Masarykova univerzita

Právnická fakulta

LL.M. v právu informačních a komunikačních technologií

Písemná práce k modulu
Kyberkriminalita

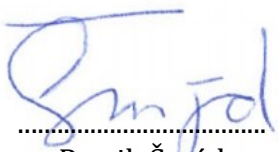
Zajišťování uložených dat v trestních věcech

Vedoucí práce k modulu:
Mgr. Karel Kuchařík

10.1.2020 Patrik Šmýd

Čestné prohlášení

Prohlašuji, že jsem písemnou práci na téma **Zajišťování uložených dat v trestních věcech** zpracoval sám. Veškeré prameny a zdroje informací, které jsem použil k sepsání této práce, byly citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury.



V Brně 10. ledna 2020 .....

Patrik Šmýd

Obsah

1 Úvod

S ohledem na mohutný technický rozmach a začlenění prostředků výpočetní techniky do takřka všech aspektů našich každodenních životů, je zřejmé, že data uložená na těchto zařízeních na nás mohou mnoho prozradit. To může být praktické mimo jiné i v rámci trestního řízení, kdy data uložená ve výpočetní technice mohou posloužit jako výmluvné prameny důkazů, na jejichž základě mohou orgány činné v trestním řízení rekonstruovat skutkové okolnosti trestného činu v rozsahu požadovaném právním řádem pro meritorní rozhodnutí o vině a trestu či o nárocích poškozeného. Orgány činné v trestním řízení si mohou prameny důkazů opatřit a nakládat s nimi prostřednictvím k tomu určených institutů (důkazních prostředků). Aby byl důkaz v trestním řízení použitelný, musí být získán právně přípustným způsobem. Při zajištění důkazů tak musí být zajištěn soulad se všemi relevantními ustanoveními trestního řádu týkajícími se dokazování, aby se z přípustného důkazu nestal důkaz nepřípustný či neúčinný. Stávající právní úprava je v tomto ohledu nicméně zastaralá a neobsahuje žádná specifická ustanovení pro zajišťování elektronických důkazů. Ty jsou proto zajišťovány prostřednictvím stávajících institutů a to začasto postupem v praxi netestovaným a judikatorně nepodloženým, což s sebou nese riziko, že se takto získaný důkaz může stát v trestním řízení nevyužitelný. Tato práce se zaměřuje právě na problematiku zajišťování dat uložených ve výpočetní technice pro účely dokazování v trestním řízení.

2 Specifikace problému, definice cíle a postup řešení

Aby byl důkaz v trestním řízení použitelný, musí být získán právně přípustným způsobem. Při zajištění důkazů tak musí být zajištěn soulad se všemi relevantními ustanoveními trestního řádu týkajícími se dokazování, aby se z přípustného důkazu nestal důkaz nepřípustný či neúčinný. Stávající trestní řád je v tomto ohledu zastaralý a neobsahuje žádná specifická ustanovení pro zajišťování elektronických důkazů, které jsou proto zajišťovány prostřednictvím stávajících institutů a to začasto postupem v praxi netestovaným a judikatorně nepodloženým, což s sebou nese riziko, že se takto získaný důkaz může stát v trestním řízení nevyužitelný. Byť tedy situace není jednoznačná a dostatečně podložená judikaturou, v této stati se pokusíme shrnout současný stav z pohledu právního i z pohledu praktického a učinit doporučení pro praxi.

Východiskem této stati bude obecný úvod do problematiky dokazování dle platného trestního řádu. Definujeme klíčové pojmy, jako je dokazování, důkaz, důkazní prostředek, pramen důkazu či elektronické prameny důkazů a elektronické důkazní prostředky. Rozebereme některé základní zásady trestního řízení, které jsou z hlediska dokazování pomocí elektronických pramenů důkazů relevantní – konkrétně zásadu zjištění skutkového stavu bez důvodných pochybností, zásadu vyhledávací a zásadu zákonnosti, respektive nepřípustnost některých důkazů. Orgány činné v trestním řízení mají zajišťovat důkazy ve prospěch i v neprospěch obviněného. Je tedy na policejním orgánu a státním zástupci, aby zajistili data uložená ve výpočetní technice, je-li to pro trestní řízení relevantní. Prameny důkazů si mohou opatřovat a nakládat s nimi výlučně prostřednictvím k tomu určených institutů (důkazních prostředků).

