Vijeće
Europske unije

Bruxelles, 24. studenoga 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

NAPOMENA

Od:	Predsjedništvo
Za:	Delegacije
Br. preth. dok.:	12863/20
Predmet:	Rezolucija Vijeća o šifriranju – Sigurnost s pomoću šifriranja i sigurnost unatoč šifriranju

Za delegacije se u prilogu nalazi Rezolucija Vijeća o šifriranju.

PRILOG

Rezolucija Vijeća o šifriranju
Sigurnost s pomoću šifriranja i sigurnost unatoč šifriranju

1. Preambula: Sigurnost s pomoću šifriranja i sigurnost unatoč šifriranju

Europska unija u potpunosti podupire razvoj, provedbu i upotrebu snažnog šifriranja. Naglašava da je potrebno osigurati puno poštovanje temeljnih i ljudskih prava te vladavine prava u svim djelovanjima povezanima s ovom rezolucijom, na internetu i izvan njega. Šifriranje je neophodno sredstvo za zaštitu temeljnih prava i digitalne sigurnosti vlada, industrije i društva. Europska unija istodobno treba osigurati da nadležna tijela u području sigurnosti i kaznenog pravosuđa, npr. tijela za izvršavanje zakonodavstva i pravosudnih tijela, mogu izvršavati svoje zakonite ovlasti na internetu i izvan njega i tako štititi naša društva i građane.

U skladu sa zaključcima Europskog vijeća od 1. i 2. listopada 2020. (EUCO 13/20) *EU će se poslužiti svojim alatima i regulatornim ovlastima kako bi pomogao u oblikovanju globalnih pravila i standarda*. Dogovoreno je da će se sredstva u okviru Mehanizma za oporavak i otpornost upotrijebiti za ostvarivanje ciljeva kao što su *jačanje sposobnosti EU-a da se štiti od kiberprijetnji, osigura sigurno komunikacijsko okružje, pogotovo kvantnim šifriranjem, i osigura pristup podacima za pravosudne potrebe i potrebe izvršavanja zakonodavstva*.

2. Aktualna upotreba šifriranja / trenutačno stanje u vezi s njime

U današnjem se svijetu tehnologija šifriranja sve više upotrebljava u svim područjima javnog i privatnog života. Sredstvo je za zaštitu pojedinaca, civilnog društva, kritičnih infrastruktura, medija i novinara, industrije i vlada kojim se osigurava privatnost, povjerljivost, cjelovitost podataka i dostupnost komunikacije i osobnih podataka: očito je da sve strane ostvaruju koristi od tehnologije šifriranja. EU-ova tijela za zaštitu podataka i kibersigurnost utvrdila su da je šifriranje važan alat kojim se, primjerice, doprinosi zaštiti osobnih podataka koji se prenose izvan EU-a, a koji podliježu obvezi da se osigura u načelu istovjetna razina zaštite, što je, prema mišljenju Suda pravni zahtjev za prijenos podataka[1]. Elektronički uređaji i aplikacije sve se više programiraju tako da se pohranjeni korisnički podaci automatski šifriraju, a sve je više komunikacijskih kanala i usluga pohrane podataka također zaštićenih prolaznim šifriranjem. To se pozitivno odražava u sve većem odazivu industrije komunikacija i aplikacija koja je prolazno šifriranje provela i u većini aplikacija za trenutačnu razmjenu poruka i drugim internetskim platformama.

3. Izazovi u osiguravanju sigurnosti

„Digitalni život" i kiberprostor nisu samo izvrsna prilika nego i velik izazov: digitalizacija modernog društva donosi određene slabosti i mogućnost iskorištavanja u kriminalne svrhe. Stoga se kriminalci u svom radu mogu koristiti lako dostupnim standardnim rješenjima za šifriranje osmišljenim za legitimne svrhe[2].

Istodobno tijela za izvršavanje zakonodavstva sve više ovise o pristupu elektroničkim dokazima kako bi se učinkovito borila protiv terorizma, organiziranog kriminala, seksualnog zlostavljanja djece (osobito njegovih internetskih aspekata) te niza drugih oblika kiberkriminaliteta i kaznenih djela omogućenih kibertehnologijama. Pristup elektroničkim dokazima može nadležnim tijelima biti od ključne važnosti, i to ne samo za provođenje uspješnih istraga i privođenje kriminalaca pravdi, nego i za zaštitu žrtava i osiguravanje sigurnosti.

---

[1] Presuda od 16. srpnja 2020. u predmetu C-311/18, Data Protection Commissioner protiv Facebook Ireland Ltd i Maximilliana Schremsa, ECLI:EU:C:2020:559:

[2] iOCTA 2020., str. 25.

