POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

DIPLOMOVÁ PRÁCE

2022 HANA ČEJPOVÁ

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra veřejného práva

Elektronické důkazy v evropském právu

Diplomová práce

Electronic Evidence in European Law

Master thesis

VEDOUCÍ PRÁCE
prof. Dr. iur. Harald Christian Scheu, Mag. phil., Ph.D.

AUTOR PRÁCE
Mgr. Hana Čejpová

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 31. 8. 2022

Mgr. Hana Čejpová

Poděkování

Na tomto místě bych ráda poděkovala prof. Dr. iur. Haraldu Christianu Scheuovi, Mag. phil., Ph.D. za odborné vedení mé práce, za jeho čas a trpělivost a také za cenné a velmi podnětné rady při zpracovávání práce.

.

ANOTACE

Diplomová práce se věnuje návrhu nového Nařízení Evropského parlamentu a Rady o evropských příkazech a návrhu Směrnice ustanovující pravidla pro jmenování právních zástupců poskytovatelů služeb v trestním řízení. Cílem obou návrhů je usnadnění a zrychlení přístupu orgánů činných v trestním řízení k elektronickým důkazům, které jsou uchovávány na území jiného státu. V práci jsou současně popsány stávající metody justiční spolupráce, které jsou pro získávání elektronických důkazů, kde hrozí jejich ztráta, neefektivní. Nové Nařízení přináší nejen výhody co do rychlosti obdržení požadovaných důkazů, ale i úskalí v podobě zásahů do základních práv a svobod občanů i účastníků trestního řízení. Doporučení na odstranění nedostatků návrhu Nařízení je součástí práce, stejně tak, jako momentální postoje Rady a Parlamentu k jednotlivým článkům návrhu.

KLÍČOVÁ SLOVA

Elektronické důkazy * Počítačová kriminalita * Úmluva o počítačové kriminalitě * Druhý dodatkový protokol k Úmluvě * Evropský předávací příkaz * Evropský uchovávací příkaz

ANNOTATION

The thesis focuses on the proposal of a new Regulation of the European Parliament and Council on European Production and Preservation Orders for electronic evidence, including Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. The aim of both proposals is to facilitate and speed up the access of the police and judicial authorities to the electronic evidence held at the territory of another state. The thesis also describes existing methods of judicial cooperation, ineffective for obtaining electronic evidence, which is at risk of being lost. The new Regulation brings not only advantages in terms of quick access to the requested evidence, but also pitfalls related to the interference to the fundamental rights of citizens and participants of the criminal proceedings. Recommendations to remedy the shortcomings of the draft Regulation are included in the thesis, as well as the current positions introduced by the Council and Parliament on the respective articles of the Regulation.

KEYWORDS

Electronic evidence* Cybercrime* Cybercrime treaty* Second additional protocol*Mutual Legal Assistance*European Investigation Order* European production order* European preservation order

Obsah

Seznam zkratek

COPEN	Pracovní skupina pro spolupráci v trestních věcech
EJS	Evropská justiční síť
EJCN	Evropská justiční síť pro boj s počítačovou kriminalitou
EU	Evropská unie
EP	Evropský parlament
EPPO	Úřad Evropského veřejného žalobce
EPP	Evropský předávací příkaz
EPOC	Certifikát evropského předávacího příkazu pro předání elektronických důkazů
EPOC – CR	Certifikát evropského uchovávacího příkazu pro uchování elektronických důkazů
EUP	Evropský uchovávací příkaz
EVP	Evropský vyšetřovací příkaz
LIBE	Výbor Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní záležitosti
MLA	Mutual Legal Assitance
OČTŘ	Orgány činné v trestním řízení
SDEU	Soudní dvůr Evropské Unie
SVT	Společné vyšetřovací týmy
ZMJS	Zákon o mezinárodní justiční spolupráci

Úvod

Prudký nárůst využívání digitálních technologií v posledních 15 letech a jejich pokračující rozvoj na jedné straně významně usnadnil náš každodenní život, na druhé straně bohužel zvýšil bezpečnostní riziko v podobě jejich zneužívání. Krajním případem takového zneužívání je trestná činnost v kyberprostoru neboli tzv. počítačová kriminalita.

Předmětem této práce není věnovat se všem aspektům počítačové kriminality, nýbrž možnostem jejího prokazování prostřednictvím tzv. elektronických důkazů. Dané je aktuálně horké téma diskusí na půdě Evropské komise. Právě na této platformě se projednává návrh Nařízení Evropského parlamentu a Rady o evropských příkazech k vydání a uchování elektronických důkazů v trestním řízení (dále jen Nařízení) spolu s návrhem Směrnice stanovující harmonizovaná pravidla pro ustanovení právních zástupců za účelem získávání důkazů v trestním řízení (dále jen Směrnice). Jde o zavedení nových nástrojů mezinárodní justiční spolupráce v trestních věcech v boji s počítačovou trestnou činností, jejichž implementace do evropského práva by měla přispět především k rychlejšímu a efektivnějšímu přeshraničnímu získávání elektronických důkazů orgánům činným v trestním řízení.

Než se budu věnovat samotnému návrhu Nařízení, jeho přínosům a rizikům, hned v úvodu vysvětlím pojem elektronických důkazů a jejich definici z hlediska právní úpravy. Jelikož český trestní řád neobsahuje definici elektronického důkazu jako takového, je nutné vysvětlit, jaká ustanovení trestního řádu se k elektronickým důkazům vztahují. Pojem elektronických důkazů bude vysvětlen i ve vztahu k jazykovým odlišnostem v mezinárodním prostředí, a to především pro potřeby navrhované nové právní úpravy. Přestože téma elektronických důkazů není žádnou novinkou v oblasti vyšetřování a stíhání počítačové trestné činnosti, rozhodně nemůže být řečeno, že by se interpretace definice elektronických důkazů jednotlivými členskými státy shodovala. Proto jsem se rozhodla porovnat odlišné pojetí definic a jejich zakotvení v trestních řádech vybraných členských států.

Považuji za nezbytné detailně uvést jednotlivé druhy elektronických důkazů, jelikož jejich uchovávání, shromažďování a získávání je předmětem nové právní úpravy. Na jednotlivé druhy elektronických údajů, které OČTŘ zpravidla vyžadují, se vztahují různá přístupová pravidla, která stanovují, kdo a jakým způsobem může o tato data žádat. Všechny kategorie elektronických údajů obsahují osobní údaje, a proto je nutné podotknout, že se na ně vztahují záruky o ochraně osobních údajů. Právě problematika zásahu do základních práv přináší řadu sporných otázek, které budou rozebrány v příslušné kapitole o možných rizicích.

Důvodem nové navrhované právní úpravy pro elektronické důkazy je fakt, že stávající nástroje mezinárodní justiční spolupráce sloužící k jejich získávání jsou nedostačující. Lze konstatovat, že nejsou z důvodu příliš zdlouhavého procesu vyřizování žádostí o poskytnutí důkazů příliš efektivní. Přesto jsou zatím jedinou možností OČTŘ, a proto je potřeba tyto formy spolupráce představit. V souvislosti s aktuálními nástroji justiční spolupráce budu následně pracovat s Úmluvou o počítačové kriminalitě včetně jejího Druhého dodatkového protokolu coby s nejvýznamnější a nejucelenější dohodou Rady Evropy o počítačové kriminalitě a elektronických důkazech[1]. Dále se pokusím specifikovat další významné subjekty evropského i mezinárodního práva, které hrají významnou roli v dotčené oblasti, včetně projektů k ní se vztahujících.

V návaznosti na překážky, se kterými se OČTŘ potýkají při získávání elektronických důkazů, bych ráda představila nové a doufám, že efektivnější nástroje justiční spolupráce, jimiž jsou evropský předávací a uchovávací příkaz, a na nich následně názorně demonstrovala jejich přidanou hodnotu. V roce 2018 předložila Rada tzv. legislativní balíček pro elektronické důkazy, jehož součástí je Návrh nařízení Evropského parlamentu a Rady o evropských příkazech k vydání a k uchování elektronických důkazů v trestním řízení (dále jen Nařízení) a Návrh směrnice Evropského parlamentu a Rady stanovující harmonizovaná pravidla pro stanovení právních zástupců za účelem získávání důkazů v trestním řízení (dále jen Směrnice), který, bude-li přijat, usnadní OČTŘ získávání elektronických

[1] Convention on Cybercrime. In: Council of Europe [online], 2001, 23. 11. 2001 [cit. 2022-05-29], čl 36, odst 4. Dostupné z: https://rm.coe.int/1680081561

důkazů. Tyto nástroje budou zásadní především pří získávání důkazů nacházejících se u poskytovatelů služeb se sídlem v jiném státě. Abych demonstrovala rozdíly mezi stávající a očividně nedostatečnou právní úpravou a úpravou budoucí, pokusím se v praktické části práce analyzovat příklady využití nových nástrojů na reálných případech, v nichž je žádáno o právní pomoc.

Návrh Nařízení, přestože jeho případné přijetí nabízí převážně pozitiva v podobě usnadnění a urychlení získávání elektronických důkazů, současně přináší celkem obsáhlý seznam rizik. Ta vyplývají zejména z nevyjasněných postupů tohoto návrhu ohledně přeshraničního přístupu k elektronickým důkazům, stejně tak jako z jeho možných dopadů na teritorialitu a státní suverenitu a na základní práva a svobody poskytovatelů či uživatelů služeb. Rizika/úskalí návrhu Nařízení budou představena prostřednictvím jednotlivých studií a stanovisek nejen zúčastněných stran, organizací občanských sdružení, ale i výborů zabývajících se elektronickými důkazy v evropském právu. V neposlední řadě se pokusím vyhodnotit přínos nové úpravy do oblasti boje s počítačovou kriminalitou.

Ve své práci budu vycházet zejména z českých právních předpisů, stejně tak jako z mezinárodních úmluv a právních předpisů Evropské unie a z dostupné odborné literatury, elektronicky dostupných článků a pracovních dokumentů. Ve vztahu k přínosům a rizikům návrhu Nařízení jsem použila odborné studie vypracované jak Výborem Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní záležitosti (dále jen LIBE), tak právními odborníky zabývající se problematikou elektronických důkazů, potažmo návrhem nového Nařízení.

Vzhledem k tomu, že Rada a Parlament stále nedosáhli konsensu, či kompromisu ohledně jednotlivých článků návrhu Nařízení, je možné, že se jeho obsah bude ještě měnit. Není tak úplně jasné, kdy a v jaké podobě bude nařízení přijato. Přesto věřím, že tato práce pomůže čtenáři nahlédnout do problematiky elektronických důkazů a poskytne mu nejen teoretickou, ale i praktickou představu o tom, jak by mohlo nové nařízení fungovat v reálu.

1. Vymezení pojmu elektronické důkazy

Vzhledem k tomu, že význam elektronických důkazů je zásadní z pohledu v úvodu zmíněného návrhu nového Nařízení, bude tento pojem v následujících kapitolách blíže definován z hlediska právní úpravy, porovnání jeho definice v trestních řádech různých členských států EU, jazykové terminologie a v neposlední řadě bude vymezena důležitost pojmu v rámci nového Nařízení.

1.1. Definice elektronických důkazů

Chceme-li definovat elektronické důkazy, je třeba se na chvíli zastavit u definice důkazů obecně. Vyjdeme-li z české právní úpravy, která v podstatě reflektuje obecně přijímanou definici důkazů napříč právními systémy, definujeme důkaz jako *„vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání“* (§ 89 odst. 2 věta první trestního řádu České republiky[2]).

Pro potřeby naleznutí definice elektronických důkazů se podívejme ještě do dalších ustanovení, a to konkrétně do § 112 trestního řádu: (1) Věcnými důkazy jsou předměty, kterými nebo na kterých byl trestný čin spáchán, jiné předměty, které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu. (2) Listinnými důkazy jsou listiny, které svým obsahem prokazují nebo vyvracejí dokazovanou skutečnost vztahující se k trestnému činu nebo k obviněnému[3].

Český trestní řád neobsahuje definici elektronického důkazu jako takového, hovoří však o tzv. uchování dat uložených v počítačovém systému: § 7b odst. 1 trestního řádu: Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou

[2] Zákon č. 141/1961 Sb., trestní řád v posledním znění
[3] Více viz JELÍNEK, Jiří. Dokazování v trestním řízení v kontextu práva na spravedlivý proces. Praha: Leges, 2018. ISBN 978-807-5022-875.

v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat. Trestní právo procesní také nijak nerozlišuje mezi pojmy důkaz, důkazní prostředek a pramen důkazu.

Například doc. Polčák ve své knize o Elektronických důkazech uvádí, že *„za elektronický důkazní prostředek by se mělo považovat vše, co může sloužit jako zdroj relevantní informace a co je uchováno v elektronické podobě, především data. Data jako elektronické důkazní prostředky lze chápat jako nezpracovaná fakta a údaje bez přidané interpretace či analýzy. Samotné důkazy, tedy informace, jsou data, která byla interpretována tak, aby měla nějaký smysl pro jejich zpracovatele.“*[4] Jak je již uvedeno výše, pojem elektronické důkazy není v současném platném právu České republiky nikde definován, a proto doporučuje definovat elektronické důkazy spíše pomocí jejich specifických vlastností, kdy jedním z hlavních znaků, který je charakteristický pro data jako elektronické důkazní prostředky, je to, že jsou informace v nich uchovávány v podobě, která je bez dalších nástrojů pro běžného člověka obtížně smyslově vnímatelná.[5]

Podobně se o elektronických důkazech hovoří v učebnici Dokazování v trestním řízení od prof. Kalvodové, kde se uvádí, že… *„jako nejvhodnější se jeví definovat elektronické důkazní prostředky pomocí jejich specifických vlastností. Jedním z hlavních znaků, který je společný všem typům elektronických důkazních prostředků je to, že jsou informace v nich uchovávané v podobě, která je bez dalších nástrojů pro běžného člověka obtížně smyslově vnímatelná. Ze základního binárního zobrazení dat nedokáže člověk běžně získat žádnou relevantní informaci, a proto je za účelem jejich interpretace nutno využít nějakého elektronického zařízení, které je schopné tato data převést do podoby vnímatelné lidskými smysly. Nejobecněji lze v tomto smyslu elektronické důkazní prostředky*

[4] POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, 264 s. Beckova edice právo a hospodářství. s. 94. ISBN SBN978-80-210-8073-7.
[5] POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, 264 s. Beckova edice právo a hospodářství. s. 95. ISBN SBN978-80-210-8073-7.

definovat jako takové důkazní prostředky, k jejichž převodu do podoby srozumitelné pro člověka je třeba použít nějaké elektronické zařízení".[6]

Oba výše uvedení autoři tedy považují za důležitý atribut elektronických důkazů především jejich specifické vlastnosti, které právě elektronické důkazy jako takové definují a jsou tak pro zpracovatele snáze pochopitelné.

Pro srovnání mohu uvést několik definic elektronických důkazů přeložených ze zahraničních pracovních dokumentů dostupných převážně elektronicky.

Například v pracovním dokumentu Evropského parlamentu k předávacímu a uchovávacímu příkazu jsou elektronické důkazy definovány jako jakákoli data, která mohou sloužit jako důkaz bez ohledu na to, zda jsou uložena v elektronickém zařízení nebo jsou jím vytvářeny, zpracovávány či přenášeny. Zahrnují jak data obsahová (e-maily, textové zprávy nebo fotografie), tak data bezobsahová (údaje o účastnících a jejich provozní údaje, např. směrování nebo načasování zprávy).[7]

Dle důvodové zprávy Rady Evropy na téma „Elektronické důkazy v občanskoprávním a správním řízení", se elektronickým důkazem rozumí jakýkoli důkaz odvozený z údajů obsažených v nebo vytvořené jakýmkoli zařízením, jehož fungování závisí na softwaru, programu nebo na datech uložených v počítačovém systému nebo síti nebo přenášených prostřednictvím počítačového systému nebo sítě.[8] Uvedené informace je možné shrnout tak, že za elektronický důkaz lze považovat jakákoliv data uchovávaná v počítači (či v/na jakémkoliv jiném elektronickém či virtuálním úložišti dat, např. flash discu, tzv. claudu atp.), která svým obsahem prokazují nebo vyvracejí

---

[6] KALVODOVÁ, Věra a Milana HRUŠÁKOVÁ. Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty. Brno: Masarykova univerzita, 2015., s. 312. ISBN 978-80-210-8072-0.

[7] BĄKOWSKI, Piotr a Sofija VORONOVA. Electronic evidence in criminal matters. EU Legislation in Progress [online]. 2021, 1. 3. 2021, 12 [cit. 2022-08-30]., s. 2. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf

[8] *ELECTRONIC EVIDENCE IN CIVIL AND ADMINISTRATIVE PROCEEDINGS: Guidelines and explanatory memorandum [online]. F-67075 STRASBOURG Cedex: Council of Europe Publishing, 2019 [cit. 2022-08-30].* s. 6. *ISBN ISBN 978-92-871-8929-5. Dostupné z: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5*

dokazovanou skutečnost vztahující se k trestnému činu nebo k obviněnému, tj. mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele.

Ze všeho shora uvedeného vyplývá, že elektronickými důkazy jsou digitální údaje, zásadní pro vyšetřování a stíhání trestných činů. Jsou to takové informace, které jsou získány zákonem požadovaným způsobem, a proto mohou být použity v řízení před soudem, jako důkaz kriminálního jednání.

Otázka elektronických důkazů se netýká pouze trestněprávního postihu počítačové kriminality. Proto by bylo vhodné si hned v úvodu také ujasnit, že elektronické důkazy se nevztahují pouze k prokazování počítačové kriminality ve smyslu obsahu tohoto pojmu tak, jak byl vysvětlen výše. Elektronickými důkazy může být prokazována jakákoliv trestná činnost, o níž mají tyto v důkazním slova smyslu vypovídat. Bude-li například plánována vražda prostřednictvím emailu a obsah dotčené e-mailové komunikace se podaří OČTŘ zajistit, bude elektronický důkaz sloužit k usvědčení pachatele násilné trestné činnosti. Nicméně zatímco v případě jiných druhů trestné činnosti hrají elektronické důkazy spíše vedlejší roli, u kriminality počítačové jsou v roli hlavní – a to právě pro její shora popsaný charakter. Mezi trestné činy, ve kterých elektronické důkazy (především rychlost jejich obstarání) hrají významnou roli, patří především terorismus a sexuální zneužívání dětí po internetu.

V dalších částech této práce je tak s termínem „elektronický důkaz“ pracováno ve smyslu „uchovaných digitálních dat“ (konkrétně viz níže), která se OČTŘ snaží získat pro naplnění jeho účelu, přičemž užití termínu „důkazy“ na místo „údaje“ či „data“ zároveň odkazuje na jeho použitelnost v trestním řízení.[9]

Konkrétně jimi mohou být např. emaily, zprávy na sociálních sítích, IP adresy, informace o majiteli e-mailové adresy, fotografie, uživatelská jména,

[9] § 1 odst. 1 trestního řádu: Účelem trestního řádu je upravit postup orgánů činných v trestním řízení tak, aby trestné činy byly náležitě zjištěny a jejich pachatelé podle zákona spravedlivě potrestáni.

časové údaje a obsah zpráv zasílaných prostřednictvím služby Facebook Messenger a údaje z různých aplikací nebo dokumenty uložené v Cloudu[10].

Vzhledem k tomu, že cílem této práce je zejména rozbor návrhu nového nařízení upravujícího získávání důkazů členských států Evropské unie i mimo ni, je nutné zdůraznit důležitý aspekt bezprostředně související s elektronickými důkazy, a to přeshraniční přístup k nim. Přístup k zahraničním důkazům je důležitý, hlavně z toho důvodu, že jsou tyto uchovávány poskytovateli služeb, jejichž většina má sídla v zahraničí. OČTŘ se na poskytovatele služeb často obrací právě s žádostí o získání těchto údajů. Na současném trhu dominují velké společnosti jako je Google, vlastnící YouTube; Meta vlastnící také Instagram a WhatsApp; Microsoft vlastnící Skype, Amazon a Apple. A protože servery mohou být uloženy v datových centrech, která se mohou nacházet v jiné zemi, data těchto společností mohou být spravována dceřinými společnostmi se sídlem v Evropě, stává se tím získávání důkazů ještě komplikovanější. V dalších kapitolách bude postup vyřizování žádostí o poskytnutí elektronických důkazů uveden.

[10] Termín, který se používá pro popis globální sítě serverů, z nichž každý má svoji funkci. Cloud není fyzický objekt, ale rozsáhlá síť vzájemně propojených vzdálených serverů po celém světě, které fungují jako jeden ekosystém. Tyto servery jsou navržené buď k ukládání a správě dat, spouštění aplikací, nebo doručování obsahu a služeb, jako je streamování videí, webová pošta, kancelářský software nebo sociální média. Místo přistupování k souborům a aplikacím z místního nebo osobního počítače k nim přistupujete online z jakéhokoli zařízení s podporou internetu – informace tak budou dostupné kdekoli a kdykoli ječlověk potřebuje.
Co je cloud?. Azure [online]. [cit. 2022-08-30]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-the-cloud/

1.2. Porovnání definice elektronických důkazů u vybraných členských států EU

Nástroj Evropské soudí sítě[11] (dále jen ESS) „Fiches Belges[12]“ definuje elektronické důkazy v trestním řízení jako jakákoli data nebo informace, které jsou generovány, uchovávány nebo přenášeny v digitální podobě prostřednictvím elektronických zařízení, která jsou relevantní pro vyšetřování a stíhání trestných činů.[13] ESS, jejímž hlavním účelem je zlepšení justiční spolupráce mezi členskými státy EU na právní a praktické úrovni s cílem bojovat proti závažné trestné činnosti, zejména organizovanému zločinu, korupci, obchodu s drogami a terorismu, se logicky zabývá problematikou elektronických důkazů. Proto v rámci zmíněného nástroje „Fiches Belges“ vytvořila samostatnou složku obsahující informace o jednotlivých vnitrostátních právních úpravách členských států EU poskytnutých jednotlivými kontaktními body v souvislosti s elektronickými důkazy. Zde je právě možné porovnat právní úpravu v jednotlivých státech.

Jak je uvedeno v předchozí kapitole, český trestní řád neobsahuje definici elektronického důkazu jako takového. Podobně jsou na tom i další státy EU, například Rakousko, Belgie, Bulharsko, Dánsko, Estonsko, Finsko a další, které, stejně jako Česká republika odkazují na jiná ustanovení svého trestního řádu v souvislosti s institutem uchovávání dat.

Naopak Lotyšsko má ve svém trestním právu (§ 136 lotyšského trestního řádu) jasnou definici elektronických důkazů, kdy elektronickým důkazem se rozumí „informace o skutečnostech v podobě elektronických informací, které byly

---

[11] ESS je síť kontaktních míst pro usnadnění spolupráce a pro zřízení přímých kontaktů mezi justičními orgány v členských státech EU. Internetové stránky ESS nabízejí vhodné elektronické nástroje vyžadované pro fungování sítě a pro usnadnění spolupráce. Více viz https://www.ejn-crimjust.europa.eu/ejn/EJN_DynamicPage/CS/2

[12] Fiches Belges je nástrojem, který poskytuje praktické informace o konkrétních souborech opatření, na něž se vztahuje justiční spolupráce v trestních věcech. Pomáhá ověřit, zda je v určité zemi dané opatření použitelné, v jakém jazyce se musí žádost o spolupráci vypracovat, získat všeobecný přehled o tom, jaké informace se musí v žádosti uvést, porovnat opatření dvou zemí. Tato opatření jsou rozdělena do deseti skupin. Více viz Portál evropské e-justice. *Fiches Belges* [online]. [cit. 2022-08-30]. Dostupné z : https://e-justice.europa.eu/528/CS/fiches_belges?init=true

[13] Fiches Belges on electronic evidence. *European Judicial Network* [online]. [cit. 2022-08-30]. Dostupné z : https://www.ejn-crimjust.europa.eu/ejnupload/Evidence/FB_Eevidence_SP.pdf

zpracovány, uloženy nebo odvysílány pomocí zařízení nebo systémů pro automatizované zpracování dat“.

Neméně zajímavé je pojetí maďarského trestního práva procesního, které rozlišuje mezi dvěma pojmy, a to elektronická data a elektronické důkazy, a proto zavedlo do svého trestního řádu (§ 205 odst. 1) pouze definici elektronických dat, kterými se rozumí „jakékoli zobrazení skutečností, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programů vhodných k tomu, aby počítačový systém plnil určitou funkci. (Tato definice odpovídá pojmu "počítačová data" definovanému v čl. 1 písm. b) Úmluvy o počítačové kriminalitě). Elektronickým důkazem jsou pak samotné informace, které lze v důsledku procesu vyhodnocení vyvodit z dat. Jinými slovy, údaje jsou důkazním prostředkem, který nese informace považované za důkaz. Elektronické důkazy v podstatě pocházejí z elektronických dat automaticky uložených, zpracovaných nebo přenesených v informačním systému.[14] Z výše uvedeného porovnání je evidentní, že problematika elektronických důkazů je stále čerstvá a různorodá právní úprava vypovídá o tom, že legislativa členských států ještě není plně připravena ji jednomyslně uchopit. Možná právě nové Nařízení pomůže v budoucnu sjednotit roztříštěnost jednotlivých trestních řádů.

1.3. Vymezení pojmu elektronický důkaz dle návrhu Nařízení

Evropská Komise při tvorbě dokumentů týkajících se elektronický důkazů a Nařízení převážně používá anglický a francouzský jazyk, tak jak je v této instituci zvykem. Dokumenty jsou následně neoficiálně překládány do dalších jazyků, aby s nimi mohlo být nadále pracováno. V případě České republiky neoficiální překlad poskytují členové pracovní skupiny pro spolupráci v trestních věcech (COPEN), kteří se jednotlivých jednání a diskusí účastní a následně předávají aktuální informace kolegům z mezinárodního odboru Ministerstva spravedlnosti. Do doby, než bude návrh nového Nařízení přijat a jeho obsah přeložen tak, že dané bude

[14] Porovnání jednotlivých trestních řádů členských států EU v souvislosti s definicí elektronických důkazů Více viz *European Judicial Network: Fiche Belge on electronic evidence* [online]. [cit. 2022-08-30]. Dostupné z: https://www.ejnforum.eu/cp/e-evidence-fiche/223/0

oficiálně akceptováno, může samozřejmě docházet k odlišnostem v interpretaci jak v terminologii, tak případně v chápání jednotlivých výrazů a termínů.

Z obsahu předchozích kapitol, je zřejmé, že za elektronické důkazy se v návrhu nového Nařízení považují e-maily, zprávy v aplikacích (facebook messenger, whatsapp, telegraph…) IP adresy, fotografie, uživatelská jména atd. Používaným českým termínem jsou „elektronické důkazy“. Francouzským termínem používaným v dokumentu o návrhu nového Nařízení je „preuves électroniques“, kdy „preuves“ v českém překladu znamená důkaz. Oproti tomu, důkaz v anglickém jazyce se překládá jako „proof“ (podobné francouzskému překladu), ale i „evidence“. Ovšem používaným termínem je „electronic evidence“.

Důvodem použití slova „evidence“ je v anglickém jazyce jeho odlišné chápání od slova „proof“. I přesto, že oxfordský výkladový slovník označuje obě slova jako synonyma[15], právnický výkladový slovník tuto odlišnost popisuje následovně: „Evidence“ se vztahuje k určitým skutečnostem nebo údajům, které umožňují prokázat existenci určitých skutečností, zatímco „proof“ je souhrnem těchto důkazů.[16] Zjednodušeně lze konstatovat, že z pohledu české terminologie termín “proof” obvykle označuje výsledek procesu dokazování, zatímco evidence jednotlivé důkazní prostředky (důkazy). Napovídá tomu i skutečnost, že z oficiálních dokumentů můžeme vypozorovat, že v psané podobě se ustálil výraz (zkratka) e-evidence, a to pravděpodobně nejen z důvodu úspory času při zápisu během jednotlivých jednání, ale i pro další využití při komunikaci mezi OČTŘ a stává se tak oficiálním termínem. Mám za to, že do budoucna se tento výraz promítne i do česky psaných právních norem.

---

[15] *Oxford Learner´s Dictionaries* [online]. [cit. 2022-08-30]. Dostupné z: https://www.oxfordlearnersdictionaries.com/definition/american_english/proof_1

[16] What Is the Difference Between Proof and Evidence? *Law Corner* [online]. [cit. 2022-08-30]. Dostupné z: https://lawcorner.in/what-is-the-difference-between-proof-and-evidence/#_ftn1

1.4. Druhy elektronických údajů

Tato část kapitoly se zaměřuje především na popsání způsobu, jak po technické stránce dochází k zachování a shromažďování informací, potažmo důkazů. Považuji za nezbytné se touto problematikou zabývat, neboť bez znalosti praktických aspektů nelze vytvořit adekvátní a přiléhavou právní úpravu a tuto správně posoudit z hlediska kompatibility a efektivity.

Ustanovení čl. 2 odst. 7–10 návrhu Nařízení definuje mimo jiné, konkrétní typy/druhy údajů, které OČTŘ zpravidla vyžadují a které budou moci díky EPP získat. Jsou jimi **bezobsahové údaje,** mezi které řadíme a) údaje o účastnících, b) přístupové údaje, c) transakční údaje a **údaje o obsahu,** kam patří jakákoli data uložená v digitálním formátu.

Níže uvádím pro přehled tabulku s výše uvedenými typy údajů včetně jejich definic a přístupových pravidel, která stanovují, kdo a jakým způsobem může o tato data žádat.

Druhy údajů	Definice	Přístupová pravidla
Údaje o účastnících	Údaje, které slouží k identifikaci odběratele nebo zákazníka, jako je jméno, datum narození, poštovní adresa, fakturační a platební údaje, telefonní číslo nebo e-mailová adresa.	**Státní zástupce/soudce** v zemi A může přímo požádat poskytovatele služeb nebo jeho právního zástupce v zemi B o poskytnutí elektronických důkazů. Pokud žádost přichází od policie, musí požádat státního zástupce nebo soudce v zemi A o schválení příkazu před jeho předáním poskytovateli služeb nebo jeho právnímu zástupci.
Přístupové údaje	Údaje týkající se zahájení a ukončení přístupové relace uživatele ke službě, které samy o sobě nemohou identifikovat uživatele, ale jsou nezbytně nutné jako první krok k identifikaci. Patří sem údaje o přístupu uživatele ke službě, jako je datum a čas použití nebo přihlášení a odhlášení ke službě nebo IP adresa přidělená poskytovatelem služby.	**Státní zástupce/soudce** v zemi A může přímo požádat poskytovatele služeb nebo jeho právního zástupce v zemi B o poskytnutí elektronických důkazů. Pokud žádost přichází od policie, musí požádat státního zástupce nebo soudce v zemi A o schválení příkazu před jeho předáním poskytovateli služeb nebo jeho právnímu zástupci.
Transakční/provozní údaje	Týká se poskytování služby, například zdroje a cíle zprávy, údajů o poloze zařízení, data, času, trvání, velikosti, trasy, formátu, použitého protokolu a typu komprese.	**Soudce** v zemi A může přímo požádat poskytovatele služeb nebo jeho právního zástupce v zemi B o poskytnutí elektronických důkazů. Pokud žádost přichází od policie nebo státního zástupce, musí požádat soudce v zemi A o schválení příkazu před jeho předáním poskytovateli služeb nebo jeho právnímu zástupci.
Obsahové údaje	Jakákoli data uložená v digitálním formátu, jako je text, hlas, videa, obrázky a zvuk, kromě údajů o účastnících, přístupu nebo transakcích.	**Soudce** v zemi A může přímo požádat poskytovatele služeb nebo jeho právního zástupce v zemi B o poskytnutí elektronických důkazů. Pokud žádost přichází od policie nebo státního zástupce, musí požádat soudce v zemi A o schválení příkazu před jeho předáním poskytovateli služeb nebo jeho právnímu zástupci.

