visas attiecīgās ieinteresētās personas.

---

[36] Ziņojuma vairākās nodaļās ir vairākkārtēja atsauce uz unikālu "tehnoloģiju ceļvedi".

[37] Sk. *"Moving the Encryption Policy Conversation Forward"* (Virzīt uz priekšu atšifrēšanas politikas apspriešanu), *Carnegie Endowment for International Peace* – https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

Ciktāl šāds izvērtējums apstiprinātu iepriekš minētajiem nosacījumiem atbilstošu integrētas likumīgas piekļuves pienākumu esamību vai īstenojamību, tehnoloģiju ceļvedī būtu jādefinē arī process ilgstspējīgai ilgtermiņa *sadarbībai ar standartizācijas struktūrām*. Tiesībaizsardzības līdzdalību šajā standartizācijas procesā varētu koordinēt Eiropols ar *EACTDA* atbalstu.

Pamatojoties uz kartēšanu, kas veikta attiecībā uz dalībvalstu pašreizējo tiesisko regulējumu, kurā noteikti digitālās aparatūras un programmatūras ražotāju pienākumi, kas paredz tiesībaizsardzības iestāžu datu pieprasījumu izpildi, būtu iespējams izvērtēt, vai ir vajadzīgi *tiesību akti vai pamatnostādnes un ieteikumi* [par šīs jomas tiesību aktu tuvināšanas veicināšanu].

Galvenā darbība: Augsta līmeņa grupas eksperti aicina pastiprināt sadarbību ar nozari, sekmēt atsauci uz attiecīgajiem standartiem gaidāmajās ES iniciatīvās un tuvināt tiesību aktus likumīgas piekļuves jomā saskaņā ar EST un Eiropas Cilvēktiesību tiesas judikatūru

Aktori: Eiropols; Eiropas Komisija *Laiks: sākot ar 2025. gadu* *Budžets: nav norādīts*

- Augsta līmeņa grupas eksperti aicina **Eiropas Komisiju** izstrādāt īpašu **tehnoloģiju ceļvedi**, lai izpētītu iespējas likumīgi piekļūt digitālajām ierīcēm.
- Augsta līmeņa grupas eksperti aicina **Eiropolu** apkopot paraugpraksi un zināšanas par to, kā produktu īpašnieki, ražotāji un aparatūras ražotāji varētu atvieglot piekļuvi un darīt tās pieejamas visām tiesībaizsardzības iestādēm ar ***SIRIUS*** (vai līdzvērtīgas platformas) starpniecību.

II nodaļa: Datu saglabāšana

PROBLĒMJAUTĀJUMI

Ja agrāk vāktie pierādījumi primāri bija lietiski pierādījumi, mūsdienās milzīgu daudzumu potenciālo pierādījumu metadatu veidā glabā sakaru nodrošinātāji. Lai gan digitālie dati nav vienīgie pierādījumi, kas nepieciešami kriminālizmeklēšanu kontekstā, šāda veida pierādījumi ir kritiski svarīgi – jo īpaši, lai noteiktu aizdomās turēto vai interesējošo subjektu, kuriem var būt svarīga informācija, identitāti – gandrīz visās izmeklēšanās neatkarīgi no tā, vai tie attiecas uz noziegumiem, kas izdarīti fiziskajā vai digitālajā pasaulē. Jo īpaši attiecībā uz pēdējo minēto aspektu – saziņas metadati (jo īpaši IP adreses un pieslēgvietu numuri) bieži vien var būt vienīgais veids, kā identificēt aizdomās turēto [38].

Tāpēc, lai tiesībaizsardzības iestādes varētu izmeklēt noziegumus digitālajā laikmetā, ir nepieciešams, lai digitālie pierādījumi vajadzības gadījumā tiktu darīti pieejami lasāmā formātā un piekļūstamā veidā, pienācīgi ievērojot atbilstošus kriminālprocesa aizsardzības pasākumus, procesuālās tiesības un privātumu un datu aizsardzību. Datus var glabāt uzņēmējdarbības vajadzībām (piemēram, rēķinu un pavadzīmju izrakstīšanai) vai tiesībaizsardzības nolūkos. Datu saglabāšana var palīdzēt nodrošināt, ka dati ir pieejami, lai kompetentās iestādes tiem varētu piekļūt kriminālizmeklēšanu un kriminālvajāšanu kontekstā. Pakalpojumu sniedzēju saglabātajiem datiem var būt izšķiroša nozīme, lai efektīvi apkarotu noziedzību, un šādu datu saglabāšana ir priekšnoteikums, lai nodrošinātu turpmāku tiesībaizsardzības piekļuvi tiem un nodrošinātu, ka tiesībaizsardzības iestādes var veikt izmeklēšanas [39]. Tajā pašā laikā datu minimizēšanas princips, kas noteikts E-privātuma direktīvā [40] un Vispārīgajā datu aizsardzības regulā (VDAR) [41], paredz, ka pakalpojumu sniedzējiem būtu jāglabā (vai citādi jāapstrādā) datplūsmas dati tikai tik ilgi, cik tas nepieciešams pašas saziņas vajadzībām, rēķinu izrakstīšanai vai – konkrētās situācijās – *ECS* tirdzniecības nolūkā. Jebkura cita glabāšana ir jāreglamentē ar tiesisko regulējumu, kas atbilst E-privātuma direktīvas 15. pantā noteiktajām prasībām. Šis režīms atspoguļo nepieciešamību līdzsvarot pamattiesības uz privātumu un datu aizsardzību ar tiesībaizsardzības pasākumu mērķiem.

---

38 Eksperti apsprieda vairākus piemērus attiecībā uz digitālo datu nozīmi izmeklēšanā un datu pieprasījumu skaitu. Viens no ekspertiem norādīja, ka pēdējos piecos gados visās izmeklēšanās, kas saistītas ar terorismu vai organizēto noziedzību, tika izmantoti no pakalpojumu sniedzējiem pieprasīti dati. 2023. gadā vienā dalībvalstī no operatoriem identifikācijas nolūkos kriminālprocesos tika pieprasīti vairāk nekā 1 300 000 numuru, un gandrīz visus no tiem vēlāk validēja tiesu sistēma.

39 Šajā dokumentā "piekļuve datiem" ir piekļuve, ko piešķir tiesībaizsardzības iestādēm, vajadzības gadījumā saņemot *ex ante* tiesas atļauju, kriminālizmeklēšanas nolūkos un izskatot katru gadījumu atsevišķi.

40 Direktīva 2002/58/EK, 6. pants.

41 Regula (ES) 2016/679, 5. panta 1. punkta c) apakšpunkts.

Pašlaik nav ES tiesību aktu, kas reglamentētu datu saglabāšanu. ES Tiesa 2014. gadā atcēla ES Datu saglabāšanas direktīvu [42], uzsverot būtisko iejaukšanos pamattiesībās uz privātumu un datu aizsardzību, kas raksturīga pakalpojumu sniedzēju sākotnēji savākto datu glabāšanai tiesībaizsardzības nolūkos [vispārīgi un nediferencēti] [43]. Tā rezultātā ir notikušas izmaiņas valstu tiesiskajā regulējumā, kā rezultātā visā ES ir radušās būtiskas atšķirības [44]: kamēr dažās dalībvalstīs joprojām ir spēkā noteikumi, kas uzliek sakaru pakalpojumu sniedzējiem pienākumu saglabāt noteiktas datu kategorijas tiesībaizsardzības nolūkos, citas ir ieviesušas izmaiņas, lai izpildītu judikatūrā ierosināto kritēriju – mērķorientēta datplūsmas datu saglabāšana; [45] citās (arī tāpēc, ka valstu tiesas attiecīgi ir pieņēmušas turpmākus spriedumus) nav īpašu noteikumu par datu saglabāšanu tiesībaizsardzības nolūkos, un tās paļaujas tikai uz datiem, ko uzņēmumi saglabājuši uzņēmējdarbības nolūkos. Nosacījumi piekļuvei šādiem datiem ir atkarīgi no piemērojamā valsts tiesiskā regulējuma un no datu veida (abonentu, datplūsmas vai satura dati). Tas, ka trūkst saskaņotu un harmonizētu datu saglabāšanas pienākumu visā ES, noved pie atšķirīgām prasībām dalībvalstīs attiecībā uz to, kā tiek reglamentēta dažādu veidu metadatu saglabāšana (un tās ilgums), ko veic pakalpojumu sniedzēji.

---

42 Direktīva 2006/24/EK. Direktīvā ES dalībvalstīm tika noteikts pienākums pieņemt pasākumus, lai nodrošinātu, ka elektronisko sakaru pakalpojumu sniedzēji un tīklu nodrošinātāji saglabā datu plūsmas datus un atrašanās vietas datus, kā arī saistītos datus, kas vajadzīgi abonenta vai reģistrētā lietotāja identificēšanai laikposmā no sešiem mēnešiem līdz diviem gadiem, lai kompetentajām iestādēm nodrošinātu piekļuvi smagu noziegumu izmeklēšanas, atklāšanas un kriminālvajāšanas saistībā ar tiem nolūkos, kā noteikts valsts tiesību aktos.

43 Pārskatu par attiecīgo judikatūru sk.: *The future of national data retention obligations – How to apply Digital Rights Ireland at national level? – European Law Blog*, *V. Franssen*; *Recalibrating Data Retention in the EU – eucrim*; *Eurojust/EJCN* 2024. gada ziņojums. *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*; *Cybercrime Judicial Monitor* – Nr. 6; *Cybercrime Judicial Monitor* – Nr. 9

44 Dalībvalstu reakcija uz Datu saglabāšanas direktīvas atcelšanu atšķīrās, un valsts līmenī sāktās darbības palielināja valstu datu saglabāšanas sistēmu dažādību. Kā atzīmēts *Eurojust/EJCN* 2024. gada ziņojumā par datu saglabāšanu , 2018.–2022. gadā izmaiņas savos tiesību aktos veica 12 valstis. Respondenti atbildēja, ka šīs izmaiņas bija tiešas sekas ES Tiesas lietai C-746/18 *Prokuratuur* un apvienotajām lietām C-511/18, C-512/18 un C-520/18 *La Quadrature du Net u. c*. 23 no 27 dalībvalstīm ir ieviesti noteikumi par datu saglabāšanu; septiņas dalībvalstis jau ir ieviesušas noteikumus par mērķorientētu datu saglabāšanu. Pārskatu sk. Komisijas dokumentā *Study on the retention of electronic communications non-content data for law enforcement purposes* (Apsekojums par elektroniskās saziņas ar saturu nesaistītu datu saglabāšanu tiesībaizsardzības nolūkos), 2020, 39. lpp.

45 Datu plūsmas un atrašanās vietas datu mērķorientētas saglabāšanas jēdzienu Tiesa ir izstrādājusi vairākos spriedumos, lemjot, ka datu saglabāšana var būt saderīga ar ES tiesībām, ja tā ir izstrādāta, lai to vērstu uz konkrētiem mērķiem un konkrētām vajadzībām. Tomēr Tiesas ierosināto kritēriju praktiskā piemērošana šādu mērķu izstrādei ir radījusi grūtības un izaicinājumus augstākās instances tiesās tajās dalībvalstīs, kuras to mēģināja.

Dalībvalstīs, kurās nav datu saglabāšanas pienākumu, ir grūti vai dažkārt neiespējami kriminālizmeklēšanā identificēt aizdomās turēto vai personu, kurai var būt būtiska informācija ("interesējošu subjektu") [46]. Kad jaunie e-pierādījumu noteikumi būs stājušies spēkā, to pievienotā vērtība arī tiktu uzlabota, ja tos papildinātu ar datu saglabāšanas pienākumiem, jo pretējā gadījumā nav garantijas, ka būs pieejama informācija, uz kuru attiecas Eiropas saglabāšanas vai sniegšanas rīkojumi (kas aptver datplūsmas datus, datus, kas pieprasīti vienīgi lietotāja identificēšanai, un abonentu datus).

Pašreizējie apstākļi ietekmē gan **tiesībaizsardzību**, gan **sakaru pakalpojumu sniedzējus**, bet, pats svarīgākais, tie **ietekmē iedzīvotājus un cietušos**, kuru tiesības uz tiesu pieejamību nevar nodrošināt, ja izmeklēšana sākas tad, kad dati jau ir dzēsti vai nav saglabāti [47].

I. Jautājumi, kas ir atsevišķu dalībvalstu jurisdikcijā

Dalībvalstīs, **kurās nav konkrētu pienākumu** attiecībā uz datu saglabāšanu tiesībaizsardzības nolūkos, izmeklēšana papildus jebkādiem citiem pieejamiem pierādījumiem balstās uz datiem, ko uzņēmumi glabā saviem uzņēmējdarbības un komerciālajiem mērķiem. Uz komercdatiem attiecas pakalpojumu sniedzēju iekšējā politika, proti, uzņēmumi glabā datplūsmas datus uz dažādiem periodiem (piemēram, aptuveni 6 mēnešus), savukārt atrašanās vietas datus, kuriem parasti nav nozīmes uzņēmējdarbības nolūkos, bieži glabā īsāku laiku. Bieži vien mazie uzņēmumi vispār neglabā abonentu vai saziņas metadatus vai uzglabā tos ļoti īsu laiku. Tā rezultātā izmeklēšana bieži vien ir sacensība ar laiku, jo izmeklētājiem datu sniedzējs ir jāidentificē un pieprasījums saskaņā ar piemērojamajiem noteikumiem jānosūta pirms dati tiek dzēsti, kas dažkārt var notikt dažu dienu vai stundu laikā. Dažos gadījumos uzņēmumi nesniedz informāciju par konkrētiem datiem, kurus tie apstrādā un tur, tāpēc kompetentajām iestādēm ir grūti iesniegt mērķorientētus pieprasījumus, kad tās cenšas iegūt datus. Daži mitināšanas pakalpojumi ļauj lietotājiem nomāt vietu uz servera, izmantojot fiktīvus datus, kas nozīmē, ka pat tad, ja tie glabā lietotāju datus, tie nav uzticami [48].

---

46 Sk. piemēru, kas aprakstīts informatīvajā dokumentā *Operational challenges faced by law enforcement related to access to data Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement* (Operatīvie izaicinājumi, ar kādiem saskaras tiesībaizsardzība saistībā ar piekļuvi datiem. Ieguldījums pirmajā Augsta līmeņa grupa jautājumos par piekļuvi datiem efektīvas tiesībaizsardzības nolūkos plenārsēdē), 4. lpp.

47 Saistībā ar ietekmi uz iedzīvotājiem un cietušajiem sk. *Dwyer*/*Commissioner of An Garda Siochána* – [2020] IESC 4 (24/02/2020), īpaši 9. punktu.

48 https://en.wikipedia.org/wiki/Bulletproof_hosting.

Lielākajā daļā dalībvalstu **ir spēkā** tiesību akti **par datu saglabāšanu**. Tomēr, kā aprakstīts iepriekš, dažu valstu tiesību aktos ir veiktas izmaiņas pēc ES Tiesas nolēmumiem, kas izrietēja no Datu saglabāšanas direktīvas atzīšanas par spēkā neesošu. Tas ir radījis daudzveidīgu vidi, un dalībvalstis uz spriedumiem reaģē atšķirīgi. Dažās dalībvalstīs ir īstenoti centieni, lai ieviestu mērķorientētu saglabāšanas veidu, ko ES Tiesa ir ierosinājusi kā iespējamu turpmāko virzienu datu saglabāšanas jomā. Tomēr Augsta līmeņa grupas eksperti ir uzsvēruši, ka šādu kritēriju īstenošana rada juridiskas un tehniskas problēmas attiecībā uz to īstenojamību [49], un pakalpojumu sniedzēji ir kritizējuši izmaksas, kas saistītas ar mērķorientētas saglabāšanas un, vispārīgāk, bieži mainīgu tiesību aktu tehnisko īstenošanu. Vēl viena būtiska juridiska problēma, kas novērota valsts līmenī, ir tas, ka valstu tiesību akti vairumā gadījumu neattiecas uz *OTT* pakalpojumiem. Konkrētais gadījums saistībā ar *OTT* pakalpojumiem plašāk tiks aplūkots 1.3. iedaļā.

II. Pārrobežu problēmjautājumi Eiropas Savienībā

Problēmas datu saglabāšanas jomā rodas arī saistībā ar pārrobežu pieprasījumiem, t. i., kad kompetentā iestāde cenšas iegūt datus no pakalpojumu sniedzēja, kas atrodas citā dalībvalstī. Gadījumos, kas saistīti ar pārrobežu pieprasījumiem, saņēmējas valsts iestādes var nespēt izpildīt citas valsts izdotu pieprasījumu (datu trūkuma vai attiecīgu tiesību normu neesamības dēļ).

