Rada
Evropské unie

Brusel 24. listopadu 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

Odesílatel:	Předsednictví
Příjemce:	Delegace
Č. předchozího dokumentu:	12863/20
Předmět:	Usnesení Rady o šifrování – bezpečnost prostřednictvím šifrování a bezpečnost navzdory šifrování

Delegace naleznou v příloze usnesení Rady o šifrování.

PŘÍLOHA

Usnesení Rady o šifrování

Bezpečnost prostřednictvím šifrování a bezpečnost navzdory šifrování

1. Preambule: Bezpečnost prostřednictvím šifrování a bezpečnost navzdory šifrování

Evropská unie plně podporuje rozvoj, zavádění a používání silného šifrování. Evropská unie zdůrazňuje, že v rámci všech opatření souvisejících s tímto usnesením je třeba zajistit plné dodržování základních a lidských práv a zásad právního státu, a to online i offline. Šifrování je nezbytným prostředkem ochrany základních práv a digitální bezpečnosti vlád, průmyslu a společnosti. Evropská unie zároveň musí zajistit, aby příslušné orgány v oblasti bezpečnosti a trestního soudnictví, např. donucovací a justiční orgány, mohly vykonávat své zákonné pravomoci a současně chránit naše společnosti a občany, a to online i offline.

Podle závěrů Evropské rady ze dnů 1. a 2. října 2020 (dokument EUCO 13/20) *bude EU využívat své nástroje a regulační pravomoci k tomu, aby pomáhala utvářet globální pravidla a normy*. Bylo dohodnuto, že finanční prostředky v rámci facility na podporu oživení a odolnosti budou použity k dosažení cílů, jako je *posílení schopnosti EU chránit se před kybernetickými hrozbami, vytvářet bezpečné komunikační prostředí, především za využití kvantového šifrování, a zajistit přístup k údajům pro účely justice a vymáhání práva*.

2. Současné používání / stav šifrování

V dnešním světě se šifrovací technologie stále více využívají ve všech oblastech veřejného i soukromého života. Jsou prostředkem, jehož uplatněním lze chránit jednotlivce, občanskou společnost, kritickou infrastrukturu, sdělovací prostředky a novináře, průmysl a vlády zajištěním soukromí, důvěrnosti, integrity údajů a dostupnosti komunikace a osobních údajů: je zřejmé, že ze šifrovacích technologií mají prospěch všechny strany. Orgány EU pro ochranu údajů a kybernetickou bezpečnost označily šifrování za důležitý nástroj, jenž přispívá například k ochraně osobních údajů, které jsou předávány mimo EU, ale vztahuje se na ně požadavek na úroveň ochrany, která je v zásadě rovnocenná, což je podle Soudního dvora jedním z právních požadavků na předávání údajů[1]. Nejenže jsou elektronická zařízení a aplikace stále častěji naprogramovány tak, aby uložené údaje uživatelů šifrovaly již na úrovni standardního nastavení, ale vzrůstají i počty komunikačních kanálů a služeb ukládání dat, jež jsou zabezpečeny pomocí šifrování mezi koncovými body (E2E). Tato skutečnost se pozitivně odráží v posilující reakci ze strany odvětví komunikace a aplikací, v jehož rámci zavedla šifrování mezi koncovými body rovněž většina aplikací pro výměnu rychlých zpráv a dalších on-line platforem.

3. Výzvy z hlediska zajištění bezpečnosti

„Digitální život“ a kybernetický prostor přinášejí nejen velké příležitosti, ale i povážlivé výzvy: digitalizace moderních společností vytváří jistá zranitelná místa a potenciál pro zneužívání pro účely trestné činnosti. Její pachatelé tak mohou do svého způsobu práce zahrnout snadno a běžně dostupná šifrovací řešení určená pro legitimní účely[2].

Zároveň je vymáhání práva rostoucí měrou závislé na přístupu k elektronickým důkazům, aby bylo možné účinně bojovat proti terorismu, organizované trestné činnosti, pohlavnímu zneužívání dětí (zejména jeho online aspektům), jakož i proti celé řadě dalších forem kyberkriminality a trestné činnosti prováděné kybernetickými prostředky. Pro příslušné orgány může mít přístup k elektronickým důkazům zásadní význam, a to nejen pro to, aby mohly vést úspěšné vyšetřování, a na jeho základě pak postavit pachatele před soud, ale také aby mohly chránit oběti a napomáhat k zajištění bezpečnosti.

---

[1] Rozsudek ze dne 16. července 2020 ve věci C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559.

[2] Posouzení hrozeb organizované trestné činnosti z roku 2020 (IOCTA 2020), s. 25.

