EUROPOS
KOMISIJA

Briuselis, 2017 01 25
COM(2017) 41 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, EUROPOS VADOVŲ TARYBAI IR TARYBAI

Ketvirtoji pažangos, padarytos kuriant tikrą veiksmingą saugumo sąjungą, ataskaita

Ketvirtoji pažangos, padarytos kuriant tikrą veiksmingą saugumo sąjungą, ataskaita

I. ĮVADAS

Tai ketvirtoji mėnesinė pažangos, padarytos kuriant tikrą veiksmingą saugumo sąjungą, ataskaita; joje apžvelgiami pokyčiai, susiję su dviem pagrindiniais ramsčiais: *kova su terorizmu ir organizuotu nusikalstamumu bei jų rėmimo priemonėmis ir mūsų apsaugos nuo šių grėsmių ir atsparumo joms didinimu.* Šioje ataskaitoje daugiausia dėmesio skiriama keturioms pagrindinėms sritims: informacinėms sistemoms ir sąveikumui, pažeidžiamų taikinių apsaugai, kibernetinėms grėsmėms ir duomenų apsaugai vykdant nusikalstamų veikų tyrimus.

Gruodžio mėn. įvykdytas išpuolis Berlyno Kalėdų mugėje dar kartą pabrėžė didelius mūsų informacinių sistemų trūkumus, kuriuos būtina nedelsiant pašalinti, visų pirma ES lygmeniu, siekiant padėti nacionalinėms sienos apsaugos ir teisėsaugos institucijoms veiksmingiau atlikti jų sunkų darbą vietoje. Kadangi įvairios informacinės sistemos nėra tarpusavyje susietos, išpuolių vykdytojai gali, naudodamiesi keliomis tapatybėmis, judėti neaptikti, be kita ko, per sienas; be to, valstybės narės reguliariai neįkelia šios informacijos į atitinkamas ES duomenų bazes. Visa tai yra praktinio įgyvendinimo trūkumai, kurie turi būti nedelsiant pašalinti. Be to, reikia daugiau nuveikti dėl teisėsaugos priemonių pasienyje ir asmenų, kurių prieglobsčio prašymai buvo atmesti, grąžinimo[1].

Pažeidžiamų taikinių apsaugos srityje Komisija paspartins vykdomą darbą, kad sutelktų valstybių narių ekspertus dalytis geriausia patirtimi ir susitarti dėl standartinių gairių.

Apie ES kylančią kibernetinę grėsmę plačiai kalbama žiniasklaidoje, ir šioje ataskaitoje apžvelgiamos įvairios jau vykdomų veiksmų šioje srityje kryptys. Tai apima ir prevencines priemones (darbą su pramone siekiant didinti pritaikytąjį saugumą (angl. „security by design“) ir įgyvendinti Tinklų ir informacijos saugumo direktyvą), ir valstybių narių tarpusavio bendradarbiavimo ir bendradarbiavimo su tarptautinėmis organizacijomis ir partneriais kovojant su kylančiais kibernetiniais išpuoliais stiprinimą. Per ateinančius mėnesius remdamosi 2013 m. ES kibernetinio saugumo strategija Komisija ir Sąjungos vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai nustatys veiksmus, kurių reikia imtis siekiant ES mastu veiksmingai reaguoti į šias grėsmes.

Asmens privatumo ir asmens duomenų apsauga yra pagrindinė teisė, todėl ji yra visų veiksmų kuriant tikrą saugumo sąjungą pagrindas. 2016 m. balandžio mėn. priimta policijos ir baudžiamosios teisenos srities Duomenų apsaugos direktyva užtikrinamas bendras aukštas duomenų apsaugos standartas, taigi ji sudarys lengvesnes sąlygas valstybių narių teisėsaugos institucijoms sklandžiai keistis svarbiais duomenimis. Komisija taip pat pradėjo persvarstyti E. privatumo direktyvą, kuri yra duomenų dokumentų rinkinio dalis, kad direktyva būtų taikoma visiems elektroninio ryšio tiekėjams ir kad jos nuostatos būtų suderintos su Bendruoju duomenų apsaugos

[1] Komisija per ateinančiais savaites pateiks atnaujintą veiksmų planą grąžinimo srityje; žr. Komisijos ataskaitą Europos Parlamentui, Europos Vadovų Tarybai ir Tarybai dėl Europos sienų ir pakrančių apsaugos pajėgų veiksmingumo didinimo, COM(2017) 42.

reglamentu. Šiuo pasiūlymu siekiama užtikrinti elektroninių ryšių privatumą, kartu nustatant pagrindą, kuriuo remiantis galima numatyti E. privatumo reglamento taikymo srities apribojimus, be kita ko, nacionalinio saugumo arba baudžiamųjų tyrimų sumetimais.