Tā kā visā ES nav saskaņotu pienākumu attiecībā uz metadatu glabāšanu, rodas šķēršļi tiesībaizsardzības iestādēm vienā dalībvalstī, kuras **cenšas iegūt datus** no pakalpojumu sniedzējiem, kas atrodas citās dalībvalstīs. Pat tad, ja valsts līmenī ir ieviesti datu saglabāšanas režīmi, nav saskaņotības starp valstu sistēmām attiecībā uz saglabāšanas periodiem, un tie dalībvalstu starpā ievērojami atšķiras [50].

---

[49] Lai gan ES Tiesa sniedz zināmus norādījumus un piemērus tam, kā interpretēt datplūsmas datu **mērķorientētu saglabāšanu**, judikatūra var sniegt tikai indikatīvas norādes un nav pietiekami precīza, lai sīki izklāstītu iespējamos ierobežojumus attiecībā uz visu datu kategoriju saglabāšanu. Attiecīgi pēdējos gados Tiesā ir iesniegtas vairākas lietas par datu saglabāšanas noteikumiem, un dalībvalstis nespēj nodrošināt juridisko noteiktību.

[50] Atkarībā no datiem un nozieguma veida metadati var tikt saglabāti no 6 līdz 72 mēnešiem. *Eurojust/EJCN* 2024. gada ziņojumā par datu saglabāšanu respondenti norādīja, ka bija pieejams mazāk datu saglabāto datu trūkuma dēļ, ierobežojumu dēļ, kas noteikti saglabājamo datu kategorijām, un īsu (īsāku) saglabāšanas periodu dēļ. Līdz ar to datu nepieejamība ietekmē arī iestāžu spēju izpildīt Eiropas izmeklēšanas rīkojumus un savstarpējās tiesiskās palīdzības pieprasījumus.

Tāpat ES līmenī nav saskaņotas pieejas attiecībā uz saglabājamo **datu definēšanu** [51]. Valsts tiesību akti var uzlikt pakalpojumu sniedzējiem pienākumu glabāt dažādas datu kategorijas dažādiem mērķiem (nodokļi, revīzijas, tiesībaizsardzība). Tie arī atšķiras pēc detalizācijas pakāpes, ko tie šajā sakarā sniedz, jo dažos tiesību aktos ir sīki uzskaitīti ar saturu nesaistīti dati, kas jāsaglabā, savukārt citos ir sniegtas plašākas ar saturu nesaistītu datu definīcijas [52]. Atkarībā no piedāvātā pakalpojuma un uzņēmējdarbības un komerciālajām vajadzībām pakalpojumu sniedzēji arī saglabā dažādu veidu datus uz dažādiem periodiem. Tas rada ļoti daudzveidīgu vidi, kur pastāv būtiskas atšķirības ne tikai starp dalībvalstīm, bet arī starp pakalpojumiem.

Šādas atšķirības ir būtiskas arī tādēļ, ka tās starp dalībvalstīm pastāv attiecībā uz piekļuvi saglabātajiem datiem: dažās dalībvalstīs tiek prasīta tiesas atļauja piekļuvei dažu veidu metadatiem, bet citās ne. Pakalpojumu sniedzēji norāda, ka viens no iemesliem, kāpēc notiek kavēšanās un tiesībaizsardzības pieprasījumu neizpilde, ir juridiskā nenoteiktība attiecībā uz noteikumiem, kas piemērojami datu izpaušanai.

---

51 Kā norādīts Komisijas apsekojumā par datu saglabāšanu, 48. lpp.: "Lai gan noteiktus informācijas veidus visās dalībvalstīs vienmēr klasificē kā abonentu datus vai datu plūsmas datus, nav vienprātības par šādu datu punktu klasifikāciju: IP adreses, *SIM* numuri, ierīces identifikācijas numuri (piemēram, *IMSI*, *IMEI*) un dinamisko IP adrešu pieslēgvietu numuri. Dažās dalībvalstīs (EE, FR, IE) šos datu punktus klasificē kā abonentu datus, savukārt citās (DE, ES, IT, PL, SI) – kā datu plūsmas datus."

52 Sk. Komisijas apsekojuma par datu saglabāšanu III pielikumu, kur sniegts pārskats par katrā dalībvalstī saglabātajiem datiem.

Kompetentajām iestādēm ir jāievēro valsts noteikumi, kas piemērojami pakalpojumu sniedzējam, kurš tur pieprasītos datus, kā arī konkrētās prasības, ko nosaka paši pakalpojumu sniedzēji. Kā ziņots *SIRIUS* 2022. gada ziņojumā [53], pakalpojumu sniedzēji var pieprasīt, lai tiktu izmantoti īpaši šim nolūkam domāti portāli vai pieprasījumi tiktu iesniegti konkrētās veidnēs vai valodās. Tie var arī pieprasīt informāciju par lietas raksturu, skaidru atsauci uz pieprasījuma juridisko pamatu valsts tiesību aktos vai to, ka attiecībā uz prasītajiem datiem tiek noteikti konkrēti īsi laikposmi. Lai gan daži no šiem jautājumiem tiks risināti, līdz 2026. gadam īstenojot e-pierādījumu paketi, Augsta līmeņa grupas eksperti uzsvēra, ka ir vajadzīga saskaņotība starp šiem noteikumiem un jebkādu iespējamu saskaņotu datu saglabāšanas satvaru. Lai gan Eiropas Telesakaru standartu institūts (*ETSI*) ir izstrādājis standartus numuratkarīgu starppersonu sakaru pakalpojumu (tradicionālo telesakaru) metadatu pieprasījumu formātam, tos pakalpojumu sniedzēji nepiemēro visās dalībvalstīs konsekventi. Standarti attiecībā uz datu pārraidi no *OTT* [54] pakalpojumu sniedzējiem uz tiesībaizsardzības iestādēm ir darbs, kas turpinās, un tie nav pilnībā īstenoti. Turklāt pakalpojumu sniedzēji var brīvi izlemt, kādā formā tie vāc un glabā lietotāju datus, un tā rezultātā praktiķi saņem neapstrādātus datus ļoti dažādās formās; tas rada ievērojamu slogu tiesībaizsardzības iestādēm, kas gūtu labumu no racionalizētiem procesiem, **saziņas sistēmām un formātiem** pieprasījumu iesniegšanai un atbilžu uz pieprasījumiem un datu nosūtīšanai un saņemšanai. Standartizētas saziņas sistēmas un formāti arī samazinātu pieprasījumu apstrādes izmaksas uzņēmumiem.

Tiklīdz tiesībaizsardzības iestādes ir ieguvušas likumīgu piekļuvi datiem, tām jāspēj tos izmantot; tāpēc datiem jābūt **lasāmiem**. Tomēr pakalpojumu sniedzēji arvien vairāk piedāvā pakalpojumus, kas ļauj pilnīgi (*end-to-end*) šifrēt datplūsmas datus, un, ja tie pēc pieprasījuma sniedz šos datus tiesībaizsardzības un tiesu iestādēm, tie tos bieži vien sniedz šajā šifrētajā formā.

---

53 sirius-eu-digital-evidence-situation-report-2022, 14. lpp.

54 Šajā ziņojumā "*over-the-top* (*OTT*) sakaru pakalpojumi" apzīmē lietojumprogrammas un pakalpojumus, kas nodrošina sakaru un mediju pakalpojumus (piemēram, ziņojumapmaiņu un balss un video zvanus) internetā bez tradicionālo telesakaru pakalpojumu sniedzēju (telesakaru uzņēmumu) iesaistīšanās vai kontroles. Izplatīti *OTT* sakaru pakalpojumu piemēri ir ziņojumapmaiņas lietotnes, piemēram, *WhatsApp*, *Telegram*, *Facebook Messenger*; balss un video zvanu pakalpojumi, piemēram, *Skype*, *Zoom*, *Google Meet*, *Viber*; un sociālo mediju platformas, piemēram, *Instagram* un *Snapchat* (ziņojumapmaiņa un multimediāla satura kopīgošana).

Visbeidzot, citas šāda *status quo* apjaustās sekas ir saistītas ar risku, ka tiesībaizsardzības **pierādījumi tiks apstrīdēti** tiesā [55]. ES Tiesa ir precizējusi, ka datu saglabāšanas ceļā iegūtu pierādījumu pieņemamība ir valsts tiesību jautājums [56], ievērojot līdzvērtības un efektivitātes principus [57]; Tādējādi atšķirības starp valstu datu saglabāšanas režīmiem var ietekmēt pierādījumu pieņemamību pārrobežu tiesvedībā [58].

---

55 Sk. nodaļu "Pierādījumu vākšana un pieņemamība" *Eurojust/EJCN* 2024. gada ziņojumā par datu saglabāšanu.

56 ES Tiesas 2020. gada 6. oktobra spriedums *La Quadrature du Net u. c.*, lieta C-511/18, ECLI:EU:C:2020:791 222.–228. punkts; 2022. gada 5. aprīļa spriedums *Commissioner of An Garda Síochána u. c.*, lieta C-140/20, ECLI:EU:C:2022:258, 127. punkts.

57 Turpat, 223. punkts: "(..) ar nosacījumu, ka (..) minētie noteikumi nav mazāk labvēlīgi par noteikumiem, kas reglamentē līdzīgas iekšējās darbības (līdzvērtības princips), un ka tie nepadara praktiski neiespējamu vai pārmērīgi grūtu ES tiesību sistēmas piešķirto tiesību izmantošanu (efektivitātes princips)."

58 Vairākās tiesvedībās ir apstrīdēta ar saturu nesaistītu datu kā pierādījumu pieņemamība. Kopsavilkumu sk. Komisijas apsekojumā par datu saglabāšanu, 41. lpp.

III. Problēmjautājumi, kas saistīti ar *OTT* un citiem pakalpojumu sniedzējiem

Lai gan iepriekš minētie jautājumi attiecas uz visiem *ECS* sniedzējiem, *OTT* pakalpojumu sniedzēji rada papildu izaicinājumus tiesībaizsardzības iestāžu likumīgā piekļuvē datiem. Gan valstu, gan ES līmenī *OTT* pakalpojumu sniedzēji bieži vien neuzskata, ka tiem ir saistoši tādi paši pienākumi kā tradicionālajiem sakaru pakalpojumu sniedzējiem. Lai gan *OTT* pakalpojumu sniedzēji ietilpst *EECC* darbības jomā, tas, ka tie bieži vien ir iedibināti ārpus ES un ka nepastāv licencēšanas sistēmas (t. i., uz tiem var attiekties tikai vispārējas atļaujas) un sankcijas, rada nenoteiktību attiecībā uz to pienākumiem saglabāt datus, tostarp konkrētus datu veidus, un apgrūtina atbilstības nodrošināšanu. Turklāt, lai gan tradicionālie sakaru pakalpojumu sniedzēji vairumā gadījumu uzņēmējdarbības vajadzībām saglabā dažus datus, kas ļauj identificēt lietotājus (piemēram, IP numurus ar pieslēgvietas numuru un laikposmu), tas tā nav ar ***OTT* pakalpojumu sniedzējiem**, kuri glabā tikai tādus ar saturu nesaistītus datus, kas nepieciešami to komerciālajām vajadzībām, un dažos gadījumos tikai uz īsu laiku [59]. *OTT* pakalpojumu sniedzēji nesaglabā nekādus ar saturu nesaistītus datus, kas piesaistīti dinamiskai IP adresei (pieslēgvietas numurs un laikposms). Tas var apgrūtināt vai pat padarīt neiespējamu metadatu izgūšanu par saziņu, kas notiek, izmantojot tādas sistēmas kā *WhatsApp* vai *Telegram*, kuras tiek izmantotas arvien vairāk. Kā jau minēts, saglabāto datu veidi atšķiras arī atkarībā no piedāvātā pakalpojuma. Lai gan dažos gadījumos pakalpojumu sniedzēji izdod pamatnostādnes, kurās aprakstīti to saglabāto datu veidi [60], citos gadījumos *OTT* pakalpojumu sniedzēji šo informāciju neatklāj. Tas, kā arī fakts, ka nepastāv **pārredzamības pienākumi** attiecībā uz datu veidiem, ko pakalpojumu sniedzēji ģenerē, apstrādā un uzglabā uzņēmējdarbības nolūkos, bieži rada problēmas tiesībaizsardzības iestādēm, kad tās mēģina noteikt, vai dati ir saglabāti, kas tur kādus datus un kāda veida datu kopas var pieprasīt, un galu galā tad, kad tās nosūta pieprasījumus pakalpojumu sniedzējiem.

---

[59] Tas jo īpaši attiecas uz maziem pakalpojumu sniedzējiem. Saskaņā ar Komisijas apsekojumu par datu saglabāšanu,103. lpp., IP adreses tiek saglabātas vidēji 30 dienas.

[60] Sk., piemēram, law-enforcement-guidelines-outside-us.pdf (apple.com).

Tajā pašā laikā arvien pieaugošais pieprasījumu skaits, ko saņem pakalpojumu sniedzēji, [61] apvienojumā ar vajadzību apstrādāt liela apjoma datu kopas veicina pieprasījumu aizkavēšanos vai noraidīšanu [62]. Papildus cēloņiem, kas izriet no konkrētiem pakalpojumu sniedzēju lēmumiem saskaņā ar to uzņēmējdarbības modeli, tas ir saistīts arī ar to, ka pastāv **ierobežots skaits mehānismu sadarbībai** starp tiesībaizsardzības un tiesu iestādēm, no vienas puses, un privātiem uzņēmumiem, no otras puses.

Visbeidzot, lai gan uz tiem var neattiekties *EECC* sakaru pakalpojumu sniedzēju definīcija, vairākas jaunās tehnoloģijas un citi digitālie dalībnieki (piemēram, automobiļu ražotāji un lielu valodu modeļu (*LLM*) MI sistēmas) ģenerē saziņas metadatus, kas var sniegt informāciju par noziedzīgām darbībām, un rīkojas ar tiem. Neraugoties uz pieaugošo datu apjomu, ar kuriem šie pakalpojumi rīkojas, pašlaik tiem nav saistoši datu saglabāšanas pienākumi.

IESPĒJAMIE RISINĀJUMI

I. Stiprināt sadarbību starp sakaru pakalpojumu sniedzējiem un praktiķiem

Situācijā, kad digitālo pierādījumu vākšanu kavē saskaņotu noteikumu trūkums, tiesībaizsardzības iestādēm izmeklēšanas veikšanā bieži ir jāpaļaujas uz **brīvprātīgu sadarbību** ar pakalpojumu sniedzējiem. Lai gan šis risinājums ir palīdzējis dažās redzamās izmeklēšanās [63], to vajā juridiska nenoteiktība un tas ne vienmēr ir dzīvotspējīgs: brīvprātīga sadarbība ir atkarīga no pakalpojumu sniedzēja veida un lieluma, un mazie uzņēmumi salīdzinājumā ar lielākiem bieži glabā datus ļoti īsu laiku vai tiem nav resursu, lai atbildētu uz tiesībaizsardzības iestāžu pieprasījumiem [64].

---

61 Kā atzīmēts *SIRIUS* 2023. gada ziņojumā, pakalpojumu sniedzējiem iesniegto datu pieprasījumu apjoms katru gadu pastāvīgi pieaug (sk. 66. lpp. un turpmāk).

62 *SIRIUS* 2023. gada ziņojumā (61. zemsvītras piezīme) sniegts pārskats par galvenajiem elektronisko pierādījumu pieprasījumu kavēšanās/noraidīšanas iemesliem (sk. 68. lpp. un turpmāk).

63 Sk. piemērus *SIRIUS* 2023. gada ziņojumā (61. zemsvītras piezīme), 19. lpp.

64 *SIRIUS* 2023. gada ziņojumā (61. zemsvītras piezīme), 79. lpp. norādīts, ka lielais pieprasījumu skaits brīvprātīgas sadarbības ietvaros pakalpojumu sniedzējiem ir problemātisks, un tiem tiek ieteikts piedalīties *SIRIUS* starptautiskajos pasākumos, lai "mazāki *OSP* varētu izmantot *SIRIUS* projekta speciālās zināšanas sadarbībā ar varasiestādēm nolūkā palielināt izpratni par šo jautājumu, strukturēt savu politiku reaģēšanai uz iestāžu pieprasījumiem un nodrošināt, ka tie ir gatavi gaidāmajām norisēm likumdošanā".

