Europos Sąjungos Taryba

Briuselis, 2025 m. kovo 13 d.
(OR. en)

15941/2/24
REV 2

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

PRANEŠIMAS

nuo:	Pirmininkaujančios valstybės narės
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	11281/24
Dalykas:	Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupės baigiamoji ataskaita

Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupės bendrapirmininkių vardu pirmininkaujanti valstybė narė priede pateikia delegacijoms aukšto lygio grupės baigiamąją ataskaitą.

Ši peržiūrėta redakcija atspindi redakcinius pakeitimus, padarytus lingvistinės peržiūros metu.

PRIEDAS

Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupės baigiamoji ataskaita

2024 m. lapkričio 15 d.

Pareikštos nuomonės yra tik aukšto lygio grupės ekspertų nuomonės ir neturėtų būti laikomos atspindinčiomis oficialias Europos Komisijos arba Tarybos pozicijas.

Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupės pateiktos rekomendacijos turi būti įgyvendinamos visapusiškai atsižvelgiant į valstybių narių kompetenciją. Jos taikomos tik teisėsaugos veiklai ir teisminėms reikmėms naudojamoms komercinėms priemonėms ir nedaro poveikio išimtinei valstybių narių atsakomybei už nacionalinį saugumą. Todėl suverenioms priemonėms ir priemonėms, naudojamoms ir / arba sukurtoms tik nacionalinio saugumo tikslais, šios rekomendacijos netaikomos.

Turinys

Santrauka

Europos Sąjunga yra laisvės, saugumo ir teisingumo erdvė, kurioje gerbiamos pagrindinės teisės bei skirtingos valstybių narių teisinės sistemos ir tradicijos. Ji siekia užtikrinti aukšto lygio saugumą[1], taikydama nusikalstamumo prevencijos ir kovos su juo priemones, ir palengvinti teisėsaugos, teisminių ir kitų kompetentingų institucijų veiklos koordinavimą ir bendradarbiavimą.

Technologinė plėtra ir mūsų visuomenėse vykstanti skaitmenizacija lėmė tiek reikšmingus kasdienio piliečių gyvenimo pokyčius, tiek naujus iššūkius teisėsaugos ir teisminėms institucijoms užtikrinant aukšto lygio saugumą tiek nacionaliniu, tiek ES lygmenimis. Dabartiniame skaitmeniniame amžiuje beveik kiekvienas nusikalstamos veikos tyrimas pasižymi skaitmeniniu komponentu. Šis klausimas buvo aptartas 2023 m. balandžio mėn. Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupės veiklos apimties nustatymo dokumente:

> [t]echnologijomis ir priemonėmis [...] piktnaudžiaujama ir nusikalstamais tikslais. Dėl to tampa vis sunkiau toliau užtikrinti veiksmingą teisėsaugą visoje ES, garantuoti visuomenės saugumą ir užkirsti kelią nusikaltimams, juos atskleisti, tirti ir užtikrinti baudžiamąjį persekiojimą už juos, taip pat patenkinti teisėtus nukentėjusiųjų lūkesčius, susijusius su teisingumu ir kompensavimu. Jei šis klausimas nebus tinkamai sprendžiamas, kyla realus pavojus, kad ši dabartinė tendencija sudarys sąlygas nusikaltėliams likti nepastebėtiems [...]. Tai kelia didelę grėsmę asmenų ir visuomenės saugumui ir galiausiai gali sutrukdyti pozityviai valstybės pareigai toliau užtikrinti teisinę valstybę ir demokratinę visuomenę[2].

[1] Šio dokumento tikslais terminas „saugumas“ reiškia kovą su nusikalstamumu arba grėsmių visuomenės saugumui prevenciją.

[2] 2023 m. balandžio 13 d. dok. 8281/23.

ES pagrindinių teisių chartijoje užtikrinama teisė į tai, kad būtų gerbiamas privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas, taip pat teisė į asmens duomenų apsaugą. Komunikacijos (tiek raštu, tiek telefonu) konfidencialumas yra itin svarbus demokratinių visuomenių laimėjimas, užtikrinantis, kad nei valstybė, nei privatūs subjektai negalėtų kliudyti žmonėms naudotis saviraiškos laisve, ir sudarantis sąlygas kurti klestinčią pilietinę visuomenę. Naudojimuisi tomis teisėmis gali būti taikomi teisės aktuose nustatyti apribojimai, visų pirma susiję su priemonėmis, skirtomis nacionaliniam saugumui, gynybai ar visuomenės saugumui užtikrinti, taip pat nusikalstamų veikų arba neteisėto elektroninių ryšių sistemų naudojimo prevencijai, tyrimui, atskleidimui ir baudžiamajam persekiojimui už juos vykdyti, jei šios priemonės demokratinėje visuomenėje yra būtinos, tinkamos ir proporcingos. Todėl teisėsaugos ir teisminės institucijos gali atidaryti ir skaityti rašytinius pranešimus, perimti telefoninius skambučius ir klausytis pokalbių, jei manoma, kad tai būtina, proporcinga ir pagrįsta, jei tokios priemonės atitinka taikytinas teisines nuostatas ir jei jos taikomos tinkamai gerbiant pagrindines teises. Šia galimybe turėtų galėti naudotis visos kompetentingos institucijos, neatsižvelgiant į technologinę plėtrą. Pastaraisiais metais plintant naujoms asmenų tarpusavio ryšio formoms, prie naujų realijų turi prisitaikyti visa visuomenė. Turime užtikrinti, kad piliečių komunikacija išliktų apsaugota, o teisėsaugos ir teisminės institucijos toliau galėtų vykdyti savo pareigą apsaugoti piliečius užkirsdamos kelią sunkių formų ir organizuotam nusikalstamumui ir terorizmui ir su šiais reiškiniais kovodamos. Poreikis prisitaikyti yra skubus ir ekspertai ragina politikos formuotojus veikti nedelsiant, nes teisėsaugos institucijos jau nebežengia koja kojon su technologine plėtra ir tai daro tiesioginį poveikį jų gebėjimui ginti piliečių teises.

2023 m. sausio 26 d. neformaliame teisingumo ir vidaus reikalų ministrų posėdyje vidaus reikalų ministrai apsvarstė iššūkius, kuriuos technologinė plėtra teisėsaugai kelia skaitmeniniame amžiuje. Jie taip pat išreiškė susirūpinimą dėl to, kad dėl taikytinų taisyklių ir jų aiškinimo jurisprudencijoje, taip pat praktinių ir veiklos kliūčių teisėsaugos institucijoms vis sunkiau atlikti savo darbą, visų pirma kiek tai susiję su duomenų, reikalingų nusikaltimų tyrimui ir baudžiamajam persekiojimui už juos vykdyti, saugojimu ir prieiga prie jų[3].

[3] Žr. 2023 m. kovo 23 d. dok. 7184/1/23 REV 1 (valstybių narių pastabų rinkinys).

Po šios diskusijos Taryba pritarė tam, kad būtų sudaryta grupė, kuri parengtų strateginę į ateitį orientuotą viziją dėl veiksmingos ir teisėtos teisminių ir teisėsaugos institucijų prieigos prie duomenų, elektroninių įrodymų ir informacijos skaitmeniniame amžiuje – **Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupė (toliau – aukšto lygio grupė)[4].**

Aukšto lygio grupės tikslas buvo išsiaiškinti, kaip įveikti iššūkius, susijusius su teisėtos prieigos prie duomenų suteikimu, kad visiems ES gyvenantiems žmonėms būtų užtikrintas aukšto lygio saugumas, kartu užtikrinant pagrindinių teisių, įskaitant teises į privatumą ir duomenų apsaugą, laikymąsi, taip pat aukšto lygio kibernetinį saugumą, taikant veiksmingus ir ateities iššūkiams pritaikytus sprendimus.

42 rekomendacijos[5], kurios yra pagrindinis aukšto lygio grupės darbo rezultatas, pateikiamos tokiu metu, kai daugėja raginimų užtikrinti atsakomybę internete. Rekomendacijose nagrinėjami su technologine plėtra susiję dabartiniai ir numatomi iššūkiai, o jų tikslas – sudaryti sąlygas taikyti visapusišką ES požiūrį užtikrinant veiksmingą nusikalstamų veikų tyrimą ir baudžiamąjį persekiojimą už jas. Rekomendacijos suskirstytos į tris grupes: **pajėgumų stiprinimas, bendradarbiavimas su pramonės sektoriumi bei standartizacija ir teisėkūros priemonės.** Jose pabrėžiama, kad teisėsaugos institucijoms kyla iššūkių, susijusių su prieiga prie duomenų skaitomu formatu nusikalstamų veikų tyrimų tikslais, kadangi nėra nustatytų suderintų duomenų saugojimo pareigų ir griežtų ES jurisprudencijos reikalavimų, vis dažniau naudojamas ištisinis šifravimas ir trūksta tam tikrų netradicinių telekomunikacijų paslaugų teikėjų bendradarbiavimo. Rekomendacijose palankiai vertinamos taisyklės dėl e. įrodymų, tačiau pabrėžiama, kad jos yra nepakankamos šifravimo keliamiems iššūkiams įveikti, ir raginama stiprinti teisėsaugos ir teisminių institucijų bei paslaugų teikėjų bendradarbiavimą, kad būtų puoselėjamas nuolatinis dialogas ir abipusis supratimas apie veiklos, techninius ir verslo poreikius ir pašalinti prieigos prie šifruotų duomenų sunkumai. Ekspertų teigimu, tvirtesnis teisėsaugos institucijų ir paslaugų teikėjų bendradarbiavimas padėtį pagerins tam tikru mastu, tačiau ateities iššūkiams pritaikytam sprendimui užtikrinti taip pat reikia, kad teisės aktais būtų užtikrintas paslaugų teikėjų pareigos bendradarbiauti vykdymas, bendrai ar sistemingai nesusilpninant šifravimo paslaugų naudotojams.

---

4 Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupė – Europos Komisija (europa.eu)

5 Aukšto lygio grupės rekomendacijos.

2024 m. birželio 13 d. **Taryba pasikeitė nuomonėmis** dėl aukšto lygio grupės rekomendacijų, iš esmės palankiai įvertino aukšto lygio grupės ekspertų atliktą darbą ir pabrėžė, kad reikia skubiai tęsti darbą, susijusį su prieiga prie duomenų veiksmingai teisėsaugai užtikrinti[6]. Vidaus reikalų ministrai nustatė šiuos prioritetus: 1) sukurti suderintą ES teisinę duomenų saugojimo teisėsaugos tikslais sistemą; 2) nustatyti taisykles dėl veiksmingos prieigos prie duomenų, aktualių tarpasmeninių elektroninių ryšių atžvilgiu, ir 3) nustatyti teisiškai ir techniškai pagrįstus prieigos prie šifruotų elektroninių ryšių sprendimus atskirais atvejais ir kai yra priimta teisminė nutartis sunkių ir organizuotų nusikaltimų, taip pat terorizmo prevencijos, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais.

Be to, ministrai pasisakė už tai, kad būtų stiprinamas ES poveikis protokolų ir technologijų standartizavimui ir kad būtų laikomasi suderinto požiūrio į skaitmeninės ekspertizės priemonių ir procedūrų sertifikavimą. Galiausiai jie ragino parengti rekomendacijų įgyvendinimo veiksmų gaires, kuriose pateikiamas tikslus tvarkaraštis ir įvertinamas įgyvendinamumas bei tinkami finansiniai ištekliai. Jie taip pat nurodė, kad svarbu koordinuoti atskirų rekomendacijų įgyvendinimą.

Šios baigiamosios ataskaitos tikslas – išsamiai apibūdinti ekspertų nustatytus iššūkius ir nurodyti galimybes tęsti darbą ir **įgyvendinti rekomendacijas**. Joje išdėstyti keli pagrindiniai klausimai, kuriuos nustatė ekspertai ir kuriais buvo grindžiamas darbas trimis kryptimis pagal aukšto lygio grupės įgaliojimus.

Pirma, **skaitmeninei ekspertizei** atlikti yra labai svarbi prieiga prie duomenų, kad teisėsaugos institucijos galėtų rinkti ir analizuoti įrodymus iš elektroninių įtaisų. Šie duomenys suteikia patikimos informacijos apie nusikalstamą veiklą ir padeda nustatyti už nusikalstamas veikas atsakingus asmenis. Dėl sparčios tam tikrų technologijų, pavyzdžiui, šifravimo, pažangos ir plataus jų naudojimo teisėsaugos institucijos turi stiprinti savo išteklius, įgūdžius ir techninius sprendimus, susijusius su prieiga prie šifruotų duomenų. Todėl, o taip pat kalbant apie komercinių sprendinių naudojimą, gali padėti veiksmingas tarpvalstybinis bendradarbiavimas, pasitelkiant dalijimąsi ekspertinėmis žiniomis, standartizuotų priemonių ir procedūrų kūrimą ir išteklių sutelkimą. Tačiau ekspertai sutiko, kad teisėsaugos pajėgumų nesustiprins vien gebėjimų stiprinimas. Kai kurių ekspertų nuomone, tvaresnis ilgalaikis sprendimas yra prieigos prie duomenų skaitomu formatu aiškiai reglamentuojamomis aplinkybėmis suteikimas.

[6] 2024 m. birželio 21 d. dok. 11281/24.

Antra, tam, kad teisėsaugos institucijos galėtų veiksmingai tirti nusikaltimus ir vykdyti baudžiamąjį persekiojimą už juos, reikia suderintų ir nuoseklių **duomenų saugojimo** teisės aktų, kuriuose būtų visapusiškai atsižvelgiama į pagrindines teises. Dėl sparčios technologijų pažangos vis vertingesnė tampa savalaikė teisėsaugos institucijų prieiga prie atitinkamų paslaugų teikėjų saugomų duomenų. Visų pirma prieiga prie paslaugų teikėjų saugomų komunikacijos metaduomenų yra labai svarbi siekiant nustatyti įtariamuosius ir suprasti jų veiklą, be to, įrodyta jos svarba darant pažangą tyrimuose.

Trečia, **teisėtas duomenų perėmimas** yra labai svarbus siekiant veiksmingai tirti organizuotus nusikaltimus ir teroristinių grupuočių veiklą ir patraukti už juos arba jas baudžiamojon atsakomybėn. Tai sudaro sąlygas valdžios institucijoms, vadovaujantis teismo nurodymais ir visapusiškai gerbiant pagrindines teises, prašyti paslaugų teikėjų pateikti komunikacijos turinį, nes tas turinys suteikia vertingų įžvalgų apie nusikalstamą veiklą. Atsižvelgiant į perėjimą nuo tradicinių ryšių paslaugų teikėjų teikiamų paslaugų prie internetu teikiamų paslaugų (OTT), kaip apibrėžta Europos elektroninių ryšių kodekse (EERK)[7], ir į tai, kad nusikaltėliai vis dažniau pereina į ištisinio šifravimo platformas[8], kalbant apie teisėtą prieigą prie komunikacijos tikruoju laiku reikia įvertinti poreikį nustatyti aiškias teisėsaugos institucijų ir technologijų įmonių bendradarbiavimo taisykles, taip pat sustiprinti bendradarbiavimą ES lygmeniu, kad būtų lengviau teikti tarpvalstybinius prašymus.

Rekomendacijos ir tai, kas apžvelgiama šioje baigiamojoje ataskaitoje, atspindi **tik aukšto lygio grupės ekspertų lūkesčius ir prašymus**.

Pateikusi šią ataskaitą **aukšto lygio grupė užbaigė savo darbą** ir ragina Komisiją, valstybes nares, Europos Parlamentą ir visus susijusius suinteresuotuosius subjektus šiomis rekomendacijomis ir ataskaita remtis rengiant priemones, skirtas prieigos prie duomenų veiksmingos teisėsaugos tikslais klausimui spręsti. Tokias priemones turėtų lydėti tvirtas naratyvas, jog reikia skubiai imtis reikšmingų veiksmų, kad būtų užtikrinta veiksminga teisėta prieiga prie duomenų. Ekspertai ragina visas ES institucijas ir įstaigas nedelsiant daryti pažangą šiame darbe ir įgyvendinti konkrečias iniciatyvas specialių veiksmų gairių kontekste.

---

[7] Pagal 2018 m. gruodžio 11 d. direktyvą (ES), kuria nustatomas Europos elektroninių ryšių kodeksas, dalis teisinės sistemos, taikomos tradicinėms telekomunikacijoms, yra taikoma ir įmonėms, kurios teikia internetines paslaugas naudodamosi telekomunikacijų infrastruktūra, kuri joms nepriklauso ir kurios jos nevaldo, įskaitant su numeriu nesiejamo asmenų tarpusavio ryšio paslaugas.

[8] 2024 m. Europolo atliktas organizuoto nusikalstamumo internete grėsmės vertinimas (OCTA).

Teisėta prieiga: pagrindiniai iššūkiai

Pastaraisiais metais mūsų gebėjimas kovoti su nusikalstamumu ir užtikrinti ES saugumą patobulėjo daugelyje sričių. Teisėsaugos ir teisminis bendradarbiavimas tapo veiksmingesnis, įgyvendinami nauji kovos su sunkių formų ir organizuotu nusikalstamumu teisės aktai ir priemonės, taip pat sustiprintos bendros pastangos kovoti su neteisėtu migrantų gabenimu, prekyba žmonėmis, neteisėta prekyba šaunamaisiais ginklais ir narkotikais, korupcija ir kitais sunkiais nusikaltimais.

Tačiau užtikrindamos mūsų piliečių saugumą teisėsaugos institucijos kasdien susiduria su naujais iššūkiais, visų pirma tais, kurie kyla dėl mūsų visuomenėje vykstančios skaitmenizacijos.

Skaitmeninės technologijos keičia mūsų gyvenimus – nuo mūsų bendravimo būdo iki gyvenimo ir darbo būdo, o visuomeniniai šio pokyčio aspektai yra itin reikšmingi. Skaitmenizacija gali padėti įveikti daugelį iššūkių, su kuriais susiduria Europa ir europiečiai, ir suteikia daug didelių galimybių – kurti darbo vietas, tobulinti švietimą, skatinti konkurencingumą ir inovacijas, kovoti su klimato kaita, palengvinti žaliąją pertvarką ir dar daugiau.

Tačiau ji taip pat sudaro sąlygas nusikaltėliams naudotis technologijų pažanga nusikaltimams daryti tiek internete, tiek realiame gyvenime. Šifruoti įrenginiai ir programėlės, nauji ryšių operatoriai, virtualieji privatieji tinklai (VPN) ir kt. yra kuriami taip, kad būtų saugomas teisėtų naudotojų privatumas. Tačiau jie taip pat suteikia nusikaltėliams veiksmingų priemonių tapatybei nuslėpti, prekiauti savo nusikalstamais produktais ir paslaugomis, nukreipti mokėjimus, nuslėpti savo veiklą bei komunikaciją ir taip veiksmingai išvengti nustatymo, tyrimo ir baudžiamojo persekiojimo. Nors yra specialiai sukurtų priemonių ir paslaugų, naudojamų pirmiausia neteisėtai veiklai vykdyti, akivaizdu, kad nusikaltėliai vis dažniau išnaudoja teisėtų elektroninių ryšių paslaugų (ERP) teikėjų teikiamų privatumo apsaugos priemonių privalumus. ***Šiuo atžvilgiu teisėsaugos institucijos dažnai atsilieka nuo nusikaltėlių, nes joms trūksta tinkamai parengtų darbuotojų ir priemonių šiam iššūkiui veiksmingai įveikti.*** Dėl šių pokyčių pastaraisiais metais vykdant nusikalstamų veikų tyrimus ir baudžiamąjį persekiojimą už jas vienu iš pagrindinių iššūkių tapo prieiga prie duomenų teisėsaugos tikslais. Tačiau buvo ir puikių sėkmės pavyzdžių: teisėsaugos institucijoms pavyko išardyti tokius nusikalstamo pobūdžio šifruoto ryšio tinklus kaip „EncroChat“ ir SkyECC ir jos toliau vykdo tokias operacijas kaip „Desert Light“ („Dykumos šviesa“) – vykdant šią operaciją 2022 m. lapkričio mėn. buvo sužlugdytas prekiautojų kokainu megakartelis. Per pastaruosius kelerius metus Europolo iššifravimo platforma padėjo atlikti kelis aukšto lygio tyrimus ir taip prisidėjo prie sėkmingų teisėsaugos veiksmų kovojant su terorizmu ir sunkių formų bei organizuotu nusikalstamumu.

Tačiau už šių sėkmės istorijų slepiasi daug uždelstų ir nesėkmingų tyrimų, nes, anot specialistų, nuolat kyla sunkumų laiku patenkinti operatyvinius poreikius.

Teisėta prieiga apsunkina technologijų naudojimą nusikalstamais tikslais, nes teisėsaugos institucijos gali tikslingai stebėti ir perimti nusikaltėlių komunikaciją ir sužlugdyti jų veiklą. Ir priešingai – neturėdamos patikimos teisinės sistemos ir tinkamų išteklių, teisėsaugos institucijos ir toliau susidurs su neįveikiamais sunkumais; be to, yra rizikos, kad itin svarbūs įrodymai liks nepasiekiami dėl įvairių priežasčių.

- **Duomenys ne visada yra prieinami**, ypač kai jie ištrinami, nes teisėsaugos tikslais taikomos duomenų saugojimo taisyklės yra nenuoseklios ir netinkamos. Ši spraga labai trukdo tirti sunkių formų ir organizuotą nusikalstamumą. Iš tiesų, 2023 m. pagal projektą SIRIUS[9] atliktoje apklausoje beveik pusė apklaustų tyrėjų nurodė, kad pagrindinė jų darbo kliūtis yra suderintos duomenų saugojimo tvarkos nebuvimas. Kai nėra suderintų taisyklių, kyla rizika, kad itin svarbūs duomenys liks nepasiekiami, o tai kenkia pastangoms veiksmingai kovoti su nusikalstamumu.

- **Duomenų neįmanoma išgauti,** ypač kai jų nepavyksta išgauti iš įrenginio. Jei nėra reikiamų įgūdžių, tinkamų priemonių ir nepakankamai bendradarbiaujama su įrenginių gamintojais ir tarp jų, skaitmeninė ekspertizė tampa sudėtinga, brangi ir ilgai užtrunkanti, o kartais ir visiškai neįmanoma. Šis didelis trūkumas kliudo veiksmingai atlikti tyrimus. Jei trūksta pažangių pajėgumų bei įgūdžių kriminalistikos srityje ir geresnio bendradarbiavimo su pramonės sektoriaus atstovais ir tarp nacionalinių valdžios institucijų, itin svarbūs skaitmeniniai įrodymai lieka neprieinami, o tai daro didelį poveikį teisėsaugos pastangoms.

- **Duomenis ne visada įmanoma perskaityti** dėl to, kad jie yra šifruoti. Daugelis tarnybų dabar naudoja ištisinį šifravimą, kad apsaugotų komunikacijos konfidencialumą, privatumą ir užtikrintų kibernetinį saugumą, tačiau dėl to teisėsaugos institucijoms gali būti labai sunku gauti prieigą prie komunikacijos duomenų. Tai reiškia, kad net jei duomenys perimami teisėtai, dažnai neįmanoma jų iššifruoti. Jei šių duomenų perskaityti negebama, svarbūs įrodymai lieka neatskleisti, todėl nusikaltimus tirti tampa daug sunkiau.

[9] SIRIUS: tarpvalstybinė prieiga prie elektroninių įrodymų (projektas SIRIUS), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Duomenis ne visada įmanoma analizuoti**, pvz., ne visada turima technologijų ir (arba) žmogiškųjų išteklių dideliems duomenų kiekiams tikrinti arba perimtiems duomenims veiksmingai filtruoti ir analizuoti taip, kad tai būtų suderinama su ES pagrindinėmis vertybėmis ir ES bei valstybių narių teisinėmis sistemomis.

- **Duomenų neįmanoma gauti** dėl skirtingų jurisdikcijų įstatymų kolizijos. Duomenys dažnai kerta tarptautines sienas, todėl kyla sudėtingų iššūkių dėl jurisdikcijos. Skirtingose šalyse galioja skirtingi įstatymai ir kiti teisės aktai, susiję su prieiga prie duomenų, todėl užsienyje saugomus duomenis gauti yra sunku. Naujasis ES E. įrodymų reglamentas ir direktyva yra svarbūs žingsniai siekiant palengvinti šį procesą, tačiau vis dar reikia daug nuveikti, kad šios priemonės būtų visiškai įgyvendintos – jų neįgyvendinus iki galo, prieiga prie kitose šalyse esančių itin svarbių duomenų teisėsaugos institucijoms ir toliau bus didelis iššūkis.

Tai keli kasdieninių šiandien teisėsaugos institucijoms tenkančių iššūkių pavyzdžiai.

Nusikaltėliai nuolat keičia savo veikimo būdus, kad nebūtų aptikti. Turimi statistiniai duomenys[10] rodo, kad nusikaltėliai vis dažniau persikelia į teisėtas ištisinio šifravimo platformas. Vis dėlto ir tuomet, kai randamos veiksmingos atsakomosios priemonės, tikėtina, kad jie savo komunikaciją perkels į dar kitus ryšių kanalus. Dėl šios priežasties labai svarbu, kad teisėsauga, padedama visų atitinkamų bendruomenių ekspertų, gebėtų stebėti technologinę plėtrą ir numatyti nusikalstamo elgesio pokyčius, pavyzdžiui, susijusius su 6G, daiktų internetu ir palydoviniu ryšiu. Be to, pajėgumai, kurie leido sėkmingai įvykdyti operacijas prieš nusikaltėliams skirtas komunikacijos paslaugas (pvz., „EncroChat“, Ghost ECC), turi būti išlaikyti ir pritaikomi, kad būtų galima įveikti būsimus panašaus pobūdžio iššūkius.

[10] Europol IOCTA, 2024 m.

Teisėsaugoms institucijoms vis dažniau prireikia galėti teisėtai prieiti prie skaitmeninės informacijos. Kadangi nusikaltėliai vis labiau kliaujasi internetinėmis paslaugomis, internetinių paslaugų teikėjai gauna vis daugiau prašymų pateikti duomenis; Išties, nuo 2017 m. iki 2022 m. tokių prašymų padaugėjo tris kartus[11]. Komunikacijos duomenys (tiek metaduomenys, tiek turinio duomenys) yra itin svarbūs atliekant daugelį nusikalstamų veikų tyrimų. Manoma, kad prieiga prie skaitmeninių įrodymų yra itin svarbus veiksnys atliekant 85 % tyrimų[12]. Naujosios taisyklės dėl tarpvalstybinės prieigos prie elektroninių įrodymų kompetentingoms institucijoms suteiks daugiau galimybių gauti prieigą prie tokių duomenų. Tačiau šios taisyklės gali veikti tik tada, kai duomenys yra prieinami skaitomu formatu. Be to tiek teisiškai, tiek praktiškai prieiga prie konfiskuotuose įrenginiuose saugomų duomenų ir teisėtas komunikacijos perėmimas ir toliau kelia didžiulių iššūkių. Kalbant apie veiksmingą perduodamų duomenų perėmimą tarpvalstybinėse bylose, valstybės narės gali prašyti teisminio bendradarbiavimo pagal Konvenciją dėl savitarpio pagalbos baudžiamosiose bylose[13] ir Europos tyrimo orderį[14]; tačiau šios priemonės buvo rengiamos pirmiausia galvojant apie keitimąsi fiziniais įrodymais, todėl jų veiksmingumas technologinės plėtros kontekste gali būti ribotas.

Suteikiant teisėtą prieigą turi būti taikomos griežtos nacionalinėje, ES ir tarptautinėje teisėje įtvirtintos ***sąlygos***, o šios prieigos reguliavimo procesai turi būti tokie, kad būtų užtikrinamas skaidrumas ir atskaitomybė, be kita ko, užkertamas kelias bet kokiam neteisėtam komercinių paslapčių atskleidimui, o teisėto atskleidimo atveju užtikrinama, kad būtų imamasi tinkamų priemonių konfidencialumui išsaugoti.

Teisėta prieiga turi būti suteikiama visapusiškai laikantis būtinumo ir proporcingumo principų ir prireikus jos suteikimas turi būti patvirtinamas teismo arba nepriklausomos institucijos. Turi būti išlaikoma pusiausvyra tarp prieigos prie duomenų ir patikimų privatumo apsaugos ir kibernetinio saugumo priemonių (tokių kaip šifravimas, užkardos, antivirusinės programos ir kovos su kenkimo programine įranga priemonės). Užtikrinant, kad suteikiant prieigą prie duomenų nebūtų viršijama to, kas būtina tyrimui atlikti, padedama apsaugoti atskirų naudotojų privatumą.

