Svet
Evropske unije

PUBLIC

Bruselj, 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

DOPIS

Pošiljatelj:	predsedstvo
Prejemnik:	delegacije
Št. predh. dok.:	12863/20
Zadeva:	Resolucija Sveta o šifriranju – varnost s pomočjo šifriranja in varnost kljub šifriranju

V prilogi vam pošiljamo resolucijo Sveta o šifriranju.

PRILOGA

Resolucija Sveta o šifriranju

Varnost s pomočjo šifriranja in varnost kljub šifriranju

1. Preambula: Varnost s pomočjo šifriranja in varnost kljub šifriranju

Evropska unija v celoti podpira razvoj, uvedbo in uporabo močnega šifriranja. Evropska unija poudarja, da je treba zagotoviti dosledno spoštovanje temeljnih in človekovih pravic ter pravne države pri vseh ukrepih, povezanih s to resolucijo, tako na spletu kot sicer. Šifriranje je nepogrešljivo sredstvo za zaščito temeljnih pravic in digitalne varnosti vlad, industrije in družbe. Hkrati mora Evropska unija zagotoviti, da lahko pristojni organi na področju varnosti in kazenskega pravosodja, npr. organi kazenskega pregona in pravosodni organi, izvajajo svoja zakonita pooblastila tako na spletu kot sicer ter na ta način varujejo naše družbe in državljane.

V skladu s sklepi Evropskega sveta z dne 1. in 2. oktobra 2020 (EUCO 13/20) bo EU *s pomočjo svojih orodij in regulativnih pristojnosti pripomogla k oblikovanju globalnih pravil in standardov*. Dogovorjeno je bilo, da se bodo sredstva iz mehanizma za okrevanje in odpornost namenila za cilje, kot je *krepitev zmožnosti EU, da se zaščiti pred kibernetskimi grožnjami, zagotovi varno komunikacijsko okolje, zlasti prek kvantnega šifriranja, in dostop do podatkov za namene pravosodja in kazenskega pregona*.

2. Zdajšnja uporaba/stanje glede šifriranja

V sodobnem svetu se šifrirna tehnologija vse bolj uporablja na vseh področjih javnega in zasebnega življenja. Je sredstvo za zaščito posameznikov, civilne družbe, kritičnih infrastruktur, medijev in novinarjev, industrije in vlad, ki zagotavlja zasebnost, zaupnost, integriteto podatkov in razpoložljivost komunikacij in osebnih podatkov: jasno je, da šifrirna tehnologija šifriranja prinaša koristi vsem stranem. Organi EU za varstvo podatkov in kibernetsko varnost so šifriranje opredelili kot pomembno orodje, ki na primer prispeva k varstvu osebnih podatkov, prenesenih iz EU, za katere pa je v bistvu treba zagotoviti enako raven varstva, kar je po mnenju Sodišča pravna zahteva za prenos podatkov[1]. Elektronske naprave in aplikacije so vedno pogosteje programirane za privzeto šifriranje shranjenih uporabniških podatkov, poleg tega je čedalje več komunikacijskih kanalov in storitev shranjevanja podatkov zavarovanih tudi s šifriranjem od konca do konca (E2E). To se pozitivno odraža v vse večjem odzivu industrije komunikacij in aplikacij, ki je tudi pri večini aplikacij za takojšnje sporočanje in drugih spletnih platform uvedla šifriranje od konca do konca.

3. Izzivi pri zagotavljanju varnosti

„Digitalno življenje“ in kibernetski prostor sta ne le izjemna priložnost, temveč tudi precejšen izziv: digitalizacija sodobne družbe s seboj prinaša določeno mero ranljivosti in omogoča zlorabo za kriminalne namene. Kriminalci se lahko tako pri svojem delovanju poslužujejo enostavno dostopnih, standardnih rešitev za šifriranje, zasnovanih za legitimne namene[2].

Hkrati organi kazenskega pregona za učinkovit boj proti terorizmu, organiziranemu kriminalu, spolni zlorabi otrok (zlasti njenim spletnim vidikom) ter vrsti drugih oblik kibernetske kriminalitete in kibernetsko omogočenih kaznivih dejanj vse bolj potrebujejo dostop do elektronskih dokazov. Za pristojne organe je dostop do elektronskih dokazov lahko ključnega pomena, ne le za izvajanje uspešnih preiskav in s tem privedbo storilcev kaznivih dejanj pred sodišče, temveč tudi za zaščito žrtev in zagotavljanje varnosti.

---

1 Sodba z dne 16. julija 2020 v zadevi C-311/18, Data Protection Commissioner proti Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

2 iOCTA 2020, str. 25.

