332—349

Elektronické důkazy jako výzva pro trestní proces

Václav Stupka* – Jan Provazník – Jakub Vostoupal*****

Abstrakt: Článek se věnuje problematice využití elektronických důkazů v rámci trestního řízení. Analyzuje aktuální právní úpravu procesních nástrojů v českém, evropském a mezinárodním právu a praxi využívání těchto procesních nástrojů českými orgány činnými v trestním řízení. Následně mapuje hlavní praktické, technické, teoretickoprávní a ústavněprávní výzvy, kterým aktuální teorie a praxe ve vztahu k tomuto typu důkazů čelí. Cílem článku je vyvolat odbornou diskusi k jednotlivým identifikovaným výzvám a vytvořit základ pro další výzkum.

Klíčová slova: elektronické důkazy, trestní řízení, využitelnost důkazu, důkazní síla, digitální forenzní věda, instrumenty mezinárodního práva, trestní proces, kriminalistika

Úvod

V rámci rozvoje takzvané informační společnosti realizuje stále větší množství lidí podstatnou část svého života v online prostředí a za využití informačních a komunikačních technologií, jejichž prostřednictvím komunikují s přáteli, rodinami, kolegy, se státními institucemi, sdílí a uchovávají informace, realizují ekonomické aktivity a podobně. Technologie rovněž do značné míry zajišťují chod naší společnosti a ekonomiky. Důsledkem vývoje je, že každý z nás produkuje stále větší množství digitálních stop. Proto je při dokazování stále častěji využíváno důkazů v elektronické formě, a to samozřejmě i v trestním řízení. Ačkoliv orgány činné v trestním řízení s elektronickými důkazy pracují již poměrně dlouhou dobu a využívají relativně efektivní postupy produkující kvalitní a zákonné důkazy, a přestože došlo v minulosti k mnoha legislativním i nelegislativním počinům upravujícím související procesní nástroje a jejich využití, lze stále identifikovat mnoho výzev, kterým praxe v souvislosti s využíváním elektronických důkazů v trestním řízení čelí. Cílem článku je tyto výzvy identifikovat a tím přispět k odborné i celospolečenské diskusi, která je poháněna snahou o nalezení obecného konsenzu o pravidlech práce s elektronickými důkazy.

* Mgr. Václav Stupka, Ph.D. Autor působí v Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a na Fakultě informatiky Masarykovy univerzity. Je rovněž členem expertních skupin zaměřených na kyberkriminalitu a elektronické důkazy při OSN, Europolu, Agentuře Evropské unie pro kyberbezpečnost a Ministerstva spravedlnosti ČR. E-mail: vaclav.stupka@law.muni.cz. ORCID: https://orcid.org/0000-0003-1458-1507. Tento článek vznikl v rámci projektu č. VJ01010084 *Elektronické důkazy v trestním řízení* realizovaného v programu Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019–2025 (IMPAKT-1). Článek je stanoviskem autorů a projektového týmu, nejde o oficiální stanoviska jimi reprezentovaných institucí ani Ministerstva vnitra ČR.

** JUDr. Jan Provazník, Ph.D. Autor je odborným asistentem na katedře trestního práva Právnické fakulty Masarykovy univerzity, odborným asistentem Centra vzdělávání, výzkumu v informačních a komunikačních technologiích Fakulty informatiky Masarykovy univerzity a asistentem místopředsedy Ústavního soudu České republiky. E-mail: jan.provaznik@law.muni.cz. ORCID: https://orcid.org/0000-0002-2253-8958.

*** Mgr. Jakub Vostoupal. Autor je doktorandem v Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a působí rovněž jako odborný pracovník Centra vzdělávání, výzkumu a inovací v informačních a komunikačních technologiích Fakulty informatiky Masarykovy univerzity. E-mail: jakub.vostoupal@law.muni.cz, ORCID: https://orcid.org/0000-0002-1669-9931.

1. Elektronické důkazy a nakládání s nimi

Důkazy mohou mít různé formy a jejich zákonná definice je velmi široká; pojem elektronické důkazy pak není jednoznačně definován vůbec. Ani odborná literatura či judikatura ať již v ČR nebo v zahraničí s ním nepracuje konsistentně. Obecně relativně přijímanou definici tohoto pojmu nabízí například projekt EU *Evidence*,[1] který za elektronické důkazy označuje *„[…] jakákoliv data, která jsou výstupem analogového nebo digitálního zařízení potenciální důkazní hodnoty, která jsou generována, zpracována, uchována, nebo přenášena jakýmkoliv elektronickým zařízením“*[2]. K pojmu elektronické důkazy tak můžeme přistupovat poměrně zeširoka a považovat za ně digitalizované fyzické nebo jiné tradiční důkazy (např. digitální záznam rozhovoru, digitální fotografie zbraně, analogové záznamy převedené do elektronického formátu apod.) a samozřejmě původně generovaná elektronická data bez ohledu na to, jaká zařízení jsou jejich zdrojem.[3]

Za zpracování elektronických důkazů pak můžeme považovat sběr, uchovávání, využívání a předávání důkazů; někdy je tento proces popisován jako *chain of custody* důkazů[4] v trestním řízení. Sběrem důkazů se rozumí sběr relevantních zařízení, úložišť a dat, které obsahují elektronické důkazy. To lze realizovat prostřednictvím mnoha procesních nástrojů včetně zajištění a ohledání věci, v rámci domovní prohlídky, v rámci sledování osob a věcí, ale rovněž může dojít k získání takových důkazů například od ISP nebo jiných správců systémů a dat, prostřednictvím různých mechanismů spolupráce se soukromým i veřejným sektorem a podobně. Ve chvíli, kdy dojde k zajištění důkazu, musí tento být uchován pro další použití v trestním řízení, kdy je nutné zajistit a zabezpečit integritu a původní podobu potenciálního důkazu[5]. Jakákoliv manipulace s důkazem nebo jeho zdrojem musí být prováděna tak, aby se předešlo znehodnocení důkazu nebo snížení jeho důvěryhodnosti a důkazní síly. Především by měl být důkazní materiál zpřístupněn jen oprávněným osobám, měla by být vedena evidence o manipulaci s ním a jakékoliv úkony by měly být prováděny vhodnými postupy a za využití vhodných nástrojů. Aby mohly být elektronické důkazy využity u soudu v rámci trestního řízení, je zpravidla nutné provést jejich analýzu. Ta je často prováděna znalcem, který vypracuje znalecký posudek bezprostředně využitelný u soudu. Elektronický důkaz a jeho zdroj je tak během svého životního cyklu často v držení nebo zpracováván prostřednictvím různých osob a dochází k jeho předávání. I v této fázi je nutné zajistit integritu důkazu. Je-li tedy důkazní materiál předáván (například mezi jednotlivými složkami policie, znalci, jinými subjekty či v rámci

---

1 Jde o výzkumný projekt financovaný z prostředků EU s názvem *European Informatics Data Exchange Framework for Court and Evidence*, který se komplexně věnoval problematice elektronických důkazů. Více informací viz online z: <http://www.evidenceproject.eu>.

2 Viz EVIDENCE PROJECT CONSORTIUM. *EVIDENCE Semantic Structure*. 2015, s. 7. Dostupné také z: <http://s.evidence-project.eu/p/e/v/evidence-ga-608185-d2-1-410.pdf>. Pojem data je zde chápán ve smyslu údaje – zahrnuje jak spojité signály generované analogovými zařízeními, tak diskrétní data generovaná technologiemi digitálními.

3 Pojem důkaz ve výčtech zde zmíněných pracujeme s pojmem důkaz v širším smyslu slova a zahrnujeme pod něj i prameny důkazu či důkazní prostředky.

4 Tento pojem je definován v různých zdrojích různě, kde v zásadě sledování nakládání s důkazy a související dokumentaci. Viz např. AYERS, Rick – BROTHERS, Sam – JANSEN, Wayne. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Guidelines on Mobile Device Forensics*. USA, 2014, 75 s. Dostupné také z: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>.

5 K problematice zajišťování integrity elektronického důkazu viz rovněž např. zde: AMIRIDU, Radka. *Zajištění integrity elektronického důkazu: technické a organizační prostředky*. Diplomová práce. Brno: Masarykova univerzita, 2021.

přeshraniční spolupráce), mělo by k tomu docházet technicky i právně správným způsobem, aby byla zachována využitelnost důkazu.[6]

Elektronické důkazy jsou v mnoha ohledech specifické, z čehož plynou požadavky na specifické postupy a techniky aplikované při jejich zpracování, na technické a personální kapacity orgánů činných v trestním řízení a na mechanismy zapojení dalších subjektů do celého procesu. Odlišnost od jiných druhů důkazů spočívá u elektronických důkazů zejména v jejich charakteru, konkrétně v dosažitelnosti, obsahu a integritě, informační hodnotě, skrytosti, časové trasovatelnosti, komplexnosti a replikovatelnosti.