Partnerību un sadarbības ar nozari pamatā ir jābūt **skaidram tiesiskajam regulējumam**, kas ir būtisks elements jebkurā dzīvotspējīgā risinājumā, kas ļauj tiesībaizsardzības un tiesu iestādēm pārvarēt grūtības likumīgi piekļūt digitāliem pierādījumiem. Papildus tam, ka abas puses pilda savus attiecīgos juridiskos pienākumus, ir svarīgi izveidot pastāvīgas un uzticībā balstītas attiecības starp tiesībaizsardzības praktiķiem un pakalpojumu sniedzējiem, lai tie saprastu viens otra vajadzības un kopīgi varētu rast praktiskus risinājumus. Ir vajadzīgi stabili **mehānismi sadarbībai** ar privāto sektoru, lai **palielinātu pārredzamību** attiecībā uz datiem, ko pakalpojumu sniedzēji ģenerē un uzglabā, un to, cik ilgi tie tiek saglabāti, kā arī lai nodrošinātu to **datu saskaņotu kategorizāciju**, kuri jāsaglabā un kuriem paredzēts piekļūt, izstrādātu **standartizētus formātus** datu pieprasīšanai un izveidotu **drošus kanālus** tiešai apmaiņai starp kompetentajām iestādēm un pakalpojumu sniedzējiem.

Var izpētīt vairākus iespējamos variantus šādas sadarbības stiprināšanai, no kuriem dažiem ir saistošs raksturs (saistoši tiesību akti), bet citi ir ieteikuma tiesību risinājumi. Daži no šajā iedaļā uzskaitītajiem risinājumiem būtu jāizvērtē II iedaļā minētā ietekmes novērtējuma kontekstā un pēc tam jānosaka tiesību aktos.

5. ieteikumu kopa

Lai nodrošinātu, ka kompetentās iestādes būtu spējīgas meklēt attiecīgus datus, pareizi identificējot datu turētājus, ka šādus pieprasījumus pakalpojumu sniedzēji saņem standartizētos formātos un ka pārrobežu sadarbību nekavē tiesību normu kolīzijas, eksperti iesaka:

1. *izveidot un stiprināt sadarbību starp tiesībaizsardzības praktiķiem un pakalpojumu sniedzējiem, lai atbalstītu informācijas apmaiņu, spēju veidošanu un apmācību un lai noteiktu sadarbības principus un kārtību [13. ieteikums], piemēram, izveidojot starpniecības iestādi, kas ļautu kompetentajām iestādēm identificēt attiecīgos pakalpojumu sniedzējus un labāk orientēt likumīgus pieprasījumus [18. ieteikums]. To varētu panākt šādi:*

    a. *par pamatu izmantojot esošās ES līmeņa struktūras, piemēram, SIRIUS, Eiropas Tiesiskās sadarbības tīklu (EJN) / Eiropas Tiesu iestāžu tīklu kibernoziedzības jautājumos (EJCN), ES Interneta forumu;*

    b. *ar saprašanās memorandiem, izmantojot paraugpraksi, kas iedibināta dažās dalībvalstīs valsts līmenī [14. ieteikums];*

2. *veicinot pārredzamības noteikumus elektronisko sakaru pakalpojumu un citu sakaru pakalpojumu sniedzējiem attiecībā uz datiem, ko tie apstrādā, ģenerē vai glabā savas uzņēmējdarbības gaitā, un par to, kā informēt tiesībaizsardzības iestādes par to, kādi dati ir pieejami, ņemot vērā ierobežojumus, kurus rada izmeklēšanas konfidencialitāte, izmantojot sadarbības nolīgumus ar pakalpojumu sniedzējiem vai vajadzības gadījumā nosakot obligātus pienākumus [17. ieteikums, 16. ieteikums];*

3. *izstrādājot racionalizētus procesus un formātus, pamatojoties uz saskaņotiem standartiem pieprasījumu iesniegšanai pakalpojumu sniedzējiem un atbilžu saņemšanai strukturētā veidā [15. ieteikums], un platformās veicinot vienoto kontaktpunktu izraudzīšanos kompetento iestāžu pieprasījumu apstrādei un saziņai ar tām [36. ieteikums];*

4. *izveidojot mehānismus ar mērķi nodrošināt, ka pārrobežu pieprasījumi tiek mērķorientēti uz pakalpojumu sniedzējiem efektīvā veidā un novērš iespējamus konfliktus, iedvesmojoties no e-pierādījumu mehānismiem un nodrošinot šādu mehānismu saskaņotību ar noteikumiem, kas paredzēti E-pierādījumu regulā [19. ieteikums].*

Pašlaik ir izveidotas ES struktūras, kas ļauj attiecīgiem aktoriem iepazīties ar rīkiem un paraugpraksi. Vienuviet pulcējot tiesībaizsardzības iestādes, tiesu iestādes un pakalpojumu sniedzējus, projekts *SIRIUS* varētu veicināt apmaiņu ar zināšanām un rīkiem, kas saistīti ar pieprasījumiem pēc pakalpojumu sniedzēju turētiem lietotāju datiem [65], un, jo īpaši pateicoties esošajam *SIRIUS* vienoto kontaktpunktu tīklam, kalpot par platformu tiešai saskarsmei starp pieprasījuma iesniedzējām iestādēm un pakalpojumu sniedzējiem [66]. *SIRIUS* varētu kalpot kā juridisko instrumentu, judikatūras, formātu utt. **centrālais repozitorijs**, kā tas ir pārrobežu e-pierādījumu apmaiņas gadījumā [67].

ES Interneta forums [68], būdams jau esoša kopdarbības vide dalībvalstīm, interneta nozarei un citiem partneriem, varētu kalpot kā telpa, kurā ES līmenī varētu veidot tiešus kontaktus un uzticēšanos starp attiecīgajiem aktoriem saistībā ar darbībām, kas saistītas ar piekļuvi digitāliem datiem. Tas varētu palīdzēt izveidot un atjaunināt **atvērtu katalogu** ar datu veidiem, ko vāc un apstrādā pakalpojumu sniedzēji un tie, kas ar datiem rīkojas, šādu katalogu, iespējams, centralizēti pārvaldītu *SIRIUS*. Šāds katalogs mazinātu pašreizējo pārredzamības trūkumu un radītu lielāku skaidrību tiesībaizsardzības un tiesu iestādēm par to, kādus datus tās var pieprasīt, kā arī darbotos kā starpniecības iestāde, lai noteiktu, kam pieprasījums būtu jānosūta. Turklāt gadījumā, ja pakalpojumu sniedzējiem tiktu uzlikti juridiski pienākumi, katalogs sniegtu pievienoto vērtību pārredzamības pienākumu īstenošanas uzraudzībā un novērtēšanā attiecībā uz to datu veidiem, ko pakalpojumu sniedzēji glabā vai citādi apstrādā.

---

65 *SIRIUS* vienoto kontaktpunktu tīkls, kas ir ekspertu tīkls likumīgu datu pieprasījumu jomā, popularizē paraugpraksi un mudina valstis izveidot pašām savu vienoto kontaktpunktu tīklu. Vienotie kontaktpunkti ir izraudzītas personas, struktūrvienības vai iestādes, kas centralizē, pārskata un iesniedz valdības iestāžu pieprasījumus pakalpojumu sniedzējiem. Pašlaik šajā tīklā piedalās 36 tiesībaizsardzības iestādes no 25 valstīm.

66 Projekts *SIRIUS* kalpo kā punkts, kurā vērsties saistībā ar elektronisko datu iegūšanu no pakalpojumu sniedzējiem, kas atrodas citās jurisdikcijās. *SIRIUS* nodrošina ierobežotas piekļuves platformu zināšanu un paraugprakses apmaiņai tiesībaizsardzības un tiesu iestāžu kopienām. Projektā *SIRIUS* tiek uzturēta atjaunināta vairāk nekā 1000 uzņēmumu kontaktinformācijas krātuve, kurā galvenā uzmanība pievērsta mazākiem, grūti atrodamiem vai dažkārt nepieejamiem pakalpojumu sniedzējiem. Tāpēc kompetentās iestādes ar vienu operāciju var izgūt vairākas adreses, kas tām palīdz efektīvāk apstrādāt lielus sarežģītas informācijas apjomus. SIRIUS project | Eiropols (europa.eu).

67 *SIRIUS* ir ES finansēts projekts, kas palīdz tiesībaizsardzības un tiesu iestādēm piekļūt pārrobežu elektroniskajiem pierādījumiem kriminālizmeklēšanas un tiesvedības ietvaros. Projekts *SIRIUS*, ko ciešā partnerībā ar Eiropas Tiesiskās sadarbības tīklu (*EJN*) īsteno Eiropols un *Eurojust*, ir centrāls atsauces punkts Eiropas Savienībā zināšanu apmaiņai par pārrobežu piekļuvi elektroniskiem pierādījumiem. SIRIUS project | Eiropols (europa.eu).

68 European Union Internet Forum (EUIF) – Eiropas Komisija (europa.eu).

Izmantojot priekšrocības, ko dod sinerģija ar e-pierādījumu paketi, tiktu ietaupītas izmaksas un resursi un veicināta e-pierādījumu tiesību aktu pilnīga īstenošana. Piemēram, to, ka tiesībaizsardzības iestādes tiktu rosinātas izveidot vai paplašināt to vienību spējas, kuras darbojas kā vienotais kontaktpunkts attiecībā uz (pārrobežu) datu izpaušanas pieprasījumiem, – minēto varētu attiecināt arī uz pieprasījumiem, kas iesniegti valsts līmenī; vai prasību nodrošināt apmācības programmas izmeklētājiem un ātrās reaģēšanas dienestu darbiniekiem. Tāpat arī centienus, kas pašlaik tiek īstenoti saistībā ar e-pierādījumu paketes īstenošanu, proti, izveidot **digitālu platformu**, kas ļautu veikt tiešu apmaiņu starp kompetentajām iestādēm un pakalpojumu sniedzējiem, varētu kopēt attiecībā uz saziņas metadatiem, ko saglabā, pamatojoties uz valsts tiesību aktiem.

Dalībvalstis varētu apsvērt iespēju **saprašanās memorandus** ieviest kā instrumentus sadarbības veicināšanai un vienotas izpratnes veidošanai starp pakalpojumu sniedzējiem, valdību un tiesībaizsardzības iestādēm, lai atbalstītu valsts tiesību aktu darbību. Pozitīvi piemēri dažās dalībvalstīs varētu kalpot par iedvesmu to strukturēšanai, iesaistot visus attiecīgos aktorus (uzņēmumus, aģentūras u. c.), lai nodrošinātu, ka tiek aptverti visi nozīmīgie sadarbības aspekti (vienoto kontaktpunktu izvirzīšana pakalpojumu sniedzējiem un tiesībaizsardzības iestādēm, tehniskās vajadzības, sniedzamo datu kategoriju kopīga definēšana, kopīgas procedūras, standartizētu pieprasījumu modeļu izstrāde, datu drošība un datu minimizēšanas pasākumi utt.) [69]. Kā tika ieskicēts, **standartizēti protokoli** datu vākšanai no pakalpojumu sniedzējiem (tostarp *OTT* pakalpojumu sniedzējiem) un datu pieprasījumiem no kompetentajām iestādēm būtu izdevīgi gan tiesībaizsardzībai, gan pakalpojumu sniedzējiem, un tādējādi varētu izveidot automatizētus mehānismus atbilžu sniegšanai, samazinot izmaksas un taupot laiku. Lai gan starp **valsts līmeņa** un **pārrobežu pieprasījumiem** (saskaņā ar e-pierādījumu regulējumu) pastāv atšķirības prasību ziņā, tomēr varētu izstrādāt darbplūsmas un kanālus, pa kuriem dati tiek pieprasīti, jo standartizācija attiecas uz pieprasīto/saņemto datu formātu. Šādus standartizētus formātus vislabāk izstrādāt var tādas standartizācijas struktūras kā *ETSI*. Tomēr dalībvalstu tiesībaizsardzības ekspertu iesaiste šajos procesos līdz šim ir bijusi neliela. Šā iemesla dēļ esošā **Eiropas iekšējās drošības standartizācijas darba grupa**, ko vada Eiropols un Komisija, varētu koordinēt un veicināt dalībvalstu dalību šādos forumos. Darbu varētu balstīt uz pašreizējiem *ETSI* izstrādātajiem standartiem, kurus varētu paplašināt, lai aptvertu vēl citas datu kategorijas [70].

---

[69] Īrijas 2024. gada 6. aprīļa saprašanās memorands ir paredzēts, lai atbalstītu 2011. gada Sakaru (datu saglabāšanas) likuma (ar grozījumiem) darbību. Tieslietu departaments ir iecēlis neatkarīgu priekšsēdētāju, noteicis darba uzdevumus un uzaicinājis tiesībaizsardzības un pakalpojumu sniedzēju pārstāvjus.

[70] TS 102 657: Rīcība ar saglabātajiem datiem; nodošanas saskarne saglabāto datu pieprasīšanai un piegādei un saglabāto datu kategorijas (abonentu, lietošanas, aprīkojuma, tīkla elementu un rēķinu dati); TS 103 120: Saskarne informācijai par orderi (nosaka elektronisku saskarni starp divām sistēmām drošai informācijas apmaiņai saistībā ar likumīgas nepieciešamās rīcības izveidi un pārvaldību; parasti izmanto likumīgai pārtveršanai, bet to var izmantot saglabātiem datiem; parasti izmanto starp pakalpojumu sniedzēju, no vienas puses, un valdību vai tiesībaizsardzības iestādi, kas ir tiesīga pieprasīt likumīgu rīcību, no otras puses; TS 103 705: Datu struktūras likumīgai informācijas atklāšanai (izstrādes stadijā; tikai datu struktūras, bez nodošanas saskarnes, iepriekš noteiktas kokveida struktūras, pakalpojumu sniedzēja definēti veidi un informācija).

Galvenā darbība: Augsta līmeņa grupas eksperti aicina veicināt sadarbību un veidot vienotu izpratni starp pakalpojumu sniedzējiem, valdību un tiesībaizsardzības iestādēm

Aktori: Eiropas Komisija, dalībvalstis, Eiropols (SIRIUS), Eurojust, ES Interneta forums

Laiks: tiks noteikts vēlāk

- Augsta līmeņa grupas eksperti aicina **Eiropas Komisiju, Eiropolu** un **dalībvalstis** izvērtēt veidus, kā veicināt un uzlabot sadarbību starp tiesībaizsardzības iestādēm un privātiem uzņēmumiem, veicinot pastāvīgu dialogu un savstarpēju izpratni par operatīvajām, tehniskajām un uzņēmējdarbības vajadzībām. Saistībā ar II iedaļā minēto ietekmes novērtējumu augsta līmeņa grupas eksperti arī aicina Komisiju apsvērt īpašu pienākumu izstrādi attiecībā uz pārredzamību datu vākšanā un pastāvīgas sadarbības struktūras.

- Augsta līmeņa grupas eksperti aicina **Eiropas Komisiju**, **Eiropolu** un ***Eurojust*** izveidot vai popularizēt esošās platformas apmaiņai starp tiesībaizsardzības iestādēm un tiesu iestādēm, no vienas puses, un sakaru pakalpojumu sniedzējiem, no otras puses, lai izveidotu to datu katalogu par datiem, kurus sakaru pakalpojumu sniedzēji un tie, kas rīkojas ar datiem, ģenerē un glabā savas uzņēmējdarbības gaitā, un katalogu pārvaldītu *SIRIUS*.

- Augsta līmeņa grupas eksperti aicina **dalībvalstis** izpētīt iespēju noslēgt sadarbības nolīgumus un/vai saprašanās memorandus, kas radītu saikni starp pakalpojumu sniedzējiem, valdību un tiesībaizsardzības iestādēm, lai atbalstītu valstu tiesību aktu darbību, kopīgi nosakot principus un standarta praksi.

- Augsta līmeņa grupas eksperti aicina **Eiropolu** un **Eiropas Komisiju** izmantot esošo iekšējās drošības standartizācijas darba grupu, lai veicinātu dalībvalstu dalību standartizācijas forumos, tādējādi palīdzot definēt attiecīgos standartus un kopīgi izstrādāt protokolus, kuros detalizēti izklāstītas procedūras sadarbībai ar pakalpojumu sniedzējiem.

- Augsta līmeņa grupas eksperti aicina **Eiropas Komisiju**, **Eiropolu**, ***Eurojust/EJN*** un dalībvalstis izmantot sinerģiju ar tādiem instrumentiem kā e-pierādījumu pakete, lai izveidotu vai iegūtu attiecīgus rīkus, piemēram, paplašinot izstrādē esošo digitālo platformu izmantošanu, lai tās darbotos kā pieprasījumu iesniegšanas portāli.