II. INFORMACINIŲ SISTEMŲ IR SĄVEIKUMO STIPRINIMAS

Pirmininko J.-C. Junckerio 2016 m. rugsėjo mėn. pranešime apie Sąjungos padėtį ir 2016 m. gruodžio mėn. Europos Vadovų Tarybos išvadose nurodoma, kad svarbu pašalinti esamus informacijos valdymo trūkumus ir pagerinti **esamų informacinių sistemų sąveikumą ir sujungiamumą**. Pastarojo meto įvykiai dar kartą parodė, kad būtina skubiai susieti esamas ES duomenų bazes, visų pirma vietoje veikiantiems sienos apsaugos ir teisėsaugos pareigūnams suteikti priemonių, reikalingų tapatybės klastojimui nustatyti. Pavyzdžiui, 2016 m. gruodžio mėn. teroro išpuolio Berlyne vykdytojas naudojo bent 14 skirtingų tapatybių ir galėjo nenustatytas keliauti tarp valstybių narių. Akivaizdu, kad siekiant atimti šią galimybę iš teroristų ir nusikaltėlių būtina užtikrinti, kad esamose ir būsimose ES informacinėse sistemose būtų galima vienu metu atlikti paiešką naudojant biometrinius identifikatorius.

Atsižvelgdama į tai, Komisija 2016 m. balandžio mėn. pradėjo rengti pasiūlymą dėl „patikimesnių ir pažangesnių sienų ir saugumo informacinių sistemų“[2]. Jame nustatyta, kad dėl to, kad esamos sistemos buvo sukurtos veikti atskirai, o ne kartu, yra esamų sistemų veikimo trūkumų, ES duomenų valdymo architektūros spragų, sudėtinga skirtingai reglamentuojamų informacinių sistemų įvairovė ir visa apimantis susiskaidymas. Per šį procesą Komisija su ES agentūromis, valstybėmis narėmis ir atitinkamais suinteresuotais subjektais sukūrė **Aukšto lygio informacinių sistemų ir sąveikumo ekspertų grupę**. 2016 m. gruodžio 21 d.[3] pirmininko ataskaitoje pristatytos grupės **tarpinės išvados**, viena iš jų – prioritetinė galimybė sukurti bendrą paieškos portalą, kuriame nacionalinės teisėsaugos ir sienos apsaugos institucijos galėtų vienu metu atlikti paiešką esamose ES duomenų bazėse ir informacinėse sistemose. Tarpinėje ataskaitoje taip pat pabrėžiama duomenų kokybės svarba (kadangi informacinės sistemos yra veiksmingos tik jeigu jose įvesti duomenys yra kokybiški ir tinkamos formos) ir pateikiamos rekomendacijos pagerinti ES sistemose esančių duomenų kokybę taikant automatizuotas duomenų kokybės kontrolės priemones.

Komisija greitai išnagrinės galimybę sukurti bendrą paieškos portalą ir kartu su ES didelės apimties IT sistemų operacijų valdymo agentūra „eu-LISA“ pradės darbą dėl portalo, kuriame būtų galima vienu metu atlikti paiešką visose susijusiose esamose ES sistemose. Susijęs tyrimas turėtų būti atliktas iki birželio mėn. ir juo būtų remiamasi iki metų pabaigos kuriant ir išbandant portalo prototipą. Komisija mano, kad Europolas tuo pačiu metu turėtų tęsti darbą, susijusį su sistemų sąsaja, kuri sudarys sąlygas valstybių narių pasienio pareigūnams atliekant paiešką nacionalinėse sistemose tuo pačiu metu automatiškai ieškoti informacijos Europolo duomenų bazėse.

[2] Komunikatas „Patikimesnės ir pažangesnės sienų ir saugumo informacinės sistemos“, COM(2016) 205 *final*.