Tabulka 1- Druhy elektronických důkazů[17]

[17] Frequently Asked Questions: New EU rules to obtain electronic evidence. *European Commission* [online]. Brussels, 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

Toto rozdělení, **kromě přístupových údajů**, existuje v právních řádech mnoha členských států a též v právních rámcích zemí mimo EU. Autoři návrhu rozlišují mezi kategoriemi údajů následovně: Údaje, které se týkají výhradně identifikace uživatele, jsou považovány za méně invazivní, a proto mohou být snadněji dostupné, zatímco údaje spočívající především v činnostech dané osoby, by měly být chráněny přísněji.

Pro **transakční a údaje o obsahu** je stanovena prahová hodnota, jelikož o ně lze požádat pouze v případě trestných činů, za které lze ve vydávajícím státě uložit trest s horní hranicí sazby v délce nejméně tři roky, nebo v případě určitých trestných činů souvisejících s kybernetickou činností nebo s terorismem.[18]

Transakční data jsou komplikovanější a potřebují vysvětlit více podrobně. Patří mezi ně:

- metadata[19], která se vztahují k poskytování služeb a zahrnují údaje týkající se připojení, provozu nebo místa komunikace (například IP nebo MAC adresy);
- záznamy o přístupu, které zaznamenávají čas a datum připojení uživatele ke službě a IP adresu, ze které se k službě připojovalo;
- záznamy o transakcích identifikující produkty nebo služby, které uživatel získal od poskytovatele nebo třetí strany (např. nákup úložného prostoru v cloudu)[20].

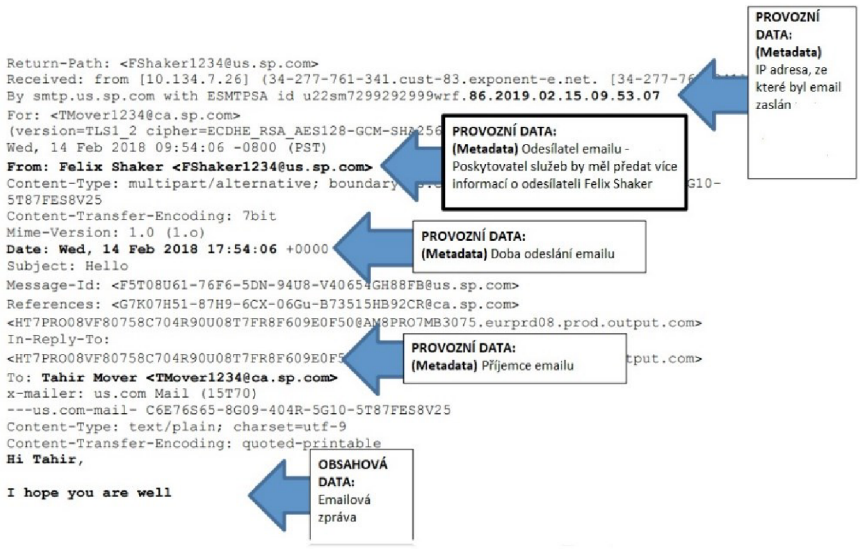
Transakční a údaje o účastnících jsou tzv. uložené elektronické údaje (jméno uživatele, doba, po kterou účastník používá danou službu a adresa internetového protokolu – IP adresa – od doby prvního přihlášení). Pro představu uvádím formát nezpracované zprávy e-mailu znázorňující tyto uložené elektronické důkazy.

---

[18] Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji. *Evropská rada a Rada Evropské unie : Tisková zpráva* [online]. 7.12.2018 [cit. 2022-08-30]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

[19] Jedná se o data, která mají informační hodnotu o webové stránce, ale nejsou na první pohled vidět. Tato data se nacházejí v kódu HTML webové stránky, většinou mezi tagy <head> a </head> a slouží především jako informace pro roboty vyhledávačů. Mezi metadata patří například popis stránky nebo seznam klíčových slov. Co jsou metadata: Slovníček webových pojmů. *Mioweb* [online]. [cit. 2022-08-30]. Dostupné z: https://www.mioweb.cz/slovnicek/metadata/

[20] *COMMISSION STAFF WORKING DOCUMENT: IMPACT ASSESSMENT*. In. Brussels, 2018. s 43. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN



Obrázek 1 – Formát nezpracovaného emailu (uložené el. důkazy)[21]

Všechny výše uvedené kategorie dat obsahují osobní údaje a vztahují se na ně záruky dle acquis EU[22] o ochraně osobních údajů. Intenzita dopadu na základní práva je různá, a to zejména mezi údaji o účastníkovi na jedné straně a údaji o transakcích a obsahu na straně druhé. Nástroj by měl obsáhnout všechny kategorie: údaje o účastníkovi a přístupu jsou často výchozím bodem pro získání vodítek k totožnosti podezřelé osoby při vyšetřování. Údaje o transakcích a obsahu mohou být zase nejrelevantnější jako důkazní materiál. Z důvodu různé míry zásahu do základních práv je důvodné spojit různé podmínky s údaji o účastníkovi na jedné straně a s údaji o transakcích a obsahu na straně druhé, jak je provedeno v několika ustanoveních nařízení.[23]

Jednou z dalších možností získávání elektronických důkazů je jejich opatřování v reálném čase, ale na tento způsob se návrh nového Nařízení nevztahuje, proto se v těchto případech využije žádost o právní pomoc. Opatřením

[21] EUROMED DIGITAL EVIDENCE MANUAL: Practical Guide for Requesting Electronic Evidence from Service Providers [online]. s. 15. 2018 [cit. 2022-08-30]. Dostupné z: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/manual-on-digital-evidence%204-4-19.pdf

[22] *Obecné nařízení o ochraně osobních údajů: Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů*, 2016. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN Nařízení vstoupilo v platnost 24. května 2016 a uplatňuje se od 25. května 2018.

[23] Čl.2 návrhu Nařízení, odst. 7

se rozumí za **a)** získávání informací z **provozních údajů** o tom, s kým a odkud podezřelý subjekt komunikuje za účelem zjištění statické a dynamické IP adresy a za **b)** získávání **obsahových údajů**, resp obsahu nebo textu e-mailu, zprávy, blogu nebo příspěvku, videí, obrázků, zvuků uložených v digitálním formátu.

Pro představu uvádím teoretický příklad, který se může vyskytnout v praxi:

Ze zpravodajských informací je zjištěno, že e-mailové účty amerického poskytovatele služeb byly použity pro komunikaci v rámci teroristické sítě. K identifikaci uživatelů e-mailových účtů potřebuje policie provozní údaje ke zjištění místa, odkud byly e-maily odesílány. Do USA byla odeslána žádost o právní pomoc s požadavkem na zjištění místa odeslání emailů a opatření IP adresy v reálném čase. Na základě této žádosti bylo zjištěno, že IP adresy patřily kybernetickým kavárnám, kde následně policie v dožadujícím státě zahájila sledování. Po obdržení dat IP adres v reálném čase byla policie schopna identifikovat a následně zatknout odesílatele emailových zpráv.[24]

2. Formy získávání elektronických důkazů prostřednictvím aktuálních nástrojů justiční spolupráce v a mimo EU de lege lata

Jak bylo vysvětleno výše, jedním z úskalí odhalování a vyšetřování počítačové kriminality je potřeba OČTŘ získat elektronické důkazy fakticky existující na území cizího (dožádaného) státu, tj. odlišného od státu, v němž probíhá dotčené trestní řízení, v kterém se vyskytla potřeba obstarání takových důkazů (dožadující stát). Pro přesnost je vhodné zmínit, že sousloví „na území cizího státu“ je míněno z právního hlediska, neboť z toho faktického takové důkazy vlastně existují ve virtuálním prostoru, na území toho kterého státu se nachází „správce“ tohoto prostoru, či „poskytovatel“ dotčené využívané IT služby, cloudu apod. (opět zjednodušeně).

---

[24] *EUROMED DIGITAL EVIDENCE MANUAL: Practical Guide for Requesting Electronic Evidence from Service Providers* [online]. 2018 [cit. 2022-08-30]. s. 16. Dostupné z: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/manual-on-digital-evidence%204-4-19.pdf

Jediným způsobem, jak lze důkazy z jiného státu získat ve formě použitelné pro trestní řízení, je využití existujících způsobů právní pomoci, tj. institutů mezinárodní policejní či justiční spolupráce[25]. V tomto směru je třeba hned úvodem zdůraznit, že formální postup pro získání elektronických důkazů ze zahraničí se neliší od získání jiných druhů důkazů, vždy je třeba zvolit odpovídající formu/institut mezinárodní policejní/justiční spolupráce, kterou/který je možné (a zároveň nutné) použít pro komunikaci mezi konkrétními zúčastněnými státy. Využití toho kterého institutu je předurčeno existující právní (smluvní) úpravou, kterou se řídí vztahy mezi zainteresovanými státy v oblasti mezinárodní spolupráce v dotčené právní oblasti, z hlediska zaměření této práce, v tomto případě v oblasti trestněprávní. Zde považuji za vhodné shrnout základní rozlišení takových institutů podle kritéria, zda o mezinárodní právní pomoc v trestním řízení žádají státy EU či třetí státy, se zaměřením především na státy EU.

Základním prostředkem, nebo spíše stavebním kamenem právní úpravy, jsou mezinárodní úmluvy upravující danou právní oblast[26], na jejichž základě je žádáno o právní pomoc v případě, že mezi dotčenými státy neexistuje užší (většinou efektivnější) forma spolupráce. Užší formu spolupráce představují například právní předpisy EU, které nejsou použitelné pro všechny členské státy, jsou aplikovány v závislosti na tom, zda se tzv. posílené spolupráce dotčený stát účastní. Aktuálně nejvyšším stupněm mezinárodní justiční spolupráce v trestní oblasti pak představuje fungování Úřadu evropského veřejného žalobce.

Pro úplnost považuji za vhodné zmínit, že neexistuje-li dohoda/úmluva, vychází státy obvykle z tzv. zásady vzájemnosti.[27] Z užších forem spolupráce bych se chtěla podrobněji věnovat Evropskému vyšetřovacímu příkazu (dále jen

[25] Rozdíl mezi justiční a policejní spoluprací: policejní spoluprací se získávají informace (tj. údaje o tom, že někde mohou existovat důkazy), justiční spoluprací použitelné důkazy tomu odpovídajícím procesním způsobem.
[26] Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské Unie ze dne 29. května 2000.
[27] Při provádění mezinárodní justiční spolupráce v trestních věcech se uplatňují určité obecné zásady. Především jde o zásadu reciprocity, tedy vzájemnosti. Tato zásada znamená, že dožádaný stát poskytne spolupráci v takovém rozsahu, v jakém by ji dožádanému státu poskytl stát dožadující.

EVP)[28], a samozřejmě nemohu nezmínit také Evropský zajišťovací příkaz[29]. Oba zmíněné nástroje mezinárodní justiční spolupráce mají za cíl usnadnit vyžadování důkazů či zajišťování majetkových hodnot důležitých pro trestní řízení v dožadujícím státě, s využitím principu vzájemného uznávání rozhodnutí, tj. uznání dotčeného rozhodnutí vydaného ve státě dožadujícím. Dožádaný stát tak (zjednodušeně) nepřezkoumává, potažmo ani nesmí přezkoumávat, konkrétní důkazy, které dožadující stát opravňují k vydání toho kterého příkazu. Přezkoumává spíše splnění formálních náležitostí pro využití toho kterého procesního institutu, případně přezkoumává ne/existenci vnitrostátních překážek pro uznání vydaného rozhodnutí. Jde o vyšší míru vzájemné důvěry mezi zúčastněnými státy EU, postavené na důvodném předpokladu, že se v případě všech těchto států jedná o tzv. právní státy, tj. státy, v nichž jsou plně respektována základní lidská práva a svobody a tomu odpovídají právní mechanismy jednotlivých zemí

Samostatnou kapitolu v obstarávání důkazů z cizích států aktuálně představuje spolupráce uvnitř nově vzniklého Úřadu Evropského veřejného žalobce[30] (dále jen EPPO), umožňující účastným státům ještě přímější formu získávání takových důkazu (viz níže).
K tomu je nicméně třeba zdůraznit, že tato spolupráce se vztahuje pouze na vyšetřování trestných činů, spadajících do pravomoci tohoto úřadu.

---

[28] Dne 3. dubna 2014 přijala Rada Směrnici Evropského parlamentu a Rady 2014/41/EU o evropském vyšetřovacím příkazu v trestních věcech, čl. 6: V důsledku potřeby nového přístupu založeného na zásadě vzájemného uznávání, který však rovněž zohlední pružnost tradičního systému vzájemné právní pomoci, byl vytvořen komplexní systém, který nahradil všechny stávající nástroje v této oblasti včetně rámcového rozhodnutí 2008/978/SVV. Vztahuje se na všechny druhy důkazů, obsahuje lhůty pro vykonání a omezuje důvody pro odmítnutí. Více viz: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32014L0041

[29] Dne 22. července 2003 přijala Rada Rámcové rozhodnutí 2003/577/SVV o výkonu příkazů k zajištění majetku nebo důkazních prostředků v Evropské unii. Cílem tohoto rámcového rozhodnutí je „stanovení pravidel, podle nichž členský stát uznává a vykonává na svém území příkaz k zajištění vydaný justičním orgánem jiného členského státu v rámci trestního řízení.“ Více viz rámcové rozhodnutí Rady 2003/577/SVV článek 1. Dostupné na https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32003F0577

[30] Nařízení Rady (EU) 2017/1939 ze dne 12. října 2017, kterým se provádí posílená spolupráce za účelem zřízení Úřadu evropského veřejného žalobce. Více viz https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32017R1939

EPPO vzniklo Nařízením o EPPO, které je přímo aplikovatelné uvnitř státu na EPPO účastných, bez nutnosti implementace do právního řádu členského státu formou zákona.

Hlavním účelem vzniku EPPO, který začal fakticky fungovat od 1. 6. 2021, bylo vytvoření evropského právního prostoru pro ochranu finančních zájmů EU[31].

Pod pravomoc EPPO spadá vyšetřování trestných činů poškozujících finanční zájmy EU, tj. namířené proti všem výdajovým i příjmovým stránkám rozpočtu EU v tom nejširším slova smyslu, stejně tak jako trestné činy s těmito související v podobě korupce či legalizace výnosů z trestně činnosti a dále trestné činy s těmito tzv. neoddělitelně spjaté. Mimo to spadá pod pravomoc EPPO vyšetřování trestných činů v souvislosti s neodvedením či krácením DPH, pokud škoda přesahuje 10 milionů EUR a jednání se týká dvou nebo více zúčastněných států. Doposud mohly tyto trestné činy vyšetřovat a stíhat pouze vnitrostátní orgány, ale jejich pravomoci končily na hranicích jejich země.

Úřad působí na dvou úrovních. Centralizované, kterou představují tzv. evropští žalobci (EP, jeden za každý účastný stát), sídlící v Lucemburku a dohlížející na práci tzv. evropských pověřených žalobců (EDP), a decentralizované, kterou představují právě tito EDP působící v jednotlivých zúčastněných státech. Ti jsou zde v postavení státních zástupců, tj. vykonávají dozor nad vyšetřováním trestných činů spadajících pod kompetence Úřadu, jejichž spáchání zde také posléze žalují u vnitrostátních soudů. Na rozdíl od svých klasických dozorových státních zástupců jsou tito se svým případem „spojeni“ až do jeho pravomocného ukončení, tzn., zastupují věc i u odvolacího soudu.

Průlomový nástroj „mezinárodním justiční spolupráce“ pak představuje právě možnost EDP z jednoho státu požádat přímo EDP ze státu jiného o provedení toho úkonu, který je nezbytný provést na území tohoto jiného státu. Jedná se o tzv. přeshraniční vyšetřování upravené v ČL. 31 Nařízení.[32]

---

[31] Mezi finanční zájmy EU patří veškeré příjmy, výdaje a aktiva hrazené z rozpočtu EU, pořízené z něj nebo do něj náležející, jakož i rozpočty orgánů, institucí a jiných subjektů zřízených smlouvami a rozpočty jimi spravované a sledované.

[32] European Public Prosecutor’s Office: Mission and tasks. *European Union* [online]. [cit. 2022-08-30]. Dostupné z: https://www.eppo.europa.eu/en/mission-and-tasks

Jde o zcela novou formu spolupráce v trestní oblasti, kdy se státy historicky poprvé vzdávají části své jurisdikce za účelem ochrany finančních zájmů EU. Do tohoto projektu jsou vkládány velké naděje, a to především proto, že došlo touto úpravou k posílení nestrannosti a nezávislosti státního zástupce v podobě evropského pověřeného žalobce.

V případech, které nespadají do kompetence EPPO, státy v instituci EPPO účastné postupují standardními způsoby mezinárodní justiční spolupráce.

2.1. Vzájemná právní pomoc

Z pohledu zaměření práce, tj. z pohledu získávání elektronických důkazů, stanoví hlavní právní rámec pro formu takové pomoci Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy EU ze dne 29. května 2000[33] a její protokol ze dne 16. října 2001. Primárním cílem úmluvy je zlepšení justiční spolupráce prostřednictvím rozvoje a modernizace stávajících ustanovení dotýkajících se vzájemné pomoci. Tato úmluva doplňuje následující akty a usnadňuje jejich uplatňování v zemích EU:

1) Evropskou úmluvu o vzájemné pomoci ve věcech trestních přijatou Radou Evropy dne 20. dubna 1959 a její dodatkový protokol ze dne 17. března 1978. Tato je zásadní v boji proti přeshraniční trestné činnosti. Stanoví pravidla pro výkon soudních dožádání orgány jedné strany (''dožádaná strana''), jejichž cílem je zajistit důkazy (výslech svědků, znalců a stíhaných osob, doručení soudních příkazů a záznamů o soudních rozsudcích) nebo sdělit důkazy (záznamy nebo dokumenty) v trestním řízení vedeném justičními orgány strany druhé (''dožadující strana''). Úmluva rovněž stanoví požadavky, které musí žádosti o vzájemnou pomoc splňovat (předávající orgány, jazyky, odmítnutí vzájemné pomoci).[34]

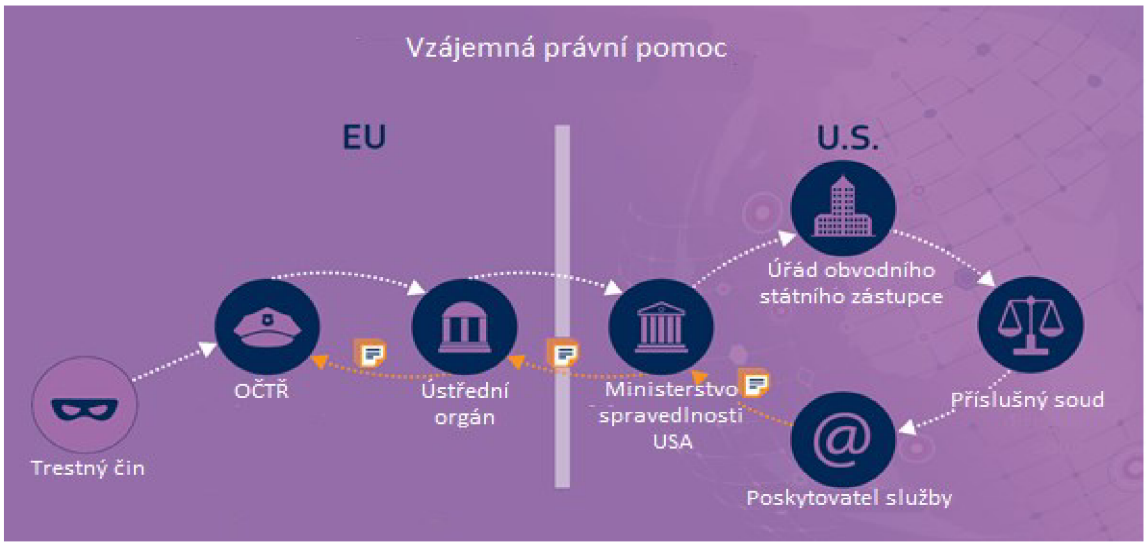
[33] Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské Unie ze dne 29. května 2000.
[34] Mutual legal assistance and extradition: Combating crime across borders. *European Commission* [online]. [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en

2) ustanovení úmluvy ze dne 19. června 1990 k provedení Schengenské dohody týkající se vzájemné pomoci v trestních věcech.

Podle Úmluvy se dožadující orgán může obrátit na vydávající (tj. jinými slovy dožádaný) orgán přímo. S výjimkou případů, kdy se vykonávající orgán dovolává důvodů pro odmítnutí, se žádost vyřídí co nejdříve a pokud možno ve lhůtě stanovené dožadujícím orgánem. Až do 22. května 2017 byla úmluva hlavním nástrojem pro získávání důkazů v EU. Od uvedeného data nahradila příslušná ustanovení úmluvy a protokolu směrnice o evropském vyšetřovacím příkazu použitelná v členských státech EU, které jsou jí vázány. Úmluva a protokol však mají stále zvláštní význam jak pro uvedené země, jelikož některá ustanovení (např. o společných vyšetřovacích týmech) nebyla směrnicí nahrazena, tak pro členské státy EU, které nejsou směrnicí vázány.[35]

Vzájemná právní pomoc je forma spolupráce mezi různými zeměmi za účelem shromažďování a výměny informací. Orgány jedné země mohou rovněž požádat o důkazy nacházející se v jedné zemi a poskytnout je na pomoc při vyšetřování trestných činů nebo trestním řízení v zemi druhé. Mechanismy vzájemné právní pomoci jsou postupně nahrazovány nástroji vzájemného uznávání. V rámci mezinárodní spolupráce uzavřela EU dohody o vzájemné právní pomoci se Spojenými státy americkými, jakož i s Japonskem, Islandem a Norskem a Velkou Británií. Níže uvádím názorný příklad vyžádání elektronických důkazů ze země EU od poskytovatele služeb v US prostřednictvím vzájemné právní pomoci (angl. Mutual Legal Assistance – MLA), kdy průměrná doba vyřízení je 10 měsíců.

[35] Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy. *Portál evropské e-Justice* [online]. [cit. 2022-08-30]. Dostupné z: https://e-justice.europa.eu/92/CS/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams



Obrázek 2 - vyžádání el. důkazů ze země EU od poskytovatele služeb v US [36]

Je třeba si uvědomit, že mezinárodní úmluvy tvoří nutný právní rámec pro vzájemnou spolupráci, jejíž konkrétní podoba je nicméně zakotvena v zákonech toho kterého státu. V ČR představuje základní právní předpis upravující mezinárodní justiční spolupráci Zákon č. č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních (dále jen ZMJS), který podrobně upravuje jednotlivé způsoby mezinárodní justiční spolupráce včetně způsobu zvláštních, tj. např. EVP.

Obdobně je třeba připomenout z pohledu práva EU rozdíl mezi Směrnicí EU a Nařízením EU. Směrnici je třeba implementovat – tj. opět převést do podoby konkrétních zákonných ustanovení, nařízení nikoliv – je přímo použitelné. Ve všech případech se však státy účastny na té které úmluvě zavazují, že budou podnikat kroky nutné k tomu, aby byla ustanovení úmluvy uváděna v život v tomu odpovídající podobě uvnitř právního řádu toho kterého státu.

[36] Frequently Asked Questions: New EU rules to obtain electronic evidence. *European Commission* [online]. Brussels, 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

Společné vyšetřovací týmy

Společný vyšetřovací tým (dále jen SVT) je v současné době jedním z nejmodernějších nástrojů mezinárodní spolupráce v trestních věcech. Podmínky, za kterých jsou SVT zřizovány, jsou ustanoveny v článku 13 výše uvedené Úmluvy 2000. Vzhledem k pomalému průběhu její ratifikace přijala Rada 13. července 2002 rámcové Rozhodnutí o společných vyšetřovacích týmech, které měly členské státy provést do ledna 2003. Rámcové Rozhodnutí stejnoměrně poskytuje základy pro zřízení těchto SVT.[37] Úmluva 2000 stanoví zvláštní formy vzájemné dohody, mimo jiné i zřízení společných vyšetřovacích týmů. Na základě vzájemné dohody mezi dvěma nebo více členskými státy, mohou příslušné orgány dotčených států vytvořit za konkrétním účelem a na omezenou dobu SVT. Doba trvání však může být po vzájemné dohodě prodloužena. Každý členský stát, který vyšetřuje přeshraniční trestné činy, může požádat o zřízení SVT. Takový tým se skládá z policistů, státních zástupců, soudců a dalších relevantních osob. Tým vede osoba ze státu, ve kterém SVT působí. I když členové týmu pochází z různých jurisdikcí, musí vykonávat své povinnosti v souladu s vnitrostátními právními předpisy na území, kde vyšetřování probíhá[38].

Při složitých a časově náročných přeshraničních vyšetřováních je zásadní rychlost a efektivita. Na rozdíl od tradičních forem mezinárodní justiční a policejní spolupráce, a to včetně paralelních vyšetřování a výměny dožádání o právní pomoc, SVT usnadňuje, a především urychluje přímou výměnu informací a zjednodušuje spolupráci, komunikaci a koordinaci mezi jejími členy a účastníky. Právě tato přímá spolupráce a komunikace mezi orgány je (resp. dosud byla – viz níže k EPPO) nejefektivnější metodou, jak se vypořádat se zvýšenou sofistikovaností organizované trestné činnosti. Po zřízení SVT si mohou partneři v rámci dohody přímo vyměňovat informace a důkazy, spolupracovat v reálném čase a společně provádět operace. Na základě operativních akčních plánů členové týmu stanoví společné strategie ve vyšetřování a stíhání, včetně

[37] Joint investigation teams. *Eurojust* [online]. [cit. 2022-08-30]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/jits-network

[38] § 72 zákona č. 104/2013 Sb. o mezinárodní justiční spolupráci ve věcech trestních (dále jen ZMJS)

donucovacích opatření. SVT umožňují, aby jejich členové byli přítomni při vyšetřovacích úkonech na území ostatních smluvních stran, a mohli tak asistovat kolegům provádějícím tyto úkony.

Významnou výhodou pro členy SVT je finanční podpora poskytovaná společným vyšetřovacím týmům agenturou pro justiční spolupráci – Eurojustem[39], což snižuje dopad nákladů na vnitrostátní rozpočty[40].

2.2. Evropský vyšetřovací příkaz[41]

Směrnice o evropském vyšetřovacím příkazu (dále jen EVP) je samostatným právním nástrojem pro shromažďování důkazů, který se vztahuje na všechny členské státy Evropské unie s výjimkou Dánska a Irska. EVP je rozhodnutí justičního orgánu vydané či potvrzené justičním orgánem jednoho členského státu EU za účelem provedení vyšetřovacích úkonů v jiném členském státě EU s cílem shromáždit důkazy v trestních věcech. EVP je založen na vzájemném uznávání, což znamená, že vykonávající orgán je povinen uznat žádost jiné země a zajistit její výkon. Příkaz je třeba vykonat stejným způsobem a za stejných podmínek, jako by daný vyšetřovací úkon byl nařízen orgánem vykonávajícího státu. EVP lze též vydat za účelem získání již existujících důkazů. Směrnice vytváří jednotný ucelený rámec pro získávání důkazních prostředků, kdy vyšetřovací úkony mohou zahrnovat například výslech svědků[42], telefonické odposlechy[43], skryté vyšetřování[44] a informace o bankovních operacích[45].

Vydávající orgány mohou EVP využít pouze v případě, je-li daný vyšetřovací úkon: nezbytný, přiměřený a použitelný v obdobných vnitrostátních případech. EVP se vydává za použití standardního formuláře a je přeložen do úředního jazyka vykonávajícího členského státu EU nebo do jiného jazyka určeného vykonávajícím

---

[39] EUROJUST. *European Union Agency for Criminal Justice Cooperation* [online]. [cit. 2022-09-02]. Dostupné z: https://www.eurojust.europa.eu/

[40] Joint investigation teams. *Eurojust* [online]. [cit. 2022-08-30]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/jits-network

[41] Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech; zákona č. 104/2013 Sb. ZMJS, Hlava XI

[42] § 383 a § 384 zákona č. 104/2013 Sb. ZMJS

[43] § 390, § 391, § 392 a § 393 zákona č. 104/2013 Sb. ZMJS

[44] § 389 zákona č. 104/2013 Sb. ZMJS

[45] § 385 a § 386 zákona č. 104/2013 Sb. ZMJS

státem. Podle nové směrnice musí vykonávající členský stát provést vyšetřovací úkon se stejnou rychlostí a prioritou jako v obdobném vnitrostátním případě.

Směrnice stanoví lhůty nejvýše 30 dnů pro přijetí rozhodnutí o uznání a výkonu žádosti a 90 dnů pro provedení požadovaného úkonu v návaznosti na přijetí uvedeného rozhodnutí. Členské státy EU mohou žádost na základě určitých důvodů odmítnout. Důvody pro odmítnutí se vztahují na všechny úkony: imunita nebo výsada nebo pravidla omezující trestněprávní odpovědnost týkající se svobody tisku; poškození základních zájmů v oblasti národní bezpečnosti; jiné než trestní řízení; zásada ne bis in idem[46]; extrateritorialita[47] spojená s oboustrannou trestností a neslučitelnost se závazky v oblasti základních práv.

Některé úkony lze odmítnout na základě dalších důvodů: neexistence oboustranné trestnosti (kromě vymezených závažných trestných činů); a nemožnost provést úkon (vyšetřovací úkon neexistuje nebo není v obdobných vnitrostátních případech dostupný a není k dispozici žádná alternativa). Ačkoli členské státy měly povinnost zavést své vnitrostátní prováděcí právní předpisy do 22. května 2017, teprve od 15. září 2018 se stal tento nástroj v členských státech, které jsou jím vázány, plně funkční.[48]

EVP zavedl jasný postup spolupráce mezi justičními orgány v různých členských státech při shromažďování a uchovávání důkazů. Ze shora uvedeného je zřejmé, že oproti klasické žádosti o právní pomoc, EVP nabízí justičním orgánům jednodušší a rychlejší alternativu k tradičním nástrojům pro vyžádání důkazů, státy mohou jeho výkon odmítnout pouze ze zcela konkrétních a omezených důvodů[49], užití shodného formuláře usnadňuje vzájemné porozumění a zavedené lhůty[50] zvyšují nároky na rychlost vyřízení. Jde o formu

---

[46] § 11odst. 2 zákona č. 141/1961 Sb., trestní řád. Tato zásada vyjadřuje zákaz někoho stíhat nebo potrestat dvakrát za stejnou věc, je neodmyslitelnou a nezpochybnitelnou součástí spravedlivého trestního procesu a jako taková byla v ústavní rovině výslovně vyjádřena v Listině základních práv a svobod.