Technologií, zařízení a formátů, které slouží k elektronickému zpracování informací, existuje obrovské množství. Jinak se přistupuje například ke SCADA systémům využívaným k řízení průmyslových celků,[7] jinak k mobilnímu telefonu a jinak k systémům postaveným na umělé inteligenci či kvantovém zpracování dat. Díky mimořádně dynamickému rozvoji ICT je navíc nutné počítat s dalším vývojem, kdy se mohou využívané nástroje, technologie i mechanismy jejich fungování fundamentálně měnit. To vše klade mimořádně vysoké nároky na orgány činné v trestním řízení – především z hlediska dostupnosti potřebného technického vybavení k vytěžování těchto technologií a z hlediska schopnosti všech osob zúčastněných na procesu dokazování pochopit jejich fungování a interpretovat získaný důkazní materiál. I samotné postupy vyšetřování a sběru důkazů musí často zohledňovat vazby mezi jednotlivými technologiemi. Jsou-li například v zajištěném mobilním zařízení uchována data v zašifrované podobě, mohou být dostupná rovněž v cloudovém úložišti, ke kterému může být přes poskytovatele služby snadnější přístup než k samotnému zařízení prostřednictvím nástrojů pro překonání šifry.

Velmi významnou roli pak hraje rovněž související vliv charakteru informačních sítí či kyberprostoru.[8] Celosvětové informační sítě umožňují zcela decentralizované a distribuované fungování služeb, které jsou často zneužívány a využívány pachateli trestné činnosti k nejrůznějším účelům (od komunikace po páchání kybernetické kriminality). Získávání důkazů z těchto služeb je však komplikované právě kvůli jejich distribuovanému charakteru. Sídlo provozovatele služby, bydliště pachatele, místo spáchání trestného činu, bydliště poškozených a místo, kde se nachází relevantní data a důkazy o příslušné trestné činnosti, se mohou nacházet v různých zemích a jurisdikcích. To způsobuje nejen potíže při určování příslušnosti orgánů činných v trestním řízení (dále také jako „OČTŘ"),[9] ale rovněž i při sběru důkazního materiálu, ke kterému musí být využíváno mechanismů mezinárodní policejní a justiční spolupráce, které jsou ve většině případů nedostatečně efektivní.[10]

---

6 V současné době však nejsou mechanismy zajištění integrity důkazu závazně stanoveny. V praxi se tedy vychází zejména z toho, co státní zástupce v přípravném řízení a soudce v soudním řízení akceptuje a považuje za adekvátní ochranu a zajištění integrity. Viz dále.

7 Jde o zkratku anglického pojmu *„supervisory control and data acquisition"*, což je počítačový systém schopný sběru a zpracování dat a uplatnění operativních pokynů na velké vzdálenosti. Tyto systémy se využívají v různých odvětvích průmyslu.

8 Informační sítě, respektive jimi tvořený kyberprostor není možné chápat jako pouhé médium, nýbrž jako prostředí, které neslouží jenom k přenosu informací, ale jako prostor pro kompletní realizaci informačních transakcí. Více k teorii informačních sítí viz např. POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 72.

9 Kybernetická kriminalita je například páchána zejména v podobě tzv. distančních deliktů (jiné místo spáchání a jiné místo následku). Zejména „majetková kybernetická kriminalita" je páchána tzv. sériově (§116 tr. z.), proto nelze hledět jen na příslušnost OČTŘ u jednotlivých skutků, ale zaměřit se i na zjištění totožných znaků spáchání (*modus operandi*), které mohou prokazovat sériovou trestnou činnost jednoho pachatele či jedné skupiny pachatelů.

10 Viz dále.

S charakterem informačních technologií souvisí i problematika významu poskytovatelů služeb. Ty Polčák označuje za definiční autority,[11] které vykonávají přímý vliv na informační sítě a uživatele informačních služeb, protože nastavují pravidla prostřednictvím technických limitů a podmínek poskytování svých služeb. Současně je často nutné elektronické důkazy získávat od definičních autorit nebo ve spolupráci s nimi, neboť mají technické prostředky k jejich získání nebo mají příslušná data přímo v držení na svých úložištích. V rámci důkazního řízení je tak ze strany orgánů činných v trestním řízení v mnoha případech nutné spolehnout se na součinnost či spolupráci s poskytovateli služeb, a to buďto napřímo, nebo prostřednictvím mezinárodní spolupráce.

2. Specifická právní úprava

Rozvoj využívání informačních a komunikačních technologií představuje pro trestní řízení a proces dokazování zjevnou výzvu. V některých případech jej komplikuje uplatnění zavedených postupů, v některých případech vyžaduje vytváření nových přístupů a postupů. Poměrně rigidní proces dokazování a jeho pravidla se na tyto výzvy snaží reagovat jak na národní, tak i na mezinárodní úrovni, zpravidla však z pochopitelných důvodů nepružně a pomalu.

Právní úprava trestního řízení je realizována na úrovni jednotlivých států, které vycházejí z různých právních kultur, tradic a právních mechanismů, může se proto napříč jurisdikcemi poměrně významně lišit. Na druhou stranu se národní legislativy často inspirují zahraničními přístupy či mezinárodními instrumenty nebo přímo mezinárodní instrumenty implementují – může jít o implementaci mezinárodních úmluv, komunitárního práva apod. Úprava trestního procesu v České republice je ovlivněna především jejím členstvím v Evropské unii a instrumenty uplatňovanými v evropské právní kultuře. Při popisu právní úpravy relevantní pro uplatnění elektronických důkazů je proto vhodné zohlednit tyto instrumenty.

Na mezinárodní ani evropské úrovni neexistuje žádný komplexní právní rámec věnovaný (elektronickému) dokazování. Sběr, uchovávání, užívání a předávání důkazů tak probíhá v souladu s národními právními úpravami trestního řízení, které byly mnohdy konstruovány před mnoha lety, před tím, než vznikl internet nebo technologie generující elektronické důkazy. To platí i pro Českou republiku, jejíž úprava, ačkoliv mnohokrát novelizovaná, pochází z šedesátých let minulého století.[12] Český trestní řád tak sice místy obsahuje specifická ustanovení zavádějící procesní nástroje k zajišťování některých druhů elektronických důkazů,[13] ve většině případů jsou však orgány činné v trestním řízení často odkázány na „ohýbání" tradičních procesních nástrojů pro potřeby dokazování těmito důkazy.[14] Podobně tomu je často i v jiných státech, což vede k poměrně zásadním rozdílům v přístupech, které způsobují problémy při přeshraničním nakládání s elektro-

11 Definičními autoritami mohou být nejrůznější poskytovatelé informačních služeb, kteří mají kompetenci přímo ovlivňovat pravidla chování v informačních sítích prostřednictvím kódu, respektive pravidel využívání jejich služeb. Více k problematice definičních autorit viz POLČÁK, Radim. *Internet a proměny práva*, s. 88 an.

12 Viz zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

13 Jde například o ust. § 7b trestního řádu o uchování a znepřístupnění dat, či § 88a trestního řádu o příkazu k zjištění údajů o telekomunikačním provozu.

14 Zajišťování dat uchovávaných v počítačových systémech je například zhusta realizováno jako operativně pátrací činnost sledování osob a věcí. Zde jde však o nástroj původně konstruovaný pro zcela jiné situace a procesní úkony. Viz dále.

nickými důkazy. I OSN ve své studii k problematice kyberkriminality konstatovala poměrně významné rozdíly v národních legislativách, a to i mezi státy s podobnou právní kulturou.[15] Mezinárodní a nadnárodní organizace se tak zaměřují především na harmonizaci národních právních úprav, budování mechanismů spolupráce a budování institucionální podpory.

V Česku jsou mechanismy nakládání s elektronickými důkazy ovlivněny dvěma hlavními mezinárodními právními režimy, a to právem EU a dalšími mezinárodněprávními instrumenty, především z pera Rady Evropy.

2.1 Mezinárodní právo

Patrně nejúspěšnější instrument mezinárodního práva trestního věnující se mimo jiné i problematice elektronických důkazů pochází z pera Rady Evropy. Jde o notoricky známou Úmluvu o kyberkriminalitě[16] z roku 2001, kterou ČR podepsala v roce 2005 a ratifikovala pak po dosažení plné harmonizace v roce 2013.[17] Úmluva je v podstatě hlavní a jedinou mezinárodní smlouvou,[18] která definuje konkrétní činy, které mají signatářské státy považovat za (kybernetickou) kriminalitu, a rovněž obsahuje procesní úpravu poskytující nástroje pro prevenci, detekci a stíhání těchto trestných činů. I když nemusí být elektronické důkazy nutně generovány jen pachateli kyberkriminality, je úmluva v podstatě klíčovým rámcem, který zefektivňuje vyšetřování kriminality, kde se pracuje s tímto druhem důkazů.