---

11 Projektas SIRIUS.

12 Komisijos poveikio vertinimas dėl pasiūlymų dėl E. įrodymų reglamento ir E. įrodymų direktyvos (2018 m. balandžio 17 d.).

13 MLA – Europos Tarybos standartai – PC-OC (coe.int).

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

Nors teisėta prieiga prie duomenų teisėsaugos tikslais yra itin svarbi, kad mūsų piliečiams būtų užtikrintas didžiausias įmanomas saugumas, ji neturi būti užtikrinama pagrindinių teisių ar sistemų ir produktų kibernetinio saugumo sąskaita. Neturi būti kompromiso tarp, viena vertus, asmenų neliečiamumo ir saugumo apsaugos ir, kita vertus, jų teisių; būtina rasti pusiausvyrą, kuri užtikrintų, kad viena neužgožtų kita. Pareiga užtikrinti, kad piliečiai galėtų naudotis aukšto lygio pagrindinių teisių apsauga ir jaustųsi saugūs kasdieniame gyvenime, tenka tiek ES, tiek valstybėms narėms. Technologinė plėtra neturi sukurti saugaus prieglobsčio nusikaltėliams: jei yra pagrįstas įtarimas, kad nusikaltimas daromas ar kad ketinama jį daryti, teisėsauga turi turėti priemonių, kurios leistų jai prieiti prie atitinkamų duomenų.

Tiek Europos žmogaus teisių konvencijoje, tiek nacionalinėse konstitucijose ir ES pagrindinių teisių chartijoje pripažįstama, kad visi turi teisę į privatų gyvenimą ir kad tai apima ir asmenų komunikaciją. ES pagrindinių teisių chartijoje taip pat nustatyta teisė į duomenų apsaugą. Teisė į privatumą ir teisė į asmens duomenų apsaugą nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų visuomeninę paskirtį[15]. Valdžios institucijos negali trukdyti naudotis šiomis teisėmis, ***nebent tai daroma laikantis įstatymų, atsižvelgiant į pačią teisių esmę ir demokratinėje visuomenėje yra būtina bei proporcinga.*** Laikantis tų sąlygų, teisė į privatumą ir teisė į asmens duomenų apsaugą gali būti apribotos, be kita ko, nacionalinio ir visuomenės saugumo labui ir nusikaltimų prevencijos, tyrimo, nustatymo ir baudžiamojo persekiojimo už juos tikslais.

Labai svarbu užtikrinti tvirtą atskaitomybę. Mūsų demokratinėse visuomenėse už tai, kad būtų sudarytos sąlygos tokiai atskaitomybei ir užtikrinamas aukšto lygio privatumas ir saugumas, yra atsakingi teisės aktų leidėjai. ***Privatumas ir saugumas nėra tarpusavyje nesuderinami.***

Sprendimai pagrįstais atvejais užtikrinti teisėtą prieigą turi būti rengiami bendradarbiaujant su visais atitinkamais suinteresuotaisiais subjektais, įskaitant pramonę, kad būtų skatinamos inovacijos ir tvirtas kibernetinis saugumas. ***Šie sprendimai turi būti rengiami tinkamai atsižvelgiant į visus atitinkamus poreikius ir reikalavimus ir negali būti paliekami vien technologijų bendrovių nuožiūrai.***

---

[15] 2024 m. balandžio 30 d. Sprendimas *La Quadrature du Net ir kt.*, byla C-470/21, EU:C:2024:370, 70 punktas.

Prieš imantis tolesnių veiksmų būtina atlikti techninius vertinimus, kad būtų atsakyta į kai kuriems kibernetinio saugumo ekspertams susirūpinimą keliančius klausimus dėl to, kad sudėtinga užtikrinti teisėtą prieigą kartu išlaikant tvirtą kibernetinį saugumą. ***Produktų ir paslaugų kibernetinis saugumas ir teisėta prieiga prie duomenų kyla iš teisinių pareigų ir turi galėti egzistuoti kartu.*** Teisėtos prieigos reikalavimai turi būti įgyvendinami remiantis aiškiais visų atitinkamų suinteresuotųjų subjektų (įskaitant pramonės atstovus, duomenų apsaugos ir kibernetinio saugumo ekspertus ir teisėsaugos specialistus) parengtais standartais, atspindinčiais atitinkamus teisinius reikalavimus, ir remiantis tinkamai įvertintais galimais sprendimais, taip užtikrinant, kad teisėta prieiga nepakenktų produktų ir paslaugų saugumui.

Daugelis įmonių ir paslaugų teikėjų nelabai nori bendradarbiauti su teisėsaugos institucijomis dėl teisinio netikrumo, susijusio su savanoriškomis priemonėmis, ir bijodami galimos neigiamos jų paslaugų ir produktų naudotojų reakcijos. Šis nenoras trukdo tyrimams. Be to, suvokdami, kad naudotojai pirmenybę teikia privatumui, o ne visuomenės saugumui, pramonės subjektai gali nenorėti atverti ryšių su teisėsaugos institucijomis kanalų ir sukurti pritaikytus mechanizmus, užtikrinančius teisėtą prieigą. Šiai problemai spręsti reikalinga aiški teisėtos prieigos prie duomenų teisinė sistema. Pagal galiojančius teisės aktus yra didelių kliūčių, kurios apsunkina tokios prieigos suteikimą, ypač savanoriškais pagrindais.

Įmonių ir teisėsaugos institucijų bendradarbiavimas yra netinkamas bei nepakankamas ir turi būti papildytas aiškiomis taisyklėmis. ***Neturėdamos aiškių ir vykdytinų teisinių pareigų, įmonės dažnai negali padėti teisėsaugos institucijoms prieiti prie duomenų.***

Nesant veiksmingų sprendimų teisėtai prieigai užtikrinti, ***dažnai vienintele galimybe laikomi pažeidžiamumu grindžiami sprendimai.***

Kai perimti duomenys (ir galbūt kiti iš įrenginio išgauti duomenys) tvarkomi privačių įmonių sukurtomis priemonėmis, nepriklausomai nuo garantijų, kurias tos įmonės gali suteikti, nacionalinės institucijos negali iš tiesų žinoti, kokie duomenys yra tikrinami ir kaip, ir turi remtis tik šalies, kurioje yra įsikūrusios duomenų perėmimo paslaugą teikiančios įmonės, vyriausybės išduotais sertifikatais. Šią problemą dar labiau apsunkina tai, kad, norint išlaikyti priemonių ir (arba) paslaugų veiksmingumą, būtina laikyti paslaptyje pažeidžiamumą, kuriuo pasinaudota. Šis klausimas ypač didelį susirūpinimą kelia tuomet, kai paslaugų teikėjas yra įsikūręs ne ES.

Ne mažiau svarbu ir tai, kad privačios įmonės, teikiančios intervencinių tyrimo metodų taikymo paslaugas, yra suinteresuotos kuo didesniu pelnu, todėl gali nuspręsti parduoti savo priemones nedemokratiškiems režimams (kaip buvo „Hacking Team“ skandalo[16] atveju).

Kita vertus, iššūkiai, kylantys norint prieiti prie duomenų, gali ***teisėsaugos institucijas paskatinti imtis labiau intervencinių tyrimo priemonių.*** Tokiais atvejais teisėsaugos institucijos yra priverstos pasitelkti labiau privatumui kenkiančias priemones, pavyzdžiui, fizinį sekimą, o ne prieigą prie geografinės vietos nustatymo duomenų, ir kratas namuose, o ne teisėtą duomenų perėmimą.

Dėl teisėsaugos institucijų negebėjimo prieiti prie duomenų gali smarkiai sumažėti visuomenės pasitikėjimas teisingumo sistema. Kai tyrimai uždelsiami arba diskredituojami, piliečiai gali pamanyti, kad sistema yra neveiksminga. Sumažėjęs pasitikėjimas gali pakenkti teisėtvarkai ir sumažinti visuomenės norą padėti teisėsaugai.

Galiausiai ***teisėta prieiga leidžia teisėsaugos institucijoms rinkti įrodymus siekiant užtikrinti teisingumą aukoms ir apsaugoti jas nuo didesnės žalos.*** Duomenys gali užvesti ant svarbių pėdsakų ir padėti atskleisti visų rūšių nusikaltimus tiek realiame gyvenime, tiek internete, ir patraukti už juos baudžiamojon atsakomybėn. Asmenys gali patirti sunkių formų patyčias kibernetinėje erdvėje, tapatybės vagystes, sukčiavimą ir kt., kylančius iš nusikalstamo piktnaudžiavimo skaitmeninėmis technologijomis, paslaugomis ir komunikacija. Ši patirtis gali turėti sunkių emocinių ir psichinių pasekmių aukoms, o tai gali padidinti esamą nelygybę ir pažeidžiamumą.

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

Atliekant bet kokį nusikalstamos veikos tyrimą reikalingi įrodymai, kad būtų galima nustatyti nusikalstamos veikos vykdytojo tapatybę arba teisme įrodyti jo atsakomybę. Jie taip pat gali padėti išteisinti pilietį, jei šis buvo neteisingai apkaltintas. Jei tyrėjai ir prokurorai negali prieiti prie reikiamos informacijos, jie gali negebėti daryti pažangos vykdydami tyrimus ir nustatyti nusikalstamos veikos vykdytojo tapatybę, o auka gali patirti papildomų kančių ir finansinių nuostolių, taip pat gali sumažėti pasitikėjimas teisingumo sistema. Vien tradicinių fizinių įrodymų ne visada pakanka, kad būtų galima nustatyti ryšius ir aptikti pėdsakus. ***Teisėsaugos ir teisminės institucijos turi būti prisitaikiusios prie skaitmeninio amžiaus. Tik tuomet jos galės visapusiškai apsaugoti mūsų visuomenes ir ekonomiką*** nuo didėjančių grėsmių, kylančių dėl kibernetinių išpuolių ir hibridinių grėsmių, taip pat nuo organizuoto nusikalstamumo veiklos.

Galima daryti išvadą, kad jei teisėsaugos institucijos negali veiksmingai prieiti prie duomenų, jos yra gerokai mažiau pajėgios užtikrinti saugumą ir sulaikyti sunkiausių nusikalstamų veikų vykdytojus. ***Teisėsaugos institucijoms turėtų būti suteikta teisėta ir griežtai kontroliuojama veiksminga prieiga prie duomenų, užtikrinant tvirtas privatumo apsaugos ir kibernetinio saugumo garantijas, kad būtų galima užkirsti kelią nusikaltimams, juos atskleisti, tirti ir patraukti už juos baudžiamojon atsakomybėn; tokiu būdu šioms institucijoms būtų sudaromos sąlygos užtikrinti saugumą, o ES piliečiams – saugiai gyventi ir sulaukti teisingumo už prieš juos padarytus nusikaltimus.***

I skyrius: Skaitmeninė ekspertizė

SU KOKIAS SUNKUMAIS SUSIDURIAMA?

Skaitmeninė ekspertizė – tai bet kokia skaitmenine forma elektroniniame įrenginyje saugomų skaitmeninių įrodymų (tiek komunikacijos metaduomenų, tiek turinio duomenų), įskaitant informaciją iš kompiuterių standžiųjų diskų, mobiliųjų telefonų, išmaniųjų prietaisų, transporto priemonių navigacijos sistemų, elektroninių durų užraktų, debesijoje saugomų duomenų ir kitų skaitmeninių įrenginių, rinkimas, analizė ir išsaugojimas.

Kadangi prieiti prie komunikacijos duomenų darosi vis sunkiau, informacijos išgavimas iš konfiskuotų įrenginių (arba prijungtųjų įrenginių tinklų) atliekant nusikalstamų veikų tyrimus tampa vis svarbesnis. Turėdamos prieigą prie įrenginiuose saugomų duomenų teisėsaugos institucijos gali gauti kokybiškesnės informacijos apie, pavyzdžiui, organizuotų nusikalstamų grupių narių tapatybę negu naudodamosi kitais būdais, pavyzdžiui, teisėtu duomenų perėmimu. Kai kurie ekspertai teigia, kad neįmanoma iš anksto žinoti, kokie duomenys yra svarbūs konkrečiam tyrimui: net informacija, kuri iš pradžių gali atrodyti nereikšminga, vykstant tyrimui gali pasirodyti esanti esminė. Prieiga prie visų įrenginyje esančių duomenų taip pat gali būti svarbi įtariamojo nekaltumui patvirtinti ir atsakovo teisėms apsaugoti[17]. Be to, tyrimo metodai visada turi būti proporcingi.

Nuolatinį **išteklių** ir pajėgumų **trūkumą**, su kuriuo šioje srityje susiduria teisėsaugos institucijos, dar labiau apsunkina tai, kad diegiamos naujos technologijos (pvz., naujų rūšių įrenginiai, daiktų internetas ir debesijos kompiuterija), todėl reikia naujų įgūdžių ir priemonių. Net jei valstybių narių agentūros ir institucijos jau yra įgijusios daug kompetencijos skaitmeninės ekspertizės srityje, tos žinios yra išsibarsčiusios ir nėra aiškių dalijimosi pajėgumais ir jų sklaidos mechanizmų, o tai reiškia, kad jos ir toliau lieka sutelktos atskiruose taškuose.

[17] Vienas ekspertas minėjo atvejį, kai įrenginio veikimo analizė buvo esminis veiksnys įrodant, kad įtariamasis negalėjo dalyvauti įvykdant žmogžudystę.

Tai, kad **skaitmeninės ekspertizės laboratorijoms trūksta palyginamų pajėgumų** ir apskritai trūksta **standartizuotų ekspertizės procedūrų** ir mechanizmų, leidžiančių **pripažinti skaitmeninės ekspertizės ekspertų įgūdžius ir kompetenciją**, gali trikdyti tarpvalstybinį bendradarbiavimą.

Aukšto lygio grupės ekspertai aiškiai nurodė: standartizuotas duomenų **šifravimas** įrenginiuose yra vienas iš pagrindinių iššūkių, su kuriuo susiduria teisėsaugos institucijos. Teisėsaugos institucijos, net ir naudodamosi galingiausiomis iššifravimo platformomis, negali prieiti prie duomenų, laikomų tam tikrų rūšių šiuolaikiniuose įrenginiuose, apsaugotuose kriptoprocesoriais[18] arba patikimais šifravimo algoritmais ir sudėtingais slaptažodžiais. Šifravimas ir kitos kibernetinio saugumo ir privatumo priemonės yra būtini informacinėms sistemoms, komunikacijai ir asmens duomenims apsaugoti, tačiau šios priemonės, o visų pirma vis dažnesnis standartizuoto šifravimo naudojimas, mažina teisėsaugos galimybes rinkti įrodymus.

Šioje srityje valstybių narių **kompetencija ir pajėgumai** yra riboti: beveik visos valstybės narės nurodo, kad joms trūksta techninių sprendimų specialistų poreikiams patenkinti, o didžioji jų dauguma mano, kad jų įgūdžiai ir finansiniai ištekliai yra nepakankami. Teisėsaugos institucijų pajėgumai iššifruoti konfiskuotuose įrenginiuose saugomą informaciją įvairiose valstybėse narėse labai skiriasi: kai kuriais atvejais sėkmės rodiklis siekia 15–20 %, o kitais – daugiau kaip du trečdalius. Tais atvejais, kai pajėgumų turima, jie paprastai yra neveiksmingi tuomet, kai reikia iššifruoti duomenis, apsaugotus tvirtais slaptažodžiais ir laikomus failuose, saugomuose specialiuose šifruotuose konteineriuose. Net ir tais atvejais, kai iššifruoti pavyksta, dažnai tai padaroma pavėluotai. Iššifravimo įranga yra brangi ir labai specializuota, o aparatinė įranga reikalauja daug pajėgumų.

Dauguma teisėsaugos skaitmeninės ekspertizės padalinių, norėdami prieiti prie duomenų įrenginiuose, naudojasi komerciniais sprendiniais, o tai kelia papildomų iššūkių: šie sprendiniai sunkiai vejasi technologinę plėtrą ir greitai sensta; dėl didelių licencijų kainų labai sumažėja įgaliotųjų naudotojų skaičius; be to, tokie sprendiniai dažnai kuriami ne Europoje ir gali būti netinkamai pritaikyti ES teisėsaugos institucijų poreikiams arba neatitikti ES skaitmeninės ekspertizės atskaitomybės standartų.

[18] Pavyzdžiui, kriptoprocesorius T2 naujausių modelių „Apple“ knyginiuose kompiuteriuose.

Dažnai teisėsaugos institucijos neturi kito pasirinkimo, kaip tik pasinaudoti **pažeidžiamumu**, kad gautų prieigą prie įrenginių iššifravimo raktų. Tačiau šiuo požiūriu grindžiami tyrimo metodai turi derėti su tikslu užtikrinti saugesnę aparatinę ir programinę įrangą, kaip įtvirtinta Kibernetinio atsparumo akte; pažeidžiamumo valdymo ir informacijos atskleidimo sistemos sumažintų nenumatytas tokių metodų pasekmes. Ekspertai apsvarstė alternatyvius sprendimus, pavyzdžiui, įtariamiesiems taikomą įpareigojimą tiriančiosioms institucijoms perduoti tuos elementus, kurių reikia prieigai prie atitinkamų įrenginių (pvz., slaptažodžius). Tokiais atvejais taikomos nacionalinės teisinės sistemos labai skiriasi ir tik trys valstybės narės nurodė turinčios konkrečias teisės aktų nuostatas, pagal kurias įtariamasis įpareigojamas suteikti prieigą prie šifravimo raktų arba iššifruotų duomenų[19]. Kai kurios valstybės narės įtariamuosius įpareigoja pateikti tam tikrus biometrinius duomenis (pvz., pirštų atspaudus) ir taip suteikti prieigą prie įrenginio; kitais atvejais įtariamieji privalo atskleisti slaptažodį. Apskritai tai tebėra sritis, kurioje turi būti toliau atliekami vertinimai.

Kai kurios pirmiau nurodytos problemos gali būti sušvelnintos **dalijantis valstybių narių pajėgumais**, kartu gerbiant jų išimtinę kompetenciją nacionalinio saugumo klausimais. Tačiau šis sprendimas vis dar netaikomas, kartais dėl teisinių apribojimų (septyniose valstybėse narėse ribojamas dalijimasis priemonėmis, o penkiose iš jų nustatyti ribojimai naudotis priemonėmis, kuriomis dalijasi kitos valstybės narės), tačiau labiau dėl to, kad nėra nustatytų dalijimosi priemonėmis ar bendro licencijų pirkimo mechanizmų.

Anksčiau teisėsaugos institucijos turėjo aiškiai nustatytus **ryšių su gamintojais ir tiekėjais kanalus**. Todėl jos galėdavo parengti bendradarbiavimo protokolus, kurie savo ruožtu padėdavo joms geriau suprasti naujai įdiegtus technologinius pokyčius ir tai palengvindavo teisėsaugos veiksmus, o kartu būdavo užtikrinamas kibernetinis saugumas. Tačiau dėl naujų technologijų diegimo ir naujų įmonių patekimo į rinką tempo sąlygos pasikeitė, ir su pramonės sektoriumi daugiau nebendradarbiaujama.

Priėmus atitinkamus standartus produktų protokolai ir techninė struktūra galėtų būti rengiami taip, jog būtų užtikrinta, kad į teisėsaugos institucijoms susirūpinimą keliančius klausimus ir techninius reikalavimus būtų atsižvelgiama ankstyvame etape. Tačiau **teisėsaugos institucijų dalyvavimas atitinkamų standartizacijos institucijų veikloje** yra nepakankamas, o tai turi įtakos jų gebėjimui veiksmingai dalyvauti rengiant būsimus technologinius standartus.

---

[19] Eurojust Cybercrime Judicial Monitor (Eurojustas, Kibernetinių nusikaltimų teisminės stebėsenos apžvalga) Nr. 4, 2018 m. gruodžio mėn., p. 34, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

GALIMI SPRENDIMAI

I. Dėti daugiau pastangų siekiant didinti pajėgumus skaitmeninės ekspertizės priemonių srityje ir šias pastangas racionalizuoti

Valstybės narės jau turi ekspertinių žinių ir pajėgumų atlikti skaitmeninę ekspertizę; tačiau dalydamosi savo techniniais sprendimais ir juos abipusiai taikydamos, atitinkamos nacionalinės institucijos ir valdžios institucijos gali pasinaudoti kitų agentūrų patirtimi ir pasiekti didelę masto ekonomiją, taip sumažindamos reikiamus finansinius išteklius. Valstybės narės gali toliau ieškoti sprendimų šiuo tikslu tiek skaitmeninės ekspertizės priemonių srityje, tiek mokymo ir įgūdžių ugdymo srityse.

1 rekomendacijų grupė

Siekiant stiprinti bendradarbiavimą ir kolektyvinius pajėgumus skaitmeninės ekspertizės srityje, ekspertai rekomenduoja:

1. *nustatyti ir sujungti esamus skaitmeninės ekspertizės tinklus ir įsteigti sekretoriatą [1 rekomendacija];*
2. *užtikrinti, kad žinios būtų prieinamesnės, ir skleisti jas tarp ekspertų [1 rekomendacija];*
3. *apsvarstyti žinių telkimo mechanizmus [2 rekomendacija];*
4. *didinti mokslinių tyrimų ir plėtros finansavimą, nustatant aiškius rezultatus [4 rekomendacija];*
5. *propaguoti Europolo priemonių saugyklą kaip pagrindinį dalijimosi priemonėmis centrą [4 rekomendacija];*
6. *sudaryti palankesnes sąlygas valstybėms narėms dalytis sprendimais ir skaitmeninės ekspertizės priemonėmis esant pasitikėjimo atmosferai (kartu atsižvelgiant į nacionalines taisykles) [2 rekomendacija];*
7. *sukurti ES lygmens mechanizmą, pagal kurį būtų bendrai perkamos skaitmeninės ekspertizės priemonių licencijos, siekiant jomis dalytis tarp valstybių narių [3 rekomendacija];*
8. *skatinti bendradarbiavimą su skaitmeninės ekspertizės priemonių gamintojais ir plėtotojais, siekiant supaprastinti naudojant tas priemones teisėsaugos institucijų gaunamų duomenų struktūrą ir formatą, idealiu atveju laikantis sutartų standartų [12 rekomendacija];*
9. *ES lygmeniu sukurti komercinės skaitmeninės ekspertizės priemonių vertinimo ir, kai aktualu, sertifikavimo mechanizmą / schemą, atkreipiant dėmesį į tai, kad nebūtų sukelta neigiamo poveikio tyrimams ir baudžiamajam persekiojimui, pvz., neužkrauti nereikalingos naštos [5 rekomendacija].*

Kelios organizacijos, tinklai, asociacijos ir projektai vienija specialistus ir įvairių kategorijų partnerius, kad būtų stiprinami ES teisėsaugos gebėjimai skaitmeninių tyrimų srityje:

- *Europos kriminalistikos institutų tinklas* (ENFSI)[20] yra pagrindinis Europos tinklas, apimantis (be kitų temų) skaitmeninę ekspertizę; jį sudaro 73 nariai iš 39 šalių, kurie dalyvauja darbo grupėse, pavyzdžiui, ekspertizės informacinių technologijų ir skaitmeninio vizualizavimo klausimais;

- *Europos kovos su kibernetiniais nusikaltimais technologijų plėtojimo asociacija* (EACTDA)[21] vienija teisėsaugos institucijas, mokslinių tyrimų ir technologijų organizacijas, pramonės partnerius ir akademinę bendruomenę iš daugelio valstybių narių, kad būtų sudarytos palankesnės sąlygos panaudoti saugumo srities mokslinių tyrimų projektų rezultatus ir pateikti visiškai išbandytas ir operacijoms parengtas programinės įrangos priemones, o ES viešojo saugumo organizacijos nepatirtų jokių išlaidų licencijoms ir turėtų prieigą prie pirminio kodo;

- Europos kovos su sukčiavimu tarnyba (OLAF) nuo 2007 m. nacionalinėms teisėsaugos institucijoms siūlo specialų *skaitmeninės ekspertizės ekspertų ir analitikų mokymą*, kuriame ypač daug dėmesio skiriama sukčiavimui, korupcijai ir kitai neteisėtai veiklai, kenkiančiai Europos Sąjungos finansiniams interesams; per metus mokymuose sudalyvauja apie 175 skaitmeninės ekspertizės ekspertai, taip sukuriama tvirta bendruomenė šioje kovos su nusikalstamumu srityje;

- kiti projektai, pavyzdžiui, *CYCLOPES*[22] ir *I-LEAD*[23], nėra nuolatinės struktūros, tačiau vis tiek suburia ekspertus ir atlieka atitinkamą trūkumų analizę.

Tačiau esami nuolatiniai tinklams nepavyksta suburti ES teisėsaugos institucijų skaitmeninės ekspertizės padalinių, taip pat glaudžiai su jais bendradarbiaujančių organizacijų (pavyzdžiui, Dublino universitetinio koledžo Kibernetinio saugumo ir kibernetinių nusikaltimų tyrimo centras arba Lietuvos kibernetinių nusikaltimų mokymo, mokslinių tyrimų ir švietimo kompetencijos centras).

---

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

Europolas (visų pirma Europolo inovacijų laboratorija kartu su Europos kovos su elektroniniu nusikalstamumu centru) jau tam tikru mastu bendradarbiauja su visais pirmiau išvardytais tinklais ir parodė, kad gali suburti daug specialistų, pavyzdžiui, suformuojant Europos inovacijų koordinavimo tarybos (EuCB) pagrindines grupes, organizuojant *Ekspertizės srities ekspertų forumą*[24] ir užmezgant ekspertų ryšius su atitinkamais partneriais, pavyzdžiui, per *Kibernetinių inovacijų forumą*[25].

Europolas taip pat siūlo jau parengtą infrastruktūrą – Europolo ekspertų platformą (EPE), kuri sudaro sąlygas ekspertams bendradarbiauti ir dalytis žiniomis konkrečiais klausimais.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina stiprinti Europolo skaitmeninės ekspertizės pajėgumus

Dalyviai: Europolas, Europos Komisija, valstybės narės,	*Laikas: 2028 m.*	*Biudžetas: bus aptarta vėliau, atsižvelgiant į vykstančių diskusijų dėl kitos DFP rezultatus*

- 2024–2029 m. Europos Komisijai skirtose politinėse gairėse paskelbus apie didelį Europolo stiprinimą, aukšto lygio grupės ekspertai ragina stiprinti Europolo gebėjimus padėti valstybėms narėms **sutelkti išteklius, žinias bei ekspertines žinias ir dalytis sprendimais bei skaitmeninėmis ekspertizės priemonėmis** esant pasitikėjimo atmosferai. Suverenios priemonės ir priemonės, naudojamos ir / arba sukurtos tik nacionalinio saugumo tikslais, neturėtų būti įtraukiamos į taikymo sritį.

- Aukšto lygio grupės ekspertai ragina Europolą **atlikti centro**, suteikiančio galimybę naudotis atitinkamomis operatyvinėmis ekspertinėmis žiniomis šioje srityje, **vaidmenį** ir galbūt **parengti į SIRIUS panašų projektą skaitmeninės ekspertizės srityje**, kad būtų sudarytos palankesnės sąlygos dalytis žiniomis ir ekspertinėmis žiniomis bei keistis geriausios praktikos pavyzdžiais.

- Aukšto lygio grupės ekspertai ragina Europolą sustiprinti savo vaidmenį **koordinuojant organizacijas ir projektus**, kuriais prisidedama prie žinių skaitmeninės ekspertizės srityje kūrimo ES lygmeniu, vadovaujant Europos inovacijų koordinavimo tarybai ir atsižvelgiant į kitų atitinkamų agentūrų indėlį.

[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

Esama keleto finansinių priemonių, skirtų skaitmeninės ekspertizės srities moksliniams tyrimams ir priemonių plėtrai remti.

- Pagal *Vidaus saugumo fondą (VSF)* Europos Komisija periodiškai skelbia atvirus kvietimus teikti pasiūlymus kibernetinių nusikaltimų ir skaitmeninių tyrimų srityje. Nepaisant gana riboto biudžeto (pagal dabartinę DFP šiems veiksmams skirta apie 15 mln. EUR), pagal šiuos kvietimus atrinkti projektai pasirodė esą tiksliniai ir sėkmingi.