Ve zvláštní části práce pak rozebereme, jakou podobu mohou elektronické prameny důkazů mít, kde mohou být uloženy a v čem mohou být v rámci dokazování v průběhu trestního řízení užitečné. Prozkoumáme různé kategorie dat, která mohou být relevantní pro trestní řízení relevantní – tzv. zájmové soubory. Zmíníme, že místo uložení zájmových souborů ovlivňuje volbu procesního nástroje pro jejich zajištění. Podrobněji pak rozebereme možné způsoby získání dat uložených ve výpočetní technice - zajištění zařízení nebo datových nosičů jako takových, získání zájmových souborů prostřednictvím vzdáleného přístupu, a získání dat od poskytovatelů služeb. Použitelnými důkazními prostředky podle současného trestního řádu jsou vydání či odnětí věci, domovní či osobní prohlídka či prohlídka pozemků a prostor nesloužících k bydlení, dále pak operativně pátrací prostředek sledování osob a věcí, nebo institut odposlechu a záznamu telekomunikačního provozu či vyžádání údajů o uskutečněném telekomunikačním provozu.

Na závěr se krátce zmíníme o způsobu využití zajištěných dat pro účely trestního řízení. Za tímto účelem je třeba důkazy před soudem provést. V

jednodušších případech je lze provést jako věcné či listinné důkazy, ve složitějších případech je možné vyžádat si odborné vyjádření či přibrat znalce.

Tato stať je založena na diskusi odborné literatury a současné právní úpravy. Deskriptivní část je doplněna doporučeními pro praxi.

3 Analýza problému[1]

3.1 Dokazování v trestním řízení

Púry proces dokazování popisuje jako postup pro rekonstrukci, poznání a vyhodnocení minulých dějů a událostí jako podkladu pro vydání určitého rozhodnutí nebo pro zajištění určitého procesního postupu, přičemž účelem dokazování je zjištění skutkového stavu, o němž nejsou důvodné pochybnosti.[2] Dle Kratochvíla dokazování představuje rekonstrukci skutkových okolností, které jinak nejsou orgánům činným v trestním řízení ani stranám trestního řízení známy, a je jediným a nenahraditelným postupem ke zjištění pravdy v rozsahu požadovaném právním řádem pro meritorní rozhodnutí o vině a trestu či o nárocích poškozeného.[3] V širším smyslu se dokazováním rozumí i zákonem upravený postup pro opatřování, provádění, použití a hodnocení důkazů. Tento postup se řídí především zákonem č. 141/1961 Sb., trestní řád,[4] zejména pak § 89 až 118 trestního řádu.[5]

Púry podotýká, že „orgány činné v trestní řízení se mohou seznámit s posuzovanými skutečnostmi jen nepřímo tím, že si jejich průběh rekonstruují pomocí zprostředkujících skutečností, jimiž jsou právě důkazy.“[6] Dále uvádí, že „dokazováním si orgány činné v trestním řízení opatřují hodnověrné informace o určité minulé události či o jiné skutečnosti významné pro trestní řízení, z nichž

---

[1] Tato kapitola částečně vychází z autorova dřívějšího pojednání na související téma (dokazování v trestním řízení pomocí metadat z mobilního komunikačního zařízení) a dále ji rozpracovává, viz ŠMÝD, Patrik, *Dokazování metadaty z mobilního komunikačního zařízení*, Brno, 2018. 25 s. Modulová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Marián SVETLÍK.

[2] PÚRY, František. *Dokazování v trestním řízení. Elektronické důkazy* [prezentace]. Brno: Právnická fakulta Masarykovy univerzity, 14. 4. 2018, s. 3 [cit. 14. 4. 2018].

[3] KALVODOVÁ, Věra; HRUŠÁKOVÁ, Milana a kol. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty* [online]. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015 [cit. 12. 10. 2019]. s. 29.

[4] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále jen „trestní řád“).

[5] Problematika dokazování má pochopitelně zásadní přesah do práva ústavního a do ochrany základních lidských práv a svobod, jakož i do některých dalších oblastí. Vedle Listiny základních práv a svobod a bohaté judikatury Ústavního soudu je relevantní i Úmluva o ochraně lidských práv a svobod a některé další zákony. Ty však přesahují rozsah této práce. Podrobněji viz POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení* [online]. 1. vyd. Brno: Masarykova univerzita, 2015 [cit. 9. 10. 2019]. s. 49.