Ve vztahu k elektronickým důkazům úmluva vybavuje příslušné orgány procesními nástroji, formuluje pravidla pro určení jurisdikce a nastavuje mechanismy pro mezinárodní spolupráci. Ačkoliv se úmluva vyjadřuje k pravidlům pro určení jurisdikce, fakticky nejde o skutečnou delimitaci jurisdikce nebo založení nějaké procesní povinnosti, nýbrž pouze o uplatnění principů teritoriality a personality, kdy mají státy uplatňovat jurisdikci u trestných činů formulovaných v úmluvě, byly-li spáchány na jejich území nebo jejími občany. Úprava mezinárodní spolupráce v úmluvě směřuje na situace, kdy stát stíhající příslušnou trestnou činnost potřebuje přistupovat k elektronickým důkazům nacházejícím se v jiné jurisdikci. Ačkoliv úmluva nevytváří nové mechanismy a spoléhá se na standardní nástroje mezinárodní justiční spolupráce v trestních věcech založené národními právními úpravami a multilaterálními či bilaterálními smlouvami a dohodami, snaží se orgány činné v trestním řízení vybavit sadou nástrojů umožňujících co nejširší a efektivní využití těchto nástrojů. Signatářské státy proto mají povinnost příslušným orgánům umožnit realizaci forem spolupráce konkrétně vyjmenovaných v článcích 29.–35., které upravují i konkrétní pravidla pro přeshraniční uchování dat, sdělování provozních dat, zajištění přístupu k obsahovým datům, jejich shromažďování a odposlech. Mechanismy

15 Srov. ORGANIZACE SPOJENÝCH NÁRODŮ – KANCELÁŘ PRO DROGY A KRIMINALITU. *Comprehensive Study on Cybercrime (draft)* [online]. Vídeň: OSN, 2013, s. 158 [cit. 2021-10-11]. Dostupné z: <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

16 Jde o Úmluvu Rady Evropy o kyberkriminalitě (CETS č. 185), známou rovněž jako Budapešťská úmluva. Dostupná online z: <https://rm.coe.int/1680081561> a český překlad z: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0>. Dále též jako „úmluva".

17 Viz Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě.

18 Není podepsaná jen státy Rady Evropy, ale i mnoha dalšími. Aktuálně má úmluva celkem 48 ratifikací a 2 podpisy bez ratifikace.

mezinárodní justiční spolupráce v trestních věcech jsou však obvykle limitovány zdlouhavými procedurami a ověřováním požadavků. V praxi se proto často před využitím tohoto nástroje uplatňuje vzájemná policejní spolupráce nebo jiný mechanismus výměny informací, často zprostředkovaný mezinárodními organizacemi, například Interpolem nebo Europolem. Tyto zdlouhavé procedury úmluva bohužel nijak neeliminuje, vytváří však síť nonstop dostupných kontaktních bodů, které by měly příslušné požadavky urychleně zpracovávat.

Vlastní procesní nástroje, které musí být na úrovni signatářských států implementovány, mají být využitelné pro vyšetřování trestných činů vyjmenovaných v úmluvě, ale i pro zajišťování jakýchkoliv elektronických důkazů o trestné činnosti.[19] Konkrétně pak úmluva signatářské státy zavazuje, aby se vybavily pro zajišťování elektronických důkazů procesními nástroji k urychlenému uchování uložených počítačových dat, urychlenému zachování a částečnému zpřístupnění provozních dat, vydání příkazu k předložení dat, realizaci prohlídky a zajištění uložených počítačových dat, shromažďování provozních dat v reálném čase a k odposlechu obsahových dat. Podobně jako některé jiné státy přistoupila ČR k tomuto závazku tak, že některé z požadavků splnila již dříve platnými procesními nástroji, které byly dostatečně obecně formulované a umožňovaly samostatně nebo v kombinaci s jinými procesními nástroji orgánům činným v trestním řízení získat přístup k příslušné kategorii důkazů, v některých případech bylo nutné pro zajištění souladu pro změnu provést potřebnou aktualizaci nebo rozšíření pravomocí.

Samotná Rada Evropy si je vědoma, že Úmluva o kyberkriminalitě, vytvořená v roce 2001, již v současné době zaslouží aktualizaci. Proto byla Výborem smluvních stran Úmluvy (T-CY) sestavena v roce 2017 pracovní skupina, která dostala za úkol vypracovat návrh dodatkového protokolu k úmluvě, který by reagoval na technologický a společenský vývoj a vybavil orgány signatářských států dodatečnými nástroji pro sběr a zpracování elektronických důkazů. Pracovní skupina na základě tohoto mandátu připravila návrh „Druhého dodatkového protokolu k Úmluvě o kyberkriminalitě o posílené spolupráci a zpřístupnění elektronických důkazů“,[20] který byl výborem T-CY schválen v květnu letošního roku. V současné chvíli je posuzován jednotlivými orgány Rady Evropy a měl by být formálně schválen a zpřístupněn k podepisování v první polovině roku 2022.[21]

Dodatkový protokol reaguje především na to, že standardní mechanismy mezinárodní justiční spolupráce v trestních věcech jsou v mnoha případech zdlouhavé, což vede k jejich neefektivitě a často i přetížení orgánů, které žádosti zpracovávají. Elektronické důkazy jsou volatilní a hrozí jejich znehodnocení, trvá-li z procesních důvodů jejich zajišťování příliš dlouho. Může totiž dojít k jejich smazání nebo změnění jejich uživateli, k jejich exspiraci a podobně. Dodatkový protokol proto vytváří nové nástroje, které jsou méně formální a pro specifické situace či kategorie důkazů zavádějí zrychlený proces jejich získávání a předávání. Nejčastěji získávané údaje od poskytovatelů informačních služeb jsou údaje k uživatelským účtům, respektive síťovým identifikátorům.[22] Pro tyto případy

19 Srov. článek 14. Úmluvy o kyberkriminalitě.

20 Dodatkový protokol je ve formě návrhu dostupný online z: <https://rm.coe.int/0900001680a2aa1c>. Dále též „návrh dodatkového protokolu“.

21 Tento termín je však podle názoru autorů poněkud optimistický vzhledem k tomu, jak rychlé jsou schvalovací procesy Rady Evropy a k tomu, že je dodatkový protokol i v současném znění obsahuje poněkud kontroverzní nástroje.

22 Např. údaje k doménám, IP adresám, emailům apod.

dodatkový protokol vytváří mechanismus přímé součinnosti, kdy příslušné orgány jednoho státu mohou žádat informace o doménách a uživatelích přímo od poskytovatelů služeb na území jiného signatářského státu. Došlo by tak k přemostění celého procesu žádání o mezinárodní spolupráci,[23] což by mohlo potenciálně vést ke zefektivnění především procesu trasování digitální stopy pachatelů trestné činnosti. Dodatkový protokol rovněž vytváří mechanismy posilující stávající mezinárodní spolupráci při získávání a předávání elektronických důkazů. Ty by měly urychlit získávání informací o uživatelích a provozních dat prostřednictvím nastavení lhůt pro poskytnutí této spolupráce ze strany dožadovaných států a získávání obsahových dat od poskytovatelů služeb a další spolupráce v naléhavých případech prostřednictvím využití sítě nonstop kontaktních bodů vytvořených v rámci úmluvy. V neposlední řadě dodatkový protokol počítá se zavedením nástrojů pro poskytování výpovědí prostřednictvím videokonferenčních nástrojů a zavádí mechanismy pro budování společných vyšetřovacích týmů.

Ačkoliv je návrh dodatkového protokolu díky komplikovanému procesu draftování v případě některých navrhovaných institutů poněkud vágní a není zatím jasné, zda je toto jeho finální podoba, kdy bude otevřen k podpisům a jak dlouho bude trvat implementace nových nástrojů, lze tuto iniciativu považovat jednoznačně za přínosný krok k posílení mezinárodní spolupráce při práci s elektronickými důkazy.

2.2 Evropské právo

Dalším zdrojem výrazného vlivu pro českou praxi práce s elektronickými důkazy je jednoznačně právo Evropské unie. Ačkoliv EU nemůže přijímat společnou unijní trestní legislativu, díky Lisabonské smlouvě[24] a v rámci navazujícího budování takzvaného Prostoru svobody, bezpečnosti a práva[25] může v rámci svých kompetencí budovat určité specifické právní nástroje aplikovatelné na úrovni členských států. Ve vztahu k elektronickým důkazům určitě není možné na úrovni EU hovořit o komplexním právním rámci. Existuje ale několik instrumentů a iniciativ, které jsou přímo nebo nepřímo relevantní pro nakládání s elektronickými důkazy v trestním řízení.

Dosavadním klíčovým legislativním počinem EU je v tomto směru Směrnice o Evropském vyšetřovacím příkazu[26] z roku 2014, která je účinná od roku 2017. Směrnice vytváří v zásadě nový komplexní systém umožňující členským státům získat v trestních věcech s přeshraničním prvkem důkazy z ostatních členských států. Evropský vyšetřovací příkaz[27] je konstruován na principu vzájemného uznávání a nahrazuje dosavadní nástroje

23 V návrhu dodatkového protokolu však stále existuje možnost zavést povinnosti notifikace takové žádosti odpovědným orgánům ve státě příslušného ISP.

