Rada
Evropské unie

Brusel 2. prosince 2021
(OR. en)

14614/21

Interinstitucionální spis:
2021/0383(NLE)

JAI 1333
COPEN 433
CYBER 321
ENFOPOL 483
TELECOM 453
EJUSTICE 106
MI 913
DATAPROTECT 277

NÁVRH

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	25. listopadu 2021
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2021) 719 final
Předmět:	Návrh ROZHODNUTÍ RADY, kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů

Delegace naleznou v příloze dokument COM(2021) 719 final.

Příloha: COM(2021) 719 final

EVROPSKÁ
KOMISE

V Bruselu dne 25.11.2021
COM(2021) 719 final

2021/0383 (NLE)

Návrh

ROZHODNUTÍ RADY,

kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů

DŮVODOVÁ ZPRÁVA

1. PŘEDMĚT NÁVRHU

Tento návrh se týká rozhodnutí, kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Budapešťské úmluvě Rady Evropy o počítačové kriminalitě (dále jen „protokol“) o posílené spolupráci a zpřístupňování elektronických důkazů.[1] Cílem protokolu je poskytovat společná pravidla na mezinárodní úrovni, aby byla posílena spolupráce v oblasti kyberkriminality a shromažďování důkazů v elektronické formě pro účely vyšetřování trestných činů nebo trestního řízení.

Tento návrh doplňuje samostatný návrh rozhodnutí Rady Evropské unie (dále jen „Rada“) vypracovaný Komisí, kterým se členské státy zmocňují, aby v zájmu Evropské unie protokol podepsaly.

Kyberkriminalita i nadále představuje pro naši společnost velkou výzvu. Navzdory úsilí donucovacích a justičních orgánů se kybernetické útoky, včetně ransomwarových útoků, šíří a jsou stále sofistikovanější.[2] Zejména kvůli bezhraniční povaze internetu má vyšetřování kyberkriminality téměř vždy svou povahou přeshraniční charakter, a tudíž vyžaduje úzkou spolupráci mezi orgány v různých zemích.

Význam elektronických důkazů při vyšetřování trestných činů stále roste. Komise odhaduje, že v současné době potřebují donucovací a justiční orgány přístup k elektronickým důkazům při 85 % vyšetřování trestných činů, včetně kyberkriminality.[3] Důkazy o trestných činech v elektronické formě stále častěji disponují poskytovatelé služeb v zahraničních jurisdikcích, a aby trestní soudnictví mohlo efektivněji reagovat, je pro získání těchto důkazů nutné přijetí vhodných opatření na podporu právního státu.

Snaha o zlepšení přeshraničního přístupu k elektronickým důkazům při vyšetřování trestných činů je vyvíjena po celém světě na vnitrostátní, celounijní[4] a mezinárodní úrovni, a to i prostřednictvím protokolu. Pokud je vyžadován přeshraniční přístup k elektronickým důkazům, je důležité zajistit vzájemně slučitelná pravidla na mezinárodní úrovni, aby se zamezilo kolizi norem.

2. SOUVISLOSTI NÁVRHU

2.1. Souvislosti

Cílem Budapešťské úmluvy Rady Evropy o počítačové kriminalitě (CETS č. 185) (dále jen „úmluva“) je usnadnit boj proti trestným činům spáchaným prostřednictvím počítačových sítí. Úmluva 1) obsahuje ustanovení, která harmonizují prvky trestných činů v oblasti vnitrostátního trestního práva hmotného a související ustanovení v oblasti kyberkriminality, 2) stanoví pravomoci v oblasti vnitrostátního trestního práva procesního, které jsou nezbytné pro vyšetřování a trestní stíhání takových trestných činů, jakož i ostatních trestných činů spáchaných prostřednictvím počítačového systému, nebo pokud důkazy existují v elektronické formě, a 3) má za cíl zřídit rychlý a účinný režim mezinárodní spolupráce.

---

1 Znění protokolu je zahrnuto jako příloha tohoto návrhu.
2 Posouzení hrozeb závažné a organizované trestné činnosti v Evropské unii za rok 2021 (EU SOCTA 2021).
3 SWD(2018) 118 final
4 COM(2018) 225 a 226 final.

Úmluva je otevřena členským státům Rady Evropy a nečlenským státům je otevřena na základě pozvání. V současné době je smluvními stranami úmluvy 66 zemí, včetně 26 členských států Evropské unie.[5] Úmluva nepředpokládá, že by Evropská unie mohla k úmluvě přistoupit. Evropská unie je však uznávána jako pozorovatelská organizace Výboru k Úmluvě o počítačové kriminalitě (T-CY).[6]

Bez ohledu na snahu o vyjednání nové úmluvy o počítačové kriminalitě na úrovni Organizace spojených národů[7] je Budapešťská úmluva i nadále hlavní mnohostrannou úmluvou v boji proti kyberkriminalitě. Unie soustavně Úmluvu podporuje[8], mimo jiné také v rámci financování programů budování kapacit.[9]

V návaznosti na návrhy skupiny Rady Evropy pro důkazy v cloudech[10] přijal Výbor k Úmluvě o počítačové kriminalitě několik doporučení, mimo jiné prostřednictvím jednání o druhém dodatkovém protokolu k Úmluvě o počítačové kriminalitě o posílené mezinárodní spolupráci, aby řešil problematickou situaci, kdy poskytovatelé služeb v zahraničních jurisdikcích mají stále častěji k dispozici elektronické důkazy související s kyberkriminalitou a jinými trestnými činy, přičemž pravomoci donucovacích orgánů jsou i nadále omezovány územními hranicemi. V červnu 2017 schválil Výbor k Úmluvě o počítačové kriminalitě mandát k přípravě druhého dodatkového protokolu v období od září 2017 do prosince 2019.[11] S ohledem na potřebu delší lhůty k završení jednání, jakož i na omezení, která přinesla pandemie COVID-19 v letech 2020 a 2021, prodloužil Výbor k Úmluvě o počítačové kriminalitě mandát dvakrát, nejprve do prosince 2020 a poté do května 2021.

V návaznosti na výzvu Evropské rady v jejích závěrech z 18. října 2018[12] přijala Komise dne 5. února 2019 doporučení pro rozhodnutí Rady o zmocnění Komise k účasti – jménem Evropské unie – na jednáních o druhém dodatkovém protokolu k Úmluvě Rady Evropy o počítačové kriminalitě.[13] Evropský inspektor ochrany údajů vydal k doporučení stanovisko dne 2. dubna 2019.[14] Rozhodnutím ze dne 6. června 2019 Rada Evropské unie zmocnila Komisi k účasti jménem Evropské unie na jednáních o druhém dodatkovém protokolu.[15]

Jak bylo uvedeno ve Strategii bezpečnostní unie EU z roku 2020[16], Strategii kybernetické bezpečnosti EU pro digitální dekádu z roku 2020[17] a Strategii EU pro boj proti organizované

---

5 Kromě Irska, které úmluvu podepsalo, ale neratifikovalo, avšak se zavázalo, že o přistoupení bude usilovat.

6 Jednací řád Výboru k Úmluvě o počítačové kriminalitě (T-CY (2013)25 rev), k dispozici na adrese www.coe.int/cybercrime.