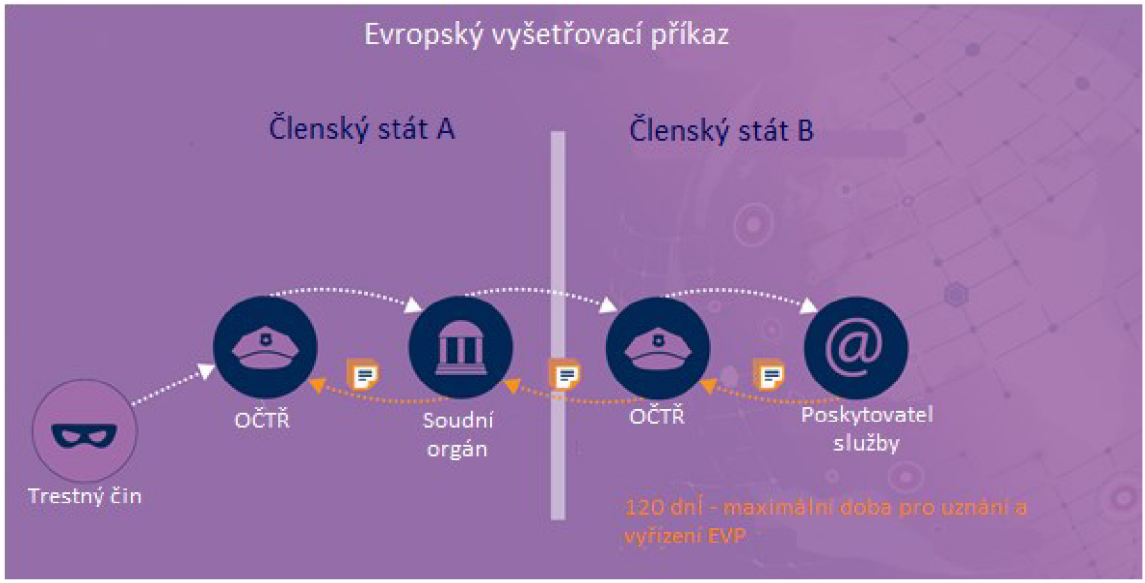
[47] Spáchání trestného činu mimo území příslušného státu

[48] Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy. *Portál evropské e-Justice* [online]. [cit. 2022-08-30]. Dostupné z: https://e-justice.europa.eu/92/CS/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams

[49] § 365 zákona č. 104/2013 Sb. ZMJS

[50] § 364 zákona č. 104/2013 Sb. ZMJS

spolupráce mezi různými zeměmi za účelem shromažďování a výměny informací, včetně elektronických důkazů. Orgány jedné země mohou požádat/poskytnout důkazy nacházející se v jiné zemi a poskytnout je na pomoc při vyšetřování trestných činů nebo trestním řízení v zemi druhé. Níže uvádím názorný příklad žádost o elektronické důkazy v rámci EU, kdy doba pro vyřízení je přesně stanovena do 120 dnů.



Obrázek 3 - Žádost o elektronické důkazy v rámci EU prostřednictvím EVP

2.3. Tzv. Přeshraniční vyšetřování v rámci EPPO

U přeshraniční spolupráce upravené čl. 31 Nařízení EPPO se jedná o zcela průlomovou formu mezinárodní justiční spolupráce svého druhu, která (zjednodušeně) probíhá tak, že evropský pověřený žalobce působící ve státu, kde je vedeno trestní řízení, požádá evropského pověřeného žalobce působícího ve státu, kde je třeba opatřit důkaz, o opatření tohoto důkazy prostředky práva státu, v němž bude důkaz zajištěn. Nařízení vychází z toho, že evropští pověření žalobci (dále jen EDP) stále zůstávají státními zástupci toho kterého státu, v němž působí, se všemi právy a povinnostmi, resp. se všemi zákonnými pravomocemi. Tato forma spolupráce si klade za cíl významně urychlit výměnu informací, EDP mezi sebou komunikují přímo, v angličtině, prostřednictvím elektronického informačního systému uvnitř úřadu, situaci spolu konzultují, vysvětlují si odlišnosti právních

úprav a požadavky, které tedy musí být pro získání dotčených důkazů splněny, výsledky si pak rovněž zasílají přímo.

Postup při získávání důkazů na/z území států účastných se na posílení spolupráci v podobě EPPO v rámci (omezených) kompetencí EPPO představuje článek 31 Nařízení[51].

Vzhledem k nedostatku odborné literatury na toto téma nezbývá než ocitovat alespoň částečné znění Článku 31 Nařízení EPPO, které upravuje zvláštní formu spolupráce mezi účastnými státy, představující zatím nejvyšší stupeň spolupráce v této oblasti:

Článek 31 Přeshraniční vyšetřování

1. Evropští pověření žalobci jednají v úzké spolupráci a v přeshraničních případech si vzájemně pomáhají a pravidelně je spolu konzultují. Má-li být opatření přijato v jiném členském státě, než je členský stát evropského pověřeného žalobce, který případ projednává, rozhodne tento evropský pověřený žalobce o přijetí nezbytného opatření a přidělí je evropskému pověřenému žalobci nacházejícímu se v členském státě, kde má být toto opatření provedeno.

2. Evropský pověřený žalobce, který případ projednává, může přidělit jakákoli opatření, která má k dispozici podle článku 30. Odůvodnění a přijetí takových opatření se řídí právem členského státu evropského pověřeného žalobce, který případ projednává. Pokud evropský pověřený žalobce, který případ projednává, přidělí provedení vyšetřovacího úkonu jednomu nebo několika evropským pověřeným žalobcům z jiného členského státu, informuje o tom současně svého dohlížejícího evropského žalobce.

„Přidělení“ uvedené v prvním odstavci článku 31, znamená, že „dožadující“ Evropský pověřený žalobce (dále jen EDP) shrne, že vede trestní řízení spadající

[51] Více viz: HERRNFELD, Hans-Holger, Dominik BRODOWSKI a Christoph BURCHARD. *European Public Prosecutor's Office: Article-by-Article Commentary*. München, Germany: Nomos/Hart, 2020, 704 s. ISBN 9781509947157.

pod pravomoc EPPO, a že v tomto vyvstala potřeba provést úkon na území jiného státu, účastného na EPPO. Vysvětlí, co konkrétně potřebuje, (např. výslech svědka včetně otázek) a pověří „dožádaného“ EDP provedením takového úkonu. „Dožádaný“ EDP již nic zvláštního nepřezkoumává, a ten který úkon provede podle právního řádu práva svého státu a výsledky následně zašle „dožadujícímu“ EDP, který je pak může přímo použít v trestním řízení, které vede ve svém státě (pod dozorem EPPO).

V souvislosti s čl. 30 uvedeném ve výše uvedeném druhém odstavci, týkající se vyšetřovacích úkonů a jiných opatření, bych ráda uvedla, že právě tento článek upravuje v odst. 1 písm. c) zajišťování elektronických důkazů, kdy konkrétně stanoví, že: „*Členské státy zajistí, aby alespoň v případech, kdy je pro trestný čin, který je předmětem vyšetřování, stanoven trest odnětí svobody s horní hranicí trestní sazby ve výši nejméně čtyř let, měli evropští pověření žalobci pravomoc nařídit nebo vyžádat si následující vyšetřovací úkony:*

c) zajistit předložení uložených počítačových dat, šifrovaných či nešifrovaných, v původní nebo jiné stanovené podobě, včetně údajů o bankovních účtech a provozních údajů, s výjimkou údajů konkrétně zadržených v souladu s vnitrostátními právními předpisy podle čl. 15 odst. 1 druhé věty směrnice Evropského parlamentu a Rady 2002/58/ES (1);[52]

2.4. Způsoby zajišťování elektronických důkazů na území „dožádaného“ státu a jejich význam pro trestní řízení

Poté, co byly shora vysvětleny aktuální způsoby, jakými lze, zejména mezi státy Evropské unie (s odkazem na jejich zapojení do toho kterého stupně vzájemné spolupráce v trestní oblasti), žádat o mezinárodní justiční spolupráci, potažmo zajištění a vydání elektronických důkazů, je třeba minimálně krátce zmínit způsob, jakým skutečně dochází k jejich zajištění na území jednotlivých států, s využitím příkladu právní úpravy České republiky.

[52] Nařízení EPPO, kterým se provádí posílená spolupráce za účelem zřízení EPPO, ODDÍL 2, Pravidla pro vyšetřovací úkony a jiná opatření, čl. 30 Vyšetřovací úkony a jiná opatření. Odst. 1, písm. c)

Jsou-li tedy justiční orgány České republiky jedním ze shora uvedených způsobů požádány o zajištění elektronického důkazu na „jejich území“, postupují při jejich zajištění standardním způsobem, jaký by k tomu využily při vnitrostátním trestním řízení, tj. s využitím právních nástrojů, které mají k dispozici. (Obdobně, žádají-li české OČTŘ o zajištění těchto důkazů v cizích státech, postupují tyto podle své vlastní úpravy.) Rozsah a účel této práce neumožňuje věnovat se jednotlivým důkazním prostředkům (resp. způsobům získávání těchto důkazů) podrobně, shrňme si tedy alespoň nejčastější způsoby, jakým se elektronické důkazy mohou dostat do dispozice českých orgánů činných v trestním řízení (OČTŘ).

Z pohledu této práce jsou naprosto zásadní žádosti OČTŘ (samostatné, případně podmíněné souhlasem soudu), směřující vůči poskytovatelům dotčených IT služeb o vydání údajů, které tyto shromažďují či jimi z důvodů poskytování té které služby disponují. Takové žádost českých OČTŘ i v rámci „dožádání“ od cizích států tedy směřují vůči poskytovatelům těchto služeb sídlících na území ČR.

Mimo to je dále vhodné zmínit institut vydání nebo odnětí věci podle § 78, 79 trestního řádu, jímž může OČTŘ získat datový nosič elektronická data obsahující, typicky flash disk či mobilní telefon. Dalším způsobem zajištění elektronických důkazů je provedení domovní prohlídky podle § 89, během které jsou zajišťovány nosiče dat (počítače, laptopy, notebooky, harddisky, …), které jsou posléze předmětem znaleckého zkoumání, během kterého znalec uchovaná data na těch kterých nosičích fakticky nalézá, případně tato analyzuje.

Samostatnou kapitolu pak tvoří využití tzv. operativně pátracích prostředků, jejichž prostřednictvím jsou získávány důležité údaje takzvaně on-line. Z hlediska využívaných institutů trestního řádu se jedná o odposlechy podle § 88 trestního řádu, o zjištění údajů o telekomunikačním provozu podle § 88a trestního řádu, o sledování osob a věcí podle § 158d trestního řádu, apod[53].

[53] DVOŘÁK, Vratislav a Martin KLOUBEK. *Základy operativně pátrací činnosti policie v definicích a schématech*. Praha: Policejní akademie České republiky v Praze, 2011. s 22, 25. ISBN ISBN978-80-7251-351-2.

Za zmínku stojí, že citované instituty lze většinou využít také v řízení pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva[54].

Využití zmíněných institutů pak může předcházet (a často také předchází) tzv. zmražení dat podle § 7b trestního řádu, které již bylo zmíněno výše.

Způsoby, jakými se elektronické důkazy dostávají do dispozice OČTŘ cizích států v rámci dožádání pak závisí na jejich vnitrostátní úpravě. A právě k harmonizaci jednotlivých právních úprav slouží nástroje mezinárodní spolupráce v podobě již zmíněných mezinárodních úmluv, směrnic a nařízení, v dané oblasti s důrazem na plánované Nařízení, kterému se budu věnovat níže.

2.5. Úmluva o počítačové kriminalitě

Přesto, že hlavním tématem práce je představení návrhu nového Nařízení Evropského parlamentu a Rady o evropských příkazech k vydání a k uchování elektronických důkazů v trestním řízení, Úmluva o počítačové kriminalitě[55] (dále jen Úmluva) je zásadním dokumentem pro oblast počítačové kriminality, a především v boji proti ní. Současně je považována za dosud nejucelenější mezinárodní dohodu o počítačové kriminalitě a elektronických důkazech. Jejím hlavním cílem je harmonizace vnitrostátních zákonů, zlepšení vyšetřovacích technik a zvýšení spolupráce mezi jednotlivými zeměmi. Než se budu věnovat Úmluvě jako takové, je třeba vysvětlit pojem počítačové kriminality, jelikož s ní elektronické důkazy úzce souvisí.

2.5.1. Vymezení pojmu počítačové kriminality

Počítačová kriminalita neboli tzv. kyberkriminalita, je nejčastěji definována jako trestná činnost páchána proti informačním a komunikačním technologiím a jejich prostřednictvím.

---

[54] § 88a odst. 1, § 88a odst. 1 zákona č. 141/1961 Sb. trestní řád
[55] *Convention on Cybercrime* [online]. [cit. 2022-08-30]. Dostupné z: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Různí autoři i různé právní normy používají pro označení této aktivity různé pojmy, mezi které patří: informační[56], informatická[57], elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost (Computer crime), computer – related-crime, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita aj. U této problematiky přetrvávají rozdíly nejen v označování tohoto jevu, ale rozdílně je chápán též jejich obsahový význam, což mnohdy přispívá k nesprávnému pochopení významu a škodlivosti tohoto druhu trestné činnosti.

V 90. letech 20. století se pro trestnou činnost páchanou pomocí informační techniky ustálil pojem „počítačová kriminalita“ (Computercrime, Computerkriminalität).[58] Prof. Smejkal ve své publikaci definuje, v polovině 90. let 20. století, počítačovou kriminalitu, jako různorodou směsici trestných činů, jejichž společným faktorem je počítač, program a data. Pod pojmem počítačová kriminalita „…*je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti.*“ [59] Z této definice vyplývá, že v té době se počítačová kriminalita vztahovala jen na počítačové systémy, jako na cíle útoku.

V mezinárodním společenství jsou také často používány pojmy ”kyberzločin” (”Cyber-Crime”) nebo ”high-tech” zločin. Z hlediska trestního práva již v minulých letech došlo k vymezení, kdy se jako počítačová, respektive informační kriminalita nechápe taková trestná činnost, která je zaměřená na techniku jako objekt zájmu pachatele majetkového trestného činu (například krádež počítače). Pochopitelně může docházet a dochází k prolínání, kdy je výpočetní a jiná technika objektem zájmu ryze ”počítačového” trestného činu, ale současné poškození této techniky

---

[56] Informační kriminalita: jedná se o trestné činy, jejichž prostředkem jsou informace. V tomto případě nezáleží na tom, jak byly informace zpracovány, či užity k útoku.
[57] Informatická kriminalita: cílem útoku v tomto případě nebývá pouze počítač, jeho data a programy, ale celé informační (počítačové) systémy, včetně jejich komponentů.
[58] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, 522 s. CZ.NIC. s. 31–32. ISBN SBN978-80-88168-15-7.
[59] SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo*. Praha: C.H. Beck, 1995, 264 s. Beckova edice právo a hospodářství. s. 99. ISBN 80-717-9009-5.

vede k souběhu s majetkovým trestným činem (např. v případě, kdy počítačový vir způsobí poškození hardwaru).[60] Například Evropská komise definuje počítačovou kriminalitu celkem jednoduše jako trestné činy páchané online prostřednictvím sítí elektronických komunikací a informačních systémů, přičemž je pak dále rozděluje to tří obecných definic: 1) trestné činy typické pro jejich páchání prostřednictvím internetu, jimiž jsou útoky proti informačním systémům nebo phishing[61] (např. falešně vytvořené webové stránky bank, jejich prostřednictvím útočníci vyžadují hesla umožňující přístup k bankovním účtům obětí). 2) online podvody a padělání: rozsáhlé podvody páchané online prostřednictvím krádeže identity, phishingu, spamu a škodlivého kódu. 3) nezákonný online materiál, obsahující sexuální zneužívání dětí, podněcování k rasové nenávisti, teroristickým činům a oslavování násilí, terorismu, rasismu a xenofobie.[62]

Tento druh kriminality se rozpíná do všech oblastí trestné činnosti, zdokonaluje se a postupem času míří na větší, výnosnější cíle a nové technologie. Nové hrozby v podstatě nevznikají jen díky novým technologiím, ale často vycházejí z nedostatků těch současných.

Orgány činné v trestním řízení (dále jen OČTŘ) a další subjekty, které se věnují oblasti počítačové kriminality, by se proto měly zaměřit nejen na potenciální dopad budoucího technologického vývoje v oblasti počítačové kriminality, ale měly by k ní přistupovat komplexně, včetně prevence, zvyšování povědomí a kybernetického vzdělávání. Stejně tak se musí justiční orgány jednotlivých států ve spolupráci s kompetentními zákonodárci na půdě Evropské unie a nečlenských států snažit o soustavné zdokonalování právního rámce, který vyšetřování takového druhu trestné činnosti usnadní a především urychlí.

---

[60] Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a
internetu včetně návrhu řešení. Odbor bezpečnostní politiky ministerstva vnitra, dostupná na https://www.mvcr.cz/soubor/informacni-pdf.aspx

[61] Snaha počítačových podvodníků získat citlivé osobní informace, jako jsou hesla, údaje o platebních kartách, rodná čísla nebo čísla bankovních účtů. Šíří se podvodnými emailovými zprávami nebo přesměrováním na falešné webové stránky. Dostupné z https://www.avast.com/cs-cz/c-phishing

[62] Volně přeloženo z oficiálních webových stránek Evropské komise na https://ec.europa.eu/home-affairs/cybercrime_en

Důsledkem využívání informačních a komunikačních technologií dochází k nebývalým možnostem shromažďování a zpracování dat jednotlivců, proto je tento druh kriminality velkou hrozbou nejen pro lidská práva. Díky narůstající aktivitě hackerských útoků jsou ohroženy i vládní a zdravotnické organizace. Klíčovým prvkem počítačové kriminality jsou data, která jsou uchovávána v tom kterém počítačovém systému.[63] Právě taková data představují tzv. elektronické důkazy, které je třeba zajistit v trestním řízení za účelem odhalení a vyšetření předmětné trestné činnosti. Problematika elektronických důkazů je blíže rozebírána v dalších kapitolách této práce.

2.6. Vývoj, obsah, význam a cíle Úmluvy

Historie

Úmluva byla otevřena k podpisu v listopadu 2001 v Budapešti – proto se jí říká „Budapešťská úmluva" a v platnost vstoupila 1. července 2004. Rada Evropy ji vypracovala ve Štrasburku s účastí pozorovatelských států Kanady, Japonska, Filipín, Jižní Afriky a Spojených států amerických. Do současnosti Úmluvu ratifikovalo 66 států včetně 26 členských států EU[64] (všechny kromě Irska). Rusko se odmítá připojit k Úmluvě z důvodu, že by jejím přijetím byla porušena ruská suverenita, a také často odmítá spolupracovat s OČTŘ při vyšetřování trestných činů týkajících se počítačové kriminality. Česká republika se stala stranou této Úmluvy 1. prosince 2013 dle odstavce 4 článku 36.

Význam úmluvy

Tato Úmluva je první mezinárodní smlouvou o trestných činech spáchaných prostřednictvím internetu a jiných počítačových sítí, která se zabývá zejména

[63] Na tomto místě bych chtěla vysvětlit, že pro dosažení srozumitelnosti textu je místy pracováno s určitým zjednodušením při užívání pojmů z oblasti informačních technologií, které tak z odborného hlediska nemusí být vždy zcela přesné. Pevně věřím, že takové zjednodušení vyváží zasazení dotčených pojmů do právní oblasti, resp. do vysvětlovaného kontextu.

[64] Proposal for a COUNCIL DECISION: authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. *EUROPEAN COMMISSION* [online]. Brussels, 2021 [cit. 2022-08-30]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0718&from=EN#;

porušováním autorských práv, počítačovými podvody, dětskou pornografií a porušováním bezpečnosti sítí. Obsahuje také řadu a postupů, jako je prohledávání počítačových sítí a odposlechy[65]. Slouží jako vodítko pro všechny země utvářející vnitrostátní právní předpisy v oblasti počítačové kriminality, a jako právní rámec pro mezinárodní spolupráci mezi státy, které jsou stranami této smlouvy. Slučuje vizi svobodného internetu volně přístupných a sdílených informací s potřebou účinné reakce trestního soudnictví v případech jejich zneužití. Vyšetřovány a stíhány mohou být pouze konkrétní trestné činy, které jsou v Úmluvě úzce vymezeny. Údaje, které jsou potřebné jako důkazy v konkrétním trestním řízení, jsou zajištěny za okolností zaručující lidská práva a respektující právní stát.[66]

Navzdory vývoji technologií založených na datech a šíření počítačové kriminality, jsou pojmy obsažené v úmluvě technologicky neutrální, a proto lze hmotné trestní právo použít jak na současné, tak na budoucí případné technologie. Úmluva má tak v boji proti počítačové kriminalitě i nadále zásadní význam. Dalo by se říci, že je svým způsobem nadčasová. Cílem úmluvy je především: harmonizovat vnitrostátní trestněprávní hmotněprávní skutkové podstaty trestných činů a související ustanovení v oblasti počítačové kriminality; stanovit vnitrostátní trestněprávní procesní pravomoci nezbytné pro vyšetřování a stíhání těchto trestných činů, jakož i jiných trestných činů spáchaných prostřednictvím počítačového systému nebo v souvislosti s využitím elektronických důkazů; zavést rychlý a účinný režim mezinárodní spolupráce.

Úmluva stanoví trestnost jednání nezákonného přístupu, zásahů do dat a systémů, podvodů souvisejících s počítači a dětskou pornografií, procesní pravomoci při vyšetřování počítačové kriminality a zajišťování elektronických důkazů v souvislosti s jakýmkoli trestným činem; představuje právní základ pro účinnou mezinárodní spolupráci. Ke smlouvě může přistoupit kterákoli země.

---

[65] Convention on Cybercrime. In: *Council of Europe* [online], 2001, 23.11.2001 [cit. 2022-05-29], čl 36, odst 4. Dostupné z: https://rm.coe.int/1680081561

[66] *The Budapest Convention on Cybercrime: benefits and impact in practice* [online]. Strasbourg: Cybercrime Convention Committee (T-CY), 2020, 45 [cit. 2022-08-30]. Dostupné z: T-CY(2020)16_BC_Benefits_rep_Prov_1.docx

Struktura, smluvní strany, podmínky a průběh přistoupení k Úmluvě

Úmluva je doplněna prvním dodatkovým protokolem o trestnosti činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů, který byl otevřen k podpisu v roce 2015[67]. Jednání o jejím druhém dodatkovém protokolu o počítačové kriminalitě pojednává o posílení mezinárodní spolupráce a zpřístupňování elektronických důkazů, který je zásadní pro budoucí vývoj úpravy nakládání s elektronickými důkazy, byla zahájena v září 2017. Tento druhý dodatkový protokol byl přijat v listopadu 2021 a bude podepsán v květnu 2022.

Státy, které se účastnily jednání o Úmluvě (členové Rady Evropy, Kanada, Japonsko, Jihoafrická republika a USA), mohou smlouvu podepsat a ratifikovat. Dle článku 37 se může smluvní stranou stát "přistoupením" jakýkoli jiný stát, pokud je připraven provádět ustanovení této smlouvy. Ať už se smluvní stranou stane stát ratifikací nebo přistoupením, konečný výsledek bude stejný.[68] Je důležité upozornit na to, že samotná EU se nemůže stát smluvní stranou Budapešťské úmluvy, ani jejích protokolů, protože jsou otevřeny pouze jednotlivým státům.

Při uplatňování Úmluvy jednotlivé smluvní strany respektují odpovědnost, kterou nesou jednotlivé vlády za ochranu jednotlivců před trestnou činností prostřednictvím účinného vyšetřování a stíhání takových trestných činů, a to ať už je tato páchána přes internet, nebo „off-line“. Smluvní strany se neustále snaží plnit svůj závazek v oblasti boje proti počítačové kriminalitě tím, že využívají různých mechanismů a orgánů vytvořených v souladu s Úmluvou a přijímají nezbytná opatření umožňující účinnější vyšetřování a trestní řízení. Důležité je zmínit, že využívání a provádění Úmluvy usnadňuje Výbor úmluvy o počítačové kriminalitě zřízený dle článku 46 Úmluvy.[69]

---

[67] *Convention on cybercrime: Protocol on xenophobia and racism* [online]. 2015 [cit. 2022-08-30]. Dostupné z: https://edoc.coe.int/en/module/ec_addformat/download?cle=dc36f18a9a0a776671d4879cae69b551&k=06dc6305622ca0ca43992ae64c25b80f

[68] *Convention on Cybercrime* [online]. [cit. 2022-08-30]. Dostupné z: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[69] Council of Europe. *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* [online]. s.1–2. Strasbourg, 61 [cit. 2022-09-01]. Dostupné z: https://rm.coe.int/1680a49c9d

Úmluva je více než jen právním dokumentem. Je to rámec, který umožňuje stovkám odborníků smluvních stran sdílet zkušenosti a vytvářet vztahy, které usnadňují spolupráci v konkrétních případech počítačové kriminality, včetně mimořádných situací, a to nad rámec konkrétních ustanovení uvedených v této Úmluvě. Každá země ji může využít jako vodítko, kontrolní seznam nebo vzorový zákon. Být smluvní stranou této smlouvy navíc přináší další výhody. Jak již bylo zmíněno, k Úmluvě může přistoupit kterýkoli stát postupem stanoveným článkem 37. Jakmile je k dispozici návrh zákona, z něhož vyplývá, že stát již provedl nebo se předpokládá, že provede ustanovení Úmluvy ve vnitrostátním právu, zašle ministr zahraničních věcí (nebo jiný pověřený zástupce) dopis generálnímu tajemníkovi Evropské rady, v němž uvede zájem svého státu o přistoupení k Úmluvě. Jakmile dojde k dohodě mezi současnými stranami Úmluvy, bude stát vyzván k přistoupení.[70] Vzhledem k tomu, že je přijetí druhého dodatkového protokolu zásadní ve vztahu k elektronickým důkazům a jejich získávání, bude tento blíže rozebrán v následující kapitole, především jeho obsah a cíle.

2.7. Druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílení spolupráce a zpřístupňování elektronických důkazů

Dne 17. listopadu 2021 přijal Výbor ministrů Rady Evropy druhý dodatkový protokol k Úmluvě o počítačové kriminalitě o posílení spolupráce a zpřístupňování elektronických důkazů[71]. Ačkoliv pachatelé počítačové kriminality žádné hranice nerespektují (čímž narůstají obtíže při získávání elektronických důkazů, které mohou být uloženy na území jiných států), jsou pravomoci orgánů činných v trestním řízení omezeny územními hranicemi.

[70] Convention on Cybercrime. In: *Council of Europe* [online], 2001, 23.11.2001 [cit. 2022-05-29]. Dostupné z: https://rm.coe.int/1680081561

[71] , Cybercrime Convention Committee (T-CY). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* [online]. 2021 [cit. 2022-09-01]. Dostupné z: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d#globalcontainer

V důsledku toho dochází k úspěšnému vyšetření pouze velmi malé části počítačové kriminality, která byla orgánům činným v trestním řízení nahlášena.

V reakci na výše uvedené protokol poskytuje právní základ pro zveřejňování informací o registraci doménových jmen a pro přímou spolupráci s poskytovateli služeb v oblasti informací o uživatelích, účinné prostředky pro získávání informací o uživatelích a provozních údajů, okamžitou spolupráci v naléhavých případech, nástroje vzájemné spolupráce a záruky ochrany osobních údajů.

Důvody navržení a následného přijetí druhého dodatkového protokolu

Jedním z důvodů potřeby druhého dodatkového protokolu (dále jen Protokol) byl rychlý vývoj informačních a komunikačních technologií, který přináší nejen nové možnosti, ale také výzvy, kterým budou muset orgány činné v trestním řízení čelit. S jeho přijetím bude mít mechanismus Úmluvy ještě větší význam. Bude efektivněji řešit problémy související s přeshraničními elektronickými důkazy uloženými nejen v členských státech Evropské unie, ale i mimo ni.

Zatímco počítačová a další trestná činnost zahrnující elektronické důkazy v počítačových systémech roste a tyto důkazy jsou stále častěji ukládány na serverech v cloudu, pravomoci orgánů činných v trestním řízení jsou omezeny územními hranicemi. Výbor Úmluvy si byl vědom těchto obtíží a v roce 2012 vytvořil pracovní skupinu, jejímž úkolem bylo se těmito zabývat. Nakonec se pracovní skupina transformovala do tzv. skupiny pro cloudové důkazy, která nakonec doporučila ujednání Protokolu k Úmluvě o posílené mezinárodní spolupráci.[72] Výbor Úmluvy proto v červnu 2017 schválil zadání k jeho přípravám a samotné projednávání Protokolu bylo zahájeno v září 2017.[73] Po čtyřech letech

[72] Council of Europe. *Enhanced international cooperation on cybercrime and electronic evidence:: Towards a Protocol to the Budapest Convention* [online]. Strasbourg, 5.9.2019 [cit. 2022-09-01]. Dostupné z: https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07

[73] *Proposal for authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: EXPLANATORY MEMORANDUM*. In: Brussels, 2021. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0718&from=EN#

a více než 90 zasedáních, byl Výborem ministrů Rady Evropy dne 17. listopadu 2021 přijat protokol, který obsahuje celou řadu ustanovení.

Protokol je navržen tak, aby reagoval na následující problémy:

- jak nejúčinněji získat informace o užívání účtu nebo adresy internetového protokolu, které byly použity ke spáchání trestného činu. Tyto informace o uživateli, který je podezřelý ze spáchání trestného činu, jsou nezbytné pro vyšetřování;
- jak, a za jakých podmínek je možné spolupracovat přímo s poskytovateli služeb v jiném státě za účelem získání takových informací;
- jak neprodleně dosáhnout získání údajů, a to včetně údajů o obsahu v případech ohrožení života;
- jak docílit zefektivnění spolupráce mezi vládami, včetně vzájemné pomoci, a jak zpřístupnit další nástroje justiční spolupráce v oblasti počítačové kriminality a elektronických důkazů;
- jak harmonizovat účinné a efektivní prostředky spolupráce s požadavky právního státu a ochrany údajů;

Protokol poskytne inovativní nástroje pro získání elektronických důkazů, a to zejména:

- přímou spolupráci s poskytovateli služeb (článek 6 a článek 7);
- urychlenou formu spolupráce mezi stranami při zpřístupňování informací o uživatelích a provozních údajích (článek 8);
- urychlenou spolupráci a zpřístupnění údajů v mimořádných situacích (články 9 a 10);
- další nástroje vzájemné pomoci (články 11 a 12);
- ochranu údajů a další záruky právního státu (články 13 a 14).

Ustanovení protokolu budou přínosná jak z provozního, tak z politického hlediska a zajistí, že Úmluva bude i nadále podporovat svobodu internetu, v jehož rámci plní jednotlivé vlády své povinnosti chránit jednotlivce a jejich práva

v kyberprostoru.[74] Protokol byl otevřen k podpisu ve Štrasburku dne 12. května 2022 a je k němu přiložena tzv. důvodová zpráva[75], která smluvním stranám poskytuje návod a pomoc při jeho provádění.

2.8. Instituce, projekty a programy EU a Rady Evropy v oblasti elektronických důkazů a počítačové kriminality

Na poli evropského a celosvětového práva vznikla za účelem uvádění ustanovení Úmluvy do praxe v oblasti elektronických důkazů řada nástrojů – institucí, projektů a programů budování kapacit Rady Evropy a EU, a to v podobě poskytování konkrétní pomoci jak účastnickým, tak třetím státům při boji s počítačovou kriminalitou.

Přístup Rady Evropy v souvislosti s řešením výzev v oblasti počítačové kriminality a s ní související problematikou elektronických důkazů se skládá ze tří vzájemně propojených prvků, a to:

- Úmluvy o počítačové kriminalitě;
- Výboru Úmluvy o počítačové kriminalitě;
- Projektů a programů budování kapacit, které provádí programová kancelář Rady Evropy pro počítačovou kriminalitu (C-PROC[76]) s cílem pomoci zemím na celém světě posílit jejich kapacity v oblasti trestního soudnictví v případech počítačové kriminality a dalších případech zahrnujících elektronické důkazy v souladu s Úmluvou o počítačové kriminalitě a doporučeními Výboru.

[74] Council of Europe. *Future of the Convention* [online]. [cit. 2022-09-01]. Dostupné z: https://www.coe.int/en/web/cybercrime/future-of-the-convention
[75] Council of Europe. *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* [online]. Strasbourg, 61 [cit. 2022-09-01]. Dostupné z: https://rm.coe.int/1680a49c9d
[76] Council of Europe. *Cybercrime Programme Office (C-PROC)* [online]. [cit. 2022-09-01]. Dostupné z: https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

Mezi tyto projekty patří například Glacy+[77], OCTOPUS[78], CyberSouth[79], iPROCEEDS[80] a CyberEast[81]. Některé z nich jsou projekty Rady Evropy, některé EU, ale v zásadě se vždy jedná o tematicky zaměřené projekty financované buď primárně EU, nebo Radou Evropy, případně jde o projekt společný, který je vytvořený za účelem přispění k úspěšnému řešení konkrétního problému, v daném případě problému elektronických důkazů a počítačové kriminality. Jejich úlohou a cílem je posílení schopnosti států po celém světě uplatňovat právní předpisy týkající se počítačové kriminality a elektronických důkazů, sdílení a výměna informací, vzdělávání a školení v této oblasti. Nejvýznamnějším projektem v oblasti elektronických důkazů je projekt Sirius, jehož úloha je popsána níže v kapitole 2.8.2. Nesmím opomenout zmínit Evropskou justiční síť pro boj proti počítačové kriminalitě, jež umožňuje výměnu odborných znalostí, osvědčených postupů a dalších relevantních poznatků týkajících se počítačové kriminality a elektronických důkazů, více viz kapitola 2.8.3.