24 Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství, podepsaná v Lisabonu dne 13. prosince 2007 (2007/C 306/01).

25 *The area of freedom, security and justice* (AFSJ) je souborem politik věnujících se otázkám spravedlnosti, které jsou navrženy za účelem zajištění bezpečnosti, práv a svobodného pohybu v rámci Evropské unie. Zahrnují především oblasti harmonizace soukromého mezinárodního práva, smlouvy o extradici mezi členskými státy, politiku ochrany vnitřních a vnějších hranic, společná cestovní víza, politiku imigrace a azylů a politiku justiční spolupráce. Více viz např. zde: <https://www.europarl.europa.eu/factsheets/en/sheet/150/an-area-of-freedom-security-and-justice-general-aspects>.

26 Viz Směrnice Evropského parlamentu a rady č. 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech. Dostupné online z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014L0041>. Dále též „směrnice".

27 Dále též EIO z anglického *European Investigation Order*.

– především evropský důkazní příkaz.[28] Konkrétně zde EU cílí především na zjednodušení a zrychlení přeshraničního vyšetřování trestných činů.

Evropský vyšetřovací příkaz je rozhodnutí justičního orgánu vydané či potvrzené justičním orgánem jednoho členského státu za účelem provedení jednoho nebo několika konkrétních vyšetřovacích úkonů v jiném členském státě s cílem získat důkazy v souladu s touto směrnicí. Vydaný příkaz je pak uznatelný na straně vykonávajícího členského státu a musí být tímto státem promptně vykonán. Lze jej navíc využít k realizaci téměř jakéhokoliv vyšetřovacího úkonu kromě sestavení a činností společného vyšetřovacího týmu.[29] Jednoznačnou výhodou tohoto nástroje nejen při zajišťování elektronických důkazů je, že jsou ve směrnici jasně nastaveny lhůty pro vykonání příslušných úkonů a omezeny důvody k odmítnutí uznání nebo výkonu příkazu. EIO má rovněž potenciál snížit administrativní zátěž celého procesu spolupráce, neboť je vydáván v podobě jednoho standardizovaného formuláře, jehož prostřednictvím se příslušným orgánům dostává pomoci při získávání důkazů. Vzniká tedy potenciál díky tomuto nástroji zrychlit a zefektivnit proces získávání důkazů ze zahraničí, přinejmenším ze států EU. Směrnice však neřeší některé potenciálně významné záležitosti. Není například nijak upraven způsob předávání a uchovávání důkazů, zde tedy budou nadále uplatňovány postupy běžné v jednotlivých členských státech, které se však mohou v podstatných rysech lišit.

Významný krok by mohlo představovat přijetí navrhovaného Nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech,[30] které má za cíl usnadnit zajištění a shromažďování elektronických důkazů pro trestní řízení uchovávaných nebo držených poskytovateli služeb v jiné jurisdikci v rámci EU. Vzhledem k tomu, že navrhovaný mechanismus je postaven na principu vzájemného uznávání a že by byly příkazy směřovány přímo poskytovatelům služeb, eliminovala by se tím stále relativně komplikovaná a zdlouhavá procedura realizovaná přes orgány vykonávajícího nebo dožádaného státu. Oba navrhované příkazy by mohly být adresovány přímo poskytovatelům služeb usídleným nebo poskytujícím služby na území EU a mohly by požadovat uchování elektronických důkazů, které mají příslušní poskytovatelé služeb v držení, respektive jejich následné vydání příslušným orgánům činným v trestním řízení. Adresáty příkazů by podle návrhu nařízení měli být „poskytovatelé služeb“, tedy poskytovatelé služeb elektronických komunikací, služeb informační společnosti a služeb číslování IP adres a domén. Jde navíc o jakékoliv poskytovatele služeb na území EU. Přístup je zde podobný jako v případě GDPR,[31] tedy takový, že povinnost vykonat vydané příkazy budou mít i subjekty usídlené mimo EU a podnikající podle mimoevropského práva. Za elektronické údaje pak návrh nařízení označuje poměrně širokou paletu dat zahrnující údaje o účastníkovi, údaje o přístupu, údaje o transakcích a údaje o obsahu.

---

28 Zavedený Rámcovým rozhodnutím Rady 2008/978/SVV ze dne 18. prosince 2008 o evropském důkazním příkazu k zajištění předmětů, listin a údajů pro účely řízení v trestních věcech. Dostupné online z: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.350.01.0072.01.ENG>.

29 K tomu nadále dochází v souladu s ustanovením čl. 13 Úmluvy o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie z roku 2000. Viz zde: <https://op.europa.eu/cs/publication-detail/-/publication/31c5655f-4ea3-44a1-985e-2ce7f67f3b96/language-cs>.

30 Navrhované znění je online dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018PC0225&from=EN>. Dále též „návrh nařízení“.

31 Srov. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Návrh nařízení je v současné době stále v legislativním procesu a současně je stále poměrně kontroverzním předpisem. Kritika například směřuje na nedostatečný právní základ pro přijetí takové legislativy na straně EU,[32] nedostatečnou ochranu práv a svobod osob,[33] kterých se data mohou týkat, či na problematiku rozporu požadavku na součinnost ze strany mimoevropských poskytovatelů s limity právních předpisů v zemích, kde sídlí.[34]

2.3 České právo

Dokazování v trestním řízení upravuje v České republice především trestní řád,[35] který vybavuje orgány činné v trestním řízení sadou nástrojů k zajišťování důkazů, kterými může být obecně cokoliv, co může přispět k objasnění věci. Jak bylo ovšem uvedeno již výše, český trestní řád je poněkud zastaralým právním předpisem, který je polepen značným množstvím novelizovaných ustanovení, jež tento handicap zmírňují. V oblasti právní úpravy elektronických důkazů však zcela jednoznačně ne dokonale. Základním problémem trestního řádu je v tomto ohledu skutečnost, že chybí nejen ucelená regulace elektronických důkazů, ale i regulace, byť jen zcela obecná, zakotvující základní definici, principy atd.

Trestní řád s elektronickými důkazy výslovně nepočítá,[36] a proto si aplikační praxe musí vystačit s kreativním výkladem procesních institutů, které původně nebyly k zajišťování či provádění elektronických důkazů určeny. V důsledku toho je právní úprava aplikovaná na elektronické důkazy roztříštěná, neintuitivní a nepřehledná. Dokonce lze říci, že je do určité míry i nahodilá podle toho, pod kterou právní normu se zrovna určitá situace ohledně elektronického důkazu dá nejlépe subsumovat s nejmenší pochybností o tom, zda ještě do jejího rozsahu spadá. Jak orgány činné v trestním řízení, tak povinné osoby často tápají v tom, podle jakého ustanovení a jak postupovat.

Situaci ztěžuje dále i to, že Nejvyšší soud jakožto orgán povolaný ke sjednocování judikatury v oboru trestního řízení má jen omezené možnosti přezkumu provedeného dokazování, neboť vady dokazování zpravidla nelze podřadit pod žádný dovolací důvod dle § 265b trestního řádu.[37] Dovolání je přitom mimořádným opravným prostředkem, který se na nápadu Nejvyššího soudu podílí patrně největším dílem a který mu poskytuje nejširší možnost zaujmout k určité výkladové otázce právní názor. Obdobná situace pak panuje i v řízení o ústavní stížnosti před Ústavním soudem.

---

32 Na nedostatečný právní základ ve svém stanovisku poukazuje například Rada evropských advokátních komor (CCBE). Viz plné znění stanoviska online z: <https://www.cak.cz/assets/priloha_7_2018_11.pdf>.

33 Na kterou poukazuje například Stanovisko Evropského inspektora ochrany osobních údajů č. 7/2019 dostupné online z: <https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf>.

34 Například americké telekomunikační předpisy zakazují v některých případech americkým poskytovatelům služeb bez dalšího poskytovat data zahraničním orgánům a vyžadují využití mechanismů mezinárodní justiční spolupráce. Teoreticky by v tomto případně dal tento rozpor vyřešit uzavření exekutivní smlouvy podle *Cloud Act*, ke kterému ale zatím mezi EU a USA nedošlo.

35 Viz zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

36 Výjimkou je § 7b trestního řádu, který však dle důvodové zprávy zajišťuje provedení požadavků Úmluvy o kyberkriminalitě, tedy nejde o projev snahy koncepčně danou problematiku vyřešit, ale pouze v duchu nejlepších tradic salámové metody vytvořit ustanovení, které zapracovává mezinárodněprávní požadavek v minimální nutné míře při rezignaci na komplexní přístup a přehodnocení i všech dalších souvisejících oblastí trestního řízení, které se elektronických důkazů dotýkají.

