

V Bruseli 23. novembra 2016
(OR. en)

14711/16

LIMITE

CYBER 137
JAI 976
ENFOPOL 429
GENVAL 122
COSI 192
COPEN 352

POZNÁMKA

Od:	Predsedníctvo
Komu:	Výbor stálych predstaviteľov/Rada
Č. predch. dok.:	13993/16
Predmet:	Šifrovanie: výzvy pre trestné súdnictvo v súvislosti s využívaním šifrovania – ďalšie kroky – správa o pokroku

Úvod

1. Internet zmenil spôsob, akým dnes vo svete prebieha komunikácia; súčasťou týchto nových komunikačných modelov sa čoraz viac stávajú šifrovacie technológie. Používanie šifrovania slúži na napĺňanie legitímnych potrieb ochrany súkromia a bezpečnosti a na účely uplatňovania základných práv jednotlivcov, ako aj na napĺňanie potrieb podnikov a vlád disponovať bezpečným a chráneným kybernetickým priestorom. Podniky začali investovať do vývoja nástrojov – alebo samy takéto nástroje vyvíjajú – s cieľom ponúknuť svojim zákazníkom čo najlepšiu ochranu ich súkromia prostredníctvom silného šifrovania a zvýšiť kybernetickú bezpečnosť. Akákoľvek snaha o oslabenie šifrovania alebo bezpečnostných protokolov vo všeobecnosti môže viesť nielen k zneužitiu súkromných alebo citlivých obchodných informácií inými stranami, ale aj k vzniku významných rizík z hľadiska kybernetickej bezpečnosti.

2. Na zabezpečenie a ochranu svojich osobných údajov alebo komunikácie môže využívať šifrovanie prakticky ktokoľvek. Bezpečné spracúvanie je dôležitým prvkom ochrany osobných údajov, pričom v nedávno prijatom všeobecnom nariadení o ochrane údajov sa šifrovanie považuje za jedno z bezpečnostných opatrení. Spoločnosti, orgány verejnej správy a jednotlivci sa nabádajú, aby využívali šifrovanie na ochranu svojich údajov a elektronickej komunikácie. Aj smernica o súkromí a elektronických komunikáciách obsahuje výzvu na používanie šifrovacích technológií na ochranu komunikácie používateľov. Avšak možnosti, ktoré ponúkajú šifrovacie technológie, využívajú aj zločinci s cieľom ukryť svoje údaje a potenciálne dôkazy, chrániť svoju komunikáciu a maskovať svoje finančné transakcie.
3. Podľa hodnotenia hrozieb internetovej organizovanej trestnej činnosti (I-OCTA), ktoré Europol poskytol v roku 2016, je silné šifrovanie veľmi dôležité pre elektronický obchod a iné činnosti v kybernetickom priestore, ale primeraná bezpečnosť závisí od toho, či sú orgány presadzovania práva schopné úspešne vyšetrovať trestnú činnosť. Používanie šifrovania bráni orgánom presadzovania práva získavať kľúčové dôkazy, najmä vzhľadom na skutočnosť, že šifrovanie sa už neobmedzuje len na stolové počítače, ale je čoraz dostupnejšie pre mobilné zariadenia, pričom mnohé komerčne dostupné komunikačné platformy šifrovanie využívajú štandardne (čoraz viac vo forme *šifrovania bez medzifáz (end-to-end)*, čo vedie k situáciám, keď služby nemožno odpočúvať).
4. Počas strategického seminára na tému „Kľúče od kybernetického priestoru“, ktorý Eurojust usporiadal 2. júna 2016, si odborníci vymenili informácie o rôznych otázkach vrátane šifrovania. Diskusia sa sústredila hlavne na prístup k uzamknutým mobilným zariadeniam, a najmä na možnosť využitia už skôr zozbieraných odtlačkov prstov podozrivej osoby na odomknutie zamknutého zariadenia s cieľom získať prístup k údajom. Účastníci sa vo všeobecnosti zhodli na tom, že je potrebné chrániť súkromie občanov, a to aj prostredníctvom šifrovania, ale mala by sa nájsť správna rovnováha medzi touto potrebou a potrebou bojovať proti trestnej činnosti, čím sa zabezpečí vyššia úroveň bezpečnosti pre všetkých občanov.

5. Vzhľadom na rastúci význam tejto záležitosti viedli ministri spravodlivosti na neformálnom zasadnutí v júli tohto roku politické rokovanie venované šifrovaniu. Jeho výsledkom bolo uznanie problémov, ktoré šifrovanie predstavuje, a mandát na ďalšie skúmanie tejto problematiky. Ministri vyjadrili rôzne názory na to, aký prístup by sa mal použiť, a to od zachovania súčasného stavu v oblasti ochrany súkromia a obchodných štandardov až po nájdenie účinnejších nástrojov pre orgány presadzovania práva, či dokonca rozšírenie riešení do iných oblastí, aj nad rámec trestného súdnictva.