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

Informacinių sistemų sąveikumas kuriamas siekiant pašalinti esamą ES sienų kontrolės ir saugumo srities duomenų valdymo architektūros susiskaidymą ir susijusias „akląsias zonas“. Kai duomenų bazės naudoja tą pačią tapatybės duomenų saugyklą, kaip numatyta pagal pasiūlytą ES atvykimo ir išvykimo sistemą ir pasiūlytą Europos kelionių informacijos ir leidimų sistemą (ETIAS), asmuo skirtingose duomenų bazėse gali būti užregistruotas tik pagal vieną tapatybę – tai neleidžia naudotis skirtingomis suklastotomis tapatybėmis. Kaip rekomenduota aukšto lygio ekspertų grupės tarpinėse išvadose Komisija pirmiausia paprašė „eu-LISA“ išanalizuoti techninius ir operacinius bendros biometrinių duomenų atitikties tikrinimo paslaugos įgyvendinimo aspektus. Tokia paslauga suteiktų galimybes atlikti paiešką skirtingose duomenų bazėse naudojant biometrinius duomenis, o tai galėtų padėti aptikti suklastotas tapatybes, kuriomis naudojasi atitinkamas asmuo kitoje sistemoje. Be to, aukšto lygio ekspertų grupė dabar turėtų įvertinti, ar būtina, techniškai įmanoma ir proporcinga taikyti atvykimo ir išvykimo sistemai ir ETIAS numatytą **bendrą tapatybių saugyklą** ir kitoms sistemoms. Be biometrinių duomenų, laikomų biometrinių duomenų atitikties tikrinimo paslaugos sistemoje, tokioje bendroje tapatybių saugykloje būtų saugomi ir raidiniai skaitmeniniai duomenys. Su tuo susijusias išvadas grupė turėtų pateikti galutinėje ataskaitoje iki 2017 m. balandžio mėn. pabaigos.

Dėl pastarojo meto saugumo incidentų išryškėjo poreikis dar kartą persvarstyti **privalomo** valstybių narių **dalijimosi informacija** klausimą. 2016 m. gruodžio mėn. Komisijos pasiūlyme stiprinti **Šengeno informacinę sistemą** pirmą kartą numatyta valstybių narių prievolė skelbti perspėjimus dėl asmenų, susijusių su teroristiniais nusikaltimais. Svarbu, kad teisėkūros institucijos bendradarbiautų, kad pasiūlytos priemonės būtų greitai priimtos. Komisija yra pasirengusi išnagrinėti, ar prievolė dalytis informacija turėtų būti nustatyta dėl kitų ES duomenų bazių.

III. MŪSŲ PAŽEIDŽIAMŲ TAIKINIŲ APSAUGA NUO TERORISTINIŲ IŠPUOLIŲ

Išpuolis Berlyne buvo paskutinysis ES įvykdytas išpuolis prieš vadinamuosius pažeidžiamus taikinius, kurie paprastai yra civilinės paskirties vietos, kuriose susirenka daug žmonių (pvz., viešosios erdvės, ligoninės, mokyklos, sporto arenos, kultūros centrai, kavinės ir restoranai, prekybos centrai ir transporto centrai). Dėl savo pobūdžio šios vietos yra pažeidžiamos ir jas sunku apsaugoti, taip pat yra didelė tikimybė, kad išpuolio metu bus daug aukų. Dėl šių priežasčių tokias vietas pasirenka teroristai. Grėsmė, kad ateityje bus įvykdyta išpuolių prieš pažeidžiamus taikinius, įskaitant transporto priemones, tebėra didelė, kaip patvirtina turimuose vertinimuose, įskaitant Europolo ataskaitą dėl „Da'esh“ veikimo būdų pokyčių[4].

2015 m. Europos saugumo darbotvarkėje ir 2016 m. komunikate dėl saugumo sąjungos pabrėžtas poreikis intensyviau stengtis didinti saugumą ir naudoti naujoviškas aptikimo priemones ir technologijas siekiant apsaugoti pažeidžiamus taikinius. Komisija dėjo pastangas, kad paremtų ir paskatintų valstybes nares dalytis geriausia patirtimi kuriant

[4] 2016 m. lapkričio mėn. Europolo ataskaita „Islamo valstybės veikimo būdų pokyčių apžvalga“ (angl. *Changes in modus operandi of Islamic State (IS) revisited*), Europolo viešos informacijos puslapis, pateikta adresu https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

geresnes išpuolių prieš pažeidžiamus taikinius prevencijos ir reagavimo į juos priemones. Šių pastangų rezultatas – parengti veiklos vadovai ir rekomendacinė medžiaga. Šiuo metu Komisija, glaudžiai bendradarbiaudama su valstybių narių ekspertais, rengia išsamų saugumo procedūrų vadovą ir šablonus, skirtus įvairiems pažeidžiamiems taikiniams (pvz., prekybos centrams, ligoninėms, sporto ir kultūros renginiams). Tikslas – remiantis valstybių narių geriausia patirtimi 2017 m. pradžioje paskelbti valstybėms narėms skirtas pažeidžiamų taikinių apsaugos gaires.