37 Otázky dokazování nicméně často souvisí s právem na spravedlivý proces, kterému podle ustálené judikatury musí i Nejvyšší soud poskytovat ochranu. V tomto směru tedy vady dokazování na základě podaných dovolání přezkoumávat může, ačkoliv to příliš často nečiní.

Neznamená to jistě, že by Nejvyšší soud či Ústavní soud byly zcela vyloučeny z možnosti vyjádřit se k aplikaci právní úpravy trestního řádu ve vztahu k elektronickým důkazům (viz i jejich judikáty, na něž odkazujeme níže). U Nejvyššího soudu tuto možnost otevírá především řízení o stížnosti pro porušení zákona a u obou těchto vrcholných orgánů moci soudní se pak nabízí možnost k zásahu v případě vad dosahujících intenzity porušení základních lidských práva a svobod. Tyto příležitosti jsou však spíše sporadické. Chybí zde tolik potřebná „masa" judikatury, která postupně s narůstajícím množstvím precizuje přístup aplikační praxe a ustaluje výklad i aplikaci předmětných právních norem.

Byť takový stav věcí jistě není optimální, aplikační praxe si dokáže poradit i za něj a zejména v posledních přibližně dvou dekádách v ní došlo k vytvoření pragmaticky fungujícího přístupu k elektronickým důkazům. Nevděčný úkol hlavního tvůrce aplikační architektury právní úpravy trestního řízení ve vztahu k elektronickým důkazům na sebe vzalo Nejvyšší státní zastupitelství (dále jen „NSZ"), které v rámci své metodické činnosti vydalo stěžejní dokumenty, které poprvé měly ambici uchopit tento problém systémově a komplexně.[38] Tento přístup pak v podstatě aplikační praxe převzala. Současný stav lze obecně shrnout tak, že procesní nástroje využívané pro zajišťování elektronických důkazů se uplatňují v závislosti na:

a) charakteru získávaného elektronického důkazu (zejména jde-li o přepravovanou či doručenou zprávu, data uložená na pevném nosiči, data uložená v cloudu, tzv. metadata elektronické komunikace atd.),

b) způsobu získávání elektronického důkazu (zda se data extrahují přímo z elektronického zařízení jako je mobilní telefon či laptop, zda se získávají od poskytovatele služeb elektronické komunikace či služeb informační společnosti, od třetí osoby, u níž se data nachází atd.),

c) okamžiku, v němž se zajištění provádí (typicky v případě zpráv přepravovaných prostřednictvím služeb elektronické komunikace, zda byly doručeny ještě před okamžikem zajištění nebo až po něm).

Základní (a pro přehlednost notně zjednodušené) schéma struktury přístupu aplikační praxe k elektronickým důkazům lze shrnout následovně:

V případě zajišťování a vyhodnocování obsahu a metadat souvisejících s elektronickou komunikací se uplatňují ustanovení § 88 trestního řádu o odposlechu a záznamu telekomunikačního provozu a § 88a trestního řádu upravující postupy při zjišťování provozních a lokalizačních údajů o telekomunikačním provozu. Obě ustanovení se pak vztahují na širokou škálu služeb elektronických komunikací – od telefonické komunikace, přes datový přenos po sítích elektronických komunikací až po zajišťování obsahu komunikace prostřednictvím e-mailu a jiných typů komunikačních služeb.[39]

---

38 Jedná se zejména o stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů, k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek (dostupné z: <https://verejnazaloba.cz/wp-content/uploads/2020/03/1_SL_760-2014.pdf>), navazující na starší stanovisko poř. č. 4/2005 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů k postupu v případech, kdy je třeba pro účely trestního řízení zjistit obsah údajů uložených v nalezeném, vydaném či odňatém mobilním telefonu, včetně údajů uložených na SIM kartě.

39 Viz stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství, s. 8.

Získání obsahu elektronické komunikace od poskytovatele příslušné služby do budoucna (respektive v reálném čase) je možné toliko na základě příkazu dle § 88 trestního řádu. K získání metadat o elektronické komunikaci pak slouží § 88a trestního řádu, který má v porovnání s § 88 trestního řádu poněkud benevolentnější podmínky a lze jej uplatnit jak na metadata, která mají do budoucna na zájmovém zařízení vzniknout, tak na metadata, která vznikla již v minulosti a byla poskytovatelem příslušné služby uchována.

Minulý obsah elektronické komunikace (e-maily, zprávy přes messengery či sociální sítě, ale v zásadě i celý obsah e-mailové schránky včetně zpráv teprve rozepsaných atd.), k němuž již měl adresát přístup, je zajišťován dle § 158d odst. 3 trestního řádu. Na získání obsahu takové komunikace, který ještě nebyl adresátovi zpřístupněn (s jejímž obsahem se ještě neseznámil, tedy typicky doručená, ale nepřečtená zpráva) se vztahuje opět § 88 trestního řádu, neboť jde v podstatě o dosud neukončenou komunikaci, případně neměl-li adresát ani příležitost se s obsahem zprávy seznámit (např. byla doručena až po jeho zadržení), je možné uvažovat o aplikaci § 8 odst. 5 trestního řádu[40] jako o určitém východisku z nouze.

Data, která nemají povahu elektronické komunikace, ale jsou získávána od třetích subjektů (typicky dokumenty uložené v cloudových úložištích či na vzdálených serverech, např. informace z profilů sociálních sítí atd.), mají v zásadě dvojí režim. Nejde-li o data, vůči nimž by poskytovatel předmětné služby byl vázán povinností mlčenlivosti (např. data zveřejněná samotným uživatelem), postačí k jejich zajištění tzv. dožádání dle § 8 odst. 1 trestního řádu; pokud zde tato povinnost je, je nutno postupovat dle § 158d odst. 3 trestního řádu.[41]

Ve vztahu k poskytovatelům předmětných služeb či k jiným třetím osobám, které mají ve své dispozici zájmové elektronické důkazy, je pak v této souvislosti relevantní ještě relativně nový institut tzv. „zmrazení dat" dle § 7b trestního řádu, umožňující orgánům činným v trestním řízení uložit takové osobě povinnost uchování zájmových dat po dobu až 90 dní, případně znemožnit jiným osobám přístup k nim. Tento institut slouží toliko k zajištění dat u této třetí osoby, nikoliv i k jejich vydání orgánu činnému v trestním řízení. To je pak třeba realizovat s využitím jednoho ze shora nastíněných procesních institutů podle toho, o jakou situaci jde z hlediska výše uvedených parametrů rozlišujících použitelnost jednotlivých procesních institutů ve vztahu k elektronickým důkazům. Právě proto, že jde o toliko zajištění integrity dat, a nikoliv o jejich zpřístupnění orgánům činným v trestním řízení, je i procesní standard záruk zajištění práv třetích osob poměrně nízký, neboť v přípravném řízení postačí příkaz policejního orgánu se souhlasem státního zástupce, a při nebezpečí z prodlení i bez něj.

Specifickou otázkou je získávání informací z neveřejných částí profilů či stránek sociálních sítí. K této problematice se již vyjadřoval Ústavní soud, podle jehož obecných závěrů je třeba vždy důsledně rozlišovat u každého konkrétního příspěvku, zda byl učiněn soukromě nebo veřejně, a aplikovat příslušná ustanovení trestního řádu.[42] Toto pilotní rozhodnutí však neposkytovalo příliš přesné směrnice, podle nichž by měly orgány činné v trestním řízení postupovat. Neproblematické jsou příspěvky učiněné veřejně tak, že si

40 Viz stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství, s. 10–11.

41 Srov. STUPKA, Václav. In: POLČÁK, Radim – PÚRY, František – HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 107.

42 Viz nález Ústavního soudu sp. zn. III. ÚS 3844/13 (N 201/75 SbNU 259).

je může zobrazit kdokoliv bez dalších zvláštních omezení. V těchto případech lze nepochybně jejich obsah zajistit bez potřeby vyžadování jakéhokoliv souhlasu. Jde-li o uzavřené komunikace činěné prostřednictvím aplikací typu messenger, uplatní se všechna pravidla uvedená výše pro zajišťování obsahu elektronické komunikace.