Vendar pa sta v nekaterih primerih zaradi šifriranja dostop do vsebine komunikacij in njena analiza v okviru dostopa do elektronskih dokazov izjemno zahtevna ali praktično nemogoča, kljub temu da bi bil dostop do takih podatkov zakonit. Zato je bistveno, da pristojni organi na področju varnosti in kazenskega pravosodja neodvisno od aktualnega tehnološkega okolja ohranijo pooblastila z zakonitim dostopom za opravljanje njihovih nalog, kot je določeno in dovoljeno z zakonom. Taki zakoni, ki določajo izvršilna pooblastila, morajo vedno v celoti spoštovati predpisane postopke in druge zaščitne ukrepe ter temeljne pravice, zlasti pravico do spoštovanja zasebnega življenja in komunikacij ter pravico do varstva osebnih podatkov.

4. Vzpostavitev pravega ravnovesja

Načelo varnosti s pomočjo šifriranja in varnosti kljub šifriranju je treba v celoti spoštovati. Evropska unija še naprej podpira močno šifriranje. Na šifriranju temelji zaupanje v digitalizacijo in varstvo temeljnih pravic ter bi ga bilo treba spodbujati in razvijati.

Izjemno pomembno je, da se s šifriranjem varujeta zasebnost in varnost komunikacij ter da se hkrati pristojnim organom na področju varnosti in kazenskega pravosodja zagotovi, da lahko v legitimne, jasno določene namene v boju proti hudim kaznivim dejanjem in/ali organiziranemu kriminalu in terorizmu, tudi v digitalnem okolju, zakonito dostopajo do relevantnih podatkov, pri čemer mora biti zagotovljeno tudi spoštovanje pravne države. Pri vseh dejavnostih je treba te interese skrbno uravnovesiti z načeli nujnosti, sorazmernosti in subsidiarnosti.

5. Združitev moči s tehnološko industrijo

Evropska unija si v naslednji fazi prizadeva za dejavno razpravo s tehnološko industrijo, s povezovanjem raziskovalnih in akademskih krogov, da bi zagotovila kontinuirano uvajanje in uporabo močne šifrirne tehnologije. Pristojnim organom je treba omogočiti zakonit in ciljno usmerjen dostop do podatkov, ob doslednem spoštovanju temeljnih pravic in ustrezne zakonodaje o varstvu podatkov, pri čemer je treba zagotoviti kibernetsko varnost. Tehnične rešitve za dostop do šifriranih podatkov morajo biti skladne z načeli zakonitosti, preglednosti, nujnosti in sorazmernosti, vključno z vgrajenim in privzetim varstvom osebnih podatkov.

Ker za doseganje zastavljenih ciljev ni enega samega načina, morajo vlade, industrija ter raziskovalna in akademska skupnost to ravnovesje strateško vzpostaviti s preglednim sodelovanjem.

6. Regulativni okvir

Natančneje bi lahko preučili, ali je treba na ravni EU oblikovati regulativni okvir, ki bi pristojnim organom omogočal učinkovito izvajanje njihovih operativnih nalog ob varovanju zasebnosti, temeljnih pravic in varnosti komunikacij.

Morebitne tehnične rešitve bodo morale organom omogočiti, da uporabljajo svoja preiskovalna pooblastila, za katera veljajo načeli sorazmernosti in nujnosti ter sodni nadzor v skladu z nacionalno zakonodajo, hkrati pa bodo morale zagotavljati spoštovanje skupnih evropskih vrednot in temeljnih pravic ter ohranjati prednosti šifriranja. Morebitne rešitve bi bilo treba razviti na pregleden način in v sodelovanju z nacionalnimi in mednarodnimi ponudniki komunikacijskih storitev ter drugimi ustreznimi deležniki. Pri takih tehničnih rešitvah in standardih – ter hitrem tehnološkem razvoju na splošno – bi bilo treba tudi nenehno izpopolnjevati tehnična in operativna znanja in spretnosti ter strokovno znanje prisojnih organov, da bi se ti lahko pri svojem delu na svetovni ravni učinkovito spoprijemali z izzivi digitalizacije.

7. Inovativne preiskovalne zmogljivosti

Nenazadnje je nujno treba izboljšati usklajevanje na ravni EU, da bi:

1) združili prizadevanja vseh držav članic ter institucij in organov EU;

2) določili in uvedli inovativne pristope ob upoštevanju novih tehnologij;

3) analizirali ustrezne tehnične in operativne rešitve ter

4) zagotovili prilagojeno visokokakovostno usposabljanje.

Pri razvoju tehničnih in operativnih rešitev, umeščenih v regulativni okvir, ki temelji na načelih zakonitosti, nujnosti in sorazmernosti, bi se bilo treba tesno posvetovati s ponudniki storitev, drugimi ustreznimi deležniki in vsemi ustreznimi pristojnimi organi, pri tem pa ne bi smeli predpisati enotne tehnične rešitve za zagotavljanje dostopa do šifriranih podatkov.