II. Minimālo noteikumu saskaņošana attiecībā uz metadatu saglabāšanu, ko veic sakaru pakalpojumu sniedzēji, un kompetento iestāžu piekļuvi

Eksperti lielā mērā ir vienisprātis, ka ir vajadzīgs saskaņots ES regulējums, kas reglamentē metadatu saglabāšanu tiesībaizsardzības nolūkos. Šāds regulējums nodrošinātu standartizētus risinājumus, kā arī skaidrus un izpildāmus pienākumus sakaru pakalpojumu sniedzējiem un tiem, kas rīkojas ar datiem, attiecībā uz to, kad un kā saglabāt datus un kādos apstākļos nodrošināt piekļuvi minētajiem datiem. Nosakot skaidrus noteikumus par saglabāšanu un piekļuvi, šis regulējums paredzētu skaidrus pamattiesību un būtisko interešu aizsardzības pasākumus, ņemot vērā piemērojamās judikatūras norādes, kā arī skaidrību par noteikumiem, kas piemērojami sakaru pakalpojumu sniedzējiem attiecībā uz datu saglabāšanu un kopīgošanu tiesībaizsardzības nolūkos. Turklāt, nodrošinot datu saglabāšanu, šāda sistēma atbalstītu e-pierādījumu paketes pilnīgu īstenošanu.

6. ieteikumu kopa

Lai nodrošinātu, ka ir pieejami digitālie pierādījumi, kas vajadzīgi noziegumu izmeklēšanai un krimināvajāšanai saistībā ar tiem, ka starp dalībvalstīm nepastāv sadrumstalotība saglabāšanas noteikumos un aizsardzības pasākumos attiecībā uz pamattiesībām, jo īpaši privātumu un datu aizsardzību, vārda brīvību un apsūdzēto personu tiesībām, tostarp tiesībām uz pienācīgu procesu, un lai nodrošinātu juridisko noteiktību gan kompetentajām iestādēm, no vienas puses, gan elektronisko un citu sakaru pakalpojumu sniedzējiem, no otras puses, eksperti iesaka:

1. *noteikt metadatu kategorijas, pamatojoties uz datu izmantošanas nolūku (interesējošā subjekta tiešsaistes darbības identificēšana, atrašanās vietas noteikšana, konstatēšana vai novērtēšana) [28. ieteikums], lai nodrošinātu, ka elektronisko sakaru pakalpojumu sniedzēji un citi sakaru pakalpojumu sniedzēji saglabā datus, kas ir pietiekami vismaz subjekta identificēšanai [27. ieteikuma v) punkts];*
2. *paredzēt minimālos šādu datu glabāšanas termiņus;*
3. *izstrādāt nosacījumus piekļuvei saglabātajiem datiem [27. ieteikuma iv) punkts], kas atšķiras atkarībā no datu kategorijas, nozieguma kategorijas (piemēram, noziegumi, kas notiek tikai internetā) vai draudiem cietušajiem [29. ieteikums];*
4. *izstrādāt šādus juridiskus, regulatīvus un tehniskus noteikumus tā, lai tie nodrošinātu subjektu pamattiesību un pamatbrīvību pilnīgu ievērošanu un lai jebkādi minēto tiesību ierobežojumi būtu nepieciešami un samērīgi [27. ieteikuma vi) punkts];*
5. *nodrošināt, ka tie paši noteikumi, pienākumi un aizsardzības pasākumi attiecas uz tradicionālajiem sakaru pakalpojumu sniedzējiem,* OTT *pakalpojumiem un jebkuriem citiem esošiem vai turpmākiem pakalpojumu sniedzējiem, kas ģenerē un apstrādā datus [27. ieteikuma i) un ii) punkts];*
6. *nodrošināt, ka komerciālos un uzņēmējdarbības nolūkos glabātie lietotāju dati ir faktiski pieejami tiesībaizsardzībai saskaņā ar attiecīgajiem aizsardzības pasākumiem (31. ieteikums) un ka kompetentās iestādes spēj lasīt datus, kas likumīgi saņemti no pakalpojumu sniedzējiem [27. ieteikuma iii) punkts];*
7. *nodrošināt, ka dalībvalstis var piemērot sankcijas elektronisko un citu sakaru pakalpojumu sniedzējiem, kas nesadarbojas attiecībā uz datu saglabāšanu un sniegšanu, piemēram, īstenojot administratīvas sankcijas vai ierobežojot to spēju darboties ES tirgū [30. ieteikums].*

Attiecībā uz **metadatu saglabāšanu** būtu jānošķir datu kategorijas, proti, nošķirot interesējošā subjekta identificēšanai nepieciešamos datus (abonentu dati [71] un avota saziņas IP adreses [72]) no datu plūsmas [73] un atrašanās vietas [74] datiem un katrai kategorijai paredzot atšķirīgus saglabāšanas periodus un aizsardzības pasākumus. Arī piekļuves datiem posmā mērķis ir nodrošināt līdzsvaru starp izmeklējamā nozieguma smagumu un to, cik lielā mērā veicamie pasākumi iejaucas privātajā dzīvē. Saskaņā ar nesenu judikatūru [75] varētu izpētīt iespējas attiecībā uz minimālām prasībām ģeneriskai datu saglabāšanai, kas ir pietiekama, lai nodrošinātu, ka jebkuru lietotāju var skaidri identificēt. Attiecībā uz datu plūsmas un atrašanās vietas datiem ir jāizskata vēl citi un stingrāki kritēriji.

Lai šādu satvaru izstrādātu pēc iespējas nākotnes vajadzībām atbilstošākajā un **tehnoloģiski neitrālākajā** veidā, saglabājamo datu kategorizācija būtu jāformulē, pamatojoties uz tālredzīgu pieeju, ietverot ģeneriskas datu kopas, kuru pamatā ir, piemēram, datu funkcijas (dati, kas ļauj unikāli identificēt saziņas avotu vai galamērķi, dati, kas ļauj identificēt saziņas avota atrašanās vietu utt.), apvienojumā ar esošo datu veidu sarakstu (IP adrese, *IMEI* u. c.). Šis regulējums ļautu pienācīgi novērtēt to, cik lielā mērā katra datu kategorija rada iejaukšanos, un līdz ar to – nepieciešamos aizsardzības pasākumus.

---

71 Ar dažiem izņēmumiem mazu pakalpojumu sniedzēju gadījumā lietotāju dati parasti jau tiek saglabāti uzņēmējdarbības vajadzībām. Šādā gadījumā un neskarot samērīgus aizsardzības pasākumus, šādi dati būtu jādara pieejami tiesībaizsardzībai.

72 Judikatūra ļauj vispārēji un nediferencēti saglabāt datus, kas saistīti ar elektronisko sakaru lietotāju civilo identitāti, lai aizsargātu sabiedrības intereses, kā arī ģenerisku un nediferencētu IP adrešu saglabāšanu, lai aizsargātu valsts drošību, apkarotu smagus noziegumus un novērstu nopietnus draudus sabiedrības drošībai (2020. gada 6. oktobra spriedums *La Quadrature du Net u. c.*, apvienotās lietas C-511/18, C-512/18 un C-520/18, un 2024. gada 30. aprīļa spriedums *La Quadrature du Net u. c.*, lieta C-470/21 (turpmāk tekstā "*Hadopi* lieta"), ECLI:EU:C:2024:370).

73 "datplūsmas dati" ("informācija par datu plūsmu") ir jebkuri dati, kas apstrādāti ar nolūku pārsūtīt komunikāciju elektronisko komunikāciju tīklā vai ar nolūku sagatavot rēķinu (Direktīvas 2002/58/EK 2. pants).

74 "atrašanās vietas dati" ir jebkuri dati, kas elektronisko komunikāciju tīklā apstrādāti, norādot publiski pieejamu elektronisko komunikāciju pakalpojuma lietotāja gala iekārtas ģeogrāfisko atrašanās vietu (Direktīvas 2002/58/EK 2. pants); lietotāja iekārtu atrašanās vietas dati būtu jāuzskata par atrašanās vietas datiem, kas nav datplūsmas dati (informācija par datu plūsmu), kā definēts Direktīvas 2002/58/EK 9. pantā.

75 Spriedums *Hadopi* lietā.

Kā norādījuši eksperti un nesenā judikatūra [76], saglabāšanas pienākumu apvienošana ar **stingrām prasībām attiecībā uz piekļuvi datiem** nodrošinātu pamattiesību, jo īpaši privātuma un datu aizsardzības, papildu aizsardzību. Tādējādi Augsta līmeņa grupas eksperti apsprieda vajadzību izstrādāt piekļuves noteikumus, kas atšķiras atkarībā, piemēram, no nozieguma veida un smaguma, nodarījuma radītā apdraudējuma cietušajiem pakāpes, piekļuves mērķa un iestādēm, kas ir kompetentas piekļūt datiem. Šāda pieeja arī tika uzskatīta par lietderīgu veidu, kā paredzēt konkrētus noteikumus tādu noziegumu izmeklēšanai un kriminālvajāšanai saistībā ar tiem, kurus ir īpaši sarežģīti izmeklēt, piemēram, internetā izdarītu noziegumu izmeklēšanai, kur vienīgie pieejamie pierādījumi ir digitāli pierādījumi.

Kad datiem ir likumīgi piekļūts, pieprasījuma iesniedzējām iestādēm jāspēj tos lasīt. Tāpēc pakalpojumu sniedzējiem dati ir jāsniedz **saprotamā formātā**. Bieži vien pakalpojumu sniedzēji piedāvā pilnīgi (*end-to-end*) šifrētus pakalpojumus [77] attiecībā uz datu plūsmas un abonentu datiem, un, kad tie šos datus kopīgo ar kompetentajām iestādēm, tie tos neatšifrē. Augsta līmeņa grupas eksperti uzskatīja, ka datu saglabāšanas režīmā būtu jāiekļauj pakalpojumu sniedzēju pienākumi sniegt nešifrētus datus, vienlaikus nodrošinot spēcīgu kiberdrošību un pilnīgu atbilstību datu aizsardzības un privātuma tiesību aktiem un neapdraudot šifrēšanu.

Minimālās prasības konkrētu kategoriju datu saglabāšanai būtu jāpiemēro (un jānodrošina, ka tās tiek izpildītas) jebkuram (pašreizējam vai nākotnes) ekonomikas dalībniekam, kas sniedz elektronisko sakaru pakalpojumus, lai datu saglabāšanas regulējums būtu iedarbīgs gan tagad, gan turpmāk. Lai ņemtu vērā tehnoloģiju turpmāko attīstību, starp subjektiem, uz kuriem attiecas datu saglabāšanas pienākumi, būtu jāietver telesakaru pakalpojumu sniedzēji, *OTT* pakalpojumu sniedzēji un citi operatori, kas vāc datus, kuri saistīti ar konkrētu fizisku vai juridisku personu, kas izmanto to pakalpojumu, piemēram, automobiļu ražotāji vai lielu valodas modeļu MI sistēmas. Ir jāspēj nodrošināt šo pienākumu izpildi, un jābūt iespējai prasīt atbildību no pakalpojumu sniedzējiem; to varētu panākt, izmantojot dažādus risinājumus, kas varētu ietvert tirgus šķēršļus (darbības licences) un administratīvas sankcijas.

---

[76] Nesenajā *Hadopi* lietā Tiesa secināja, ka privātumu var garantēt, apvienojot saglabāšanu un piekļuvi.

[77] Sk. I iedaļu.

Jebkura turpmāka ES regulējuma būtisks aspekts ir īstenojamu sankciju sistēma attiecībā uz pakalpojumu sniedzējiem, kas nesadarbojas, un pakalpojumu sniedzējiem, kuri mitina nelikumīgus pakalpojumus. Ņemot vērā mijiedarbību starp šo konkrēto aspektu un iespējamiem risinājumiem, kas apspriesti saistībā ar likumīgu pārtveršanu, sankcijas jāapspriež nākamajā sanāksmē par likumīgu pārtveršanu.

Lai gan lielākajai daļai pakalpojumu sniedzēju pienākums saglabāt un sniegt datus prasītu galvenokārt tehnisku īstenošanu (t. i., uzņēmējdarbības nolūkos savāktos vai apstrādātos datus darīt pieejamus kompetentajām iestādēm), tas nozīmētu noteikt lietotāju reģistrācijas procedūras pēc noklusējuma tiem pakalpojumu sniedzējiem, kuri pašlaik savus lietotājus nereģistrē, jo tiem nav komerciālas vajadzības to darīt (piemēram, *OTT* pakalpojumu sniedzējiem). Šāda veida pienākumus Augsta līmeņa grupas eksperti uzskatīja par pozitīviem saistībā ar diskusijām par nepieciešamību palielināt pakalpojumu sniedzēju **pārredzamību un pārskatatbildību** attiecībā uz datiem, ko tie vāc un uzglabā, un cik ilgi. Pašreizējie pienākumi kategorizēt saskaņā ar citiem instrumentiem (VDAR) var sniegt ieskatu saistībā ar šo pakalpojumu sniedzēju apstrādātajiem datiem.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina izveidot jaunu ES datu saglabāšanas un piekļuves sistēmu

Aktori: Eiropas Komisija, Padome, Eiropas Parlaments

Laiks: 2025–2026

- Augsta līmeņa grupas eksperti mudina **Eiropas Komisiju** sākt ietekmes novērtējuma procesu, lai izvērtētu dažādās iespējas, kā uzlabot kompetento iestāžu spēju efektīvi izmeklēt noziegumus un veikt kriminālvajāšanu saistībā ar tiem, piekļūstot vēsturiskajiem metadatiem, ko ģenerē un glabā sakaru pakalpojumu sniedzēji. Ietekmes novērtējumā būtu jāaptver arī subsidiaritātes prasības, ietekme uz pamattiesībām un iekšējo tirgu, kā arī saistība ar citiem spēkā esošiem tiesību aktiem. Tam vajadzētu būt par pamatu leģislatīvā akta priekšlikumam, kas jāpieņem, izmantojot parasto likumdošanas procedūru.

III nodaļa. Likumīga pārtveršana

PROBLĒMJAUTĀJUMI

Jēdziens "saziņas likumīga pārtveršana" apzīmē to, ka trešā persona, proti, varasiestāde vai cits subjekts, kas ir pilnvarots saskaņā ar tiesību aktiem, slēpti piekļūst datiem aizdomīgā saziņā. Lai gan pagātnē likumīga pārtveršana galvenokārt attiecās uz tālruņa zvaniem, pieaugošā pāreja no tradicionālajiem balss zvaniem uz ziņojumapmaiņas pakalpojumiem un citiem elektronisko sakaru veidiem ir radījusi jaunus izaicinājumus.

EECC šīs pārmaiņas tika atzītas un daļa no tiesiskā regulējuma, kas attiecas uz tradicionālajiem telesakariem, tika attiecināta arī uz uzņēmumiem, kuri piedāvā interneta pakalpojumus telesakaru infrastruktūrā, kas tiem nepieder vai ko tie nepārvalda, tostarp numurneatkarīgus starppersonu sakaru pakalpojumus *(NI-ICS*). Praksē tas nozīmē, ka uz *NI-ICS* pakalpojumu sniedzējiem var attiekties tas pats tiesiskais regulējums, kas ir ticis piemērots tradicionālajiem telesakaru operatoriem, ietverot likumīgu pārtveršanu. Dalībvalstis var prasīt, lai operatori ļautu valstu kompetentajām iestādēm likumīgi pārtvert elektronisko saziņu saskaņā ar Regulu (ES) 2016/679 un Direktīvu 2002/58/EK, kurās paredzēti noteikumi par saziņas konfidencialitāti un izņēmumi saistībā ar to. Saskaņā ar *EECC* paredzēto vispārējo atļauju režīmu dalībvalstis var atkārtoti noteikt šo prasību.

Likumīgai piekļuvei nav jābūt tīkla līmenī, kā tas ir tradicionālu tālruņa zvanu un teksta (*SMS*) ziņojumapmaiņas gadījumā, bet tā var būt arī lietotāja ierīcē (pirms informācijas nosūtīšanas) vai galamērķa līmenī (piemēram, kad ziņojumi tiek saglabāti mākonī). Šā ziņojuma kontekstā likumīga pārtveršana aptver šos trīs izmantošanas gadījumus un attiecas uz datiem, kuriem piekļūst reāllaikā vai ar nelielu nobīdi.