Be to, Komisija vasario mėn. surengs pirmą praktinį seminarą su nacionalinėmis institucijomis pažeidžiamų taikinių apsaugos klausimais, kurio tikslas – pasikeisti informacija ir nustatyti būdus, kaip geriausiai spręsti sudėtingą pažeidžiamų taikinių apsaugos ir viešojo saugumo bei apsaugos klausimą. Taip pat Komisija iš Vidaus saugumo fondo finansuoja bandomąjį Belgijos, Nyderlandų ir Liuksemburgo projektą, kuriuo siekiama sukurti regioninį kompetencijos centrą specialiems teisėsaugos intervenciniams veiksmams; šis centras teiks mokymus policijos pareigūnams, kurie išpuolio atveju dažnai reaguoja pirmiausia.

Reagavimas į išpuolius prieš pažeidžiamus taikinius yra pagrindinė Komisijos darbo civilinės saugos srityje dalis. Gruodžio mėn. Komisija paskelbė, kokių veiksmų ji ketina imtis su valstybėmis narėmis, kad apsaugotų ES piliečius ir sumažintų pažeidžiamumą iškart po teroristinių išpuolių. Šie veiksmai padės sustiprinti visų subjektų, dalyvaujančių šalinant išpuolių padarinius, veiksmų koordinavimą, o Komisija įsipareigojo remti valstybių narių pastangas – rengti bendrus mokymus bei pratybas ir užtikrinti ilgalaikį dialogą esamuose ryšių punktuose ir ekspertų grupėse. Komisija taip pat skatins plėtoti specialius reagavimo į teroristinius išpuolius modulius pagal Sąjungos civilinės saugos mechanizmą ir iniciatyvas, kad būtų dalijamasi įgyta patirtimi ir didinamas visuomenės informuotumas.

Kartu su valstybėmis narėmis Komisija taip pat išnagrinės, kokią paramą ES galėtų sutelkti, kad padėtų didinti galimų pažeidžiamų taikinių atsparumą ir saugumą. Valstybės narės taip pat galėtų prašyti Europos investicijų banko (EIB) (įskaitant Europos strateginių investicijų fondą) finansavimo pagal ES ir EIB grupės politika. Visiems projektams būtų taikoma įprasta teisės aktuose nustatyta sprendimų priėmimo tvarka.

Dėl konkrečių pažeidžiamų taikinių, susijusių su viešomis transporto vietomis, kaip antai viešomis oro uostų ar geležinkelių zonomis, Komisija 2016 m. lapkričio mėn. surengė specialų praktinį seminarą, kuriame dalyvavo įvairūs suinteresuotieji subjektai ir kuriame pabrėžtas poreikis išlaikyti saugumo poreikių, keleivių patogumo ir transporto operacijų pusiausvyrą. Išvadose pabrėžiama, kad svarbu kurti saugumo kultūrą, apimančią ne tik darbuotojus, bet ir keleivius, taip pat svarbu, kad tinkamos atsakomosios priemonės būtų pagrįstos vietos rizikos vertinimais ir kad būtų stiprinami visų dalyvaujančiųjų šalių tarpusavio ryšiai.

IV. KIBERNETINIŲ GRĖSMIŲ KELIAMI IŠŠŪKIAI

Kibernetiniai nusikaltimai ir kibernetiniai išpuoliai yra vieni pagrindinių iššūkių, kylančių Sąjungai, ir siekdami juos įveikti ES lygmeniu galime sustiprinti bendrą savo atsparumą. Kasdien kibernetinio saugumo incidentai daro didelę žalą žmonių gyvenimui ir sukelia didelę ekonominę žalą Europos ekonomikai ir verslui. Kibernetiniai išpuoliai yra viena pagrindinių hibridinių grėsmių dalių – suplanuoti tiksliai kartu su fizinėmis grėsmėmis, pavyzdžiui, teroristiniais išpuoliais, jie gali turėti katastrofiškų padarinių. Jie

taip pat gali prisidėti prie šalies destabilizavimo arba sutrikdyti politinių institucijų ir pagrindinių demokratinių procesų veikimą. Vis labiau esame priklausomi nuo internetinių technologijų, taigi mūsų ypatingos svarbos infrastruktūros objektai (nuo ligoninių iki branduolinių elektrinių) taps vis labiau pažeidžiami.