2.8.1. Výbor Úmluvy o počítačové kriminalitě

Výbor Úmluvy o počítačové kriminalitě zastupuje smluvní státy Úmluvy. Na základě článku 46 Úmluvy[82] je cílem konzultací výboru usnadnit účinné využívání a provádění Úmluvy, výměnu informací a zvážení případných budoucích změn.[83]

Funkce Výboru Úmluvy o počítačové kriminalitě:

Výbor Úmluvy o počítačové kriminalitě je mechanismus umožňující konzultace smluvních stran v souladu s výše uvedeným článkem 46, který stanoví,

---

[77] Council of Europe. *Global Action on Cybercrime Extended (GLACY)+* [online]. [cit. 2022-09-01]. Dostupné z: https://www.coe.int/en/web/cybercrime/glacyplus
[78] , Council of Europe. *Octopus Project* [online]. [cit. 2022-09-02]. Dostupné z: https://www.coe.int/en/web/cybercrime/octopus-project
[79] Council of Europe and European Union. *Octopus Project* [online]. [cit. 2022-09-02]. Dostupné z: https://www.coe.int/en/web/cybercrime/cybersouth
[80] Council of Europe a European Union. *IPROCEEDS -2: Targeting crime proceeds on the internet and securing electronic evidence in South East Europe and Türkiye* [online]. [cit. 2022-09-02]. Dostupné z: https://www.coe.int/en/web/cybercrime/iproceeds-2
[81] Council of Europe. *CyberEast* [online]. [cit. 2022-09-02]. Dostupné z: https://www.coe.int/en/web/cybercrime/cybereast
[82] *Convention on Cybercrime* [online]. [cit. 2022-08-30]. čl. 46. Dostupné z: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
[83] Council of Europe. *Cybercrime Convention Committee* [online]. [cit. 2022-09-02]. Dostupné z: https://www.coe.int/en/web/cybercrime/tcy

že smluvní strany Úmluvy "budou ... pravidelně konzultovat ... s cílem usnadnit": účinné využívání a provádění této úmluvy, výměnu informací a zvážení možného doplnění nebo změny úmluvy.

Článek 46 je právním základem pro činnost Výboru. Konzultace se mají řídit tzv. pružným postupem a ponechávají na smluvních stranách, aby rozhodly, jak a kdy se sejdou. Výbor přijal jednací řád, ve kterém jsou vymezeny jeho fungování a činnost.

Článek 1 tohoto jednacího řádu stanoví, že v rámci plnění svých funkcí Výbor: hodnotí provádění Úmluvy smluvními stranami; přijímá stanoviska a doporučení k výkladu a provádění Úmluvy, včetně pokynů; zvažuje přípravu návrhů právních nástrojů; přijímá stanoviska na žádost orgánů Rady Evropy; přezkoumává fungování stálých kontaktních bodů; podporuje přistoupení k Úmluvě; prosazuje společné postoje smluvních stran na mezinárodních fórech; zapojuje se do dialogu s příslušnými mezinárodními organizacemi; podporuje budování kapacit a zřizuje pracovní skupiny pro řešení konkrétních otázek.[84]

V souladu se svým mandátem podle čl. 46 odst. 1 Úmluvy k výměně "informací o významném právním, politickém nebo technologickém vývoji týkajícího se počítačové kriminality a shromažďování důkazů v elektronické podobě"[85] a ke zvážení "možného doplnění nebo změny Úmluvy" zřídil výbor v roce 2012 ad hoc podskupinu pro příslušnost a přeshraniční přístup k údajům ("přeshraniční skupina"). V prosinci 2014 Výbor rovněž dokončil posouzení ustanovení o vzájemné pomoci v Úmluvě o počítačové kriminalitě a přijal soubor doporučení, včetně těch, která se projednávala v souvislosti s přijetím Druhého dodatkového protokolu. Na základě těchto událostí došlo v roce 2015 k vytvoření pracovní skupiny pro přístup trestního soudnictví k důkazům uloženým v cloudu, a to i prostřednictvím vzájemné právní pomoci (tzv. skupina pro cloudové důkazy).

V roce 2016 tato skupina pro cloudové důkazy mimo jiné dospěla k závěru, že počítačová kriminalita, počet služeb a uživatelů a s nimi i počet obětí dosáhly

---

[84] Cybercrime Convention Committee (T-CY). *25th Plenary Meeting report* [online]. s. 3[cit. 2022-09-02]. Dostupné z: https://rm.coe.int/0900001680a49f74/

[85] *Convention on Cybercrime* [online]. [cit. 2022-08-30]. čl. 46, odst. 2. Dostupné z: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

takových rozměrů, že jen nepatrná část počítačové kriminality nebo jiných trestných činů zahrnujících elektronické důkazy, bude někdy zaznamenána a vyšetřena. Hlavní problémy, které skupina identifikovala, se týkaly „cloud computingu“[86], teritoriality a jurisdikce. Jednoduše řečeno, zazanamenala potíže při získávání přístupu k elektronickým důkazům nebo jejich zveřejňování.[87]

2.8.2. Projekt SIRIUS

SIRIUS je čistě projektem EU, který společně realizují Europol[88] a Eurojust v úzkém partnerství s EJS a je ústředním referenčním bodem v EU pro sdílení znalostí o přeshraničním přístupu k elektronickým důkazům. Cílem projektu je pomoci vyšetřovatelům a státním zástupcům vyrovnat se se složitostí a objemem informací v rychle se měnícím on-line prostředí, a to poskytnutím informací o konkrétních poskytovatelích on-line služeb (dále jen OSP) a vyšetřovacích nástrojích, jakož i kontaktních údajů na OSP. Tyto průběžně aktualizované zdroje jsou přístupné prostřednictvím specifické platformy pro experty, která je přístupná pouze OČTŘ z členských států EU a zemí, které mají operativní dohodu s Europolem[89] a Eurojustem. V rámci projektu byl vypracován soubor samostatných vzorových formulářů pro vnitrostátní orgány, které chtějí zasílat žádosti o uchovávání a zpřístupňování údajů poskytovatelům služeb prostřednictvím dobrovolné spolupráce. Jsou jimi: žádost o uchování elektronických dat, žádost o mimořádné zpřístupnění dat a formulář přímé

---

[86] Doručování výpočetních služeb, včetně serverů, úložišť, databází, sítí, softwaru, analytických nástrojů a inteligentních funkcí, přes internet („cloud“) a nabízí rychlejší inovace, flexibilitu prostředků a cenové výhody. Více viz What is cloud computing?: A beginner's guide. *Azure* [online]. [cit. 2022-09-02]. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-cloud-computing/

[87] Council of Europe. *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* [online]. Strasbourg, 61 [cit. 2022-09-01]. s. 3. Dostupné z: https://rm.coe.int/1680a49c9d

[88] Agentura Evropské unie - Evropský policejní úřad pro spolupráci v oblasti prosazování práva. Jejím cílem je zlepšit bezpečnostní situaci v Evropě prostřednictvím podpory donucovacích orgánů v členských státech EU. Více viz: *O Europolu* [online]. [cit. 2022-09-02]. Dostupné z: https://www.europol.europa.eu/about-europol:cs

[89] Existují dva typy dohod o spolupráci, které může Europol uzavřít se státy a dalšími subjekty mimo EU: strategické a operativní dohody. Cílem obou typů dohod je posílit spolupráci mezi Europolem a danou zemí, existuje však jeden zásadní rozdíl: strategické dohody se omezují na výměnu obecných zpravodajských informací a strategických a technických informací, zatímco operativní dohody umožňují výměnu informací včetně osobních údajů. Více viz *Partners & Collaboration: Fostering cooperation among law enforcement and other partners around the world* [online]. [cit. 2022-09-02]. Dostupné z: https://www.europol.europa.eu/partners-collaboration

žádosti.[90] Projekt SIRIUS je financován Útvarem pro zahraniční politiku Evropské komise (FPI) na základě dohody č. PI/2020/417-500.

2.8.3. Evropská justiční síť pro boj proti počítačové kriminalitě

Tato síť (dále jen EJCN) skládající se ze státních zástupců specializujících se na počítačovou kriminalitu byla založena v roce 2016 s cílem podpořit kontakty mezi odborníky z praxe v jednotlivých členských státech (ale i třetích zemích), kteří bojují proti výzvám, jež představuje počítačová kriminalita páchaná v kyberprostoru s cílem zvýšit účinnost vyšetřování a stíhání trestných činů v této oblasti. EJCN umožňuje výměnu odborných znalostí, osvědčených postupů a dalších relevantních poznatků týkajících se vyšetřování a stíhání kyberkriminality. Síť rovněž podporuje dialog mezi různými aktéry a zúčastněnými stranami, které hrají roli při zajišťování práva v kyberprostoru. V souladu se závěry Rady ze dne 9. června 2016 Eurojust tuto síť hostí, podporuje a zajišťuje úzkou spolupráci.[91] Tato síť existuje zatím jen virtuálně, nicméně vznik jejího sekretariátu je podporovaný předsednictvím České republiky a předpokládá se v následujícím roce. Její plenární zasedání probíhá dvakrát ročně a je financováno z rozpočtu Eurojustu. Síť spravuje také několik pracovních skupin, které se zabývají aktuálními tématy v oblasti počítačové kriminality. Jsou jimi například právě skupina pro elektronické důkazy, virtuální měny, útoky ransomware, uchovávání dat a další. Skupina pro elektronické důkazy se momentálně zabývá výměnou zkušeností se získáváním informací od poskytovatelů služeb se sídlem v Evropě, návrhem nového Nařízení pro elektronické důkazy a přímým přístupem k elektronickým důkazům. Výstupy z těchto diskusí jsou postupovány

3. Nedostatky právní úpravy elektronických důkazů v EU a mimo státy EU

Na úvod této kapitoly bych pro správné pochopení jejího obsahu ráda osvětlila rozdíl mezi informací a důkazem ve vyšetřování. Policie potřebuje nejen vědět –

[90] Eurojust. EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION. *SIRIUS: preservation and data disclosure requests* [online]. [cit. 2022-09-02]. Dostupné z: https://www.eurojust.europa.eu/document/preservation-request-model-form

[91] Eurojust. EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION. *Cybercrime* [online]. [cit. 2022-09-02]. Dostupné z: https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

tedy získat informaci, ale musí ji opatřit ve formě použitelné u soudu tak, aby mohla být použita jako důkaz. Jak uvádí doc. Polčák ve své učebnici o nakládání s elektronickými důkazy, *„aby mohl být důkaz využit v trestním řízení, ať už ve prospěch nebo neprospěch obviněného, musí být zajištěn zákonnou cestou bez podstatných vad. Existence podstatné vady v procesním postupu orgánů činných v trestním řízení může totiž mít za následek absolutní nebo relativní neúčinnost důkazu. Takový důkaz pak nemůže být zohledněn při dokazování a je tudíž pro trestní řízení bezcenný.“*[92]

V dnešní době je většina zásadních informací a důkazů potřebných pro vyšetřování trestných činů uložena v cloudu, na serveru v jiné zemi a/nebo u poskytovatelů služeb, kteří se nacházejí v jiných zemích. Nicméně pro získávání elektronických důkazů uložených v zahraničí a/nebo u poskytovatele služeb, který se nachází v jiné zemi, se vnitrostátní orgány EU spoléhají buď na tradiční existující nástroje justiční spolupráce, nebo na dobrovolnou spolupráci poskytovatelů služeb. V případě žádostí v rámci EU justiční orgány obvykle využívají k získání důkazů EVP či mechanismy uvnitř EPPO. Dohody o vzájemné právní pomoci používají orgány členských států EU k získávání důkazů ze zemí mimo EU a z Irska a Dánska. Tyto postupy dobře fungují při standardním vyšetřování. Nicméně, pro získávání elektronických důkazů, kde hrozí jejich ztráta, vymazání, či přesunutí, je třeba stále hledat metody, které by takovou spolupráci ještě více urychlily a zefektivnily. Mechanismy EU tak, jak jsou popsány výše, fungují celkem dobře. V kapitole o chystaném navrhovaném Nařízení se pak budu věnovat zachycení nových forem mezinárodní spolupráce, které by do budoucna měly vést ke zvýšení efektivity vyšetřování počítačové trestné činnosti.

[92]POLČÁK, Radim ; PÚRY, František ; HARAŠTA, Jakub a kolektiv. Elektronické důkazy v trestním řízení. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7. s. 100

3.1. Přístup získávání elektronických důkazů ve vztahu k třetím státům

Pokud EU uplatňuje pravomoci mimo území členských států, může tím zasáhnout do svrchovanosti třetího státu, v němž se poskytovatel služeb nachází nebo v němž jsou požadované údaje uloženy. I když nelze prokázat porušení zásad mezinárodního práva, jednostranný přístup návrhu Komise může mít negativní dopad nejen na právní jistotu, ale i mezinárodní vztahy. O tom však více v kapitole věnující se rizikům návrhu nového Nařízení. Výbor Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní věci (dále jen Výbor LIBE[93]) ve své studii[94] odkazuje v souvislosti s mezinárodním právem na situaci, kdy od rozsudku Stálého soudního dvora ve věci Lotus[95] je v mezinárodním právu pevně zakotveno, že stát nesmí vykonávat svou moc na území jiného státu (tzv. Lotusův přístup říká, že suverénní státy mohou jednat jakýmkoli způsobem, pokud tím neporušují výslovný zákaz).[96] Právní situace se stává složitější, pokud se donucovací opatření neprovádějí, ale vyvolávají účinek na území jiného státu. Převažující uplatňování soudních příkazů dokládá, že USA se v souvislosti s těmito opatřeními tolik nezajímá o územní svrchovanost. Příkaz k předvolání vyžaduje, aby osoba, která se nachází v jeho jurisdikci, předložila důkazy, které se nacházejí v jiném státě. Mezinárodní rámec vzájemné právní pomoci se nepovažuje za výlučný, ani se nepovažuje používání předvolání za rozporné s mezinárodním právem, protože předvolání je založeno na extrateritoriální soudní pravomoci k předvolání, která podléhá méně přísným požadavkům podle mezinárodního práva, a soudní pravomoc k výkonu se vykonává pouze na vnitrostátním území. Oproti tomu, právní předpisy Spojených států týkající se

---

[93] zkr. LIBE z angl. European Parliament Committee on Civil Liberties, Justice and Home Affairs

[94] Studie Výboru Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní věci: BĄKOWSKI, Piotr a Sofija VORONOVA. *EU Legislation in Progress: Electronic evidence in criminal matters* [online]. [cit. 2022-08-31]. s. 30 – 32. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf

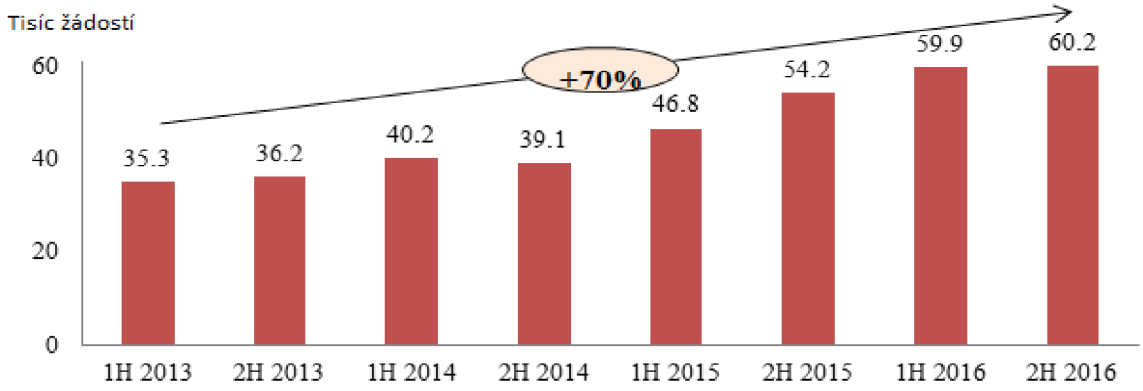
[95] *PUBLICATIONS OF THE PERMANENT COURT OF INTERNATIONAL JUSTICE: The Case of the S.S. "LOTUS"*. In: . 1927. Dostupné také z: https://www.icj-cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf

[96] Čl. 4 odst. 2 Úmluvy Organizace spojených národů proti nadnárodnímu organizovanému zločinu ze dne 15. listopadu 2000 stanoví, že: „Nic v této Úmluvě neopravňuje žádnou smluvní stranu k tomu, aby na území jiného státu uplatňovala výkon soudní pravomoci a výkon funkcí, které jsou vyhrazeny výlučně orgánům tohoto jiného státu na základě jeho vnitrostátního práva“.

povinnosti poskytovatelů služeb zveřejňovat údaje o uživatelích byly vykládány spíše restriktivně. Více viz kapitola 3.2.1.

3.2. Problematika spolupráce se třetími státy

Nicméně s třetími státy je situace významně problematičtější, a to zejména s USA, ačkoliv rozhodující hráči na poli uchovávání dat mají sídlo právě zde. Elektronické důkazy jsou zapotřebí přibližně v 85 % vyšetřování trestných činů a ve dvou třetinách těchto vyšetřování je třeba požádat o důkazy poskytovatele online služeb se sídlem v jiné jurisdikci. Například v letech 2013 až 2016 vzrostl počet žádostí členských států adresovaných hlavním poskytovatelům online služeb (na základě zpráv o transparentnosti společností Facebook, Google, Microsoft, Twitter a Apple) o 70 % (viz graf).



Obrázek 4 - Vývoj počtu žádostí.[97]

Jak již bylo zmíněno, současné postupy spolupráce mezi justičními orgány při získávání elektronických důkazů v přeshraničních situacích jsou příliš pomalé ve srovnání s rychlostí, s jakou lze elektronické údaje měnit nebo mazat. Kromě toho se justiční orgány potýkají s rostoucím počtem případů zahrnujících přeshraniční žádosti o elektronické důkazy. Tyto zdlouhavé postupy ztěžují OČTŘ dokončení vyšetřování a potrestání pachatelů trestné činnosti. V důsledku toho se oběti cítí méně chráněny a občané se cítí méně bezpečně.

[97] Frequently Asked Questions: New EU rules to obtain electronic evidence. *European Commission* [online]. Brussels, 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

Jak již bylo uvedeno v kapitole 2.1.1, vzájemná právní pomoc, je forma spolupráce mezi různými zeměmi za účelem shromažďování a výměny informací, kdy orgány jedné země mohou požádat o důkazy nacházející se v jedné zemi a poskytnout je na pomoc při vyšetřování trestných činů nebo trestním řízení v zemi druhé. V rámci vyřizování vzájemných právních pomocí se uplatňují dva základní postupy, které jsou klíčové při stanovení, "kdo" je oprávněn dát souhlas k přístupu k elektronickým datům? Zaprvé, přijetí a posouzení žádosti o přístup bude vydán určeným ústředním orgánem dožádaného státu a za druhé, nezávislý soudní orgán potvrdí/vydá souhlas se zákonností pro povolení přístupu k údajům a jejich zpracování. Šíření a stále rostoucí využívání elektronických informací zapříčinilo iniciativy žádající urychlení a legalizaci přístupu třetích zemí k údajům uchovávaným soukromými společnostmi nevyužívající postupy vzájemné právní pomoci. Hlavním argumentem zastánců nových postupů je to, že současný platný model vzájemné právní pomoci v praxi nefunguje efektivně, a to z důvodu existence překážek, které je činí příliš složitými a zdlouhavými. Na zdlouhavost vyřizování těchto žádostí poukázala vláda USA v souvislosti s níže popsaným případem Microsoft, když uvedla, že postupy v průběhu vzájemné právní pomoci byly zdlouhavé a nevedly k rychlému zpřístupnění požadovaných údajů. Ve stejném duchu probíhaly diskuse v rámci Rady Evropy/Výboru Úmluvy o počítačové kriminalitě (T-CY), kdy zazněla podobná tvrzení, že postupy vyřizování vzájemné pomoci jsou "obecně neúčinné, a to zejména v souvislosti se získáváním elektronických důkazů.[98]

3.2.1. Případ Microsoft

Komplikace nastalé v průběhu procesu se společností Microsoft, který byl zahájen v roce 2013, jsou příkladem nezprostředkovaného přístupu, kdy se orgány USA snažily získat přístup k údajům týkajících se emailového účtu této společnosti. V prosinci 2013 vláda USA předložila místopřísežné prohlášení, v němž se uvádí, že existuje pravděpodobný důvod domnívat se, že e-mailový účet založený společností Microsoft byl používán k obchodování s narkotiky.

[98] CARRERA, Sergio, Gloria GONZÁLEZ FUSTER, Elspeth GUILD a Valsamis MITSILEGAS. *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*. Brussels, 2015. s. 65. ISBN SBN 978-94-6138-468-3. Dostupné také z: https://www.ceps.eu/cart/?add-to-cart=18574

Příslušný americký magistrátní soudce vydal příkaz k prohlídce podle zákona o uložených komunikacích[99], kterým společnost požádal o zpřístupnění veškerého obsahu emailového účtu. Společnost však odmítla požadovaný obsah zveřejnit s odůvodněním, že americký soud nemůže společnost Microsoft k tomuto úkonu donutit, protože údaje jsou uloženy v datovém centru v Dublinu, v Irsku. Společnost Microsoft poté předložila soudci návrh na zrušení soudního příkazu, který byl zamítnut, neboť soudce zdůraznil, že příkaz zavazuje společnost Microsoft předložit vyžádané údaje bez ohledu na jejich umístění.[100] Soudce zaujal stanovisko, že požadavek vlády nebyl v souladu se zákonem o ochraně osobních údajů, ale spíše o "nucené zpřístupnění" nebo předvolání, a rozhodl, že se v žádném případě nejedná o extrateritoriální uplatnění práva USA. Toto rozhodnutí bylo napadeno u Okresního soudu USA, ale předseda tohoto soudu potvrdil předchozí rozhodnutí[101], přičemž konstatoval, že Kongres USA měl v úmyslu příkazem donutit poskytovatele elektronických komunikací poskytnout veškeré informace pod jejich správou, včetně informací uložených v zahraničí. Hlavní předsedající soudce proto vydal příkaz proti společnosti Microsoft za to, že nadále odmítala vyhovět příkazu. Microsoft se ale odvolal a napadl rozhodnutí soudu s odůvodněním, že požadované záznamy jsou uloženy v datovém centru v cizí zemi, které nepatří společnosti Microsoft, ale uživateli e-mailu, a že příkaz vede ke střetu právních předpisů a k nepřípustnému výkonu extrateritoriální pravomoci.[102] Americká vláda uvedla, že ke střetu zákonů nedochází a že USA si zachovávají pravomoc nařídit subjektu v rámci své jurisdikce, aby záznamy zpětně vydal.[103] Z tohoto pohledu, jak tvrdí americká vláda, je společnost Microsoft společností se sídlem v USA, požívající tzv. "korporátní občanství", s nímž jsou

---

[99] Zákon o uložených komunikacích je součástí zákona o ochraně soukromí v elektronických komunikacích (Electronic Communications Privacy Act, ECPA) a upravuje přístup OČTŘ k obsahu komunikace, pokud je v držení poskytovatele "elektronické komunikační služby" nebo "služby vzdálené výpočetní techniky" pro veřejnost

[101] Příkaz k prohlídce určitého e-mailového účtu kontrolovaného a vedeného společností Microsoft

[102] K Microsoftu se připojilo devět tzv. amici curiae, mezi nimiž byli dva poslanci EP, technologické a mediální společnosti, obchodní sdružení a další občanské společnosti a zástupci akademické obce.

[103] Podle názoru americké vlády "moc nuceného zpřístupnění informací sahá až k záznamům uchovávaným v zahraničí, pokud existuje osobní jurisdikce nad jejich správcem a správce má nad záznamy kontrolu".

spojeny povinnosti, především povinnosti dodržovat právní předpisy, které se týkají příkazu k poskytnutí informací vydaného soudem USA. Tzv. dokument Amicus Curiae[104], předložený dvěma poslanci Evropského Parlamentu na podporu společnosti Microsoft argumentoval, že společnost by měla mít možnost předat údaje prostřednictvím dohody o vzájemné spolupráci, ale nikoliv společnost Microsoft přímo orgánům USA. Irsko rovněž předložilo stanovisko Amicus Curiae, v němž uvedlo, že zahraniční soudy by měly respektovat irskou svrchovanost[105] , a konstatovalo, že "by rádo co nejrychleji zvážilo žádost na základě smlouvy o právní pomoc, pokud by byla podána" v rámci trestního soudnictví. Dokument Amicus Brief, který předložily společnosti Digital Rights Ireland Limited (DRI), Liberty a Open Rights Group zdůrazňuje, že dohoda o vzájemné právní pomoci s EU musí být v právu USA považována za "samovykonatelnou", a tudíž schopnou ovlivnit předchozí právní úpravu USA, aniž by vyžadovala další právní předpisy. Zdůraznily povinnost dodržovat ustanovení dohody o vzájemné spolupráci a uvedly, že "přijetí stanoviska USA by umožnilo americké vládě jednostranně nahradit soudní donucení vyvážením procesu v podobě vyžádání informací dle dohody o vzájemné spolupráci. Vláda USA tvrdí, že použití této dohody by nebylo účinné, neboť údaje by mohly být rychle přesunuty do jiné země, a protože postupy vzájemné právní pomoci jsou zdlouhavé, nevedou k rychlému zpřístupnění údajů.[106] V průběhu projednávání tohoto případu, v březnu 2018 vstoupil v platnost zákon Clarifying Lawful Overseas Use of Data Act (tzv. CLOUD Act), kterým se změnil zákon o uchovávaných komunikacích[107], a to tak, že byl doplněn: *"Poskytovatel služeb musí dodržovat povinnosti stanovené v této kapitole, pokud jde o uchovávání, zálohování nebo zpřístupnění obsahu drátové nebo elektronické*

---

[104] *CRIMINAL JUSTICE (MUTUAL ASSISTANCE) ACT 2008* [online]. 2008 [cit. 2022-08-30]. Dostupné z: https://www.irishstatutebook.ie/eli/2008/act/7/enacted/en/print.html

[105] Institut anglosaského právního systému, který označuje osobu, která není stranou sporu, ale dobrovolně nabídne soudu informaci o svém právním nebo jiném pohledu na projednávaný případ. Obvyklou formou je zpráva nazvaná **amicus curiae brief** (*amici curiae brief*), odborná publikace na téma související s případem nebo přímé svědectví nevyžádané žádnou ze stran sporu. Rozhodnutí, zda přijmout takovou informaci, leží na úvaze soudu.

[106] CARRERA, Sergio, Gloria GONZÁLEZ FUSTER, Elspeth GUILD a Valsamis MITSILEGAS. *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*. Brussels, 2015. s. 12-14. ISBN SBN 978-94-6138-468-3. Dostupné také z: https://www.ceps.eu/cart/?add-to-cart=18574

[107] *18 U.S.C. § 2701: UNLAWFUL ACCESS TO STORED COMMUNICATIONS* [online]. [cit. 2022-08-30]. Dostupné z: https://www.justice.gov/archives/jm/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701

komunikace a jakéhokoli záznamu nebo jiné informace týkající se zákazníka nebo účastníka, které má takový poskytovatel v držení, správě nebo pod kontrolou, bez ohledu na to, zda se taková komunikace, záznam nebo jiná informace nachází na území Spojených států nebo mimo ně." Vláda poté opatřila a doručila společnosti Microsoft nový příkaz podle novelizovaného zákona, přičemž se strany se dohodly, že nový příkaz nahradil příkaz původní. Soud konstatoval, že vzhledem k neexistenci sporného řízení mezi stranami, případ se stal bezpředmětným. Soud zrušil rozhodnutí o přezkumu a vrátil věc soudu prvního stupně s pokynem, aby zrušil rozhodnutí okresního soudu o pohrdání soudem a jeho zamítnutí návrhu společnosti Microsoft na zrušení příkazu a okresnímu soudu nařídil, aby případ (žalobu) zamítl.[108]

Z důvodu nedostatečnosti institutu vzájemné právní pomoci se vyvinula dobrovolná spolupráce mezi OČTŘ a poskytovateli služeb se sídlem ve Spojených státech jako alternativní způsob získávání tzv. bezobsahových údajů[109]. Tato forma spolupráce je sice obecně rychlejší než justiční spolupráce, ale chybí jí spolehlivost, transparentnost, odpovědnost a právní jistota. Zároveň neexistuje jasný rámec pro spolupráci s poskytovateli služeb, kteří dobrovolně přijímají přímé žádosti o bezobsahové údaje, tak jak je povoleno jejich vnitrostátními právními předpisy.

Poskytovatelé služeb se rovněž potýkají s překážkami při přijímání a vyřizování žádostí o přeshraniční přístup k údajům. Posuzování zákonnosti a oprávněnosti těchto žádostí je časově náročné, když musí kontaktovat vydávající orgány za účelem získání doplňujících informací. Kromě toho může být v některých případech zjišťování pravosti a oprávněnosti žádosti podmíněno uzavřením smlouvy s externím poradcem nebo jinou třetí stranou, což vede k dodatečným nákladům, které jdou k tíži poskytovatelů služeb.[110]

---

[108] *United States v. Microsoft Corporation* [online]. 2018 [cit. 2022-08-30]. Dostupné z: https://www.oyez.org/cases/2017/17-2

[109] Jde o poskytnutí údajů o účastnících, přístupových a transakčních údajů, více viz kapitola 1.4 o druzích elektronických důkazů

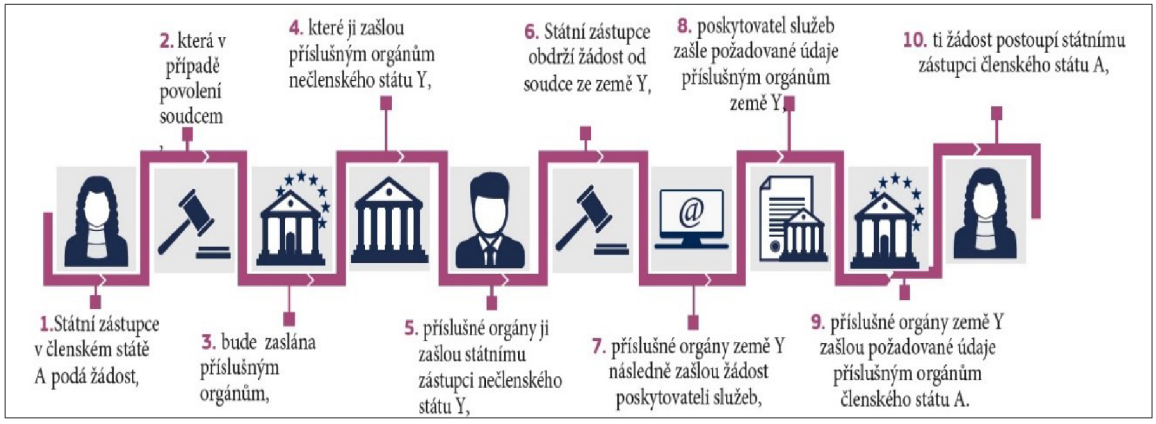
[110] *Summary Report of the public consultation on improving cross-border access to electronic evidence in criminal matters* [online]. [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/info/sites/default/files/report_of_open_public_consultation_on_e_evidence_april2018.pdf

Řešením uvedených nedostatků je navrhované Nařízení o evropském předávacím příkazu a evropském uchovávacím příkazu, které by zavedlo nová pravidla mající orgánům pomoci zajistit a získat elektronické důkazy uložené poskytovateli služeb bez ohledu na to, kde jsou důkazy uloženy. Tato pravidla budou vycházet ze stávajících zásad vzájemného uznávání mezi členskými státy.