Někdy se však v rámci přístupu k elektronickým důkazům vyskytují případy, kdy šifrování mimořádně komplikuje nebo prakticky znemožňuje přístup k obsahu komunikace a jeho analýzu, a to navzdory skutečnosti, že by přístup k těmto údajům byl v souladu se zákonem. Nezávisle na stávajících technologických podmínkách je proto nezbytné zachovat pravomoci příslušných orgánů v oblasti bezpečnosti a trestního soudnictví a zajistit jim zákonný přístup umožňující jim plnění jejich úkolů, jak je stanoveno a povoleno právními předpisy. Tyto právní předpisy, které stanoví pravomoci v oblasti vymáhání práva, musí vždy plně dodržovat zásady řádného procesu a další záruky, jakož i základní práva, zejména právo na respektování soukromého života a komunikace a právo na ochranu osobních údajů.

4. Nalezení vhodné rovnováhy

Zásada bezpečnosti prostřednictvím šifrování a bezpečnosti navzdory šifrování musí být v plném rozsahu dodržována. Evropská unie nadále podporuje silné šifrování. Šifrování je základem důvěry v digitalizaci a ochranu základních práv a mělo by být podporováno a rozvíjeno.

Je mimořádně důležité chránit šifrováním soukromí a bezpečnost komunikace a zároveň zachovat možnost, aby příslušné orgány v oblasti bezpečnosti a trestního soudnictví měly v rámci boje proti závažné nebo organizované trestné činnosti a terorismu zákonný přístup k relevantním údajům pro legitimní a jasně vymezené účely, a to i v digitálním světě, a dodržovat zásady právního státu. V rámci jakýchkoli přijatých opatření musí tyto zájmy pečlivě vyváženy se zásadami nezbytnosti, proporcionality a subsidiarity.

5. Spojení sil s technologickým průmyslem

V zájmu zajištění pokroku se Evropská unie snaží zahájit aktivní diskusi s technologickým průmyslem a zároveň zapojit výzkum a akademickou obec s cílem zajistit nepřetržité zavádění a používání technologií silného šifrování. Příslušným orgánům musí být umožněn zákonný a cílený přístup k údajům, a to při plném dodržování základních práv a relevantních právních předpisů v oblasti ochrany údajů a při současném zachování kybernetické bezpečnosti. Technická řešení pro získání přístupu k zašifrovaným údajům musí být v souladu se zásadami zákonnosti, transparentnosti, nezbytnosti a proporcionality, včetně ochrany osobních údajů již na úrovni návrhu a na úrovni standardního nastavení ochrany údajů.

Vzhledem k tomu, že neexistuje žádný jediný způsob, jak stanovených cílů dosáhnout, musí vlády, průmysl, výzkum a akademická obec transparentně spolupracovat, aby tuto rovnováhu strategicky zajistily.

6. Regulační rámec

Mohla by být dále posouzena potřeba vytvořit regulační rámec v celé EU, který by příslušným orgánům umožňoval účinně plnit jejich operační úkoly a zároveň by chránil soukromí, základní práva a bezpečnost komunikace.

Případná technická řešení budou muset orgánům umožnit, aby využívaly své vyšetřovací pravomoci, jež podléhají zásadám proporcionality a nezbytnosti a soudnímu dohledu podle jejich vnitrostátních právních předpisů, a to při respektování společných evropských hodnot a dodržování základních práv a zachování výhod šifrování. Možná řešení by měla být vypracována transparentním způsobem ve spolupráci s vnitrostátními a mezinárodními poskytovateli komunikačních služeb a dalšími relevantními zainteresovanými stranami. Tato technická řešení a normy – a rychlý rozvoj technologií obecně – by rovněž vyžadovaly nepřetržité zlepšování technických a operačních dovedností a odborných znalostí příslušných orgánů, aby bylo v rámci jejich činnosti v celosvětovém měřítku možné účinně řešit výzvy spojené s digitalizací.

7. Inovativní vyšetřovací schopnosti

V neposlední řadě je nanejvýš důležité zlepšit koordinaci na úrovni EU zaměřenou na:

1) spojení úsilí všech členských států a orgánů a institucí EU;

2) definování a zavádění inovativních přístupů s ohledem na nové technologie;

3) analýzu vhodných technických a operačních řešení a

4) poskytování vysoce kvalitní a individuálně přizpůsobené odborné přípravy.

Technická a operační řešení zakotvená v regulačním rámci založeném na zásadách zákonnosti, nezbytnosti a proporcionality by měla být vypracována v úzké spolupráci s poskytovateli služeb, dalšími relevantními zainteresovanými stranami a všemi relevantními příslušnými orgány, ačkoli by pro zajištění přístupu k šifrovaným údajům nemělo existovat žádné jediné předepsané technické řešení.