Ir svarīgi nošķirt pārtveršanas tehnoloģijas, ko **īsteno sakaru operators**, un tehnoloģijas, ko tiesībaizsardzības iestādes var izvērst autonomi. *ETSI* standartu definīcijā jēdzienam "likumīga pārtveršana" ir iekļauta tikai pirmā no minētajām [šajā ziņojumā saukta par **"operatora veiktu pārtveršanu"**], kas paredz, ka sakaru operatoram ir jāuzstāda tehniskās sistēmas, ar kurām vākt un nosūtīt pārtvertos datus pieprasījuma iesniedzējām iestādēm. Otra minētā tehnoloģija [šajā ziņojumā saukta par **"taktisko pārtveršanu"**] apzīmē rīkus, kuriem nav nepieciešama pastāvīga fiziska instalācija tīklā, piemēram, *IMSI* uztvērējus [78] vai programmatūru datu pārtveršanai viedtālruņos. Minētie izmantošanas gadījumi sevī ietver dažāda līmeņa iejaukšanos un atšķirīgus izaicinājumus, un uz tiem neattiecas viens un tas pats tiesiskais režīms.

Kaut gan likumīga tradicionālo telesakaru pārtveršana joprojām ir būtisks instruments daudzās izmeklēšanās [79], šā pasākuma efektivitāte ir ievērojami samazinājusies, jo telesakaru pakalpojumus tagad galvenokārt sniedz citi aktori: saskaņā ar dažādiem avotiem aptuveni 97 % no visiem mobilajiem ziņojumiem tagad tiek nosūtīti, izmantojot ziņojumapmaiņas lietotnes, piemēram, *WhatsApp*, *Facebook Messenger* un *WeChat*, savukārt tradicionālā *SMS* un *MMS* ziņojumapmaiņa veido tikai aptuveni 3 % no ziņojumiem. Turklāt 2023. gadā vairāk nekā 90 % *OTT* saziņas tika veikta, izmantojot pilnīgi (*end-to-end*) šifrētus pakalpojumus [80].

Eksperti ir vienisprātis par šādām tendencēm: vispirms noziedznieki sāka pāriet no tradicionālajiem sakaru operatoriem pie *OTT*; pēc tam nozīmīgākie noziedzīgie aktori pakāpeniski sāka izmantot īpaši noziedzīgiem nolūkiem domātus tīklus (piemēram, *Encrochat* un *Sky ECC*); savukārt kopš 2020. gada pēc lielo šifrēto noziedzīgiem nolūkiem paredzēto sakaru tīklu darbības izjaukšanas daudzi no tiem ir nolēmuši atgriezties pie parastajiem pilnīgi (*end-to-end*) šifrētajiem *OTT*.

---

78 *IMSI* uztvērēji ir novērošanas ierīces, kas imitē mobilo sakaru torņus, lai pārtvertu mobilo tālruņu signālus, tādējādi uztverot starptautisko mobilo sakaru abonentu identifikācijas (*IMSI*) numurus un sakaru datus.

79 Pēdējos gados Eiropā ir ievērojami un stabili pieaudzis likumīgas pārtveršanas pieprasījumu skaits. Tādās valstīs kā Vācija, Francija un Apvienotā Karaliste ir novērots īpaši daudz šādu pieprasījumu, un Vācija vien pieaugums ir bijis ievērojams. Piemēram, 2023. gadā *Deutsche Telekom* ziņoja par vairāk nekā 31 000 pārtveršanas pieprasījumu salīdzinājumā ar aptuveni 26 000 pieprasījumiem 2022. gadā (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Avoti: *Comparitech* un *Statista*.

Šajā kontekstā sakaru pakalpojumu sniedzēji, atbildot uz likumīgas pārtveršanas pieprasījumiem, saskaras ar tik lieliem sarežģījumiem, ka tie ar grūtībām var izpildīt Budapeštas Konvencijā par kibernoziegumiem noteiktās pamatprasības attiecībā uz likumīgu pārtveršanu [81]. Līdz ar to tradicionālās likumīgās pārtveršanas darbības vērtība bieži vien aprobežojas ar taktiskas informācijas iegūšanu, piemēram, konstatējot, vai ierīce ir ieslēgta vai izslēgta, tīkla antenas atrašanās vietu vai to, kurš ir savienots ar kuru; tomēr ar *OTT* pakalpojumu sniedzēju starpniecību pārraidīto satura datu likumīga pārtveršana pārsvarā nav iespējama.

Attiecīgi tiesībaizsardzības iestādes bieži vien nespēj piekļūt mērķorientētas saziņas saturam [82] un to lasīt vai pat saprast, kurš reāllaikā izmanto konkrēto interneta pakalpojumu, un filtrēt attiecīgo informāciju. Šāds ievērojams piekļuves zudums tranzītā esošiem datiem ietekmē izmeklēšanas vairākos veidos:

- rodas lielas grūtības novērst noziegumus, apzināt noziedzīgas organizācijas un konstatēt vainīgos noziedzīgās darbībās, kas veiktas tiešsaistē vai bezsaistē;

- tiesībaizsardzības iestādes arvien vairāk izmanto tā sauktās īpašās metodes [83], kas bieži vien ir invazīvāki un daudz bīstamāki amatpersonām, piemēram, ja tiesu iestāde nosaka, ka ir jāuzstāda kameras vai mikrofoni mērķa tuvumā;

- tiesībaizsardzības iestādes biežāk izmanto mazāk mērķorientētas izmeklēšanas metodes: bez piekļuves saziņas saturam vai precīziem ģeolokācijas datiem izmeklētājiem bieži ir jāizmeklē **visas** personas, kas saistītas ar personu, kuru tur aizdomās par noziedzīgām darbībām.

Šajā kontekstā Augsta līmeņa grupas eksperti norādīja uz četrām galvenajām izaicinājumu kategorijām.

---

81 https://rm.coe.int/1680081561 [20. un 21. pants].

82 Viens eksperts norādīja, izmantojot tradicionālu likumīgu pārtveršanu, 99 % gadījumu satura dati nav pieejami.

83 Tā sauktās īpašās metodes aptver virkni taktisku līdzekļu, informācijas par interesējošo mērķi iegūšanai, izmantojot kameras, mikrofonus, attālinātu piekļuvi ierīcēm, *GPS* izsekošanas ierīces u. c.

I. Ar netradicionālo sakaru pakalpojumu sniedzēju starpniecību veiktas saziņas likumīga pārtveršana

Lielākā daļa dalībvalstu ir ieviesušas kāda veida regulējumu, kas reglamentē likumīgu pārtveršanu, nosakot sakaru pakalpojumu sniedzēju pienākumus izvērst pārtveršanas spējas [84]. Lai gan likumīgu pārtveršanas rīkojumu izdošanas nosacījumi dažādās valstīs ievērojami atšķiras, operatoriem piemērojamie pienākumi bieži vien ir līdzīgi [85]: tiem jāspēj bez jebkādām nepilnībām pārtvert visus attiecīgos paziņojumus no konkrēta mērķa valsts teritorijā, un tiem jānodrošina infrastruktūra, kas vajadzīga, lai vāktu un pārsūtītu pārtvertos datus tiesībaizsardzības iestādēm.

Gadījumos, kad telesakaru tīklu operatori (sakaru nodrošinātāji, kuriem pieder tīkls un kuri var piekļūt tā infrastruktūrai) sniedz arī sakaru pakalpojumus (tālruņa zvanus, SMS utt.), tie visbiežāk spēj izpildīt likumīgas pārtveršanas pienākumus [86]. Vairumā gadījumu tie balstās uz ETSI standartiem un paļaujas uz specializētiem tehnoloģiju nodrošinātājiem, lai pārvaldītu savus ierobežojumus, tostarp izmaksu lietderību, minimālu ietekmi uz tīkla infrastruktūru, sadarbspēju, uzticamību un drošību.

Attiecībā uz *OTT* pakalpojumiem situācija ir sarežģītāka: likumīgu pārtveršanu var veikt vai nu telesakaru tīklu operatori, vai *OTT* pakalpojumu sniedzējs, kas sniedz pakalpojumu.

Ja saziņas pārtveršana, izmantojot *OTT* pakalpojumus, tiek īstenota telesakaru tīkla līmenī, tās efektivitāte bieži vien ir ierobežota. Pirmkārt, sakaru tīklu operators var nespēt identificēt mērķa saziņu (piemēram, ja pieslēgšanās notiek caur publisku Wi-Fi). Turklāt *OTT* pakalpojumi bieži izmanto patentētus protokolus, kas ir jāatkodē ar likumīgām pārtveršanas sistēmām, un tas palielina procesa izmaksas, laiku un sarežģītību. Visbeidzot, tas, ka *OTT* pakalpojumu sniedzēji izmanto pilnīgu šifrēšanu, padara piekļuvi satura datiem ļoti problemātisku un arvien vairāk kavē piekļuvi metadatiem, jo lielākā daļa valstu uzskata, ka telesakaru tīklu operatoru pienākums sniegt nešifrētu informāciju beidzas, kad šifrēšanu īsteno trešā persona, saskaņā ar Budapeštas konvenciju.

---

84 Sk. "*Lawful interception – A market access barrier in the European Union*", *Vadim Doronin in Computer Law & Security Review* 51 (2023) 105867.

85 Lai gan pastāv atšķirības attiecībā uz pienākumiem, kas saistīti ar satura vai nesatura datiem.

86 Lai gan tādi elementi kā maršrutēšana, izmantojot mājas operatora tīklu, slāņošana vai bagātinātie saziņas pakalpojumi var kavēt telesakaru tīkla operatoru spēju pildīt savus pienākumus (sk. iedaļu par tehnoloģiskām problēmām).

Eiropas Elektronisko sakaru kodeksā (*EECC*) dotā "elektronisko sakaru pakalpojumu" definīcija, kas kopš 2018. gada ietver numurneatkarīgus starppersonu sakaru pakalpojumus (*NI-ICS*), tiek izmantota, atsaucoties uz Direktīvas par privāto dzīvi un elektronisko komunikāciju 5. panta 1. punktu. Tas savukārt nozīmē, ka tagad plašāks elektronisko sakaru pakalpojumu (*ECS*) jēdziens (salīdzinājumā ar laiku, kad tika pieņemta Direktīva par privāto dzīvi un elektronisko komunikāciju) ļauj dalībvalstīm tieši paļauties uz *OTT* pakalpojumu sniedzējiem, lai veiktu likumīgu pārtveršanu [87]. Līdz šim dalībvalstis šo iespēju ir izmantojušas nevienmērīgi, un dažas no tām ir noteikušas līdzīgus pienākumus visu veidu *ECS* pakalpojumu sniedzējiem, tostarp *OTT* pakalpojumu sniedzējiem, savukārt citas izslēdz *OTT* pakalpojumu sniedzējus [88]. **Praksē neatkarīgi no spēkā esošajiem pienākumiem galvenie *OTT* pakalpojumi nav izstrādājuši tehniskus mehānismus, lai reaģētu uz likumīgiem pārtveršanas pieprasījumiem no ES dalībvalstu iestādēm,** galvenokārt juridisku iemeslu dēļ [89].

Turpretī Apvienotā Karaliste saskaņā ar Likumu par izmeklēšanas pilnvarām ir izveidojusi regulējumu *OTT* sakaru likumīgai pārtveršanai, kas, pateicoties Apvienotās Karalistes un ASV nolīgumam par piekļuvi datiem, attiecas arī uz *OTT* pakalpojumiem, kas atrodas ASV. Saskaņā ar attiecīgo Apvienotās Karalistes iestāžu sniegto informāciju tas būtiski ietekmē noziedzības novēršanu un izmeklēšanu.

Visbeidzot, valstu iestāžu eksperti skaidri norādīja, ka taktiskā pārtveršana, kuras pamatā ir ievainojamības izmantošana, nav ne efektīva, ne vēlama alternatīva izpildāmiem likumīgas pārtveršanas noteikumiem, kas piemērojami *OTT* pakalpojumu sniedzējiem, un tā būtu jāattiecina tikai uz konkrētiem gadījumiem ar stingrām garantijām, kas noteiktas valsts tiesību aktos, lai nodrošinātu samērīgumu.

---

87 Lai gan joprojām notiek diskusijas par precīzu piemērojamības jomu, un interpretācijas dalībvalstīs atšķiras.

88 Sk. "*Lawful interception – A market access barrier in the European Union*", *Vadim Doronin in Computer Law & Security Review* 51 (2023) 105867.

89 To neapstiprina statistika, jo valstu iestādes ļoti reti nosūta likumīgas pārtveršanas (*LI*) pieprasījumus *OTT*, labi apzinoties, ka šāda rīcība, visticamāk, nesniegs rezultātus.

II. Pārrobežu pieprasījumi

Pārrobežu likumīgas pārtveršanas pieprasījumi, kas adresēti *OTT* pakalpojumu sniedzējiem un – mazākā mērā – tradicionālajiem sakaru pakalpojumu sniedzējiem (*CSP*), rada vairākas problēmas tiesībaizsardzības iestādēm.

Attiecībā uz tradicionālajiem sakaru pakalpojumu sniedzējiem iestādes galvenokārt saskaras ar organizatoriskām problēmām. Pirmkārt, starptautiskās sadarbības instrumenti, jo īpaši savstarpējās tiesiskās palīdzības (STP) mehānismi, var būt nepraktiski attiecībā uz steidzamu pārtveršanu, kam atļauja un īstenošana nepieciešama stundu, nevis dienu vai nedēļu laikā [90]. Tas ir saistīts ar to pasākumu skaitu, kas jāveic, lai nodrošinātu tiesību aktu ievērošanu gan pieprasījuma iesniedzējā, gan saņēmējā dalībvalstī. Kopumā tiek uzskatīts, ka STP process ir neefektīvs un apgrūtinošs, ja to piemēro likumīgai pārtveršanai. Ar Eiropas izmeklēšanas rīkojumu (EIR), kas stājās spēkā 2017. gadā, tika aizstāti tradicionālie STP procesi ES [91], nosakot stingrus termiņus [92] pieprasīto pierādījumu vākšanai, ierobežojot šādu pieprasījumu noraidīšanas iemeslus un ieviešot vienotu standarta veidlapu, kas iestādēm jāizmanto, lai lūgtu palīdzību pierādījumu meklēšanā. Turklāt, ja no dalībvalsts, kurā atrodas pārtveršanas subjekts, nav vajadzīga tehniska palīdzība, lai veiktu pārtveršanu, minētā dalībvalsts tiek informēta par pārtveršanu, izmantojot standarta veidlapu, un tai tiek dota iespēja 96 stundu laikā iebilst pret pārtveršanu. Nozīmīgajā lietā C-670/22 EST pieņēma plašu "telesakaru pārtveršanas" jēdzienu, nospriežot, ka slēpta piekļuve galiekārtām, lai no interneta sakaru pakalpojuma iegūtu informāciju par datu plūsmu, atrašanās vietas un saziņas datus, ir "telesakaru pārtveršana". Tomēr eksperti uzskata, ka ar EIR panāktie būtiskie uzlabojumi nav pietiekami, lai apmierinātu vajadzību pēc ātras un saskaņotas pārrobežu piekļuves sūtīšanā esošiem datiem.

Turklāt dalībvalstu iestādes ziņoja, ka esošā tehniskā arhitektūra bieži vien neatbilst mērķim īstenot likumīgu pārtveršanu vienā dalībvalstī un nosūtīt datus gandrīz reāllaikā citai dalībvalstij. Dažos gadījumos, kad ir ieviesti attiecīgi organizatoriskie protokoli, nosūtāmo datu apjoms vienkārši nav savietojams ar joslas platumu, kas pieejams, izmantojot drošus sakaru kanālus.

---

90 Eksperti minēja gadījumus, kad lieta bija beigusies pirms pārrobežu likumīgas pārtveršanas efektīvas īstenošanas, vai gadījumus, kad STP neizskatīto lietu uzkrājums pārsniedza astoņus mēnešus.

91 Izņemot DK un IE, kur EIR nepiemēro.

92 30 dienas EIR atzīšanai un 90 papildu dienas tā izpildei.

OTT sakaru pārtveršana rada sarežģītus jurisdikcijas jautājumus salīdzinājumā ar telefonsakaru pārtveršanu, kad pakalpojumu sniedzēji piedāvā savus pakalpojumus skaidri noteiktā teritorijā. Tradicionālie telesakaru pakalpojumi ir saistīti ar konkrētu fizisko tīkla infrastruktūru, nodrošinot, ka pakalpojumu sniedzējam ir iekārtas un juridiska klātbūtne valstī, kurā notiek pārtveršana. Šāda lokalizēta struktūra samazina juridisko konfliktu risku ES iekšienē un vienkāršo atbilstību.

Savukārt *OTT* pakalpojumu gadījumā pieprasījuma iesniedzēja iestāde, pārtveršanas mērķis, fiziskā īstenošana un uzņēmuma reģistrācijas vieta var aptvert vairākas dažādas jurisdikcijas. Šo jurisdikciju tiesiskā regulējuma mijiedarbība varētu izraisīt tiesību normu kolīzijas [93].

