

V Bruseli 24. novembra 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

**POZNÁMKA**

|                  |                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------|
| Od:              | Predsedníctvo                                                                                      |
| Komu:            | Delegácie                                                                                          |
| Č. predch. dok.: | 12863/20                                                                                           |
| Predmet:         | Závery Rady o šifrovaní<br>– bezpečnosť prostredníctvom šifrovania a bezpečnosť napriek šifrovaniu |

Delegáciám v prílohe zasielame závery Rady o šifrovaní.

**Závery Rady o šifrovaní**

**Bezpečnosť prostredníctvom šifrovania a bezpečnosť napriek šifrovaniu**

1. Preambula: Bezpečnosť prostredníctvom šifrovania a bezpečnosť napriek šifrovaniu

Európska únia plne podporuje vývoj, implementáciu a využívanie silného šifrovania. Európska únia zdôrazňuje, že je potrebné zabezpečiť úplné dodržiavanie základných a ľudských práv a zásad právneho štátu vo všetkých opatreniach súvisiacich s týmto uznesením, a to online aj offline. Šifrovanie je prostriedkom potrebným na ochranu základných práv a digitálnej bezpečnosti vlád, príslušných odvetví a spoločnosti. Európska únia zároveň musí zabezpečiť, aby príslušné orgány v oblasti bezpečnosti a trestnej justície, napr. orgány presadzovania práva a justičné orgány, boli schopné vykonávať svoje zákonné právomoci online aj offline a chrániť pritom naše spoločnosti a občanov.

Podľa záverov Európskej rady z 1. – 2. októbra 2020 (EUCO 13/20) *EÚ využije svoje nástroje a regulačné právomoci na to, aby pomohla pri formovaní globálnych pravidiel a noriem. Dohodlo sa, že finančné prostriedky Mechanizmu na podporu obnovy a odolnosti sa využijú na plnenie cieľov, ako je napríklad posilnenie schopnosti EÚ chrániť sa pred kybernetickými hrozbami, zaistiť bezpečné komunikačné prostredie, najmä prostredníctvom kvantového šifrovania, a zabezpečiť prístup k údajom na justičné účely a na účely presadzovania práva.*

## 2. Využívanie a stav šifrovania v súčasnosti

V dnešnom svete sa technológia šifrovania čoraz viac využíva vo všetkých oblastiach verejného a súkromného života. Je nástrojom ochrany fyzických osôb, občianskej spoločnosti, kritickej infraštruktúry, médií a novinárov, priemyslu a vlád prostredníctvom zaistenia súkromia, dôvernosti, integrity údajov a dostupnosti komunikácie a osobných údajov: je zrejmé, že technológia šifrovania je prínosom pre všetkých. Orgány EÚ pre ochranu údajov a kybernetickú bezpečnosť označili šifrovanie za dôležitý nástroj, ktorý prispieva napríklad k ochrane osobných údajov prenášaných mimo EÚ, na ktoré sa ale vzťahuje požiadavka v podstate rovnocennej úrovne ochrany, ktorá je podľa Súdneho dvora zákonnou požiadavkou vzťahujúcou sa na prenos údajov<sup>1</sup>. Elektronické zariadenia a aplikácie sú nielenže čoraz častejšie naprogramované na štandardné šifrovanie uchovávaných údajov používateľov, ale čoraz viac komunikačných kanálov a služieb uchovávaných údajov je tiež zabezpečených šifrovaním medzi koncovými zariadeniami (E2E). To sa pozitívne odráža v rastúcej reakcii odvetvia komunikácií a aplikácií, v ktorom aj väčšina aplikácií na posielanie rýchlych správ a iné online platformy zaviedli šifrovanie medzi koncovými zariadeniami.

## 3. Výzvy spojené so zaistením bezpečnosti

„Digitálny život“ a kybernetický priestor nepredstavujú len veľké príležitosti, ale aj značné výzvy: digitalizácia moderných spoločností so sebou prináša určité slabé miesta a potenciál na zneužívanie na účely trestnej činnosti. Zločinci tak môžu do svojich *modi operandi* začleniť ľahko dostupné hotové šifrovacie riešenia vytvorené na legitímne účely<sup>2</sup>.

Zároveň je presadzovanie práva čoraz viac závislé od prístupu k elektronickým dôkazom s cieľom účinne bojovať proti terorizmu, organizovanej trestnej činnosti, sexuálnemu zneužívaniu detí (najmä jeho online aspektom), ako aj rôznym druhom inej počítačovej kriminality a trestnej činnosti umožnenej počítačom. Pre príslušné orgány môže byť prístup k elektronickým dôkazom nevyhnutný nielen na úspešné vyšetrovanie, a tým na potrestanie páchatel'ov trestných činov, ale aj na ochranu obetí a pomoc pri zaisťovaní bezpečnosti.

---

<sup>1</sup> Rozsudok zo 16. júla 2020 vo veci C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

<sup>2</sup> iOCTA 2020, s. 25.