7 Rezoluce Valného shromáždění OSN č. 74/247 z prosince 2019 o „boji proti využívání informačních a komunikačních technologií pro účely trestné činnosti“.

8 JOIN(2020) 81 final.

9 Viz například projekt Globální akce v oblasti kyberkriminality + (Global Action on Cybercrime Extended + (GLACY+)), na adrese https://www.coe.int/en/web/cybercrime/glacyplus

10 Závěrečná zpráva skupiny pro důkazy v cloudech působící v rámci Výboru k Úmluvě o počítačové kriminalitě s názvem „Přístup k elektronickému důkaznímu materiálu v cloudu v rámci trestního soudnictví: doporučení ke zvážení ze strany T-CY“ ze dne 16. září 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690

12 https://www.consilium.europa.eu/cs/press/press-releases/2018/10/18/20181018-european-council-conslusions/

13 COM(2019) 71 final.

14 Stanovisko evropského inspektora ochrany údajů 3/2019 týkající se účasti na jednáních s ohledem na druhý dodatkový protokol k Budapešťské úmluvě o počítačové kriminalitě ze dne 2. dubna 2019.

15 Rozhodnutí Rady č. 9116/19.

16 COM(2020) 605 final.

17 JOIN(2020) 81 final.

trestné činnosti z roku 2021[18], Komise se zavázala k rychlému a zdárnému dokončení jednání o protokolu. Evropský parlament rovněž uznal potřebu dokončit práci na protokolu ve svém usnesení z roku 2021 o Strategii kybernetické bezpečnosti EU pro digitální dekádu.[19]

V souladu s rozhodnutím Rady Evropské unie se Komise zúčastnila jménem Evropské unie jednání o protokolu. Komise soustavně konzultovala otázku postoje Unie se zvláštním výborem Rady pro jednání.

V souladu s rámcovou dohodou o vztazích mezi Evropským parlamentem a Evropskou komisí[20] také Komise průběžně informovala Evropský parlament o jednáních písemnými zprávami a ústně.

Na svém plenárním zasedání dne 28. května 2021 schválil Výbor k Úmluvě o počítačové kriminalitě návrh protokolu na své úrovni a předal jej k přijetí Výboru ministrů Rady Evropy.[21] Výbor ministrů Rady Evropy protokol přijal dne 17. listopadu 2021.

2.2. Druhý dodatkový protokol

Cílem protokolu je posílit spolupráci v oblasti kyberkriminality a shromažďování důkazů v elektronické formě o trestném činu pro účely konkrétních vyšetřování trestných činů nebo trestních řízení. Protokol uznává potřebu lepší a účinnější spolupráce mezi státy a se soukromým sektorem, větší transparentnosti a právní jistoty pro poskytovatele služeb a ostatní subjekty, pokud jde o okolnosti, za nichž mohou odpovídat na žádosti, které jsou podávány orgány v jiných smluvních stranách činnými v trestním řízení a které se týkají zpřístupnění elektronických důkazů.

Protokol rovněž uznává, že účinná přeshraniční spolupráce pro účely trestního soudnictví, mimo jiné mezi orgány veřejného sektoru a subjekty soukromého sektoru, vyžaduje účinné podmínky a silné záruky pro ochranu základních práv. Za tímto účelem se protokol řídí přístupem založeným na právech a stanoví podmínky a záruky v souladu s mezinárodními nástroji pro lidská práva, včetně Úmluvy Rady Evropy z roku 1950 o ochraně lidských práv a základních svobod. Jelikož se elektronické důkazy často týkají osobních údajů, obsahuje protokol rovněž silné záruky na ochranu soukromí a osobních údajů.

Ustanovení uvedená v následujících pododstavcích mají v protokolu obzvlášť důležitý charakter. Protokol doplňuje podrobná vysvětlující zpráva. Ačkoli vysvětlující zpráva nepředstavuje nástroj pro závazný výklad protokolu, jejím záměrem je „poskytnout smluvním stranám poradenství a pomoc“ při provádění protokolu.[22]

2.2.1. Společná ustanovení

Kapitola I protokolu stanoví společná ustanovení. Článek 2 stanoví oblast působnosti protokolu v souladu s oblastí působnosti úmluvy: použije se na konkrétní vyšetřování trestných činů nebo řízení související s trestnými činy, které se týkají počítačových systémů a údajů, a na shromažďování důkazů v elektronické formě o trestném činu.

---

[18] COM(2021) 170 final.

[19] Usnesení Evropského parlamentu ze dne 10. června 2021 o Strategii kybernetické bezpečnosti EU pro digitální dekádu.

[20] Odkaz L 304/47.

[21] https://rm.coe.int/0900001680a2aa42

[22] Viz odstavec 2 vysvětlující zprávy k protokolu.

V článku 3 jsou uvedeny definice týkající se „ústředních orgánů“, „příslušných orgánů“, „mimořádných událostí“, „osobních údajů“ a „předávající smluvní strany“. Tyto definice se společně s definicemi uvedenými v úmluvě vztahují na protokol.

Článek 4 stanoví jazyky, v nichž by měly smluvní strany podle protokolu předkládat příkazy, žádosti či oznámení.

2.2.2. Opatření týkající se spolupráce

Kapitola II protokolu stanoví opatření pro posílenou spolupráci. Ustanovení čl. 5 odst. 1 stanoví, že smluvní strany mají v co nejvyšší možné míře spolupracovat na základě protokolu. Ustanovení čl. 5 odst. 2 až 5 stanoví uplatňování opatření protokolu ve vztahu ke stávajícím smlouvám o vzájemné pomoci nebo ujednáním. Ustanovení čl. 5 odst. 7 stanoví, že opatření v kapitole II neomezují spolupráci mezi smluvními stranami, nebo s poskytovateli služeb či subjekty prostřednictvím dalších platných dohod, ujednání, postupů či vnitrostátních právních předpisů.

Článek 6 poskytuje základ pro přímou spolupráci mezi příslušnými orgány v jedné smluvní straně a subjekty poskytujícími služby registrace jména domény v jiné smluvní straně, pokud jde o zpřístupnění údajů registrace jména domény.

Článek 7 poskytuje základ pro přímou spolupráci mezi příslušnými orgány v jedné smluvní straně a poskytovateli služeb v jiné smluvní straně, pokud jde o zpřístupnění údajů o účastníkovi.