  Maždaug du trečdaliai VSF biudžeto skiriami taikant pasidalijamąjį valdymą, o valstybės narės pasirenka, kuriuos projektus finansuoti, ir prisiima atsakomybę už kasdienį valdymą. Taigi valstybės narės turi galimybę remti skaitmeninės ekspertizės projektus pagal savo atitinkamas nacionalines programas.

- Programos „Europos horizontas“ veiksmų grupės „Civilinė visuomenės sauga“, kurios bendras septynerių metų biudžetas yra 1,596 mlrd. EUR, tikslas – skatinti saugią Europos visuomenę precedento neturinčių pokyčių ir didėjančios pasaulinės tarpusavio priklausomybės bei grėsmių kontekste, kartu stiprinant Europos laisvės ir teisingumo kultūrą. Pastaraisiais metais pagal ją buvo remiami keletas atitinkamų mokslinių tyrimų projektų, pavyzdžiui, FORMOBILE[26] ir EXFILES[27], kurie padėjo specialistams vykdyti kasdienę veiklą.

- *Skaitmeninės Europos programa* yra pagrindinė ES finansavimo priemonė, kuria siekiama stiprinti ES skaitmeninę infrastruktūrą įgyvendinant įvairias iniciatyvas. Pagal šią programą, kurios bendras 2021–2027 m. biudžetas yra 7,5 mlrd. EUR, skiriama daug išteklių būtent kibernetiniam saugumui ir ji taip pat apima skaitmeninę ekspertizę.

[26] FORMOBILE – „From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices“ („Nuo mobiliųjų telefonų iki teismo. Išsami ekspertizės tyrimų grandinė, kiek tai susiję su mobiliaisiais įrenginiais“): https://cordis.europa.eu/project/id/832800.

[27] EXFILES – „Europe fights against crime and terrorism“ („Europa kovoja su nusikalstamumu ir terorizmu“): https://exfiles.eu/.

Europolo iššifravimo platforma yra pavyzdinis VSF projektas. Ši platforma, kurią 2020 m. įsteigė Europolas, glaudžiai bendradarbiaudamas su Europos Komisijos Jungtiniu tyrimų centru (JRC), padeda nacionalinėms teisėsaugos institucijoms iššifruoti jų skaitmeninius įrodymus. Ja siekiama pateikti tvarų sprendimą teisėsaugos institucijoms, kad jos galėtų naudotis joms reikalingais techniniais ir IT ištekliais. Per pastaruosius kelerius metus platforma buvo naudojama daugeliu svarbių atvejų ir beveik pusė jų davė naudingų rezultatų, o tai lėmė keletą sėkmės istorijų. 2023 m. platforma sėkmingai padėjo atlikti 37 tyrimus (dėl vaikų seksualinio išnaudojimo, terorizmo, kibernetinių nusikaltimų, organizuoto nusikalstamumo, narkotikų kontrabandos ir sukčiavimo, taip pat didelio atgarsio sulaukusius finansinius tyrimus), įskaitant didelio prioriteto tyrimus, pavyzdžiui, susijusius su „SkyECC“ ir „Encrochat“. Platforma tapo itin svarbia teisėsaugos institucijoms skirta priemone, tačiau jos nepakanka visiems su iššifravimu susijusiems klausimams, su kuriais susiduria ES institucijos, spręsti.

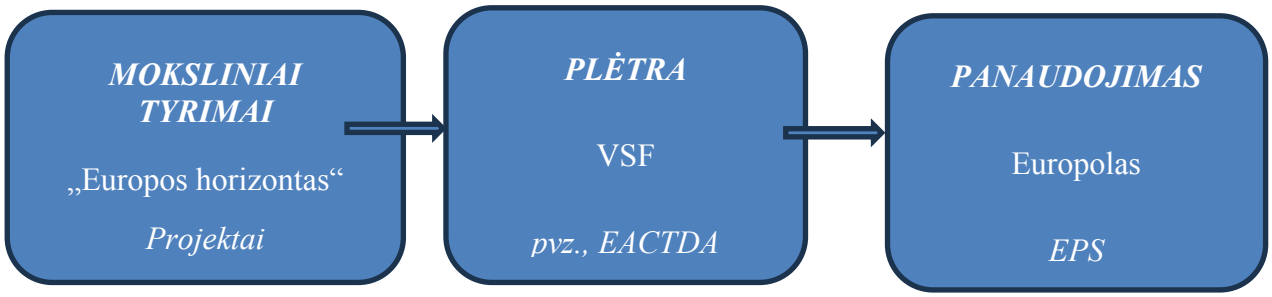
Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina toliau plėtoti ir skatinti ES iššifravimo pajėgumų naudojimą

Dalyviai: Europos Komisija, Europolas	*Laikas: 2028 m.*	*Biudžetas: nustatys valstybės narės (pvz., pagal VSF nacionalines programas)*

- Aukšto lygio grupės ekspertai ragina Europos Komisiją remti nacionalinių valdžios institucijų gebėjimą rinkti aukštos kokybės kontekstinę informaciją, kartu gerbiant išimtinę valstybių narių kompetenciją nacionalinio saugumo klausimais, skiriant specialų finansavimą (pavyzdžiui, pagal VSF nacionalines programas) ir keičiantis geriausia patirtimi, kad jos galėtų prisidėti prie Europolo iššifravimo platformos veiksmingumo didinimo.
- Aukšto lygio grupės ekspertai ragina Europos Komisiją remti Europolo investicijas į techninių pajėgumų išlaikymą ir iššifravimo pajėgumų stiprinimą, neatsiliekant nuo technologinės plėtros ir atsižvelgiant į kvantinės kriptografijos mokslinius tyrimus.
- Aukšto lygio grupės ekspertai ragina Europos Komisiją finansiškai remti valstybes nares plėtojant **nacionalinius ir regioninius iššifravimo pajėgumus**, kad būtų papildytos Europolo pastangos.

Pagal esamas ES finansavimo programas teikiama didelė parama teisėsaugai. Toliau racionalizavus šias galimybes būtų padidintas jų indėlis gerinant skaitmeninės ekspertizės padalinių pajėgumus ir mažinant susaistymą su pardavėju ir teisėsaugos kliovimąsi „juodosios dėžės“ priemonėmis (t. y. priemonėmis, kuriomis tvarkomi duomenys, o patikimos institucijos negali patikrinti, kaip jos veikia), sukurtomis už ES ribų.

Veiklos ciklo etapai (moksliniai tyrimai, plėtra, panaudojimas), kuriuos reikėtų įgyvendinti, kad teisėsaugos institucijoms būtų suteikta apčiuopiamos pridėtinės vertės, yra remiami įvairiomis schemomis. Kad būtų visapusiškai pasinaudota ES lygmeniu teikiamomis galimybėmis, nacionalinės administracijos, teisėsaugos institucijos ir specialistai turėtų žinoti kiekvienos konkrečios programos ir mechanizmo funkcijas ir tikslus.



Pagal programą „Europos horizontas“ buvo remiami įvairūs sėkmingi projektai, aktyviai dalyvaujant teisėsaugos specialistams. Tačiau programa „Europos horizontas“ yra mokslinių tyrimų programa, todėl reikėtų pakoreguoti lūkesčius, susijusius su tuo, per kiek laiko sukurtos priemonės būtų parengtos praktiniam naudojimui.

Projekto „*Tools4LEAs*“, finansuojamo VSF lėšomis ir administruojamo EACTGA, tikslas – palengvinti saugumo srities mokslinių tyrimų projektų rezultatų panaudojimą ir sukurti visiškai išbandytas ir operacijoms parengtas programinės įrangos priemones, nepatiriant jokių išlaidų licencijoms ir suteikiant ES viešojo saugumo organizacijoms prieigą prie pirminio kodo. Projektas „*Tools4LEAs*“ yra tinkamiausias siekiant remtis mokslinių tyrimų projektų rezultatais, kad būtų padedama įgyvendinti operatyvines priemones. Europolas dalyvauja projekte „*Tools4LEAs*“ ir, kartu su visais galutiniais naudotojais, kurie yra EACTGA nariai, vadovauja jo darbui.

Europos inovacijų koordinavimo taryba yra suformavusi daugiau kaip 15 valstybių narių pagrindinių grupių, kad galėtų kartu išnaudoti naujas technologijas ir kartu kurti novatoriškas priemones. Valstybės narės pasinaudojo Europos inovacijų koordinavimo tarybos pagrindinėmis grupėmis, kad koordinuotų dalį novatoriškų priemonių, finansuojamų VSF dotacijomis, pavyzdžiui, MARIT-D, „ProfID“ ir žiniatinklio dokumentų aptikimo programų, kūrimo. Pagrindinės grupės yra ideali sistema, kuria naudodamosi valstybės narės gali koordinuoti bendrą skaitmeninių tyrimo priemonių kūrimą.

Skelbdama tikslinius *kvietimus teikti pasiūlymus pagal VSF*, Europos Komisija toliau finansuoja projektus, kurie labai prisidėjo prie operatyvinių veiksmų sėkmės. Pavyzdžiui, vykdant projektą CERBERUS buvo nustatyti sistemos „EncroChat“ pažeidžiamumai, dėl kurių Prancūzijos žandarmerija, remiama Nyderlandų nacionalinio teismo ekspertizės instituto ir Dublino universitetinio koledžo, galės ją išardyti. Tuo tarpu projektas FRETOOL[28], kuriam vadovavo Dublino universitetinio koledžo Kibernetinio saugumo ir elektroninių nusikaltimų tyrimų centras, leido sukurti įvairias nemokamas kibernetinių nusikaltimų tyrimo priemones[29], pritaikytas konkretiems teisėsaugos reikalavimams atliekant skaitmeninius tyrimus ir analizę. Šios priemonės buvo parengtos bendradarbiaujant su teisėsaugos institucijomis ir jomis gali laisvai naudotis teisėsaugos bendruomenė. 3000 naudotojų iš daugiau kaip 100 teisėsaugos institucijų, esančių dešimtyse jurisdikcijų, užsiregistravo gauti prieigą prie priemonių, kurias taip pat organizaciniu lygmeniu patvirtino kelios teisėsaugos institucijos ir kurios yra naudojamos aukšto lygio tyrimuose. *Teisingumo programa* taip pat apima teisminį bendradarbiavimą baudžiamosiose bylose ir galėtų skatinti tarpvalstybinį bendradarbiavimą skaitmeninių tyrimo priemonių naudojimo srityje.

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

[29] Priemonės apima įvairius tyrimo etapus: atvirųjų šaltinių žvalgybos informacijos (OSINT) rinkimas prieš išankstinę paiešką; realiuoju laiku pateikiamų duomenų ekspertizę; atminties analizę; po paieškos gautą OSINT ir išteklių išsaugojimą internete; automatinę rinkmenų ir (arba) artefaktų paiešką; teismo ekspertizės ataskaitų teikimą; medijų apdorojimą ir artefaktų geolokaciją.

Nuo tada, kai buvo sukurta, *Europolo priemonių saugykla* (EPS) išsiplėtė ir apima daugiau kaip 40 pažangių priemonių, suteikiančių tiesioginę prieigą prie pažangiųjų Europos teisėsaugos technologijų. Kiekvieną mėnesį pridedama naujų priemonių ir saugykla tapo pagrindiniu šaltiniu ES specialistams, ieškantiems programinės įrangos, kuri padėtų jiems atlikti tyrimus. Šiuo metu EPS turi daugiau kaip 2 700 naudotojų, o įvairių jos priemonių buvo parsisiųsta daugiau kaip 7 800 kartų. Šias priemones plačiai naudoja nacionaliniai tyrimų padaliniai, atlikdami įvairias operacijas, be kita ko, įvairiose nusikalstamumo srityse, pavyzdžiui, prekybos žmonėmis, sunkių formų ir organizuoto nusikalstamumo, kibernetinių nusikaltimų ir seksualinės prievartos prieš vaikus internete srityse. EPS suteikia galimybę tiesiogiai pasinaudoti ES finansuojamais projektais, kurie duoda konkrečių ir brandžių rezultatai ir kurių kūrėjai nori suteikti Europolui licencijas juos naudoti, kad jie būtų platinami visoms Europos teisėsaugos institucijoms. Atrinkti partneriai iš INSPECTr, „Tools4LEAs“ ir FORMOBILE projektų jau pasidalijo priemonėmis Europolo priemonių saugykloje. Europolas koordinuoja veiklą su ES teisėsaugos mokymo agentūra (CEPOL), kad galėtų rengti naudotojų mokymus apie EPS priemones.

Be to, Skaitmeninės Europos programa turėtų vis labiau skatinti kibernetinio saugumo ir kovos su kibernetiniais nusikaltimais – jie dažnai grindžiami tomis pačiomis skaitmeninės ekspertizės priemonėmis ir metodais – sinergiją ir papildomumą.

Šiuo metu nėra mechanizmo, kuriuo būtų užtikrinama, kad skaitmeninės ekspertizės priemonės atitiktų atskaitomybės ir kriminalistikos standartus ES. Tokiu mechanizmu turėtų būti numatytas techninis vertinimas, kuriuo būtų užtikrinta, kad būtų visapusiškai laikomasi proporcingumo principo (t. y. pateikiami įrodymai, kad priemone suteikiama prieiga prie tikslinės informacijos, taip analizę apribojant tik tuo, kas būtina), skaidrumo principo ir kaltinamojo teisių (t. y. pateikiami įrodymai, kad naudojantis priemone yra gaunama autentiška ir tiksli informacija, taip leidžiant advokatams ir nepriklausomiems teismo ekspertizės ekspertams, liudijantiems teisme, jaustis užtikrintai) ir kitų teisinių reikalavimų (pvz., dėl atitikties DI aktui). Tai padidintų įrodymų patikimumą teisme nacionaliniu ir tarpvalstybiniu lygmenimis, taip sustiprinant tarpvalstybinį bendradarbiavimą.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina skirti tikslinį finansavimą skaitmeninių ekspertizės priemonių mokslinių tyrimų, kūrimo ir panaudojimo projektams

Dalyviai: Europos Komisija, Europolas, valstybės narės, EACTDA, ENFSI | *Laikas: nuo 2024 m.* | *Biudžetas:*

- Aukšto lygio grupės ekspertai ragina valstybes nares **integruoti skaitmeninės ekspertizės projektus, finansuojamus pagal jų atitinkamas VSF nacionalines programas, į esamus mechanizmus** (pvz., EMPACT) arba tinklus (pvz., ECTEG, EACTDA), kad būtų galima pasinaudoti kitų valstybių narių specialistų patirtimi ir kartu skatinti kitų teisėsaugos institucijų rezultatų sklaidą ir panaudojimą.

- Aukšto lygio grupės ekspertai palankiai vertina Europos Komisijos dedamas pastangas remti skaitmeninės ekspertizės priemonių mokslinius tyrimus, plėtrą ir diegimą skiriant finansavimą pagal atitinkamas finansines programas: **programą „Europos horizontas“, Skaitmeninės Europos programą** ir **VSF**. Atsižvelgdama į turimus išteklius, Europos Komisija kas dvejus metus pagal VSF skelbs **atvirus kvietimus teikti pasiūlymus** kibernetinių nusikaltimų ir skaitmeninių tyrimų srityje.

- Aukšto lygio grupės ekspertai palankiai vertina Europos Komisijos dedamas pastangas finansuoti **EACTGA** pagal VSF, kad EACTGA galėtų teikti ES viešojo saugumo organizacijoms visiškai išbandytas ir veiklai parengtas programinės įrangos priemones be išlaidų licencijoms ir prieigą prie pirminio kodo.

- Aukšto lygio grupės ekspertai palankiai vertina Europos Komisijos dedamas pastangas skatinti, atsižvelgiant į finansavimo galimybes, **Europolo priemonių saugyklos**, kaip pagrindinio priemonių sklaidos centro, naudojimą; jie ragina **Europolo inovacijų laboratoriją** toliau dėti pastangas, kad ES teisėsaugos institucijos galėtų naudotis patikimomis, saugiomis, nemokamomis, lengvai įdiegiamomis ir pritaikomo masto tyrimo priemonėmis.

- Aukšto lygio grupės ekspertai ragina toliau svarstyti galimybę ES lygmeniu **nustatyti** komercinių skaitmeninių ekspertizės priemonių **vertinimo ir, kai tinkama, sertifikavimo sistemas**. Tai gali būti daroma, pavyzdžiui, **per Europos kriminalistikos institutų tinklą**.

Skaitmeninių ekspertizės priemonių licencijos yra brangios ir kartais neįperkamos kai kurioms teisėsaugos institucijoms. Licencijas įsigyjant bendrai – jomis paskui gali dalytis skirtingų valstybių narių teisėsaugos institucijos – gali būti deramasi dėl mažesnių kainų.

Įgyvendinant projektą „*iProcureNet*“[30], finansuojamą pagal programą „Europos horizontas“, sukurta bendrų viešųjų pirkimų saugumo srityje metodika, taip pat sukurtas valstybių narių viešųjų pirkimų institucijų tinklas. *ES vidaus saugumo inovacijų centras, atsižvelgiant į jo* sudėtį ir darbo organizavimą, galėtų padėti valstybėms narėms apsibrėžti bendrus poreikius ir nustatyti, kurios priemonės būtų naudingiausios, jei būtų sukurta speciali skaitmeninės ekspertizės darbo kryptis.

Dažnai skaitmeninės ekspertizės priemonės kelia papildomų problemų, ne vien dėl savo kainos. Pavyzdžiui, šiomis priemonėmis gauti duomenys gali būti struktūrizuoti arba pateikti tokiu formatu, kuris netinka esamoms vidaus informacinėms sistemoms, naudojamoms tolesniam tvarkymui (pvz., duomenų analizei ar dalijimuisi jais). Todėl būtina suformuluoti bendrus valstybių narių reikalavimus, susijusius su duomenų, gautų naudojant skaitmenines ekspertizės priemones, struktūra ir formatu. Tuo remdamosi valstybių narių institucijos galėtų dalyvauti diskusijose su skaitmeninių ekspertizės priemonių teikėjais, kad būtų galima tinkamai atsižvelgti į jų reikalavimus, pavyzdžiui, vykdant bendras viešųjų pirkimų procedūras, kaip nurodyta pirmiau.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai pabrėžia, kad įsigyjant skaitmenines ekspertizės priemones reikia užtikrinti didesnį ekonominį naudingumą

Dalyviai: valstybės narės, Europos Komisija, ES vidaus saugumo inovacijų centras, Europolas	*Laikas: nuo 2025 m. (bendri viešieji pirkimai)*	*Biudžetas: nenurodyta*

- Aukšto lygio grupės ekspertai ragina Europos Komisiją:
  - padėti valstybėms narėms **nustatyti skaitmeninės ekspertizės priemones**, kurių labiausiai reikia veiksmingiems tyrimams atlikti (galbūt per ES vidaus saugumo inovacijų centrą);
  - remti „iProcureNet“ suburtą **operatyvinių padalinių ir viešųjų pirkimų institucijų kontaktinių punktų bendradarbiavimą**;
  - nustatyti **bandomuosius bendrus skaitmeninių ekspertizės priemonių licencijų pirkimus**.
- Aukšto lygio grupės ekspertai mano, kad **Europolas** gali padėti valstybėms narėms apibrėžti **bendrus reikalavimus dėl duomenų, gautų** naudojant skaitmenines ekspertizės priemones, **struktūros ir formato**, ir tuo remdamasis skatinti atitinkamų nacionalinių institucijų ir ekspertų bendradarbiavimą, kad būtų sudaryta galimybė jiems bendradarbiauti su tų priemonių rengėjais ir kūrėjais, kad jie galėtų susitarti dėl standartų ir būtų galima tinkamai atsižvelgti į valstybių narių reikalavimus.

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

II. Keitimasis pajėgumais ir dalijimasis jautriomis priemonėmis

Šiuo metu, atsižvelgiant į ribotus iššifravimo pajėgumus (pvz., Europolo iššifravimo platformą) ir tai, kad nėra veiksmingo bendradarbiavimo su pramonės sektoriumi arba specialios teisinės sistemos, kuria būtų užtikrinta teisėta prieiga prie informacijos skaitmeniniuose įrenginiuose, naudojimasis pažeidžiamumu siekiant gauti prieigą prie įrenginiuose esančių iššifravimo raktų tebėra pagrindinė teisėsaugos institucijoms likusi galimybė.

Net jei (kai kurios) šios sąlygos tam tikru mastu gali būti nustatytos, tikėtina, kad nusikaltėliai pasikliaus specialiais šifruotais įrenginiais informacijai ar neteisėtam turiniui nuslėpti. Todėl artimiausioje ateityje teisėsaugos institucijos ir toliau turės naudoti jautrias priemones[31] ir pajėgumus ir galbūt jais dalytis.

2 rekomendacijų grupė

Siekiant dalytis jautriomis priemonėmis ir užtikrinti atsakingą susijusių pajėgumų valdymą, ekspertai rekomenduoja:

1. *apsvarstyti galimybę sukurti mechanizmus, kuriais būtų užtikrinta, kad jautriomis priemonėmis būtų galima dalytis visapusiškai laikantis nacionalinių taisyklių [1 rekomendacija];*

2. *nustatyti keitimosi pajėgumais procesą; tai gali apimti naudojimąsi pažeidžiamumu, ir tai leistų sutelkti žinias ir išteklius, kartu užtikrinant, kad būtų laikomasi konfidencialumo ir informacijos neskelbtinumo nuostatų [6 rekomendacija];*

3. *galbūt būtų galima išnagrinėti, koks turėtų būti europinis požiūris į pažeidžiamumo valdymą ir atskleidimą, kuriuo užsiima teisėsauga, remiantis esama geroja praktika [2 rekomendacija].*

Pagal programą „Europos horizontas“ ir VSF Europos Komisija rėmė pažeidžiamumo ir programinės įrangos naudojimo aspektams skirtus projektus (*EXFILES* ir *FORRES*[32]), kuriais teisėsaugos specialistams suteiktos greito ir nuoseklaus duomenų išgavimo, kuris vis dėlto atitinka visas atitinkamas teisines nuostatas, priemonės ir protokolai.

---

31 „Jautrios priemonės“ apima tiek skaitmeninės ekspertizės, tiek taktines perėmimo priemones.

32 https://forres.eu.

Patikimiems europiniams partneriams dalijantis jautriomis priemonėmis ir susijusiais pajėgumais palengvinamas operatyvinis bendradarbiavimas, sudaromos sąlygos dalytis žiniomis ir sukuriama masto ekonomija, sumažinant būtinus išteklius.

Nors kartais naudojimasis pažeidžiamumu yra vis dar labai svarbus atliekant tyrimus, tai turi būti daroma itin atsargiai, laikantis atitinkamos nacionalinės teisinės sistemos, nes tai kenkia aparatinės ir programinės įrangos saugumo būklei.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina remti dalijimąsi jautriomis priemonėmis ir atsakingą susijusių pajėgumų valdymą

Dalyviai: Valstybės narės, Europos Komisija *Laikas: nuo 2024 m.* *Biudžetas: nenurodyta*

- Aukšto lygio grupės ekspertai prašo Europos Komisijos toliau remti projektus, skirtus dalijimuisi jautriomis priemonėmis (tiek skaitmeninės ekspertizės, tiek taktinio perėmimo priemonėmis) ir išteklių sutelkimui pagal atitinkamas finansavimo programas; Komisija taip pat galėtų remti **tarpvalstybinės žinių struktūrizavimo ir dalijimosi jomis platformos sukūrimą**.
- Aukšto lygio grupės ekspertai prašo Europos Komisijos JRC išnagrinėti galimybę nustatyti **Europos požiūrį dėl pažeidžiamumo valdymo ir atskleidimo**, kuriuos vykdo teisėsaugos institucijos, remiantis esama gerąja praktika.

III. Kolektyvinės investicijos, kuriomis siekiama ugdyti įgūdžius ir didinti ekspertines žinias skaitmeninės ekspertizės srityje

Atitinkami teisėsaugos darbuotojai turėtų būti mokomi naudoti jų tyrimuose taikomas tyrimo priemones ir metodus, o jų ekspertinės žinios turėtų būti sertifikuotos. Iš jų reikalaujama ir dokumentais pagrįsta kompetencija turėtų atspindėti jų vaidmenį ir apimti bent bendrąją mobiliųjų įrenginių skaitmeninę ekspertizę (nuo priemonės nepriklausomą), teisingumo sistemos / įrodymų temas ir pagrindinę informaciją apie įsigijimo, analizės, pranešimo ir atvykimo į teismą rūšis. Dokumentai turėtų atspindėti, ar ši kompetencija įgyta mokantis, ar dirbant.

3 rekomendacijų grupė

Siekdami remti įgūdžių ir ekspertinių žinių skaitmeninės ekspertizės srityje, įskaitant iššifravimą ir standartizavimą, plėtojimą, ekspertai rekomenduoja:

1. *didinti ekspertų mokymo galimybių skaičių [7 rekomendacija];*
2. *sukurti ES lygmens skaitmeninės ekspertizės ekspertų sertifikavimo sistemą, kad būtų užtikrinta teikiamų techninių mokymų kokybė ir vienodumas [7 rekomendacija];*
3. *investuoti, kad būtų užpildyta techninių standartizavimo įgūdžių spraga ir didinamas informuotumas, sudarant susitarimus su akademine bendruomene ir kitais atitinkamais institutais [8 rekomendacija].*

CEPOL rengia mokymo kursus keliomis svarbiomis temomis[33]. Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupė[34] rengia kursus apie kibernetinius nusikaltimus ir skaitmeninę ekspertizę ir suteikia galimybę juose nemokamai dalyvauti CEPOL ir nacionalinėms teisėsaugos institucijoms.

Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupė sukūrė „*Decrypt*“ – mokymo priemonę, skirtą ES valstybių narių teisėsaugos institucijų teisėtiems iššifravimo pajėgumams stiprinti taikant sudėtingas teisėto šifruotų įrodymų tvarkymo strategijas. CEPOL ir nacionaliniai padaliniai gali įdiegti „Decrypt“, naudodamiesi JTC teikiama infrastruktūra.

---

[33] Skaitmeninės ekspertizės srities tyrėjų mokymas, nešiojamųjų prietaisų ekspertizė, realiuoju laiku pateikiamų duomenų ekspertizė ir „Mac“ ekspertizė.

[34] Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupė yra ne pelno organizacija, vienijanti 30 teisėsaugos institucijų iš 20 Europos šalių, tarptautines organizacijas ir akademinę bendruomenę. Padedama VSF, Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupė kuria mokymo išteklius, sprendimus ir medžiagą, juos propaguoja ir jais dalijasi. Žr. https://www.ecteg.eu/.

Lygiai taip pat svarbu specialistams, kurie reaguoja pirmieji, suteikti pagrindinius skaitmeninės ekspertizės įgūdžius. Be kitų projektų, Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupė sukūrė „*eFirst*“ („Teisėsaugos specialistų, kurie reaguoja pirmieji, švietimas esminiais kibernetiniais klausimais“). „eFirst“ yra internetinis, savarankiško mokymosi mokymo modulis, skirtas vietoje dirbantiems (patruliavimas, nusikaltimo vieta, krata namuose) policijos pareigūnams arba tiems, kuriems pavesta priimti pirminį aukos skundą. Jis suteikia pagrindinių žinių apie kibernetinius nusikaltimus ir skaitmeninę ekspertizę. Juo taip pat galima remtis policijos akademijose rengiant kursus, kuriuose dalyvaujama fiziškai.

Ekspertų profilių sertifikavimas užtikrina, kad kiekvienas asmuo turėtų reikiamų žinių ir įgūdžių. Jis motyvuoja specialistus tobulinti įgūdžius ir nuolat atnaujinti žinias apie pokyčius savo srityje, taip pat padeda siekti karjeros ir asmeninio pripažinimo. Tai lemia kokybiškesnį ir tikslesnį darbą. Be to, asmeninis sertifikavimas gali:

- pateikti aiškų ir skaidrų skaitmeninės ekspertizės ekspertų įgūdžių ir kompetencijų aprašymą, kad specialistai ir skyrių vadovai galėtų nustatyti, ko jiems reikia siekiant patenkinti būtinus reikalavimus, kad galėtų veiksmingai vykdyti atitinkamas užduotis;

- palengvinti mokymo kursų rengimą ir vadovauti jų organizavimui nacionaliniu, regioniniu ir ES lygmenimis; palyginamu policijos mokymu visose ES valstybėse narėse užtikrinama, kad visi policijos pareigūnai turėtų prieigą prie vienodo lygio žinių ir įgūdžių, nepriklausomai nuo to, iš kurios šalies jie yra;

- prisidėti prie skaidresnio teismo proceso;

- padidinti tyrėjų ir kitų subjektų tarpusavio pasitikėjimą, taip sustiprinant tarptautinį nacionalinių teisėsaugos institucijų tarpusavio bendradarbiavimą.