3.2.2. Příklady vyřizování žádostí

Pro praktické znázornění zdlouhavého procesu vyřizování žádostí mezi členskými státy EU a třetími státy za stávající právní úpravy, uvádím dva příklady, kdy první se týká spolupráce OČTŘ v případě terorismu a druhý sexuálního zneužívání dětí po internetu. Oba dva příklady uvádí Evropská komise ve svém pracovním dokumentu k novému návrhu Nařízení:

1. *Po teroristickém útoku v členském státě A policie zjistí, že podezřelý je napojen na teroristickou buňku, která se podílela na dalších útocích v jiných členských státech. Policie disponuje informací, že teroristická buňka komunikuje prostřednictvím emailových zpráv s použitím cloudové emailové služby. Policie potřebuje získat údaje o transakcích týkajících se e-mailů odeslaných podezřelým, aby mohla identifikovat další členy teroristické buňky.*



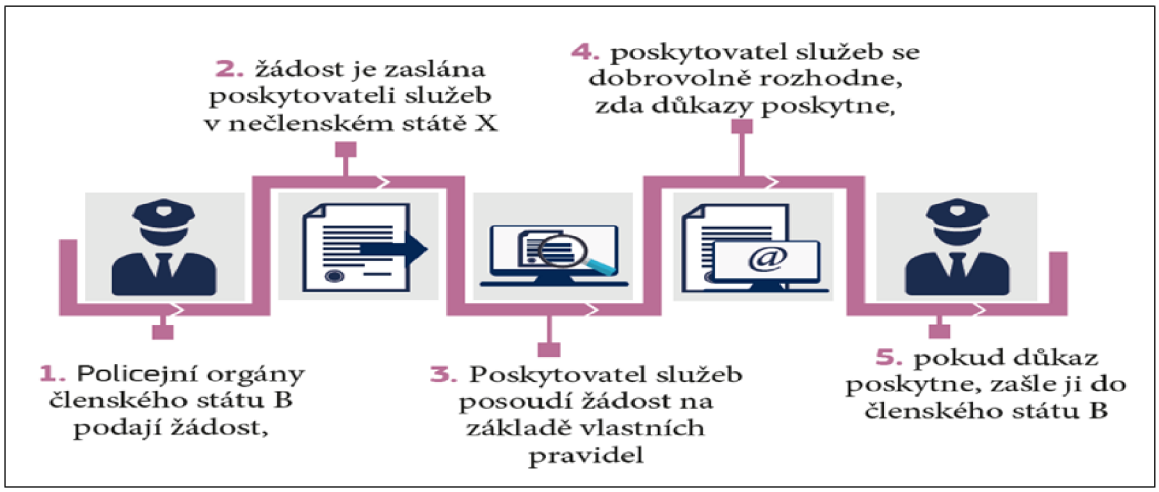
Obrázek 5 - Vyřizování vzájemné právní pomoci mezi nečlenskými státy[111]

[111] *SECURITY UNION: FACILITATING ACCESS TO ELECTRONIC EVIDENCE* [online]. April 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf

Vzhledem k tomu, že poskytovatel služeb provozující cloudovou e-mailovou službu má sídlo ve třetí (nečlenské) zemi **Y**, musí orgány členského státu EU **A** zaslat žádost o právní pomoc orgánům třetí země **Y**, které žádost posoudí a přemění ji na žádost o vnitrostátní příkaz k získání transakčních údajů od poskytovatele služeb. Následně orgány třetí země **Y** předají vyžádané údaje orgánům členského státu EU **A**. Vzhledem k tomu, že vyřízení žádosti o právní pomoc může trvat několik měsíců, bývá vyšetřování značně zpožděno. Nové stopy, které vyplynou ze získaných údajů, jsou pak z důvodu časové prodlevy nepoužitelné.

Níže uvedený praktický příklad znázorňuje vyřizování žádostí mezi třetími státy a členskými státy EU a stávající právní úpravy v případě sexuálního zneužívání dětí:

Poté, co na online fórum Darknetu pronikl materiál zaměřující se na výměnu materiálu s dětskou pornografiíi, policejní orgány třetí země Z se po více než rok věnovaly shromažďování informací čítající více než milion uživatelů na celém světě, které pak sdíleli s OČTŘ po celém světě. Některé z dětských obětí a podezřelých se objevují v členském státě EU B, který dostává informace od nečlenského státu Z. Informace a následné vyšetřování v členském státě EU B vede k odhalení profilu podezřelého na sociálních sítích. Členský stát EU B potřebuje k identifikaci pachatele informace o tom, kdo se za profilem sociální sítě skrývá. Společnost provozující sociální síť sídlí v nečlenské zemi X, jejíž právní předpisy umožňují policii členského státu EU B požadovat od společnosti v nečlenské zemi X dobrovolné poskytnutí informací o předplatitelích využívajících jejich služby.



Obrázek 6 - Vyřizování žádostí mezi třetími státy a členskými státy EU[112]

Výše uvedený proces je závislý pouze na dobré vůli poskytovatele služeb. Přijetí nového návrhu Nařízení by vyřešil doposud nestandardizované postupy napříč službami poskytovatelů služeb, kdy tento proces je za stávající právní úpravy netransparentní a nespolehlivý. Oproti zdlouhavému procesu zasílání žádostí skrze příslušné orgány v jednotlivých státech, jehož výsledek je navíc nejistý, nová pravidla umožní zasílání žádostí přímo poskytovateli služeb, resp. jeho právnímu zástupci.

4. Právní úprava vyřizování žádostí de lege ferenda orgánů EU zvyšující efektivitu získávání elektronických důkazů

EVP měl nabídnout komplexní řešení pro přeshraniční shromažďování důkazů v rámci prostoru svobody, bezpečnosti a práva Evropské unie, který by nahradil různorodé nástroje a zajistil tak jeden standardizovaný příkaz pro všechny druhy důkazů. Ani ne rok po uplynutí lhůty pro jeho zavedení Komise přišla s návrhem tzv. legislativního balíčku elektronických důkazů obsahující nový nástroj použitelný pro získávání elektronických důkazů, a tím je EPP a EUP spolu s návrhem směrnice Evropského parlamentu a Rady stanovující harmonizovaná pravidla pro stanovení právních zástupců za účelem získávání důkazů v trestním řízení. Tato iniciativa vznikla z rostoucí frustrace při shromažďování tohoto typu důkazů a přesvědčení, že EVP není pro tento účel

[112] *SECURITY UNION: FACILITATING ACCESS TO ELECTRONIC EVIDENCE* [online]. April 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf

vhodný. Pokud bude tento nový návrh přijat, vytvoří se dvojí systém přeshraničního shromažďování důkazů s odlišnou filozofií, postupem, vymáháním práva a ochranným právním rámcem.

Ponecháme-li pro potřeby této kapitoly stranou mechanismus přeshraniční spolupráce u států účastných na Úřadu evropského veřejného žalobce, je v současné době právní rámec EU pro získávání jakýchkoli důkazů, včetně těch elektronických, založen především na směrnici 2014/41/EU o EVP v trestních věcech (dále jen "směrnice o evropském vyšetřovacím příkazu"). Kromě toho většina členských států EU – s výjimkou Irska – ratifikovala Úmluvu Evropské rady o počítačové kriminalitě, která, jak je již uvedeno v kapitole 2 o této Úmluvě, specifikuje řadu právních mezinárodních mechanismů pro spolupráci v boji proti počítačové kriminalitě. Podle Úmluvy o počítačové kriminalitě jsou země povinny zavést pravomoci a postupy, které umožní orgánům získat elektronické důkazy a vzájemně si poskytovat právní pomoc, a to nejen v oblasti počítačové kriminality. Úmluva o počítačové kriminalitě rovněž vyžaduje právní předpisy zahrnující možnost požádat o předplatitele údajů přímo od poskytovatelů internetových služeb, pokud jsou služby poskytovány ve smluvním státě[113]. Z toho vyplývá, co bylo vyjádřeno dříve, že přímá spolupráce s OSP je klíčovým prvkem i pro OČTŘ.

4.1. Návrh Nařízení Evropského parlamentu a Rady o evropských příkazech a návrh Směrnice ustanovující pravidla pro jmenování právních zástupců poskytovatelů služeb

Dne 17. 4. 2018 předložila Komise Evropskému parlamentu a Radě návrh nařízení Evropského parlamentu a Rady o evropských příkazech k vydání a k uchování elektronických důkazů v trestním řízení (dále jen Nařízení). Spolu s návrhem nařízení byl předložen i návrh směrnice Evropského parlamentu a Rady stanovující harmonizovaná pravidla pro stanovení právních zástupců za účelem získávání důkazů v trestním řízení. Jde o tzv. legislativní balíček pro

[113] *Convention on Cybercrime* [online]. Article 18(1.b) [cit. 2022-08-30]. Dostupné z: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

elektronické důkazy. V této kapitole bude popsán obsah tohoto balíčku i jeho formy.

Cílem obou návrhů je usnadnění a zrychlení přístupu policie a justičních orgánů k elektronickým důkazům, které jsou uchovávány na území jiného státu. Elektronické důkazy, jimiž mohou být např. e-maily, zprávy na sociálních sítích, údaje z různých aplikací nebo dokumenty uložené v cloudu, jsou pro trestní řízení s rozvojem technologií čím dál důležitější.

Toto nařízení je doprovázeno návrhem směrnice stanovující poskytovatelům služeb povinnost zřídit si na území daného členského státu právního zástupce. Právě ten by měl v budoucnu přijímat a vykonávat příkazy k vydání a uchování elektronických důkazů. Tento zástupce může provedení příkazu také odmítnout, a to ze stanovených důvodů (např. rozpor s právem třetího státu). V takovém případě pak bude do procesu zapojen i příslušný orgán státu, ve kterém má být příkaz vykonán. Členské státy by rovněž měly zavést účinné a přiměřené sankce k případnému vynucení provedení příkazu.

Návrh tedy stanoví, že „předávací a uchovávací příkazy se předávají přímo poskytovateli služeb, který nabízí služby v Unii, nebo právnímu zástupci, kterého ustanovil poskytovatel služeb a který se nachází se v některém členském státě, za použití zvláštních formulářů: certifikátu evropského předávacího příkazu (dále jen EPOC) a certifikátu evropského uchovávacího příkazu (dále jen EPOC-PR).“ Vzory těchto formulářů budou uvedeny v přílohách této práce. Cílem těchto certifikátů je poskytnutí nezbytných informací adresátovi a umožnění snadné identifikace údajů. Z důvodu zabránění ohrožení vyšetřování nejsou v certifikátech zahrnuty důvody pro nezbytnost a přiměřenost ani žádné jiné podrobnosti případu.[114]

[114] *Interinstitutional File: 2018/0108(COD): Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters. s 1 -2. (*In:Brussels, 17 May 2019. l. Dostupné také z: https://data.consilium.europa.eu/doc/document/ST-9365-2019-INIT/en/pdf

Návrh dále stanoví mimo níže uvedené, možnost orgánů členských států i nadále využívat ke shromažďování elektronických důkazů evropské vyšetřovací příkazy a v případě přijetí Nařízení bude stanovena šestiměsíční implementační lhůta,

4.1.1. Právní základ návrhu Nařízení

Návrh Nařízení zavádí příkaz k vydání a příkaz k uchování elektronických důkazů, které mohou být vydány ve vztahu k údajům, které jsou uchovávány poskytovatelem služeb nacházejícím se v jiné jurisdikci a jsou nezbytné jako důkaz v trestním řízení.

Přijetí Nařízení předchází určitá rozhodovací procedura, kdy právním základem EU je Čl. 82 (1) Smlouvy o fungování Evropské unie (dále jen SFEU). Tento stanoví, že opatření mohou být přijímána řádným legislativním postupem s cílem stanovit pravidla a postupy pro zajištění uznávání všech forem rozsudků a soudních rozhodnutí v celé Unii. Opatření mohou být též přijímána s cílem usnadňovat spolupráci mezi justičními nebo rovnocennými orgány členských států v rámci trestního řízení a vymáhání rozhodnutí. Tento právní základ se uplatňuje na mechanismy zahrnuté do tohoto Nařízení. Ustanovením čl. 82 odst. 1 je zajištěno vzájemné uznávání soudních rozhodnutí, která justiční orgán ve vydávajícím státě adresuje právnické osobě v jiném členském státě a jimiž jí dokonce ukládá povinnosti bez předchozího zásahu justičního orgánu v tomto jiném členském státě. Evropský předávací nebo uchovávací příkaz může v případě potřeby vést k zásahu justičního orgánu vykonávajícího státu za účelem výkonu rozhodnutí. Jelikož se návrh týká přeshraničních postupů, v nichž jsou vyžadována jednotná pravidla, není nutné nechávat členským státům prostor k provedení takových pravidel. Nařízení je přímo použitelné, poskytuje jasnost a větší právní jistotu a předchází odchylnému výkladu v členských státech a dalším problémům při provádění, ke kterým dochází v případě rámcových rozhodnutí o vzájemném uznávání rozsudků a soudních rozhodnutí. Nařízení navíc umožňuje, aby stejná povinnost byla v celé Unii uložena jednotným způsobem. Z těchto důvodu se má za to, že nejvhodnější formou pro tento nástroj

vzájemného uznávání je právě nařízení.[115] Při hlasování se EP usnáší nadpoloviční většinou odevzdaných hlasů a Rada rozhoduje kvalifikovanou většinou.

Cílem obou návrhů je usnadnění a zrychlení přístupu policie a justičních orgánů k elektronickým důkazům, které jsou uchovávány na území jiného státu. Komise předložila návrhy těchto předpisů v reakci na nedostatky současné právní úpravy vzájemné právní pomoci v této oblasti, která je pro potřeby trestního řízení příliš pomalá a komplikovaná.

4.1.2. Zásada subsidiarity a proporcionality

EU plně respektuje práva a zásady stanovené Listinou základních práv. K těmto respektovaným zásadám patří mimo jiné zásada subsidiarity a proporcionality. Podle zásady subsidiarity může EU v případech, kdy nemá výlučnou pravomoc, jednat pouze tehdy, pokud je k tomu vzhledem k rozsahu nebo účinkům navrhovaného opatření vhodnější než opatření členských států. Dle zásady proporcionality nesmí obsah a forma činnosti EU překročit rámec toho, co je nezbytné k dosažení cílů Smluv EU. Ustanovení čl. 4 odst. 1 SFEU jasně stanoví, že pokud Smlouvy svěřují Unii pravomoc a není v nich uvedeno žádné zvláštní ustanovení, bude se o tuto pravomoc dělit s členskými státy.

a) Zásada subsidiarity

Vzhledem k přeshraničnímu rozsahu problematiky elektronických důkazů, musí být jednotlivá opatření uvedená v návrhu, přijata na úrovni Unie. Pro trestné činy s existencí elektronických důkazů jsou typické situace, kdy infrastruktura, v níž jsou elektronické důkazy uloženy, a poskytovatel služeb provozující infrastrukturu spadají pod jiný vnitrostátní právní rámec, ať už v Unii nebo mimo ni, než vnitrostátní právní rámec oběti a pachatele trestného činu. V důsledku toho může být pro příslušnou zemi velmi časově nákladné a náročné získat bez společných minimálních pravidel účinný přeshraniční přístup k elektronickým důkazům. Zejména pro členské státy, které jednají samy, by bylo obtížné řešit

[115] ŠTRASBURK. *Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech: DŮVODOVÁ ZPRÁVA*. In: . 2018. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

roztříštěnost právních rámců v členských státech, kterou poskytovatelé služeb snažící se vyhovět žádostem na základě různých vnitrostátních právních předpisů, považují za velký problém; Ukazuje se větší prospěšnost justiční spolupráce na základě stávajících právních předpisů Unie, zejména prostřednictvím EVP.

Vzhledem k rozmanitosti právních přístupů, počtu dotčených oblastí politiky (bezpečnost, základní práva včetně procesních práv a ochrany osobních údajů, hospodářské otázky) a velkému množství zúčastněných stran jsou nejvhodnějšími prostředky k řešení zjištěných problémů právní předpisy na úrovni Unie.[116]

b) Zásada proporcionality

Návrh stanoví pravidla, za nichž příslušný orgán v Unii může nařídit poskytovateli služeb, který nabízí služby v Unii a není usazen v témže členském státě, aby předal nebo uchoval elektronické důkazy. Klíčové prvky návrhu, např. věcná působnost evropského předávacího příkazu, podmínky zaručující mezinárodní zdvořilost, sankční mechanismus a systém záruk a právních prostředků, se soustřeďují na to, co je nezbytné pro dosažení hlavních cílů návrhu. Návrh se zejména omezuje na žádosti o uložené údaje, kdy údaje z odposlechů telekomunikačního provozu v reálném čase do něho nejsou zahrnuty a dále na příkazy vydané v trestních řízeních ve věci vyšetřování konkrétního trestného činu. Nezahrnuje tudíž prevenci trestné činnosti ani jiné druhy řízení či porušení např. právních norem v rámci správního řízení a nevyžaduje, aby poskytovatelé služeb systematicky shromažďovali nebo uchovávali více údajů, než jaké již shromažďují nebo uchovávají z obchodních důvodů nebo za účelem plnění jiných právních požadavků. Navíc zatímco příkazy k předání údajů o účastníkovi a přístupu lze vydat u jakéhokoli trestného činu, příkaz k předání údajů o transakcích nebo obsahu lze vydat pouze u trestných činů postihnutelných ve vydávajícím státě trestem odnětí svobody s horní hranicí sazby nejméně tří let nebo u konkrétních trestných činů závislých

---

[116] ŠTRASBURK. *Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech: DŮVODOVÁ ZPRÁVA*. s. 6. In: 2018. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

na kybernetické činnosti a umožněných kybernetickou činností definovaných v návrhu a u trestných činů souvisejících s terorismem. A konečně návrh objasňuje procesní pravidla a záruky použitelné na přeshraniční přístup k elektronickým důkazům, avšak nezachází až k harmonizaci vnitrostátních opatření. Je omezen na to, co je nezbytné a přiměřené k řešení potřeb donucovacích orgánů a justičních orgánů v digitálním věku.[117]

4.1.3. Důvody a cíle návrhu

Tyto dva nástroje pro usnadnění získávání elektronických důkazů byly koncipovány nejen z důvodu rostoucí potřeby získávání přeshraničních důkazů, ale i z důvodu již zmíněné neefektivnosti současného právního rámce upravujícího tuto problematiku. Dalším důvodem je střet technologického vývoje s tradičními právními normami upravující místní příslušnost a zvýšené potřeby přístupu k digitálním důkazům. Tato potřeba je přímým důsledkem toho, jaké významné místo informační a komunikační technologie zaujímají v našem každodenním životě. Elektronické důkazy se v mnoha ohledech liší od klasických důkazů "z reálného života", a tedy vymáhání práva za současného právního rámce je krajně nepraktické. Přístup k výkonu rozhodnutí z hlediska místní příslušnosti - tj. založený na umístění údajů, je nejen nepraktický, ale vzhledem k nárůstu využívání „cloud computingu“[118], také technologicky zastaralý. Mimo to mohou být údaje přenášeny způsobem, kdy nejsou uloženy na jediném serveru, a tudíž nelze zaslaným žádostem vyhovět. OČTŘ jsou stále více závislé na spolupráci poskytovatelů služeb i z praktických důvodů. Zatímco razie ve společnosti, která odmítá předložit požadované dokumenty, by byla reálnou možností, razie v datovém centru by podobné výsledky nepřinesla, pokud by k získání potřebných údajů nebyly použity nepřiměřeně velké síly, včetně náročných dešifrovacích kapacit, pokud by to vůbec bylo možné.

---

[117] ŠTRASBURK. *Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech: DŮVODOVÁ ZPRÁVA*. s. 6. In: 2018. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

[118] Doručování výpočetních služeb, včetně serverů, úložišť, databází, sítí, softwaru, analytických nástrojů a inteligentních funkcí přes internet

Návrh Komise zavádí závazný příkaz, který, v případě, že bude návrh přijat, bude vypadat takto: Příslušné orgány členského státu A zašlou přímo poskytovateli služeb v členském státu B příkaz k poskytnutí důkazů, a to v zásadě bez zapojení orgánů členského státu B. Kromě toho návrh opouští místní příslušnost jako zásadu rozhodující o tom, kam mají být příkazy adresovány. Podle tohoto nového systému by poskytovatelé služeb byli povinni určit alespoň jednoho právního zástupce v daném členském státě EU pro "přijímání, plnění a vymáhání" těchto příkazů.[119] Pokud by tak neučinili, znamenalo by to, že příslušné orgány mohou zaslat příkaz kterékoli provozovně poskytovatele služeb v zemi, kde se nachází[120]. Tyto povinnosti se týkají všech poskytovatelů služeb, kteří služby v Unii nabízejí. Nebyl-li jmenován žádný zvláštní právní zástupce, mohou být jak evropský předávací příkaz, tak evropský uchovávací příkaz adresovány jakékoli provozovně poskytovatele služeb v Unii.[121] Výše uvedené ale neznamená, že každá služba dostupná z EU, spadá do oblasti působnosti této směrnice. Zejména místo, kde se údaje nacházejí, nemá pro rozhodnutí o tom, zda a kterému místu lze žádost podat a kterému místu má být adresována, žádný význam. Tento přístup ale může poskytovatele služeb dostat do rozporu s právními předpisy mimo EU, zejména s americkými. Konflikt může být ještě závažnější, protože nařízení potencionálně umožňuje požadovat údaje o osobách, které nejsou občany EU. V této souvislosti je důležité upozornit na jednání, která vede EU s USA o dohodě podle nedávno přijatého zákona Clarifying Lawful Overseas Use of Data (dále jen zákon Cloud)[122]. Právní předpisy USA (Electronic Communications and Privacy Act 1986) v zásadě zakazují, aby jejich služby sdílely údaje o obsahu se zahraničními orgány činnými v trestním řízení mimo postup Vzájemné právní pomoci (údaje, které nejsou obsahem, mohou být sdíleny dobrovolně).[123] Zákon Cloud by zrušil toto tzv. blokovací ustanovení za

[119] Článek 3 (1) návrhu Nařízení
[120] Článek 7 (2) návrhu Nařízení
[121] Článek 2 (1), (2), (4) návrhu Nařízení
[122] Spojené státy přijaly v březnu 2018 zákon Clarifying Lawful Overseas Use of Data (tzv. Cloud), aby urychlily přístup k elektronickým informacím uchovávaným celosvětovými poskytovateli služeb se sídlem v USA, které jsou klíčové pro vyšetřování závažné trestné činnosti našimi zahraničními partnery, od terorismu a násilné trestné činnosti až po sexuální zneužívání dětí a kyberkriminalitu.
[123] DASKAL, Jennifer. *Unpacking the CLOUD Act* [online]. 31.1.2019, 220-225 [cit. 2022-08-31]. Dostupné z: https://eucrim.eu/articles/unpacking-cloud-act/

předpokladu, že Spojené státy americké podepíšou s danou zemí dohodu na základě posouzení instituce právního státu a ochrany soukromí v dané zemi. [124]

Pro zajištění prostoru svobody, bezpečnosti a práva je nanejvýš důležité, aby mezi EU a USA existovala jen jedna dohoda namísto roztříštěné mozaiky různých dohod, ke kterým navíc některé členské státy zatím ani nepřistoupily. Zavedením jednoho nástroje pro přeshraniční výměnu elektronických důkazů na úrovni EU by se EU měla stát preferovaným partnerem Spojených států[125]. Nařízení o EPP obsahuje také možnost uchovávat údaje s ohledem na následné žádosti o předložení takto uchovaných údajů nejen prostřednictvím EPP, ale i vzájemné právní pomoci, nebo evropského vyšetřovacího příkazu.[126]

4.1.4. Evropský předávací příkaz

Evropským předávacím příkazem (dále jen EPP) se rozumí závazné rozhodnutí vydávajícího orgánu členského státu nutící poskytovatele služeb nabízejícího služby v Unii a usazeného nebo zastoupeného v jiném členském státě předat elektronické důkazy.[127] V praxi to bude znamenat, že příkaz umožní justičnímu orgánu v jednom členském státě požádat o přístup k elektronickým důkazům (jako jsou e-maily, textové zprávy nebo zprávy v aplikacích) přímo právního zástupce poskytovatele služeb v jiném členském státě, který bude povinen odpovědět do 10 dnů a v naléhavých případech do 6 hodin (ve srovnání se 120 dny u stávajícího evropského vyšetřovacího příkazu nebo 10 měsíci u řízení o vzájemné právní pomoci). Níže je názorně uvedeno, jak bude vyřizování žádostí o elektronické důkazy vypadat v praxi.

---

[124] TOSZA, Stanislaw. All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order. *New Journal of European Criminal Law* [online]. 2020, 161-183 [cit. 2022-08-31]. Dostupné z: doi:https://doi.org/10.1177/2032284420919802

[125] *Doporučení pro ROZHODNUTÍ RADY o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech: DŮVODOVÁ ZPRÁVA*. Brusel, 2019. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52019PC0070&from=EN

[126] Článek 6 (2) návrhu Nařízení

[127] Článek 2 (1) Nařízení o EPP

Obrázek 7 – Vyřizování žádostí o el. důkazy prostřednictvím budoucího EPP[128]

4.1.5. Evropský uchovávací příkaz

Jde o závazné rozhodnutí vydávajícího orgánu členského státu nutící poskytovatele služeb nabízejícího služby v Unii a usazeného nebo zastoupeného v jiném členském státě uchovávat elektronické důkazy vzhledem k následné žádosti o předání údajů[129]. Evropský příkaz k uchování dat umožní soudním orgánům v jednom členském státě uložit poskytovateli služeb nebo jeho právnímu zástupci v jiné zemi EU, aby zabránil vymazání elektronických důkazů ještě před vyřízením žádosti o jejich předložení. Příkazy se budou vztahovat pouze na uložené údaje. Na odposlech telekomunikací v reálném čase se tento návrh nevztahuje.

Pojem elektronické důkazy je nepříliš jednoznačně definován v nařízení o EPP, jako důkazy uložené v elektronické podobě poskytovatelem služeb nebo jeho jménem v době obdržení certifikátu předávacího nebo uchovávacího příkazu, sestávající z uložených údajů o účastníkovi, údajů o přístupu, údajů o transakcích a údajů o obsahu.[130] Měly by ale být chápány spíše jako důkazy uložené v elektronické podobě poskytovatelem služeb nebo jeho jménem v momentě přijetí

[128] Frequently Asked Questions: New EU rules to obtain electronic evidence. *European Commission* [online]. Brussels, 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
[129] Čl. 2 (2) Návrh nařízení o EPP a EUP
[130] Článek 2 (6) Nařízení o EPP

příkazu a sestávající z jedné ze čtyř kategorií údajů: účastník, přístupové, transakční a obsahové údaje. Každá z těchto kategorií je definována v čl. 2 nařízení o EPP. Legislativa definuje elektronické důkazy s požadavkem mít je k dispozici od poskytovatelů služeb v okamžiku přijetí žádosti. Jedná se ale spíše o to, jaký nástroj použít než o to, co je, či není elektronickým důkazem. Tento aspekt bude relevantní pro vymezení oblasti působnosti evropského vyšetřovacího příkazu a evropského vyšetřovacího příkazu.[131]

4.1.6. Návrh směrnice

Stejně tak jako Nařízení, tak i návrhu Směrnice předchází určitý rozhodovací postup. Právním základem EU je Čl. 53 a 62 SFEU a v průběhu hlasovací procedury se EP také usnáší nadpoloviční většinou odevzdaných hlasů a Rada rozhoduje kvalifikovanou většinou.

Návrh Směrnice slouží jako nástroj na překonání rizika, které představují rozdílné vnitrostátní postupy dokazování v trestních řízeních, neboť stanoví pravidla pro jmenování právních zástupců poskytovatelů služeb s cílem harmonizovat různé vnitrostátní přístupy, jež v současnosti zahrnují: uplatňování vnitrostátní jurisdikce na poskytovatele služeb na základě jeho sídla, místa, kde nabízí služby, nebo umístění jeho údajů; rozšíření pravomoci vymáhat právo (extrateritorialita); nebo požadavek, aby byl jmenován zvláštní zástupce pro některé poskytovatele služeb pro daný členský stát.

Obsah návrhu směrnice stanovuje poskytovatelům služeb povinnost zřídit si na území daného členského státu právního zástupce. Čl. 2 odst. 1 návrhu Směrnice definuje právního zástupce jako právnickou nebo fyzickou osobu jmenovanou poskytovatelem služeb písemně za účelem přijímání, dodržování

---

[131] TOSZA, Stanislaw. All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order. *New Journal of European Criminal Law* [online]. 2020, 161-183 [cit. 2022-08-31]. Dostupné z: doi: https://doi.org/10.1177/2032284420919802

a vymáhání rozhodnutí a příkazů vydaných příslušnými orgány členských států za účelem shromažďování důkazů v trestním řízení.[132]

Právě tento právní zástupce by měl v budoucnu přijímat a vykonávat příkazy k vydání a uchování elektronických důkazů. Tento ale může provedení příkazu také odmítnout, a to ze stanovených důvodů např. v případě rozporu s právem třetího státu. V takovém případě pak bude do procesu zapojen i příslušný orgán státu, ve kterém má být příkaz vykonán. Členské státy by rovněž měly zavést účinné a přiměřené sankce k případnému vynucení provedení příkazu.[133]

Jelikož neexistuje obecný právní požadavek, aby poskytovatelé služeb ze zemí mimo EU byli fyzicky přítomni na území Unie při poskytování služeb v rámci Unie, bylo nutné vytvoření právních zástupců. Právní zástupci jmenovaní podle této směrnice by ostatně mohli být využívání rovněž pro vnitrostátní řízení.[134]

Rada stanovila lhůtu pro provedení ve vnitrostátním právu v délce 18 měsíců s cílem zajistit, že právní zástupci začnou naplno pracovat, jakmile o 6 měsíců později vstoupí v platnost nařízení o elektronických důkazech.[135]

---

[132] Čl. 1 odst. a Čl. 3 odst. 1, 2 a 3 návrhu Směrnice, více viz. https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0226&from=CS

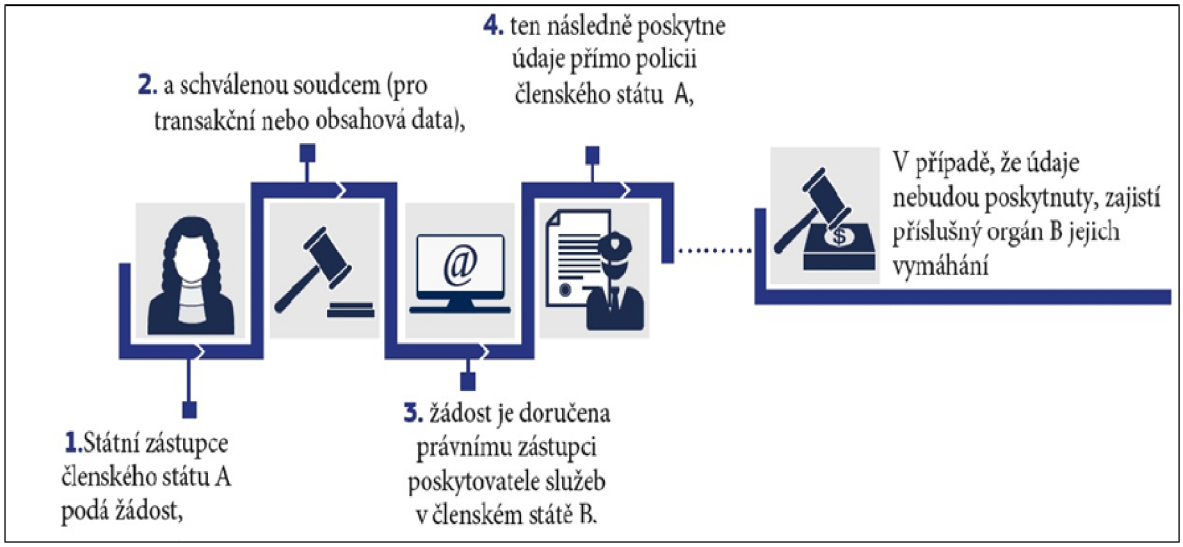
[133] Čl. 5 odst. 1 návrhu Směrnice, více viz https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0226&from=CS

[134] Více viz https://www.consilium.europa.eu/cs/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/

[135] Čl. 7 odst. 1 návrhu směrnice, více viz https://www.consilium.europa.eu/cs/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/

4.1.7. Příklad postupu vyřizování žádostí dle navrhované právní úpravy

Níže uvádím znázornění procesu vyřizování žádostí dle navrhované právní úpravy v praxi:



Obrázek 8 - Vyřizování žádostí při kontaktování poskytovatele služeb napřímo[136]

Tradiční nástroje justiční spolupráce jako je EVP a vzájemná právní pomoc budou i nadále využívané, ale ve specifických případech souvisejících s potřebou rychlého získání elektronických důkazů, a to právě v případech trestného činu terorismu nebo sexuálního zneužívání dětí, bude k dispozici evropský předávací příkaz. S tímto novým nástrojem související nová pravidla umožní rychlejší získávání elektronických důkazů bez ohledu na to, kde jsou data uložena.