Článek 8 poskytuje základ pro posílenou spolupráci mezi orgány, pokud jde o zpřístupnění počítačových údajů.

Článek 9 poskytuje základ pro spolupráci mezi orgány, pokud jde o zpřístupnění počítačových údajů v případě mimořádné události.

Článek 10 poskytuje základ pro vzájemnou právní pomoc v případě mimořádné události.

Článek 11 poskytuje základ pro spolupráci prostřednictvím videokonference.

Článek 12 poskytuje základ pro společná vyšetřování a společné vyšetřovací týmy.

2.2.3. Záruky

Protokol se řídí přístupem založeným na právech se zvláštními podmínkami a zárukami, z nichž některé jsou stanoveny ve zvláštních opatřeních týkajících se spolupráce, jakož i v kapitole III protokolu. Článek 13 protokolu vyžaduje, aby smluvní strany zajistily, že pravomoci a postupy budou podléhat přiměřené úrovni ochrany základních práv, což v souladu s článkem 15 úmluvy zajistí uplatnění principu přiměřenosti.

Článek 14 protokolu stanoví ochranu osobních údajů, jak je vymezeno v článku 3 protokolu v souladu s pozměňovacím protokolem Úmluvy o ochraně osob se zřetelem na zpracování osobních dat (CETS 223) (úmluva č. 108+) a právem Unie.

Na tomto základě stanoví čl. 14 odst. 2 až 15 základní zásady ochrany údajů, včetně účelového omezení, právního základu, kvality údajů a pravidel vztahujících se na zpracovávání zvláštních kategorií údajů, povinností správců údajů, jako jsou uchovávání a vedení záznamů, bezpečnost s ohledem na další předávání údajů, vymahatelná individuální

práva, včetně oznamování, přístupu, opravy a automatizovaného rozhodování, nezávislého a účinného dohledu jednoho nebo více orgánů, jakož i správní a soudní ochrany. Záruky se vztahují na všechny formy spolupráce stanovené v protokolu, včetně nezbytných úprav prováděných v případě potřeby k řešení specifických rysů přímé spolupráce (např. v kontextu oznamování v případě porušení pravidel). Výkon některých práv jednotlivce lze pozdržet, omezit nebo odmítnout, je-li to nezbytné a přiměřené k dosažení důležitých cílů veřejného zájmu, zejména k zamezení rizika ohrožení probíhajících vyšetřování v oblasti vymáhání práva, což je rovněž v souladu s právem Unie.

Článek 14 protokolu je rovněž třeba vykládat ve spojení s článkem 23 protokolu. Článek 23 posiluje účinnost záruk v protokolu stanovením, že Výbor k Úmluvě o počítačové kriminalitě posoudí provádění a uplatňování opatření přijatých ve vnitrostátních právních předpisech s cílem uvést v účinnost ustanovení protokolu. Ustanovení čl. 23 odst. 3 výslovně uvádí, že se provádění článku 14 smluvními stranami posoudí ve chvíli, kdy deset smluvních stran úmluvy vyjádřilo svůj souhlas s tím, že budou protokolem vázány.

Další zárukou je – podle čl. 14 odst. 15 situace – to, že má-li jedna strana podstatný důkaz, že druhá strana soustavně nebo závažně porušuje záruky stanovené v protokolu, může po konzultaci (konzultace se nevyžaduje v naléhavém případě) pozastavit předávání osobních údajů uvedené smluvní straně. S veškerými osobními údaji předanými před tímto pozastavením je třeba i nadále zacházet v souladu s protokolem.

S ohledem na mnohostrannou povahu protokolu umožňuje čl. 14 odst. 1 písm. b) a c) protokolu smluvním stranám, aby se v rámci svých dvoustranných vztahů za určitých podmínek dohodly na jiných způsobech zajištění ochrany osobních údajů předávaných podle protokolu. Ačkoli se záruky podle čl. 14 odst. 2 až 15 standardně použijí na smluvní strany přijímající osobní údaje, smluvní strany, pro něž je vzájemně závazná mezinárodní dohoda, která stanoví komplexní rámec pro ochranu osobních údajů v souladu s příslušnými požadavky právních předpisů dotčených stran, mohou na základě čl. 14 odst. 1 písm. b) takový rámec rovněž využít. Týká se to například úmluvy č. 108+ (pro ty smluvní strany, které podle úmluvy umožňují předávání údajů druhým smluvním stranám) nebo zastřešující dohody mezi EU a USA (v rámci oblasti její působnosti, tj. pro předávání osobních údajů mezi orgány a v kombinaci s konkrétním ujednáním o předávání údajů mezi USA a EU v případě přímé spolupráce mezi orgány a poskytovateli služeb). Kromě toho mohou na základě čl. 14 odst. 1 písm. c) smluvní strany rovněž vzájemně stanovit, že se předávání osobních údajů uskuteční na základě jiných dohod nebo ujednání mezi dotčenými stranami. Členské státy EU se na tyto alternativní dohody nebo ujednání mohou spoléhat pouze v případě předávání údajů podle protokolu, pokud takové předávání splňuje požadavky práva Unie v oblasti ochrany údajů, zejména požadavky kapitoly V směrnice (EU) 2016/680 (směrnice o prosazování práva) a (pro přímou spolupráci mezi orgány a poskytovateli služeb podle článků 6 a 7 protokolu) požadavky kapitoly V nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů).

2.2.4. Závěrečná ustanovení

Kapitola IV protokolu stanoví závěrečná ustanovení. Ustanovením čl. 15 odst. 1 písm. a) je mimo jiné zajištěno, že smluvní strany mohou upravit své vztahy týkající se záležitostí stanovených v protokolu jinak, a to v souladu s čl. 39 odst. 2 úmluvy. Ustanovením čl. 15 odst. 1 písm. b) je zajištěno, že členské státy EU, které jsou smluvní stranou protokolu, mohou ve svých vzájemných vztazích nadále uplatňovat právo Unie. Ustanovení čl. 15 odst. 2 rovněž stanoví, že se čl. 39 odst. 3 úmluvy použije na protokol.

Z čl. 16 odst. 3 vyplývá, že protokol vstoupí v platnost v okamžiku, kdy pět smluvních stran úmluvy vyjádřilo svůj souhlas s tím, že budou protokolem vázány.

Ustanovení čl. 19 odst. 1 stanoví, že smluvní strany mohou využít výhrad v souvislosti s čl. 7 odst. 9 písm. a) a b), čl. 8 odst. 13 a článkem 17. Ustanovení čl. 19 odst. 2 stanoví, že smluvní strany mohou učinit prohlášení v souvislosti s čl. 7 odst. 2 písm. b) a odst. 8, čl. 8 odst. 11, čl. 9 odst. 1 písm. b) a odst. 5, čl. 10 odst. 9, čl. 12 odst. 3 a čl. 18 odst. 2. Ustanovení čl. 19 odst. 3 stanoví, že smluvní strana může učinit prohlášení, oznámení nebo sdělení uvedená v čl. 7 odst. 5 písm. a) a e), čl. 8 odst. 4 a 10 písm. a) a b), čl. 14 odst. 7 písm. c) a odst. 10 písm. b) a čl. 17 odst. 2.