Mapovanie problému

6. V záujme nadviazania na výsledok uvedeného politického rokovania sa predsedníctvo rozhodlo získať podrobnejšie informácie prostredníctvom dotazníka s cieľom posúdiť súčasnú situáciu z pohľadu orgánov presadzovania práva v členských štátoch, a tak zvážiť možné smery ďalšieho postupu.
7. Odpovede poskytlo 25 členských štátov a Europol. Odhaľujú nasledujúce prvky prítomné vo väčšine členských štátov:
- v rámci vyšetrovania trestnej činnosti sa šifrovanie vyskytuje často alebo takmer vždy. (Iba 5 delegácií uviedlo, že sa s ním stretávajú len zriedka),
 - vyskytli sa prípady šifrovania online (vo forme šifrovaných e-mailov alebo iných foriem elektronickej komunikácie alebo komerčných aplikácií, napr. Facebook, Skype, WhatsApp alebo Telegram) aj šifrovania off-line (najčastejšie pri vyšetrovaní trestných činov zahŕňajúcich šifrované digitálne zariadenia a šifrovacie aplikácie),

- ani na podozrivú, ani na obvinenú osobu, ktorá je držiteľom digitálneho zariadenia/elektronických údajov, sa nevzťahuje zákonná povinnosť poskytnúť orgánom presadzovania práva šifrovacie kľúče/heslá, vo väčšine prípadov v dôsledku práva nevypovedať vo svoj neprospech. V niektorých členských štátoch sa však uplatnili odlišné legislatívne prístupy, na základe ktorých takéto možnosti existujú voči podozrivej osobe alebo tretím osobám,
- poskytovatelia služieb sú podľa vnútroštátneho práva povinní poskytnúť orgánom presadzovania práva šifrovacie kľúče/heslá; súdny príkaz nie je vždy potrebný. V uvedených odpovediach sa však nerozlišuje, či sa táto povinnosť vzťahuje len na poskytovateľov služieb elektronickej komunikácie alebo zahŕňa aj poskytovateľov služieb informačnej spoločnosti,
- odpočúvanie/monitorovanie šifrovaných dátových tokov v záujme získania dešifrovaných údajov je možné za určitých podmienok ustanovených vo vnútroštátnom práve; často je potrebný predchádzajúci súdny príkaz,
- vnútroštátny právny rámec zameraný na zabezpečenie elektronických dôkazov v prípade šifrovania sa na rozdiel od všeobecných právnych ustanovení týkajúcich sa elektronických dôkazov považuje za dostatočne účinný,
- nedostatočné technické kapacity z hľadiska účinných technických riešení na dešifrovanie, ako aj z hľadiska príslušného vybavenia patria medzi najzásadnejšie 3 výzvy, pričom za nimi nasledujú nedostatočné finančné zdroje a personálne kapacity (tak z hľadiska počtu, ako aj odbornej prípravy personálu),
- potreba prijať prakticky orientované opatrenia prevažuje nad potrebou prijatia nových právnych predpisov na úrovni EÚ (s výnimkou jednej delegácie, ktorá identifikovala takúto potrebu v oblasti uchovávaní údajov a zákonného odpočúvania),

8. Vo všetkých opatreniach prijatých v budúcnosti by sa malo zohľadniť politické prostredie vymedzené v záveroch Rady o zlepšení trestnej justície v kybernetickom priestore a v záveroch Rady o Európskej justičnej sieti na boj proti počítačovej kriminalite, ktoré boli prijaté na júnovom zasadnutí Rady (SVV) počas holandského predsedníctva, a z nich vyplývajúce pokračujúce procesy týkajúce sa elektronických dôkazov vzhľadom na skutočnosť, že značné množstvo elektronických údajov je šifrovaných; týkajúce sa vytvárania rámca spolupráce s poskytovateľmi služieb vzhľadom na ich kľúčovú úlohu; a týkajúce sa sfunkčnenia justičných zložiek, ktoré sa zaoberajú prípadmi počítačovej kriminality/prípady založenými na počítačovej kriminalite alebo vyšetrovaniami v kybernetickom priestore, tým, že sa im poskytne osobitné fórum na výmenu špecializovaných odborných znalostí s cieľom podporiť vykonávanie ich funkcií.

Ďalšie kroky

9. Na zasadnutí horizontálnej pracovnej skupiny pre kybernetické otázky 28. októbra predložilo predsedníctvo štyri kroky ako možný budúci prístup k otázke šifrovania. Členské štáty uvítali iniciatívu predsedníctva a uvedené kroky vo všeobecnosti podporili. Uviedli, že v tejto fáze uprednostňujú oddelenie procesu šifrovania od odborného procesu v oblasti elektronických dôkazov, pričom nevylučujú potrebu koordinácie týchto dvoch procesov ani možnosť ich zosúladenia v budúcnosti, či zamerania sa vo väčšej miere na politické a praktické riešenia než na tvorbu právnych nástrojov. Delegácie uznali šifrovanie za nástroj na ochranu súkromia a kybernetickej bezpečnosti v spoločnosti. Zdôraznili, že je dôležité, aby sa nevyslal signál, že šifrovanie by sa malo oslabiť. Bezpečnosť jednotlivcov v kybernetickom priestore by sa mala zaistiť, ale skôr prostredníctvom vyváženého riešenia zaisťujúceho ochranu ľudských práv a bezpečnosť jednotlivcov a spoločnosti. Delegácie takisto zdôraznili význam odbornej prípravy a uvítali iniciatívu Europolu a agentúry ENISA vytvoriť spoločnú pracovnú skupinu pre ochranu a bezpečnosť online s cieľom prerokovať, posúdiť a hľadať riešenia na boj proti zneužívaniu šifrovania a anonymity na internete.