Složitější situaci musela aplikační praxe řešit již ve vztahu k příspěvkům publikovaným v rámci uzavřených, „poloveřejných" stránek (tzv. skupin), které určitá omezení vstupu ze strany veřejnosti vztyčují (např. nutností schválení přístupu ze strany administrátora stránky, který tak učiní pouze za splnění určitých podmínek), nejedná se však o ryze soukromou konverzaci typu vyměňování zpráv či hovorů v reálném čase. Stěžejním vodítkem při řešení těchto situací je právní závěr Ústavního soudu, že data z takových poloveřejných stránek (typicky ve formě *printscreenu*), která Policii ČR předá informátor ve smyslu § 73 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, který takovou stránku infiltroval, nevyžadují k použití pro důkazní účely v trestním řízení žádný souhlas ani příkaz soudu a je možno je využít bez dalšího.[43] Tento závěr lze patrně rozšířit i na situace, v nichž data nebudou předána osobou přímo v postavení policejního informátora, ale někoho, kdo měl k těmto datům legální přístup (např. poškozený, který jako člen neveřejné stránky měl přístup k příspěvku jiného uživatele, jehož prostřednictvím na něm byl spáchán trestný čin). V praxi bývají rovněž data z poloveřejných či neveřejných stránek rovněž prostřednictvím operativních profilů, které si vytvářejí vyšetřovatelé. Pokud pak nedochází k umisťování nevhodného obsahu do těchto stránek ani k podněcování k nevhodné komunikaci či distribuci nevhodného obsahu, ale pouze k dokumentaci již probíhajícího trestněprávního jednání a zajišťování obsahu, nejedná se o tzv. policejní provokaci.[44]

Poslední typizovanou a v praxi častou situací je extrakce dat přímo z jejich hmotného nosiče majícího podobu hmotného datového nosiče v jakékoliv podobě (USB, přenosné pevné disky, snad ještě i DVD či CD, telefony, tablety, notebooky atd.). Tento postup nastává tehdy, je-li při realizaci jiného zajišťovacího úkonu (domovní prohlídka a prohlídka jiných prostor, vydání či odnětí věci, osobní prohlídka atd.) takový datový nosič nalezen a zajištěn. Co se týče elektronické komunikace vedené tímto nosičem, uplatní se ohledně komunikace, k níž dochází od okamžiku zajištění takového nosiče do budoucna, výše uvedený režim § 88 trestního řádu.

Ohledně ostatních dat (uložené dokumenty, obrazové, zvukové i audiovizuální soubory, programy atd., ale i v paměti uložené akty minulé elektronické komunikace) se dosavadní přístup kloní ke stanovisku, že za těchto okolností není třeba pro extrakci dat z datového nosiče žádný další zvláštní procesní postup.[45] Orgány činné v trestním řízení pak typicky vlastními silami či s využitím externích expertů na informační technologie ze zajištěného datového nosiče extrahují zájmová data, je-li to technicky možné.

Nezdá se, že by se tento přístup v aplikační praxi soudů setkával s odporem či odmítáním, naopak má oporu v judikatuře,[46] ostatně dobře zapadá do dosavadní koncepce věc-

43 Viz nález Ústavního soudu sp. zn. III. ÚS 3564/18 (N 101/94 SbNU 229).

44 K policejní provokaci viz např. usnesení Nejvyššího soudu ČR ze dne 16. 1. 2014, sp. zn. 7 Tdo 1106/2013.

45 Viz výrok shora citovaného výkladového stanoviska poř. č. 4/2005 a jeho s. 11 a výrok I. citovaného výkladového stanoviska poř. č. 1/2015.

46 Srov. usnesení Nejvyššího soudu ze dne 15. 12. 2000, sp. zn. 7 Tz 9/2000, potvrzené i usnesením Nejvyššího soudu ze dne 16. 3. 2016, sp. zn. 7 Tdo 173/2016.

ných důkazů v trestním řízení. Orgány činné v trestním řízení totiž běžně se zajištěnými věcnými důkazy nakládají bez dalšího tak, jak je pro potřeby dokazování nutné (např. využití fyzikálních a chemických metod kriminalistické techniky na zajištěné věcné nosiče důkazů s cílem objevení mikrostop), a to včetně takových postupů, při nichž jsou odhalovány rovněž citlivé informace osobní povahy (např. analýza DNA s využitím zajištěného biologického materiálu či analýza zajištěného osobního deníku, fotografií se sexuálním obsahem atd.), a podrobují je znaleckému zkoumání a jiným expertizním činnostem v podstatě bez omezení (jistě však v mezích obecných limitů zásady přiměřenosti, hospodárnosti atd.).

Přesto lze v tomto přístupu spatřovat zřejmá úskalí z hlediska ochrany základních lidských práv a svobod osoby, u níž byl takový datový nosič zajištěn, jakož i osob, jejichž data jsou na něm uložena (nemusí se totiž nutně jednat o stejné osoby), a do budoucna lze pochybovat, zda tento přístup obstojí. Nedostatečná se zdá především absence jakékoliv diferenciace jednak typu nosiče (zpřístupnění obsahu pracovního flash disku zpravidla nelze mírou zásahu do soukromí srovnávat se zpřístupněním obsahu např. celého mobilního telefonu či počítače), jednak způsobu zabezpečení (tj. zda např. daný datový nosič nebyl nijak zabezpečen a ke zpřístupnění jeho obsahu postačovala pouhá dispozice s ním, zda je třeba k jeho zpřístupnění prolomit heslo či provést dešifrování obsahu atd.) a jednak i možnou extenzi zpřístupnění na další data, která nejsou uložena fyzicky na daném nosiči (tj. např. zda zpřístupnění obsahu telefonu, tabletu či počítače umožňuje i zpřístupnění dat uložených v cloudu či na vzdáleném úložišti díky tomu, že jsou v něm uloženy přístupové údaje).

Dalším bílým místem současné právní úpravy v těchto situacích je i absence úpravy intruzivních (penetračních) postupů orgánů činných v trestním řízení při překonávání softwarového zabezpečení, a to zejména s ohledem na to, že tento problém dříve či později narazí (respektive v praxi již naráží) nutně na limity vybavenosti Policie ČR v porovnání s možnostmi světových technologických leaderů zabezpečovat své produkty. I kdyby totiž bylo možno připustit, že jakmile se datový nosič dostane do dispozice orgánů činných v trestním řízení, tyto mají pravomoc s ním nakládat (při zachování zásady přiměřenosti atd.), jak nejlépe umí, a prolamovat jeho zabezpečení i bez souhlasu soudu, jsou-li toho technicky schopny, nejsou tím pokryty případy, kdy toho technicky schopny nejsou a zpřístupnění obsahu datového nosiče by vyžadovalo součinnost s jeho výrobcem (např. při nemožnosti prolomit šifrování uložených dat). Nešlo by zde totiž o vydání dat třetím subjektem, u nějž je využitelný § 158d odst. 3 trestního řádu, ale pouze o poskytnutí součinnosti při zpřístupňování předmětného datového nosiče. Dílčí pravomoc orgánů činných v trestním řízení něco takového nařídit a procesní záruky práv dotčených osob v platné a účinné právní úpravě chybí.

Poslední potřebná „vstupní" informace k domácí právní úpravě se týká elektronických důkazů *de lege ferenda* v návrhu nového trestního řádu, jehož paragrafované znění je již veřejně přístupné.[47] Z dosud zveřejněných informací se zdá, že zvažovaný nový trestněprocesní kodex hodlá na elektronické důkazy výslovně pamatovat, avšak příliš ambiciózní v tomto ohledu není. Východiskem je právní konstrukce ustanovení pracovně označeného jako § e42 odst. 2, podle nějž: *„Ustanovení o věcech se vztahují i na data uchovávaná*

47 Online na adrese: <https://tpp.justice.cz/>.

v elektronické podobě, nevyplývá-li z jednotlivých ustanovení trestněprocesního zákona něco jiného.“ I v řadě dalších ustanovení se objevuje pojem „data“ samostatně vedle listin a věcí, což značí odlišování jejich svébytnosti od jiných nosičů důkazu. Alfou a omegou připravované nové právní úpravy však bude pochopitelně především to, jak toto odlišení bude provedeno v části týkající se zajišťovacích institutů ve vztahu k elektronickým důkazům, nicméně část návrhu týkající se zajišťovacích institutů nebyla ještě v době psaní tohoto článku veřejně přístupná.

3. Hlavní právní výzvy

Z předchozího textu je patrné, že ačkoliv došlo v minulosti k poměrně dynamickému rozvoji legislativy a praxe uplatňované při nakládání s elektronickými důkazy, výzev lze vnímat stále velké množství. Tyto výzvy lze v ČR identifikovat hned v několika oblastech. První oblast se týká samotné právní úpravy – ta je nucena reagovat na aktuální technologický vývoj a poskytnout orgánům činným v trestním řízení efektivní nástroje pro stíhání kriminality a současně zohlednit požadavky na ochranu ústavních práv. Do této oblasti lze rovněž zahrnout výzvy související s implementací stávajících a budoucích právních nástrojů konstruovaných na úrovni mezinárodní komunity a Evropské unie. Druhá oblast souvisí s problematikou uplatňované kriminalistické techniky a metodiky při zajišťování elektronických stop, která je i přes evidentní snahy na všech úrovních orgánů činných v trestním řízení stále poněkud nekonzistentní a mnohdy i neefektivní. Poslední oblast navazuje na vývoj nových technologií, které mohou znamenat zásadní zásah do trestního procesu i vnímání elektronických důkazů jako takových. Ačkoliv je úprava procesních nástrojů zásadně technologicky neutrální, může rozvoj umělé inteligence, kvantových počítačů či neurotechnologií vyžadovat nejen budování nových procesních nástrojů a postupů, ale i kritický přístup při konstrukci ústavních limitů při využívání těchto technologií pro dokazování v trestním řízení.