Ustanovení čl. 23 odst. 1 stanoví základ pro konzultace mezi smluvními stranami, mimo jiné prostřednictvím Výboru k Úmluvě o počítačové kriminalitě, v souladu s článkem 46 úmluvy. Ustanovení čl. 23 odst. 2 rovněž poskytuje základ pro hodnocení použití a provádění ustanovení protokolu. Ustanovením čl. 23 odst. 3 je zajištěno, že hodnocení použití a provádění článku 14 o ochraně údajů bude zahájeno v okamžiku, kdy deset smluvních stran vyjádřilo svůj souhlas s tím, že bude protokolem vázáno.

2.3. Právo Unie a oblast politiky

Na oblast řízenou protokolem se z velké části vztahují společná pravidla vycházející z čl. 82 odst. 1 a článku 16 SFEU. Současný právní rámec Evropské unie zahrnuje především nástroje týkající se prosazování práva a justiční spolupráce v trestních záležitostech, například směrnici 2014/41/EU o evropském vyšetřovacím příkazu v trestních věcech, Úmluvu o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie a rámcové rozhodnutí Rady 2002/465/SVV o společných vyšetřovacích týmech. Evropská unie externě uzavřela řadu dvoustranných dohod mezi Unií a třetími zeměmi, například dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými, mezi Evropskou unií a Japonskem a mezi Evropskou unií a Norskem a Islandem. Současný právní rámec Evropské unie rovněž zahrnuje nařízení (EU) 2017/1939, kterým se provádí posílená spolupráce za účelem zřízení Úřadu evropského veřejného žalobce (EPPO). Členské státy, které se podílejí na posílené spolupráci, by měly zajistit, aby EPPO mohl při výkonu svých pravomocí ve smyslu článků 22, 23 a 25 nařízení (EU) 2017/1939 usilovat o spolupráci podle protokolu stejným způsobem jako státní žalobci těchto států. Tyto nástroje a dohody se týkají zejména článků 8, 9, 10, 11 a 12 protokolu.

Kromě toho Unie přijala několik směrnic, které posilují procesní práva podezřelých a obžalovaných osob.[23] Tyto nástroje se týkají zejména článků 6, 7, 8, 9, 10, 11, 12 a 13 protokolu. Jedna konkrétní řada záruk se týká ochrany osobních údajů, což je základní právo

[23] Směrnice Evropského parlamentu a Rady 2010/64/EU ze dne 20. října 2010 o právu na tlumočení a překlad v trestním řízení (Úř. věst. L 280, 26.10.2010, s. 1); směrnice Evropského parlamentu a Rady 2012/13/EU ze dne 22. května 2012 o právu na informace v trestním řízení (Úř. věst. L 142, 1.6.2012, s. 1); směrnice Evropského parlamentu a Rady 2013/48/EU ze dne 22. října 2013 o právu na přístup k obhájci v trestním řízení a řízení týkajícím se evropského zatýkacího rozkazu a o právu na informování třetí strany a právu na komunikaci s třetími osobami a konzulárními úřady v případě zbavení osobní svobody (Úř. věst. L 294, 6.11.2013, s. 1); směrnice Evropského parlamentu a Rady (EU) 2016/1919 ze dne 26. října 2016 o právní pomoci pro podezřelé nebo obviněné osoby v trestním řízení a pro osoby vyžádané v rámci řízení týkajícího se evropského zatýkacího rozkazu (Úř. věst. L 297, 4.11.2016, s. 1); směrnice Evropského parlamentu a Rady (EU) 2016/800 ze dne 11. května 2016 o procesních zárukách pro děti, které jsou podezřelými nebo obviněnými osobami v trestním řízení (Úř. věst. L 132, 21.5.2016, s. 1); směrnice Evropského parlamentu a Rady (EU) 2016/343 ze dne 9. března 2016, kterou se posilují některé aspekty presumpce neviny a právo být přítomen při trestním řízení před soudem (Úř. věst. L 65, 11.3.2016, s. 1); směrnice Evropského parlamentu a Rady 2012/13/EU ze dne 22. května 2012 o právu na informace v trestním řízení.

zakotvené ve Smlouvách EU a v Listině základních práv Evropské unie. Osobní údaje je možné zpracovávat pouze v souladu s nařízením (EU) 2016/679 (obecné nařízení o ochraně osobních údajů) a směrnicí (EU) 2016/680 (směrnice o prosazování práva). Základní právo jednotlivců na respektování jejich soukromého a rodinného života, obydlí a komunikace zahrnuje jako základní prvek právo na respektování soukromí komunikace. Údaje o elektronických komunikacích lze zpracovávat pouze v souladu se směrnicí 2002/58/ES (směrnice o soukromí a elektronických komunikacích). Tyto nástroje se týkají zejména článku 14 protokolu.

Ustanovení čl. 14 odst. 2 až 15 protokolu stanoví vhodné záruky na ochranu údajů ve smyslu pravidel Unie pro ochranu osobních údajů, zejména článku 46 obecného nařízení o ochraně osobních údajů a článku 37 směrnice o prosazování práva a příslušné judikatury Soudního dvora Evropské unie. V souladu s požadavky práva Unie[24] a za účelem zajištění účinnosti záruk stanovených v článku 14 protokolu by členské státy měly zajistit, aby bylo osobám, jejichž údaje byly předány, v tomto smyslu zasláno oznámení, s výhradou některých omezení, například, aby nedošlo k ohrožení probíhajícího vyšetřování. Ustanovení čl. 14 odst. 11 písm. c) protokolu poskytuje základ pro plnění tohoto požadavku ze strany členských států.

Soulad čl. 14 odst. 1 protokolu s pravidly Unie pro ochranu osobních údajů rovněž vyžaduje, aby následující skutečnosti členské státy zvážily s ohledem na možné alternativní způsoby zajištění vhodné ochrany osobních údajů předávaných podle protokolu. Pokud jde o jiné mezinárodní dohody, které stanoví komplexní rámec pro ochranu osobních údajů v souladu s použitelnými požadavky právních předpisů dotčených smluvních stran, členské státy by podle čl. 14 odst. 1 písm. b) měly vzít na vědomí, že pro přímou spolupráci musí být zastřešující dohoda mezi EU a USA doplněna dalšími zárukami – které budou stanoveny ve zvláštním ujednání o předávání údajů mezi USA a EU / jejími členskými státy, – jež zohlední jedinečné požadavky na předávání elektronických důkazů přímo poskytovateli služeb, a nikoliv mezi orgány.[25]

Podle čl. 14 odst. 1 písm. b) protokolu by členské státy rovněž měly vzít na vědomí, že pro členské státy EU, které jsou smluvními stranami úmluvy č. 108+, neposkytuje úmluva sama o sobě vhodný základ pro přeshraniční předávání údajů v rámci protokolu druhým smluvním stranám uvedené úmluvy. V tomto ohledu by měly zvážit poslední větu čl. 14 odst. 1 úmluvy č. 108+[26].

