Europos Sąjungos
Taryba

Briuselis, 2020 m. lapkričio 24 d.
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

PRANEŠIMAS

nuo:	Pirmininkaujančios valstybės narės
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	12863/20
Dalykas:	Tarybos rezoliucija dėl šifravimo – Saugumas naudojant šifravimą ir saugumas nepaisant šifravimo

Delegacijoms priede pateikiama Tarybos rezoliucija dėl šifravimo.

PRIEDAS

Tarybos rezoliucija dėl šifravimo
Saugumas naudojant šifravimą ir saugumas nepaisant šifravimo

1. Preambulė: saugumas naudojant šifravimą ir saugumas nepaisant šifravimo

Europos Sąjunga visapusiškai remia patikimo šifravimo plėtojimą, įgyvendinimą ir naudojimą. Europos Sąjunga pabrėžia, kad reikia užtikrinti visapusišką pagarbą pagrindinėms ir žmogaus teisėms ir teisinės valstybės principo laikymąsi visuose su šia rezoliucija susijusiuose veiksmuose, vykdomuose tiek internete, tiek realiame gyvenime. Šifravimas yra būtina pagrindinių teisių ir valdžios institucijų, pramonės bei visuomenės skaitmeninio saugumo apsaugos priemonė. Kartu Europos Sąjunga turi užtikrinti kompetentingų saugumo ir baudžiamosios teisenos srities institucijų, pavyzdžiui, teisėsaugos ir teisminių institucijų, galimybes naudotis savo teisėtais įgaliojimais tiek internete, tiek realiame gyvenime, apsaugant mūsų visuomenes ir piliečius.

Remiantis 2020 m. spalio 1–2 d. Europos Vadovų Tarybos išvadomis, *ES naudosis savo priemonėmis ir reguliavimo įgaliojimais siekdama padėti formuoti pasaulines taisykles ir standartus*. Buvo susitarta, kad lėšos pagal ekonomikos gaivinimo ir atsparumo didinimo priemonę bus panaudotos siekiant *stiprinti ES galimybes apsisaugoti nuo kibernetinių grėsmių, kurti saugią ryšių aplinką, visų pirma naudojant kvantinį šifravimą, ir užtikrinti prieigą prie duomenų teisminiais ir teisėsaugos tikslais*.

2. Dabartinis šifravimo naudojimas / šifravimo padėtis

Šiandieniniame pasaulyje šifravimo technologijos vis dažniau naudojamos visose viešojo ir privataus gyvenimo srityse. Tai viena iš priemonių, skirtų apsaugoti piliečius, pilietinę visuomenę, ypatingos svarbos infrastruktūros objektus, žiniasklaidą ir žurnalistus, pramonę ir valdžios institucijas, užtikrinant ryšių ir asmens duomenų privatumą, konfidencialumą, duomenų vientisumą ir prieinamumą: akivaizdu, kad šifravimo technologijos yra naudingos visiems subjektams. ES duomenų apsaugos ir kibernetinio saugumo institucijos yra įvardijusios šifravimą kaip svarbią priemonę, padedančią, pavyzdžiui, apsaugoti asmens duomenis, perduodamus už ES ribų su sąlyga, kad jiems taikomas iš esmės lygiaverčio apsaugos lygio reikalavimas (kaip teigia Teisingumo Teismas, tai yra teisinis duomenų perdavimo reikalavimas)[1]. Ne tik elektroniniai įtaisai ir taikomosios programos yra vis dažniau programuojami taip, kad juose būtų standartiškai šifruojami saugomi naudotojų duomenys, bet ir vis daugiau ryšių kanalų ir duomenų saugojimo paslaugų yra taip pat apsaugomos ištisiniu šifravimu. Tai teigiamai atsispindi intensyvėjančiame ryšių ir taikomųjų programų pramonės atsake – daugumoje tikralaikių pokalbių programėlių ir kitų interneto platformų taip pat yra įdiegtas ištisinis šifravimas.

3. Iššūkiai saugumo užtikrinimo srityje

Skaitmeninis gyvenimas ir kibernetinė erdvė ne tik suteikia didelių galimybių, bet ir kelia didžiulių iššūkių: šiuolaikinių visuomenių skaitmeninimas reiškia ir pažeidžiamumą, ir galimybes naudotis nusikalstamais tikslais. Taigi nusikaltėliai gali įtraukti lengvai prieinamus, standartinius šifravimo sprendimus, skirtus teisėtiems tikslams, į savo *modus operandi*[2].

Tuo pačiu metu teisėsauga vis labiau priklauso nuo prieigos prie elektroninių įrodymų, kad galėtų veiksmingai kovoti su terorizmu, organizuotu nusikalstamumu, vaikų seksualiniu išnaudojimu (visų pirma kalbant apie šio reiškinio internetinius aspektus), taip pat su įvairiausiais kitais kibernetiniais nusikaltimais ir nusikaltimais pasinaudojant kibernetine erdve. Kompetentingoms institucijoms prieiga prie elektroninių įrodymų gali būti itin svarbi net tik siekiant sėkmingai atlikti tyrimus ir taip patraukti nusikaltėlius baudžiamojon atsakomybėn, bet ir apsaugoti aukas ir padėti užtikrinti saugumą.

---

[1] 2020 m. liepos 16 d. Sprendimas byloje C-311/18, *Data Protection Commissioner prieš Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559.

[2] 2020 m. Organizuoto nusikalstamumo internete grėsmės vertinimas, p. 25.