CEPOL pradėjo kurti viešosios tvarkos palaikymo *sektorinę kvalifikacijų sistemą*, kurioje daugiausia dėmesio skiriama tarpvalstybiniam bendradarbiavimui. Šis modelis gali būti įgyvendinamas remiantis Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupės (ECTEG) atliktu darbu, susijusiu su skaitmeninės ekspertizės ekspertų sertifikavimu pagal jos vykdomą *Visuotinio sertifikavimo kibernetinių nusikaltimų srityje projektą*[35].

Tiek ECTEG, tiek EACTDA dalį savo išteklių investuoja į veiksmingo *atitinkamų teisėsaugos specialistų dalyvavimo standartizacijos procesuose* rėmimą, pavyzdžiui, palengvindamos būtinų įgūdžių įgijimą.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina gerinti techninius įgūdžius ir profilių sertifikavimą

Dalyviai: CEPOL, ECTEG	*Laikas: vykdomi veiksmai; skaitmeninės ekspertizės ekspertų sertifikavimo schema turi būti įgyvendinta iki 2026 m.*	*Biudžetas:*

- Aukšto lygio grupės ekspertai ragina CEPOL toliau **rengti** mokymo kursus (ypač instruktorių mokymo kursus).
- Aukšto lygio grupės ekspertai ragina ECTEG toliau **rengti, atnaujinti** mokymo kursus skaitmeninės ekspertizės klausimais, skirtus ekspertams ir specialistams, kurie reaguoja pirmieji, ypatingą dėmesį skiriant šifravimui, taip pat **rengti bandomuosius** mokymo kursus šiais klausimais.
- Aukšto lygio grupės ekspertai palankiai vertina Komisijos pastangas (skelbiant atvirus kvietimus teikti pasiūlymus pagal VSF) siekiant remti ECTEG, taip pat tai, kad **rengiami** mokymo kursai regioniniu lygmeniu.
- Aukšto lygio grupė ragina ECTEG toliau nagrinėti galimybę įdiegti skaitmeninės ekspertizės ekspertų sertifikavimo sistemą ES lygmeniu, o CEPOL – kuo labiau prisidėti prie šių pastangų, remiantis savo darbu, susijusiu su viešosios tvarkos palaikymo **sektorine kvalifikacijų sistema** ir **visuotiniu sertifikavimu kibernetinių nusikaltimų srityje**.
- Aukšto lygio grupė ragina ECTEG toliau sudaryti palankesnes sąlygas atitinkamiems specialistams įgyti su **standartizacijos procesais susijusių kompetencijų ir ekspertinių žinių**.

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

IV. Teisėtos prieigos palengvinimas

Nesant normų, reglamentuojančių integruotąją teisėtą prieigą, teisėsaugos institucijos turi vis dažniau pasinaudoti pažeidžiamumu, kad gautų prieigą prie konfiskuotų įrenginių, kuriuose informacija apsaugota šifravimu. Tačiau, nors taikant šį metodą galima paspartinti tyrimus, finansinės sąnaudos yra didelės. Todėl būtina apsvarstyti galimas alternatyvas.

4 rekomendacijų grupė

Siekiant sukurti bendradarbiavimo su atitinkamais pramonės partneriais mechanizmus ir išnagrinėti galimybę nustatyti privalomus standartus ir suderinti teisės aktus teisėtos prieigos srityje pagal Europos Sąjungos Teisingumo Teismo (ESTT) ir Europos Žmogaus Teisių Teismo jurisprudenciją, ekspertai rekomenduoja:

1. *sukurti platformą (SIRIUS ar lygiavertę), skirtą dalytis priemonėmis, geriausia praktika ir žiniomis apie tai, kaip produktų savininkai, gamintojai ir aparatinės įrangos gamintojai galėtų suteikti prieigą prie duomenų [11 rekomendacija];*

2. *sudaryti skaitmeninės aparatinės ir programinės įrangos gamintojų kontaktinių punktų ryšiams su teisėsauga žemėlapį [11 rekomendacija];*

3. *sudaryti išsamų galiojančių teisės aktų valstybėse narėse žemėlapį ir parengti tokių aktų ES vadovą, kad būtų išsamiai nurodyta skaitmeninės aparatinės ir programinės įrangos gamintojų teisinė atsakomybė vykdyti teisėsaugos institucijų prašymus pateikti duomenis, atsižvelgiant į konkrečius scenarijus ir reikalavimus, pagal kuriuos įmonės privalėtų prieiti prie įrenginių; [25 rekomendacija];*

4. *įsteigti tyrimų grupę, kad būtų įvertintos techninės galimybės dėl pareigų, kiek tai susiję su į skaitmeninius įrenginius įmontuota teisėta prieiga (be kita ko, prieiga prie šifruotų duomenų), kartu išlaikant įrenginių saugumą ir informacijos privatumą visų naudotojų atžvilgiu ir nekeliant tam pavojaus, taip pat nesusilpninant ryšių saugumo ir jam nepakenkiant [26 rekomendacija];*

5. *priklausomai nuo pirmiau minėto sudaryto žemėlapio, parengti privalomus pramonės standartus, taikomus ES rinkai pateiktiems įrenginiams, siekiant integruoti teisėtą prieigą, ir skatinti teisės aktų derinimą šioje srityje [25 rekomendacija].*

Dabartinis teisėsaugos bendradarbiavimas su pramone nepadeda pasiekti konkrečių rezultatų; reikia stiprinti bendradarbiavimą su pramone, kad būtų sukurti teisėsaugos institucijų teisėtos prieigos prie įrenginių ir taikomųjų programų būdai. Pavyzdžiui, stebėjimo vaizdo kameromis įrašų atveju teisėsaugos institucijos vis dažniau susiduria su šifruotomis rinkmenomis, kurių negalima analizuoti naudojant automatinę programinę įrangą, ypač kai tai susiję su daug vaizdo įrašų.

Teoriškai teisėsaugos institucijos gali prašyti įrenginių gamintojų pagalbos – jie savo ruožtu gali pateikti savo programinės įrangos pirminį kodą, kad būtų lengviau prieiti prie turinio duomenų, arba pateikti įrangos, su kuria susidurta atliekant nusikalstamų veikų tyrimus, techninius dokumentus.

Europolas turėtų geras galimybes rinkti geriausios praktikos pavyzdžius (pvz., įsteigti kontaktinius punktus ryšiams su teisėsauga) ir žinias apie tai, kaip produktų savininkai, gamintojai ir aparatinės įrangos gamintojai galėtų palengvinti prieigą, ir suteikti tas žinias ir galimybę susipažinti su tais pavyzdžiais visoms teisėsaugos institucijoms per SIRIUS (arba lygiavertę platformą).

Kartu reikėtų apsvarstyti skaidresnius sprendimus, kuriais suteikiama prieiga prie nešifruotų duomenų konfiskuotuose įrenginiuose, siekiant padidinti tyrimų veiksmingumą ir tuo pačiu metu užtikrinti vienodas sąlygas pramonės subjektams, kartu išsaugant kibernetinį saugumą ir apsaugant privatumą.

Remdamiesi išsamia teisėsaugos reikalavimų dėl teisėtos prieigos analize, ekspertai ragina Europos Komisiją parengti *technologijų veiksmų gaires*[36], kurios apimtų technologijų, kibernetinio saugumo, privatumo, standartizacijos ir saugumo ekspertų veiksmus ir užtikrintų tinkamą koordinavimą.

Pagrindinis veiksmas pagal šias technologijų veiksmų gaires būtų įvertinti *technines galimybes dėl pareigų, kiek tai susiję su teisėta prieiga, įmontuota* į skaitmenines rinkmenas ir įrenginius (be kita ko, prieiga prie šifruotų duomenų ir šifruotų AVSS įrašų)[37], kartu užtikrinant griežtas kibernetinio saugumo priemones ir nesusilpninant ryšių saugumo ar jam nepakenkiant. Šis vertinimas būtų atliekamas dalyvaujant visiems atitinkamiems suinteresuotiesiems subjektams.

---

[36] Ataskaitoje keliais atvejais ir keliuose skyriuose minimos vienodos „technologijų veiksmų gairės“.

[37] Žr. „Moving the Encryption Policy Conversation Forward“, Carnegie Endowment for International Peace (Toliau kalbėkime apie šifravimo politiką. Carnegie tarptautinės taikos fondas), https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

Tokiu mastu, kokiu atlikus tokį vertinimą būtų patvirtinta, kad esama pareigų dėl įmontuotos teisėtos prieigos, atitinkančių pirmiau nurodytas sąlygas, arba esama techninių galimybių tokias pareigas nustatyti, technologijų veiksmų gairėse taip pat turėtų būti apibrėžtas tvaraus ir ilgalaikio *bendradarbiavimo su standartizacijos institucijomis* procesas. Teisėsaugos dalyvavimą šiame standartizacijos procese galėtų koordinuoti Europolas, padedamas EACTDA.

Remiantis valstybių narių esamų teisinių sistemų, kuriomis nustatoma skaitmeninės aparatinės ir programinės įrangos gamintojų atsakomybė, susijusi su teisėsaugos institucijų prašymų pateikti duomenis vykdymu, žemėlapiu, būtų galima įvertinti *teisės aktų arba gairių ir rekomendacijų poreikį* [skatinant teisės aktų derinimą šioje srityje].

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina intensyvinti bendradarbiavimą su pramone, būsimose ES iniciatyvose remtis atitinkamais standartais ir suderinti teisėtos prieigos srities teisės aktus laikantis ESTT jurisprudencijos ir Europos Žmogaus Teisių Teismo praktikos.

Dalyviai: Europolas; Europos Komisija *Laikas: Nuo 2025 m.* *Biudžetas: nenurodyta*

- Aukšto lygio grupės ekspertai ragina **Europos Komisiją** parengti specialias **technologijų veiksmų gaires**, kad būtų išnagrinėtos teisėtos prieigos prie skaitmeninių įrenginių galimybės.
- Aukšto lygio grupės ekspertai ragina **Europolą** rinkti geriausios praktikos pavyzdžius ir žinias, susijusius su tuo, kaip produktų savininkai, gamintojai ir aparatinės įrangos gamintojai galėtų palengvinti prieigą, ir suteikti tas žinias ir galimybę susipažinti su tais pavyzdžiais visoms teisėsaugos institucijoms per **SIRIUS** (arba lygiavertę platformą).

II skyrius: Duomenų saugojimas

SU KOKIAIS SUNKUMAIS SUSIDURIAMA?

Anksčiau didžiausią surinktų įrodymų dalį sudarė daiktiniai įrodymai, o dabar didžiulį potencialių įrodymų kiekį saugo ryšių paslaugų teikėjai metaduomenų pavidalu. Nors skaitmeniniai duomenys nėra vieninteliai įrodymai, reikalingi atliekant nusikalstamų veikų tyrimus, šios rūšies įrodymai yra itin svarbūs – visų pirma siekiant nustatyti įtariamųjų arba tyrimui svarbių asmenų, kurie gali turėti svarbios informacijos, tapatybę – atliekant beveik visus tyrimus, nepriklausomai nuo to, ar jie susiję su nusikaltimais, įvykdytais fiziniame ar skaitmeniniame pasaulyje. Ypač kalbant apie skaitmeninį pasaulį, komunikacijos metaduomenys (visų pirma IP adresai ir prievado numeriai) dažnai gali būti vienintelis būdas nustatyti įtariamojo tapatybę[38].

Todėl tam, kad teisėsaugos institucijos galėtų tirti nusikaltimus skaitmeniniame amžiuje, būtina, kad skaitmeniniai įrodymai būtų pateikiami skaitomu formatu ir prireikus būtų prieinami tinkamai atsižvelgiant į tinkamas baudžiamojo proceso apsaugos priemones, procesines teises, privatumą ir duomenų apsaugą. Duomenys gali būti saugomi verslo tikslais (pvz., sąskaitų ir sąskaitų faktūrų išrašymas) arba teisėsaugos tikslais. Duomenų saugojimas gali padėti užtikrinti, kad duomenys būtų pasiekiami ir kompetentingos institucijos galėtų prie jų prieiti vykdydamos nusikalstamų veikų tyrimus ir baudžiamąjį persekiojimą. Paslaugų teikėjų saugomi duomenys gali būti itin svarbūs siekiant veiksmingai kovoti su nusikalstamumu, o tokių duomenų išsaugojimas yra būtina sąlyga siekiant sudaryti sąlygas tolesnei teisėsaugos institucijų prieigai ir užtikrinti, kad teisėsaugos institucijos galėtų vykdyti tyrimus[39]. Be to, laikantis E. privatumo direktyvoje[40] ir Bendrajame duomenų apsaugos reglamente (BDAR)[41] nustatyto duomenų kiekio mažinimo principo, paslaugų teikėjai srauto duomenis turėtų saugoti (arba kitaip tvarkyti) tik tol, kol tai būtina pačios komunikacijos, sąskaitų išrašymo tikslais arba, tam tikrais atvejais, ERP rinkodaros tikslais. Bet koks kitas saugojimas turi būti reglamentuojamas pagal teisinę sistemą, atitinkančią E. privatumo direktyvos 15 straipsnyje nustatytus reikalavimus. Šis režimas atspindi poreikį nustatyti pusiausvyrą tarp pagrindinių teisių į privatumą bei duomenų apsaugą ir teisėsaugos priemonių tikslais.

---

38 Ekspertai aptarė keletą pavyzdžių, parodančių skaitmeninių duomenų svarbą atliekant tyrimus, taip pat prašymų pateikti duomenis skaičių. Vieno eksperto teigimu, per pastaruosius penkerius metus visuose su terorizmu ar organizuotu nusikalstamumu susijusiuose tyrimuose buvo naudojami duomenys, kurių buvo paprašyta iš paslaugų teikėjų. 2023 m. vienoje valstybėje narėje ryšių operatorių buvo paprašyta baudžiamųjų procesų tikslais identifikuoti daugiau kaip 1 300 000 numerių; vėliau teismų sistema beveik visus tuos prašymus pripažino.

39 Šio dokumento tikslais prieiga prie duomenų suprantama kaip prieiga, suteikiama teisėsaugos institucijoms, prireikus gavus *ex ante* teismo leidimą, nusikalstamų veikų tyrimo tikslais ir atsižvelgiant į kiekvieną konkretų atvejį.

40 Direktyvos 2002/58/EB 6 straipsnis.

41 Reglamento (ES) 2016/679 5 straipsnio 1 dalies c punktas.

Šiuo metu joks ES teisės aktas nereglamentuoja duomenų saugojimo. 2014 m. ESTT panaikino ES duomenų saugojimo direktyvą[42], pabrėždamas didelius pagrindinių teisių į privatumą ir duomenų apsaugą apribojimus, atsirandančius, kai [paprastai ir nediferencijuojant] duomenys, kuriuos iš pradžių surinko paslaugų teikėjai, saugomi teisėsaugos tikslais[43]. Todėl nacionalinėse teisinėse sistemose įvyko pokyčių, dėl kurių visoje ES atsirado didelių skirtumų[44]: nors kai kurios valstybės narės vis dar taiko taisykles, pagal kurias ryšių pasaugų teikėjai turi pareigą saugoti tam tikrų kategorijų duomenis teisėsaugos tikslais, kitos valstybės narės yra įgyvendinusios pakeitimus, kad atitiktų teismų praktikoje pasiūlytą srauto duomenų tikslinio saugojimo kriterijų[45]; kitos, taip pat ir dėl vėlesnių nacionalinių teismų sprendimų, neturi specialių taisyklių dėl duomenų saugojimo teisėsaugos tikslais ir remiasi tik įmonių verslo tikslais saugomais duomenimis. Prieigos prie tokių duomenų sąlygos priklauso nuo taikomos nacionalinės teisinės sistemos ir nuo duomenų rūšies (abonento, srauto ar turinio duomenys). Dėl to, kad visoje ES nėra nustatyta pakankamai nuoseklių ir suderintų pareigų dėl duomenų saugojimo, valstybėse narėse skiriasi reikalavimai, kuriais reglamentuojamas paslaugų teikėjų vykdomas įvairių rūšių metaduomenų saugojimas (ir jo trukmė).

---

42 Direktyva 2006/24/EB. Direktyva ES valstybėms narėms buvo nustatyta pareiga priimti priemones, kuriomis būtų užtikrinta, kad elektroninių ryšių paslaugų ir tinklų teikėjai nuo šešių mėnesių iki dvejų metų saugotų srauto ir vietos nustatymo duomenis ir susijusius duomenis, būtinus abonentui ar registruotam naudotojui identifikuoti, kad kompetentingoms institucijoms būtų suteikta prieiga sunkių nusikaltimų tyrimo, nustatymo ir patraukimo už juos baudžiamojon atsakomybėn tikslais, kaip apibrėžta nacionalinės teisės aktuose.

43 Atitinkamos jurisprudencijos apžvalgą žr.: The future of national data retention obligations – How to apply Digital Rights Ireland at national level? (Nacionalinės duomenų saugojimo pareigos ateityje: kaip nacionaliniu lygmeniu taikyti sprendimą byloje *Digital Rights Ireland*?) – European Law Blog (Europos teisės tinklaraštis), V. Franssen; Recalibrating Data Retention in the EU - eucrim (Duomenų saugojimo perkalibravimas, ES, EUCRIM); Eurojusto / Europos teisminio kovos su kibernetiniais nusikaltimais tinklo 2024 m. ataskaita. The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU (Europos Sąjungos Teisingumo Teismo jurisprudencijos poveikis nacionaliniams duomenų saugojimo režimams ir teisminiam bendradarbiavimui ES); Cybercrime Judicial Monitor - Issue 6 (Kibernetinių nusikaltimų teisminės stebėsenos apžvalga Nr. 6); Cybercrime Judicial Monitor - Issue 9 (Kibernetinių nusikaltimų teisminės stebėsenos apžvalga Nr. 6);

44 Valstybės narės skirtingai reagavo į Duomenų saugojimo direktyvos panaikinimą ir nacionaliniu lygmeniu inicijuoti veiksmai padidino nacionalinių duomenų saugojimo sistemų įvairovę. Remiantis Eurojusto / Europos teisminio kovos su kibernetiniais nusikaltimais tinklo 2024 m. ataskaita dėl duomenų saugojimo, 2018–2022 m. laikotarpiu 12 šalių pakeitė savo teisės aktus. Respondentai atsakė, kad šiuos pakeitimus tiesiogiai lėmė ESTT bylos C-746/18, *Prokuratuur*, ir sujungtos bylos C-511/18, C-512/18 ir C-520/18, *La Quadrature du Net ir kt.* 23 iš 27 valstybių narių yra nustačiusios duomenų saugojimo taisykles; septynios valstybės narės jau yra nustačiusios tikslines duomenų saugojimo taisykles. Apžvalgą žr. Commission Study on the retention of electronic communications non-content data for law enforcement purposes (Komisijos tyrimas dėl elektroninių ryšių duomenų, nesusijusių su turiniu, saugojimo teisėsaugos tikslais), 2020 m., p. 39.

45 Teismas keliuose sprendimuose išplėtojo srauto ir vietos nustatymo duomenų tikslinio saugojimo sąvoką, nuspręsdamas, kad duomenų saugojimas gali būti suderinamas su ES teise, jei jis nustatomas remiantis konkrečiais siekiais ir konkrečiais tikslais. Tačiau praktiškai taikant Teisingumo Teismo pasiūlytus kriterijus tokiems tikslams nustatyti, kilo sunkumų ir iššūkių tų valstybių narių, kurios bandė tai padaryti, aukštuosiuose teismuose.

Tose valstybėse narėse, kurios nėra nustačiusios duomenų saugojimo pareigų, sunku arba kartais neįmanoma nustatyti įtariamojo arba asmens, kuris gali turėti svarbios informacijos (tyrimą dominančio asmens) nusikalstamų veikų tyrime, tapatybę[46]. Naujųjų e. įrodymų taisyklių, joms įsigaliojus, pridėtinė vertė padidėtų, jeigu jas papildytų duomenų saugojimo pareigos, nes priešingu atveju nėra garantijos, kad informacija, kuriai taikomi Europos duomenų saugojimo arba pateikimo orderiai (apimanti srauto duomenis, duomenis, kurių prašoma tik naudotojo tapatybei nustatyti, ir duomenis apie abonentą) bus prieinama.

Dabartinės aplinkybės daro poveikį tiek **teisėsaugai**, tiek **ryšių paslaugų teikėjams**, tačiau svarbiausia, kad jos daro **poveikį piliečiams ir aukoms**, kurių teisės kreiptis į teismą negalima užtikrinti, jei tyrimai pradedami tada, kai duomenys jau ištrinti arba nebuvo išsaugoti[47].

I. Atskirų valstybių narių jurisdikcijai priklausantys klausimai

Valstybėse narėse, **kuriose nėra** nustatyta **konkrečių pareigų**, susijusių su duomenų saugojimu teisėsaugos tikslais, tyrimai grindžiami, be visų kitų įrodymų, duomenimis, kuriuos bendrovės saugo savo verslo ir komerciniais tikslais. Komerciniams duomenims taikoma paslaugų teikėjų vidaus politika, pagal kurią bendrovės srauto duomenis saugo skirtingus laikotarpius (pvz., maždaug 6 mėnesius), o vietos nustatymo duomenys, kurie paprastai nėra svarbūs verslui, dažnai saugomi trumpiau. Dažnai mažos bendrovės apskritai nesaugo metaduomenų apie abonentus ar komunikacijos metaduomenų arba juos saugo labai trumpą laiką. Todėl tyrimus dažnai reikia atlikti labai skubiai, nes tyrėjai turi nustatyti duomenų teikėją ir perduoti prašymą pagal taikytinas taisykles prieš ištrinant duomenis, o tai kartais būna dienų ar valandų klausimas. Kai kuriais atvejais įmonės nepateikia informacijos apie konkrečius duomenis, kuriuos jos tvarko ir turi, todėl kompetentingoms institucijoms yra sunku pateikti tikslinius prašymus, kai jos siekia gauti duomenis. Kai kurie prieglobos paslaugų teikėjai leidžia naudotojams nuomotis serverio erdvę naudojantis fiktyviais duomenimis, o tai reiškia, kad net jei jie ir saugo naudotojų duomenis, jie nėra patikimi[48].

---

[46] Žr. pavyzdį, pateiktą: Background document 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 (Informacinis dokumentas. Operatyviniai iššūkiai, su kuriais susiduria teisėsauga, dėl prieigos prie duomenų. Indėlis į pirmąjį plenarinį Aukšto lygio grupės (ALG) posėdį prieigos prie duomenų veiksmingos teisėsaugos tikslais tema), p. 4.

[47] Poveikio piliečiams ir aukoms kontekste, žr. *Dwyer* v *Commissioner of An Garda Siochána* – [2020] IESC 4 (24/02/2020), visų pirma 9 punktą.

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

Daugumoje valstybių narių teisės aktai **dėl duomenų saugojimo yra nustatyti**. Tačiau, kaip aprašyta pirmiau, kai kurie nacionalinės teisės aktai buvo iš dalies pakeisti ESTT priėmus sprendimus, priimtus atsižvelgiant į DRD pripažinimą negaliojančia. Dėl to susidarė įvairi teisinė aplinka, kurioje valstybės narės skirtingai reaguoja į teismo sprendimus. Kai kuriose valstybėse narėse buvo dedamos pastangos įgyvendinti tikslinę duomenų saugojimo formą, kurią ESTT pasiūlė kaip galimą tolesnį duomenų saugojimo būdą. Tačiau Aukšto lygio grupės ekspertai pabrėžė, kad dėl tokių kriterijų įgyvendinimo kilo teisinių ir techninių problemų, susijusių su jų įgyvendinamumu[49], o paslaugų teikėjai pareiškė kritikos dėl išlaidų, susijusių su tikslinio saugojimo techniniu įgyvendinimu ir apskritai su dažnai keičiamų teisės aktų įgyvendinimu. Kita svarbi teisinė problema, su kuria susiduriama nacionaliniu lygmeniu, yra tai, kad daugeliu atvejų nacionalinės teisės aktai neapima OTT paslaugų. Konkretus OTT paslaugų atvejis bus išsamiau išnagrinėtas 1.3 skirsnyje.

II. Tarpvalstybiniai klausimai ES

Su duomenų saugojimu susijusių problemų kyla ir tarpvalstybinių prašymų atveju, t. y. kai kompetentinga institucija siekia gauti duomenų iš kitoje valstybėje narėje įsisteigusio paslaugų teikėjo. Tarpvalstybinių prašymų atvejais prašymą gaunančios šalies institucijos gali neturėti galimybės įvykdyti kitos šalies pateikto prašymo (nes nėra duomenų arba atitinkamų teisinių taisyklių).

Kadangi visoje ES nėra suderintų pareigų dėl metaduomenų saugojimo, teisėsaugos institucijoms vienoje valstybėje narėje kyla kliūčių **siekiant gauti** duomenis iš kitose valstybėse narėse įsisteigusių paslaugų teikėjų. Net jei duomenų saugojimo tvarka nacionaliniu lygmeniu yra taikoma, nacionalinės sistemos nėra suderintos, kiek tai susiję su saugojimo laikotarpiais, nes įvairiose valstybėse narėse tie laikotarpiai gerokai skiriasi[50].

---

[49] Nors ESTT pateikia tam tikrų gairių dėl srauto duomenų **tikslinio saugojimo** aiškinimo ir pateikia jo pavyzdžių, jurisprudencijoje gali būti tik nuorodų ir ji nėra pakankamai tiksli, kad būtų galima išsamiai apibrėžti galimus visų kategorijų duomenų saugojimo apribojimus. Todėl pastaraisiais metais Teisingumo Teismui buvo pateikti keli ieškiniai dėl duomenų saugojimo taisyklių, o valstybės narės negali užtikrinti teisinio tikrumo.

[50] Priklausomai nuo duomenų ir nusikaltimo rūšies, metaduomenys gali būti saugomi nuo 6 iki 72 mėnesių. Eurojusto / Europos teisminio kovos su kibernetiniais nusikaltimais tinklo 2024 m. ataskaitoje respondentai nurodė, kad buvo turima mažiau duomenų dėl saugomų duomenų trūkumo, nustatytų apribojimų dėl duomenų, kuriuos galima saugoti, kategorijų ir trumpų (-esnių) saugojimo laikotarpių. Todėl duomenų nebuvimas taip pat daro poveikį institucijų gebėjimui vykdyti Europos tyrimo orderius ir savitarpio teisinės pagalbos prašymus.

Be to, ES lygmeniu nėra suderinto požiūrio į **duomenų**, kuriuos reikia saugoti, **apibrėžtį**[51]. Nacionalinės teisės aktais paslaugų teikėjams gali būti nustatyta pareiga saugoti skirtingų kategorijų duomenis skirtingais tikslais (mokesčiai, auditas, teisėsauga). Teisės aktais taip pat nustatomas skirtingas išsamumo šiuo klausimu lygis: kai kuriuose teisės aktuose pateikiami išsamūs saugotinų su turiniu nesusijusių duomenų sąrašai, o kituose pateikiamos platesnės su turiniu nesusijusių duomenų apibrėžtys[52]. Priklausomai nuo siūlomos paslaugos ir verslo bei komercinių poreikių, paslaugų teikėjai taip pat saugo skirtingų rūšių duomenis skirtingos trukmės laikotarpius. Dėl to susidarė itin įvairi teisinė aplinka, kurioje esama didelių skirtumų ne tik tarp valstybių narių, bet ir tarp paslaugų.

Tokie skirtumai taip pat svarbūs atsižvelgiant į esamus valstybių narių skirtumus, kiek tai susiję ir su prieiga prie saugomų duomenų: kai kurios valstybės narės reikalauja teismo leidimo, siekiant prieigos prie kai kurių rūšių metaduomenų, o kitos tokio reikalavimo netaiko. Paslaugų teikėjai praneša, kad teisinis netikrumas dėl taisyklių, taikomų atskleidžiant duomenis, yra viena iš priežasčių, kodėl vėluojama ir nevykdomi teisėsaugos prašymai.