---

[24] Viz posudek 1/15 Soudního dvora (velkého senátu), ECLI:EU:C:2017:592, odstavec 220. Viz také příspěvek EDPB ke konzultaci o návrhu druhého dodatkového protokolu k Úmluvě Rady Evropy o počítačové kriminalitě (Budapešťská úmluva), 13. listopadu 2019, s. 6 („Příslušné vnitrostátní orgány, jimž byl poskytnut přístup k údajům, musí o tomto přístupu vyrozumět dotčené osoby v rámci použitelných vnitrostátních postupů, a to od okamžiku, kdy tímto sdělením nebude možné ohrozit probíhající vyšetřování vedené těmito orgány. … Toto oznámení je nezbytné k tomu, aby dotčené osoby mohly mimo jiné uplatnit své právo na podání opravného prostředku a práva na ochranu údajů v souvislosti se zpracováním jejich údajů“).

[25] Z tohoto důvodu rozhodnutí Rady ze dne 21. května 2019 o zmocnění k zahájení jednání za účelem uzavření dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech (9114/19) ve svých směrnicích pro jednání obsahuje řadu dalších záruk na ochranu údajů. Směrnice o jednání konkrétně uvádějí, že „Dohoda by měla zastřešující dohodu doplňovat o další záruky, které zohlední úroveň citlivosti kategorií dotčených údajů a jedinečné požadavky na předávání elektronických důkazů přímo poskytovateli služeb spíše než mezi orgány a předávání příslušnými orgány přímo poskytovatelům služeb.“

[26] Viz také vysvětlující zpráva k protokolu o změně Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat, ze dne 10. října 2018, body 106–107.

Pokud jde o jiné dohody nebo ujednání podle čl. 14 odst. 1 písm. c), členské státy by měly vzít na vědomí, že mohou těchto jiných dohod nebo ujednání využít pouze v případě, že Evropská komise v souvislosti s dotčenou třetí zemí přijala – podle článku 45 obecného nařízení o ochraně osobních údajů (nařízení (EU) 2016/679) či podle článku 36 směrnice (EU) 2016/680 o prosazování práva – rozhodnutí o odpovídající ochraně, které se týká příslušných předávání údajů, nebo v případě, že tato jiná dohoda nebo ujednání samy o sobě poskytují přiměřené záruky ochrany údajů podle článku 46 obecného nařízení o ochraně osobních údajů nebo čl. 37 odst. 1 písm. a) směrnice o prosazování práva.

Je třeba, aby se přihlédlo nejen k současnému stavu práva Unie v dané oblasti, ale rovněž k jeho budoucímu vývoji do té míry, do jaké to lze předvídat v době provedení analýzy. Oblast, na níž se vztahuje protokol, je přímo relevantní pro předpokládaný budoucí vývoj práva Unie. V této souvislosti je třeba připomenout návrhy Komise o přeshraničním přístupu k elektronickým důkazům z dubna 2018.[27] Tyto nástroje se týkají zejména článků 6 a 7 protokolu.

Komise při účasti na jednáních jménem Unie zajistila, aby byl protokol plně slučitelný s právem Unie a povinnostmi členských států, které z něj vyplývají. Komise zejména zajistila, aby ustanovení protokolu umožnila členským státům dodržovat základní práva, svobody a obecné zásady práva Unie, jak jsou zakotveny ve Smlouvách EU a Listině základních práv, včetně proporcionality, procesních práv, presumpce neviny a práv na obhajobu osob, proti nimž je vedeno trestní řízení, jakož i práva na soukromí a ochranu osobních údajů a údajů o elektronických komunikacích při jejich zpracovávání, předávání údajů donucovacím orgánům v zemích mimo Evropskou unii, a veškerých povinností, které v této souvislosti mají donucovací a justiční orgány. Komise rovněž vzala na vědomí stanovisko evropského inspektora ochrany údajů[28] a Evropského sboru pro ochranu osobních údajů.[29]

Komise dále zajistila, aby byla ustanovení protokolu a návrhy Komise k elektronickým důkazům slučitelné – mimo jiné proto, že se tyto návrhy právních předpisů vyvíjely během diskusí se spolunormotvůrci – a aby protokol nevedl ke kolizi norem. Komise zejména zajistila, aby protokol obsahoval vhodné záruky týkající se ochrany údajů a soukromí, což umožňuje poskytovatelům služeb EU, aby dodržovali své povinnosti v rámci právních předpisů EU o ochraně osobních údajů a soukromí, pokud protokol stanoví právní důvod pro předání údajů v reakci na příkazy vydané nebo žádosti podané orgánem ze státu mimo EU, jenž je smluvní stranou protokolu, kterými se vyžaduje, aby správce nebo zpracovatel zpřístupnil osobní údaje nebo údaje o elektronických komunikacích.

2.4. Výhrady, prohlášení, oznámení, sdělení a další komentáře

Protokol poskytuje základ k tomu, aby smluvní strany mohly využít některých výhrad a učinit prohlášení, oznámení nebo sdělení ve vztahu k některým článkům. Členské státy by měly zaujmout jednotný přístup k některým výhradám, prohlášením, oznámením a sdělením

[27] COM(2018) 225 a 226 final.

[28] Stanovisko evropského inspektora ochrany údajů 3/2019 týkající se účasti na jednáních s ohledem na druhý dodatkový protokol k Budapešťské úmluvě o počítačové kriminalitě ze dne 2. dubna 2019.

[29] Mimo jiné také „příspěvek EDPB ke konzultaci o návrhu druhého dodatkového protokolu k Úmluvě Rady Evropy o počítačové kriminalitě (Budapešťská úmluva) ze dne 13. listopadu 2019“; „stanovisko 02/201 o novém návrhu ustanovení druhého dodatkového protokolu k Úmluvě Rady Evropy o počítačové kriminalitě (Budapešťská úmluva) přijatého dne 2. února 2021“; „příspěvek EDPB k šestému kolu konzultací o návrhu druhého dodatkového protokolu k Budapešťské úmluvě Rady Evropy o počítačové kriminalitě ze dne 4. května 2021“.

stanoveným v příloze tohoto rozhodnutí. Aby byl zajištěn soulad provádění protokolu s právem Unie, měly by členské státy EU ve vztahu k těmto výhradám a prohlášením zaujmout níže uvedený postoj. Stanoví-li protokol základ pro jiné výhrady a jiná prohlášení, oznámení nebo sdělení, opravňuje tento návrh členské státy k tomu, aby zvážily a učinily vlastní výhrady, prohlášení, oznámení nebo sdělení.

