Euroopa Liidu
Nõukogu

Brüssel, 24. november 2020
(OR. en)

13084/1/20
REV 1

LIMITE

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

MÄRKUS

Saatja:	Eesistujariik
Saaja:	Delegatsioonid
Eelmise dok nr:	12863/20
Teema:	Nõukogu resolutsioon krüpteerimise kohta – Turvalisus krüpteerimise abil ja krüpteerimisest hoolimata

Delegatsioonidele esitatakse lisas nõukogu resolutsioon krüpteerimise kohta

LISA

Nõukogu resolutsioon krüpteerimise kohta
Turvalisus krüpteerimise abil ja krüpteerimisest hoolimata

1. Preambul: turvalisus krüpteerimise abil ja krüpteerimisest hoolimata

Euroopa Liit toetab täielikult tugeva krüpteerimise arendamist, rakendamist ja kasutamist. Euroopa Liit rõhutab vajadust tagada põhi- ja inimõiguste ning õigusriigi põhimõtte täielik austamine kõigis käesoleva resolutsiooniga seotud tegevustes nii internetis kui ka väljaspool seda. Krüpteerimine on vajalik vahend valitsuste, tööstuse ja ühiskonna põhiõiguste ja digitaalse turvalisuse kaitsmiseks. Samal ajal peab Euroopa Liit tagama julgeoleku- ja kriminaalõiguse valdkonna pädevate asutuste, nt õiguskaitse- ja kohtuasutuste suutlikkuse kasutada oma seaduslikke volitusi nii internetis kui mujal, kaitstes meie ühiskondi ja kodanikke.

Vastavalt Euroopa Ülemkogu 1.–2. oktoobri 2020. aasta järeldustele (EUCO 13/20) *võimendab EL oma vahendeid ja regulatiivseid volitusi, et aidata kujundada ülemaailmseid norme ja standardeid*. Lepiti kokku, et taaste ja vastupidavuse rahastamisvahendi vahendeid kasutatakse selleks, et saavutada muu hulgas järgmisi eesmärke: *suurendada ELi suutlikkust kaitsta ennast küberohtude vastu, pakkuda turvalist kommunikatsioonikeskkonda, eriti kvantkrüpteerimise abil, ja tagada juurdepääs andmetele kohtute tegevuse ja õiguskaitse eesmärgil*.

2. Krüpteerimise praegune kasutamine/olukord

Krüpteerimistehnoloogiat kasutatakse tänapäeval kõigis avaliku ja eraelu valdkondades üha enam. See on vahend üksikisikute, kodanikuühiskonna, elutähtsate taristute, meedia ja ajakirjanike, tööstuse ja valitsuste kaitsmiseks, tagades teabevahetuse ja isikuandmete privaatsuse, konfidentsiaalsuse, andmetervikluse ja kättesaadavuse: see, et kõik osapooled saavad krüpteerimistehnoloogiast kasu, on ilmne. ELi andmekaitse- ja küberturvalisusasutused peavad krüpteerimist oluliseks vahendiks, mis aitab kaitsta näiteks isikuandmeid, mis edastatakse väljapoole ELi, kuid mille suhtes kohaldatakse sisuliselt samaväärse kaitsetaseme nõuet, mis vastavalt Euroopa Kohtu praktikale on õiguslik nõue, mida andmete edastamisel tuleb järgida[1]. Lisaks sellele, et elektroonilisi seadmeid ja rakendusi programmeeritakse üha enam nii, et salvestatud kasutajaandmeid krüpteeritakse vaikimisi, turvatakse ka otspunktkrüpteerimise abil üha rohkem sidekanaleid ja andmesalvestusteenuseid. Selle arvessevõtmine kajastub positiivselt side- ja rakendussektoris, kus enamik kiirsõnumiäppe ja muid veebiplatvorme on samuti rakendanud otspunktkrüpteerimist.

3. Turvalisuse tagamisega seotud väljakutsed

Nn digitaalelu ja küberruum ei paku mitte ainult ulatuslikke võimalusi, vaid tekitab ka märkimisväärseid väljakutseid: tänapäeva ühiskondade digitaliseerimine toob endaga kaasa teatavaid haavatavusi ja võimalusi kuritegelikel eesmärkidel ärakasutamiseks. Seega võivad kurjategijad oma toimimismeetodites kasutusele võtta kergesti kättesaadavad, kasutusvalmis krüpteerimislahendused, mis on välja töötatud õiguspärastel eesmärkidel[2].

Samal ajal sõltub õiguskaitse üha enam juurdepääsust elektroonilistele tõenditele, et võidelda tõhusalt terrorismi, organiseeritud kuritegevuse, laste seksuaalse kuritarvitamise (eelkõige selle internetipõhiste aspektide) ning mitmesuguste muude küberkuritegude ja küberruumi kasutades toime pandud kuritegude vastu. Pädevate asutuste jaoks võib juurdepääs elektroonilistele tõenditele olla oluline mitte ainult selleks, et viia läbi edukaid uurimisi ja seeläbi kurjategijad kohtu alla anda, vaid ka selleks, et kaitsta ohvreid ja aidata tagada julgeolekut.

---

[1] Euroopa Kohtu 16. juuli 2020. aasta otsus kohtuasjas C-311/18, Data Protection Commissioner *vs*. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559.

