Eiropas Savienības
Padome

Briselē, 2020. gada 24. novembrī
(OR. en)

13084/1/20
REV 1

LIMITE

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

PIEZĪME

Sūtītājs:	prezidentvalsts
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	12863/20
Temats:	Padomes rezolūcija par šifrēšanu – Drošība, izmantojot šifrēšanu, un drošība, neraugoties uz šifrēšanu

Pielikumā ir pievienota Padomes rezolūcija par šifrēšanu.

PIELIKUMS

Padomes rezolūcija par šifrēšanu

Drošība, izmantojot šifrēšanu, un drošība, neraugoties uz šifrēšanu

1. Preambula. Drošība, izmantojot šifrēšanu, un drošība, neraugoties uz šifrēšanu

Eiropas Savienība pilnībā atbalsta spēcīgas šifrēšanas izstrādi, ieviešanu un izmantošanu. Eiropas Savienība uzsver, ka visās ar šo rezolūciju saistītajās darbībās – gan tiešsaistē, gan bezsaistē – ir jānodrošina pilnīga pamattiesību, cilvēktiesību un tiesiskuma ievērošana. Šifrēšana ir līdzeklis, kas nepieciešams, lai aizsargātu pamattiesības un valdību, rūpniecības un sabiedrības digitālo drošību. Vienlaikus Eiropas Savienībai ir jāgādā par to, lai drošības un krimināljustīcijas jomā kompetentās iestādes, piemēram, tiesībaizsardzības un tiesu iestādes, spētu īstenot savas likumīgās pilnvaras un tādējādi gan tiešsaistē, gan bezsaistē aizsargāt mūsu sabiedrības un iedzīvotājus.

Saskaņā ar Eiropadomes 2020. gada 1. un 2. oktobra secinājumiem (EUCO 13/20) *ES pēc iespējas vairāk izmantos savus rīkus un regulatīvo varu, lai palīdzētu veidot globālos noteikumus un standartus*. Tika panākta vienošanās, ka Atveseļošanas un noturības mehānisma līdzekļus izmantos, lai veicinātu tādu mērķu sasniegšanu kā, piemēram, *palielināt ES spēju aizsargāties pret kiberdraudiem, nodrošināt drošu vidi saziņai, īpaši ar kvantu šifrēšanas palīdzību, un garantēt piekļuvi datiem tiesu iestāžu un tiesībaizsardzības nolūkos*.

2. Pašreizējais šifrēšanas izmantojums/stāvoklis

Mūsdienu pasaulē šifrēšanas tehnoloģija tiek arvien vairāk izmantota visās sabiedriskās un privātās dzīves jomās. Šifrēšana ir līdzeklis, ar ko, garantējot privātumu, konfidencialitāti, datu integritāti un saziņas un persondatu pieejamību, aizsargāt indivīdus, pilsonisko sabiedrību, kritiskās infrastruktūras, plašsaziņas līdzekļus un žurnālistus, rūpniecību un valdības: ir acīmredzams, ka labumu no šifrēšanas tehnoloģijas gūst visas puses. ES datu aizsardzības un kiberdrošības iestādes ir konstatējušas, ka šifrēšana ir svarīgs instruments, kas palīdz, piemēram, aizsargāt persondatus, kuri tiek pārsūtīti ārpus ES, bet uz kuriem attiecas prasība garantēt pēc būtības līdzvērtīgu aizsardzības līmeni, kas saskaņā ar Tiesas spriedumu ir juridiska prasība attiecībā uz datu pārsūtīšanu [1]. Elektroniskās ierīces un lietojumprogrammas tiek arvien vairāk programmētas, lai pēc noklusējuma šifrētu saglabātos lietotāja datus, taču arī aizvien vairāk saziņas kanālu un datu glabāšanas pakalpojumu tiek nodrošināti ar pilnīgu (*end-to-end* (*E2E*)) šifrēšanu. To pozitīvi atspoguļo saziņas un lietojumprogrammu nozares pieaugošā reakcija, proti, arī vairumā tūlītējās ziņapmaiņas lietotņu un citu tiešsaistes platformu ir ieviesta pilnīga šifrēšana.

3. Izaicinājumi saistībā ar drošības garantēšanu

"Digitālā dzīve" un kibertelpa ne tikai sniedz lieliskas iespējas, bet arī rada ievērojamus izaicinājumus: mūsdienu sabiedrības digitalizācija ir saistīta ar zināmu neaizsargātību un rada iespējas datus izmantot noziedzīgos nolūkos. Tādējādi noziedznieki savās darbībās (*modi operandi*) var izmantot viegli pieejamus standarta šifrēšanas risinājumus, kas izstrādāti leģitīmos nolūkos [2].

Vienlaikus tiesībaizsardzība arvien vairāk ir atkarīga no piekļuves elektroniskiem pierādījumiem, lai efektīvi apkarotu terorismu, organizēto noziedzību, seksuālu vardarbību pret bērniem (jo īpaši tās tiešsaistes aspektus), kā arī dažādus citus kibernoziegumus un noziegumus, ko iespējamus dara kibertelpa. Kompetentajām iestādēm piekļuve elektroniskiem pierādījumiem var būt būtiska ne tikai, lai sekmīgi veiktu izmeklēšanu un tādējādi sauktu noziedzniekus pie atbildības, bet arī lai aizsargātu cietušos un palīdzētu garantēt drošību.

---

[1] 2020. gada 16. jūlija spriedums lietā C-311/18, Datu aizsardzības komisārs / *Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559.

[2] *iOCTA*, 2020. gads, 25. lpp.