Aby byl zajištěn soulad mezi ustanoveními protokolu a příslušným právem a politikami Unie, neměly by členské státy využít výhrad podle čl. 7 odst. 9 písm. a)[30] a písm. b)[31]. Členské státy by navíc měly učinit prohlášení podle čl. 7 odst. 2 písm. b)[32] a oznámení podle čl. 7 odst. 5 písm. a)[33]. Skutečnost, že členské státy nevyužijí těchto výhrad a učiní prohlášení a oznámení, je důležitá k zajištění souladu protokolu s legislativními návrhy Komise k elektronickým důkazům, mimo jiné proto, že se tyto návrhy právních předpisů vyvíjejí během diskusí se spolunormotvůrci.

Aby bylo navíc zajištěno jednotné provádění protokolu členskými státy EU v okamžiku, kdy spolupracují se smluvními stranami, které nejsou členskými státy EU, vyzývají se členské státy k tomu, aby nevyužily výhradu podle čl. 8 odst. 13[34], mimo jiné vzhledem k recipročnímu účinku takové výhrady[35]. Členské státy by měly učinit prohlášení podle čl. 8 odst. 4, aby bylo možné zajistit provedení příkazů v případě, že by byly třeba další podpůrné informace – např. o okolnostech dotčeného případu – s cílem posoudit proporcionalitu a nezbytnost.[36]

Členské státy se rovněž vyzývají k tomu, aby nečinily prohlášení podle čl. 9 odst. 1 písm. b)[37], s cílem zajistit účinné provádění protokolu.

Členské státy by měly učinit sdělení podle čl. 7 odst. 5 písm. e)[38], čl. 8 odst. 10 písm. a) a b)[39], čl. 14 odst. 7 písm. c) a odst. 10 písm. b), aby bylo celkově zajištěno účinné provádění protokolu.[40]

---

[30] Umožňující smluvním stranám vyhradit si právo neuplatňovat článek 7 (zpřístupnění údajů o účastníkovi).

[31] Umožňující smluvním stranám vyhradit si právo neuplatňovat článek 7 (zpřístupnění údajů o účastníkovi) na určité druhy přístupových čísel, pokud by to bylo v rozporu se základními zásadami jejich vnitrostátního právního systému.

[32] Umožňující smluvním stranám prohlásit, že příkaz podle čl. 7 odst. 1 (zpřístupnění údajů o účastníkovi) musí být vydán žalobcem nebo jiným justičním orgánem nebo pod jejich dohledem, nebo musí být vydán jiným způsobem pod nezávislým dohledem.

[33] Umožňující smluvním stranám oznámit generálnímu tajemníkovi Rady Evropy, že pokud je podle čl. 7 odst. 1 (zpřístupnění údajů o účastníkovi) vydán poskytovateli služeb příkaz na jejím území, vyžaduje smluvní strana v každém případě, nebo za určitých zjištěných okolností, souběžné oznámení příkazu, doplňující informace a shrnutí skutečností, které souvisejí s vyšetřováním nebo řízením.

[34] Umožňující smluvním stranám vyhradit si právo neuplatňovat článek 8 (provedení příkazů jiné smluvní strany) na provozní údaje.

[35] Viz odstavec 147 vysvětlující zprávy k protokolu, který stanoví, že „smluvní straně, která si vyhrazuje svá práva, pokud jde o tento článek, není povoleno, aby předkládala příkazy týkající se provozních údajů druhým smluvním stranám podle [čl. 8,] odst. 1“.

[36] Umožňující smluvním stranám prohlásit, že jsou k provedení příkazů podle čl. 8 odst. 1 (provedení příkazů jiné smluvní strany) vyžadovány další podpůrné informace.

[37] Umožňující smluvním stranám prohlásit, že nebudou vyřizovat žádosti podle čl. 9 odst. 1 písm. a) (urychlené zpřístupnění počítačových údajů v případě mimořádné události), v nichž se požaduje pouze zpřístupnění údajů o účastníkovi.

[38] Umožňující smluvním stranám sdělovat kontaktní údaje orgánu určeného k přijímání oznámení podle čl. 7 odst. 5 písm. a) a provádět činnosti uvedené v čl. 7 odst. 5 písm. b), c) a d) (zpřístupnění údajů o účastníkovi).

[39] Umožňující smluvním stranám sdělit kontaktní údaje orgánů určených k předkládání a přijímání příkazů podle článku 8 (provedení příkazů jiné smluvní strany). V souladu s požadavky nařízení (EU) 2017/1939 by

Členské státy by rovněž měly přijmout nezbytná opatření podle čl. 14 odst. 11 písm. c) s cílem zajistit, aby přijímající smluvní strana byla v okamžiku předání informována o povinnosti podle práva Unie zaslat oznámení osobě, jíž se údaje týkají[41], a poskytnout příslušné kontaktní údaje, aby přijímající smluvní strana mohla informovat příslušný orgán v členském státě EU, jakmile přestanou platit omezení týkající se důvěrnosti a jakmile bude možné oznámení učinit.

2.5. Odůvodnění návrhu

Protokol vstoupí v platnost v okamžiku, kdy pět smluvních stran vyjádřilo svůj souhlas s tím, aby byly protokolem vázány v souladu s ustanoveními čl. 16 odst. 1 a 2. Slavnostní podpis protokolu se má uskutečnit v březnu 2022.

Členské státy by měly podniknout nezbytné kroky, aby protokol rychle vstoupil v platnost a byl ratifikován, což je důležité z několika důvodů.

Za prvé, protokol zajistí, aby donucovací a justiční orgány byly lépe vybaveny k získávání elektronických důkazů nezbytných k vyšetřování trestných činů. S ohledem na rostoucí význam elektronických důkazů pro vyšetřování trestných činů je urgentní, aby donucovací a justiční orgány měly k dispozici vhodné nástroje k získání přístupu k elektronickým důkazům efektivním způsobem, a mohly tak účinně bojovat proti trestné činnosti online.

Za druhé, protokol zajistí, aby taková opatření k získání přístupu k elektronickým důkazům byla využívána způsobem, který členským státům umožní dodržovat základní práva, včetně procesních práv v trestním řízení, práva na soukromí a práva na ochranu osobních údajů. Neexistují-li jasná pravidla na mezinárodní úrovni, mohou současné praktiky představovat výzvu z hlediska právní jistoty, transparentnosti, odpovědnosti a dodržování základních práv a procesních záruk pro podezřelé ve vyšetřování trestných činů.