[2] iOCTA 2020, lk 25

Siiski esineb juhtumeid, kus krüpteerimine muudab elektroonilistele tõenditele juurdepääsu raames juurdepääsu side sisule ja selle analüüsi äärmiselt keeruliseks või praktiliselt võimatuks, vaatamata asjaolule, et juurdepääs sellistele andmetele oleks seaduslik. Sõltumata igapäevasest tehnoloogilisest keskkonnast on seetõttu oluline säilitada pädevate asutuste volitused julgeoleku ja kriminaalõiguse valdkonnas, andes neile seadusliku juurdepääsu oma ülesannete täitmiseks, nagu on õiguses ette nähtud ja lubatud. Sellistes õigusaktides, millega nähakse ette täitmisvolitused, tuleb alati täielikult järgida nõuetekohast menetlust ja muid kaitsemeetmeid, samuti põhiõigusi, eelkõige õigust eraelu austamisele ja teabevahetusele ning õigust isikuandmete kaitsele.

4. Õige tasakaalu saavutamine

Täielikult tuleb järgida põhimõtet, et turvalisus tuleb tagada krüpteerimise abil ja krüpteerimisest hoolimata. Euroopa Liit toetab jätkuvalt tugevat krüpteerimist. Krüpteerimine on pidepunkt digitaliseerimise vastu usalduse loomisel ja põhiõiguste kaitsmisel ning seda tuleks edendada ja arendada.

Äärmiselt oluline on kaitsta krüpteerimise abil side privaatsust ja turvalisust ning samal ajal säilitada julgeoleku ja kriminaalõiguse valdkonna pädevatele asutustele võimalus pääseda õiguspärastel ja selgelt kindlaks määratud eesmärkidel seaduslikult juurde asjakohastele andmetele, et võidelda raske ja/või organiseeritud kuritegevuse ja terrorismiga, sealhulgas digitaalses maailmas, ning kaitsta õigusriigi põhimõtet. Kõigi võetavate meetmete puhul peavad need huvid olema hoolikalt kooskõlas vajalikkuse, proportsionaalsuse ja subsidiaarsuse põhimõttega.

5. Jõudude ühendamine tehnoloogiatööstusega

Oma edasises tegevuses püüab Euroopa Liit seada sisse aktiivse mõttevahetuse tehnoloogiatööstusega, viies samal ajal kokku teadus- ja akadeemilised ringkonnad, et tagada tugeva krüpteerimistehnoloogia jätkuv rakendamine ja kasutamine. Pädevatel asutustel peab andmetele olema seaduslik ja eesmärgipärane juurdepääs, austades täielikult põhiõigusi ja asjakohaseid andmekaitsealaseid õigusnorme ja tagades seejuures küberturvalisuse. Krüpteeritud andmetele juurdepääsu võimaldavad tehnilised lahendused peavad olema kooskõlas seaduslikkuse, läbipaistvuse, vajalikkuse ja proportsionaalsuse põhimõttega, sealhulgas lõimitud ja vaikimisi andmekaitse põhimõttega.

Kuna seatud eesmärkide saavutamiseks ei ole olemas ainult ühte viisi, peavad valitsused ning tööstus-, teadus- ja akadeemilised ringkonnad tegema läbipaistvalt koostööd, et see strateegiline tasakaal saavutada.

6. Õigusraamistik

Põhjalikumalt tuleks hinnata vajadust töötada välja kogu ELi hõlmav õigusraamistik, mis võimaldaks pädevatel asutustel täita tõhusalt oma tegevusülesandeid, kaitstes samas privaatsust, põhiõigusi ja side turvalisust.

Võimalikud tehnilised lahendused peavad ametiasutustel võimaldama kasutada oma uurimisvolitusi, mille suhtes kohaldatakse proportsionaalsuse ja vajalikkuse põhimõtet ja kohtulikku järelevalvet, nagu on sätestatud nende siseriiklikus õiguses, austades samas ühiseid Euroopa väärtusi, kaitstes põhiõigusi ja säilitades krüpteerimise eelised. Võimalikud lahendused tuleks välja töötada läbipaistval viisil koostöös siseriiklike ja rahvusvaheliste sideteenuse pakkujate ja muude asjaomaste sidusrühmadega. Ühtlasi nõuavad sellised tehnilised lahendused ja standardid – ja tehnoloogia kiire areng üldiselt – pädevate asutuste tehniliste ja tegevusoskuste ning eksperditeadmiste pidevat arendamist, et nad saaksid oma töös tõhusalt käsitleda digitaliseerimisega kaasnevaid ülemaailmseid väljakutseid.

7. Innovaatiline uurimissuutlikkus

Ülitähtis on parandada koordineerimist ELi tasandil, eesmärgiga:

1) ühendada kõigi liikmesriikide ning ELi institutsioonide ja asutuste jõupingutused;

2) määratleda ja kehtestada uusi tehnoloogiaid arvesse võtvad innovaatilised lähenemisviisid;

3) analüüsida asjakohaseid tehnilisi ja tegevusega seotud lahendusi; ning

4) pakkuda vajadustest lähtuvat kvaliteetset koolitust.

Tehnilised ja tegevusega seotud lahendused, mille aluseks on seaduslikkuse, vajalikkuse ja proportsionaalsuse põhimõttele tuginev õigusraamistik, tuleks välja töötada tihedas koostöös teenusepakkujate, muude asjaomaste sidusrühmade ja kõigi pädevate asutustega, kuigi krüpteeritud andmetele juurdepääsuks ei tohiks olemas olla ainult ühte ettenähtud tehnilist lahendust.