Policijas un tiesu iestāžu ekspertiem nav šaubu, ka rīcības ar likumīgiem pārtveršanas pieprasījumiem balstīšana uz starptautiskiem instrumentiem nav dzīvotspējīgs risinājums. Ja tiesībaizsardzības iestādes apiet savstarpējās tiesiskās palīdzības procesu un tā vietā izmanto rīkojumus tieši pakalpojumu sniedzējiem saskaņā ar to valsts tiesību aktiem, *OTT* pakalpojumu sniedzēji, piemēram, *Microsoft*, *META* vai *Google*, var saskarties ar pretrunīgām juridiskām prasībām. Piemēram, daudzos gadījumos pieprasījuma iesniedzējai dalībvalstij būtu noteikumi, kas reglamentē likumīgu piekļuvi un kas ir pretrunā Īrijas tiesību aktiem [94], kuri reglamentē vairākus nozīmīgus *OTT* pakalpojumu sniedzējus, jo tie atrodas Īrijā, taču tos var reglamentēt arī to dalībvalstu tiesību akti, kurās tie sniedz savus pakalpojumus.

Šīs problēmas var efektīvi risināt, izmantojot kopīgus pasākumus un zināmā mērā saskaņojot likumīgas pārtveršanas noteikumus ES līmenī, lai atvieglotu un paātrinātu pārrobežu pieprasījumus par likumīgu pārtveršanu. Tas būtu priekšnoteikums, lai risinātu citas organizatoriskas un tehniskas problēmas, kurām var rast risinājumus, ja noteikumi ir skaidri izstrādāti un praktiski īstenojami.

---

93 Sk. "*LE interception concerns under the EECC*", *Microsoft*, 2020. gada janvāris.

94 Īrijas tiesību akti aizliedz *OTT* pakalpojumu sniedzējiem iesaistīties pārtveršanā reāllaikā.

III. Tehnoloģijas

Neatkarīgi no juridiskajiem apsvērumiem sakaru tehnoloģiju attīstība ietekmē tiesībaizsardzības iestāžu tehnisko spēju pārtvert sakarus, izmantojot pakalpojumus, ko tieši sniedz *CSP* vai *OTT* pakalpojumu sniedzēji.

Attiecībā uz tradicionālajiem sakaru sniedzējiem likumīgas pārtveršanas spējas parasti izstrādā tehnoloģiju nodrošinātāji, pamatojoties uz *ETSI* standartiem, un tās ir iekļautas 3*GPP* [95]. Tā rezultātā labi aprīkoti policijas dienesti var apmierinoši veikt tradicionālās saziņas – balss un īsziņu – pārtveršanu un, iespējams, pārtvert internetā balstītus sakarus, izmantojot to tīklos sniegtos pakalpojumus.

Tomēr 5G sakaru infrastruktūru un protokolu, piemēram, virtualizācijas, tīkla slāņošanas, perifērdatošanas un privātuma uzlabošanas funkciju, pieaugošā sarežģītība tradicionālajiem operatoriem rada jaunas tehnoloģiskas problēmas [96]. Augsta līmeņa grupas eksperti jo īpaši uzstāja uz problēmām, kas saistītas ar maršrutēšanu, izmantojot mājas operatora tīklu [97], un bagātinātiem saziņas pakalpojumiem (*RCS*) [98].

Raugoties uz nākotni un pamatojoties uz 5G pieredzi, Augsta līmeņa grupas eksperti paredz problēmas saistībā ar 6G (paredzēta laikposmam pēc 2030. gada) turpmāku ieviešanu, kas būs solis tālāk attiecībā uz privātuma uzlabošanas funkcijām [99], iespējams, ietverot pilnīgu (*end-to-end*) šifrēšanu kā standartu, kas kopumā varētu apgrūtināt pārtveršanu. Tajā pašā laikā jaunas sakaru tehnoloģijas, piemēram, lietu internets (*IoT*), satelītsakari, un kvantiskās datošanas [100] attīstība rada vēl vienu problēmu kopumu, kas ir jāparedz.

---

95 Trešās paaudzes partnerības projekts, kas nodrošina pamatu tādu sakaru tehnoloģiju attīstībai kā 5G, lietu internets (*IoT*) un mobilā platjosla.

96 Sk. "Tiesībaizsardzības un tiesiskie aspekti saistībā ar 5G", ES terorisma apkarošanas koordinators, 2019. gads, https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Eiropols – Position paper on Home routing.pdf (europa.eu).

98 *RCS* protokols ļauj apmainīties ar grupas tērzētavām, video, audio un augstas izšķirtspējas attēliem; to bieži izmanto SMS vietā. Atkarībā no tā īstenošanas *RCS* ziņojumu likumīga pārtveršana var būt neiespējama, un tas būtiski ietekmē tiesībaizsardzību (vairāk nekā 1 miljards *RCS* aktīvo lietotāju 2023. gadā).

99 Sk. 6G ceļvedi: https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf.

100 The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Eiropols (europa.eu).

Visbeidzot, Augsta līmeņa grupas eksperti uzsvēra, ka viena no galvenajām tehniskajām problēmām, kas rodas tiesībaizsardzības iestādēm, ir pilnīga šifrēšana, jo īpaši *OTT* sakariem, jo vairāk nekā 80 % sakaru tiek pārvaldīti, izmantojot pilnīgi šifrētus pakalpojumus (tiešie sakari un rezerves kopiju uzglabāšana), tādējādi liedzot izmeklētājiem piekļuvi saziņas saturam. Tajā pašā laikā eksperti arī piekrīt, ka pilnīga šifrēšana tiek uzskatīta par stingru drošības pasākumu, kas efektīvi aizsargā iedzīvotājus no dažādiem noziedzības veidiem. Nodrošinot, ka tikai saziņā esošie lietotāji var piekļūt savu ziņojumu saturam, pilnīga šifrēšana efektīvi aizsargā pret nelikumīgu noklausīšanos, datu zādzību, valsts sponsorētu spiegošanu un citiem neatļautas piekļuves veidiem, ko veic hakeri, kibernoziedznieki vai pat paši pakalpojumu sniedzēji.

Ir grūti kvantitatīvi noteikt problēmas, ar kurām tiesībaizsardzības iestādes saskaras, uzraugot noziedznieku un teroristu saziņu, kas notiek, izmantojot pilnīgu šifrēšanu. Tāpēc tiesībaizsardzības iestādes bieži izvēlas netērēt laiku un resursus, lai iegūtu tiesas rīkojumus elektroniskai novērošanai platformās, par kurām zināms, ka tās pēc noklusējuma izmanto pilnīgu šifrēšanu [101]; tādējādi efektīvu likumīgas pārtveršanas pieprasījumu skaits attiecībā uz satura datiem, kurus nav iespējams izpildīt pilnīgas šifrēšanas dēļ, ir ļoti mazs un bez nozīmes. Tiesībaizsardzības iestādes šo novērošanas spēju trūkumu uzskata par ievērojamu aklo zonu un neaizsargātību, ko noziedznieki un teroristi pilnībā apzinās un aktīvi izmanto, kā to apliecina *EncroChat* [102] un *Sky ECC* lietas, kuru rezultātā visā Eiropā tika arestēti tūkstošiem personu, tostarp daudzi augsta līmeņa noziedznieki. Šīs bažas cita starpā ir paustas vairākos Eiropas policijas priekšnieku [103] un G7 [104] paziņojumos. Lai ilustrētu ietekmi, ko rada piekļuves zaudējums satura datiem, eksperti atsaucās uz vairākiem publiski pieejamiem piemēriem, kas cita starpā saistīti ar terorisma [105], narkotiku tirdzniecības [106] un izvarošanas lietām [107], kurās šifrēšana būtiski kavēja tiesībaizsardzības spēju novērst un apkarot smagu un organizētu noziedzību. Tiesībaizsardzības pārstāvji dotu priekšroku pieejai, kas paredz, ka uzņēmumiem ir jānodrošina tiesībaizsardzībai piekļuve nešifrētiem datiem, ievērojot stingrus nosacījumus. Tomēr jāatzīmē, ka kiberdrošības eksperti pauda bažas par to, ka šādi risinājumi apdraudētu kiberdrošību. Daži tiesībaizsardzības eksperti norādīja, ka dažos gadījumos šifrēšana ir īstenota tādā veidā, kas ir saderīgs gan ar kiberdrošību, gan ar nepieciešamību saglabāt dažus pakalpojumus, piemēram, operētājsistēmas atjauninājumus, satura skenēšanu (piemēram, e-pastus vai tīmekļa sesijas) kiberdrošības nolūkos vai galvenos atgūšanas mehānismus, kad lietotājs izvēlas šo iespēju.

---

101 *Manpearl*, 2017. gads.

102 Plašāku informāciju par *EncroChat* un *Sky ECC* sk. Eiropols un *Eurojust*, "*Third Report of the Observatory Function on Encryption*", 2021. gada jūnijs.

103 https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF.

104 https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version .

105 2017. gada martā 52 gadus vecais *Khalid Masood* veica islāmistu iedvesmotu teroristu uzbrukumu Londonas centrālajā daļā, nogalinot sešus cilvēkus un 29 ievainojot. Lai gan incidenta ziņojumi vedināja domāt, ka *Masood* bija plānojis un rīkojies viens pats, tika konstatēts, ka minūtes pirms uzbrukuma veikšanas viņš bija nosūtījis *PDF* dokumentu ar nosaukumu "*Jihad*" lielam skaitam savu kontaktpersonu *WhatsApp* un *iMessage*, kuras abas pēc noklusējuma bija pilnībā šifrētas un joprojām tiek pilnībā šifrētas. Avoti: *Max Hill, "The Westminster Bridge Terrorist Attack"* (Londona: *Stationery Office*, 2018.); *BBC News, "WhatsApp Must Be a Vlace for Terrorists to Hide" (WhatsApp Must Be a Vlace for Terrorists to Hide)*, 2017. gada 26. marts.

106 Eksperti minēja lielus narkotiku tirdzniecības gadījumus, kuros progress nebija iespējams, kamēr nebija iegūta piekļuve šifrētai saziņai *Encrochat* un *Sky ECC*.

107 Augsta līmeņa lietā Apvienotajā Karalistē policijas izmeklēšana izvarošanas lietā tika kavēta, jo aizdomās turētie izmantoja *WhatsApp* saziņai, un pilnīga šifrēšana apgrūtināja piekļuvi būtiskiem pierādījumiem. Tiesībaizsardzības iestāžu nespēja atšifrēt *WhatsApp* ziņojumus bez lietotāja piekrišanas kavēja izmeklēšanu.

Pamatojoties uz to, tiesībaizsardzības eksperti piekrita, ka šifrēšanas radītās problēmas prasa daudzšķautņainu pieeju, kas līdzsvaro tiesības uz privātumu, drošību un nepieciešamību tiesībaizsardzības iestādēm piekļūt datiem, lai cīnītos pret noziedzību un aizsargātu cilvēku dzīvību, fizisko neaizskaramību un īpašumus. Lai gan ir maz ticams, ka viens risinājums kliedēs visas attiecīgās bažas, vairāku pieeju kombinācija varētu palīdzēt mazināt šo problēmu.

IV. Noziedzīga rakstura sakaru pakalpojumu sniedzēji

Noziedznieki izmanto vispārējas pilnīgas šifrētas platformas, lai slēptu savu saziņu; tomēr tie var arī nolemt izmantot drošus sakaru kanālus, kas īpaši paredzēti noziedzīgām darbībām (saukti par "*CCC*" – "noziedzīgiem sakaru kanāliem") [108]. Gan *EncroChat*, gan *Sky ECC* ir labi pazīstami *CCC*, kas pārdod telefonus ar integrētu pilnīgi šifrētu ziņojumapmaiņas pakalpojumu, kurš pielāgots, lai slēptu noziedzīgas darbības, un tiek popularizēts tumšajā tīmeklī. Abas platformas 2020. un 2021. gadā tika likvidētas, pateicoties starptautiskām kopīgām tiesībaizsardzības operācijām, kas atklāja to plašo iesaisti organizētajā noziedzībā. Ir likvidētas arī vairākas līdzīgas platformas, piemēram, *Phantom Secure* [109] un *Exclu* [110], savukārt daudzas mazākas platformas joprojām darbojas, nodrošinot drošus centrus noziedzīgas informācijas apmaiņai. Šajā sadrumstalotajā vidē ir svarīgi, lai tiesībaizsardzības iestādes spētu identificēt *CCC*, uzraudzīt un bloķēt to darbību, tos likvidēt un noziedzniekus saukt pie atbildības.

---

108 https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf

109 https://www.fbi.gov/news/stories/phantom-secure-takedown-031618

110 New strike against encrypted criminal communications with dismantling of Exclu tool | *Eurojust* | Eiropas Savienības Aģentūra tiesu iestāžu sadarbībai krimināllietās (europa.eu)

Tā kā uz operatoru balstīta pārtveršana nav iespēja attiecībā uz šāda veida negodīgu sakaru pakalpojumu sniedzēju, tiesībaizsardzībai ir vajadzīgas attiecīgas taktiskās pārtveršanas spējas – rīki un speciālās zināšanas –, lai mērķtiecīgi uzraudzītu savus lietotājus, neraugoties uz šifrēšanu. Tiesībaizsardzības eksperti īpaši norādīja uz būtiskajām problēmām, riskiem un ierobežojumiem, kas saistīti ar šādu metožu izstrādi un izmantošanu, kuras nav mērogojamas un kuras būtu jāsaglabā vissvarīgākajiem gadījumiem. Atkarībā no to spējām un tiesiskā regulējuma valstu iestādes izmanto dažādas pieejas, tostarp rīkus, kas ir izstrādāti iekšēji, iegādāti no trešām personām vai tiek ekspluatēti kā pakalpojums; neatkarīgi no tā, kādu iespēju viņi izmanto, eksperti piekrīt, ka ir jāievieš garantijas un aizsardzības pasākumi šādu rīku izmantošanai. Tas var ietvert pārdomas par rīku uzlabotu pārraudzību, novērtēšanu un sertifikāciju, kā arī par stabilu neaizsargātības pārvaldības satvaru, vienlaikus pilnībā ievērojot dalībvalstu procesuālo autonomiju kriminālllietās un to ekskluzīvo kompetenci attiecībā uz valsts drošību.

Izmeklēšanas iestādes saskaras arī ar juridiskām problēmām, piemēram, grūtībām noteikt krimināLatbildību sakaru pakalpojumu sniedzējiem un mitināšanas pakalpojumiem, kas galvenokārt piedāvā noziedzīgus pakalpojumus (jo visa datplūsma ir šifrēta), bet tas ir nepieciešams pirmais solis pirms tiesvedības vai administratīvas darbības uzsākšanas. Turklāt dalībvalstīm ir jāspēj piemērot sankcijas *CCC*, lai ierobežotu vai bloķētu piekļuvi šādiem pakalpojumiem Eiropas Savienībā un tādējādi sagrautu to noziedzīgās uzņēmējdarbības modeli. Tas būs nepieciešams, kad un ja uz *OTT* pakalpojumiem attieksies likumīgas pārtveršanas pienākumi, lai novērstu noziedznieku atgriešanos pie negodīgiem sakaru pakalpojumu sniedzējiem.

Visbeidzot, tiesās tiek apstrīdēti dažādi aspekti tādās lietās kā pret *EncroChat* un *Sky ECC*. Prasības izmantot citā dalībvalstī pārtvertus datus kā pierādījumus ievērojami atšķiras visā ES, un tas rada juridisku nenoteiktību attiecībā uz līdzīgām darbībām, ko veic viena dalībvalsts, un tas var ietekmēt daudzas.

IESPĒJAMIE RISINĀJUMI

I. Padarīt likumīgus pārtveršanas pieprasījumus izpildāmus visu veidu elektronisko sakaru pakalpojumu sniedzējiem

Eiropas Savienībā likumīgas pārtveršanas spējas attiecas tikai uz tradicionālajiem sakaru pakalpojumu sniedzējiem, savukārt lielākā daļa sakaru pašlaik notiek ar netradicionālu sakaru pakalpojumu sniedzēju starpniecību [111]. Neatkarīgi no tā, vai sakaru pakalpojumu sniedz infrastruktūras īpašnieks vai nē, tiesībaizsardzības iestāžu spējai veikt likumīgu pārtveršanu interešu jomā vajadzētu būt tādai pašai. Alternatīvi risinājumi, piemēram, likumīga pārtveršana *NI-ICS* un citos sakaru pakalpojumos tikai telesakaru tīkla līmenī, paļaušanās uz starptautiskās sadarbības instrumentiem, lai veiktu likumīgu pārtveršanu *NI-ICS* pakalpojumu sniedzējiem, vai plaši izmantojot taktisko pārtveršanu, nav praktiski īstenojami [112].