---

[51] Kaip nurodyta Komisijos tyrime dėl duomenų saugojimo, p. 48: „Nors tam tikrų rūšių informacija visose valstybėse narėse visada klasifikuojama kaip duomenys apie abonentą arba srauto duomenys, nesutariama dėl toliau nurodytų duomenų vienetų klasifikavimo: IP adresai, SIM numeriai, įrenginio identifikavimo numeriai (pvz., IMSI, IMEI) ir dinaminių IP adresų prievado numeriai. Kai kuriose valstybėse narėse (EE, FR, IE) šie duomenų vienetai klasifikuojami kaip duomenys apie abonentą, o kitose (DE, ES, IT, PL, SI) – kaip srauto duomenys.“

[52] Dėl apžvalgos apie duomenis, kurie saugomi kiekvienoje šalyje, žr. Komisijos tyrimo dėl duomenų saugojimo III priedą.

Kompetentingos institucijos turi laikytis ne tik nacionalinių taisyklių, taikomų paslaugų teikėjui, kuris turi prašomus duomenis, bet ir pačių paslaugų teikėjų nustatytų konkrečių reikalavimų. Kaip nurodyta 2022 m. SIRIUS metinėje ataskaitoje[53], paslaugų teikėjai gali reikalauti naudoti specialius portalus arba prašymus teikti naudojant konkrečius šablonus ar konkrečiomis kalbomis. Jie taip pat gali reikalauti suteikti informacijos apie bylos pobūdį, pateikti aiškią nuorodą į prašymo nacionalinį teisinį pagrindą arba nurodyti trumpus laikotarpius, dėl kurių prašoma pateikti duomenis. Nors kai kurie iš šių klausimų bus išspręsti iki 2026 m. įgyvendinus e. įrodymų dokumentų rinkinį, Aukšto lygio grupės ekspertai pabrėžė, kad reikia užtikrinti šių taisyklių ir bet kokios galimos suderintos duomenų saugojimo sistemos suderinamumą. Europos telekomunikacijų standartų institutas (ETSI) yra parengęs prašymų pateikti su numeriu siejamo asmenų tarpusavio ryšio paslaugų (tradicinių telekomunikacijų) metaduomenis formato standartus, tačiau paslaugų teikėjai valstybėse narėse juos taiko nenuosekliai. OTT[54] paslaugų teikėjų duomenų perdavimo teisėsaugos institucijoms standartai dar nebaigti ir nėra visiškai įgyvendinti. Be to, paslaugų teikėjai gali laisvai nuspręsti, kokia forma jie renka ir saugo naudotojų duomenis, todėl specialistai gauna neapdorotus duomenis labai skirtingomis formomis; dėl to susidaro didelė našta teisėsaugos institucijoms; joms būtų naudingi supaprastinti prašymų teikimo, atsakymų į prašymus ir duomenų siuntimo ir gavimo procesai, **komunikacijos sistemos ir formatai**. Standartizuotos komunikacijos sistemos ir formatai taip pat sumažintų įmonių prašymų tvarkymo išlaidas.

Kai teisėsaugos institucijos gauna teisėtą prieigą prie duomenų, jos turi turėti galimybę jais naudotis; todėl duomenys turi būti **įskaitomi**. Tačiau paslaugų teikėjai vis dažniau siūlo paslaugas, kurios leidžia srauto duomenis užšifruoti ištisiniu šifravimu, ir pateikdami šiuos duomenis teisėsaugos ir teisminėms institucijoms jų prašymu, dažnai juos pateikia šia šifruota forma.

Galiausiai kita pastebėta šios dabartinės padėties pasekmė yra susijusi su rizika, kad teisėsaugos institucijų **įrodymai bus ginčijami** teisme[55]. ESTT išaiškino, kad saugant duomenis gautų įrodymų

---

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

54 Šioje ataskaitoje virštinklinės (OTT) komunikacijos paslaugos – tai taikomosios programos ir paslaugos, kuriomis internetu teikiamos komunikacijos ir žiniasklaidos paslaugos (pvz., pranešimai, balso ir vaizdo skambučiai), nedalyvaujant ar nekontroliuojant tradiciniams telekomunikacijų paslaugų teikėjams (telekomunikacijų operatoriams). Žinomi OTT komunikacijos paslaugų pavyzdžiai yra žinučių siuntimo programėlės, kaip „WhatsApp“, „Telegram“, „Facebook Messenger“; balso ir vaizdo skambučių paslaugos, kaip „Skype“, „Zoom“, „Google Meet“, „Viber“; taip pat socialinės žiniasklaidos platformos, pavyzdžiui, „Instagram“ ir „Snapchat“ (žinučių siuntimas ir dalijimasis žiniasklaida).

55 Žr. 2024 m. Eurojusto/Europos teisminio kovos su kibernetiniais nusikaltimais tinklo 2024 m. ataskaitos skyrių „Collection and admissibility of evidence“ (Įrodymų rinkimas ir priimtinumas).

priimtinumo klausimas sprendžiamas pagal nacionalinę teisę[56], laikantis lygiavertiškumo ir veiksmingumo principų[57]; Todėl nacionalinių duomenų saugojimo tvarkos skirtumai gali turėti įtakos įrodymų priimtinumui tarpvalstybinėse bylose[58].

III. Su OTT ir kitais paslaugų teikėjais susiję klausimai

Nors pirmiau nurodyti klausimai susiję su visais ERP teikėjais, kalbant apie OTT paslaugų teikėjus teisėsaugos institucijoms kyla daugiau sunkumų dėl teisėtos prieigos prie duomenų. Tiek nacionaliniu, tiek ES lygmeniu OTT paslaugų teikėjai dažnai nemano, kad jiems taikomos tokios pačios pareigos kaip ir tradiciniams ryšių paslaugų teikėjams. OTT paslaugų teikėjai patenka į Europos elektroninių ryšių kodekso taikymo sritį, tačiau dėl to, kad jie dažnai įsisteigę už ES ribų, ir dėl to, kad nėra licencijavimo sistemų (t. y. jiems gali būti taikomi tik bendrieji leidimai) ir netaikomos sankcijos, susidaro netikrumas dėl jų pareigų saugoti duomenis, įskaitant konkrečių rūšių duomenis, ir sunku užtikrinti reikalavimų laikymąsi. Be to, tradiciniai ryšių paslaugų teikėjai daugeliu atvejų saugo kai kuriuos duomenis verslo tikslais ir dėl to galima nustatyti naudotojus (pvz., IP numerius su prievado numeriu ir laikotarpį), tačiau taip nėra **OTT paslaugų teikėjų** atveju – jie saugo tik su turiniu nesusijusius duomenis, kurių reikia jų komerciniams tikslams, kai kuriais atvejais tik trumpą laikotarpį[59]. OTT paslaugų teikėjai nesaugo jokių su turiniu nesusijusių duomenų, susietų su dinaminiu IP adresu (prievado numeris ir laikotarpis). Dėl to gali būti sunku ar net neįmanoma gauti komunikacijos, vykstančios tokiose vis dažniau naudojamose sistemose kaip „WhatsApp“ arba „Telegram“, metaduomenų. Kaip minėta, saugomų duomenų rūšys taip pat skiriasi priklausomai nuo siūlomos paslaugos. Kai kuriais atvejais teikėjai paskelbia gaires, kuriose aprašo savo saugomų duomenų rūšis[60], tačiau kitais atvejais OTT paslaugų teikėjai šios informacijos neatskleidžia. Dėl šios priežasties ir dėl to, kad nėra pakankamai **skaidrumo pareigų**, susijusių su duomenų, kuriuos paslaugų teikėjai generuoja, tvarko ir laiko verslo tikslais, rūšimis, teisėsaugos institucijoms dažnai kyla sunkumų, joms bandant nustatyti, ar duomenys buvo saugomi, kas turi kokių duomenų ir kokių rūšių duomenų rinkinių galima prašyti, taip pat siunčiant prašymus paslaugų teikėjams.

---

56 ESTT, 2020 m. spalio 6 d. Sprendimas *La Quadrature du Net ir kt.*, byla C-511/18, ECLI:EU:C:2020:791, 222–228 punktai; 2022 m. balandžio 5 d. Sprendimas *Commissioner of An Garda Síochána ir kiti*, byla C-140/20, ECLI:EU:C:2022:258, 127 punktas.

57 Ten pat, 223 punktas: „... su sąlyga, kad jos [tos taisyklės] nėra mažiau palankios nei taisyklės, reglamentuojančios panašias situacijas, kurioms taikoma vidaus teisė (lygiavertiškumo principas), ir kad dėl jų netampa praktiškai neįmanoma ar pernelyg sudėtinga pasinaudoti Sąjungos teisės suteiktomis teisėmis (veiksmingumo principas).“

58 Keliose teismo bylose buvo ginčijamas su turiniu nesusijusių duomenų, kaip įrodymų, priimtinumas. Santrauką žr. Komisijos tyrime dėl duomenų saugojimo, p. 41.

59 Tai ypač pasakytina apie smulkius paslaugų teikėjus. Remiantis Komisijos tyrimu dėl duomenų saugojimo, p. 103, IP adresai saugomi vidutiniškai 30 dienų.

60 Žr. pavyzdžiui, law-enforcement-guidelines-outside-us.pdf (apple.com) (Gairės teisėsaugos institucijoms už JAV ribų).

Tuo pat metu dėl to, kad paslaugų teikėjai gauna vis daugiau prašymų[61] ir kartu turi tvarkyti didelės apimties duomenų rinkinius, prašymai patenkinami vėliau arba atmetami[62]. Tokia padėtis susidarė ne tik dėl paslaugų teikėjų konkrečių sprendimų dėl verslo modelio, bet ir dėl **riboto skaičiaus mechanizmų**, skirtų teisėsaugos bei teisminių institucijų ir privačių bendrovių **bendradarbiavimui**.

Galiausiai, nors kai kurios besiformuojančios technologijos ir kiti skaitmeninės srities subjektai (pvz., automobilių gamintojai ir didžiaisiais kalbos modeliais grindžiamos DI sistemos) gali nepatekti į Europos elektroninių ryšių kodekse pateiktą ryšių paslaugų teikėjų apibrėžtį, jie generuoja ir tvarko komunikacijos metaduomenis, kurie gali suteikti informacijos apie nusikalstamą veiklą. Nepaisant didėjančios duomenų, kuriuos tvarko šie paslaugų teikėjai, apimties, šiuo metu duomenų saugojimo pareigos jiems netaikomos.

GALIMI SPRENDIMAI

I. Ryšio paslaugų teikėjų ir specialistų bendradarbiavimo stiprinimas

Tokiomis aplinkybėmis, kai skaitmeninių įrodymų rinkimui trukdo suderintų taisyklių trūkumas, teisėsaugos institucijos, atlikdamos tyrimus, dažnai turi remtis paslaugų teikėjų **savanorišku bendradarbiavimu**. Šis sprendimas padėjo atlikti tam tikrus didelio atgarsio tyrimus[63], tačiau jis yra susijęs su teisiniu netikrumu ir ne visada yra perspektyvus: savanoriškas bendradarbiavimas priklauso nuo paslaugų teikėjo tipo ir dydžio, maži tiekėjai dažnai saugo duomenis labai trumpą laiką, palyginti su didesniais, arba neturi išteklių, kad galėtų atsakyti į teisėsaugos institucijų prašymus[64].

---

[61] Remiantis 2023 m. SIRIUS metine ataskaita, paslaugų teikėjams adresuotų prašymų pateikti duomenis apimtis kasmet nuolat didėja (žr. p. 66 ir toliau).

[62] 2023 m. SIRIUS metinėje ataskaitoje (61 išnaša) apžvelgiamos pagrindinės vėlavimo patenkinti prašymus pateikti elektroninius įrodymus / tokių prašymų atmetimo priežastys (žr.p 68 ir toliau).

[63] Pavyzdžius žr. 2023 m. SIRIUS metinėje ataskaitoje (61 išnaša), p. 19.

[64] 2023 m. SIRIUS metinėje ataskaitoje, (61 išnaša), p. 79, nurodyta, kad didelis prašymų remiantis savanorišku bendradarbiavimu skaičius paslaugų teikėjams kelia sunkumų, ir rekomenduojama, kad jie dalyvautų SIRIUS tarptautiniuose renginiuose, kad „mažesni internetinių paslaugų teikėjai galėtų pasinaudoti projekto SIRIUS ekspertinėmis žiniomis bendradarbiavimo su valdžios institucijomis srityje ir geriau suprastų šį klausimą, struktūrizuotų savo reagavimo į valdžios institucijų prašymus politiką ir užsitikrintų pasirengimą būsimiems teisėkūros pokyčiams“.

Partnerystės ir bendradarbiavimas su sektoriaus atstovais turi būti grindžiami **aiškia teisine sistema**, kuri yra esminis bet kokio perspektyvaus sprendimo, kuris leistų teisėsaugos ir teisminėms institucijoms įveikti sunkumus siekiant teisėtos prieigos prie skaitmeninių įrodymų, komponentas. Svarbu ne tik užtikrinti, kad abi šalys vykdytų savo atitinkamas teisines pareigas, bet ir sukurti nuolatinius ir pasitikėjimu grindžiamus teisėsaugos specialistų ir paslaugų teikėjų santykius, kad jie suprastų vieni kitų poreikius ir galėtų kartu surasti veiksmingus sprendimus. Stabilūs **bendradarbiavimo** su privačiuoju sektoriumi **mechanizmai** yra būtini siekiant **padidinti skaidrumą**, kiek tai susiję su paslaugų teikėjų generuojamais ir saugomais duomenimis ir jų saugojimo trukme, taip pat užtikrinti **suderintą** saugotinų ir prieinamų **duomenų skirstymą į kategorijas**, sukurti **standartizuotus** prašymų pateikti duomenis **formatus** ir nustatyti **saugius** tiesioginio keitimosi duomenimis tarp kompetentingų institucijų ir paslaugų teikėjų **kanalus**.

Galima išnagrinėti keletą galimybių stiprinti tokį bendradarbiavimą; kai kurios iš jų būtų privalomo pobūdžio (įpareigojanti teisė), kitos – neįpareigojančios teisės sprendimai. Kai kurie šiame skirsnyje išvardyti sprendimai turėtų būti įvertinti II skirsnyje nurodyto poveikio vertinimo kontekste ir vėliau įtvirtinti teisės aktuose.

5 rekomendacijų grupė

Siekiant užtikrinti, kad kompetentingos institucijos galėtų siekti gauti atitinkamus duomenis nustatydamos reikiamų duomenų turėtojus, kad tokius prašymus paslaugų teikėjai gautų standartizuotais formatais ir kad tarpvalstybiniam bendradarbiavimui nekliudytų teisės kolizijos, ekspertai rekomenduoja:

1. *nustatyti ir stiprinti teisėsaugos specialistų ir paslaugų teikėjų bendradarbiavimą, siekiant remti keitimąsi informacija, gebėjimų stiprinimą ir mokymą, taip pat apibrėžti bendradarbiavimo principus ir sąlygas [13 rekomendacija], pavyzdžiui, sukuriant koordinavimo centrą, kad kompetentingos institucijos galėtų nustatyti atitinkamus paslaugų teikėjus ir geriau nukreipti teisėtus prašymus [18 rekomendacija]. Tai galima būtų atlikti:*

    a. *remiantis esamomis ES lygmens struktūromis, pavyzdžiui, SIRIUS, Europos teisminiu tinklu (ETT) / Europos teisminiu kovos su kibernetiniais nusikaltimais tinklu, ES interneto forumu;*

    b. *pagal susitarimo memorandumus, pasinaudojant kai kuriose valstybėse narėse nacionaliniu lygmeniu nustatyta geriausia praktika [14 rekomendacija];*

2. *skatinant laikytis elektroninių ryšių paslaugų ir kitų komunikacijos paslaugų teikėjams taikomų skaidrumo taisyklių dėl duomenų, kuriuos jie tvarko, generuoja ar saugo vykdydami savo veiklą, ir dėl teisėsaugos institucijų informavimo apie turimus duomenis, atsižvelgiant į apribojimus dėl tyrimų konfidencialumo, sudarant bendradarbiavimo susitarimus su paslaugų teikėjais arba prireikus nustatant privalomas pareigas [17 rekomendacija, 16 rekomendacija];*

3. *parengiant supaprastintus procesus ir formatus, grindžiamus sutartais prašymų teikimo paslaugų teikėjams ir atsakymų gavimo struktūrizuota forma standartais [15 rekomendacija] ir skatinant platformose paskirti bendrus kontaktinius punktus, kurie tvarkytų kompetentingų institucijų prašymus ir palaikytų ryšius su jomis [36 rekomendacija];*

4. *sukuriant mechanizmus, kuriais būtų užtikrinta, kad tarpvalstybiniai prašymai paslaugų teikėjams būtų teikiami veiksmingai ir kad būtų išvengta galimų konfliktų, remiantis e. įrodymų mechanizmais ir užtikrinant tokių mechanizmų suderinamumą su E. įrodymų reglamentu nustatytomis taisyklėmis [19 rekomendacija].*

Šiuo metu ES veikia struktūros, leidžiančios atitinkamiems subjektams susipažinti su priemonėmis ir geriausios praktikos pavyzdžiais. Projektas SIRIUS, apimantis teisėsaugos, teismines institucijas ir paslaugų teikėjus, galėtų palengvinti keitimąsi žiniomis ir priemonėmis, kiek tai susiję su prašymais pateikti paslaugų teikėjų turimus naudotojų duomenis[65], ir, ypač dėl SIRIUS bendrų kontaktinių punktų tinklo, galėtų tapti prašančiųjų institucijų ir paslaugų teikėjų tiesioginių kontaktų platforma[66]. SIRIUS galėtų būti **centrinė** teisinių priemonių, teismų praktikos, formatų ir t. t. **saugykla**, kaip šiuo metu yra tarpvalstybinio keitimosi e. įrodymais atveju[67].

Kaip esama valstybių narių, interneto pramonės ir kitų partnerių bendradarbiavimo aplinka, **ES interneto forumas**[68] galėtų tapti erdve, kurioje būtų galima ES lygmeniu užmegzti atitinkamų subjektų tiesioginius kontaktus ir puoselėti jų tarpusavio pasitikėjimą, kiek tai susiję su veikla prieigos prie skaitmeninių duomenų srityje. Šis forumas galėtų padėti sukuriant ir nuolat atnaujinant **atvirą** duomenų, kuriuos paslaugų teikėjai ir duomenų tvarkytojai renka ir tvarko, rūšių **katalogą**, kurį galėtų centralizuotai valdyti SIRIUS. Toks katalogas sumažintų dabartinį skaidrumo trūkumą ir suteiktų teisėsaugos ir teisminėms institucijoms daugiau aiškumo dėl to, kokių duomenų jos gali prašyti, taip pat veiktų kaip koordinavimo centras siekiant nustatyti, kam turėtų būti siunčiamas prašymas. Be to, jei paslaugų teikėjams būtų nustatytos teisinės pareigos, katalogas suteiktų pridėtinės vertės stebint ir vertinant skaidrumo pareigų įgyvendinimą, kiek tai susiję su duomenų, kuriuos paslaugų teikėjai saugo ar kitaip tvarko, rūšimis.

---

65 SIRIUS bendrų kontaktinių punktų tinklas, apjungiantis ekspertus teisėtų prašymų pateikti duomenis srityje, propaguoja geriausią praktiką ir skatina šalis įsteigti savo bendrus kontaktinius punktus. Bendri kontaktiniai punktai yra paskirti asmenys, padaliniai ar institucijos, kurie centralizuoja, peržiūri ir teikia vyriausybinių institucijų prašymus paslaugų teikėjams. Šiuo metu šiam tinklui priklauso 36 teisėsaugos institucijos iš 25 šalių.

66 Projektas SIRIUS atlieka svarbų vaidmenį, kai siekiama gauti elektroninius duomenis iš kitose jurisdikcijose įsisteigusių paslaugų teikėjų. SIRIUS yra ribotos prieigos platforma, skirta teisėsaugos ir teisminėms bendruomenėms dalytis žiniomis ir geriausios praktikos pavyzdžiais. Pagal projektą SIRIUS tvarkoma nuolat atnaujinama daugiau kaip 1 000 įmonių kontaktinių duomenų saugykla, kurioje daugiausia dėmesio skiriama mažesniems, sunkiai randamiems arba kartais neprieinamiems paslaugų teikėjams. Todėl kompetentingos institucijos per vieną operaciją gali gauti kelis adresus – tai padeda joms veiksmingiau tvarkyti didelį kiekį sudėtingos informacijos. SIRIUS project | Europol (europa.eu) (Projektas SIRIUS / Europolas (europa.eu)).

67 SIRIUS yra ES finansuojamas projektas, kuriuo padedama teisėsaugos ir teisminėms institucijoms susipažinti su tarpvalstybiniais elektroniniais įrodymais nusikalstamų veikų tyrimų ir procesų kontekste. Projektas SIRIUS, kurį bendrai įgyvendina Europolas ir Eurojustas, glaudžiai bendradarbiaudami su Europos teisminiu tinklu, yra centrinis informacinis punktas ES, skirtas keistis žiniomis apie tarpvalstybinę prieigą prie elektroninių įrodymų. SIRIUS project | Europol (europa.eu) (Projektas SIRIUS / Europolas (europa.eu)).

68 European Union Internet Forum (EUIF) - European Commission (europa.eu) (Europos Sąjungos interneto forumas (EUIF) – Europos Komisija (europa.eu)).

Pasinaudojant sinergija su e. įrodymų dokumentų rinkiniu būtų sutaupyta išlaidų ir išteklių ir būtų prisidėta prie visapusiško e. įrodymų teisės aktų įgyvendinimo. Pavyzdžiui, raginimas teisėsaugos institucijoms sukurti arba išplėsti padalinių, veikiančių kaip bendri kontaktiniai punktai dėl (tarpvalstybinių) prašymų atskleisti duomenis, pajėgumus galėtų būti taip pat taikomas prašymams, teikiamiems nacionaliniu lygmeniu, arba reikalavimui rengti tyrėjų ir specialistų, kurie reaguoja pirmieji, mokymo programas. Be to, tokios pat pastangos, kurios šiuo metu, įgyvendinant e. įrodymų dokumentų rinkinį, dedamos siekiant sukurti **skaitmeninę platformą**, kuri leistų kompetentingoms institucijoms ir paslaugų teikėjams tiesiogiai keistis informacija, galėtų būti dedamos ir komunikacijos metaduomenų, saugomų pagal nacionalinės teisės aktus, tikslu.

Valstybės narės galėtų apsvarstyti galimybę parengti **susitarimo memorandumus** kaip priemones, kuriomis būtų skatinamas paslaugų teikėjų, vyriausybių ir teisėsaugos institucijų bendradarbiavimas ir plėtojamas jų bendras supratimas, siekiant remti nacionalinių įstatymų veikimą. Kai kuriose valstybėse narėse turimi teigiami pavyzdžiai galėtų suteikti įkvepiančių idėjų, kaip tokius memorandumus struktūrizuoti įtraukiant visus susijusius subjektus (įmones, agentūras ir kt.), siekiant užtikrinti, kad būtų apimti visi svarbūs bendradarbiavimo aspektai (paslaugų teikėjams ir teisėsaugos institucijoms skirtų bendrų kontaktinių punktų skyrimas, techniniai poreikiai, bendras teiktinų duomenų kategorijų apibrėžimas, bendros procedūros, standartizuotų prašymo modelių rengimas, duomenų saugumas, duomenų kiekio mažinimo priemonės ir t. t.)[69]. Kaip jau nurodyta, paslaugų teikėjų (įskaitant OTT paslaugų teikėjus) vykdomam duomenų rinkimui ir kompetentingų institucijų prašymams pateikti duomenis skirti **standartizuoti protokolai** būtų naudingi tiek teisėsaugos institucijoms, tiek paslaugų teikėjams, ir jie galėtų sukurti automatizuotus rezultatų pateikimo mechanizmus, taip sumažinant išlaidas ir sutaupant laiko. Nors **nacionalinių** ir **tarpvalstybinių prašymų** (pagal e. įrodymų sistemą) reikalavimai skiriasi, vis dėlto būtų galima sukurti darbo srautus ir kanalus duomenims prašyti, nes standartizavimas yra siejamas su prašomų / gaunamų duomenų formatu. Tokius standartizuotus formatus geriausiai gali parengti tokios standartizacijos įstaigos kaip ETSI. Tačiau valstybių narių teisėsaugos ekspertų dalyvavimas šiuose procesuose lig šiol buvo ribotas. Todėl dabartinė **Vidaus saugumo srities standartizacijos klausimų Europos darbo grupė**, kuriai vadovauja Europolas ir Komisija, galėtų koordinuoti ir skatinti valstybių narių dalyvavimą tokiuose forumuose. Darbas galėtų būti grindžiamas esamais ETSI parengtais standartais, kurie galėtų būti išplėsti įtraukiant kitas duomenų kategorijas[70].

---

[69] 2024 m. balandžio 6 d. Airijos susitarimo memorandumu siekiama remti 2011 m. Ryšių (duomenų saugojimo) akto (su pakeitimais) veikimą. Teisingumo departamentas paskyrė nepriklausomą pirmininką, nustatė įgaliojimus ir pakvietė teisėsaugos institucijų bei paslaugų teikėjų atstovus.

[70] TS 102 657: saugomų duomenų tvarkymas; prašymams pateikti saugomus duomenis ir tokių duomenų teikimui skirta perdavimo sąsaja ir saugomų duomenų kategorijos (abonentas, naudojimas, įranga, tinklo elementas ir sąskaitų duomenys); TS 103 120: informacijos apie orderį sąsaja (apibrėžiama dviejų sistemų elektroninė sąsaja, skirta saugiam keitimuisi informacija, susijusia su teisėtai reikalaujamų veiksmų nustatymu ir valdymu; paprastai naudojama teisėtam duomenų perėmimui, tačiau gali būti naudojama saugomiems duomenims; paprastai naudojama tarp, iš vienos pusės, paslaugų teikėjo ir, iš kitos pusės, vyriausybės arba teisėsaugos institucijos, kuri turi teisę prašyti imtis teisėtų veiksmų); TS 103 705: teisėtam atskleidimui naudojamos duomenų struktūros (rengiama; tik duomenų struktūros, perdavimo sąsaja nenumatyta, iš anksto nustatyta medžio struktūra nenumatyta, paslaugų teikėjų apibrėžti tipai ir informacija).

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina skatinti paslaugų teikėjų, vyriausybės ir teisėsaugos institucijų bendradarbiavimą ir bendrą supratimą

Dalyviai: Europos Komisija, valstybės narės, Europolas (SIRIUS), Eurojustas, ES interneto forumas

Laikas: dar nepatvirtinta

- Aukšto lygio grupės ekspertai ragina **Europos Komisiją, Europolą** ir **valstybes nares** įvertinti būdus skatinti ir stiprinti teisėsaugos institucijų ir privačių įmonių bendradarbiavimą, puoselėjant nuolatinį dialogą ir abipusį supratimą apie veiklos, techninius ir verslo poreikius. II skirsnyje nurodyto poveikio vertinimo kontekste Aukšto lygio grupės ekspertai taip pat ragina Komisiją apsvarstyti galimybę parengti konkrečias pareigas, susijusias su duomenų rinkimo skaidrumu, ir sukurti nuolatinio bendradarbiavimo struktūras.

- Aukšto lygio grupės ekspertai prašo **Europos Komisijos**, **Europolo** ir **Eurojusto** kurti teisėsaugos institucijų ir teisminių institucijų, iš vienos pusės, ir ryšių paslaugų teikėjų, iš kitos pusės, keitimosi informacija platformas arba skatinti naudojimąsi esamomis tokiomis platformomis siekiant, kad būtų sudarytas duomenų, kuriuos ryšių paslaugų teikėjai ir duomenų tvarkytojai generuoja ir saugo vykdydami savo verslo veiklą, katalogas, kurio valdymą užtikrintų SIRIUS.

- Aukšto lygio grupės ekspertai prašo **valstybių narių** išnagrinėti galimybę sudaryti paslaugų teikėjus, vyriausybę ir teisėsaugos institucijas sutelkiančius bendradarbiavimo susitarimus ir (arba) susitarimo memorandumus, kad kartu nustačius principus ir standartinę praktiką būtų remiamas nacionalinių įstatymų veikimas.

- Aukšto lygio grupės ekspertai ragina **Europolą** ir **Europos Komisiją** pasinaudoti esama Vidaus saugumo srities standartizacijos klausimų darbo grupe siekiant skatinti valstybių narių dalyvavimą standartizacijos forumuose, kad būtų prisidedama prie atitinkamų standartų nustatymo ir bendrai rengiami protokolai, kuriais išsamiai nustatomos bendradarbiavimo su paslaugų teikėjais procedūros.