Za třetí, protokol vyřeší a zabrání kolizi norem, která postihuje orgány, poskytovatele služeb v soukromém sektoru a další subjekty, a to stanovením slučitelných pravidel pro přeshraniční přístup k elektronickým důkazům na mezinárodní úrovni.

Za čtvrté, protokol prokáže trvalý význam úmluvy coby hlavního mnohostranného rámce v boji proti kyberkriminalitě. To bude hrát zásadní úlohu v procesu navazujícím na rezoluci Valného shromáždění OSN č. 74/247 z prosince 2019 o „boji proti užívání informačních a komunikačních technologií k trestným účelům“, jež zřídila otevřený *ad hoc* mezivládní výbor odborníků, kteří mají vypracovat komplexní mezinárodní úmluvu o boji proti užívání informačních a komunikačních technologií k trestným účelům.

3. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- *Právní základ*

členské státy, které se podílejí na posílené spolupráci za účelem zřízení Úřadu evropského veřejného žalobce (EPPO), měly uvádět tento úřad ve své komunikaci.

[40] Umožňující smluvním stranám sdělit orgán či orgány, které by měly obdržet oznámení v případě bezpečnostního incidentu, nebo by měly být pro účely předchozího oprávnění kontaktovány v případě dalšího předávání údajů do jiného státu nebo jiné organizaci.

[41] Viz výše poznámka pod čarou č. 24.

Pravomoc Unie provádět legislativní kroky v záležitostech týkajících se usnadnění spolupráce mezi justičními a rovnocennými orgány ve vztahu k řízení v trestních věcech a výkonu rozhodnutí vychází z čl. 82 odst. 1 SFEU. Pravomoc Unie v záležitostech týkajících se ochrany osobních údajů vychází z článku 16 SFEU.

V souladu s čl. 3 odst. 2 SFEU má Unie výlučnou pravomoc uzavřít mezinárodní smlouvu, pokud její uzavření může ovlivnit společná pravidla EU či změnit jejich působnost. Ustanovení protokolu spadají do oblasti, na níž se z velké části vztahují společná pravidla, jak je stanoveno v oddíle 2.3 výše.

Protokol tudíž spadá do výlučné vnější pravomoci Unie. Ratifikace protokolu členskými státy v zájmu Unie se tudíž může uskutečnit na základě článku 16, čl. 82 odst. 1 a čl. 218 odst. 6 SFEU.

- *Subsidiarita (v případě nevýlučné pravomoci)*

Nevztahuje se na tento návrh.

- *Proporcionalita*

Pokud jde o tento návrh, lze cílů Unie uvedených v oddíle 2.5 výše dosáhnout pouze uzavřením závazné mezinárodní dohody, která stanoví nezbytná pravidla spolupráce a zajistí vhodnou ochranu základních práv. Protokol tohoto cíle dosahuje. Ustanovení protokolu jsou omezena na to, co je nezbytné k dosažení jeho hlavních cílů. Jednostranné kroky nejsou alternativou, neboť by neposkytly dostatečný základ pro spolupráci se zeměmi mimo EU a nemohly by zajistit nezbytnou ochranu základních práv. Dodržování mnohostranné dohody, jako je protokol, kterou Unie byla schopná vyjednat, je účinnější než zahájení jednání s jednotlivými zeměmi mimo EU na dvoustranné úrovni. Za předpokladu, že všech 66 smluvních stran, jakož i budoucí nové smluvní strany úmluvy, protokol ratifikují, poskytne protokol společný právní rámec pro spolupráci členských států EU s jejich nejvýznamnějšími mezinárodními partnery v boji proti trestné činnosti.

- ***Volba nástroje***

Nevztahuje se na tento návrh.

4. VÝSLEDKY HODNOCENÍ *EX-POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- *Hodnocení ex-post / kontroly účelnosti platných právních předpisů*

Nevztahuje se na tento návrh.

- *Konzultace se zúčastněnými stranami*

Rada Evropy uspořádala šest kol veřejných konzultací ve vztahu k jednání o protokolu, a to v červenci a listopadu 2018, únoru a listopadu 2019, prosinci 2020 a v květnu 2021.[42] Smluvní strany zvážily podněty, které byly obdrženy v rámci těchto konzultací.

Komise si ve své úloze vyjednavače jménem Unie rovněž vyměnila názory s úřady pro ochranu údajů a v průběhu let 2019 a 2021 uspořádala cílená konzultační setkání s organizacemi občanské společnosti, poskytovateli služeb a obchodními sdruženími. Komise vzala na vědomí podněty, které byly obdrženy v rámci těchto výměn.

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations

- *Shromažďování a využití výsledků odborných konzultací*

V průběhu jednání Komise soustavně konzultovala se zvláštním výborem Rady pro jednání v souladu s rozhodnutím Rady Evropské unie ze dne 6. června 2019, které Komisi zmocňuje k účasti na jednání jménem Unie, což poskytlo příležitost odborníkům z členských států k tomu, aby přispěly k procesu vymezení postoje Unie. Řada odborníků z členských států se i nadále podílela na jednáních společně s Komisí, která se účastnila jménem Unie. Rovněž se uskutečnily konzultace se zúčastněnými stranami (viz výše).

- *Posouzení dopadů*

Posouzení dopadů bylo provedeno v letech 2017–2018, aby doplnilo návrhy Komise k elektronickým důkazům.[43] V této souvislosti bylo jednání o dohodě o druhém dodatkovém protokolu k Budapešťské úmluvě o počítačové kriminalitě součástí upřednostňované možnosti. Relevantní dopady jsou navíc uvedeny v této důvodové zprávě.

- *Účelnost právních předpisů a zjednodušení*

Protokol může mít důsledky pro některé kategorie poskytovatelů služeb, včetně malých a středních podniků, neboť se na ně mohou podle protokolu vztahovat příkazy a žádosti týkající se elektronických důkazů. Nicméně tito poskytovatelé služeb již v současné době takové žádosti často obdrží prostřednictvím jiných existujících kanálů; mnohdy jsou zasílány různými orgány, mimo jiné na základě úmluvy[44], jiných smluv o vzájemné právní pomoci nebo jiných rámců, včetně mnohostranných politik v oblasti správy internetu.[45] Poskytovatelé služeb, včetně malých a středních podniků, využijí rovněž jasného právního rámce na mezinárodní úrovni a společného přístupu smluvních stran protokolu.