4.2. Podmínky pro vydání EPP a EUP

Vydávání EPP nebo EUP bude možné pouze v rámci trestního řízení a budou uplatňována všechna stávající procesní práva v trestním řízení, stanovená ve směrnicích Evropského parlamentu a Rady 2010/64/EU[137],

[136] *SECURITY UNION: FACILITATING ACCESS TO ELECTRONIC EVIDENCE* [online]. April 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf
[137] 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).

2012/13/EU[138], 2013/48/EU[139], 2016/343[140], 2016/800[141] a 2016/1919[142], včetně dalších příslušných právních předpisů na úrovni EU, kterými jsou právo na obhájce a právo na nahlédnutí do spisu. Návrh Nařízení také zavádí povinnost orgánů získat schválení všech příkazů od soudního orgánu, aby se zajistilo, že byla ověřena jejich zákonnost, nezbytnost a přiměřenost.

Příkazy k předání údajů o účastníkovi nebo přístupových údajů bude možné vydat u všech trestných činů, kdežto příkazy k předání transakčních údajů (zdroj a cíl zprávy, údaje o poloze zařízení) nebo údajů obsahových (text, zvuk, videa nebo obrázky) budou moci být vydávány pouze v případech trestných činů, za které lze ve vydávajícím státě uložit trest s horní hranicí trestní sazby nejméně tři roky, nebo v případech konkrétních kybernetických trestných činů a trestných činů souvisejících s terorismem vymezených v návrhu.[143]

Příkaz k uchování údajů bude možné vydat pouze v případech, je-li to nezbytné a přiměřené k zabránění odstranění, smazání nebo změně údajů vzhledem k následné žádosti o předání těchto údajů prostřednictvím vzájemné právní pomoci, EVP nebo EPP. EUP lze vydat u všech trestných činů.[144]

4.3. Provedení Certifikátů EPP a EUP

EPP a EUP budou dle Čl. 7 návrhu Nařízení adresovány právnímu zástupci ustanovenému poskytovatelem služeb za účelem shromažďování důkazů v trestním řízení v souladu s výše uvedeným návrhem Směrnice. Jejich předání bude v podobě certifikátu EPP (dále jen „EPOC“) nebo certifikátu EUP (dále jen

---

[138] 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).
[139] 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).
[140] 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).
[141] 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).
[142] 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).
[143] Čl. 5 odst 3 a 4 písm. a) a c) návrhu Nařízení
[144] Čl. 6, odst. 2 návrhu Směrnice

„EPOC-PR“) podle článku 8. Tento právní zástupce bude odpovědný za jejich přijetí a včasné a úplné provedení. Poskytovatelé služeb si tak mohou vybrat, jak se zorganizují, aby údaje nařízené orgány členského státu předaly. Čl. 8 dále stanoví, že vzory obou certifikátů budou stanoveny v příloze I a II nařízení a musí být přeloženy do jednoho z úředních jazyků členského státu, kde se nachází adresát. Poskytovatel služeb může prohlásit, že příkazy budou akceptovány též v jiných úředních jazycích Unie. Cílem certifikátů je poskytnout adresátovi všechny nezbytné informace ve standardizovaném formátu, který minimalizuje příčiny chyb, umožňuje snadnou identifikaci údajů, a co nejvíce se vyhýbá volnému textu, což snižuje náklady na překlad. Úplné odůvodnění s důvody pro nezbytnost a přiměřenost nebo další podrobnosti o případu se do certifikátu neuvádějí, aby nedošlo k ohrožení vyšetřování. Tyto bude třeba uvést až na samotném příkazu, aby bylo později podezřelé osobě umožněno napadnout je během trestního řízení. Vzory certifikátů EPOC a EPOC – PR jsou přiloženy na konci této práce jako Annex 1 a Annex 2.

4.4. Zavedení povinných lhůt pro provedení certifikátů

Článek 9 stanoví povinnost adresátů odpovídat na certifikáty EPOC a zavádí povinné lhůty, kdy obvyklá lhůta činí deset dnů, přičemž orgány mohou v odůvodněných případech stanovit lhůtu kratší. V naléhavých případech, definovaných jako situace, kdy je bezprostředně ohrožen život nebo tělesná integrita osoby nebo je bezprostředně ohrožena kritická infrastruktura, činí lhůta šest hodin. Článek 10 stanoví lhůtu pro provedení certifikátu EPOC-PR a požaduje uchování údajů dostupných v době obdržení příkazu. Poskytovatelé služeb by měli uchovat údaje tak dlouho, jak to bude nezbytné k předání požadovaných údajů, pokud vydávající orgán do 60 dnů po vydání příkazu potvrdí, že vydal následnou žádost o předání. To vyžaduje, aby byly podniknuty alespoň některé formální kroky, například zaslání žádosti o překlad v rámci vzájemné právní pomoci. Na druhou stranu by žádosti o uchování měly být podávány nebo udržovány tak dlouho, jak to bude nezbytné k umožnění následné žádosti o předání těchto údajů. Aby se předešlo zbytečnému nebo nadměrně dlouhému uložení, informuje orgán, který vydal evropský uchovávací příkaz, adresáta, jakmile se rozhodne o nevydání předávacího příkazu nebo žádosti o justiční spolupráci nebo o jejich stažení.

5. Přínosy návrhu nového Nařízení

Předmětem a účelem navrhovaného nařízení je zavedení nového nástroje spolupráce, kterým bude moci donucovací orgán v jednom členském státě nařídit poskytovateli služeb usazenému nebo zastoupenému v jiném členském státě, aby předložil nebo uchoval elektronické důkazy. Komise se tak odchyluje od tradičního pravidla mezinárodní spolupráce, podle něhož je k přeshraničnímu přístupu k elektronickým údajům nutný souhlas státu, ve kterém jsou údaje uloženy.[145]

Hlavním cílem nových pravidel je nejen poskytnutí záruky urychlení přístupu k elektronickým důkazům bez ohledu na to, kde se údaje nacházejí, ale také harmonizovaná a jasná pravidla pro poskytovatele služeb a dodržování základních práv. Tato pravidla by umožnila justičním orgánům v jedné zemi EU přímo požádat o přístup k elektronickým důkazům kteréhokoli poskytovatele služeb, který nabízí služby v EU, a přitom je usazen nebo zastoupen v jiném členském státě. Tímto způsobem by se vyřízení žádosti o přístup urychlilo, jelikož by nebylo třeba žádat orgány jiného členského státu.

Návrh Komise, který rozšiřuje pravomoc v oblasti vymáhání práva na poskytovatele služeb a/nebo údaje nacházející se v nečlenském státě, vychází z nestálosti počítačových údajů a je podpořen teoretickým konceptem neteritoriality údajů. Studie Výboru LIBE zabývající se návrhem nového Nařízení konstatuje, že s ohledem na odpovídající vývoj mezinárodního smluvního práva a vnitrostátních právních předpisů nelze příslušnost k vymáhání práva založenou pouze na místě, kde poskytovatel služeb nabízí své služby, považovat za porušení státní suverenity podle mezinárodního práva. Na druhou stranu, nové nástroje spolupráce zavedou mezinárodní závaznou povinnost svého adresáta v rámci Unie, která se zásadně liší od stávajícího právního rámce mezinárodní spolupráce v oblasti svobody, bezpečnosti a práva a která může zasahovat do tradičního pojetí územní svrchovanosti.[146]

---

[145] Čl. 25 Úmluvy Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních údajů, bod 2.1.2.

[146] Studie Výboru Evropského parlamentu pro občanské svobody, spravedlnost a vnitřní věci: BĄKOWSKI, Piotr a Sofija VORONOVA. *EU Legislation in Progress: Electronic evidence in criminal matters* [online]. [cit. 2022-08-31]. s. 30 Dostupné z:

5.1. Rychlé obdržení vyžádaných elektronických důkazů

Tato pravidla by umožnila justičním orgánům v jedné zemi EU přímo požádat o přístup k elektronickým důkazům kteréhokoli poskytovatele služeb, který nabízí služby v EU, a přitom je usazen nebo zastoupen v jiném členském státě. Tímto způsobem by se vyřízení žádosti o přístup urychlilo, jelikož by nebylo třeba žádat orgány jiného členského státu.

Jde tedy především o zvýšení rychlosti v boji proti trestné činnosti. OČTŘ budou schopny získat elektronické důkazy mnohem snadněji a rychleji, než je tomu tak za současné právní úpravy. Jde například o digitální fotografie, zprávy z aplikací sociálních médií. Návrh nového Nařízení vyžaduje, aby poskytovatelé služeb vyhověli žádosti do 10 dnů a v naléhavých případech do 6 hodin. Nastavení těchto lhůt umožní vyšetřování trestných činů rychleji a účinněji, a to hlavně v případech trestné činnosti terorismu.

5.2. Harmonizovaná a jasná pravidla pro poskytovatele služeb

Nová pravidla EPP i EUP budou závazná, vnesou do nich jasnost a právní jistotu jak pro poskytovatele služeb, tak pro donucovací orgány. Návrh umožní poskytovatelům služeb v případě potřeby požádat vydávající orgány o vysvětlení a v určitých situacích vznést námitku proti výkonu příkazů.

Tato pravidla jsou zásadní především v případech, kdy jsou elektronické údaje uloženy v zemi mimo EU. Je rozdíl mezi místem uložení údajů a místem sídla poskytovatele služeb. Poskytovatel služeb může mít sídlo ve třetí zemi, ale údaje mohou být uloženy v EU, a to i v zemi vyšetřujícího státu. Přesto se podle stávajícího systému musí justiční orgány obrátit na poskytovatele služeb ve třetí zemi s žádostí o již výše vysvětlenou vzájemnou právní pomoc. To by se podle nového návrhu změnilo, a to následovně.

Návrh nového Nařízení upouští od uchovávání údajů jako rozhodujícího faktoru pro určení příslušnosti a spíše vyžaduje, aby požadované údaje byly (1)

---

https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf

nezbytné pro trestní řízení, k němuž je příslušný vydávající orgán, a (2) souvisely se službami poskytovatele, který nabízí služby v Unii. V takovém případě musí být údaje uchovány a předloženy bez ohledu na místo uložení údajů. V případě, že se poskytovatel služeb při vyžádání důkazů setká s protichůdnými povinnostmi vyplývajícími z práva země, která není členem EU, návrh předpokládá přezkumný postup pro vyjasnění takové situace. Rozhodnutí o tom, zda bude žádosti vyhověno, bude nakonec na příslušném vnitrostátním soudu. Poskytovatel služeb, který uchovává údaje týkající se jeho evropských uživatelů mimo EU, např. právě v USA, tak bude muset poskytnout údaje evropským orgánům, pokud bude osloven evropským předávacím příkazem, a pokud nedojde k rozporu s právem třetí země.[147] V takových případech poskytovatelé služeb budou moci vznést námitku založenou na těchto protichůdných povinnostech, což může vyvolat soudní přezkum a zajistit tak jasný postup v případě střetu s právním řádem nečlenského státu. Pokud bude právo třetí země chránit základní práva nebo zájmy třetí země, měl by soudce obvykle po konzultaci s orgány třetí země příkaz zrušit. Pokud právo třetí země chrání jiné zájmy, soudce bude muset tyto zájmy vyvážit. V obou případech by ale měl poskytovatel služeb údaje zachovat.[148]

Poskytovatelům služeb, kteří nesplní své závazky podle článků 9, 10, nebo 11**,** mohou být uloženy sankce**.**[149] Tyto sankce mohou dosáhnout 2 % celkového celosvětového ročního obratu za předchozí finanční rok.[150]

5.3. Dodržování základních práv dotčených osob

Nová pravidla rovněž zavedou podmínky a záruky, jejichž cílem bude zajistit základní plně chráněná práva, včetně záruk týkajících se práva na ochranu soukromí a osobních údajů subjektů žádostí a zajištění účinných opravných

[147] Frequently Asked Questions: New EU rules to obtain electronic evidence. *European Commission* [online]. Brussels, 2018 [cit. 2022-08-30]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
[148] odst. 41, 47, 48, 49, 51, 52 a 53 návrhu Nařízení
[149] Čl. 13 návrhu Nařízení
[150] Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji. *Evropská rada a Rada Evropské unie: Tisková zpráva* [online]. 7.12.2018 [cit. 2022-08-30]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

prostředků.[151] Fyzické osoby budou o tom, že jejich údaje byly vyžádány, informovány a zároveň budou informovány o svých právech.

Bude platit také to, že vyžádané údaje bude možné použít pouze pro účely, pro něž byly získány, s výjimkou využití k zabránění bezprostřednímu a závažnému ohrožení veřejné bezpečnosti vydávajícího členského státu nebo jeho základních zájmů, nebo pro účely řízení, pro něž mohl být vydán předávací příkaz. Prvkem, který je také předmětem momentálních diskusí, je vytvoření systému oznamování pro údaje o obsahu v případech, kdy se vydávající orgán domnívá, že osoba, o jejíž údaje je žádáno, nepobývá na jeho území. Účelem tohoto oznámení je informovat vykonávající stát a poskytnout mu možnost, aby sdělil, zda jsou dané údaje: chráněny imunitami a výsadami; nebo podléhají pravidlům pro vymezení a omezení trestní odpovědnosti vztahujícím se ke svobodě tisku a svobodě projevu; nebo zda by jejich sdělení mohlo mít vliv na základní zájmy daného státu. Vydávající orgán tyto okolnosti zohlední a příkaz nevydá nebo jej upraví. Oznámení nemá odkladný účinek.[152]

Nutnost k přijetí nového návrhu Nařízení ale i pozitivní kritiku vyjádřili někteří představitelé justice EU. Například tehdejší rumunský ministr spravedlnosti pan Tudorel Toader prohlásil v roce 2019 následující:

„Jedná se o důležitý krok na cestě k efektivnějšímu a rychlejšímu přístupu k důkazům v trestním řízení. Jmenování právních zástupců bude představovat klíčový prvek pro usnadňování spolupráce při shromažďování elektronických důkazů. Naším cílem je zajistit, aby nový mechanismus fungoval efektivně, ale aby zároveň nepředstavoval nepřiměřenou zátěž, zejména pro malé a střední podniky. Je mi líto, že Parlament nebude připraven zahájit jednání, avšak doufám, že bude možné pokračovat v práci hned po zvolení nového Parlamentu“.[153]

---

[151] Čl. 12 návrhu Nařízení

[152] Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji. *Evropská rada a Rada Evropské unie: Tisková zpráva* [online]. 7.12.2018 [cit. 2022-08-30]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

[153] TOADER, Tudorel. *Balíček týkající se elektronických důkazů: Rada se dohodla na svém postoji ohledně pravidel pro jmenování právních zástupců za účelem shromažďování důkazů* [online]. In: 2019, 8.3 [cit. 2022-08-31]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/

Josef Moser, rakouský ministr spravedlnosti v roce 2018 na podporu přijetí nových pravidel pronesl:

„Elektronické důkazy se stávají zásadní složkou trestního řízení. Pachatelé trestné činnosti v současnosti používají rychlé, špičkové komunikační technologie, které překračují hranice. Na základě uvedených nových pravidel budou stávající zdlouhavé metody nahrazeny rychlými a efektivními nástroji pro přeshraniční shromažďování a výměnu elektronických důkazů. Naši občané tak budou lépe chráněni, a to, aniž by byla omezena jejich práva a svobody.“[154]

Ana Birchallová, rumunská vicepremiérka a prozatímní ministryně spravedlnosti v roce 2019 uvedla:

„Pachatele trestných činů evropské hranice nezastaví. V dnešní době mohou svou nezákonnou činnost organizovat za použití rychlých a moderních technologií, jejichž prostřednictvím po sobě poté i vymažou stopy. Velké množství údajů potřebných ke sledování těchto pachatelů je uloženo v USA nebo je mají v držení americké společnosti. Dohoda mezi EU a USA o urychlení přístupu našich donucovacích orgánů k elektronickým důkazům má tudíž zásadní význam. Evropa bude díky ní bezpečnější, avšak zároveň musí být dohodou zajištěna i ochrana osobních údajů, soukromí a procesních práv našich občanů.“[155]

5.4. Studie Centra pro evropská politická studia

Centrum pro evropská politická studia (dále jen CEPS)[156] zpracovalo odbornou analýzu k návrhu Nařízení, která vyzdvihuje 3 hlavní důvody pro jeho přijetí. Patří mezi ně následující. Prvním důvodem je potřeba k získání údajů, ke

---

[154] MOSER, Josef. *Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji* [online]. In: 2018, 7.12 [cit. 2022-08-31]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

[155] BIRCHALLOVÁ, Ana. *Rada udělila Komisi mandát k dojednání mezinárodních dohod týkajících se elektronických důkazů v trestních věcech* [online]. In: . 2019, 6.6 [cit. 2022-08-31]. Dostupné z: https://www.consilium.europa.eu/cs/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[156] Společnost CEPS je všeobecně uznávána jako nejzkušenější a nejvýznamnější autoritativní think tank, který dnes působí v EU. CEPS působí jako přední fórum pro diskuse o záležitostech EU, které se vyznačuje vlastní silnou výzkumnou kapacitou a schopností a doplňuje ji rozsáhlá síť partnerských institutů po celém světě. Více viz https://www.ceps.eu/about-ceps/

kterým je ztížený přístup. To se týká především některých kategorií údajů, konkrétně těch obsahových, ve smyslu obsahu elektronické komunikace. Momentální omezení přístupu k údajům se týká primárně poskytovatelů služeb v USA, kterým platná legislativa USA umožňuje poskytovat některé údaje veřejným orgánům cizích zemí, vyjma obsahových. Právní úprava žádostí o obsahové údaje zaslaným poskytovatelům služeb USA by se mohla změnit na základě amerického zákona CLOUD, pokud by příslušné zahraniční vlády uzavřely s USA prováděcí dohodu. Ta by v případě, že by tyto žádosti byly zasílány ze zahraničí, umožňovala jejich vykonání. Právě v souvislosti s touto konkrétní možností je potřeba zavedení dohody mezi EU a USA, která by tak byla pro poskytovatele služeb v USA přínosem nejenom v tom, že by jim bylo umožněno plnit své povinnosti vyplývající z návrhu úpravy elektronických důkazů, ale také pro to, aby mohly uvést v praxi možnosti, které nabízí zákon CLOUD.

Druhým důvodem je urychlení procesu přístupu k těmto datům. Zdlouhavost stávajících postupů při získávání elektronických údajů byla mnohokrát kritizována. Například sama Rada EU uvedla, že *„současné postupy vzájemné právní pomoci musí být rychlejší"*. Ze závěrů studie mimo jiné vyplynulo, že *"tradiční mechanismy justiční spolupráce jsou pomalé ve srovnání s rychlostí, kterou lze data přesouvat, měnit nebo mazat"*. Evropský sbor pro ochranu osobních údajů výstižně konstatoval, že *„OČTŘ čelí závodu s časem, aby získaly údaje potřebné pro vyšetřování"*.

Třetím důvodem je odstranění případných překážek v procesu přístupu. Možnost OČTŘ žádat o údaje přímo poskytovatele služeb (resp. jejich právní zástupce), a to i v přeshraničních případech, lze označit za určitý způsob "nezprostředkovaného přístupu". To znamená, že OČTŘ by nebyly nezávislé na zapojení orgánu, který zprostředkovává podanou žádost v druhém státě. V případě přijetí návrhu Nařízení by takový postup znamenal výrazné usnadnění procesu získávání údajů. Otázkou zůstává, zda má být v konečném důsledku

urychlení procesu pokusem o zefektivnění výkonnosti stávajících mechanismů, či se vydat cestou navržení jiných alternativních mechanismů k získání přístupu.[157]

Výše uvedená pozitiva a přínosy návrhu Nařízení s sebou zákonitě přinášejí určitá rizika a obavy, která vyplývají z jednotlivých článků návrhu Nařízení. Těch je ale zákonitě více než výše uvedených pozitiv. Tyto obavy jsou určitě na místě, když jedním z nejvíce diskutovaných témat je zásah do základních práv osob. Myslím, že kritika a doporučení na odstranění nedostatků by měla být vnímána pozitivně, jelikož mohou přispět k vyjasnění obsahu jednotlivých článků a upřesnění nejasností a doteď zavádějících definic.

6. Úskalí návrhu Nařízení

Z výše uvedených kapitol zcela jasně vyplývá, že iniciativa Komise na zřízení evropského právního rámce umožňujícího OČTŘ v EU přímé zasílání žádostí o elektronické důkazy poskytovatelům služeb v jiném členském státě EU, je třeba považovat jednoznačně za průlomové co do rychlosti obdržení požadovaných důkazů vedoucího k následnému úspěšnému vyřešení případu. Otázkou ovšem zůstává, zda budou tato data týkající se uživatelů (ať už budou obsahová, či neobsahová) dostatečně chráněna? Kdo bude příslušný příkazy vydávat? Budou poskytovatelé služeb schopni vyhodnotit správnost obsahu příkazu? A co když se následně zjistí, že vydání příkazu, jež byl vykonán, nebylo oprávněné? Další otázkou zůstává, jak dlouho by měla být data, k jejichž uchování byl příkaz vydán, uchovávána?

V souvislosti s výše uvedenými nedořešenými otázkami je Komise momentálně v pozici, kdy se snaží nalézt mimořádně křehkou rovnováhu mezi efektivním a účelným vyšetřováním trestných činů pro OČTŘ, právní jistotou pro poskytovatele služeb a ochranou základních práv podezřelých a dalších uživatelů.

---

[157] CARRERA, Sergio, Gloria GONZÁLEZ FUSTER, Elspeth GUILD a Valsamis MITSILEGAS. *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*. Brussels, 2015. ISBN SBN 978-94-6138-468-3. Dostupné také z: https://www.ceps.eu/cart/?add-to-cart=18574

6.1. Riziko zásahu do základních práv a svobod v souvislosti s nakládáním, předáváním a uchováváním údajů

Řešení návrhu nového Nařízení a způsob, jakým je formulován, může ovlivnit základní práva občanů, účastníků trestního řízení, a to zejména pokud je dopad nepříznivý. V případech, kdy hrozí nepříznivé dopady určitých navrhovaných řešení, by měly být předloženy návrhy na změny, které by mohly odstranit tyto nedostatky nebo je alespoň zmírnit. Proto níže uvádím hodnocení jednotlivých bodů, vyjádřenou nejen zúčastněnými stranami, organizacemi občanských sdružení zabývajících se základními osobními právy na půdě evropského práva, ale i právními odborníky, kteří ve svých studiích návrhu nového Nařízení vyjadřují nejen kritiku, ale navrhují i určitá řešení, resp. doporučení, která by nejasnosti vyplývající ze stále předběžného návrhu Nařízení, mohla odstranit.

Orgány pro ochranu údajů připomínají, že přístup OČTŘ k osobním údajům představuje zásah do práva na soukromí a ochranu údajů zaručených články 7[158] a 8[159] Listiny základních práv EU (dále jen Listina EU) a že výkon těchto práv a svobod lze omezit pouze tehdy, pokud je to nezbytné a pokud to skutečně odpovídá cílům obecného zájmu uznaným EU nebo potřebě chránit práva a svobody jiných osob.

6.1.1. Stanovisko Evropského sboru pro ochranu osobních údajů

Evropský sbor pro ochranu osobních údajů (dále jen Sbor)[160] ve svém stanovisku vydaném v roce 2019 podporuje snahu o zajištění účinných nástrojů pro vyšetřování a stíhání trestných činů, a zejména oceňuje cíl návrhů urychlit a usnadnit přístup k údajům v přeshraničních případech zefektivněním postupů v rámci EU. Zároveň ale zdůrazňuje, *„že jakákoli iniciativa v této oblasti musí plně*

---

[158] Čl. 7 návrhu Nařízení stanoví, že: Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace

[159] Čl. 8, odst. 1–3 návrhu Nařízení stanoví, že: Každý má právo na ochranu osobních údajů, které se ho týkají; Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu; Na dodržování těchto pravidel dohlíží nezávislý orgán.

[160] Sbor je nezávislý evropský subjekt, který přispívá k jednotnému uplatňování pravidel ochrany údajů v celé Evropské unii a prosazuje spolupráci mezi úřady pro ochranu osobních údajů v EU. Sbor je složen ze zástupců vnitrostátních úřadů pro ochranu údajů a evropského inspektora ochrany údajů (EIOÚ). Více viz. https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_cs

respektovat Listinu EU a rámec EU pro ochranu údajů a zajistit existenci všech nezbytných záruk“. V souvislosti s účinnou ochranou základních práv v procesu přeshraničního shromažďování elektronických důkazů vyžaduje větší zapojení soudních orgánů ve vykonávajícím členském státě. Ty by měly být do tohoto procesu systematicky zapojeny co nejdříve z důvodu možnosti přezkoumání souladu příkazů s Listinou. V souvislosti s tím by měly mít povinnost na tomto základě uvádět důvody pro odmítnutí vykonání příkazu.[161] Mimoto navrhuje vyjasnění definice kategorií údajů a zajištění jejich souladu s ostatními definicemi v právu EU. Doporučuje rovněž přehodnotit rovnováhu mezi druhy trestných činů, pro které by mohly být vydávány EPP, a kategoriemi dotčených údajů s ohledem na příslušnou judikaturu Soudního dvora EU. Dále Sbor předkládá konkrétní doporučení týkajících se několika aspektů návrhů nového Nařízení, které vyžadují určité zlepšení. Jsou jimi například věrohodnost a důvěrnost příkazů a předávaných údajů, práva dotčených osob, právní zástupci, lhůty pro vykonání příkazů a možnost poskytovatelů služeb vznést námitku proti příkazům. V souvislosti s lhůtami se Sbor domnívá, že šestihodinová lhůta pro předložení údajů v naléhavých případech nemusí být vždy reálná, a doporučuje, aby tato lhůta byla spíše preferovaná než povinná.

6.2. Připomínky Stálého výboru expertů pro mezinárodní migraci, uprchlictví a trestní právo

Stálý výbor expertů pro mezinárodní migraci, uprchlictví a trestní právo (dále jen Meijersův Výbor)[162] konstatoval, že přístup návrhů se zásadně liší od všech stávajících nástrojů vzájemného uznávání. Mezi jeho obavy patří například, zda je Komisí navrhovaný "nový rozměr vzájemného uznávání" slučitelný s článkem 82 SFEU? Zda je volba nařízení oprávněná a zda by cílů nebylo lépe dosaženo prostřednictvím směrnice? Domnívám se, že doporučením užití Směrnice Meijersův Výbor sleduje vyhnutí se přímo použitelného Nařízení, které

[161] *Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters* [online]. 06.11.2019, s. 3. [cit. 2022-08-31]. Dostupné z: https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf

[162] Meijersův výbor je nezávislá skupina odborníků, která zkoumá a poskytuje poradenství v oblasti evropského trestního, migračního, uprchlického, soukromého, antidiskriminačního a ústavního práva. Více viz. https://www.commissie-meijers.nl/

je právně závazné a platí v celém rozsahu na všechny členské státy EU na rozdíl od Směrnice, jejíž způsob implementace do vnitrostátních zákonů je ponechán na uvážení členských státu. EU by neměla v souvislosti s novým nástrojem justiční spolupráce tak silné pravomoci. Co se týče pochybnosti o slučitelnosti s Ustanovením čl. 82 odst. 1, kterým je zajištěno vzájemné uznávání soudních rozhodnutí, která justiční orgán ve vydávajícím státě adresuje právnické osobě v jiném členském státě a jimiž jí dokonce ukládá povinnosti bez předchozího zásahu justičního orgánu v tomto jiném členském státě, může EPP či EUP v případě potřeby vést k zásahu justičního orgánu vykonávajícího státu za účelem výkonu rozhodnutí. Jelikož se návrh týká přeshraničních postupů, v nichž jsou vyžadována jednotná pravidla, není nutné nechávat členským státům prostor k provedení takových pravidel.

Další obavou Meijersova Výboru jsou opravné prostředky, resp. přezkumné řízení (Články 15 a 16 návrhu Nařízení) v případě rozporných povinností adresáta, podle něhož může soudce ve vydávajícím členském státě nakonec vykládat právní předpisy cizích zemí, aby posoudil, zda existuje rozpor s právními předpisy. Výbor důrazně doporučil vyjasnit pravidla týkající se toho, kde mohou jednotlivci vznášet své nároky v případě porušení jejich práv nebo procesních pravidel. Výbor v souvislosti s touto obavou navrhuje, aby zákonodárci zvážili možnost, že dotčené osoby tak budou moci učinit u soudu ve státě svého bydliště. Z důvodu svých pochybností adresoval Meijersův Výbor dokument Výboru LIBE s otázkou týkající se vztahu návrhu ke stávajícím nástrojům justiční spolupráce (vzájemná právní pomoc, EVP). Jelikož tyto nástroje již umožňují přeshraniční získávání a uchovávání elektronických důkazů, ptají se, zda je zavedení dalšího nástroje zapotřebí?[163] V souvislosti s tímto dotazem bych ráda připomněla fakta uvedená a odůvodněná na názorných příkladech již v kapitolách 2 a 3, že postupy současných nástrojů justiční spolupráce dobře fungují při standardním vyšetřování, ale pro získávání elektronických důkazů, kde hrozí jejich ztráta,

[163] Meijers Committee. *Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters* [online]. 18.7.2018 [cit. 2022-08-31]. Dostupné z: https://www.commissie-meijers.nl/wp-content/uploads/2021/09/CM1809_EN.pdf

vymazání, či přesunutí, je třeba zavedení nové právní úpravy, která by takovou spolupráci ještě více urychlila a zefektivnila.