10. Uvedený štvorkrokový prístup sa po úprave na základe prvého rokovania v rámci horizontálnej pracovnej skupiny pre kybernetické otázky predložil 18. novembra 2016 výboru CATS, kde získal širokú podporu. Členské štáty zdôraznili potrebu zaoberať sa technickými i právnymi (trestné súdnictvo) aspektmi tejto otázky a zamerať budúcu činnosť na praktické riešenia, ktoré by uľahčili prácu orgánov presadzovania práva bez oslabenia šifrovania a ochrany súkromia občanov. Členské štáty v tejto súvislosti opätovne potvrdili význam zabezpečenia primeranej rovnováhy. Zhodlo sa, že Komisia je najkompetentnejšia na organizovanie procesu reflexie s cieľom zachovať prepojenie s odborným procesom v oblasti elektronických dôkazov a zabrániť prekývaniu sa týchto procesov pri súčasnom zachovaní ich oddelenia.
11. Niektoré delegácie sa počas uvedeného rokovania konkrétnejšie dotkli úlohy poskytovateľov služieb a navrhli, aby sa rozsah ich zodpovednosti a povinností podrobnejšie preskúmal. Iné delegácie pripomenuli, že vzhľadom na rýchly technologický vývoj je potrebné myslieť dopredu a že je potrebné zabezpečiť intenzívne zapojenie príslušných agentúr EÚ, ako sú Europol a Eurojust, do tohto procesu.
12. 24. novembra 2016 sa uskutočnilo prvé zasadnutie Európskej justičnej siete na boj proti počítačovej kriminalite, na ktorom sa rokovalo aj o technických a právnych výzvach v súvislosti so šifrovaním a o právnych prekážkach utajeného vyšetrovania online. Na nadchádzajúcich zasadnutiach siete by sa malo pokračovať v rokovaní o týchto otázkach a mali by sa vymieňať najlepšie postupy a informácie o príslušných vnútroštátnych právnych predpisoch.

13. Rada sa preto vyzýva, aby:

- **zhodnotila doposiaľ dosiahnutý pokrok a**
- **schválila štvorkrokový prístup v znení uvedenom v nasledujúcich bodoch A až D ako základ pre budúce práce v tejto súvislosti:**

A. Začať pod vedením Komisie proces reflexie týkajúci sa výziev, ktorým čelí trestné súdnictvo v súvislosti s používaním šifrovania, s cieľom určiť praktické riešenia, ktoré by umožňovali prípadné sprístupnenie šifrovaných údajov/zariadení prostredníctvom integrovaného prístupu a rámca EÚ. V snahe zabezpečiť konzistentnosť a predísť duplicite by sa v tomto procese reflexie mal zohľadniť pokrok dosiahnutý v rámci prebiehajúceho odborného procesu v oblasti elektronických dôkazov a procesu vytvárania spoločného rámca pre spoluprácu s poskytovateľmi služieb na získanie osobitných kategórií údajov a vo vhodných prípadoch by sa v ňom mali využiť výsledky týchto dvoch procesov.

B. Preskúmať možnosti na zlepšenie technických odborných znalostí na národnej úrovni aj na úrovni EÚ s cieľom čeliť súčasným a budúcim výzvam vyplývajúcim zo šifrovania, a to okrem iného posilnením technických spôsobilostí, ktoré už existujú v rámci Europolu, a podporou ich používania členskými štátmi v príslušných hraniciach jeho mandátu, ako aj ďalším rozvojom Europolu ako európskeho centra odborných znalostí v oblasti šifrovania. Mohlo by sa zväžiť aj využitie pomoci iných relevantných subjektov EÚ, ako je napríklad agentúra ENISA.

C. Nabádať členov Európskej justičnej siete na boj proti počítačovej kriminalite, aby do svojho fóra, ktoré je určené na diskusiu, výmenu informácií, osvedčených postupov a odborných znalostí, prinášali aj praktické/operačné aspekty týkajúce sa šifrovania. Zdá sa, že na účely reakcie na výzvy, ktoré so sebou prináša šifrovanie, je nevyhnutná úzka spolupráca a konzultácie s Europolom, Eurojustom a uvedenou sieťou.

D. Prehĺbiť praktické/operačné aspekty odbornej prípravy v oblasti šifrovania pre orgány presadzovania práva poskytovanej subjektmi EÚ a zvýšiť úsilie o budovanie kapacít s cieľom zabezpečiť, aby odborníci mali vhodné a najnovšie vedomosti a spôsobilosti, pokiaľ ide o získanie a spracovanie elektronických dôkazov.