Tačiau esama atvejų, kai prieigos prie elektroninių įrodymų kontekste šifravimas prieigą prie komunikacijos turinio ir tokio turinio analizę padaro labai sudėtinga arba praktiškai neįmanoma nepaisant to, kad prieiga prie tokių duomenų būtų teisėta. Todėl, nepriklausomai nuo atitinkamo meto technologinės aplinkos, itin svarbu išsaugoti kompetentingų saugumo ir baudžiamosios teisenos srities institucijų įgaliojimus, suteikiant joms teisėtą prieigą, kad jos galėtų vykdyti savo užduotis, kaip nustatyta ir leidžiama įstatymu. Tokiais įstatymais, kuriuose numatyti vykdymo užtikrinimo įgaliojimai, visada turi būti visapusiškai paisoma tinkamo proceso ir kitų apsaugos priemonių, taip pat pagrindinių teisių, visų pirma teisės į tai, kad būtų gerbiamas privatus gyvenimas bei komunikacijos slaptumas, ir teisės į asmens duomenų apsaugą.

4. Rasti tinkamą pusiausvyrą

Būtina visapusiškai laikytis saugumo naudojant šifravimą ir saugumo nepaisant šifravimo principo. Europos Sąjunga toliau remia patikimą šifravimą. Šifravimas – tai pasitikėjimo skaitmeninimu ir pagrindinių teisių apsauga garantas ir jis turėtų būti skatinamas bei plėtojamas.

Nepaprastai svarbu naudojant šifravimą užtikrinti komunikacijos privatumą ir saugumą, tuo pačiu metu užtikrinant galimybę kompetentingoms saugumo ir baudžiamosios teisenos srities institucijoms teisėtai susipažinti su atitinkamais duomenimis teisėtais, aiškiai apibrėžtais tikslais kovojant su sunkių formų ir (arba) organizuotu nusikalstamumu ir terorizmu, be kita ko, skaitmeniniame pasaulyje, ir laikytis teisinės valstybės principo. Imantis bet kokių veiksmų šie interesai turi būti kruopščiai derinami su būtinumo, proporcingumo ir subsidiarumo principais.

5. Suvienyti jėgas su technologijų pramone

Kad būtų daroma pažanga, Europos Sąjunga siekia užmegzti aktyvias diskusijas su technologijų pramone, kartu įtraukdama mokslinių tyrimų ir akademinę bendruomenę, kad būtų užtikrintas tolesnis patikimų šifravimo technologijų diegimas ir naudojimas. Kompetentingos institucijos turi turėti galimybę teisėtai ir tikslingai susipažinti su duomenimis, visapusiškai gerbiant pagrindines teises ir laikantis atitinkamų duomenų apsaugos įstatymų, kartu užtikrinant kibernetinį saugumą. Techniniai prieigos prie šifruotų duomenų sprendimai turi atitikti teisėtumo, skaidrumo, būtinumo ir proporcingumo principus, įskaitant pritaikytosios ir standartizuotosios asmens duomenų apsaugos principus.

Kadangi nėra vienintelio būdo užsibrėžtiems tikslams pasiekti, valdžios institucijos, pramonė, mokslinių tyrimų ir akademinė bendruomenė turi skaidriai bendradarbiauti, kad strategiškai sukurtų šią pusiausvyrą.

6. Reguliavimo sistema

Būtų galima toliau vertinti poreikį visoje ES plėtoti reguliavimo sistemą, kuri leistų kompetentingoms institucijoms veiksmingai vykdyti savo veiklos užduotis, kartu apsaugant privatumą, pagrindines teises ir komunikacijos saugumą.

Galimi techniniai sprendimai turės suteikti valdžios institucijoms galimybę naudotis savo tyrimo įgaliojimais, kuriems pagal jų vidaus teisės aktus taikomi proporcingumo, būtinumo ir teisminės priežiūros principai, kartu gerbiant bendras Europos vertybes, užtikrinant pagrindines teises ir išsaugant šifravimo privalumus. Galimi sprendimai turėtų būti rengiami skaidriai, bendradarbiaujant su nacionaliniais ir tarptautiniais ryšių paslaugų teikėjais ir kitais atitinkamais suinteresuotaisiais subjektais. Tokie techniniai sprendimai ir standartai, kaip ir sparti technologinė plėtra apskritai, taip pat pareikalautų nuolat tobulinti kompetentingų institucijų techninius ir veiklos įgūdžius bei kompetenciją, kad jos galėtų pasauliniu mastu veiksmingai reaguoti į skaitmeninimo iššūkius, su kuriais susiduria savo darbe.

7. Inovaciniai tyrimo pajėgumai

Galiausiai, itin svarbu gerinti koordinavimą ES lygmeniu, siekiant:

1) suvienyti visų valstybių narių ir ES institucijų bei įstaigų pastangas;

2) apibrėžti ir nustatyti novatoriškus metodus atsižvelgiant į naujas technologijas;

3) analizuoti tinkamus techninius ir operacinius sprendimus ir

4) rengti specialiai pritaikytus kokybiškus mokymus.

Techniniai ir operaciniai sprendimai, įtvirtinti reguliavimo sistemoje, pagrįstoje teisėtumo, būtinumo ir proporcingumo principais, turėtų būti plėtojami glaudžiai konsultuojantis su paslaugų teikėjais, kitais atitinkamais suinteresuotaisiais subjektais ir visomis atitinkamomis kompetentingomis institucijomis, nors neturėtų būti vieno nustatyto techninio sprendimo prieigai prie šifruotų duomenų suteikti.