Existujú však prípady, keď šifrovanie mimoriadne sťažuje alebo prakticky znemožňuje prístup k obsahu komunikácie a jeho analýzu v rámci prístupu k elektronickým dôkazom napriek skutočnosti, že prístup k takýmto údajom by bol zákonný. Nezávisle od aktuálneho technologického prostredia je preto nevyhnutné zachovať právomoci príslušných orgánov v oblasti bezpečnosti a trestnej spravodlivosti prostredníctvom zákonného prístupu na účely plnenia ich úloh, ako je stanovené a povolené zákonom. Takéto zákony, ktoré ustanovujú právomoci na presadzovanie práva, musia vždy v plnej miere rešpektovať riadny proces a iné záruky, ako aj základné práva, najmä právo na rešpektovanie súkromného života a komunikácie a právo na ochranu osobných údajov.

#### 4. Dosiahnutie správnej rovnováhy

Zásada bezpečnosti prostredníctvom šifrovania a bezpečnosti napriek šifrovaniu sa musí dodržiavať v celom rozsahu. Európska únia naďalej podporuje silné šifrovanie. Šifrovanie je základom dôvery v digitalizáciu a ochranu základných práv a malo by sa podporovať a rozvíjať.

Ochrana súkromia a bezpečnosti komunikácie prostredníctvom šifrovania a zároveň zachovanie možnosti zákonného prístupu príslušných orgánov v oblasti bezpečnosti a trestnej justície k relevantným údajom na legitímne, jasne vymedzené účely v rámci boja proti závažnej a/alebo organizovanej trestnej činnosti a terorizmu, a to aj v digitálnom svete, ako aj dodržiavanie zásad právneho štátu je mimoriadne dôležité. Pri všetkých prijatých opatreniach sa musí starostlivo zaistiť rovnováha medzi uvedenými záujmami zásadami nevyhnutnosti, proporcionality a subsidiarity.

#### 5. Spojenie síl s technologickými odvetvami

Európska únia sa pri svojom postupe usiluje nadviazať aktívny dialóg s technologickým priemyslom a zároveň zapojiť výskum a akademickú obec, aby sa zaistila neustála implementácia a využívanie technológií silného šifrovania. Príslušné orgány musia mať prístup k údajom zákonným a cieleným spôsobom pri plnom dodržiavaní základných práv a príslušných právnych predpisov o ochrane údajov pri súčasnom dodržiavaní kybernetickej bezpečnosti. Technické riešenia na získanie prístupu k šifrovaným údajom musia byť v súlade so zásadami zákonnosti, transparentnosti, nevyhnutnosti a proporcionality vrátane špecificky navrhutej a štandardnej ochrany osobných údajov.

Keďže neexistuje len jeden spôsob, ako dosiahnuť stanovené ciele, vlády, príslušné odvetvia, výskum a akademická obec musia transparentne spolupracovať na strategickom vytváraní tejto rovnováhy.

## 6. Regulačný rámec

Ďalej by sa mohla posúdiť potreba vypracovať regulačný rámec pre celú EÚ, ktorý by príslušným orgánom umožnil účinne vykonávať ich operačné úlohy a zároveň chrániť súkromie, základné práva a bezpečnosť komunikácie.

Potenciálne technické riešenia budú musieť umožniť orgánom využívať ich vyšetrovacie právomoci, ktoré podliehajú zásadám primeranosti a nevyhnutnosti a súdnej kontrole podľa ich vnútroštátnych právnych predpisov, a to pri rešpektovaní spoločných európskych hodnôt a dodržiavaní základných práv a zachovaní výhod šifrovania. Potenciálne riešenia by sa mali rozvíjať transparentným spôsobom v spolupráci s vnútroštátnymi a medzinárodnými poskytovateľmi komunikačných služieb a inými príslušnými zainteresovanými stranami.

Takéto technické riešenia a normy, ako aj rýchly vývoj technológií vo všeobecnosti by si tiež vyžadovali neustále vylepšovanie technických a operačných zručností a znalostí príslušných orgánov, aby mohli pri svojej práci účinne reagovať na výzvy digitalizácie na globálnej úrovni.

## 7. Inovačné vyšetrovacie spôsobilosti

Napokon je mimoriadne dôležité zlepšiť koordináciu na úrovni EÚ zameranú na:

- 1) spojenie úsilia všetkých členských štátov a inštitúcií a orgánov EÚ;
- 2) vymedzenie a vypracovanie inovatívnych prístupov v súvislosti s novými technológiami;
- 3) analýzu vhodných technických a operačných riešení a
- 4) poskytovanie vysokokvalitnej odbornej prípravy prispôbenej potrebám.

Technické a operačné riešenia zakotvené v regulačnom rámci založenom na zásadách zákonnosti, nevyhnutnosti a proporcionality by sa mali vypracovať v úzkej spolupráci s poskytovateľmi služieb, inými relevantnými zainteresovanými stranami a všetkými dotknutými príslušnými orgánmi, aj keď by nemalo existovať len jedno predpísané technické riešenie na poskytovanie prístupu k šifrovaným údajom.