- Aukšto lygio grupės ekspertai prašo **Europos Komisijos**, **Europolo**, **Eurojusto / ETT** ir **valstybių narių** pasinaudoti sinergijomis su tokiomis priemonėmis kaip e. įrodymų aktų rinkinys, kad būtų sukurtos arba įsigytos atitinkamos priemonės, pavyzdžiui, išplečiant dar kuriamų skaitmeninių platformų naudojimą, kad jos veiktų kaip prašymų pateikimo portalai.

II. Būtiniausių taisyklių, susijusių su ryšių paslaugų teikėjų vykdomu metaduomenų saugojimu ir kompetentingų institucijų prieiga, suderinimas

Ekspertai iš esmės sutinka, kad reikalinga suderinta ES sistema, reglamentuojanti metaduomenų saugojimą teisėsaugos tikslais. Tokia sistema užtikrintų standartizuotus sprendimus, taip pat aiškias ir vykdytinas ryšių paslaugų teikėjų ir duomenų tvarkytojų pareigas, susijusias su tuo, kada ir kaip saugoti duomenis ir kokiomis aplinkybėmis suteikti prieigą prie tų duomenų. Šia sistema nustačius aiškias duomenų saugojimo ir prieigos taisykles, ji būtų naudinga užtikrinant aiškias pagrindinių teisių ir esminių interesų apsaugos priemones, atsižvelgiant į taikytinos teismų praktikos indikacijas, taip pat užtikrinant aiškumą, kiek tai susiję su ryšių paslaugų teikėjams taikomomis taisyklėmis dėl duomenų saugojimo ir dalijimosi jais teisėsaugos tikslais. Be to, tokia sistema užtikrinant, kad duomenys būtų saugomi, būtų remiamas visapusiškas e. įrodymų aktų rinkinio įgyvendinimas.

6 rekomendacijų grupė

Siekiant užtikrinti, kad nusikaltimų tyrimui ir baudžiamajam persekiojimui vykdyti reikalingi skaitmeniniai įrodymai būtų prieinami, kad tarp valstybių narių nebūtų susiskaidymo, kiek tai susiję su duomenų saugojimui taikomomis taisyklėmis ir apsaugos priemonėmis, susijusiomis su pagrindinėmis teisėmis, visų pirma privatumu ir duomenų apsauga, saviraiškos laisve ir kaltinamojo teisėmis, įskaitant teisę į tinkamą procesą, taip pat siekiant užtikrinti teisinį tikrumą tiek kompetentingoms institucijoms, tiek elektroninių ryšių ir kitų komunikacijų paslaugų teikėjams, ekspertai rekomenduoja:

1. *nustatyti metaduomenų kategorijas remiantis jų naudojimo tikslu (tyrimą dominančio subjekto internetinės veiklos, jos vykdymo vietos, vykdymo fakto nustatymas ar jos įvertinimas) [28 rekomendacija], siekiant užtikrinti, kad elektroninių ryšių paslaugų ir kitų ryšių paslaugų teikėjai saugotų tokius duomenis, kurių pakaktų bent jau subjektui identifikuoti [27 rekomendacija, v punktas];*
2. *nustatyti minimalius tokių duomenų saugojimo laikotarpius;*
3. *numatyti prieigos prie saugomų duomenų sąlygas [27 rekomendacija, iv punktas] sąlygas, kurios skirtųsi priklausomai nuo duomenų kategorijos, nusikaltimo kategorijos (pvz., nusikaltimų, kurie vykdomi tik internete, atvejais) arba grėsmės aukoms [29 rekomendacija];*
4. *numatyti tokias teisines, reguliavimo ir technines nuostatas, kad jomis būtų užtikrinta visapusiška pagarba subjektų pagrindinėms teisėms ir laisvėms ir kad bet koks tų teisių apribojimas būtų vykdomas tik kai būtina ir proporcinga [27 rekomendacija, vi punktas];*
5. *užtikrinti, kad tradiciniams ryšių paslaugų teikėjams, OTT paslaugų teikėjams ir bet kuriems kitiems esamiems ar būsimiems paslaugų teikėjams, generuojantiems ir tvarkantiems duomenis, būtų taikomos tos pačios taisyklės, pareigos ir apsaugos priemonės [27 rekomendacija, i ir ii punktai];*
6. *užtikrinti, kad komerciniais ir verslo tikslais saugomi naudotojų duomenys būtų veiksmingai prieinami teisėsaugos tikslais taikant atitinkamas apsaugos priemones (31 rekomendacija) ir kad kompetentingos institucijos galėtų skaityti teisėtai iš paslaugų teikėjų gautus duomenis [27 rekomendacija, iii punktas];*
7. *užtikrinti, kad valstybės narės galėtų užtikrinti duomenų saugojimo ir teikimo srityje nebendradarbiaujantiems elektroninių ir kitų ryšių paslaugų teikėjams skirtų sankcijų vykdymą, pvz., taikydamos administracines sankcijas arba apribodamos jų gebėjimą veikti ES rinkoje [30 rekomendacija].*

Kalbant apie **metaduomenų saugojimą**, įvairias duomenų kategorijas reikėtų traktuoti skirtingai: tyrimą dominančio subjekto tapatybei nustatyti reikalingus duomenis (duomenys apie abonentą[71] ir komunikacijos šaltinio [72] IP adresai) reikėtų atskirti nuo srauto[73] ir vietos nustatymo duomenų[74], o kiekvienai kategorijai numatyti skirtingus saugojimo laikotarpius ir apsaugos priemones. Be to, prieigos prie duomenų etape turi būti siekiama užtikrinti tam tikrą pusiausvyrą tarp tiriamo nusikaltimo sunkumo ir reikiamų imtis priemonių invazyvumo į asmeninį gyvenimą. Atsižvelgiant į naujausią jurisprudenciją[75], būtų galima išnagrinėti būtiniausius reikalavimus, skirtus įprastam duomenų, kurių pakaktų užtikrinti, kad bet kurio naudotojo tapatybę būtų galima aiškiai nustatyti, saugojimui. Srauto ir vietos nustatymo duomenų atveju reikia išnagrinėti galimybę taikyti papildomus ir griežtesnius kriterijus.

Siekiant sukurti tokią sistemą perspektyviausiu ir **technologiniu požiūriu neutraliausiu** būdu, saugotinų duomenų skirstymas į kategorijas turėtų būti grindžiamas į ateitį orientuotu metodu, apimančiu bendruosius duomenų rinkinius, formuojamus, pavyzdžiui, remiantis duomenų funkcijomis (duomenys, pagal kuriuos galima vienareikšmiškai nustatyti keitimosi duomenimis šaltinį arba paskirties vietą, duomenys, pagal kuriuos galima nustatyti keitimosi duomenimis šaltinio vietą ir kt.), ir esamų duomenų rūšių sąrašą (IP adresas, IMEI ir kt.). Ši sistema leistų tinkamai įvertinti kiekvienos duomenų kategorijos invazyvumą, taigi ir būtinas apsaugos priemones.

---

71 Su tam tikromis išimtimis, taikomomis mažų paslaugų teikėjų atveju, naudotojų duomenys paprastai jau saugomi verslo tikslais. Tokiu atveju, nedarant poveikio proporcingoms apsaugos priemonėms, tokie duomenys turėtų būti prieinami teisėsaugos institucijoms.

72 Pagal jurisprudenciją leidžiama bendrai ir nediferencijuotai saugoti duomenis, susijusius su elektroninių ryšių naudotojų civiline tapatybe, siekiant apsaugoti viešuosius interesus, taip pat bendrai ir nediferencijuotai saugoti IP adresus siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiais nusikaltimais ir užkirsti kelią didelėms grėsmėms visuomenės saugumui (2020 m. spalio 6 d. Sprendimas *La Quadrature du Net ir kt.*, sujungtos bylos C-511/18, C-512/18 ir C-520/18 ir 2024 m. balandžio 30 d. Sprendimas *La Quadrature du Net ir kt.*, C-470/21 (*Hadopi*), ECLI:EU:C:2024:370).

73 „Srauto duomenys“ – tai duomenys, tvarkomi pranešimui perduoti elektroninių ryšių tinklu, taip pat sąskaitoms už tokį perdavimą pateikti (Direktyvos 2002/58/EB 2 straipsnis).

74 „Vietos nustatymo duomenys“ – elektroninių ryšių tinkluose tvarkomi duomenys, nurodantys viešosios elektroninių ryšių paslaugos gavėjo galinių įrenginių geografinę padėtį (Direktyvos 2002/58/EB 2 straipsnis); naudotojo įrangos vietos nustatymo duomenys turėtų būti laikomi vietos nustatymo duomenimis, nesudarančiais srauto duomenų, kaip apibrėžta Direktyvos 2002/58/EB 9 straipsnyje.

75 Sprendimas *Hadopi*.

Kaip postuluojama ekspertų ir pastarojo meto jurisprudencijoje[76], pareigos saugoti duomenis derinimas su griežtais **reikalavimais dėl prieigos prie duomenų** papildomai užtikrintų pagrindines teises, visų pirma privatumą ir duomenų apsaugą. Todėl Aukšto lygio grupės ekspertai svarstė poreikį parengti prieigos taisykles, kurios būtų skirtingos priklausomai nuo, pvz., nusikaltimo rūšies ir sunkumo, nusikaltimo grėsmės aukoms laipsnio, prieigos prie duomenų tikslo ir institucijų, kurios turi kompetenciją prieiti prie duomenų. Buvo nuspręsta, kad toks metodas taip pat yra naudingas nustatant specialias taisykles dėl nusikaltimų, kuriuos ypač sunku tirti, pavyzdžiui, tik internete įvykdytų nusikaltimų, kai skaitmeniniai įrodymai yra vieninteliai turimi įrodymai, tyrimo ir baudžiamojo persekiojimo už juos.

Gavus teisėtą prieigą prie duomenų, prašančiosios institucijos turi galėti juos skaityti. Todėl reikia, kad paslaugų teikėjai duomenis teiktų **suprantamu formatu**. Dažnai paslaugų teikėjai siūlo srauto duomenų ir duomenų apie abonentą ištisinio šifravimo paslaugas[77] ir šių duomenų neiššifruoja, kai jais dalijasi su kompetentingomis institucijomis. Aukšto lygio grupės ekspertai laikėsi nuomonės, kad duomenų saugojimo tvarka turėtų apimti paslaugų teikėjų pareigas pateikti nešifruotus duomenis, kartu užtikrinant tvirtą kibernetinį saugumą ir visapusišką atitiktį duomenų apsaugos bei privatumo teisės aktams ir nepakenkiant šifravimo technologijoms.

Reikės, kad bet kuriems ERP teikiantiems ekonominės veiklos vykdytojams (esamiems ar būsimiems) būtų taikytini minimalieji konkrečių kategorijų duomenų saugojimo reikalavimai (ir kad jie būtų vykdytini), kad duomenų saugojimo sistema būtų veiksminga ir dabar, ir ateityje. Siekiant atsižvelgti į būsimus technologinius pokyčius, subjektai, kuriems taikomos duomenų saugojimo pareigos, turėtų apimti telekomunikacijų paslaugų teikėjus, OTT paslaugų teikėjus ir kitus operatorius, kurie renka su konkrečiais jų paslaugą naudojančiais fiziniais ar juridiniais asmenimis susijusius duomenis, pavyzdžiui, automobilių gamintojus arba didžiųjų kalbos modelių (LLM) DI sistemas. Šios pareigos turi būti vykdytinos, o paslaugų teikėjai turi būti atskaitingi; tai būtų galima pasiekti taikant įvairius sprendimus, kurie galėtų apimti kliūtis patekti į rinką (veiklos licencijos) ir administracines sankcijas.

---

[76] Neseniai nagrinėtoje byloje *Hadopi* Teisingumo Teismas padarė išvadą, kad privatumas gali būti užtikrintas derinant saugojimą ir prieigą

[77] Žr. I skirsnį.

Esminis bet kokios būsimos ES sistemos aspektas yra vykdytinų sankcijų nebendradarbiaujantiems paslaugų teikėjams ir paslaugų teikėjams, teikiantiems prieglobos paslaugas neteisėtoms paslaugoms, sistema. Atsižvelgiant į šio konkretaus aspekto ir teisėto duomenų perėmimo kontekste aptariamų galimų sprendimų sąveiką, sankcijos turi būti aptartos kitame posėdyje, skirtame teisėto duomenų perėmimo klausimams.

Nors daugumos paslaugų teikėjų atveju pareigos saugoti ir teikti duomenis pareikalautų daugiausia techninio įgyvendinimo (t. y. suteikti galimybę kompetentingoms institucijoms susipažinti su verslo tikslais surinktais arba tvarkomais duomenimis), tai reikštų, kad naudotojų registravimo procedūros standartiškai būtų pradėtos taikyti tokiems paslaugų teikėjams, kurie šiuo metu neregistruoja savo naudotojų, nes verslo požiūriu jie neturi poreikio tai daryti (pvz., OTT paslaugų teikėjams). Diskusijose dėl poreikio didinti paslaugų teikėjų **skaidrumą ir atskaitomybę**, kiek tai susiję su jų renkamais ir saugomais duomenimis ir tų duomenų saugojimo trukme, Aukšto lygio grupės ekspertai laikėsi nuomonės, kad tokio pobūdžio pareigos yra konstruktyvios. Pagal kitas priemones (BDAR) nustatytos esamos pareigos dėl skirstymo į kategorijas gali suteikti įžvalgų apie šių paslaugų teikėjų tvarkomus duomenis.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina sukurti naują ES duomenų saugojimo ir prieigos prie jų sistemą

Dalyviai: Europos Komisija, Taryba, Europos Parlamentas

Laikas: 2025–2026 m.

- Aukšto lygio grupės ekspertai ragina **Europos Komisiją** pradėti poveikio vertinimo procesą, kad būtų įvertintos įvairios galimybės stiprinti kompetentingų institucijų gebėjimus veiksmingai tirti nusikaltimus ir vykdyti baudžiamąjį persekiojimą už juos pasinaudojant prieiga prie ryšių paslaugų teikėjų sugeneruotų ir saugomų retrospektyvinių metaduomenų. Poveikio vertinimas taip pat turėtų apimti subsidiarumo reikalavimus, poveikį pagrindinėms teisėms ir vidaus rinkai, taip pat sąsajas su kitomis galiojančiomis teisinėmis priemonėmis. Juo turėtų būti grindžiamas pasiūlymas dėl teisėkūros procedūra priimamo akto, kuris būtų priimtas pagal įprastą teisėkūros procedūrą.

III skyrius. Teisėtas duomenų perėmimas

SU KOKIAIS SUNKUMAIS SUSIDURIAMA?

„Teisėtas ryšio duomenų perėmimas“ – trečiosios šalies – institucijos ar kito subjekto, turinčių įstatymu arba juo remiantis suteiktus įgaliojimus, – įgyjama slapta prieiga prie duomenų, kai komunikacija kelia įtarimų. Nors praeityje teisėtas duomenų perėmimas daugiausia buvo aktualus telefono skambučiams, vis didėjantis poslinkis nuo tradicinių balso skambučių prie pranešimų siuntimo paslaugų ir kitų elektroninių ryšių formų sukėlė naujų iššūkių.

Europos elektroninių ryšių kodekse šis poslinkis yra pripažintas, ir dalis tradicinėms telekomunikacijų paslaugoms taikomos teisinės sistemos yra taikoma ir įmonėms, kurios per joms nepriklausančią ar jų nevaldomą telekomunikacijų infrastruktūrą teikia internetines paslaugas, įskaitant su numeriu nesiejamo asmenų tarpusavio ryšio paslaugas. Praktiškai tai reiškia, kad su numeriu nesiejamo asmenų tarpusavio ryšio paslaugų teikėjams potencialiai gali būti taikoma ta pati teisinė sistema, kuri yra taikoma tradiciniams telekomunikacijų operatoriams, įskaitant nuostatas dėl teisėto duomenų perėmimo. Vadovaudamosi Reglamentu (ES) 2016/679 ir Direktyva 2002/58/EB, kuriuose išdėstytos nuostatos dėl ryšių konfidencialumo ir jų išimtys, valstybės narės gali reikalauti, kad operatoriai leistų nacionalinėms kompetentingoms institucijoms vykdyti teisėtą elektroninių ryšių duomenų perėmimą. Pagal Europos elektroninių ryšių kodekse nustatytą bendrojo leidimo tvarką valstybės narės gali iš naujo nustatyti šį reikalavimą.

Teisėta prieiga nebūtinai turi būti teikiama tinklo lygmeniu, kaip tai įprasta tradicinių telefono skambučių ir tekstinių pranešimų (SMS) atveju; ji taip pat gali būti teikiama naudotojo įrenginio (prieš informacijos siuntimą) arba paskirties vietos (pvz., kai pranešimai išsaugomi debesijoje) lygmeniu. Šios ataskaitos kontekste teisėtas duomenų perėmimas apima šiuos tris naudojimo atvejus ir aprėpia duomenis, prie kurių gaunama tikralaikė prieiga arba prieiga šiek tiek vėluojant.

Svarbu atskirti **ryšių operatorių diegiamas** duomenų perėmimo technologijas ir technologijas, kurias teisėsaugos institucijos gali įdiegti savarankiškai. Į ETSI standartuose nurodomą „teisėto duomenų perėmimo“ apibrėžtį įeina tik pirmesnės iš nurodytų technologijų [šioje ataskaitoje įvardijamos kaip „**operatoriaus vykdomas duomenų perėmimas**“]; šių technologijų kontekste ryšių operatorius turi įdiegti technines sistemas, skirtas perimamiems duomenims surinkti ir pateikti prašančiosioms institucijoms. Paskesnės iš nurodytų technologijų [šioje ataskaitoje įvardijamos kaip „**taktinis duomenų perėmimas**“] yra siejamos su priemonėmis, kurių nereikia visam laikui fiziškai įdiegti tinkle, pavyzdžiui, IMSI gaudyklėmis[78] arba programine įranga, skirta duomenims perimti išmaniuosiuose telefonuose. Tie naudojimo atvejai suponuoja skirtingą invazyvumą ir skirtingo pobūdžio iššūkius ir jiems netaikoma ta pati teisinė tvarka.

Nors teisėtas duomenų, perduodamų naudojantis tradicinėmis telekomunikacijų paslaugomis, perėmimas tebėra svarbi daugelio tyrimų priemonė[79], šios priemonės veiksmingumas labai sumažėjo, nes šiuo metu telekomunikacijų paslaugas daugiausia teikia kiti subjektai: remiantis įvairiais šaltiniais, apie 97 % visų mobiliųjų žinučių dabar siunčiama naudojant tokias žinučių siuntimo programėles kaip „WhatsApp“, „Facebook Messenger“ ir „WeChat“, o tradicinės SMS ir MMS žinutės sudaro tik apie 3 % žinučių. Be to, 2023 m. daugiau kaip 90 % OTT komunikacijos vyko pasitelkiant ištisinio šifravimo paslaugas[80].

Ekspertai sutaria, kad esama šių tendencijų: pirma, nusikaltėliai pradėjo pereiti nuo tradicinių ryšių operatorių prie įprastomis tapusių OTT paslaugų, vėliau vis daugiau nusikaltėlių pradėjo naudotis specialiais nusikaltėlių tinklais (pvz., „EncroChat“ ir „Sky ECC“), o nuo 2020 m., kai buvo išardyti pagrindiniai šifruojamų nusikalstamų ryšių tinklai, daugelis jų nusprendė grįžti prie įprastų ištisinio šifravimo OTT paslaugų.

---

78 IMSI gaudyklės yra sekimo įrenginiai, kurie imituoja judriojo ryšio bokštus ir taip perima judriojo telefono ryšio signalus, fiksuodami tarptautinio judriojo ryšio abonento identifikatoriaus (IMSI) numerius ir ryšio duomenis.

79 Pastaraisiais metais Europoje stebimas reikšmingas ir pastovus teisėto duomenų perėmimo prašymų skaičiaus didėjimas. Prašymų ypač padaugėjo tokiose šalyse kaip Vokietija, Prancūzija ir Jungtinė Karalystė; vien tik Vokietijoje prašymų padaugėjo pastebimai. Pavyzdžiui, „Deutsche Telekom“ pranešė 2023 m. gavusi daugiau kaip 31 000 prašymų perimti duomenis, palyginti su maždaug 26 000 prašymų 2022 m. (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Šaltiniai: *Comparitech* ir *Statista*.

Esant tokioms aplinkybėms, ryšių paslaugų teikėjai susiduria su tokiais dideliais reagavimo į teisėto duomenų perėmimo prašymus iššūkiais, kad jie vos įvykdo bazinius teisėto duomenų perėmimo reikalavimus, apibrėžtus Budapešto konvencijoje dėl elektroninių nusikaltimų[81]. Todėl tradicinio teisėto duomenų perėmimo operatyvinė vertė dažnai apsiriboja taktinėmis įžvalgomis, pavyzdžiui, nustatoma, ar įrenginys yra įjungtas ar išjungtas, kur yra tinklo antena arba kas su kuo yra sujungtas; vis dėlto teisėtas turinio duomenų, perduodamų per OTT paslaugų teikėjus, perėmimas dažniausiai yra neįmanomas.

Todėl teisėsaugos institucijos dažnai negali turėti prieigos prie tyrimą dominančių ryšio duomenų turinio ir jį matyti[82] arba net suprasti, kas naudojasi tam tikra interneto paslauga realiuoju laiku, ir išsifiltruoti aktualią informaciją. Šis didelis prieigos prie perduodamų duomenų praradimas tyrimus paveikia šiais keliais būdais:

- kyla didelių sunkumų, susijusių su nusikaltimų prevencija, nusikalstamų organizacijų buvimo vietos nustatymu ir nusikalstamų veikų, padarytų internete ar realiame gyvenime, priskyrimu;

- teisėsaugos institucijos dažniau naudoja vadinamuosius specialiuosius metodus[83], kurie dažnai yra labiau invazyvūs ir kur kas pavojingesni pareigūnams, pavyzdžiui, kai teisminė institucija nurodo įrengti kameras ar mikrofonus šalia tyrimą dominančio subjekto;

- teisėsaugos institucijos dažniau naudoja mažiau tikslinius tyrimo metodus: neturėdami prieigos prie komunikacijos turinio ar tikslių geografinės vietos nustatymo duomenų, tyrėjai dažnai turi ištirti **visus** asmenis, susijusius su asmeniu, įtariamu nusikalstama veikla.

Atsižvelgdami į tai, Aukšto lygio grupės ekspertai nurodė keturias pagrindines iššūkių kategorijas.

---

81 https://rm.coe.int/1680081561 [Art. 20 & 21]

82 Vienas ekspertas nurodė, kad pasitelkiant tradicinį duomenų perėmimą turinio duomenų neįmanoma gauti 99 % atvejų.

83 Vadinamieji specialieji metodai apima įvairias taktines priemones informacijai apie tyrimą dominantį subjektą gauti naudojant kameras, mikrofonus, nuotolinę prieigą prie įrenginių, GPS sekimo įrenginius ir t. t.

I. Teisėtas ryšio duomenų perėmimas, vykdomas per netradicinius ryšio paslaugų teikėjus

Dauguma valstybių narių yra įgyvendinusios tam tikras teisėtą duomenų perėmimą reglamentuojančias taisykles, kuriomis ryšių paslaugų teikėjams nustatomos pareigos įdiegti duomenų perėmimo pajėgumus[84]. Nors sąlygos, kuriomis išduodami teisėto duomenų perėmimo orderiai, įvairiose šalyse labai skiriasi, veiklos vykdytojams taikomos pareigos dažnai yra panašios[85]: jie turi gebėti be jokių spragų perimti visus atitinkamus pranešimus, kuriuos nacionalinėje teritorijoje siunčia nurodytas tyrimą dominantis subjektas, ir turi suteikti infrastruktūrą, būtiną perimamiems duomenims rinkti ir perduoti teisėsaugai.

Tais atvejais, kai telekomunikacijų tinklo operatoriai (ryšių paslaugų teikėjai, kuriems priklauso tinklas ir kurie gali naudotis jo infrastruktūra) teikia ir ryšio paslaugas (telefono skambučių, SMS žinučių ir kt.), jie dažniausiai geba įvykdyti teisėto duomenų perėmimo pareigas[86]. Daugeliu atvejų jie remiasi ETSI standartais ir pasitelkia specialaus profilio technologijų teikėjus, kad galėtų suvaldyti savo pačių suvaržymus, be kita ko, kiek tai susiję su ekonominiu efektyvumu, minimaliu poveikiu tinklo infrastruktūrai, sąveikumu, patikimumu ir saugumu.

OTT paslaugų atveju padėtis yra sudėtingesnė: teisėtą duomenų perėmimą gali vykdyti arba telekomunikacijų tinklo operatoriai, arba paslaugą teikiantis OTT paslaugų teikėjas.

Kai ryšio duomenų, siunčiamų naudojantis OTT paslaugomis, perėmimas įgyvendinamas telekomunikacijų tinklo lygmeniu, jo veiksmingumas dažnai yra ribotas. Pirma, telekomunikacijų tinklo operatorius gali nesugebėti identifikuoti turimą dominančio subjekto vykdomos komunikacijos (pvz., kai prisijungiama per viešą belaidį vietinį tinklą (Wi-Fi)). Be to, teikiant OTT paslaugas dažnai naudojami nuosavybiniai ryšio protokolai, kuriuos reikia dekoduoti naudojant teisėtas perėmimo sistemas, todėl procesas daugiau kainuoja, ilgiau trunka ir tampa sudėtingesnis. Galiausiai, OTT paslaugų teikėjams naudojant ištisinį šifravimą, prieiga prie turinio duomenų tampa labai problemiška, o prieiga prie metaduomenų dar labiau apsunkinama, nes didžioji dauguma šalių mano, kad, vadovaujantis Budapešto konvencija, telekomunikacijų tinklo operatorių pareiga teikti nešifruotą informaciją baigiasi tuomet, kai trečioji šalis naudoja šifravimą.

---

84 Žr. „Lawful interception – A market access barrier in the European Union“ („Teisėtas perėmimas. Patekimo į rinką kliūtis Europos Sąjungoje“), Vadim Doronin, *Computer Law & Security Review 51* (2023), 105867.

85 Tačiau įpareigos, susijusios su turinio duomenimis ar ne turinio duomenimis, skiriasi.

86 Tačiau tokios tinklo paslaugos kaip maršruto parinkimas per savąjį tinklą, tinklo padalijimas arba išplėstinės komunikacijų paslaugos gali trukdyti telekomunikacijų tinklo operatoriams vykdyti savo pareigas (žr. skirsnį apie technologinius iššūkius).

E. privatumo direktyvos 5 straipsnio 1 dalyje pavartota elektroninių ryšių paslaugų apibrėžtis, pateikiama Europos elektroninių ryšių kodekse; ši apibrėžtis nuo 2018 m. apima ir su numeriu nesiejamo asmenų tarpusavio ryšio paslaugas. Tai savo ruožtu reiškia, kad dabar platesnė ERP koncepcija (palyginti su buvusia tuo metu, kai buvo priimta E. privatumo direktyva) suteikia valstybėms narėms galimybę teisėtam duomenų perėmimui tiesiogiai pasitelkti OTT paslaugų teikėjus[87]. Iki šiol valstybės narės šia galimybe naudojosi nevienodai: kai kurios nustatė panašias pareigas visų rūšių ERP teikėjams, įskaitant OTT paslaugų teikėjus, o kitos OTT paslaugų teikėjų neįtraukė[88]. **Praktikoje, nepaisant esamų pareigų, pagrindinių OTT paslaugų teikėjai nesukūrė techninių mechanizmų, skirtų reaguoti į ES valstybių narių valdžios institucijų prašymus dėl teisėto duomenų perėmimo**; taip yra visų pirma dėl teisinių priežasčių[89].

Priešingai, Jungtinė Karalystė Tyrimo įgaliojimų įstatymu sukūrė pagrindą teisėtam OTT ryšio duomenų perėmimui, kuris, patvirtinus Jungtinės Karalystės ir JAV prieigos prie duomenų susitarimą, taip pat taikomas OTT paslaugoms, kurias teikia Jungtinėse Amerikos Valstijose įsisteigę teikėjai. Atitinkamų Jungtinės Karalystės valdžios institucijų teigimu, tai turi reikšmingą poveikį nusikaltimų prevencijai ir tyrimams.