[6] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 45.

pomocí logického postupu odvozují úsudek o předmětu dokazování."[7] Předmětem dokazování je okruh skutečností, které je v trestním řízení třeba dokazovat. Minimální rozsah dokazování je stanoven v § 89(1) trestního řádu a zahrnuje zjištění, zda se stal skutek, v němž je trestný čin spatřován, zda jej obviněný spáchal a z jakých pohnutek, a okolností, které mají vliv na posouzení povahy a závažnosti činu, osobních poměrů pachatele, stanovení následku a výše škody či bezdůvodného obohacení, a okolností, které vedly k trestné činnosti nebo umožnily její spáchání.

3.1.1 **Důkaz**

Důkazem je dle Púrého[8] výsledek činnosti orgánu činného v trestním řízení při dokazování. Důkazním prostředkem je procesní činnost, která slouží k poznání dané skutečnosti, jinými slovy prostředek, kterým orgány činné v trestním řízení mohou dospět k přímému poznatku o předmětu dokazování. Prameny důkazu pak Púry definuje jako nositele informace, z níž se čerpá poznatek, který je předmětem dokazování. Je zřejmé, že data uložená ve výpočetní technice tedy mohou sloužit jako prameny důkazů. Orgány činné v trestním řízení si mohou prameny důkazů opatřit a nakládat s nimi prostřednictvím k tomu určených institutů (důkazních prostředků), a to za účelem získání důkazu o nějakém tvrzení relevantním pro trestní řízení. Jako důkaz trestní řád připouští obecně vše, co může přispět k objasnění věci.[9] Zákon uvádí i demonstrativní okruh typických důkazních prostředků.[10]

Púry[11] uvádí, že důkazy se v teorii trestního práva dělí podle svého vztahu k předmětu obvinění na důkazy usvědčující a vyvinující; podle vztahu pramene zpráv o dokazované skutečnosti k této skutečnosti na důkazy původní (bezprostřední) a odvozené (prostředečné); a podle vztahu k dokazované skutečnosti na důkazy přímé a nepřímé. Nepřímý důkaz potvrzuje nebo vyvrací dokazovanou skutečnost pomocí skutečnosti jiné, která s ní souvisí pouze nepřímo. Logicky tak má nepřímý důkaz menší důkazní sílu než důkaz přímý a je tak třeba propojit logickou, ničím nenarušenou a uzavřenou soustavu vzájemně se doplňujících a na sebe navazujících nepřímých důkazů, které jsou ve vzájemné

---

[7] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 46.

[8] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 57.

[9] Srov. § 89(2) trestního řádu.

[10] Ke získání důkaz však mohou posloužit i jiné důkazní prostředky, byť trestní řád nestanovuje zvláštní postup při jejich provádění. Podmínkou je, aby daný důkazní prostředek měl obecné náležitosti úkonu podle trestního řádu a byl způsobilý k prokazování skutečností důležitých pro trestní řízení. Viz POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 58.

[11] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 61.

shodě a spolehlivě dokazují dokazovanou skutečnost, aniž by umožňovaly jiný závěr (souvislost může být třeba i náhodná).[12]