Nuo 2013 m. ES kibernetinio saugumo strategija yra viena iš pagrindinių politinių priemonių, kuriomis siekiama spręsti kibernetinio saugumo uždavinius. Pagrindinis elementas – pernai liepos mėn. priimta Tinklų ir informacijos saugumo (TIS) direktyva [5] Joje padėtas pagrindas ES lygmens bendradarbiavimui stiprinti ir kibernetiniam atsparumui didinti remiant valstybių narių bendradarbiavimą ir keitimąsi informacija ir skatinant vykdyti operatyvinį bendradarbiavimą kilus konkretiems kibernetinio saugumo incidentams bei keistis informacija apie riziką. Kad direktyva būtų nuosekliai įgyvendinama įvairiuose sektoriuose ir valstybėse narėse, Komisija vasario mėn. surengs pirmą TIS bendradarbiavimo grupės susitikimą su valstybėmis narėmis.

2016 m. balandžio mėn. Komisija ir ES vyriausioji įgaliotinė užsienio reikalams ir saugumo politikai patvirtino Bendrą kovos su mišriomis grėsmėmis sistemą[6], pagal kurią pasiūlyti 22 operatyviniai veiksmai, kuriais siekiama didinti informuotumą, stiprinti atsparumą, geriau reaguoti į krizes ir stiprinti ES ir NATO bendradarbiavimą. Pagal Tarybos raginimą Komisija ir ES vyriausioji įgaliotinė iki 2017 m. liepos mėn. pateiks pažangos vertinimo ataskaitą.

Komisija taip pat propaguoja ir remia technologines naujoves, įskaitant naudojimąsi ES mokslinių tyrimų lėšomis, kad būtų ieškoma naujų sprendimų ir kuriamos naujos technologijos, galinčios padėti stiprinti mūsų atsparumą kibernetiniams išpuoliams (pvz., pritaikytojo saugumo projektai). Praėjusią vasarą pradėjome vykdyti 1,8 mlrd. EUR vertės privačiojo sektoriaus partnerystę su pramone kibernetinio saugumo srityje[7].

Transporto srityje skaitmeninimas tampa vienu pagrindinių veiksnių, lemiančių labai reikalingus dabartinės transporto sistemos pokyčius. Greitas skaitmeninimo tempas teikia daug privalumų, tačiau taip pat daro transporto sistemą pažeidžiamesnę kibernetinio saugumo ar saugos rizikai. Vykdoma įvairių veiksmų siekiant sušvelninti grėsmes įvairiais lygmenimis, ypač aviacijos srityje, taip pat jūrų, upių, geležinkelių ir kelių transporto srityse[8]. Vis dar reikia labiau patikslinti, suderinti ir papildyti veiklą, kurią vykdo skirtingi suinteresuotieji subjektai, atsakingi už įvairių kibernetinio atsparumo aspektų stiprinimą.

Atsižvelgdamos į platesnes aplinkybes ir į tai, kad grėsmės sparčiai kinta, per ateinančius mėnesius Komisija ir ES vyriausioji įgaliotinė nustatys, kokių veiksmų reikia imtis, kad

---

[5] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti.

[6] JOIN(2016) 18.

[7] Paskelbta 2016 m. komunikate dėl kibernetinio atsparumo, COM(2016) 410 *final*.

[8] Pavyzdžiai: tarptautinės gairės, pavyzdžiui, parengtos Tarptautinės jūrų organizacijos, arba neseniai bendra ES ir JAV iniciatyva priimta Tarptautinės civilinės aviacijos (ICAO) rezoliucija; pranešimo apie incidentus sistema, pagal kurią Europos aviacijos saugos agentūra šiuo metu kuria geresnio reagavimo režimą, taip pat pritaikytasis kibernetinis saugumas, taikomas kuriamoms naujoms sistemoms, kaip antai, bendros įmonės SESAR rengiamam Europos oro eismo valdymo planui.

ES mastu būtų galima veiksmingai reaguoti į šias grėsmes, remiantis 2013 m. ES kibernetinio saugumo strategija.