Galiausiai nacionalinių valdžios institucijų ekspertai aiškiai nurodė, kad taktinis duomenų perėmimas, užtikrinamas naudojantis pažeidžiamumu, nėra nei veiksminga, nei pageidaujama alternatyva OTT paslaugų teikėjams taikomoms vykdytinoms teisėto duomenų perėmimo taisyklėms ir turėtų būti naudojamas tik specifiniais atvejais, numatant tvirtas nacionalinės teisės aktuose apibrėžtas garantijas, kad būtų užtikrintas proporcingumas.

---

87 Tačiau vis dar vyksta diskusijos dėl tikslios taikymo aprėpties, o aiškinimas valstybėse narėse skiriasi.

88 Žr. „Lawful interception – A market access barrier in the European Union“ („Teisėtas perėmimas. Patekimo į rinką kliūtis Europos Sąjungoje“), Vadim Doronin, *Computer Law & Security Review 51* (2023), 105867.

89 Tai nėra pagrįsta statistiniais duomenimis, nes nacionalinės valdžios institucijos prašymus dėl teisėto duomenų perėmimo labai retai siunčia OTT paslaugų teikėjams, gerai suprasdamos, jog mažai tikėtina, kad tai duos rezultatų.

II. Tarpvalstybiniai prašymai

Tarpvalstybiniai teisėto duomenų perėmimo prašymai, teikiami OTT paslaugų teikėjams ir, kiek mažesniu mastu, tradicinių ryšių paslaugų teikėjams, teisėsaugos institucijoms kelia keletą iššūkių.

Kalbant apie tradicinių ryšių paslaugų teikėjus, institucijos pirmiausia susiduria su organizaciniais iššūkiais. Pirma, tarptautinio bendradarbiavimo priemonės, visų pirma savitarpio teisinės pagalbos (STP) mechanizmai, gali būti nepraktiškos skubaus duomenų perėmimo atvejais, kai leidimus gauti ir įgyvendinimą užtikrinti reikia per kelias valandas, o ne per kelias dienas ar savaites[90]. Taip yra dėl to, kad reikia imtis įvairių veiksmų siekiant užtikrinti įstatymų laikymąsi tiek prašymą teikiančioje, tiek jį gaunančioje valstybėje narėje. Apskritai manoma, kad STP procesas, kai jis taikomas teisėtam duomenų perėmimui, yra neveiksmingas ir apsunkinantis. 2017 m. pradėta taikyti Europos tyrimo orderio (ETO) sistema pakeitė tradicinius STP procesus ES[91]: buvo nustatyti griežti prašomų įrodymų surinkimo terminai[92], apriboti tokių prašymų atmetimo pagrindai ir nustatyta bendra standartinė forma, kurią institucijos turi naudoti, kai prašo pagalbos ieškodamos įrodymų. Be to, tais atvejais, kai siekiant įvykdyti perėmimą nereikia valstybės narės, kurioje yra subjektas, kurio ryšių duomenis ketinama perimti, techninės pagalbos, tai valstybei narei standartine forma pranešama apie perėmimą ir suteikiama galimybė per 96 valandas pareikšti prieštaravimą. Precedentinėje byloje C-670/22 ESTT pateikia platų sąvokos „telekomunikacijų perėmimas“ aiškinimą, nurodydamas, kad įsiskverbimas į galinius įrenginius, skirtas srauto, vietos nustatymo ir telekomunikacijų duomenims perimti iš internetu grindžiamos ryšių paslaugos, yra „telekomunikacijų perėmimas“. Vis dėlto ekspertai mano, kad ETO sistema padarytų reikšmingų patobulinimų nepakanka, kad būtų patenkintas poreikis turėti greitą ir suderintą tarpvalstybinę prieigą prie perduodamų duomenų.

Be to, valstybių narių valdžios institucijos pranešė, kad esama techninė architektūra dažnai nėra tinkama naudoti, kai norima įgyvendinti teisėtą duomenų perėmimą vienoje valstybėje narėje ir beveik tikruoju laiku perduoti duomenis kitai valstybei narei. Kai kuriais atvejais, kai taikomi atitinkami organizaciniai protokolai, perduotinų duomenų kiekis būna tiesiog nesuderinamas su apsaugotiems ryšių kanalams būdingu tinklo pralaidumu.

---

90 Ekspertai paminėjo atvejus, kai byla buvo baigta anksčiau, nei buvo faktiškai įgyvendintas tarpvalstybinis teisėtas duomenų perėmimas, arba atvejus, kai buvo susikaupę tiek STP prašymų, kad juos vykdyti buvo vėluojama daugiau nei 8 mėnesius.

91 Išskyrus DK ir IE, kuriose ETO sistema netaikoma.

92 30 dienų ETO pripažinimui ir dar 90 dienų jo vykdymui.

OTT ryšio duomenų perėmimas kelia sudėtingų jurisdikcijos klausimų, palyginti su atvejais, kai perimami telefono ryšio duomenys, nes pastarųjų paslaugų teikėjai savo paslaugas siūlo aiškiai apibrėžtoje teritorijoje. Tradicinės telekomunikacijų paslaugos yra susietos su konkrečia fizine tinklo infrastruktūra, užtikrinant, kad paslaugų teikėjas turėtų infrastruktūrą ir juridinę buveinę šalyje, kurioje vykdomas duomenų perėmimas. Dėl tokios lokalizuotos konfigūracijos sumažėja teisinių konfliktų ES viduje rizika ir yra lengviau laikytis reikalavimų.

Priešingai, OTT paslaugų atveju prašančioji institucija, subjektas, kurio ryšių duomenis ketinama perimti, fizinis įgyvendinimas ir bendrovės įsisteigimo vieta gali aprėpti kelias skirtingas jurisdikcijas. Šių jurisdikcijų teisinių sistemų sąveika gali lemti teisės kolizijas[93].

Policijos ir teisminių institucijų ekspertai neabejoja: teisėto duomenų perėmimo prašymų vykdymas pasitelkiant tarptautinius mechanizmus nėra perspektyvus sprendimas. Jei teisėsaugos institucijos apeina STP procesą ir vietoj to orderius įteikia tiesiogiai paslaugų teikėjams pagal savo nacionalinės teisės aktus, tokie OTT paslaugų teikėjai kaip, pavyzdžiui, „Microsoft“, META ar „Google“, gali susidurti su prieštaringais teisiniais reikalavimais. Pavyzdžiui, dažnai prašančiojoje valstybėje narėje galioja teisėtą prieigą reglamentuojančios taisyklės, prieštaraujančios Airijos teisei[94], kurios laikydamiesi veikia keli pagrindiniai OTT paslaugų teikėjai, nes jie yra įsisteigę Airijoje, tačiau jiems taip pat gali būti taikoma valstybių narių, kuriose jie teikia savo paslaugas, nacionalinė teisė.

Šios problemos gali būti veiksmingai sprendžiamos pasitelkiant bendras priemones ir teisėto duomenų perėmimo taisyklių suderinimą tam tikru mastu ES lygmeniu, siekiant palengvinti tarpvalstybinių prašymų dėl teisėto duomenų perėmimo teikimą ir paspartinti jų vykdymą. Tai būtų būtina sąlyga norint spręsti kitus organizacinio ir techninio pobūdžio sunkumus, dėl kurių bus galima rasti sprendimų, kai taisyklės bus aiškiai nustatytos ir veiks praktikoje.

---

93 Žr. „LE interception concerns under the EECC“ („Europos elektroninių ryšių kodeksas: teisėsaugos tikslais vykdomo duomenų perėmimo problemos“), „Microsoft“, 2020 m. sausio mėn.

94 Pagal Airijos teisę OTT paslaugų teikėjams draudžiama vykdyti tiesioginį duomenų perėmimą.

III. Technologijos

Nepaisant teisinių sumetimų, ryšių technologijų raida daro poveikį teisėsaugos institucijų techniniam pajėgumui perimti ryšio duomenis, siunčiamus naudojantis tradicinių ryšių paslaugų teikėjų arba OTT paslaugų teikėjų tiesiogiai teikiamomis paslaugomis.

Tradicinių ryšių paslaugų teikėjų atveju teisėto perėmimo technines galimybes remdamiesi ETSI standartais paprastai sukuria technologijų teikėjai ir jos yra įtraukiamos į 3GPP[95]. Todėl priemonėmis gerai aprūpintos policijos tarnybos gali tinkamai tvarkyti tradicinių ryšių – balso ir SMS žinučių – duomenų perėmimą ir galbūt perimti internetiniu ryšiu grindžiamus pranešimus, siunčiamus naudojantis paslaugomis, teikiamomis jų tinklais.

Tačiau vis sudėtingesnės 5G ryšio infrastruktūros ir protokolai, pavyzdžiui, virtualizavimas, tinklo padalijimas, tinklo paribio kompiuterija ir privatumo didinimo elementai, tradiciniams operatoriams kelia naujų technologinių iššūkių[96]. Aukšto lygio grupės ekspertai visų pirma primygtinai rekomendavo spręsti sunkumus, susijusius su maršruto parinkimu per savąjį tinklą[97] ir išplėstinės komunikacijos paslaugomis (RCS)[98].

Žvelgiant iš ateitį ir remiantis 5G patirtimi, Aukšto lygio grupės ekspertai numato, kad bus susidurta su iššūkiais dėl būsimo 6G diegimo (numatyto po 2030 m.), nes taip bus žengtas dar vienas žingsnis privatumo didinimo elementų srityje[99], galbūt kaip standartą taikant ištisinį šifravimą, o dėl visų šių veiksnių kartu galėtų tapti sunku perimti duomenis. Tuo pat metu dėl naujų ryšių technologijų, pavyzdžiui, daiktų interneto, palydovinio ryšio ir kvantinės kompiuterijos plėtros[100], kyla dar kitų iššūkių, kuriuos reikia numatyti iš anksto.

---

95 Trečiosios kartos partnerystės projektas, kuris suteikia pagrindą plėtoti tokias ryšių technologijas kaip 5G, daiktų internetas ir judrusis plačiajuostis ryšys.

96 Žr. „Law enforcement and judicial aspects related to 5G“ („Su 5G susiję teisėsaugos ir teisminiai aspektai“), ES kovos su terorizmu koordinatorius, 2019 m., https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Europol - Position paper on Home routing (Europolas. Pozicijos dokumentas dėl maršruto parinkimo per savąjį tinklą).pdf (europa.eu).

98 RCS protokolas leidžia keistis pranešimais grupės pokalbiuose, vaizdo, garso ir didelės skiriamosios gebos vaizdais; jis dažnai naudojamas vietoj SMS. Teisėtas RCS pranešimų perėmimas, priklausomai nuo jo įgyvendinimo, gali būti neįmanomas, o tai daro reikšmingą poveikį teisėsaugai (daugiau kaip 1 mlrd. aktyvių RCS naudotojų 2023 m.).

99 Žr. „6G roadmap“ („6G veiksmų gairės“): 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 (Antroji kvantinė revoliucija: kvantinės kompiuterijos ir kvantinių technologijų poveikis teisėsaugai)| Europolas (europa.eu).

Galiausiai Aukšto lygio grupės ekspertai pabrėžė, kad vienas iš pagrindinių techninių iššūkių, su kuriais susiduria teisėsaugos institucijos, yra susijęs su ištisiniu šifravimu, visų pirma OTT ryšių atveju, kur daugiau kaip 80 % duomenų siunčiama naudojantis ištisinio šifravimo paslaugomis (tiesioginiu ryšiu ir atsarginės kopijos saugykla), todėl tyrėjai negali prieiti prie komunikacijos turinio. Kartu ekspertai taip pat sutinka, kad ištisinis šifravimas laikomas patikima saugumo priemone, kuria piliečiai veiksmingai apsaugomi nuo įvairių formų nusikaltimų. Kadangi ištisiniu šifravimu užtikrinama, kad tik komunikuojantys naudotojai galėtų gauti prieigą prie savo pranešimų turinio, juo veiksmingai apsaugoma nuo neteisėto pasiklausymo, duomenų vagystės, valstybių remiamo šnipinėjimo ir kitų formų neteisėtos prieigos, kurią gauna įsilaužėliai, kibernetiniai nusikaltėliai ar net patys paslaugų teikėjai.

Sunku kiekybiškai įvertinti iššūkius, su kuriais teisėsaugos institucijos susiduria norėdamos stebėti nusikaltėlių ir teroristų komunikaciją naudojant ištisinį šifravimą. Taip yra todėl, kad teisėsaugos institucijos dažnai nusprendžia neinvestuoti laiko ir išteklių, kad gautų teismo orderius dėl elektroninio stebėjimo tose platformose, kurios, kaip žinoma, standartiškai naudoja ištisinį šifravimą[101]; todėl realiai pateiktų teisėto turinio duomenų perėmimo prašymų, kurių negalima įvykdyti dėl ištisinio šifravimo, skaičius yra labai mažas ir nereikšmingas. Teisėsaugos institucijos mano, kad šis stebėjimo pajėgumo trūkumas yra reikšminga akloji zona ir silpna vieta, apie kurią nusikaltėliai ir teroristai puikiai žino ir kuria aktyviai naudojasi, kaip parodė „EncroChat“[102] ir „Sky ECC“ atvejai, kai visoje Europoje buvo sulaikyti tūkstančiai asmenų, įskaitant daugelį žinomų ir pagarsėjusių nusikaltėlių. Šis susirūpinimas buvo pakartotas keliuose Europos policijos vadovų susitikimų[103], be kita ko, ir G7 formatu[104], pareiškimuose. Kad paaiškintų, koks yra prieigos prie turinio duomenų praradimo poveikis, ekspertai nurodė kelis viešai žinomus pavyzdžius, be kita ko, susijusius su terorizmo[105], prekybos narkotikais[106] ir iššaginimo[107] bylomis, kai šifravimas labai apsunkino teisėsaugos gebėjimą vykdyti sunkaus ir organizuoto nusikalstamumo prevenciją ir su juo kovoti.

Teisėsaugos atstovai pirmenybę teiktų požiūriui, pagal kurį būtų reikalaujama, kad bendrovės teisėsaugos institucijoms suteiktų prieigą prie nešifruotų duomenų, taikant griežtas sąlygas. Tačiau reikėtų pažymėti, kad kibernetinio saugumo ekspertai išreiškė susirūpinimą, kad tokie sprendimai pakenktų kibernetiniam saugumui. Kai kurie teisėsaugos ekspertai nurodė, kad kai kuriais atvejais šifravimas įdiegtas tokiu būdu, kuris yra suderinamas tiek su kibernetiniu saugumu, tiek su poreikiu išlaikyti kai kurias paslaugas, pavyzdžiui, operacinės sistemos atnaujinimo, turinio skenavimo (pvz., el. laiškų ar naršymo seansų) kibernetinio saugumo tikslais, arba pagrindinius atkūrimo mechanizmus, kai naudotojas pasirenka šią funkciją.

---

101 Manpearl, 2017 m.

102 Daugiau informacijos apie „EncroChat“ ir „Sky ECC“ žr.: Europolas ir Eurojustas, „Third Report of the Observatory Function on Encryption“ („Trečioji šifravimo stebėjimo centro ataskaita“), 2021 m. birželio mėn.

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 m. kovo mėn. 52 metų vyras Khalidas Masoodas centrinėje Londono dalyje įvykdė islamistų įkvėptą teroristinį išpuolį, per kurį žuvo šeši žmonės, o 29 buvo sužeisti. Nors iš pranešimų apie šį incidentą buvo galima spręsti, kad K. Masoodas planavo ir veikė vienas, buvo nustatyta, kad likus kelioms minutėms iki išpuolio daugeliui savo kontaktų per „WhatsApp“ ir „iMessage“ jis išsiuntė PDF dokumentą, pavadintą „Jihad“; abiejose šiose programėlėse duomenys buvo ir vis dar yra standartiškai užšifruoti ištisiniu šifravimu. Šaltiniai: Max Hill, „The Westminster Bridge Terrorist Attack“ („Vestminsterio tilto teroristinis išpuolis“) (Londonas: „The Stationery Office“, 2018); „BBC News“, publikacija „WhatsApp Must Not Be a „Place for Terrorists to Hide“ („*WhatsApp* neturi būti vieta, kur teroristai gali pasislėpti“), 2017 m. kovo 26 d.

106 Ekspertai paminėjo garsiai nuskambėjusias prekybos narkotikais bylas, kuriose pažangos nebuvo galima padaryti tol, kol nebuvo gauta prieiga prie šifruotų komunikacijos per „EncroChat“ ir „Sky ECC“ duomenų.

107 Didelio atgarsio Jungtinėje Karalystėje sulaukusioje iššaginimo byloje policijai buvo sunku atlikti tyrimą, nes įtariamieji bendravimui naudojosi „WhatsApp“ ir dėl ištisinio šifravimo buvo sunku gauti esminių įrodymų. Tyrimui trukdė tai, kad teisėsaugos institucijos neturėjo galimybės iššifruoti „WhatsApp“ pranešimų be naudotojo sutikimo.

Tuo remdamiesi teisėsaugos ekspertai susitarė, kad šifravimo keliamiems iššūkiams įveikti reikia daugialypio požiūrio, kuriuo būtų užtikrinta teisių į privatų gyvenimą, saugumo ir poreikio teisėsaugos institucijoms susipažinti su duomenimis siekiant kovoti su nusikalstamumu ir apsaugoti žmonių gyvybes, fizinę neliečiamybę ir turtą, pusiausvyra. Nors mažai tikėtina, kad vienu sprendimu galėtų būti išspręsti visi susirūpinimą keliantys klausimai, derinant požiūrius būtų galima sumažinti problemos mastą.

IV. Nusikalstamo pobūdžio ryšių paslaugų teikėjai

Nusikaltėliai naudoja įprastines ištisinio šifravimo platformas, kad nuslėptų savo komunikaciją; tačiau jie taip pat gali nuspręsti naudotis saugiais ryšių kanalais, specialiai sukurtais nusikalstamai veiklai (vadinamaisiais „NRK“ – „nusikalstamais ryšių kanalais“)[108]. „EncroChat“ ir „Sky ECC“ – abu šie kanalai yra gerai žinomi NRK, kurie parduodavo telefonus su integruota ištisinio šifravimo pranešimų paslauga, skirta nusikalstamai veiklai nuslėpti, ir buvo reklamuojami „juodajame tinkle“. 2020 ir 2021 m. abi platformos buvo išardytos – tai pasiekta pasitelkus tarptautines bendras teisėsaugos operacijas, kurios atskleidė aktyvų naudojimąsi jomis organizuotoje nusikalstamoje veikloje. Taip pat išardytos kelios panašios platformos, pavyzdžiui, „Phantom Secure“[109] ir „Exclu“[110], o daugelis mažesnių platformų vis dar veikia ir suteikia saugų prieglobstį nusikaltėlių keitimusi informacija. Šioje fragmentuotoje aplinkoje labai svarbu, kad teisėsaugos institucijos galėtų identifikuoti NRK, stebėti ir blokuoti jų veiklą, juos išardyti ir patraukti nusikaltėlius baudžiamojon atsakomybėn.

[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 | European Union Agency for Criminal Justice Cooperation (europa.eu) (Naujas smūgis kovojant su šifruota nusikaltėlių komunikacija išardant „Exclu“ priemonę | Eurojustas | Europos Sąjungos bendradarbiavimo baudžiamosios teisenos srityje agentūra (europa.eu).

Nors šios rūšies nusikalstamo ryšių paslaugų teikėjo atveju perimti duomenų operatoriaus lygmeniu neįmanoma, teisėsaugos institucijoms reikia tinkamų taktinio duomenų perėmimo pajėgumų (priemonių ir ekspertinių žinių), kad galėtų tikslingai stebėti tokių paslaugų naudotojus, nepaisant šifravimo. Teisėsaugos ekspertai pabrėžė didelius iššūkius, riziką ir apribojimus, susijusius su tokių metodų, kurių mastas nėra plėstinas ir kurie turėtų būti taikomi tik svarbiausiais atvejais, plėtojimu ir naudojimu. Priklausomai nuo savo pajėgumų ir teisinės sistemos, nacionalinės valdžios institucijos taiko skirtingus metodus, įskaitant pačių parengtas priemones, priemones, kurios įsigytos iš trečiųjų šalių arba teikiamos kaip paslaugos; neatsižvelgiant į tai, kurį variantą jos naudoja, ekspertai sutaria, kad reikia įdiegti garantijas ir apsaugos priemones dėl tokių priemonių naudojimo. Tai gali apimti svarstymus dėl geresnės priemonių priežiūros, vertinimo ir sertifikavimo, taip pat tvirtą pažeidžiamumo valdymo sistemą, kartu visapusiškai gerbiant valstybių narių procedūrinį savarankiškumą baudžiamosiose bylose ir jų išimtinę kompetenciją nacionalinio saugumo srityje.

Tyrimus atliekančios institucijos taip pat susiduria su teisiniais iššūkiais, pavyzdžiui, sunkumais siekiant kriminalizuoti ryšių paslaugų ir prieglobos paslaugų teikėjus, kurie teikia daugiausia nusikalstamas paslaugas (kadangi visas srautas yra šifruotas), nes tai yra būtinas pirmasis žingsnis siekiant teisminių ar administracinių veiksmų. Be to, valstybės narės turi galėti nustatyti sankcijas NRK, siekiant riboti ar blokuoti prieigą prie tokių paslaugų ES ir tokiu būdu panaikinti jų nusikalstamą verslo modelį. Tai taps būtina, kai ir jeigu perėmimo pareigos bus pradėtos taikyti OTT paslaugoms, siekiant užkirsti kelią nusikaltėliams grįžti prie nusikalstamų ryšių paslaugų teikėjų.

Galiausiai, įvairūs tokių bylų kaip, pavyzdžiui, bylų prieš „EncroChat“ ir „Sky ECC“, aspektai ginčijami teismuose. Visoje ES labai skiriasi reikalavimai dėl kitoje valstybėje narėje perimtų duomenų naudojimo kaip įrodymų, todėl esama teisinio netikrumo dėl panašių operacijų, kurias vykdo viena valstybė narė, galimo poveikio daugeliui kitų.

GALIMI SPRENDIMAI

I. Užtikrinti, kad teisėto duomenų perėmimo prašymai taptų vykdytini visų rūšių elektroninių ryšių paslaugų teikėjams

ES teisėto duomenų perėmimo pajėgumai apima tik tradicinius ryšių paslaugų teikėjus, o didžioji dalis komunikacijos šiuo metu vyksta per netradicinius ryšių paslaugų teikėjus[111]. Nepriklausomai nuo to, ar ryšių paslaugą teikia infrastruktūros savininkas, ar ne, teisėsaugos institucijos turėtų vienodai galėti atlikti teisėtą duomenų perėmimą atitinkamo jas dominančio subjekto atžvilgiu. Alternatyvūs sprendimai, pavyzdžiui, teisėtas duomenų perėmimas NI-ICS ir kitų ryšių paslaugų atveju išskirtinai telekomunikacijų tinklo lygmeniu, kliovimasis tarptautinio bendradarbiavimo priemonėmis siekiant atlikti teisėtą duomenų perėmimą NI-ICS paslaugos teikėjo lygmeniu ar visapusiškas taktinio duomenų perėmimo naudojimas, yra praktiškai neįgyvendinami[112].

Todėl aukšto lygio grupės ekspertai mano, kad vienas iš prioritetų yra užtikrinti, kad su teisėtu turimų duomenų perėmimu susijusios pareigos būtų taikomos vienodai tradiciniams ir netradiciniams ryšių paslaugų teikėjams ir būtų užtikrinamas vienas jų vykdytinumas. Tokių pareigų suderinimas turėtų padėti įveikti iššūkius, susijusius su tarpvalstybinių prašymų vykdymu.

Siekiant šio tikslo ir kad palaipsniui būtų artėjama prie teisėto duomenų perėmimo taisyklių suvienodinimo ir suderinimo ES, aukšto lygio grupės ekspertai siūlo vadovautis laipsnišku požiūriu: pirma, ES lygmeniu turėtų būti susitarta dėl struktūros principų (1 etapas); tuomet Komisija turėtų remti šių principų gyvendinimą (2 etapas) ir, galiausiai, remiantis tolesniu vertinimu, principai gali būti kodifikuoti teisiniame dokumente (3 etapas).

---

111 2022 m. Jungtinėje Karalystėje išsiųsta 36 mlrd. SMS ir MMS, o internetinių žinučių buvo 1,3 trln. (WhatsAppening in the world of online communications? (Kas vyksta internetinių ryšių pasaulyje?) - Ofcom).

112 Žr. skirsnį dėl iššūkių.

1 etapas. Susitarimas dėl bendrų pagrindinių principų

Pirma, reikia išplėtoti bendrą supratimą apie tai, kurių kategorijų elektroninių ryšių paslaugoms (ERP) gali būti taikomos vidaus pareigos dėl teisėto duomenų perėmimo pagal e. privatumo ir BDAR taisykles.

Antra, būtina pasiekti susitarimą dėl aukšto lygmens operacinių reikalavimų, aiškiai nurodantį, ko tikimasi iš nacionalinių valdžios institucijų teisėto duomenų perėmimo srityje ir kokios turėtų būti susijusios apsaugos priemonės. Kaip geras pagrindas teisėsaugos reikalavimams apibrėžti buvo įvardytas LEON[113]. Prie šio dokumento turėtų būti pridėti reikalavimai dėl, pvz., proporcingumo, priežiūros ir skaidrumo, galimai atskiriant taisykles, taikytinas turinio duomenims ir ne turinio duomenims, visapusiškai atsižvelgiant į kibernetinį saugumą ir duomenų apsaugą bei privatumą ir nepakenkiant šifravimui. Pasinaudojus galimybe įsteigti ekspertų, įskaitant kibernetinio saugumo, privatumo ir teisėsaugos sričių ekspertus, *ad hoc* grupę, būtų galima užtikrinti, kad reikalavimai prireikus būtų atnaujinami, galimai remiantis Europolo vidaus saugumo standartizacijos darbo grupės darbu, kuris turėtų būti tęsiamas.

Trečia, reikia aiškesnės koncepcijos dėl teritorinės jurisdikcijos, kalbant apie jos taikymą OTT paslaugoms, atsižvelgiant į skirtingą nacionalinių valdžios institucijų ir, svarbiausia, nacionalinių valdžios institucijų ir OTT teikėjų, aiškinimą. Pavyzdžiui, turėtų būti patikslintos taisyklės, taikomos tais atvejais, kai tyrimą dominančio subjekto buvimo vieta nėra aiški. Taip pat reikia gairių dėl to, kas gali įvertinti prašymo teisėtumą, pavyzdžiui, kiek tai susiję su paslaugų teikėjų vaidmeniu šiame kontekste. Galiausiai, nors didžioji dauguma teismo sprendimų iki šiol patvirtino procesinių veiksmų prieš „EncroChat“ ir „Sky ECC“ teisėtumą, keletas bylų teismuose vis dar nagrinėjamos[114] ir gali turėti didelį poveikį nuosprendžiams žinomų ir pagarsėjusių nusikaltėlių bylose. Taigi gali reikėti palengvinti vykdant taktinio duomenų perėmimo priemones tarp valstybių narių gautų įrodymų priimtinumą, teismo ir teisminių institucijų sprendimų tarpusavio pripažinimą ir policijos bei teisminį bendradarbiavimą baudžiamosiose bylose.

---

[113] LEON (teisėtos prieigos prie ryšių teisėsaugos ir operaciniai poreikiai) yra Švedijos teisėsaugos institucijų darbo, atlikto glaudžiai bendradarbiaujant su teisėsaugos atstovais ES valstybėse narėse, Šiaurės Amerikoje ir Australijoje, rezultatas. Jo tikslas – nustatyti ir apibūdinti teisėsaugos poreikius, susijusius su teisėta prieiga prie ryšių turinio, su turiniu susijusių duomenų ir informacijos apie abonentą. Žr. *Tarybai pirmininkaujančios valstybės narės komunikatą dėl teisėsaugos operatyvinių teisėtos prieigos prie ryšių poreikių (LEON)*, dok. 6050/23, 2023 m. vasario 16 d.

[114] Žr. bylas T-1180/23, T-148/24, T-167/24, T-484/24 ir T-560/24.