6.3. Kritika Sítě pro evropská digitální práva

Své obavy v souvislosti s možnými negativními dopady navrhovaného nařízení na základní práva dotčených osob, vznesla organizace občanské společnosti Síť pro evropská digitální práva (European Digital Rights Network – dále jen EDRi)[164], když na svých stránkách v roce 2018 její hlavní poradce pro politické záležitosti Maryant Fernández Pérez pronesl, že *„Komise navrhuje nebezpečné „zkratky", které by vnitrostátním orgánům umožnily získávat údaje o osobách přímo od společností, čímž by se z těchto v podstatě staly soudní orgány. Stát má zákonnou povinnost respektovat a hájit základní práva lidí. Společnosti takové právní povinnosti nemají. Pokud jsou společnosti nuceny k předávání údajů občanů, jsou naše stávající práva ohrožena."*

Síť EDRi se obává, že v případě přijetí nového Nařízení by se poskytovatelé služeb dostaly na stejnou úroveň jako OČTŘ. Byly by zproštěny odpovědnosti v případech, kdy by v reakci na nezákonný nebo nesprávný příkaz údaje poskytly. V praxi by to znamenalo následující: Pokud by poskytovatel služeb vykonal neplatný příkaz (například z důvodu obavy ze sankcí z jeho neprovedení) a pokud by byla výjimka z oznamování uživateli použita k utajení tohoto příkazu, bude pro uživatele následně velmi obtížné svá práva bránit. Namísto zavedení nové právní úpravy v podobě EPP a EUP, navrhuje tato síť komplexní zlepšení a posílení stávajícího rámce justiční spolupráce založeného na smlouvách o vzájemné právní pomoci pro spolupráci se zeměmi mimo EU a v rámci členských států EU nadále využívat institut nástroje EVP. Domnívám se, že obavy z přiznaných práv poskytovatelům služeb, rovnajících se právům a povinnostem OČTŘ je přehnaná. Tato problematika by měla být vyřešena právě ustanovením právního zástupce na základě návrhu Směrnice. V čl. 3 odst. 1 a 2 je stanovena povinnost týkající se jmenování právního zástupce v Unii, která má být uložena poskytovatelům služeb, kteří poskytují služby v Unii. Čl. 1 odst. 1 Směrnice doslova stanoví pravidla

[164] Síť EDRi je kolektiv nevládních organizací, odborníků, advokátů a akademiků, jejichž cílem je hájit a prosazovat digitální práva v Evropě. Již téměř dvě desetiletí slouží jako páteř hnutí za digitální práva v Evropě. Více viz https://edri.org/about-us/who-we-are/

týkající se právního zastoupení určitých poskytovatelů služeb v Unii k přijímání, dodržování a vymáhání rozhodnutí a příkazů vydaných příslušnými orgány členských států za účelem shromažďování důkazů v trestním řízení a doslova v odst. 2 téhož článku stanoví, že členské státy nemohou poskytovatelům služeb, na něž se tato směrnice vztahuje pro účely stanovené v odstavci 1, ukládat další povinnosti navíc k povinnostem vyplývajícím z této směrnice. Dotyčný právní zástupce by měl vystupovat jako adresát vnitrostátních příkazů a rozhodnutí a příkazů a rozhodnutí podle právních nástrojů Unie přijatých v oblasti působnosti hlavy V kapitoly 4 SFEU za účelem shromažďování důkazů v trestních věcech. To zahrnuje nástroje, které umožňují přímé doručování příkazů poskytovateli služeb v přeshraničních situacích, i nástroje založené na justiční spolupráci mezi justičními orgány podle hlavy V kapitoly 4 SFEU.

6.4. Studie k návrhu Evropské komise o elektronických důkazech

Maciej Rogalski, profesor práv na právnické fakultě ve Varšavě v Polsku, k návrhu nového nařízení vypracoval studii, ve které se věnuje jednotlivým článkům a upozorňuje na jejich nedostatky, přičemž předkládá určité návrhy k jejich odstranění.

1) V souvislosti s čl. 2 (Definice), odst. 8 a 9, upozorňuje na nedostatečné označení pojmů přístupových a transakčních údajů a jejich interpretačním nejasnosti. Navrhuje, aby ustanovení těchto článků bylo upřesněno tím, že se odstraní jejich neustálé opakování, zejména pokud jde o činnosti spojené se zahájením činnosti užívání, čímž se rozumí užívání telekomunikačních služeb definovaných stejnými údaji, jako je datum a čas. Dále, toto upřesnění by mělo také zahrnovat specifikaci definice "přístupových údajů", kterými se rozumí "údaje spojené se zahájením a ukončením přístupu uživatele" v telekomunikačních systémech", zatímco "transakčními údaji" se rozumí údaje spojené s touto službou.
2) Další možný problém spatřuje ve vydávání samotných příkazů, resp. řeší otázku, který kompetentní orgán bude ony příkazy vydávat. Domnívá se,

že jediný orgán, který by měl mít možnost udělit souhlas s provedením příkazu, je soud jakožto nezávislý a samostatný orgán. V případě, že souhlas uděluje jiný orgán než soud, zejména státní zastupitelství, může být souhlas udělen pouze v případě, že nezávislost tohoto orgánu bude zajištěna. Ačkoliv lze ve státech EU důvodně předpokládat dostatečné zákonné záruky pro takovou nezávislost, nelze zcela pominout nebezpečí případných politických změn, které by ji mohly ohrožovat[165], což by mohlo mít nepříznivý vliv na právní postavení účastníků trestního řízení.

3) Doba uchovávání údajů, kterou bude upravovat ustanovení čl. 10 odst. 2 návrhu Nařízení, nestanoví jednoznačně, jak dlouho mohou být údaje uchovávány nebo po jaké době by měly být vymazány. Roginski správně uvažuje, že v praxi toto může znamenat nutnost uchovávání údajů po neurčitou dobu. To samozřejmě v případě takových citlivých osobních údajů vyvolává pochybnosti o tom, zda je to možné z hlediska ochrany práv účastníků trestního řízení. Roginski navrhuje, aby doba uchování údajů nepřesáhla 12 měsíců.[166]

Doporučení Roginskiho v souvislosti s bodem 1 a jeho návrhem na přesné označení pojmů přístupových a transakčních údajů je na místě, jelikož jasné informace o jednotlivých typech elektronických dat jsou zásadní z pohledu OČTŘ při vydávání EPP či EUP. Přesné označení požadovaných údajů snižuje riziko, že formulář EPP/EUP bude vrácen ke korekci či doplnění a zvyšují se tak šance na rychlé vykonání požadovaného příkazu, což logicky povede k rychlejšímu získání požadovaných údajů a následnému dopadení pachatele.

Návrh uvedený v bodě 2, kde Roginski doporučuje, aby soud – nebo jiný nezávislý samostatný orgán udělil souhlas s provedením příkazu, je pochopitelný a zcela na místě vzhledem k zásahu do osobních údajů. V této části bych odkázala

---

[165] LATA, Jan. *Role státního zastupitelství v právním státu* [online]. Právní prostor, 2018 [cit. 2022-08-30]. Dostupné z: https://www.pravniprostor.cz/clanky/trestni-pravo/role-statniho-zastupitelstvi-v-pravnim-statu

[166] ROGALSKI, Maciej. The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes. *European Journal of Crime, Criminal Law and Criminal Justice* [online]. 16.12.2022, 333-253 [cit. 2022-08-31]. Dostupné z: blob:https://brill.com/ba92fc8c-c25d-43bf-be72-dcb0c21ed5b9

na články Úmluvy o počítačové kriminalitě, které stanoví, … *„aby bylo možné čelit výzvám vyplývajícím z nestálosti počítačových dat, zahrnuje seznam opatření nejen vyšetřovací pravomoci* (čl. 18)*, ale také předběžná opatření zaměřená na uchování elektronických důkazů* (čl. 16 a 17)*. Tyto pravomoci podléhají podmínkám a zárukám, které vyvažují požadavky na prosazování práva a ochranu lidských práv* (čl. 15 odst. 1) *a zahrnují mimo jiné soudní nebo jiný nezávislý dohled, důvody opravňující použití, a omezení rozsahu a trvání takové pravomoci nebo postupu".* Tedy z výše uvedeného vyplývá, že souhlas s provedením příkazu přísluší jedině soudnímu, příp. jinému nezávislému justičnímu orgánu.

S přesným ustanovením doby v bodě 3 pro uchování údajů do 12 měsíců ale nemohu souhlasit. Obsah požadovaných údajů se zpravidla týká počítačové trestné činnosti, která ohrožuje především nás uživatele, a proto by měla být doba uchování údajů stanovena tak dlouho, jak by OČTŘ potřebovaly. V daném případě se jeví jako možné měřítko doby, po kterou musí být údaje uchovány, promlčecí doba trestných činů, jejichž horní hranice trestní sazby je tři roky. Vedle toho by samozřejmě doba pro uchování údajů měla být stanovena na základě důkladného odůvodnění konkrétního případu. Proto bych spíše navrhovala v této oblasti určitou flexibilitu pro dosažení požadovaných výsledků, které jsou v konečném důsledku prioritou návrhu Nařízení.

6.5. Stanovisko Rady evropských advokátních komor a právnických společností k návrhu nařízení Komise o evropských příkazech k předání a uchování elektronických důkazů v trestních věcech

Rada evropských advokátních komor a právnických společností (dále jen CCBE)[167] v říjnu 2018 vydala stanovisko, v němž Komisi navrhuje doporučení k odstranění nejasností a nedostatků návrhu Nařízení. Stejně jako M. Rogalski spatřuje nedostatky v nejasné úpravě přístupových a údajů o účastnících. Konstatuje, že neexistuje žádné řádné odůvodnění, proč EPP vydaný k získání přístupových a údajů o účastnících, obecně nevyžaduje schválení soudu. Je třeba

[167] CCBE byla založena v roce 1960 a je mezinárodním neziskovým sdružením, které od svého vzniku stojí v čele prosazování zájmů evropských právníků a obhajuje právní principy, na nichž jsou založeny demokracie a právní stát. Více viz https://www.ccbe.eu/about/who-we-are/

přesněji stanovit, jaký typ údajů spadá do třídy "údajů o účastnících nebo přístupových údajů", aby se zabránilo zajištění informací, které by za normálních okolností vyžadovaly nezávislý soudní dohled v souladu s vnitrostátními pravidly, postupy vzájemné právní pomoci nebo EVP.

6.6. Forma notifikační procedury a návrh řešení

V tomto případě se jedná o dohodnutí se na podobě oznamovací povinnosti, **tzv. notifikační procedury**, a jejího rozsahu, v jakém budou informovány osoby, a jaké tato bude mít následky. Například, zda bude nutná notifikace pro všechny typy příkazů, a zda bude možné výkon příkazu odmítnout. Další otázkou, která zůstává spornou, je tzv. kritérium pobytu osoby, jejíž údaje jsou požadovány, a informování osob, které jsou příkazem přímo dotčeny. V této věci se postoj Parlamentu a Rady liší.

Parlament se domnívá, že osoba, které se příkaz přímo týká, by měla být o příkazu informována bez zbytečného odkladu, a že notifikace mohou být odepřeny pouze na základě individuální a řádně odůvodněné žádosti orgánů. Parlament se shoduje s Radou na závěru, že není třeba vyžadovat notifikace, v případě příkazů týkajících se pouze uchování údajů. Na druhou stranu, v případě příkazů vydaných za účelem získání těch nejcitlivějších údajů, by měl notifikační systém mít dvě hlavní charakteristiky: i) měl by být shodný pro transakční i obsahové údaje a ii) měl by být nezávislý na místě pobytu osoby, jejíž údaje jsou požadovány. Problematika oznamovací povinnosti je stále ve fázi nalezení kompromisu mezi Parlamentem a Radou.

Návrh řešení problematiky formy notifikační procedury

Domnívám se, že dotčené osoby by měly být informovány jedině až po pravomocném skončení věci, a to z toho důvodu, aby žádným způsobem nemohlo být ohroženo vyšetřování případů. Současně jsem toho názoru, že obsah elektronických důkazů se nápadně podobá obsahu telekomunikačního provozu, a proto bych v tomto případě jako možné řešení této sporné otázky, navrhovala řídit se ustanovením § 88 odst. TŘ týkajícího se odposlechu a záznamu telekomunikačního provozu, konkrétně odst. 8. Ten stanoví, že: *Státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena,*

a v řízení před soudem předseda senátu soudu prvého stupně po pravomocném skončení věci, informuje o nařízeném odposlechu a záznamu telekomunikačního provozu osobu uvedenou v odstavci 2, pokud je známa. Informace obsahuje označení soudu, který vydal příkaz k odposlechu a záznamu telekomunikačního provozu, délku trvání odposlechu a datum jeho ukončení. Jako přiléhavá se jeví myšlenka, aby dotčená osoba měla právo podat žádost o přezkum pro ověření, zda byly splněny všechny právní podmínky. Tím opět navazuji na stejný výše uvedený odstavec téhož paragrafu, který stanoví, že dotčená osoba má *právo podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu.* V případě, že se během kontroly prokáže opak, měla by být dotčené osobě přiznána náhrada v podobě finančního odškodnění.

6.7. Judikatura Soudního dvora EU ve vztahu ke kategoriím údajů a porušování základních práv

V souvislosti s transakčními a obsahovými údaji odst. 30 návrhu Nařízení stanoví, že: „s ohledem na citlivější charakter údajů o transakcích a obsahu vyžaduje vydání nebo potvrzení EPP k předání těchto kategorií údajů přezkum soudcem. Protože údaje o účastníkovi a přístupu jsou méně citlivé, mohou EPP pro jejich sdělení vydávat nebo potvrzovat také příslušní státní zástupci. V návaznosti na výše uvedené, odst. 31 návrhu Nařízení uvádí, že *„… příkazy k předání/uchování údajů o účastníkovi a údajů o přístupu lze vydat v souvislosti s jakýmkoli trestným činem, zatímco na přístup k údajům o transakcích a obsahu by se měly vztahovat přísnější požadavky, které odrážejí citlivější povahu takových údajů“.* Právě tvrzení, že údaje o účastníkovi a přístupu jsou méně citlivé než transakční údaje, je kriticky vnímáno sítí EDRi z hlediska možnosti porušení základních práv, respektive osobních údajů. Posouzení předpokládaného stupně citlivosti u různých kategorií údajů, které Rada provedla, může být matoucí a není v souladu s judikaturou nejvyšších evropských soudů.

Pro příklad zde uvádím případ Tele2/Watson[168], kde klíčovou otázkou bylo, zda jsou právní předpisy Švédska a Spojeného království, které ukládají poskytovatelům veřejných komunikačních služeb povinnost uchovávat provozní a lokalizační údaje, slučitelné s právem EU. Právní předpisy Spojeného království vyžadovaly, aby veřejní poskytovatelé služeb uchovávali všechny tyto komunikační údaje po dobu maximálně 12 měsíců, pokud tak požaduje Ministerstvo zahraničí. V roce 2016 Soudní dvůr Evropské unie (dále jen SDEU) právě v souvislosti s problematikou citlivosti údajů o účastnících a přístupu v odst. 98 a 99 rozsudku uvedl, že: „… *přístupové a údaje o účastnících mohou umožnit velmi přesné závěry o soukromém životě osob, včetně jejich každodenních zvyklostí, trvalého nebo přechodného bydliště, každodenního pohybu, vykonávaných činností, sociálních vztahů a sociálního prostředí, což může částečně vytvořit profil dotčené osoby“.*

Soud také zdůraznil, že „*provozní údaje nejsou o nic méně citlivé než samotný obsah komunikace, a že zásah, který taková právní úprava představuje, je proto obzvláště závažný“.*

Dále odst. 100 stejného rozsudku uvádí, že: *„taková právní úprava je zásahem do základních práv zakotvených v článcích 7 a 8 Listiny, který se jeví jako rozsáhlý a musí být považován za zvlášť závažný. Okolnost, že k uchovávání údajů dochází bez vyrozumění uživatelů služeb elektronických komunikací, může v dotčených osobách vyvolávat dojem, že jejich soukromí je pod neustálým dohledem“.*

Z výše uvedeného rozsudku vidíme, že údaje o účastníkovi a přístupu nelze považovat za méně citlivé, než jsou transakční a obsahové údaje. Proto je momentální vypracovávání kompromisů v Radě opírajících se o myšlenku údajně více či méně citlivých údajů ve světle rozsudků evropských soudů minimálně nepřesné a vyžaduje jasnější pravidla.

[168] SDEU, Spojené věci C-203/15 a C-698/15, Tele2 a Watson, body 92-93. Více viz CURIA - List of results (europa.eu)

6.8. Jednostranný přeshraniční přístup k údajům poskytovatelů služeb v a mimo EU

Studie Výboru LIBE považuje za rizikový jednostranný přístup, který Komise ve svém návrhu sleduje. Má za to, že takový přístup představuje značná rizika pro zájmy EU, její členské státy a pro práva jejích občanů. Z důvodu předejití těmto rizikům proto navrhuje zavedení mnohostranného přístupu, který by stanovil jednotný rámec pro přeshraniční přístup k údajům poskytovatelů služeb, čímž by zajistil větší právní jistotu ve vztahu ke třetím zemím. Mezinárodní vztahy jsou založeny na zásadách svrchované rovnosti států[169]. Zavedením jednostranného režimu povinné spolupráce se zahraničními poskytovateli služeb, by EU a její členské státy musely přijmout podobné modely donucovací pravomoci uplatňované třetími zeměmi, čímž by umožnily přímý přístup k údajům uloženým a zpracovávaným v EU. Návrh Komise by navíc mohl zpochybnit námitky členských států proti jiným nástrojům extrateritoriálního vymáhání (soudní příkazy). Na druhou stranu může přímé přeshraniční vymáhání vyvolat protireakce, jako jsou blokační zákony, které by mohly vést k protichůdným právním povinnostem a roztříštěnosti internetu.[170] Obavy vyjádřené studií Výboru LIBE lze shrnout následovně: Přímý přeshraniční přístup k údajům poskytovatelů služeb může posílit tendence k jednostrannému přístupu a ohrozit tak účinné fungování stávajícího mnohostranného rámce mezinárodní spolupráce. Případné zapojení příslušných orgánů dotčeného státu může tyto potenciální účinky návrhu Komise zmírnit[171]. Výše uvedené však nemění nic na skutečnosti, že jednostranné přístupy s sebou nesou přirozené riziko narušení mezinárodní solidarity mezi státy v rámci mezinárodní spolupráce.

---

[169] Čl. 2 odst. 1 Charty Organizace spojených národů, vice viz https://www.osn.cz/wp-content/uploads/2015/03/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf

[170] BĄKOWSKI, Piotr a Sofija VORONOVA. Electronic evidence in criminal matters. *EU Legislation in Progress* [online]. 2021, 1.3.2021. s 34 – 35. [cit. 2022-08-30]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf

[171] Případ tzv. Descartes, kdy nizozemské orgány získaly přístup k údajům souvisejících s dětskou pornografií uložených na serverech se sídlem v USA a zkopírovaly je. Více viz. Cybercrime Convention Committee (T-CY). *Transborder access and jurisdiction: What are the options?* [online]. Strasbourg, 2012. s. 35 [cit. 2022-08-31]. Dostupné z: https://rm.coe.int/16802e79e8

7. Snahy o nalezení kompromisu

S ohledem na přínos a pozitiva nového Nařízení se nabízí otázka, proč stále nebylo nařízení přijato. Důsledkem toho, že doposud nebyl přijat návrh, jsou probíhající diskuse na půdě Evropské komise a výměny názorů ohledně jednotlivých problematických otázek, přičemž existují zcela rozdílné postoje Parlamentu a Rady, když se v souvislosti s uvedenými riziky snaží učinit určité kompromisy. Přístupy přijaté Radou na straně jedné a Parlamentem na straně druhé, se v klíčových aspektech výrazně liší. Kromě diskusí mezi Radou, Parlamentem a Komisí, dochází k politickým trialogům v rámci předsednictví, kdy jednotlivé předsedající členské státy se věnují projednávaným bodům a vyjadřují k nim svá stanoviska. Jednoznačnou výzvou při jednáních je nalezení rovnováhy mezi zajištěním účinného mechanismu pro získávání elektronických důkazů v trestních věcech a ochranou základních práv osob, jejichž údaje jsou vyhledávány, a to při plném zohlednění zásady vzájemné důvěry“[172].

K diskutovaným aspektům návrhu Nařízení uvádím ty nejzásadnější, na kterých se Parlament a Rada nemohou shodnout.

Dohodnutí se na **Formě notifikační procedury**, jejím rozsahu, v jakém budou informovány osoby, a jaké tato bude mít následky, je již zmíněno v kapitole 6.6 věnované případným rizikům nového Nařízení. **Rada i Parlament se ztotožňují** v zaručení práv osob, o jejichž údaje se žádá. Ovšem ve stanovení způsobu, jak toho dosáhnout, se ale liší v případě žádostí týkajících se **obsahových a transakčních údajů** (viz. Kapitola 1.4), kdy Rada zastává názor, že vykonávající stát by měl mít možnost vznést námitky související s existencí hmotněprávní a procesní imunity u konkrétních oprávněných osob, a v případě okolností vylučujících vznik trestní odpovědnosti.

Další tématem k diskusi je **platforma pro zasílání údajů** [173], kdy Rada předpokládá předávání osvědčení zabezpečeným způsobem, kdežto Parlament

[172] , Council of the European Union. *Regulation on European Production and Preservation Orders for electronic evidence: Directive on legal representatives for gathering evidence - Progress report* [online]. Brussels, 2022 [cit. 2022-08-31]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-9296-2022-INIT/en/pdf

[173] Čl. 8 odst. 2 návrhu Nařízení

upřednostňuje vytvoření zabezpečené platformy přímo určené pro předávání osvědčení a současně tak stanovila její povinné používání.

Co se týče **efektivního vymáhání příkazů**, tak kromě možnosti odmítnutí výkon rozhodnutí, se Rada s Parlamentem shodují na podání vysvětlení důvodu, proč poskytovatel služeb nevykonal příkaz ve stanovené lhůtě. Parlament také stanoví, že vykonávající stát musí informovat poskytovatele služeb, který je předmětem výkonu, o tom, že se může odvolat na důvody stanovené v článcích 8 a, 9 a 10[174]. Pokud se poskytovatel služeb odvolá na některý z těchto důvodů, vykonávající stát rozhodne, zda výkon příkazu nařídí, či nikoli.

V případě **mimořádných situací**[175] bylo dosaženo předběžné dohody o její definici a možnosti vydávat některé mimořádné příkazy bez předchozí validace, pokud to vnitrostátní právo v podobných situacích umožňuje. Co se týče lhůty pro vykonání příkazu právním zástupcem v naléhavých případech, Parlament požaduje lhůtu 16 hodin a Rada lhůtu 6 hodin. Jako kompromis se navrhuje lhůta 8 hodin.

Dalším bodem diskuse jsou právní zástupci, ale tato problematika je již zmíněna v samotném obsahu práce, především v kapitole 4.1.6 o návrhu Směrnice. Lze jen konstatovat, že v tomto bodě, se Rada s parlamentem výjimečně shodují.

O kolizi s právem třetího státu je již pojednáváno v bodě 3.1 a 4.1. Rada předpokládá, že pokud poskytovatel služeb oznámí kolizi s povinnostmi, které mu ukládá právo třetího státu, rozhoduje vydávající stát, zatímco Parlament toto rozhodnutí svěřuje vykonávajícímu státu. S cílem dosažení shody s Radou, parlament navrhuje buď celkové nezařazení ustanovení týkající se této problematiky, nebo jako řešení navrhuje, aby poskytovatel služeb, případně notifikovaný orgán informoval vydávající orgán o existenci kolize s právem třetího státu.

---

[174] Možnost poskytovatele služeb upozornit zejména na to, že příkaz je neúplný, že obsahuje zjevné chyby, že výkonu brání situace vyšší moci nebo, v případě příkazů týkajících se provozních nebo obsahových údajů, že příkaz je zjevně protiprávní nebo přesahuje účel příkazu.
[175] Čl. 2 odst. 15, čl. 4 odst. 5 návrhu Nařízení

8. Přístup České republiky k návrhu nového Nařízení

Stanovisko k návrhu Nařízení bylo z pověření Vlády České republiky (dále jen ČR) vydáno Parlamentním institutem Poslanecké sněmovny Parlamentu České republiky[176]. K návrhu se staví v zásadě pozitivně a v rámci jeho projednávání zaujímá konstruktivně kritický postoj s cílem zajištění slučitelnosti s relevantní unijní legislativou. Fakt, že návrh Nařízení zachovává možnosti použití stávajících nástrojů mezinárodní justiční spolupráce v trestních věcech, zejména EVP, považuje ČR za kladné. Jako negativní ale vnímá nedostatečnou propracovanost některých ustanovení týkajících se přezkumu kompatibility příkazu s dodržováním lidských práv subjektu dat, formy notifikační procedury, nejasného technického zabezpečení předávání příkazů i vyžádaných důkazů, ověřování identity zasílajícího orgánu a pravosti žádosti ze strany poskytovatelů služeb.

V zásadě jde o stejné body kritiky, které se ztotožňují s obsahem části výše uvedené kapitoly 6.

ČR bude při projednávání návrhu prosazovat, aby povinnosti a práva poskytovatelů služeb byly vyvážené a aby zřízení právního zástupce zbytečně nezatěžovalo administrativně ani finančně poskytovatele služeb. ČR zaujímá názor, že sankce za nedodržení transpozičních předpisů by měly být harmonizovány, aby nedocházelo k tomu, že bude výhodnější mít právního zástupce v jednom členském státě než v jiném.

Jaký dopad bude mít přijetí nového Nařízení na státní rozpočet zatím nelze v současné době určit, ale co se týče právního řádu ČR, vliv bude mít především na zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), zákon č. 127/2005 Sb., o elektronických komunikacích a zákon č. 480/2004 Sb., o některých službách informační společnosti.

[176] Parlamentní institut plní úkoly vědeckého, informačního a vzdělávacího střediska pro Poslaneckou sněmovnu, její orgány, poslance a Kancelář Poslanecké sněmovny, pro Senát, jeho orgány, senátory a Kancelář Senátu.

Návrh nového Nařízení je současně projednáván i ve Výboru pro evropské záležitosti Poslanecké sněmovny Parlamentu ČR[177], jelikož jeho úloha je zásadní při výkonu kontroly návrhů unijní legislativy. Návrh Nařízení i Směrnice jako takový podporuje, stejně tak jako stanovisko vlády ČR. Zavedení nových nástrojů mezinárodní justiční spolupráce v trestních věcech považuje za přínosné pro boj s počítačovou trestnou činností, a to především z důvodu rychlejšího a efektivnějšího přeshraničního získávání elektronických důkazů OČTŘ.[178]

[177] VEZ hraje klíčovou úlohu při výkonu parlamentní kontroly evropské agendy v Poslanecké sněmovně. Kontroluje činnost vlády v záležitostech EU při rozhodování v Radě EU a Evropské radě. V rámci své kompetence se vyjadřuje k vládním návrhům kandidátů na evropského komisaře, na soudce Soudního dvora Evropské unie a k nominacím do orgánů EIB a EBRD za ČR. Obligatorně projednává příslušnou kapitolu návrhu zákona o státním rozpočtu a státním závěrečném účtu týkající se příjmů z rozpočtu EU a odvodů do rozpočtu EU. Více viz https://www.psp.cz/sqw/hp.sqw?k=509

[178] EVA, Sochorová. *Zajištění přístupu k elektronickým důkazům: Předběžné stanovisko vlády* [online]. 2018 [cit. 2022-08-31]. Dostupné z: https://www.psp.cz/sqw/text/orig2.sqw?idd=150336

Závěr

Nárůst trestné činnosti v oblasti kyberprostoru je možné pozorovat již od samého počátku přechodu společnosti do digitální éry. V posledních dvou letech byl však přírůstek incidentů markantně vyšší než v letech předešlých. Ať už byl nárůst zapříčiněn virovou pandemií a s ní spojenými vládními nařízeními omezující pohyb obyvatel, či aktuálními válečnými konflikty, které se z velké části odehrávají i ve světě kybernetiky, stále stoupající digitalizaci všech oblastí života je nutné vnímat jako fakt. Tomu bohužel odpovídá i zvýšený počet hackerských útoků, a to nejen na systémy vládních organizací, zdravotnických zařízení, ale i na jednotlivce. Právě následky takových útoků, stejně tak jako další dopady případů počítačové kriminality tak poukázaly na nedostatky stávající právní úpravy, která by byla schopna včas reagovat na tuto oblast trestné činnosti a jejího prokazování prostřednictvím tzv. elektronických důkazů. Právě problematika elektronických důkazů, především navrhovaná právní úprava usnadňující přístup k nim, byla námětem této diplomové práce.

V návaznosti na výše uvedené bych ráda shrnula obsah své práce a zamyslela se nad splněním jejích cílů, které jsem si v úvodu stanovila. Vzhledem k tomu, že na úrovni EU momentálně neexistuje jednotný právní rámec dotčené oblasti, který by umožňoval nakládat s elektronickými důkazy včetně jejich případné výměny v rámci jednotného systému ve všech členských státech jednotným způsobem, bylo hlavním smyslem představení, rozbor, přínosy, ale i úskalí návrhu nového Nařízení o evropských příkazech k vydání a uchování elektronických důkazů spolu s návrhem Směrnice stanovující harmonizovaná pravidla pro ustanovení právních zástupců za účelem získávání důkazů v trestním řízení, jakožto nových nástrojů mezinárodní justiční spolupráce.

K vypracování práce jsem použila českou i zahraniční odbornou literaturu, mezinárodní, evropskou, a českou právní úpravu, stanoviska Evropské komise, Rady a Parlamentu, judikatury Soudního dvora EU, stejně tak jako řadu odborných článků, studií a rozborů zúčastněných stran, výborů, organizací občanských sdružení, ale i názorů a doporučení právních odborníků zabývajících se problematikou elektronických důkazů v evropském právu.

V první kapitole jsem obecně vymezila pojem elektronických důkazů z hlediska právní úpravy, porovnání jeho definice v trestních řádech různých členských států EU, jazykové terminologie a vymezila jsem důležitost pojmu v rámci návrhu nového Nařízení. V neposlední řadě jsem detailně popsala jednotlivé druhy elektronických důkazů, jelikož způsob, kterým dochází ke shromažďování informací, potažmo důkazů, je zásadní z hlediska vydání příkazu k jejich přístupu a uchování.

Následující kapitola popisovala stávající metody justiční spolupráce, které jsou pro získávání elektronických důkazů, kde hrozí jejich ztráta, vymazání, či přesunutí, neefektivní. Nevýhody postupů současné právní úpravy spočívající především ve zdlouhavosti vyřizování žádostí o přístupu k elektronickým důkazům, byly demonstrovány na jednotlivých příkladech. Ve čtvrté kapitole byla představena samotná právní úprava vyřizování žádostí de lege ferenda orgánů EU zvyšující efektivitu a rychlost přeshraničního získávání elektronických důkazů.

V kapitole páté byly zdůrazněny přínosy navrhované právní úpravy, mezi které patří především rychlost obdržení vyžádaných elektronických důkazů, jasná pravidla pro poskytovatele služeb i ochrana základních práv dotčených osob. Vedle pozitiv, která nové Nařízení bez pochyby nabízí, byla v šesté kapitole detailně představena i rizika, která s sebou nová právní úprava beze sporu přináší, a to především v podobě zásahu do základních osobních práv. Součástí této kapitoly jsou proto i doporučení a návrhy učiněné zúčastněnými stranami, právními odborníky a občanskoprávními sdruženími, kterými by bylo možné zmiňovaná rizika minimalizovat, či odstranit. Dle svých znalostí a zkušeností se k některým doporučením přikláním, či navrhuji řešení jiná.

Poslední kapitoly se věnovaly aktuálním, a v převážné většině odlišným postojům Rady a Parlamentu k jednotlivým článkům návrhu Nařízení, které jsou důsledkem toho, že doposud nebylo dosaženo kompromisu. Stručně, ale jasně bylo představeno stanovisko České republiky.

Co do hodnocení naplnění cílů bych ráda uvedla, že bylo poměrně těžké zkusit se uceleněji vyjádřit k tématu, které není odbornou literaturou zatím příliš

podrobně zpracováno, z důvodu jeho aktuálnosti a proměnlivosti. Přesto jsem se o to pokusila, se zaměřením na budoucí úpravu.