V. ASMENS DUOMENŲ APSAUGA IR VEIKSMINGESNIŲ NUSIKALSTAMŲ VEIKŲ TYRIMŲ RĖMIMAS

Policijos ir baudžiamosios teisenos srities Duomenų apsaugos direktyva[9] yra kovos su terorizmu ir sunkiais nusikaltimais dalis. Remdamosi direktyvoje nustatytais bendrais duomenų apsaugos standartais, valstybių narių teisėsaugos institucijos galės sklandžiai keistis svarbiais duomenimis, o nusikaltimų aukų, liudytojų ir įtariamųjų duomenys bus tinkamai apsaugoti.

Be to, kaip nustatyta 2015 m. balandžio mėn. bendrosios skaitmeninės rinkos strategijoje, siekiant užtikrinti didelį asmenų ir įmonių ryšių konfidencialumą ir vienodas sąlygas visiems rinkos veikėjams, Komisija sausio 11 d. priėmė pasiūlytą **E. privatumo reglamentą** (kuriuo pakeičiama Direktyva 2002/58/EB)[10]. Kaip ir dabartine direktyva, taip ir persvarstytu E. privatumo reglamentu patikslinamas Bendrasis duomenų apsaugos reglamentas[11] ir nustatoma sistema, kuria reglamentuojama privatumo ir asmens duomenų apsauga elektroninių ryšių sektoriuje.

Pagal persvarstytą reglamentą visų elektroninių ryšių duomenys, net jei ryšys nėra pagrindinis, yra laikomi konfidencialiais / riboto naudojimo, nesvarbu, ar jie perduodami naudojant tradicines telekomunikacijų paslaugas ar internetu teikiamas paslaugas (angl. „Over-The Top“ (OTT)), kurios turi tokias pačias funkcijas (pvz., „Skype“ ir „WhatsApp“) ir kurios daugeliui vartotojų dažnai pakeičia įprastų telekomunikacijų operatorių paslaugas[12]. Paslaugų teikėjams nustatytos prievolės apima ne tik pagarbą klientų sprendimams dėl privatumo, kai jų duomenys naudojami, saugomi ir tvarkomi, bet ir prievolę ne ES šalyse įsisteigusiems paslaugų teikėjams paskirti atstovą valstybėje narėje. Tai taip pat suteiks galimybę valstybėms narėms palengvinti teisėsaugos ir teisminių institucijų bendradarbiavimą su paslaugų teikėjais siekiant gauti prieigą prie elektroninių įrodymų (žr. toliau).

Kaip ir pagal šiuo metu galiojančias e. privatumo taisykles, teisėsaugos ir teisminių institucijų prieigai prie svarbios elektroninės informacijos, reikalingos nusikaltimų tyrimams, bus taikoma siūlomo E. privatumo reglamento 11 straipsnyje numatyta

---

9 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. Direktyva įsigaliojo 2016 m. gegužės 5 d. ir turi būti perkelta į valstybių narių nacionalinę teisę iki 2018 m. gegužės 6 d. Kad būtų keičiamasi nuomonėmis apie Policijos direktyvos perkėlimą, Komisija su valstybėmis narėmis sukūrė ekspertų grupę.

10 Privatumo ir elektroninių ryšių reglamentas (COM(2017) 10).

11 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), įsigaliosiantis 2018 m. gegužės 25 d.

12 Tai atitinka požiūrį 2016 m. rugsėjo 14 d. Komisijos pateiktame pasiūlyme dėl direktyvos, kuria nustatomas Europos elektroninių ryšių kodeksas (telekomunikacijų dokumentų rinkinys), COM(2016) 590 *final*.