7 rekomendacijų grupė

Siekdami ES lygmeniu susitarti dėl teisėto turimų duomenų perėmimo bendrųjų principų, taikytinų visiems ERP teikėjams, ekspertai rekomenduoja:

1. *patikslinti teisėto duomenų perėmimo apibrėžtį ir taikymo sritį pagal esamus ES aktus ir kitus atitinkamus Europos ir tarptautinius dokumentus, tokius kaip Budapešto konvencija dėl kibernetinių nusikaltimų [38 rekomendacija];*

2. *remiantis LEON dokumentu apibrėžti bendrus operatyvinius reikalavimus [21 rekomendacija];*

3. *nustatyti, kokios yra būtinos apsaugos priemonės [17 rekomendacija, 41 rekomendacija];*

4. *atsižvelgti į kibernetinio saugumo perspektyvą, kad pagal jokią priemonę nebūtų implikuota paslaugų teikėjų pareiga pritaikyti savo IRT sistemas tokiu būdu, kuris neigiamai paveiktų jų naudotojų kibernetinį saugumą [41 rekomendacija];*

5. *patikslinti teritorinės jurisdikcijos duomenų atžvilgiu koncepciją, siekiant spręsti galimos įstatymų kolizijos problemą [39 rekomendacija] ir skatinti priimti minimaliąsias ES lygmens taisykles, pagal kurias būtų palengvintas vykdant taktinio duomenų perėmimo priemones tarp valstybių narių gautų įrodymų leistinumas, kai tinkama, kiek tai būtina nuosprendžių, teismo sprendimų tarpusavio pripažinimui ir policijos bei teisminiam bendradarbiavimui baudžiamosiose bylose palengvinti [42 rekomendacija].*

Reikia apsvarstyti, koks yra geriausias požiūris siekiant nustatyti bendrus principus, kaip nurodyta 7 rekomendacijų grupėje, ir dėl jų susitarti ir siekiant nustatyti tinkamiausią priemonę, užtikrinančią, kad tie principai būtų bendri. Žvelgiant į praeitį, 1995 m. sausio 17 d. Tarybos rezoliucija dėl teisėto perėmimo[115] buvo labai svarbi priemonė palengvinant teisėto perėmimo sprendimų suderinimą, kadangi joje buvo pateikta nuoroda į ETSI parengtus teisėto perėjimo standartus. Atitinkamai galėtų būti naudingas panašus požiūris, kuris galbūt galėtų būti nustatytas Komisijos ar Tarybos rekomendacija.

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

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina ES 2025 m. pateikti rekomendaciją dėl prieigos prie duomenų realiuoju laiku

Laikas: 2025 m. *Biudžetas: turi būti nustatyta*

- Aukšto lygio grupės ekspertai ragina Europos Komisiją paskelbti rekomendaciją, kurioje būtų paaiškinta teisėto duomenų perėmimo[116] sąvoka ERP teikėjams ir kurioje būtų išsamiai išdėstyti skirtingi reikalavimai, kurie gali būti taikomi teisėtam turimų su turiniu nesusijusių duomenų ir turinio duomenų perėmimui, visapusiškai atsižvelgiant į kibernetinį saugumą, duomenų apsaugą ir privatumą, nepakenkiant šifravimui ir remiantis bendrais operaciniais reikalavimais, kaip apibrėžta LEON dokumente.

2 etapas. ES paramos teikimas siekiant užtikrinti vienodas sąlygas ir stiprinti tarpvalstybinį bendradarbiavimą

1 etape išdėstyti bendrieji principai būtų techninio, teisinio ir organizacinio suderinimo ES lygmeniu pagrindas. Tam, kad jie taptų konkrečiais rezultatais, reikalingas Komisijos vykdomas koordinavimas ir finansinė parama. Tam reikėtų sukurti specialų procesą, pasitelkus esamas darbo grupes ir prireikus sukūrus naujas, užtikrinant koordinavimą su atitinkamais suinteresuotaisiais subjektais, įskaitant OTT paslaugų teikėjus ir pramonės atstovus, ataskaitų teikimą atitinkamiems organams, visų pirma Tarybai ir Europos Parlamentui, ir skaidrumą visuomenės atžvilgiu. Tai taip pat galėtų apimti tikslinių tyrimų finansavimą tiesiogiai arba per atitinkamas partnerystes, pvz., su atitinkamomis agentūromis ar akademiniais partneriais.

[116] Taikoma tik operatoriaus vykdomam duomenų perėmimui, kaip apibrėžta pirmiau.

Be to, Aukšto lygio grupės ekspertai pabrėžė, kad reikia skubiai pagerinti tarpvalstybinio teisėto duomenų perėmimo prašymų veiksmingumą pagal dabartinę sistemą, kartu atliekant pirmiau nurodytą darbą. Šis tikslas apimtų:

- ETO[117] dabartinių trūkumų vertinimą ir darbą siekiant gerinti operatyvinį veiksmingumą;
- techninių ir organizacinių trūkumų, kurie kliudo tarpvalstybiniam keitimuisi įrodymais, surinktais vykdant teisėtą duomenų perėmimą, šalinimą, dėl kurio vėliau reikės dirbti šiose srityse:
    - problemų nustatymas (kokie yra trūkumai, kurios valstybės narės su jais susiduria, etc.),
    - duomenų struktūrų, pasitikėjimo mechanizmų ir duomenų filtravimo standartizavimas, siekiant išvengti neaktualių duomenų perdavimo ir laikytis duomenų apsaugos principų: tikslo apribojimo principo, proporcingumo principo ir duomenų kiekio mažinimo principo,
    - tarpvalstybinių perdavimo priemonių rengimas ir pajėgumai,
    - susijusių finansavimo schemų nustatymas;
- palankesnių sąlygų sudarymą prašymams dėl tarpvalstybinio teisėto duomenų perdavimo paskiriant ir apmokant bendrus kontaktinius punktus, koordinuojant veiklą su platesniu darbu bendrų kontaktinių punktų ir prieigos prie skaitmeninių įrodymų srityje, svarbų vaidmenį skiriant projektui SIRIUS;
- kai aktualu, valstybių narių ir JAV dvišalių susitarimų skatinimą kaip išankstinę sąlygą siekiant palengvinti tiesioginius nacionalinių institucijų prašymus pagrindiniams OTT paslaugų teikėjams, kadangi į ES ir JAV susitarimo dėl tarpvalstybinės prieigos prie elektroninių įrodymų, dėl kurio šiuo metu vyksta derybos, taikymo sritį pagal derybinius nurodymus teisėtas duomenų perėmimas nepatenka, o tai reiškia, kad reikia konkrečių susitarimų teisės kolizijai spręsti.

[117] 2014 m. balandžio 3 d. Europos Parlamento ir Tarybos direktyvoje 2014/41/ES dėl Europos tyrimo orderio baudžiamosiose bylose (toliau – ETO direktyva) kalbama apie telekomunikacijas; nors dauguma valstybių narių tai aiškina plačiau, laikantis atnaujinto Europos elektroninių ryšių kodekso, gali būti svarstoma ir toliau vertinamas galimas poreikis iš dalies pakeisti ETO šiuo atžvilgiu.

Galiausiai, ekspertai paragino apsvarstyti priemones, kuriomis galėtų būti patobulintos atgrasymo priemones, kurių imasi nacionalinės institucijos nebendradarbiaujančių ERP atžvilgiu. Ekspertai visų pirma paragino įvertinti galimų techninių sprendimų įgyvendinamumą ir proporcingumą.

8 rekomendacijų grupė

Siekiant užtikrinti, kad įvairūs ERP teikėjai, įskaitant OTT paslaugų teikėjus, reaguotų į prašymus dėl teisėto duomenų perėmimo, kaip nustatyta nacionalinės teisės aktuose, ekspertai rekomenduoja:

1. *vykdant koordinavimą ir teikiant finansavimą remti 1.1 rekomendacijoje nustatytų principų įgyvendinimą;*
2. *išnagrinėti, kaip būtų galima geriau pasiremti ETO veiksmingų tarpvalstybinių teisėto duomenų perėmimo prašymų tikslais, pvz., didinant teisinį tikrumą, trumpinant reagavimo į orderius terminus ir skatinant vienodą ETO naudojimą [40 rekomendacija];*
3. *kurti mechanizmus (sąveikumas ir kibernetinis saugumas) ir infrastruktūras (tinklo pralaidumas ir išplečiamumas), kurie būtų suderinami su didelių duomenų rinkinių tarpvalstybiniu perdavimu realiuoju laiku [9 rekomendacija];*
4. *skatinti paskirti bendrus kontaktinius punktus Europos Sąjungoje, kad jie tvarkytų valdžios institucijų prašymus ir palaikytų ryšius su jomis, siekiant palengvinti teisėto duomenų perėmimo pareigų vykdymo užtikrinimą ir nustatyti veiksmingo tarpvalstybinių prašymų adresavimo mechanizmus [19 ir 36 rekomendacijos];*
5. *skatinti rengti dvišalius susitarimus dėl prieigos prie duomenų tikruoju laiku su trečiosiomis valstybėmis, visų pirma su Jungtinėmis Valstijomis [38.4 rekomendacija].*

Tam tikra veikla galėtų padėti veiksmingai įgyvendinti ES rekomendaciją dėl teisėto duomenų perėmimo.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai ragina Komisiją prisidėti prie ES rekomendacijos dėl teisėto duomenų perėmimo įgyvendinimo atitinkamu koordinavimu ir finansavimu

- Aukšto lygio grupės ekspertai ragina Komisiją pasiūlyti aiškų planą, skirtą remti ES rekomendacijos dėl teisėto duomenų perėmimo įgyvendinimą, be kita ko, finansinio planavimo požiūriu.

3 etapas. Galimybės parengti teisinę priemonę dėl teisėto duomenų perėmimo įvertinimas

Siekiant užtikrinti reikiamą suderinimo lygį gali nepakakti vien koordinavimo, net jeigu jis būtų papildytas priemonėmis, kuriomis esamos teisinės priemonės taptų veiksmingesnės. Gali reikėti naujų taisyklių, kad būtų užtikrintas prašymų vykdymas ir teisinis tikrumas, pašalinta teisės kolizija ir sumažinta administracinė našta, susijusi su reikalavimų laikymusi ir teisėtumo patikrinimais. Be to, dėl teisėto duomenų perėmimo taisyklių skirtumų visoje ES reguliuojamiems subjektams, pavyzdžiui, OTT paslaugų teikėjams, nustatomi naštą sukeliantys reikalavimai, dėl kurių galimai atsiranda kliūčių ryšių paslaugų teikėjams patekti į rinką[118]. Šiuo atžvilgiu suderintos ES taisyklės dėl teisėto turimų duomenų perėmimo padėtų sukurti Europos būsimą skaitmeninę infrastruktūrą, pirmenybę teikiant modeliui, pagal kurį telekomunikacijų infrastruktūra galimai apima visą žemyną[119].

Perėjimas prie internetinių ryšio priemonių yra tvirta paskata nustatyti suderintas prieigos taisykles ES lygmeniu; tačiau teisinės priemonės priimtinumas, įgyvendinamumas ir su ja susijęs poveikis pramonei, kibernetiniam saugumui ir saugumui turėtų būti atidžiai įvertintas, atsižvelgiant į dabartinius valstybių narių teisinių sistemų teisėto duomenų perėmimo srityje skirtumus. Aukšto lygio grupės ekspertai nurodė, kad galima priemonė: i) turėtų atitikti 1.1 rekomendacijoje nustatytus principus; ii) ja turėtų būti visapusiškai atsižvelgiama į pagrindinių teisių perspektyvą ir valstybių suverenumą baudžiamųjų bylų ir nacionalinio saugumo srityse ir iii) ji turėtų būti grindžiama darbu prie e. įrodymų dokumentų rinkinio.

Aukšto lygio grupės ekspertai sutarė, kad bet kokia iniciatyva skatinti arba nustatyti teisėto duomenų perėmimo taisykles visų rūšių ERP atžvilgiu turėtų apimti aiškias ir vykdymą užtikrinančią sistemą, kuria remiantis būtų galima imtis veiksmų neteisėtai veikiančių ir (arba) atsisakančių bet kokia forma bendradarbiauti su teisėsaugos institucijomis **ryšių paslaugų teikėjų atžvilgiu.** Nenustačius tokios sistemos taisyklės neveiktų, o nusikalstami subjektai tuomet masiškai perkeltų savo komunikaciją pas reikalavimų nesilaikančius paslaugų teikėjus. Bet kokioje būsimoje ES iniciatyvoje šiuo klausimu turėtų būti atsižvelgiama į skirtį tarp OTT paslaugų teikėjų, kurie nesilaiko savo teisinių pareigų, ir ERP teikėjų, kurie tyčia siūlo paslaugas, pritaikytas nusikalstamai veikai. Be to, bet kokioje iniciatyvoje taip pat turėtų būti atsižvelgta į ES *acquis*, visų pirma Skaitmeninių paslaugų aktą.

---

118 Žr. „Teisėtas perėmimas. Patekimo į rinką kliūtis Europos Sąjungoje“ (*Lawful interception – A market access barrier in the European Union*), Vadim Doronin, *Computer Law & Security Review 51* (2023), 105867.

119 Baltoji knyga „Kaip patenkinti ES skaitmeninės infrastruktūros poreikius?“Europos skaitmeninės ateities formavimas (europa.eu).

Tokia iniciatyva galėtų apimti administracines ar teismines priemones. Aukšto lygio grupės ekspertai paragino išsamiai apsvarstyti šį klausimą, diskusijose atsižvelgiant tiek į susirūpinimą pagrindinių teisių ir kibernetinio saugumo srityse, tiek į susijusius sudėtingus technologinius iššūkius.

9 rekomendacijų grupė

Remdamiesi tolesne analize ir poveikio vertinimu, ekspertai rekomendavo ***parengti ES dokumentą dėl teisėto duomenų perėmimo (kurį sudarytų „švelniosios teisės“ arba privalomos teisinės priemonės) teisėsaugos tikslais,*** *kuriuo būtų nustatytos vykdytinos pareigos ERP teikėjams Europos Sąjungoje. Jie rekomendavo, kad šis galimas dokumentas: [38 rekomendacija]*

1. *atitiktų 7 rekomendacijų grupėje sutartus principus;*
2. *būtų technologiškai neutralus [21 rekomendacija];*
3. *skatintų baudžiamosios teisės priemonių, įskaitant laisvės atėmimą, taikomų nebendradarbiaujančių ERP teikėjų atžvilgiu, siekiant užtikrinti bendradarbiavimą, suderinimą ES lygmeniu [34 rekomendacija];*
4. *juo turėtų būti visapusiškai atsižvelgiama į pagrindinių teisių perspektyvą ir valstybių suverenumą baudžiamųjų bylų ir nacionalinio saugumo srityse [38 rekomendacija];*
5. *semtis įkvėpimo iš darbo, atlikto priimant e. įrodymų taisykles [38 rekomendacijos iv punktas];*
6. *nustatytų pareigas paslaugų teikėjams aktyvuoti arba deaktyvuoti tam tikras jų paslaugų funkcijas, kad gavus orderį būtų gauta informacija (pvz., saugoti konkretaus naudotojo geografinės vietos duomenis po to, kai dėl to naudotojo pateikiamas teisėtas prašymas) [32 rekomendacija];*
7. *apimtų mechanizmus, kuriais būtų užtikrinta, kad valstybės narės galėtų užtikrinti sankcijų (administracinių arba baudžiamosios teisės priemonių, priklausomai nuo to, ar teikėjas tiesiog nebendradarbiauja, ar sąmoningai teikia nusikalstamo pobūdžio paslaugą), taikymą nebendradarbiaujantiems ERP teikėjams, laikantis Skaitmeninio paslaugų akto taisyklių ir galbūt jomis remiantis, ir kad tokios sankcijos tuos subjektus atgrasytų [33 rekomendacija].*

ES rekomendacijoje dėl teisėto duomenų perėmimo išdėstytų principų laikymosi užtikrinimas būtų svarbus žingsnis siekiant labiau suderintų ir labiau įgyvendinamų teisėto duomenų perėmimo taisyklių. Tačiau vis tiek gali reikėti teisinės priemonės teisiniam tikrumui padidinti, siekiant užtikrinti, kad būtų taikomos reikiamos apsaugos priemonės visiems atitinkamiems ERP teikėjams įgyvendinant teisėtą duomenų perėmimą, ir siekiant užtikrinti, kad ERP teikėjai, nenorintys užtikrinti valstybių narių nustatytų taisyklių vykdymo, būtų priversti tai daryti.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai prašo Komisijos įvertinti tolesnį teisėto duomenų perėmimo teisėsaugos tikslais teisinės sistemos kūrimą

- Aukšto lygio grupės ekspertai prašo Europos Komisijos įvertinti (prieš atliekant galimą poveikio vertinimą) galimybę parengti ES teisinę priemonę teisėto duomenų perėmimo klausimu, remiantis darbu, atliktu rengiant ES E. įrodymų reglamentą ir direktyvą, ir daugiausia dėmesio sutelkiant į galimų technologiškai neutralių sprendimų nustatymą.

II. Įveikti technologinius iššūkius

Daug teisėsaugos institucijų patiriamų iššūkių, susijusių su prieiga prie duomenų, kyla dėl to, kad joms labai sudėtinga numatyti technologinius pokyčius ir prie jų prisitaikyti. Taip yra todėl, kad, priešingai nei subjektai kituose sektoriuose, pavyzdžiui, gynybos ar kosmoso, teisėsaugos institucijos neturi tam reikalingų išteklių ar tvirtų ryšių su pramone ir nėra įpratę prie poreikio tai daryti. Daugeliu atvejų vidaus saugumo srities subjektai mėgina užpildyti technologines spragas atoveiksmio būdu arba įprastai mėgina patenkinti poreikius naudodami prieinamas ir įperkamas standartines technologijas. Siekiant paskatinti perėjimą nuo reagavimu grindžiamo požiūrio prie proaktyvesnio požiūrio, technologinius iššūkius reikia siekti įveikti taikant struktūrizuotą, į ateitį orientuotą ir daugiadisciplinį požiūrį, siekiant dviejų prioritetų: iš nacionalinių institucijų perspektyvos itin svarbu užtikrinti, kad teisėsauga turėtų galimybes naudotis atitinkamais pajėgumais gauti ir tvarkyti perduodamus duomenis, o operatoriams ir technologijų teikėjams itin svarbu, kad jie galėtų vykdyti savo pareigas, susijusias su prieiga prie duomenų, privatumu ir kibernetiniu saugumu, ir kad būtų išsaugomi jų interesai.

Todėl ekspertai siūlo numatyti technologinius iššūkius įgyvendinant visapusišką ir į ateitį orientuotą politiką, grindžiamą **teisėtos prieigos technologijų veiksmų gairėmis**, kuriose bus nustatyti tikslai ir apibrėžta veikla kartu numatant finansavimą šiems tikslams pasiekti.

Kalbant apie pajėgumų stiprinimą, nors iššūkiai yra skirtingi, ekspertai siūlo laikytis požiūrio, kuris dažnu aspektu yra panašus skaitmeninės ekspertizės, duomenų saugojimo ir teisėto duomenų perėmimo[120] atveju ir kuris yra pagrįstas tomis pačiomis rekomendacijomis, kuriomis tvirtai akcentuojamas reikalavimas parengti tikslais grindžiamą planavimą finansavimo galimybėms orientuoti, glaudžiau dalyvaujant pramonės subjektams ir pagrindiniams suinteresuotiesiems subjektams, pavyzdžiui, Europos vidaus saugumo inovacijų centrui.

Tačiau teisėsaugos ekspertai primygtinai akcentavo du elementus, kurie yra būdingi teisėtam duomenų perėmimui.

- Didesnis metaduomenų – pvz., buvimo vietos duomenų, skambučių įrašų ir el. laiškų antraščių – naudojimas gali suteikti papildomos tyrimui reikalingos nukreipiančios informacijos. **Kadangi vis daugiau įrenginių prisijungia prie interneto, sugeneruotų duomenų kiekis didės, taigi atsiras daugiau galimybių nustatyti elgesio modelius.** Ekspertai paragino vykdyti daugiau mokslinių tyrimų, užtikrinti daugiau inovacijų ir įsisavinti daugiau sprendimų, susijusių su **išplėstiniu metaduomenų naudojimu**, pavyzdžiui, pasitelkiant DI, kaip vieną iš būdų sumažinti prieigos prie turinio duomenų trūkumą. Kartu jie nurodė su privatumu susijusią riziką, kylančią intensyviai naudojant DI masiniams asmens metaduomenims tvarkyti; šią riziką reikia subalansuoti su tiksliniu turinio duomenų naudojimu. Tačiau teisėsaugos ekspertai aiškiai teigia, kad vien metaduomenys negali visiškai pakeisti komunikacijos turinio įrodomosios vertės siekiant įrodyti ketinimą.

- Kai nusikaltėliai naudojasi specialiomis ištisinio šifravimo ryšių platformomis, teisėsaugos institucijos turi naudotis taktiniais sprendimais, grindžiamais **pažeidžiamumo** išnaudojimu, kad gautų prieigą prie įtariamųjų komunikacijos. Keletas teisėsaugos institucijų jau veikia pagal teisinę sistemą, leidžiančią duomenis perimti ryšių galiniuose įrenginiuose, ir turi technologijų tai daryti, tačiau yra erdvės tolesnei pažangai šioje srityje. Tai galėtų apimti paramą ES sukurtų priemonių plėtojimui ir leidimą teisėsaugos institucijoms jas įsigyti ir jas naudoti pagal esamą teisinę sistemą.

  Tačiau teisėsaugos ekspertai pažymėjo, kad šis metodas neturėtų būti išplėstas kaip pirminė įrodymų rinkimo priemonė, kadangi taktinio duomenų perėmimo mastas nėra plėstinas ir toks perėmimas nėra be problemų. Pavyzdžiui, dėl subjekto, kurio atžvilgiu vykdomas tyrimas, buvimo vietos gali kilti klausimų dėl jurisdikcijos. Be to, naudojimasis pažeidžiamumu, kurio negalima atskleisti, neišvengiamai prieštarauja pagrindiniams kibernetinio saugumo principams.

[120] Išsamiai aprašyta skaitmeninei ekspertizei skirtame skyriuje.

Kalbant apie integruotąją teisėtą prieigą, teisėsaugos ekspertai pasiūlė laikytis atsargaus požiūrio, kadangi šios industrijos subjektų neturėtų būti prašoma integruoti jokių sistemų, kurios galėtų bendrai ar sistemiškai susilpninti šifravimą visiems paslaugos naudotojams; teisėta prieiga turėtų ir toliau būti tikslinė, atsižvelgiant į kiekvieną konkretų komunikacijos atvejį. Jie sutarė dėl bendro tikslo aktualumo, tačiau pabrėžė, kad pažangą reikia daryti laipsniškai ir įtraukti visų atitinkamų kategorijų suinteresuotuosius subjektus, įskaitant technologijų, kibernetinio saugumo ir privatumo ekspertus, atsižvelgiant į galimą riziką ir viešų diskusijų opumą. Visų pirma jie primygtinai rekomendavo vadovautis įrodymais grindžiamu požiūriu ir atidžiai įvertinti techninių sprendimų, kurie nesumažintų ryšių kibernetinio saugumo ir nedarytų neigiamo poveikio operatorių kibernetiniam saugumui, prieinamumą.

10 rekomendacijų grupė

Siekdami įveikti su teisėtu duomenų perėmimu susijusius technologinius iššūkius, ekspertai rekomenduoja parengti ***teisėtos prieigos technologijų veiksmų gaires***[121]*, kurios visų pirma:*

1. *sutelks technologijų, kibernetinio saugumo, privatumo, standartizacijos bei saugumo ekspertus ir užtikrins tinkamą koordinavimą, galbūt nustatant nuolatinę struktūrą [22 rekomendacija];*
2. *skatins duomenų gavimo ir prieigos prie duomenų, įskaitant iššifravimo pajėgumus, ir DI grindžiamų duomenų analizės pajėgumų mokslinius tyrimus bei plėtrą ir priemonių diegimą*[122] *[4 rekomendacija];*
3. *skatins koordinuotą požiūrį į standartizavimą, pagal kurį bus atsižvelgiama atitinkamai į teisėtos prieigos prie duomenų poreikius ir taip pat [15, 16 ir 20 rekomendacijos]:*
    a. *skatins visų atitinkamų bendruomenių specialistų dalyvavimą atitinkamose standartizacijos grupėse;*
    b. *papildys būsimas iniciatyvas tinkamomis standartizacijos priemonėmis (siekiant skatinti technologiškai neutralų požiūrį);*
    c. *apims ryšių technologijas apskritai, daiktų internetą (įskaitant, pavyzdžiui, susietuosius automobilius) ir visų formų junglumą (įskaitant, pavyzdžiui, palydovinį ryšį);*
4. *stiprins ES veiksmų koordinavimą su pramone, siekiant spręsti situacijas, kai esama technologinių sprendimų, tačiau jie nėra įgyvendinami; tokiais atvejais*[123] *reikia aiškių gairių ir dialogo, kuriam sąlygos būtų sudarytos ES lygmeniu [24 rekomendacija];*
5. *įgyvendins integruotąją teisėtą prieigą visose atitinkamose technologijose, atsižvelgiant į teisėsaugos institucijų pareikštus poreikius, kartu užtikrinant didelį saugumą ir kibernetinį saugumą ir numatant teisinių pareigų dėl teisėtos prieigos laikymąsi [22 rekomendacija];*
6. *nuodugniai spręs šifravimo problemas šiais būdais:*
    a. *užtikrinant, kad dėl galimų naujų pareigų ir (arba) standartų paslaugų teikėjams nebūtų tiesiogiai ar netiesiogiai nustatytos pareigos susilpninti ryšių saugumą, apskritai pakenkiant ištisiniam šifravimui arba jį susilpninant [23 rekomendacija];*
    b. *užtikrinant, kad integruotoji teisėta prieiga neturėtų neigiamo poveikio jų aparatinės ar programinės įrangos architektūros saugumo būklei [23 rekomendacija];*
    c. *koordinuojant veiksmus ir naudojantis ES finansavimu parengiant tikslinių teisėtos prieigos priemonių rengimo, tvarkymo ir naudojimo metodiką, kad būtų sprendžiami klausimai, susiję su atvejais, kai bendradarbiaujant su elektroninių ryšių tarnybomis prieiga prie duomenų nėra galima [10 rekomendacija].*

---

[121] Technologijų veiksmų gairės turėtų apimti tris darbo kryptis: skaitmeninę ekspertizę, duomenų saugojimą ir teisėtą duomenų perėmimą.

[122] Ši rekomendacija taip pat taikoma prieigai prie duomenų įrenginyje (žr. skaitmeninei ekspertizei skirtą skirsnį), tačiau naudojimo atvejai šiek tiek skiriasi.

[123] Pavyzdžiui, kai susitarimai dėl maršruto parinkimo per savąjį tinklą arba kai konkretus RCS įgyvendinimas nesudaro sąlygų teisėtam duomenų perėmimui.

Nors kai kurios aukšto lygio grupės ekspertų pasiūlytos iniciatyvos iš dalies jau įgyvendinamos, labai reikia technologijų veiksmų gairėse geriau struktūrizuoti technologijų vidutinės trukmės ir ilgojo laikotarpio politiką dėl teisėtos prieigos, siekiant konkrečių tikslų ir taikant susijusią stebėsenos priemonę. Šis požiūris turėtų apimti ne tik prieigą prie perduodamų duomenų, bet ir skaitmeninę ekspertizę ir duomenų saugojimą.

Technologijų veiksmų gairės turėtų būti orientuotos į ateitį, įgyvendinamos, sutelktos į prioritetines temas ir įtvirtintos ES skaitmeninėje strategijoje. Jos turėtų apimti visų atitinkamų kategorijų suinteresuotuosius subjektus, visų pirma ES institucijas, įstaigas ir agentūras, nacionalines valdžios institucijas, visų atitinkamų sričių akademinę bendruomenę, pramonės atstovus ir NVO, glaudžiai bendradarbiaujant, ir jose turėtų būti nustatytas aiškus valdymas.

Pagrindinis veiksmas. Aukšto lygio grupės ekspertai primygtinai ragina Komisiją pateikti ir įgyvendinti prieigos prie duomenų technologijų veiksmų gaires

- Aukšto lygio grupės ekspertai ragina Europos Komisiją parengti ir įgyvendinti technologijų veiksmų gaires, kuriose daugiausia dėmesio būtų skiriama šifravimo iššūkiams, atsižvelgiant į visus susijusius aspektus, įskaitant technologinius, rinkos, kibernetinio saugumo, pagrindinių teisių, standartizacijos, teisėsaugos ir mokslinių tyrimų aspektus. Šios technologijų veiksmų gairės turėtų būti parengtos 2025 m. ir turėtų būti grindžiamos visomis atitinkamomis valstybių narių ir ES institucijų, įstaigų ir agentūrų ekspertinėmis žiniomis, be kita ko, kibernetinio saugumo, duomenų apsaugos ir privatumo srityse.