Závěrem bych ráda reagovala na jedno z ústředních úskalí, jímž je obava z možného porušení základních práv osob, a zda tato práva budou v případě přijetí návrhu Nařízení, dostatečně chráněna. Na jednu stranu jsou základní práva osob nedotknutelná, na druhé straně však stojí myšlenka, zda ochrana práv a právem chráněných zájmů jednotlivců před tak závažným druhem trestné činnosti, která je realizována za pomoci technických výdobytků současné doby, jako je internet a s ním související darknet, sociální sítě, aplikace atp. neodůvodňuje strpení minimálního zásahu do osobních práv jednotlivců. Teorie vzniku státu byla pojímána tak, že se členové společnosti dobrovolně vzdali části svých práv a svobod a delegovali je na nově vzniklou nadřazenou jednotku - na stát. Stát mu za toto vzdání se poskytl ochranu, protože kolektivní ochrana byla hlavním smyslem vzniku státu.[179] Je tedy otázkou, zda s ohledem na celosvětový vývoj kriminality a její narůstající tendenci v oblasti počítačové kriminality není na místě tuto myšlenku znovu oživit a následně více věnovat pozornost vytváření systému brzd a vyvážení, které by eliminovaly možné zneužití pravomocí účastníku zúčastněných na uchovávání a získávání údajů.

[179] HOBBES, Thomas. *Leviathan*. Oikoymenh, 2009. ISBN 978-80-7298-106-9.

SEZNAM POUŽITÝCH PRAMENŮ

Monografie:

JELÍNEK, Jiří. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018. ISBN 978-807-5022-875.

POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, 264 s. Beckova edice právo a hospodářství. ISBN SBN978-80-210-8073-7.

KALVODOVÁ, Věra a Milana HRUŠÁKOVÁ. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty*. Brno: Masarykova univerzita, 2015., s. 312. ISBN 978-80-210-8072-0.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, 522 s. CZ.NIC. ISBN SBN978-80-88168-15-7.

SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo*. Praha: C.H. Beck, 1995, 264 s. Beckova edice právo a hospodářství. ISBN 80-717-9009-5.

HERRNFELD, Hans-Holger, Dominik BRODOWSKI a Christoph BURCHARD. *European Public Prosecutor's Office: Article-by-Article Commentary*. München, Germany: Nomos/Hart, 2020, 704 s. ISBN 9781509947157.

DVOŘÁK, Vratislav a Martin KLOUBEK. *Základy operativně pátrací činnosti policie v definicích a schématech*. Praha: Policejní akademie České republiky v Praze, 2011. ISBN ISBN 978-80-7251-351-2.

HOBBES, Thomas. *Leviathan*. Oikoymenh, 2009. ISBN 978-80-7298-106-9.

Právní předpisy:

Zákon č.141/1961 Sb., trestní řád v posledním znění.

Zákon č.104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních v posledním znění.

Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech (Úř. věst. L 130, 1.5.2014, s. 1).

Návrh nařízení Evropského parlamentu a Rady (EU) o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech 2018/0108/COD.

Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví harmonizovaná pravidla pro jmenování právních zástupců za účelem shromažďování důkazů v trestním řízení 2018/0107(COD).

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) 2016/343 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 (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) 2016/1919 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).

Mezinárodní smlouvy:

Convention on Cybercrime. In: *Council of Europe* [online], 2001, 23.11.2001 [cit. 2022-05-29]. Dostupné z : https://rm.coe.int/1680081561.

Konsolidované znění Smlouvy o Evropské unii a Smlouvy o fungování Evropské unie 2012/C 326/01 (Úř. věstník C 326, 26/10/2012 S. 0001–0390). Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:12012E/TXT

Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské Unie ze dne 29. května 2000. (Úř. věstník 197, 12/07/2000 S. 0003 – 0023) Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:42000A0712(01)&from=CS

Úmluva Rady Evropy č. 108 ze dne 28. ledna 1981 o ochraně osob se zřetelem na automatizované zpracování osobních údajů. Dostupné také z: https://www.psp.cz/sqw/text/orig2.sqw?idd=150225

Charta Organizace spojených národů. Dostupné také z: https://www.osn.cz/wp-content/uploads/2015/03/charta-organizace-spojenych-narodu-a-statut-mezinarodniho-soudniho-dvora.pdf

Úmluva Organizace spojených národů proti nadnárodnímu organizovanému zločinu ze dne 15. listopadu 2000. Dostupné také z: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

Judikatura:

Rozsudek Soudního dvora EU, Tele2 Sverige AB proti Tomu Watsonovi,

ve věcech č. C-203/15 a C-698/15, ze dne 21. prosince 2016.

Elektronické zdroje:

BĄKOWSKI, Piotr a Sofija VORONOVA. Electronic evidence in criminal matters. *EU Legislation in Progress* [online]. 2021, 1.3.2021, 12 [cit. 2022-08-30]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf.

ELECTRONIC EVIDENCE IN CIVIL AND ADMINISTRATIVE PROCEEDINGS: Guidelines and explanatory memorandum [online]. F-67075 STRASBOURG Cedex: Council of Europe Publishing, 2019 [cit. 2022-08-30]. s. 6. *ISBN ISBN 978-92-871-8929-5. Dostupné z : https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5.*

Co je cloud ? *Azure* [online]. [cit. 2022-08-30]. Dostupné z : https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-the-cloud/.

Portál evropské e-justice. *Fiches Belges* [online]. [cit. 2022-08-30]. Dostupné z : https://e-justice.europa.eu/528/CS/fiches_belges?init=true.

Fiches Belges on electronic evidence. *European Judicial Network* [online]. [cit. 2022-08-30]. Dostupné z: https://www.ejn-crimjust.europa.eu/ejnupload/Evidence/FB_Eevidence_SP.pdf.

European Judicial Network : Fiche Belge on electronic evidence [online]. [cit. 2022-08-30]. Dostupné z: https://www.ejnforum.eu/cp/e-evidence-fiche/223/0.

Oxford Learner´s Dictionaries [online]. [cit. 2022-08-30]. Dostupné z : https://www.oxfordlearnersdictionaries.com/definition/american_english/proof_1.

What Is the Difference Between Proof and Evidence? *Law Corner* [online]. [cit. 2022-08-30]. Dostupné z : https://lawcorner.in/what-is-the-difference-between-proof-and-evidence/#_ftn1.

Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji. *Evropská rada a Rada Evropské unie : Tisková zpráva* [online]. 7.12.2018 [cit. 2022-08-30]. Dostupné z : https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

Co jsou metadata: Slovníček webových pojmů. *Mioweb* [online]. [cit. 2022-08-30]. Dostupné z: https://www.mioweb.cz/slovnicek/metadata/.

COMMISSION STAFF WORKING DOCUMENT: IMPACT ASSESSMENT. In: . Brussels, 2018. Dostupné také z : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN.

EUROMED DIGITAL EVIDENCE MANUAL: Practical Guide for Requesting Electronic Evidence from Service Providers [online]. 2018 [cit. 2022-08-30]. Dostupné z : https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/manual-on-digital-evidence%204-4-19.pdf.

Obecné nařízení o ochraně osobních údajů: Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, 2016. Dostupné také z : https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN.

European Public Prosecutor's Office: Mission and tasks. *European Union* [online]. [cit. 2022-08-30]. Dostupné z: https://www.eppo.europa.eu/en/mission-and-tasks.

Mutual legal assistance and extradition: Combating crime across borders. *European Commission* [online]. [cit. 2022-08-30]. Dostupné z : https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en.

Evropský vyšetřovací příkaz, vzájemná právní pomoc a společné vyšetřovací týmy. *Portál evropské e-Justice* [online]. [cit. 2022-08-30]. Dostupné z : https://e-justice.europa.eu/92/CS/european_investigation_order_mutual_legal_assistance_and_joint_investigation_teams.

Joint investigation teams. *Eurojust* [online]. [cit. 2022-08-30]. Dostupné z : https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/jits-network.

Convention on Cybercrime [online]. [cit. 2022-08-30]. Dostupné z : https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Frequently Asked Questions: New EU rules to obtain electronic evidence. *European Commission* [online]. Brussels, 2018 [cit. 2022-08-30]. Dostupné z : https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345.

Proposal for a COUNCIL DECISION: authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. *EUROPEAN COMMISSION* [online]. Brussels, 2021 [cit. 2022-08-30]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0718&from=EN#.

The Budapest Convention on Cybercrime: benefits and impact in practice [online]. Strasbourg: Cybercrime Convention Committee (T-CY), 2020, 45 [cit. 2022-08-30]. Dostupné z: T-CY (2020)16_BC_Benefits_rep_Prov_1.docx.

Convention on cybercrime: Protocol on xenophobia and racism [online]. 2015 [cit. 2022-08-30]. Dostupné z : https://edoc.coe.int/en/module/ec_addformat/download?cle=dc36f18a9a0a776671d4879cae69b551&k=06dc6305622ca0ca43992ae64c25b80f.

LATA, Jan. *Role státního zastupitelství v právním státu* [online]. Právní prostor, 2018 [cit. 2022-08-30]. Dostupné z : https://www.pravniprostor.cz/clanky/trestni-pravo/role-statniho-zastupitelstvi-v-pravnim-statu.

CARRERA, Sergio, Gloria GONZÁLEZ FUSTER, Elspeth GUILD a Valsamis MITSILEGAS. *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*. Brussels, 2015. ISBN SBN 978-94-6138-468-3. Dostupné také z : https://www.ceps.eu/cart/?add-to-cart=18574.

United States v. Microsoft Corporation [online]. 2018 [cit. 2022-08-30]. Dostupné z : https://www.oyez.org/cases/2017/17-2.

Summary Report of the public consultation on improving cross-border access to electronic evidence in criminal matters [online]. [cit. 2022-08-30]. Dostupné z : https://ec.europa.eu/info/sites/default/files/report_of_open_public_consultation_on_e_evidence_april2018.pdf.

CRIMINAL JUSTICE (MUTUAL ASSISTANCE) ACT 2008 [online]. 2008 [cit. 2022-08-30]. Dostupné z : https://www.irishstatutebook.ie/eli/2008/act/7/enacted/en/print.html.

18 U.S.C. § 2701: UNLAWFUL ACCESS TO STORED COMMUNICATIONS [online]. [cit. 2022-08-30]. Dostupné z : https://www.justice.gov/archives/jm/criminal-resource-manual-1061-unlawful-access-stored-communications-18-usc-2701.

SECURITY UNION: FACILITATING ACCESS TO ELECTRONIC EVIDENCE [online]. April 2018 [cit. 2022-08-30]. Dostupné z : https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf.

Interinstitutional File: 2018/0108(COD): Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters. s 1 -2. (In:Brussels, 17 May 2019. l. Dostupné také z: https://data.consilium.europa.eu/doc/document/ST-9365-2019-INIT/en/pdf.

Council of Europe. *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* [online]. Strasbourg, 61 [cit. 2022-09-01]. Dostupné z : https://rm.coe.int/1680a49c9d.

Cybercrime Convention Committee (T-CY). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* [online]. 2021 [cit. 2022-09-01]. Dostupné z : https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d#globalcontainer.

Council of Europe. *Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention* [online]. Strasbourg, 5.9.2019 [cit. 2022-09-01]. Dostupné z : https://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07.

Proposal for an authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence: EXPLANATORY MEMORANDUM. In : Brussels, 2021. Dostupné také z : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0718&from=EN#.

Council of Europe. *Future of the Convention* [online]. [cit. 2022-09-01]. Dostupné z : https://www.coe.int/en/web/cybercrime/future-of-the-convention.

Council of Europe. *Cybercrime Programme Office (C-PROC)* [online]. [cit. 2022-09-01]. Dostupné z : https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.

Council of Europe and European Union. *Global Action on Cybercrime Extended (GLACY)+* [online]. [cit. 2022-09-01]. Dostupné z : https://www.coe.int/en/web/cybercrime/glacyplus.

Council of Europe. *Octopus Project* [online]. [cit. 2022-09-02]. Dostupné z : https://www.coe.int/en/web/cybercrime/octopus-project.

Council of Europe and European Union. *Octopus Project* [online]. [cit. 2022-09-02]. Dostupné z: https://www.coe.int/en/web/cybercrime/cybersouth.

Council of Europe a European Union. *IPROCEEDS -2: Targeting crime proceeds on the internet and securing electronic evidence in South East Europe and Türkiye* [online]. [cit. 2022-09-02]. Dostupné z : https://www.coe.int/en/web/cybercrime/iproceeds-2.

Cybercrime Convention Committee (T-CY). *25th Plenary Meeting report* [online]. [cit. 2022-09-02]. Dostupné z : https://rm.coe.int/0900001680a49f74/.

O Europolu [online]. [cit. 2022-09-02]. Dostupné z : https://www.europol.europa.eu/about-europol:cs.

Partners & Collaboration: Fostering cooperation among law enforcement and other partners around the world [online]. [cit. 2022-09-02]. Dostupné z : https://www.europol.europa.eu/partners-collaboration.

EUROJUST. *European Union Agency for Criminal Justice Cooperation* [online]. [cit. 2022-09-02]. Dostupné z: https://www.eurojust.europa.eu/

Eurojust. EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION. *SIRIUS: preservation and data disclosure requests* [online]. [cit. 2022-09-02]. Dostupné z: https://www.eurojust.europa.eu/document/preservation-request-model-form

Eurojust. EUROPEAN UNION AGENCY FOR CRIMINAL JUSTICE COOPERATION. *Cybercrime* [online]. [cit. 2022-09-02]. Dostupné z : https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime

ŠTRASBURK. *Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech: DŮVODOVÁ ZPRÁVA*. In: 2018. Dostupné také z: https://eur-

lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0225&from=EN.

DASKAL, Jennifer. *Unpacking the CLOUD Act* [online]. 31.1.2019, 220-225 [cit. 2022-08-31]. Dostupné z: https://eucrim.eu/articles/unpacking-cloud-act/.

TOSZA, Stanislaw. All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order. *New Journal of European Criminal Law* [online]. 2020, 161-183 [cit. 2022-08-31]. Dostupné z: doi: https://doi.org/10.1177/2032284420919802.

Doporučení pro ROZHODNUTÍ RADY o zmocnění k zahájení jednání za účelem dosažení dohody mezi Evropskou unií a Spojenými státy americkými o přeshraničním přístupu k elektronickým důkazům pro justiční spolupráci v trestních věcech: DŮVODOVÁ ZPRÁVA. Brusel, 2019. Dostupné také z : https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52019PC0070&from=EN.

BĄKOWSKI, Piotr a Sofija VORONOVA. *EU Legislation in Progress: Electronic evidence in criminal matters* [online]. [cit. 2022-08-31]. Dostupné z : https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf.

TOADER, Tudorel. *Balíček týkající se elektronických důkazů: Rada se dohodla na svém postoji ohledně pravidel pro jmenování právních zástupců za účelem shromažďování důkazů* [online]. In : . 2019, 8.3 [cit. 2022-08-31]. Dostupné z : https://www.consilium.europa.eu/cs/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/.

MOSER, Josef. *Nařízení o přeshraničním přístupu k elektronickým důkazům: Rada se dohodla na svém postoji* [online]. In : 2018, 7.12 [cit. 2022-08-31]. Dostupné z : https://www.consilium.europa.eu/cs/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters [online]. 06.11.2019, 21 [cit. 2022-08-31]. Dostupné z : https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf.

Meijers Committee. *Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters* [online]. 18.7.2018 [cit. 2022-08-31]. Dostupné z : https://www.commissie-meijers.nl/wp-content/uploads/2021/09/CM1809_EN.pdf

ROGALSKI, Maciej. The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes. *European Journal of Crime, Criminal Law and Criminal Justice* [online]. 16.12.2022, 333-253 [cit. 2022-08-31]. Dostupné z : blob : https://brill.com/ba92fc8c-c25d-43bf-be72-dcb0c21ed5b9

Cybercrime Convention Committee (T-CY). *Transborder access and jurisdiction: What are the options?* [online]. Strasbourg, 2012. s. 35 [cit. 2022-08-31]. Dostupné z : https://rm.coe.int/16802e79e8

Council of the European Union. *Regulation on European Production and Preservation Orders for electronic evidence: Directive on legal representatives for gathering evidence - Progress report* [online]. Brussels, 2022 [cit. 2022-08-31]. Dostupné z : https://data.consilium.europa.eu/doc/document/ST-9296-2022-INIT/en/pdf

SEZNAM PŘÍLOH

ANNEX 1

PŘÍLOHA I

CERTIFIKÁT EVROPSKÉHO PŘEDÁVACÍHO PŘÍKAZU (EPOC) PRO PŘEDÁNÍ ELEKTRONICKÝCH DŮKAZŮ

Podle nařízení (EU)...[1] musí adresát certifikátu evropského předávacího příkazu (dále jen „EPOC“) provést certifikát EPOC a musí předat požadované údaje orgánu uvedenému v bodě i) oddílu G certifikátu EPOC. Nejsou-li údaje předány, musí adresát po obdržení certifikátu EPOC uchovat požadované údaje, ledaže mu informace v certifikátu EPOC neumožňují tyto údaje identifikovat. Uchovávání trvá až do předání údajů nebo až do té doby, kdy vydávající orgán nebo případně vymáhající orgán sdělí, že již není nutné údaje uchovávat a předat.

Adresát musí přijmout opatření nezbytná k zajištění důvěrnosti certifikátu EPOC a předaných nebo uchovaných údajů.

ODDÍL A:

Vydávající stát: ……

Pozn.: údaje o vydávajícím orgánu se uvádějí na konci (oddíly E a F)

Adresát:……

ODDÍL B: Lhůty

Požadované údaje musí být předány (zaškrtněte příslušné políčko a v případě potřeby vyplňte):

□ nejpozději do 10 dnů

□ nejpozději do 6 hodin v naléhavém případě, který představuje:

□ bezprostřední ohrožení života nebo tělesné integrity osoby. V případě potřeby odůvodněte: ……

□ bezprostřední ohrožení kritické infrastruktury definované v čl. 2 písm. a) směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

□ v jiné lhůtě (upřesněte): ……..…….. z důvodu:

□ bezprostředního nebezpečí, že požadované údaje budou smazány
□ jiných naléhavých vyšetřovacích opatření
□ blízkého data soudního jednání
□ vazby podezřelé/obviněné osoby
□ jiných důvodů: ……

ODDÍL C: Informace o uživateli

Vezměte na vědomí, že (zaškrtněte, je-li to relevantní):

□ adresát **nesmí informovat osobu**, jejíž údaje jsou prostřednictvím certifikátu EPOC žádány.

ODDÍL D: Elektronické důkazy, které mají být předány

i) Tento certifikát EPOC se týká (zaškrtněte příslušné políčko či políčka):

□ údajů o účastníkovi, k nimž patří mimo jiné:

□ jméno, bydliště, datum narození, kontaktní údaje (e-mailová adresa, telefonní číslo) a další relevantní informace týkající se totožnosti uživatele/účastníka

□ datum a čas první registrace, typ registrace, kopie smlouvy, způsob ověření totožnosti během registrace, kopie dokumentů předložených účastníkem

□ typ služby, včetně identifikátoru (telefonní číslo, IP adresa, číslo SIM karty, adresa MAC) a přidruženého (přidružených) zařízení

□ informace o profilu (uživatelské jméno, profilová fotografie)

□ údaje o potvrzení využívání služby, např. alternativní e-mailová adresa poskytnutá uživatelem/účastníkem

□ informace o debetní nebo kreditní kartě (poskytnuté uživatelem pro účely fakturace) včetně jiných platebních prostředků

□ kódy PUK

□ údajů o přístupu, k nimž patří mimo jiné:

□ záznamy/logy o připojení IP pro účely identifikace

□ údajů o transakcích:

□ údaje o provozu, k nimž patří mimo jiné:

a) u (mobilních) telefonů:

□ odchozí (A) a příchozí (B) identifikátory (telefonní číslo, IMSI, IMEI)

□ čas a trvání připojení

□ pokusy o volání

□ ID základnové stanice, včetně zeměpisných informací (souřadnice X/Y), v době začátku a ukončení spojení

□ použitý nositel / telefonní služba (např. UMTS, GPRS)

b) u internetu:

□ informace o směrování (zdrojová IP adresa, cílová IP adresa či adresy, číslo či čísla portu, prohlížeč, informace v záhlaví e-mailu, ID zprávy)

□ ID základnové stanice, včetně zeměpisných informací (souřadnice X/Y), v době začátku a ukončení spojení

□ objem dat

c) u hostingu:

□ soubory logů

□ tikety

□ historie nákupů

□ jiné údaje o transakcích, k nimž patří mimo jiné:

□ historie dobíjení zůstatku předplacené služby
□ seznam kontaktů

□ údajů o obsahu, k nimž patří mimo jiné:

□ výpis (webové) poštovní schránky
□ výpis on-line úložiště (data vygenerovaná uživatelem)
□ výpis stránek
□ log/záloha zpráv
□ výpis hlasových zpráv
□ obsah serveru
□ záloha zařízení

ii) Pro provedení certifikátu EPOC jsou vám poskytnuty tyto informace:

- IP adresa:……..
- Telefonní číslo:……..
- E-mailová adresa:……
- Číslo IMEI:……
- Adresa MAC:……
- Osoba (osoby), jejíž údaje jsou požadovány: ……..
- Název služby: ……
- Jiné: ……

iii) Případně požadované časové rozpětí, které má být předáno:

……

iv) Vezměte na vědomí, že (zaškrtněte, je-li to relevantní):

□ požadované údaje byly uchovány v souladu s dřívější žádostí o uchování, kterou vydal …… (uveďte orgán a případně datum předložení žádosti a referenční číslo) a předložil subjektu …… (uveďte poskytovatele služby / právního zástupce / veřejný orgán, jemuž byla žádost předložena, a případně referenční číslo přidělené adresátem)

v) Povaha a právní kvalifikace trestného činu (činů), v souvislosti s nímž je certifikát EPOC vydáván, a příslušná ustanovení zákona/zákoníku:

……

Tento certifikát EPOC se vydává pro údaje o transakcích a/nebo obsahu a týká se (zaškrtněte případně příslušné políčko či políčka):

□ trestného činu (činů) postihnutelného ve vydávajícím státě trestem odnětí svobody s horní hranicí sazby nejméně tří let;

□ následujících trestných činů, pokud jsou zcela nebo zčásti páchány pomocí informačního systému:

□ trestného činu (činů) definovaného v článcích 3, 4 a 5 rámcového rozhodnutí Rady 2001/413/SVV;

☐ trestného činu (činů) definovaného v článcích 3 až 7 směrnice Evropského parlamentu a Rady 2011/93/EU;

☐ trestného činu (činů) definovaného v článcích 3 až 8 směrnice Evropského parlamentu a Rady 2013/40/EU;

☐ trestných činů definovaných v článcích 3 až 12 a článku 14 směrnice Evropského parlamentu a Rady 2017/541/EU.

vi) Vezměte na vědomí, že (zaškrtněte, je-li to relevantní):

☐ Žádané údaje jsou uchovávány nebo zpracovávány jako součást infrastruktury poskytované poskytovatelem služeb společnosti nebo jinému subjektu mimo fyzických osob a tento certifikát EPOC je adresován poskytovateli služeb, jelikož vyšetřovací opatření adresovaná společnosti nebo subjektu nejsou vhodná, zejména proto, že by mohla ohrozit vyšetřování.

vii) Jakékoli další relevantní informace:

.....

ODDÍL E: Údaje o orgánu, který vydal certifikát EPOC

Druh orgánu, který vydal tento certifikát EPOC (zaškrtněte příslušné políčko):

□ soudce, soud nebo vyšetřující soudce

□ státní zástupce (u údajů o odběratelích a přístupu)

□ státní zástupce (u údajů o transakcích a obsahu) → vyplňte i oddíl (F)

□ jakýkoli jiný příslušný orgán definovaný vydávajícím státem → vyplňte i oddíl (F)

Údaje o vydávajícím orgánu a/nebo jeho zástupci, který osvědčuje, že obsah certifikátu EPOC je přesný a správný:

Název orgánu:.....

Jméno jeho zástupce:.....

Postavení
(titul/hodnost):.....

Č. spisu:.....

Adresa:.....

Tel. č.: (číslo země) (směrové číslo).....

Fax č.: (číslo země) (směrové číslo).....

E-mail:.....

Datum: .....

Úřední razítko (existuje-li) a podpis:.....

ODDÍL F: Údaje o orgánu, který potvrdil certifikát EPOC

Druh orgánu, který potvrdil tento certifikát EPOC (zaškrtněte příslušné políčko, je-li to relevantní):

- ☐ soudce, soud nebo vyšetřující soudce
- ☐ státní zástupce (u údajů o odběratelích a přístupu)

Údaje o potvrzujícím orgánu a/nebo jeho zástupci, který osvědčuje, že obsah certifikátu EPOC je přesný a správný:

Název orgánu:.....

Jméno jeho zástupce:.....

Postavení (titul/hodnost):.....

Č. spisu:.....

Adresa: .....

Tel. č.: (číslo země) (směrové číslo).....

Fax č.: (číslo země) (směrové číslo).....

E-mail:.....

Datum:.....

Úřední razítko (existuje-li) a podpis:.....

ODDÍL G: Předání údajů a kontaktní údaje

i) Orgán, jemuž se údaje předávají (v případě potřeby zaškrtněte a vyplňte):

- ☐ vydávající orgán,
- ☐ potvrzující orgán
- ☐ jiný příslušný orgán definovaný vydávajícím státem:.....

ii) Orgán / kontaktní místo, které lze kontaktovat v případě dotazů týkajících se provádění certifikátu EPOC:.....

ANNEX 2

PŘÍLOHA II

CERTIFIKÁT EVROPSKÉHO UCHOVÁVACÍHO PŘÍKAZU (EPOC-PR) PRO UCHOVÁNÍ ELEKTRONICKÝCH DŮKAZŮ

Podle nařízení (EU)..[2]. musí adresát certifikátu evropského uchovávacího příkazu (dále jen „EPOC-PR“) bez zbytečného odkladu uchovat po obdržení certifikátu EPOC-PR požadované údaje. Uchování skončí po 60 dnech, pokud vydávající orgán nepotvrdí, že byla podána následná žádost o předání. Potvrdí-li vydávající orgán v této lhůtě 60 dnů, že následná žádost o předání byla podána, musí adresát uchovat údaje tak dlouho, jak to bude nutné k předání údajů, jakmile je následná žádost o předání doručena.

Adresát musí přijmout opatření nezbytná k zajištění **důvěrnosti** certifikátu EPOC-PR a uchovaných nebo předaných údajů.

ODDÍL A:

Vydávající stát: .....

Pozn.: údaje o vydávajícím orgánu se uvádějí na konci (oddíly D a E)

Adresát:.....

ODDÍL B: Informace o uživateli

Vezměte na vědomí, že (zaškrtněte, je-li to relevantní):

□ adresát **nesmí informovat osobu**, jejíž údaje jsou prostřednictvím certifikátu EPOC-PR žádány.

ODDÍL C: Elektronické důkazy, které mají být uchovány

i) Certifikát EPOC-PR se týká (zaškrtněte příslušné políčko či políčka):

□ údajů o účastníkovi, k nimž patří mimo jiné:

□ jméno, bydliště, datum narození, kontaktní údaje (e-mailová adresa, telefonní číslo) a další relevantní informace týkající se totožnosti uživatele/účastníka

□ datum a čas první registrace, typ registrace, kopie smlouvy, způsob ověření totožnosti během registrace, kopie dokumentů předložených účastníkem

□ typ služby, včetně identifikátoru (telefonní číslo, IP adresa, číslo SIM karty, adresa MAC) a přidruženého (přidružených) zařízení

□ informace o profilu (uživatelské jméno, profilová fotografie)

□ údaje o potvrzení využívání služby, např. alternativní e-mailová adresa poskytnutá uživatelem/účastníkem

□ informace o debetní nebo kreditní kartě (poskytnuté uživatelem pro účely fakturace) včetně jiných platebních prostředků

□ kódy PUK

☐ údajů o přístupu, k nimž patří mimo jiné:

- ☐ záznamy/logy o připojení IP pro účely identifikace

☐ údajů o transakcích:

- ☐ údaje o provozu, k nimž patří mimo jiné:

  a) u (mobilních) telefonů:

  - ☐ odchozí (A) a příchozí (B) identifikátory (telefonní číslo, IMSI, IMEI)
  - ☐ čas a trvání připojení
  - ☐ pokusy o volání
  - ☐ ID základnové stanice, včetně zeměpisných informací (souřadnice X/Y), v době začátku a ukončení spojení
  - ☐ použitý nositel / telefonní služba (např. UMTS, GPRS)

  b) u internetu:

  - ☐ informace o směrování (zdrojová IP adresa, cílová IP adresa či adresy, číslo či čísla portu, prohlížeč, informace v záhlaví e-mailu, ID zprávy)
  - ☐ ID základnové stanice, včetně zeměpisných informací (souřadnice X/Y), v době začátku a ukončení spojení
  - ☐ objem dat

  c) u hostingu:

  - ☐ soubory logů
  - ☐ tikety

- ☐ historie nákupů

- ☐ jiné údaje o transakcích, k nimž patří mimo jiné:

  - ☐ historie dobíjení zůstatku předplacené služby
  - ☐ seznam kontaktů

☐ údajů o obsahu, k nimž patří mimo jiné:

- ☐ výpis (webové) poštovní schránky
- ☐ výpis on-line úložiště (data vygenerovaná uživatelem)
- ☐ výpis stránek
- ☐ log/záloha zpráv
- ☐ výpis hlasových zpráv
- ☐ obsah serveru
- ☐ záloha zařízení

ii) Pro provedení certifikátu EPOC-PR jsou vám poskytnuty tyto informace:

- ☐ IP adresa:……..
- ☐ Telefonní číslo:…….
- ☐ E-mailová adresa:……...
- ☐ Číslo IMEI:…….
- ☐ Adresa MAC:……
- ☐ Osoba (osoby), jejíž údaje jsou požadovány:……..
- ☐ Název služby: ……
- ☐ Jiné: ……

iii) Případně požadované časové rozpětí, které má být uchováno:

……

iv) Povaha a právní kvalifikace trestného činu (činů), pro něž je certifikát EPOC-PR vydáván, a příslušná ustanovení zákona/zákoníku:

……

v) Jakékoli další relevantní informace:

……

ODDÍL D: Údaje o orgánu, který vydal certifikát EPOC-PR

Druh orgánu, který vydal tento certifikát EPOC-PR (zaškrtněte příslušné políčko):

- ☐ soudce, soud nebo vyšetřující soudce
- ☐ státní zástupce
- ☐ jakýkoli jiný příslušný orgán definovaný právem vydávajícího státu → vyplňte i oddíl (E)

Údaje o vydávajícím orgánu a/nebo jeho zástupci, který osvědčuje, že obsah certifikátu EPOC-PR je přesný a správný:

Název orgánu:……

Jméno jeho zástupce:……

Postavení (titul/hodnost):……

Č. spisu:……

Adresa:……

Tel. č.: (číslo země) (směrové číslo)……

Fax č.: (číslo země) (směrové číslo)……

E-mail:……

Datum: ……

Úřední razítko (existuje-li) a podpis:……

ODDÍL E: Údaje o orgánu, který potvrdilcertifikát EPOC-PR

Druh orgánu, který potvrdil tento certifikát EPOC-PR (zaškrtněte příslušné políčko):

- ☐ soudce, soud nebo vyšetřující soudce
- ☐ státní zástupce

Údaje o potvrzujícím orgánu a/nebo jeho zástupci, který osvědčuje, že obsah certifikátu EPOC-PR je přesný a správný:

Název orgánu:……

Jméno jeho zástupce:……

Postavení (titul/hodnost):.....

Č. spisu:.....

Adresa: .....

Tel. č.: (číslo země) (směrové číslo).....

Fax č.: (číslo země) (směrové číslo).....

E-mail:.....

Datum: .....

Úřední razítko (existuje-li) a podpis:.....

ODDÍL F: Kontaktní údaje

Orgán, který lze kontaktovat v případě dotazů týkajících se provádění certifikátu EPOC-PR:

.....