Tā rezultātā Augsta līmeņa grupas eksperti uzskata, ka prioritāte ir nodrošināt, ka pienākumi par pieejamo datu likumīgu pārtveršanu vienādi attiecas uz tradicionālajiem un netradicionāliem sakaru pakalpojumu sniedzējiem un ir vienlīdz izpildāmi. Šādu pienākumu saskaņošanai būtu jāpalīdz pārvarēt problēmas, kas saistītas ar pārrobežu pieprasījumu izpildi.

Lai sasniegtu šo mērķi un pakāpeniski tuvinātu un saskaņotu likumīgas pārtveršanas noteikumus ES, Augsta līmeņa grupas eksperti ierosina pakāpenisku pieeju: pirmkārt, ES līmenī būtu jāvienojas par strukturēšanas principiem (1. posms); pēc tam Komisijai būtu jāatbalsta šo principu īstenošana (2. posms); visbeidzot, pamatojoties uz turpmāku novērtējumu, principus var kodificēt juridiskā instrumentā (3. posms).

---

111 Apvienotajā Karalistē 2022. gadā nosūtīto SMS un MMS skaits bija 36 miljardi, savukārt tiešsaistes ziņojumu skaits bija 1,3 triljoni (WhatsAppening in the world of online communications? - Ofcom).

112 Skatīt nodaļu par problēmām.

1. posms: Vienošanās par kopēju pamatscenāriju

Pirmkārt, ir jāattīsta vienota izpratne par to, uz kurām *ECS* kategorijām var attiekties iekšzemes pienākumi attiecībā uz likumīgu pārtveršanu saskaņā ar e-privātuma un VDAR noteikumiem.

Otrkārt, ir jāpanāk vienošanās par augsta līmeņa operatīvajām prasībām, kurās skaidri norādīts, ko valstu iestādes sagaida attiecībā uz likumīgu pārtveršanu un kādiem būtu jābūt saistītajiem aizsardzības pasākumiem. *LEON* [113] ir atzīta par labu pamatu tiesībaizsardzības prasību noteikšanai. Šis dokuments būtu jāpapildina ar prasībām par, piemēram, samērīgumu, pārraudzību un pārredzamību, iespējams, nošķirot noteikumus, kas piemērojami satura datiem un nesatura datiem, pilnībā ievērojot kiberdrošību un datu aizsardzību un privātumu un neapdraudot šifrēšanu. Iespējama *ad hoc* ekspertu grupas izveide, tajā ietverot kiberjautājumu, privātuma un tiesībaizsardzības ekspertus, , varētu nodrošināt, ka vajadzības gadījumā prasības tiek atjauninātas, iespējams, balstoties uz Eiropola iekšējās drošības standartizācijas darba grupas darbu, kas būtu jāturpina.

Treškārt, teritoriālās jurisdikcijas jēdziens ir jāprecizē attiecībā uz tā piemērojamību *OTT* pakalpojumiem, ņemot vērā atšķirīgās interpretācijas starp valstu iestādēm un, pats svarīgākais, starp valsts iestādēm un *OTT* pakalpojumu sniedzējiem. Piemēram, būtu jāprecizē noteikumi, kas piemērojami gadījumos, kad mērķa atrašanās vieta ir neskaidra. Ir vajadzīgi arī norādījumi par to, kas var novērtēt pieprasījuma likumību, piemēram, attiecībā uz pakalpojumu sniedzēju lomu šajā kontekstā. Visbeidzot, lai gan lielākā daļa tiesas nolēmumu līdz šim ir apstiprinājuši pret *EncroChat* un *Sky ECC* vērsto procedūras aktu likumību, joprojām tiek izskatītas vairākas tiesas lietas [114], kas var būtiski ietekmēt augsta līmeņa noziedznieku notiesāšanu. Tādējādi var būt nepieciešams atvieglot tādu pierādījumu pieņemamību, kas iegūti, veicot taktiskos pārtveršanas pasākumus starp dalībvalstīm, tiesas spriedumu un nolēmumu savstarpēju atzīšanu, kā arī policijas un tiesu iestāžu sadarbību krimināllietās.

---

[113] *LEON* (Tiesībaizsardzība – operatīvās vajadzības attiecībā uz likumīgu piekļuvi sakariem) ir rezultāts darbam, ko veikušas Zviedrijas tiesībaizsardzības iestādes, cieši sadarbojoties ar ES dalībvalstu, Ziemeļamerikas un Austrālijas tiesībaizsardzības iestāžu pārstāvjiem. Mērķis ir noteikt un aprakstīt tiesībaizsardzības vajadzības attiecībā uz likumīgu piekļuvi sakaru saturam, ar saturu saistītiem datiem un abonentu informācijai. Skatīt *Padomes prezidentvalsts paziņojums par tiesībaizsardzības iestāžu operatīvajām vajadzībām attiecībā uz likumīgu piekļuvi sakariem (LEON)*, dok. 6050/23, 2023. gada 16. februāris.

[114] Skatīt Lietas T-1180/23, T-148/24, T-167/24, T-484/24 un T-560/24.

7. ieteikumu kopa

Lai ES līmenī vienotos par kopīgiem principiem attiecībā uz pieejamo datu likumīgu pārtveršanu, kas piemērojami visu veidu ECS *pakalpojumu sniedzējiem, eksperti iesaka:*

1. *precizēt likumīgas pārtveršanas definīciju un darbības jomu saskaņā ar spēkā esošajiem ES tiesību aktiem un citiem attiecīgiem Eiropas un starptautiskiem instrumentiem, piemēram, Budapeštas Konvenciju par kibernoziegumiem [38. ieteikums];*

2. *iedvesmoties no* LEON *dokumenta, lai noteiktu kopīgas operatīvās prasības [21. ieteikums];*

3. *apzināt nepieciešamos aizsardzības pasākumus (17. ieteikums, 41. ieteikums);*

4. *pievērsties kiberdrošības perspektīvai, ka nevienam pasākumam nevajadzētu ietvert pienākumu pakalpojumu sniedzējiem pielāgot savas IKT sistēmas tā, ka tas negatīvi ietekmētu lietotāju kiberdrošību [41. ieteikums];*

5. *precizēt jēdzienu "teritoriālā jurisdikcija attiecībā uz datiem", lai risinātu iespējamus tiesību kolīziju jautājumus [39. ieteikums], un veicināt minimālo noteikumu pieņemšanu ES līmenī, kas attiecīgā gadījumā pieļauj tādu pierādījumu pieņemamību, kuri iegūti no taktiskās pārtveršanas pasākumiem starp dalībvalstīm, ciktāl tas nepieciešams, lai veicinātu tiesas spriedumu un nolēmumu savstarpēju atzīšanu un policijas un tiesu iestāžu sadarbību krimināllietās [42. ieteikums].*

Ir jāapsver labākā pieeja, lai izveidotu kopīgus principus un vienotos par tiem, kā minēts 7. ieteikumu kopā, un lai noteiktu vispiemērotāko instrumentu šo principu kopīgai izmantošanai. Atskatoties atpakaļ, Padomes 1995. gada 17. janvāra rezolūcija par likumīgu pārtveršanu [115] bija būtiska, lai veicinātu likumīgas pārtveršanas risinājumu saskaņošanu, jo tā sniedza atsauci *ETSI* izstrādātajiem standartiem attiecībā uz likumīgu pārtveršanu. Līdzīga pieeja, iespējams, izmantojot Komisijas vai Padomes ieteikumu, varētu būt vienlīdz izdevīga.

[115] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104

Galvenā darbība: Augsta līmeņa grupas eksperti aicina ES 2025. gadā izdot ieteikumu par piekļuvi datiem reāllaikā

Laiks: 2025. gads *Budžets: Tiks noteikts vēlāk*

- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju izdot ieteikumu, kurā *ECS* sniedzējiem būtu precizēts likumīgas pārtveršanas jēdziens [116] un sīki izklāstītas dažādās prasības, kas var attiekties uz pieejamo nesatura datu un satura datu likumīgu pārtveršanu, pilnībā ievērojot kiberdrošību, datu aizsardzību un privātumu, neapdraudot šifrēšanu un balstoties uz kopējām operatīvajām prasībām, kas noteiktas *LEON* dokumentā.

2. posms: ES atbalsta sniegšana, lai nodrošinātu vienlīdzīgus konkurences apstākļus un uzlabotu pārrobežu sadarbību

1. posmā izklāstītie kopīgie principi būtu pamats tehniskajai, juridiskajai un organizatoriskajai saskaņošanai ES līmenī. Lai tos pārvērstu konkrētos rezultātos, ir vajadzīga koordinācija un finansiāls atbalsts no Komisijas. Tas ietvertu īpaša procesa izveidi, pamatojoties uz esošajām darba grupām, un vajadzības gadījumā jaunu darba grupu izveidi, nodrošinot koordināciju ar attiecīgajām ieinteresētajām personām, tostarp *OTT* pakalpojumu sniedzējiem un nozares pārstāvjiem, ziņojot attiecīgajām struktūrām, jo īpaši Padomei un Eiropas Parlamentam, un nodrošinot pārredzamību sabiedrībai. Tas varētu ietvert arī mērķtiecīgu pētījumu finansēšanu tieši vai ar attiecīgu partnerību starpniecību, piemēram, ar attiecīgajām aģentūrām vai akadēmiskajiem partneriem.

[116] Attiecas tikai uz operatora veiktu pārtveršanu, kā definēts iepriekš.

Turklāt Augsta līmeņa grupas eksperti uzsvēra, ka ir steidzami jāuzlabo likumīgu pārrobežu pārtveršanas pieprasījumu efektivitāte saskaņā ar pašreizējo regulējumu, vienlaikus veicot iepriekš izklāstīto darbu. Šis mērķis ietvertu:

- izvērtēt EIR [117] pašreizējos ierobežojumus un strādāt pie darbības efektivitātes uzlabošanas;
- novērst tehniskos un organizatoriskos ierobežojumus, kas saistīti ar likumīgas pārtveršanas ceļā iegūtu pierādījumu pārrobežu apmaiņu, kam savukārt būtu vajadzīgs turpmāks darbs pie:
    - problēmas apzināšanas (kādi ir ierobežojumi, kuras dalībvalstis ar tiem saskaras utt.),
    - datu struktūru, uzticamības mehānismu un datu filtrēšanas standartizācijas, lai izvairītos no neattiecīgu datu nosūtīšanas un ievērotu datu aizsardzības principus attiecībā uz mērķa ierobežošanu, samērīgumu un datu minimizēšanu,
    - pārrobežu pārvades līdzekļu konstrukcijas un jaudas,
    - saistīto finansēšanas shēmu apzināšanas;
- veicināt pārrobežu likumīgas pārtveršanas pieprasījumus, izraugoties un apmācot vienotos kontaktpunktus, koordinācijā ar plašāku darbu saistībā ar vienotajiem kontaktpunktiem un piekļuvi digitālajiem pierādījumiem, piešķirot nozīmīgu lomu *SIRIUS* projektam;
- attiecīgā gadījumā veicināt divpusējus nolīgumus starp dalībvalstīm un ASV kā priekšnoteikumu, lai atvieglotu valstu iestāžu tiešus pieprasījumus integrēt *OTT* pakalpojumu sniedzējus, jo ES un ASV nolīguma par pārrobežu piekļuvi elektroniskiem pierādījumiem darbības joma saskaņā ar sarunu norādēm neattiecas uz likumīgu pārtveršanu, kas nozīmē, ka ir vajadzīgi īpaši nolīgumi, lai risinātu tiesību normu kolīziju jautājumus.

---

117 Eiropas Parlamenta un Padomes Direktīva 2014/41/ES (2014. gada 3. aprīlis) par Eiropas izmeklēšanas rīkojumu (EIR) krimināllietās attiecas uz "telesakariem"; lai gan lielākā daļa dalībvalstu to ir interpretējušas plašāk saskaņā ar *EECC* atjauninājumu, varētu apsvērt un turpināt izvērtēt iespējamo vajadzību grozīt EIR šajā sakarā.

Visbeidzot, eksperti aicināja apsvērt pasākumus, kas varētu uzlabot valstu iestāžu veiktos atturošos pasākumus pret *ECS* sniedzējiem, kas nesadarbojas. Eksperti jo īpaši aicināja izvērtēt iespējamo tehnisko risinājumu iespējamību un samērīgumu.

8. ieteikumu kopa

Lai nodrošinātu, ka plašs ECS *pakalpojumu sniedzēju loks, tostarp* OTT *pakalpojumu sniedzēji, atbild uz likumīgiem pārtveršanas pieprasījumiem, kā noteikts valsts tiesību aktos, eksperti iesaka:*

1. *atbalstīt 1.1. ieteikumā noteikto principu īstenošanu, izmantojot koordināciju un finansējumu;*

2. *izpētīt, kā EIR varētu labāk atbalstīt efektīvus pārrobežu likumīgas pārtveršanas pieprasījumus, piemēram, uzlabojot juridisko noteiktību, saīsinot termiņus atbildēšanai uz rīkojumiem un veicinot EIR vienādu izmantošanu [40. ieteikums];*

3. *veidot mehānismus (sadarbspēja un kiberdrošība) un infrastruktūras (joslas platums un mērogojamība), kas ir saderīgi ar lielu datu kopu pārrobežu nosūtīšanu reāllaikā [9. ieteikums];*

4. *veicināt vienoto kontaktpunktu izraudzīšanos Eiropas Savienībā, kas nodarbotos ar publisko iestāžu pieprasījumiem un sazinātos ar tām, lai atvieglotu pienākumu izpildi attiecībā uz likumīgu pārtveršanu un izveidotu mehānismus efektīvai pārrobežu pieprasījumu nosūtīšanai [19. un 36. ieteikums];*

5. *veicināt divpusēju nolīgumu izstrādi ar trešām valstīm, jo īpaši ar Amerikas Savienotajām Valstīm, par reāllaika piekļuvi datiem [38.4. ieteikums].*

Vairākas darbības varētu palīdzēt efektīvi īstenot ES ieteikumu par likumīgu pārtveršanu.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina Komisiju ES ieteikuma par likumīgu pārtveršanu īstenošanu papildināt ar pienācīgu koordināciju un finansējumu

- Augsta līmeņa grupas eksperti aicina Komisiju ierosināt skaidru plānu, lai atbalstītu ES ieteikuma par likumīgu pārtveršanu īstenošanu, tostarp no finanšu plānošanas perspektīvas.

3. posms: Juridiska instrumenta par likumīgu pārtveršanu iespējas izvērtēšana

Koordinācija vien var izrādīties nepietiekama, lai sasniegtu vajadzīgo saskaņošanas līmeni, pat ja to papildina pasākumi esošo juridisko instrumentu efektivitātes uzlabošanai. Var būt nepieciešams jauns noteikumu kopums, lai nodrošinātu pieprasījumu izpildāmību un juridisko noteiktību, novērstu tiesību normu kolīzijas un samazinātu administratīvo slogu, kas saistīts ar atbilstības un likumības pārbaudēm. Turklāt atšķirības starp likumīgas pārtveršanas noteikumiem ES rada apgrūtinošas prasības regulētajiem subjektiem, piemēram, *OTT* pakalpojumu sniedzējiem, un, iespējams, rada šķēršļus sakaru pakalpojumu sniedzēju piekļuvei tirgum [118]. Šajā ziņā saskaņoti ES noteikumi par pieejamo datu likumīgu pārtveršanu palīdzētu veidot turpmāko Eiropas digitālo infrastruktūru, dodot priekšroku modelim, kurā telesakaru infrastruktūra potenciāli nodrošina pārklājumu visā kontinentā [119].

Pāreja uz interneta sakariem ir spēcīgs stimuls, lai izstrādātu saskaņotus piekļuves noteikumus ES līmenī; tomēr juridiskā instrumenta pieņemamība, īstenojamība un ar nozari, kiberdrošību un drošību saistītā ietekme būtu rūpīgi jāizvērtē, ņemot vērā pašreizējās atšķirības starp dalībvalstu tiesiskajiem režīmiem likumīgas pārtveršanas jomā. Augsta līmeņa grupas eksperti norādīja, ka potenciālam instrumentam būtu: i) jāatbilst 1.1. ieteikumā izklāstītajiem principiem; ii) pilnībā jāņem vērā pamattiesību perspektīva un valstu suverenitāte krimināllietās un valsts drošības jomā; un iii) jāiedvesmojas no darba, kas paveikts saistībā ar e-pierādījumu paketi.