išimtis[13]. Šia nuostata suteikiama galimybė ES arba nacionalinės teisės aktais apriboti ryšių konfidencialumą, jei tai būtina ir proporcinga nacionalinio saugumo, gynybos, viešojo saugumo ir nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais. Ši nuostata ypač svarbi nacionalinėms **duomenų saugojimo** taisyklėms, t. y. siekiant įpareigoti telekomunikacijų paslaugų teikėjus saugoti ryšių duomenis konkretų laikotarpį, kad su jais būtų galima susipažinti teisėsaugos tikslais, atsižvelgiant į 2014 m. Europos Teisingumo Teismo (ETT) sprendimą panaikinti Duomenų saugojimo direktyvą[14]. Nuo tada nepriimtas nė vienas ES teisės aktas dėl duomenų saugojimo, ir kai kurios valstybės narės priėmė savo nacionalinius duomenų saugojimo įstatymus. Švedijos ir Jungtinės Karalystės duomenų saugojimo įstatymai buvo ginčijami ETT ir jis gruodžio 21 d. priėmė sprendimą *Tele2*[15]. ETT nustatė, kad nacionalinės teisės aktai, pagal kuriuos numatyta, kad kovos su nusikalstamumu reikmėms bendrai ir nediferencijuojant saugomi visi abonentų ir naudotojų srauto ir vietos duomenys, susiję su visomis elektroninio ryšio priemonėmis, yra nesuderinami su ES teise. Šio sprendimo pasekmės analizuojamos ir Komisija parengs gaires, kaip rengti nacionalinius duomenų saugojimo teisės aktus, kad jie atitiktų šį sprendimą.

Nusikaltimai palieka skaitmeninių pėdsakų, kurie gali būti naudingi teismo procese; elektroniniai įtariamųjų ryšiai dažnai yra vieninteliai įrodymai, kuriuos teisėsaugos institucijos ir prokurorai gali surinkti. Tačiau gauti prieigą prie **elektroninių įrodymų,** ypač jei jie laikomi užsienyje arba debesijoje, gali būti techniškai ir teisiškai sudėtinga ir dažnai procedūriškai sunku, o tai trukdo tyrėjams greitai veikti. Siekdama spręsti šias problemas Komisija šiuo metu nagrinėja būdus, kaip leisti tyrėjams gauti tarpvalstybinių elektroninių įrodymų, be kita ko, padaryti savitarpio teisinę pagalbą veiksmingesnę, rasti būdų, kaip tiesiogiai bendradarbiauti su interneto paslaugų teikėjais, ir pasiūlyti jurisdikcijos kibernetinėje erdvėje nustatymo ir vykdymo užtikrinimo kriterijus, visiškai laikantis galiojančių duomenų apsaugos taisyklių.[16]Komisija Teisingumo ir vidaus reikalų taryboje 2016 m. gruodžio 9 d. pristatė padarytą pažangą[17].

Išsamus (ir tebevykstantis) konsultacijų su ekspertais procesas suteikė galimybę Komisijai nustatyti įvairias ir dažnai sudėtingas problemas, susijusias su prieiga prie elektroninių įrodymų, kad ji geriau suprastų esamas valstybių narių taisykles ir praktiką ir nustatytų galimas politikos priemones. Pažangos ataskaitoje apžvelgiamos iki šiol per informacijos rinkimo ir konsultacijų su ekspertais procesą kilusios idėjos, kurias Komisija, bendradarbiaudama su suinteresuotaisiais subjektais, per ateinančius mėnesius

---

[13] Žr. 11 straipsnio 1 dalį „duomenų saugojimo sąlyga“, kuri yra tokia pati kaip ir E. privatumo direktyvos 15 straipsnio formuluotė ir suderinta su Bendruoju duomenų apsaugos reglamentu. Tokiu apribojimu neturi būti keičiama pagrindinių teisių esmė ir jis turi būti būtinas, tinkamas ir proporcingas.

[14] 2014 m. balandžio 8 d. ESTT sprendimas sujungtose bylose C-293/12 ir C-594/12 *Digital Rights Ireland.*

[15] 2016 m. gruodžio 21 d. ESTT sprendimas sujungtose bylose C-203/15 ir C-698/15 *Tele2*.

[16] Kaip įsipareigota Europos saugumo darbotvarkėje (COM(2015) 185 *final*) ir Komisijos komunikate dėl Europos saugumo darbotvarkės įgyvendinimo siekiant kovoti su terorizmu ir sukurti tikrą veiksmingą saugumo sąjungą (COM(2016) 230 *final*).

[17] Savo 2016 m. birželio 9 d. išvadose dėl baudžiamosios teisenos kibernetinėje erdvėje stiprinimo Taryba paragino Komisiją imtis konkrečių veiksmų sukurti bendrą ES požiūrį ir iki 2017 m. birželio mėn. pateikti konkrečius rezultatus.

išsamiau išnagrinės. Kaip paskelbta Komisijos darbo programoje, Komisija 2017 m. pateiks iniciatyvą.

VI. IŠVADA

Kita ataskaita turėtų būti pateikta kovo 1 d., joje bus galima apžvelgti šių ir kitų pagrindinės veiklos krypčių įgyvendinimo pažangą.