Međutim, postoje slučajevi u kojima su zbog šifriranja pristup sadržaju komunikacije i njegova analiza u okviru pristupa elektroničkim dokazima krajnje zahtjevni ili praktički nemogući iako bi pristup takvim podacima bio zakonit. Stoga je ključno da se zakonitim pristupom za obavljanje zadaća očuvaju ovlasti nadležnih tijela u području sigurnosti i kaznenog pravosuđa, kako je to propisano i dopušteno zakonom, neovisno o trenutačnom tehnološkom okružju. Takvi zakoni kojima se predviđaju izvršne ovlasti moraju uvijek u potpunosti poštovati zakonito postupanje i druge zaštitne mjere, kao i temeljna prava, a osobito pravo na poštovanje privatnog života i komunikacija te pravo na zaštitu osobnih podataka.

4. Postizanje odgovarajuće ravnoteže

Načelo sigurnosti s pomoću šifriranja i sigurnosti unatoč šifriranju mora se poštovati u cijelosti. Europska unija nastavlja podupirati snažno šifriranje. Na šifriranju se temelji povjerenje u digitalizaciju i zaštitu temeljnih prava te bi ga trebalo promicati i razvijati.

Iznimno je važno da se šifriranjem štite privatnost i sigurnost komunikacije, a da se pritom nadležnim tijelima u području sigurnosti i kaznenog pravosuđa osigura mogućnost zakonitog pristupa relevantnim podacima u legitimne, jasno definirane svrhe u borbi protiv teških kaznenih djela i/ili kaznenih djela organiziranog kriminala i terorizma, među ostalim u digitalnom svijetu, te da se poštuje vladavina prava. U svim poduzetim djelovanja treba se pažljivo uspostaviti ravnoteža između tih interesa i načela nužnosti, proporcionalnosti i supsidijarnosti.

5. Udruživanje snaga s tehnološkom industrijom

Europska unija u ostvarivanju napretka nastoji pokrenuti aktivnu raspravu s tehnološkom industrijom, uz pridruživanje istraživačke i akademske zajednice, kako bi osigurala kontinuiranu provedbu i upotrebu tehnologije snažnog šifriranja. Nadležnim tijelima mora biti omogućen zakoniti i ciljan pristup podacima, uz puno poštovanje temeljnih prava i relevantnih zakona o zaštiti podataka te istodobno očuvanje kibersigurnosti. Tehnička rješenja za pristup šifriranim podacima moraju biti u skladu s načelima zakonitosti, transparentnosti, nužnosti i proporcionalnosti, uključujući tehničku i integriranu zaštitu osobnih podataka.

Budući da ne postoji jedinstveni način za postizanje utvrđenih ciljeva, vlade, industrija, istraživačka i akademska zajednica moraju transparentno surađivati kako bi se na strateški način postigla ta ravnoteža.

6. Regulatorni okvir

Mogla bi se dodatno procijeniti potreba za izradom regulatornog okvira na razini EU-a kojim bi se nadležnim tijelima omogućilo da učinkovito obavljaju svoje operativne zadaće, uz istodobnu zaštitu privatnosti, temeljnih prava i sigurnosti komunikacije.

Mogućim tehničkim rješenjima morat će se tijelima omogućiti da izvršavaju svoje istražne ovlasti koje podliježu načelima proporcionalnosti i nužnosti te sudskom nadzoru u skladu s nacionalnim zakonodavstvom, uz istodobno poštovanje zajedničkih europskih vrijednosti i temeljnih prava te očuvanje prednosti šifriranja. Moguća rješenja trebalo bi razvijati na transparentan način u suradnji s nacionalnim i međunarodnim pružateljima komunikacijskih usluga i drugim relevantnim dionicima. Takva tehnička rješenja i standardi, kao i brz razvoj tehnologije općenito, iziskivali bi i kontinuirano unaprjeđenje tehničkih i operativnih vještina i stručnog znanja nadležnih tijela kako se bi u svojem radu učinkovito suočavali s izazovima digitalizacije na svjetskoj razini.

7. Inovativni istražni kapaciteti

Od iznimne je važnosti poboljšati koordinaciju na razini EU-a u cilju:

1) objedinjavanja napora svih država članica i institucija i tijela EU-a;

2) osmišljavanja i uspostave inovativnih pristupa s obzirom na nove tehnologije;

3) analize odgovarajućih tehničkih i operativnih rješenja i

4) osiguravanja prilagođenog visokokvalitetnog osposobljavanja.

Tehnička i operativna rješenja s uporištem u regulatornom okviru koji se temelji na načelima zakonitosti, nužnosti i proporcionalnosti trebalo bi razvijati uz blisko savjetovanje s pružateljima usluga, drugim relevantnim dionicima i svim relevantnim nadležnim tijelima, iako se pritom ne bi trebalo propisati jedinstveno tehničko rješenje za pružanje pristupa šifriranim podacima.