Augsta līmeņa grupas eksperti vienojās, ka jebkurai iniciatīvai veicināt vai noteikt likumīgas pārtveršanas noteikumus attiecībā uz visu veidu *ECS* vajadzētu būt skaidrai un izpildāmai sistēmai, lai vērstos pret sakaru pakalpojumu sniedzējiem, kas darbojas nelikumīgi un/vai atsakās no jebkāda veida sadarbības ar tiesībaizsardzību. Ja šāda regulējuma nebūtu, noteikumi tiktu apdraudēti, un noziedznieki masveidā novirzītu savu saziņu uz neatbilstīgiem pakalpojumu sniedzējiem. Jebkurā turpmākā ES iniciatīvā šajā sakarā būtu jāņem vērā atšķirība starp *OTT* pakalpojumu sniedzējiem, kas nepilda savas juridiskās saistības, un *ECS*, kas apzināti piedāvā pakalpojumus, kuri pielāgoti noziedzīgām darbībām. Turklāt visās iniciatīvās būtu jāņem vērā arī ES *acquis*, jo īpaši Digitālo pakalpojumu tiesību akts.

---

[118] Sk. "*Lawful interception – A market access barrier in the European Union*", *Vadim Doronin in Computer Law & Security Review* 51 (2023) 105867

[119] Baltā grāmata "Kā apgūt ES digitālās infrastruktūras vajadzības?"Eiropas digitālās nākotnes veidošana (europa.eu)

Šāda iniciatīva varētu ietvert administratīvus vai tiesas pasākumus. Augsta līmeņa grupas eksperti aicināja padziļināti apsvērt šo jautājumu, lai risinātu gan pamattiesību, gan kiberdrošības problēmas, kā arī ar to saistītās sarežģītās tehnoloģiskās problēmas.

9. ieteikumu kopa

Pamatojoties uz turpmāku analīzi un ietekmes novērtējumu, eksperti iesaka ***izstrādāt ES instrumentu par likumīgu pārtveršanu (kas ietvertu ieteikuma tiesības vai saistošus juridiskus instrumentus) tiesībaizsardzības nolūkos****, kas noteiktu izpildāmus pienākumus* ECS *nodrošinātājiem ES. Viņi iesaka, lai šis potenciālais instruments: [38. apsvērums]*

1. *ievērotu principus, par kuriem panākta vienošanās 7. ieteikumu kopā;*
2. *būtu tehnoloģiski neitrāls [21. ieteikums];*
3. *veicinātu pret* ECS*, kas nesadarbojas, vērstu kriminālatiesisku pasākumu, tostarp brīvības atņemšanas, saskaņošanu ES līmenī nolūkā īstenot sadarbību [34. ieteikums];*
4. *pilnībā ņemtu vērā pamattiesību perspektīvu un valstu suverenitāti krimināllietās un valsts drošības jomā [38. ieteikums];*
5. *iedvesmotos no darba, kas paveikts saistībā ar e-pierādījumu noteikumu pieņemšanu [38. ieteikuma iv) punkts];*
6. *paredzētu pakalpojumu sniedzējiem pienākumu savos pakalpojumos pieslēgt vai atslēgt konkrētas funkcijas, lai iegūtu informāciju pēc ordera saņemšanas (piemēram, konkrēta lietotāja ģeolokācijas saglabāšana pēc tam, kad par viņiem ir veikts likumīgs pieprasījums) [32. ieteikums];*
7. *iekļautu mehānismus, lai nodrošinātu, ka dalībvalstis var piemērot sankcijas pret* ECS*, kas nesadarbojas (vai nu administratīvie, vai kriminālatiesiskie pasākumi, atkarībā no tā, vai pakalpojumu sniedzējs tikai nesadarbojas vai piedāvā noziedzīga rakstura pakalpojumu), saskaņā ar Digitālo pakalpojumu akta noteikumiem un, iespējams, pamatojoties uz tiem, un ka šādas sankcijas attur no šiem subjektiem [33. ieteikums].*

ES ieteikumā par likumīgu pārtveršanu paredzēto principu izpilde būtu svarīgs solis ceļā uz saskaņotākiem un izpildāmākiem noteikumiem par likumīgu pārtveršanu. Tomēr joprojām var būt vajadzīgs juridisks instruments, lai uzlabotu juridisko noteiktību, lai nodrošinātu, ka ir ieviesti nepieciešamie aizsardzības pasākumi attiecībā uz visiem attiecīgajiem *ECS*, kad tiek īstenota likumīga pārtveršana, un lai nodrošinātu, ka *ECS*, kas nevēlas izpildīt dalībvalstu pieņemtos noteikumus, ir spiesti to darīt.

Galvenā darbība: Augsta līmeņa grupas eksperti aicina Komisiju izvērtēt tiesiskā regulējuma turpmāku izstrādi attiecībā uz likumīgu pārtveršanu tiesībaizsardzības nolūkos

- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju pirms iespējamā ietekmes novērtējuma izvērtēt iespēju izstrādāt ES juridisku instrumentu par likumīgu pārtveršanu, pamatojoties uz darbu, kas veikts, gatavojoties ES E-pierādījumu regulai un direktīvai, un koncentrējoties uz potenciālu tehnoloģiski neitrālu risinājumu apzināšanu.

II. Risināt tehnoloģiskās problēmas

Daudzas problēmas, ar kurām tiesībaizsardzības iestādes saskaras attiecībā uz piekļuvi datiem, izriet no tā, cik grūti tām ir paredzēt tehnoloģiju attīstību un pielāgoties tai. Tas ir tāpēc, ka atšķirībā no aktoriem citās jomās, piemēram, aizsardzības vai kosmosa jomā, tiesībaizsardzības iestādēm nav tam vajadzīgo resursu vai spēcīgu attiecību ar nozari, un tām arī parasti tas nav vajadzīgs. Daudzos gadījumos iekšējās drošības jomas aktori cenšas novērst tehnoloģiskās nepilnības reaktīvā veidā vai – biežāk – cenšas apmierināt savas vajadzības ar standarta tehnoloģiju, kas ir pieejama un cenas ziņā pieņemama. Lai veicinātu pāreju no reaktīvas pieejas uz proaktīvāku pieeju, tehnoloģiskās problēmas ir jārisina strukturētā, tālredzīgā un daudzdisciplīnu veidā, izvirzot divas galvenās prioritātes: no valstu iestāžu viedokļa ir būtiski nodrošināt, ka tiesībaizsardzības iestādēm ir piekļuve attiecīgajām spējām iegūt un apstrādāt pieejamus tranzītā esošus datus; lai gan operatoriem un tehnoloģiju nodrošinātājiem ir ļoti svarīgi, lai viņi spētu pildīt savus pienākumus attiecībā uz piekļuvi datiem, privātumu un kiberdrošību un lai tiktu aizsargātas viņu intereses.

Tāpēc eksperti ierosina paredzēt tehnoloģiskās problēmas, izmantojot visaptverošu un tālredzīgu politiku, kuras pamatā ir **tehnoloģiju ceļvedis likumīgai piekļuvei**, kurā tiks noteikti mērķi un noteiktas darbības ar saistīto finansējumu šo mērķu sasniegšanai.

Attiecībā uz spēju veidošanu, lai gan problēmas ir atšķirīgas, ekspertu ierosinātā pieeja digitālās kriminālistikas, datu saglabāšanas un likumīgas pārtveršanas jomā [120] bieži vien ir līdzīga, un tās pamatā ir vieni un tie paši ieteikumi, un tajā ir izteikta prasība pēc mērķorientētas plānošanas, lai virzītu finansēšanas iespējas, ciešāk iesaistot nozares aktorus un galvenās ieinteresētās personas, piemēram, ES Inovācijas centru iekšējai drošībai.

Tomēr tiesībaizsardzības eksperti īpaši norādīja uz diviem elementiem, kas ir specifiski likumīgai pārtveršanai.

- Plašāka metadatu, piemēram, atrašanās vietas datu, zvanu ierakstu un e-pasta galveņu, izmantošana var sniegt papildu uzvedinošus elementus izmeklēšanā. **Tā kā arvien vairāk ierīču tiks pieslēgtas internetam, palielināsies ģenerēto datu apjoms, sniedzot vairāk iespēju identificēt uzvedības modeļus.** Eksperti aicināja paplašināt pētniecību, inovāciju un ieviešanu attiecībā uz **metadatu plašāku izmantošanu**, piemēram, izmantojot mākslīgo intelektu, lai mazinātu piekļuves trūkumu satura datiem. Tajā pašā laikā viņi minēja riskus privātumam, kas saistīti ar personas metadatu masveida apstrādi, plašā apmērā izmantojot mākslīgo intelektu, kas ir jālīdzsvaro ar satura datu mērķtiecīgu izmantošanu. Tomēr tiesībaizsardzības eksperti ir pārliecināti, ka ar metadatiem vien nevar pilnībā aizstāt saziņas satura pierādījuma spēku nodoma pierādīšanai.

- Ja noziedznieki izmanto īpašas pilnīgi šifrētas sakaru platformas, tiesībaizsardzības iestādēm ir jāizmanto taktiski risinājumi, kuru pamatā ir **ievainojamības** izmantošana, lai iegūtu piekļuvi aizdomās turēto personu saziņai. Vairākas tiesībaizsardzības iestādes jau darbojas saskaņā ar tiesisko regulējumu, kas ļauj veikt pārtveršanu saziņas galapunktos, un tām ir tehnoloģija, lai to darītu, un šajā ziņā ir iespējami turpmāki uzlabojumi. Tas varētu ietvert atbalstu ES izstrādātu instrumentu attīstībai un ļaut tiesībaizsardzības iestādēm tos iegādāties un izmantot saskaņā ar spēkā esošo tiesisko regulējumu.

  Tomēr tiesībaizsardzības eksperti norādīja, ka šo metodi nevajadzētu izvērst kā galveno pierādījumu vākšanas līdzekli, jo taktiskā pārtveršana nav ne mērogojama, ne bez problēmām. Piemēram, varētu rasties jurisdikcijas jautājumi uz mērķa atrašanās vietas dēļ. Turklāt tādu ievainojamību izmantošana, kuras nevar atklāt, nenovēršami ir pretrunā kiberdrošības pamatprincipiem.

[120] Sīkāk izklāstīts nodaļā par digitālo kriminālistiku.

Attiecībā uz integrētu likumīgu piekļuvi tiesībaizsardzības eksperti ierosināja piesardzīgu pieeju, jo nozares aktoriem nevajadzētu lūgt integrēt kādu sistēmu, kas varētu vājināt šifrēšanu visiem pakalpojuma lietotājiem vispārējā vai sistēmiskā veidā; likumīgai piekļuvei arī turpmāk vajadzētu būt mērķorientētai, pamatojoties uz katru saziņu atsevišķi. Viņi vienojās par vispārējā mērķa atbilstību, bet īpaši norādīja, ka ir pakāpeniski jāvirzās uz priekšu un jāiesaista visas attiecīgās ieinteresēto personu kategorijas, tostarp tehnoloģiju, kiberdrošības un privātuma eksperti, ņemot vērā iespējamos riskus un publisko debašu sensitivitāti. Jo īpaši viņi stingri ieteica izmantot uz pierādījumiem balstītu pieeju un rūpīgi izvērtēt tādu tehnisko risinājumu pieejamību, kas nevājina sakaru kiberdrošību un negatīvi neietekmē operatoru kiberdrošību.

10. ieteikumu kopa

Lai risinātu likumīgas pārtveršanas tehnoloģiskās problēmas, eksperti iesaka izstrādāt ***tehnoloģiju ceļvedi likumīgai piekļuvei*** [121]*, kurā jo īpaši:*

1. *apvienos tehnoloģiju, kiberdrošības, privātuma, standartizācijas un drošības ekspertus un nodrošinās pienācīgu koordināciju, iespējams, izmantojot pastāvīgu struktūru [22. ieteikums];*
2. *veicinās datu ieguves un piekļuves datiem rīku, tostarp atšifrēšanas spēju, kā arī uz MI balstītu datu analīzes spēju pētniecību, izstrādi un ieviešanu* [122] *[4. ieteikums];*
3. *veicinās koordinētu pieeju standartizācijai, kurā attiecīgā gadījumā tiktu ņemtas vērā vajadzības pēc likumīgas piekļuves datiem un kura arī [15., 16. un 20. ieteikums]:*
    a. *veicinātu praktiķu no visām attiecīgajām kopienām iesaistīšanos attiecīgajās standartizācijas grupās;*
    b. *papildinātu turpmākās iniciatīvas ar atbilstošiem standartizācijas pasākumiem (lai veicinātu tehnoloģiski neitrālu pieeju);*
    c. *aptvertu sakaru tehnoloģijas kopumā, lietu internetu (tostarp, piemēram, satīklotus automobiļus) un jebkāda veida savienojamību (tostarp, piemēram, satelītsakarus);*
4. *uzlabos ES koordināciju ar nozari, lai risinātu situācijas, kad pastāv tehnoloģiski risinājumi, kas netiek īstenoti; šādos gadījumos* [123] *ir vajadzīgi skaidri norādījumi un ES līmenī veicināts dialogs [24. ieteikums];*
5. *īstenos integrētu likumīgu piekļuvi visām attiecīgajām tehnoloģijām saskaņā ar tiesībaizsardzības iestāžu paustajām vajadzībām, vienlaikus nodrošinot spēcīgu drošību un kiberdrošību un to, ka tiek izpildīti juridiskie pienākumi attiecībā uz likumīgu piekļuvi [22. ieteikums];*
6. *rūpīgi pievērsīsies šifrēšanas problēmām:*
    a. *nodrošinot, ka iespējamie jaunie pienākumi un/vai standarti tieši vai netieši nerada pakalpojumu sniedzējiem pienākumus vājināt sakaru drošību, kopumā vājinot vai vājinot pilnīgu šifrēšanu [23. ieteikums];*
    b. *nodrošinot, ka likumīgai integrētai piekļuvei nav negatīvas ietekmes uz iesaistītās aparatūras vai programmatūras arhitektūras drošības stāvokli [23. ieteikums];*
    c. *koordinētākā veidā un ar ES finansējuma atbalstu strādājot pie metodikas mērķorientētas likumīgas piekļuves izstrādei, rīcībai saistībā ar to un tās izmantošanai, lai risinātu gadījumus, kad nav iespējams piekļūt datiem, izmantojot sadarbību ar* ECS *[10. ieteikums]*.

---

121 Tehnoloģiju ceļvedim būtu jāaptver trīs darba virzieni: digitālā kriminālistika, datu saglabāšana un likumīga pārtveršana.

122 Šis ieteikums attiecas arī uz piekļuvi datiem ierīcē (sk. iedaļu par digitālo kriminālistiku), taču lietošanas gadījumi nedaudz atšķiras.

123 Piemēram, ja maršrutēšanas, izmantojot mājas operatora tīklu, nolīgumi vai konkrēts *RCS* īstenošanas veids neļauj veikt likumīgu pārtveršanu.

Lai gan dažas Augsta līmeņa grupas ekspertu ierosinātās iniciatīvas jau daļēji pastāv, ir ļoti svarīgi tehnoloģiju ceļvedī labāk strukturēt tehnoloģiju vidēja termiņa un ilgtermiņa politiku attiecībā uz likumīgu piekļuvi, nosakot konkrētus mērķus un ar to saistītu uzraudzības instrumentu. Šai pieejai būtu jāaptver ne tikai piekļuve tranzītā esošiem datiem, bet arī digitālā kriminālistika un datu saglabāšana.

Tehnoloģiju ceļvedim vajadzētu būt tālredzīgam, izpildāmam, koncentrētam uz prioritāriem tematiem un balstītam ES digitālajā stratēģijā. Tam ciešā partnerībā būtu jāiesaista visas attiecīgās ieinteresēto personu kategorijas, jo īpaši ES iestādes, struktūras un aģentūras, valstu iestādes, akadēmisko aprindu pārstāvji visās attiecīgajās jomās, nozare un NVO, un tam vajadzētu būt skaidrai pārvaldībai.

Galvenā darbība: Augsta līmeņa grupas eksperti mudina Komisiju nākt klajā ar tehnoloģiju ceļvedi par piekļuvi datiem un to īstenot

- Augsta līmeņa grupas eksperti aicina Eiropas Komisiju izstrādāt un īstenot tehnoloģiju ceļvedi, kurā galvenā uzmanība pievērsta šifrēšanas problēmām, pievēršoties visiem attiecīgajiem aspektiem, tostarp tehnoloģiskajiem, tirgus, kiberdrošības, pamattiesību, standartizācijas, tiesībaizsardzības un pētniecības aspektiem. Šim tehnoloģiju ceļvedim vajadzētu būt pieejamam 2025. gadā, un tam būtu jābalstās uz visām attiecīgajām dalībvalstu un ES iestāžu, struktūru un aģentūru speciālajām zināšanām, tostarp par kiberdrošību, datu aizsardzību un privātumu.