Tento článek se věnuje především právním otázkám, proto se zaměříme na první identifikovanou oblast.

Prvním a základním předpokladem nastavení vhodné úpravy a postupů pro nakládání s elektronickými důkazy je jejich pojmové zakotvení. Aktuální právní úprava pojem elektronický důkaz nezná, což je i v zahraničním srovnání spíše pravidlem než výjimkou. Problém je spíš s rozdělením jednotlivých elektronických důkazů podle jejich právní povahy. Trestní řád pracuje s pojmy jako jsou telekomunikační provoz, údaje o telekomunikačním provozu, počítačový systém, data, záznamy uchovávané v soukromí a podobně. Na vazbě konkrétní kategorie elektronických důkazů na tyto pojmy závisí i volba procesního nástroje k jejich zajištění, související úroveň ochrany lidských práv potenciálně dotčených osob i procesní náročnost pro orgány činné v trestním řízení. To v minulosti vedlo k tomu, že se jednotlivé zúčastněné strany – ať již šlo o orgány činné v trestním řízení, povinné osoby poskytující součinnost či obhajobu – snažily se všemi možnými prostředky prosadit využití těch procesních nástrojů, které jim nejvíce vyhovovaly.[48] Důsledkem je nekonsistence v trestním řízení, úrovni ochrany lidských práv, uplatnitelnosti a důkazní

[48] Na straně ISP například ve vztahu k jejich obchodnímu modelu, *public relations* nebo riziku vlastní odpovědnosti, na straně OČTŘ z hlediska procesní dostupnosti příslušných procesních nástrojů.

síle elektronických důkazů a dalším problémům. Přestože k určitým snahám o klasifikaci a zpřehlednění těchto vazeb dochází (například prostřednictvím výkladových stanovisek NSZ[49] nebo v odborné literatuře), nebyly tyto snahy doposud systematické s vazbou na zahraniční iniciativy[50] a reálie českého právního prostředí.

Podobné nekonsistence jsou patrné v nastavení jednotlivých procesních institutů v trestním řádu, které jsou běžně pro zajišťování elektronických důkazů využívány. Jak je zřejmé z předchozího výkladu, různé instituty vznikaly v různé době a s různou teleologií, a ačkoliv zákonodárce v těchto kontextech vyhodnocoval míru rizika zásahu do práv a svobod osob dotčených při jejich využití a podle toho je konstruoval, jejich využití při dokazování elektronickými důkazy může být poněkud problematické. Zajištěním a analýzou některých elektronických důkazů, respektive jejich zdrojů totiž mnohdy dochází k zásadnímu zásahu do některých ústavně zaručených práv. Například mobilní telefon, osobní počítač nebo soukromé cloudové úložiště může obsahovat větší množství informací o soukromí člověka než jeho domácnost. Přesto jsou záruky uplatňované v případech zajištění a ohledání věci či při zajišťování dat z cloudových úložišť v rámci sledování osob a věcí nesrovnatelně nižší než ty, které se uplatňují při domovní prohlídce.[51] Tento stav není ojedinělý, i v mezinárodním srovnání je patrné, že při uplatňování tradičních procesních institutů jsou mnohdy uplatňovány nedostatečné záruky ve vztahu k charakteru zajišťovaných a zpracovávaných elektronických důkazů.[52] Může však nastat i opačná situace, tedy že úroveň záruk bude nepřiměřeně vysoká a v jejím důsledku budou příslušné procesní nástroje pro orgány činné v trestním řízení v některých situacích nedostupné nebo obtížně dostupné.[53] Před ratifikací Úmluvy o kyberkriminalitě například limity nastavené u odposlechu a záznamu telekomunikačního provozu neumožňovaly využití tohoto nástroje ke sběru dat při vyšetřování kyberkriminality,[54] což mohlo do značné míry svazovat ruce při stíhání takové trestné činnosti.

Stávající instituty trestního práva procesního by z výše uvedených důvodů měly být podrobeny analýze právě z hlediska rozsahu ochrany práv dotčených osob a využitelnosti k zajištění příslušných elektronických důkazů. Podobně by bylo vhodné provést syntézu s kategorizací elektronických důkazů doporučenou výše, v jejímž rámci by byly identifikovány mezery v právní úpravě, které způsobují nemožnost získávání některých kategorií důkazů nebo naopak umožňují využití pro jednu kategorii důkazů využití více procesních nástrojů, které mají různou míru ochrany práv a procesní náročnost. Podobný analytický přístup by umožnil formulovat konkrétní doporučení *de lege ferenda* jak pro aktualizaci současné právní úpravy trestního procesu, tak pro aktuálně probíhající přípravu rekodifikace.

---

49 Výkladová stanoviska Nejvyššího státního zastupitelství jsou dostupná online z: <https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/vykladova-stanoviska/stanoviska-z-trestniho-prava-procesniho/>.

50 Například na projekty realizované v EU, snahy o kategorizaci ze strany Europolu, Evropské agentury pro kyberbezpečnost apod.

51 K problematice nedostatečné ochrany soukromí v případě využití dat z mobilního telefonu viz např. MAREŠOVÁ, Eliška. Problematika získávání informací z mobilních telefonů v rámci trestního řízení. *Trestněprávní revue*. 2021, č. 3, s. 146.

52 Viz např. srovnávací studie projektu EVIDENCE, dostupná online z: <http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d8-1-423.pdf>.

53 Například aplikace postupu podle § 158d/3 p. a. § 88/1 tr. ř. u získávání obsahu e-mailu nelze aplikovat na bagatelní trestné činy (např. Majetkovou trestnou činnost), protože postup podle § 88/1 je limitován jen na vybrané případy (sazbou, na vyjmenované trestné činy, či činy trestné podle mezinárodní smlouvy).

54 Do té doby totiž nebylo stíhání příslušných skutkových podstat vyžadování žádnou vyhlášenou mezinárodní smlouvou.

Kromě samotného nakládání s elektronickými důkazy je z hlediska praxe i podle dostupné odborné literatury[55] výzvou i hodnocení elektronických důkazů. Elektronické důkazy jsou na jednu stranu mnohdy hodnoceny jako nespolehlivé kvůli slabé ochraně integrity elektronických dat, v některých případech je k nim naopak přistupováno poněkud nekriticky, obzvlášť jsou-li prezentovány soudu prostřednictvím znaleckého posudku. Doktrína pro kritéria hodnocení elektronických důkazů neexistuje, nevyplývá ani z judikatury ani z odborné literatury. Přitom kritéria jsou klíčová jak pro přisuzování hodnoty závažnosti (důležitosti) elektronického důkazu pro rozhodnutí, tak hodnoty zákonnosti elektronického důkazu i hodnoty pravdivosti (popřípadě věrohodnosti) elektronického důkazu. Hodnocení elektronických důkazů je závislé především na technických parametrech – na charakteru příslušných dat, jejich zdroji, metodě jejich získání a uchování, využitých interpretačních, analytických a forenzních nástrojích apod. Tyto faktory mohou ovlivňovat důkazy oběma směry: nejenže nevhodný postup při zajištění důkazů může způsobit jejich znehodnocení nebo snížení jejich důkazní síly, ale může nastat i opačná situace, kdy například využitý forenzní nástroj vygeneruje nespolehlivé nebo nesprávné výstupy.[56] Kvalita hodnocení elektronických důkazů je tedy výrazně ovlivněna schopnostmi a zkušeností osob, které jej provádějí, a dostupným technickým vybavením. Dostupných právních řešení, která by mohla přispět k řešení těchto výzev je relativně málo. Jedním je určitě dobře postavený znalecký zákon. Ten český, který byl publikován ve Sbírce zákonů před dvěma lety,[57] nahradil v letošním roce velmi dlouho kritizovaný a zastaralý znalecký zákon z roku 1967.[58] Nový znalecký zákon je nesporně krokem správným směrem. Zavedení nových zkoušek pro znalce, rozšíření jejich odpovědnosti i lepší úprava náležitostí posudků jistě přispějí ke zvýšení kvality znalecké činnosti, a tedy i ke zvýšení kvality důkazů. Zákon však v některých oblastech lze považovat za promarněnou příležitost, neboť většinu připomínek ze strany odborné veřejnosti, které směřovaly ke zkvalitnění znalecké činnosti, stát přislíbil vyřešit formou vyhlášek a jiných podzákonných norem. Samotný zákon však tyto specifické požadavky neadresuje a je proto otázkou, zda k tomu budou mít v tomto směru příslušné orgány veřejné moci dostatek potřebné vůle, kvalifikace, prostředků a kapacit.[59] Současně je potřeba počítat se souvisejícím rizikem, že zvýšením kvalifikačních předpokladů a nároků na znalce dojde k faktickému snížení

---

55 Viz např. zde: MASON, Stephen. Electronic evidence: A proposal to reform the presumption of reliability and hearsay. *Computer Law & Security Review* [online]. 2014, Vol. 30, Iss. 1, s. 80–84 [cit. 2021-10-12]. Dostupné z: doi:10.1016/j.clsr.2013.12.005. Online dostupné také z: <https://www.sciencedirect.com/science/article/pii/S0267364913002057?casa_token=jUrSqEeyRDgAAAAA:xw-jROONSJZ5d6UH_GQ2qZtUURyiGmkewxs_L3-6A2sli9DqcrrzoHAbx1zy4O8aSIKptQCLMcA>.