Tomēr ir gadījumi, kad šifrēšana piekļuvi saziņas saturam un tā analīzi saistībā ar piekļuvi elektroniskiem pierādījumiem padara ārkārtīgi sarežģītu vai praktiski neiespējamu, neraugoties uz to, ka piekļuve šādiem datiem būtu likumīga. Tādēļ neatkarīgi no mūsdienu tehnoloģiskās vides ir būtiski saglabāt drošības un krimināljustīcijas jomā kompetento iestāžu pilnvaras, lai tās, izmantojot likumīgu piekļuvi, varētu veikt savus uzdevumus, kā noteikts un atļauts tiesību aktos. Šādos tiesību aktos, kuros paredzētas izpildes pilnvaras, vienmēr ir pilnībā jāievēro pienācīgs process un citi aizsardzības pasākumi, kā arī pamattiesības, jo īpaši tiesības uz privātās dzīves un saziņas neaizskaramību un tiesības uz persondatu aizsardzību.

4. Panākt pareizo līdzsvaru

Ir pilnībā jāievēro princips "drošība, izmantojot šifrēšanu, un drošība, neraugoties uz šifrēšanu". Eiropas Savienība turpina atbalstīt spēcīgu šifrēšanu. Uz šifrēšanu balstās uzticēšanās digitalizācijai un pamattiesību aizsardzībai, un tā būtu jāsekmē un jāpilnveido.

Ārkārtīgi svarīgi ir ar šifrēšanas palīdzību aizsargāt privātumu un saziņas drošību un vienlaikus drošības un krimināljustīcijas jomā kompetentajām iestādēm nodrošināt iespēju likumīgi piekļūt attiecīgiem datiem leģitīmos un skaidri noteiktos nolūkos, lai apkarotu smagus noziegumus un/vai organizēto noziedzību, kā arī terorismu, tostarp digitālajā pasaulē, un atbalstīt tiesiskumu. Visos veiktajos pasākumos šīm interesēm jābūt rūpīgi izlīdzsvarotām ar nepieciešamības, proporcionalitātes un subsidiaritātes principiem.

5. Apvienot spēkus ar tehnoloģiju nozari

Virzoties uz priekšu, Eiropas Savienība cenšas veidot aktīvu diskusiju ar tehnoloģiju nozari, vienlaikus iesaistot pētniekus un akadēmiskās aprindas, lai nodrošinātu nepārtrauktu spēcīgas šifrēšanas tehnoloģijas ieviešanu un izmantošanu. Kompetentajām iestādēm ir jāspēj likumīgi un mērķtiecīgi piekļūt datiem, pilnībā ievērojot pamattiesības un attiecīgos datu aizsardzības tiesību aktus un vienlaikus atbalstot kiberdrošību. Tehniskiem risinājumiem, kuru mērķis ir iegūt piekļuvi šifrētiem datiem, jāatbilst likumības, pārredzamības, nepieciešamības un proporcionalitātes principiem, tostarp integrētai persondatu aizsardzībai un persondatu aizsardzībai pēc noklusējuma.

Tā kā nav viena veida, kā sasniegt izvirzītos mērķus, valdībām, rūpniecībai, pētniecībai un akadēmiskajām aprindām ir pārredzami jāsadarbojas, lai stratēģiski radītu šo līdzsvaru.

6. Tiesiskais regulējums

Varētu turpināt izvērtēt nepieciešamību visā ES izstrādāt tiesisko regulējumu, kas kompetentajām iestādēm ļautu efektīvi veikt savus operatīvos uzdevumus, vienlaikus aizsargājot privātumu, pamattiesības un saziņas drošību.

Ar iespējamiem tehniskiem risinājumiem būs jānodrošina, ka iestādes var izmantot savas izmeklēšanas pilnvaras, uz kurām saskaņā ar valsts tiesību aktiem attiecas proporcionalitātes un nepieciešamības principi un tiesu iestāžu veikta pārraudzība, vienlaikus ievērojot Eiropas kopējās vērtības, iestājoties par pamattiesībām un saglabājot šifrēšanas priekšrocības. Iespējamie risinājumi būtu jāizstrādā pārredzamā veidā sadarbībā ar valsts un starptautiskiem sakaru pakalpojumu sniedzējiem un citām attiecīgajām ieinteresētajām personām. Saistībā ar šādiem tehniskiem risinājumiem un standartiem – un straujo tehnoloģiju attīstību kopumā – būtu arī nepārtraukti jāuzlabo kompetento iestāžu tehniskās un operatīvās prasmes un speciālās zināšanas, lai tās savā darbā globālā mērogā sekmīgi tiktu galā ar digitalizācijas radītajiem izaicinājumiem.

7. Inovatīvas izmeklēšanas spējas

Visbeidzot, ir ārkārtīgi svarīgi uzlabot koordināciju ES līmenī ar mērķi:

1) apvienot visu dalībvalstu un ES iestāžu un struktūru centienus,

2) noteikt un ieviest inovatīvas pieejas, ņemot vērā jaunās tehnoloģijas,

3) analizēt atbilstīgus tehniskos un operatīvos risinājumus un

4) nodrošināt speciāli pielāgotu kvalitatīvu apmācību.

Tehniskie un operatīvie risinājumi, kas balstās uz tiesisko regulējumu, kura pamatā ir likumības, nepieciešamības un proporcionalitātes principi, būtu jāizstrādā, rūpīgi konsultējoties ar pakalpojumu sniedzējiem, citām attiecīgajām ieinteresētajām personām un visām attiecīgajām kompetentajām iestādēm, kaut arī nevajadzētu būt vienam noteiktam tehniskam risinājumam, ar ko nodrošina piekļuvi šifrētiem datiem.