- *Základní práva*

V případech, kdy lze údaje o dané osobě získat v rámci trestního řízení, budou mít nástroje spolupráce uvedené v protokolu pravděpodobně vliv na základní práva, tedy např. právo na spravedlivý proces, právo na soukromí a právo na ochranu osobních údajů. Protokol se řídí přístupem založeným na právech a stanoví podmínky a záruky v souladu s mezinárodními nástroji pro lidská práva, včetně Úmluvy Rady Evropy z roku 1950 o ochraně lidských práv a základních svobod. Protokol zejména stanoví zvláštní záruky ochrany údajů. Protokol v případě potřeby rovněž poskytuje základ k tomu, aby smluvní strany mohly využít některých výhrad, prohlášení nebo oznámení a uvádí důvody k odmítnutí spolupráce v reakci na žádost ve zvláštních situacích. Tím je zajištěn soulad protokolu s Listinou základních práv EU.

5. ROZPOČTOVÉ DŮSLEDKY

Rozhodnutí nemá žádné důsledky pro rozpočet Unie. Členským státům mohou vzniknout jednorázové náklady na zavedení protokolu a vyšší náklady by mohly vzniknout orgánům členských států z důvodu očekávaného nárůstu případů.

---

[43] SWD(2018) 118 final.

[44] Viz například pokyny Výboru k Úmluvě o počítačové kriminalitě č. 10 ze dne 1. března 2017 o příkazech k předložení týkajících se informací o účastníkovi (článek 18 Budapešťské úmluvy).

[45] Viz například usnesení rady Internetového sdružení pro přidělování jmen a čísel (ICANN) ze dne 15. května 2019 o doporučení k dočasné specifikaci registračních údajů domén gTLD, k dispozici na adrese www.icann.org.

6. OSTATNÍ PRVKY

- *Plány provádění a způsoby monitorování, hodnocení a podávání zpráv*

Není zaveden žádný prováděcí plán, neboť se po podpisu a ratifikaci protokolu bude od členských států požadovat jeho provádění.

Pokud jde o monitorování, Komise se bude účastnit schůzí Výboru k Úmluvě o počítačové kriminalitě, kde bude Evropská unie uznávána jako pozorovatelská organizace.

2021/0383 (NLE)

Návrh

ROZHODNUTÍ RADY,

kterým se členské státy zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16, čl. 82 odst. 1 a čl. 218 odst. 6 této smlouvy,

s ohledem na návrh Evropské komise,

s ohledem na souhlas Evropského parlamentu,

vzhledem k těmto důvodům:

(1) Dne 9. června 2019 zmocnila Rada Komisi k účasti na jednáních jménem Evropské unie o druhém dodatkovém protokolu k Budapešťské úmluvě neboli Úmluvě Rady Evropy o počítačové kriminalitě.

(2) Znění druhého dodatkového protokolu k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů (dále jen „protokol“) bylo přijato Výborem ministrů Rady Evropy dne 17. listopadu 2021 a očekává se, že bude otevřeno k podpisu v březnu 2022.

(3) Ustanovení protokolu spadají do oblasti, na níž se ve velké míře vztahují společná pravidla ve smyslu čl. 3 odst. 2 Smlouvy o fungování EU, včetně nástrojů k usnadnění justiční spolupráce v trestních věcech, které zajišťují minimální standardy procesních práv, jakož i záruky na ochranu údajů a soukromí.

(4) Komise rovněž předložila legislativní návrh nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech (COM(2018) 225 final), jakož i návrh směrnice, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení (COM(2018) 226 final), jimiž se zavádí závazné přeshraniční evropské předávací a uchovávací příkazy, které mají být určeny přímo zástupci poskytovatele služeb v jiném členském státě.

(5) Během své účasti na jednáních jménem Unie zajistila Komise soulad druhého dodatkového protokolu s příslušnými společnými pravidly Evropské unie.

(6) K zajištění souladu protokolu s právem a politikami Unie a jednotného provádění protokolu mezi členskými státy EU v jejich vztahu ke smluvním stranám, které nejsou členskými státy EU, jakož i k zajištění účinného provádění protokolu, jsou důležité některé výhrady, prohlášení, oznámení a sdělení.

(7) Vzhledem k tomu, že protokol stanoví rychlá řízení, která zlepšují přeshraniční přístup k elektronickým důkazům, a vysokou úroveň záruk, jeho vstup v platnost přispěje k boji proti kyberkriminalitě a jiným formám trestné činnosti na celosvětové úrovni tím, že usnadní spolupráci mezi smluvními stranami protokolu, které jsou členskými státy

EU, a smluvními stranami protokolu, které členskými státy EU nejsou, zajistí vysokou úroveň ochrany fyzických osob a vyřeší kolizi norem.

(8) Vzhledem k tomu, že protokol stanoví vhodné záruky v souladu s požadavky na mezinárodní předávání osobních údajů podle nařízení (EU) 2016/679 a směrnice (EU) 2016/680, jeho vstup v platnost přispěje k podpoře standardů Unie pro ochranu údajů na celosvětové úrovni, usnadní toky údajů mezi smluvními stranami protokolu, které jsou členskými státy EU, a smluvními stranami protokolu, které členskými státy EU nejsou, a zajistí, aby členské státy EU plnily své povinnosti v souladu s pravidly Unie pro ochranu údajů.

(9) Kromě toho rychlý vstup protokolu v platnost rovněž potvrdí úlohu Budapešťské úmluvy Rady Evropy coby hlavního mnohostranného rámce v boji proti kyberkriminalitě.

(10) Evropská unie se nemůže stát smluvní stranou protokolu, neboť protokol i Úmluva Rady Evropy o počítačové kriminalitě jsou otevřeny pouze státům.

(11) Členské státy by proto měly být zmocněny k ratifikaci protokolu, jednajíce společně v zájmu Evropské Unie.

(12) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne…

(13) [V souladu s články 1 a 2 protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a aniž je dotčen článek 4 uvedeného protokolu, se Irsko neúčastní přijímání tohoto rozhodnutí a toto rozhodnutí pro ně není závazné ani použitelné].

[NEBO]

[V souladu s články 1 a 2 protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, a aniž je dotčen článek 4 uvedeného protokolu, Irsko oznámilo [dopisem ze dne... ,] své přání účastnit se přijímání a používání tohoto rozhodnutí.]

(14) V souladu s články 1 a 2 Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o Evropské unii a ke Smlouvě o fungování Evropské unie, se Dánsko neúčastní přijímání tohoto rozhodnutí a toto rozhodnutí pro ně není závazné ani použitelné,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Členské státy se zmocňují, aby v zájmu Evropské unie ratifikovaly druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílené spolupráci a zpřístupňování elektronických důkazů (dále jen „protokol“).

Článek 2

Při ratifikaci protokolu členské státy vznesou výhrady či učiní prohlášení, oznámení nebo sdělení uvedená v příloze.

Článek 3

Toto rozhodnutí vstupuje v platnost dnem přijetí.

Článek 4

Toto rozhodnutí se vyhlašuje v *Úředním věstníku Evropské unie*.

Článek 5

Toto rozhodnutí je určeno členským státům.

V Bruselu dne

Za Radu
předseda/předsedkyně