56 Viz např. zde: VAN BUSKIRK, Eric – LIU, Vincent T. Digital Evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice* [online]. 2006, Vol. 1, No. 1, 19–26 [cit. 2021-10-12]. Dostupné z: doi:10.1080/15567280500541421. Online dostupné také z: <https://www.bishopfox.com/files/articles/2006/Journal_of_Digital_Forensic_Practice–Challenging_the_Presumption_of_Reliability–Mar2006.pdf>.

57 Viz zákon č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech z 9. října 2019.

58 Viz zákon č. 36/1967 Sb., o znalcích a tlumočnících.

59 Více k problematice kvality znalecké činnosti ve vztahu k novému znaleckému zákonu viz např. zde: SVETLÍK, Marián, jr. Dorazil nový zákon o znalcích. Tak nějak po česku. *Digital Forensic Review*. 2020, roč. 4, Vol. 6–7, č. 1–2, s. 21–23. Dostupné také z: <https://d6scj24zvfbbo.cloudfront.net/5d65ad9dd870a17415aa5ba965f32d66/200000055-c77ecc77ee/6_1-2020-021-024.pdf?ph=03c57292e5> nebo <https://www.dfreview.cz/l/dfr-c-6-1-2-2020/>, a/nebo zde: SVETLÍK, Marián, sr. Kvalita znalců očima návrhu zákona. *Digital Forensic Review*. 2019, roč. 3, Vol. 4, č. 1, s. 7. Dostupné také z: <https://d6scj24zvfbbo.cloudfront.net/5d65ad9dd870a17415aa5ba965f32d66/200000012-b2756b2759/2019_1-1.pdf?ph=03c57292e5> nebo <https://www.dfreview.cz/l/dfr-4/>.

jejich dostupnosti a tím k dalším procesním průtahům. Dalším nástrojem, který by mohl potenciálně proces hodnocení elektronických důkazů zkvalitnit, je koordinace a tvorba metodických materiálů. Již v současné době jsou některé postupy harmonizovány pomocí interních aktů řízení Policie ČR,[60] ty jsou však veřejnosti nedostupné a věnují se jen omezenému rozsahu postupů. V rámci Národní centrály proti organizovanému zločinu byl vybudován tým metodiků, kteří by mohli přinejmenším přispět k uplatňování vhodné metodiky práce s elektronickými důkazy, což by mohlo v konečném důsledku vést i k vyšší kvalitě jejich zpracování, provádění i hodnocení.

Zásadní výzvy jednoznačně souvisí s problematikou dostupnosti elektronických důkazů zpracovávaných zahraničními subjekty a uchovávaných v zahraničí. Jak bylo uvedeno výše, současné mechanismy pro mezinárodní spolupráci jsou mnohdy poměrně neefektivní a s rozvojem nových technologií, především cloudu, dochází k posilování decentralizace uchovávání dat a ke snižování jejich lokální dostupnosti. Tuto výzvu není v podstatě možné řešit na úrovni jednoho státu, což je reflektováno v rámci mezinárodní komunity snahami o přípravu nejrůznějších instrumentů umožňujících efektivní přeshraniční práci s elektronickými důkazy. Klíčovou roli v tomto směru budou pro ČR v budoucnosti hrát snahy Evropské unie v podobě Evropských předávacích a uchovávacích příkazů a Rady Evropy v podobě institutů druhého dodatkového protokolu k úmluvě o kyberkriminalitě. Obě tyto iniciativy v podstatě směřují k přemostění standardních procedur mezinárodní justiční spolupráce tak, aby mohly příslušné orgány činné v trestním řízení získávat důkazy a součinnost přímo od poskytovatelů služeb působících v zahraničí. Navržené mechanismy zatím ale nejsou dostupné, navíc jsou podrobovány poměrně intenzivní kritice pro nesystémovost, slabou ochranu práv dotčených osob či neexistenci autentizačních mechanismů.[61] Proto je v současnosti nutné spoléhat na klasické a široce dostupné mechanismy mezinárodní justiční spolupráce, respektive nově dostupný evropský vyšetřovací příkaz v rámci EU. I v případě těchto tradičních a ověřených nástrojů lze však identifikovat rezervy, zejména z hlediska existujících formálních postupů při přípravě žádostí a poskytování součinnosti. Především v rámci projektů EU[62] je často realizována komparativní analýza, jejímž prostřednictvím jsou identifikována praktická, organizační i právní opatření, jimiž je možné procesy související s elektronickým dokazováním zefektivnit. Ačkoliv jsou tato opatření zpravidla formulována spíše obecně, mohou po přizpůsobení najít uplatnění i v českém prostředí.

Závěr

Rozvoj informační společnosti vede k stále většímu využívání informačních a komunikačních technologií ve všech společenských aktivitách. Nejinak tomu je v případě trestné činnosti; ve stále větší míře se ICT objevují jako cíle nebo prostředky pachatelů. Z toho

60 Více viz zde: VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů*. Diplomová práce. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013, s. 18, například jde o Metodický pokyn ředitele KÚP č. 7/2001, kterým se upravuje činnost orgánů Policie ČR při zajišťování výpočetní techniky a dat pro účely následného znaleckého zkoumání. Je však otázkou, do jaké míry jsou tyto postupy uplatňovány v praxi, zpravidla totiž mají jen nezávazný charakter doporučení.

61 Viz výše.

62 Příkladem může být projekt *Evidence* (<https://evidenceproject.eu>), zaměřený obecně na elektronické důkazy, nebo projekt *For-mobile* (<https://formobile-project.eu>), věnovaný problematice mobilních zařízení.

důvodu stoupá význam dokazování prostřednictvím elektronických důkazů, což představuje v mnoha ohledech velkou výzvu pro právní teorii i praxi. Odborná literatura se však této problematice po hříchu věnuje jen v poměrně omezené míře.

Tento článek si proto klade za cíl vyvolat odbornou diskusi prostřednictvím identifikace souvisejících právních výzev, které jsou z pohledu autorů významné a mohou do budoucna výrazně ovlivňovat kvalitu trestního procesu. Autoři nejprve mapují aktuální právní prostředí ovlivňující práci s elektronickými důkazy tvořené mezinárodními, evropskými i českými prameny práva a identifikují, jaké důsledky má toto prostředí v kombinaci s charakteristickými znaky elektronických důkazů pro praxi v trestním řízení.

Následně identifikují hlavní výzvy, které z právního hlediska současný stav představuje. Ty lze rozdělit do několika skupin. První skupinou jsou výzvy související s procesněprávní úpravou trestního řádu a limity její aplikace na reálné situace při práci s elektronickými důkazy a při zohlednění nezbytné ochrany práv osob, vůči kterým jsou příslušné procesní nástroje uplatňovány. Do druhé spadá problematika přeshraničního zajišťování elektronických důkazů a související obecné i specifické mezinárodní právní úpravy a její aplikace v českých podmínkách. Třetí skupinu tvoří výzvy související s hodnocením jednotlivých typů elektronických důkazů co do jejich kvality a spolehlivosti ve vazbě na jejich charakter a postupy při jejich zajišťování, analýze a hodnocení.

Autoři jsou si vědomi toho, že článek nenabízí řešení identifikovaných výzev, to ostatně není ani jeho cílem. Článek by měl být vnímán jako příspěvek do potřebné diskuse o problematice elektronického dokazování a jako východisko a mapa pro další výzkumné a analytické práce.

Electronic Evidence as a Challenge to Criminal Proceedings

Václav Stupka (https://orcid.org/0000-0003-1458-1507) –
Jan Provazník (https://orcid.org/0000-0002-2253-8958) –
Jakub Vostoupal (https://orcid.org/0000-0002-1669-9931)

Abstract: This article deals with the use of electronic evidence in criminal proceedings. It analyzes the current legal regulation of relevant procedural tools in Czech, European and international law, and the practice of using these procedural tools by Czech law enforcement authorities. Subsequently, the article maps the main practical, technical, theoretical, and constitutional challenges that current theory and practice face in relation to this type of evidence. The aim of the article is to provoke an expert discussion on identified challenges and to create a basis for further research.

Keywords: electronic evidence, criminal proceedings, evidence admissibility, evidentiary value, digital forensics, international law instruments, criminalistics