3.1.2 Zásady dokazování

Proces dokazování dle trestního řádu je postaven na několika zásadních zásadách a principech, které určují jeho základní obrysy. V tomto ohledu je přínosné zmínit historické souvislosti, z nichž současná právní úprava trestního řízení vychází. Provazník uvádí, že pro současný model dokazování v českém trestním řízení je určující příslušnost k okruhu kontinentální právní kultury se zřejmým vlivem tradice inkvizičního procesu, který se projevuje ústřední rolí státu ve vedení trestního řízení. To je vnímáno jako spor státu a jednotlivce, přičemž se zásadně liší od civilního řízení, které je vedeno zásadou procesní rovnosti stran a dělením důkazních břemen.[13] V tomto ohledu je třeba připomenout, že současný trestní řád byl přijat v roce 1961, za období komunismu, a je tak postaven na principu ústřední role státu. Trestní řízení v této době bylo pojato jako doména orgánů činných v trestním řízení, kterým byla svěřena odpovědnost za jeho iniciaci a průběh, včetně zjištění skutkového stavu. Orgány činné v trestním řízení v tomto pojetí mají zajišťovat důkazy ve prospěch i v neprospěch, byť obhajoba má možnost činit návrhy na doplnění dokazování.[14] Ačkoliv byl trestní řád po roce 1989 významně novelizován – byla podstatně posílena práva obhajoby a učiněny snahy o zavedení tzv. rovnosti zbraní mezi stranami – model dokazování, za které odpovídají orgány činné v trestním řízení, však zůstal zachován.[15] Zásada rovnosti zbraní mezi veřejnou žalobou a obhajobou se tedy neprojevuje v podobě faktické rovnosti procesních postavení (povaha obhajoby je reakční a defenzivní), ale v podobě kompenzace nevýhod obhajoby některými instituty a zásadami, jako je například presumpce neviny, zásada vyšetřovací, absolutní neúčinnost některých důkazů nebo přítomnost obhájce při zajišťování či provádění důkazů.[16]

S ohledem na předmět a rozsah této práce se nebudeme zabývat zásadami trestního řízení v celé své šíři. V souvislosti se zaměřením této práce se podrobněji zaměříme na zásadu zjištění skutkového stavu bez důvodných pochybností, zásadu vyhledávací a v neposlední řadě na nepřípustnost některých důkazů. Zmíněné zásady nacházejí svůj odraz například v ustanovení § 2 odst. 5 trestního řádu, které stanoví, že orgány činné v trestním řízení postupují tak, aby byl zjištěn skutkový stav

[12] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 64.
[13] KALVODOVÁ, 2015, op. cit., s. 30.
[14] KALVODOVÁ, 2015, op. cit., s. 30.
[15] KALVODOVÁ, 2015, op. cit., s. 31.
[16] KALVODOVÁ, 2015, op. cit., s. 32.

věci, o němž nejsou důvodné pochybnosti, a to v rozsahu, který je nezbytný pro jejich rozhodnutí. V přípravném řízení orgány činné v trestním řízení objasňují způsobem uvedeným v trestním řádu i bez návrhu stran stejně pečlivě okolnosti svědčící ve prospěch i v neprospěch osoby, proti níž se řízení vede.

Ve vztahu k zásadě zjišťování skutkového stavu bez důvodných pochybností Deset poznamenává, že tato historicky nahradila zásadu materiální pravdy, podle které orgány činné v trestním řízení a soudy měly zjišťovat úplnou pravdu o stíhaném trestním činu, bez ohledu na nezbytný rozsah takového zjišťování. Současný přístup však bere ohled na skutečnost, že prostředky sloužící soudci k poznání okolností trestného činu jsou nutně omezené, a uznává, že pravda zjištěná v rámci trestního řízení může být nanejvýš pravdou relativní, nikoliv absolutní. To ale samozřejmě neznamená, že cílem trestního řízení by nemělo být co největší přiblížení tomu, co se skutečně při páchání trestného činu stalo.[17] Zásada zjišťování skutkového stavu bez důvodných pochybností připouští přetrvání určitých pochybností o objasňovaném skutku (činností obhajoby zpravidla budou určité pochybnosti do řízení vneseny), nicméně aby bylo možné vydat konečné rozhodnutí, nesmí být tyto přetrvávající pochybnosti důvodné, tedy takové, které by nebylo možno vysvětlit logickými úvahami soudce v souladu se zásadou volného hodnocení důkazů.[18] K osvětlení skutkového stavu a rozptýlení případných důvodných pochybností mohou v dnešní době často sloužit i důkazy založené na pramenech důkazů v podobě dat uložených ve výpočetní technice.

Pokud jde o zásadu vyhledávací, ta, jak bylo zmíněno výše, vychází z kořenů trestního řízení v inkvizičním procesu a silné role státu v komunistické společnosti, a je se zásadou zjištění skutkového stavu bez důvodných pochybností úzce spjata. Zásada vyhledávací stanoví povinnost orgánů činných v trestním řízení zjišťovat skutečnosti a opatřovat důkazy důležité pro trestní řízení jak ve prospěch, tak neprospěch obviněného, a to i bez návrhu obviněného a bez ohledu na jeho případné doznání. Čep zásadu vyhledávací vymezuje jako povinnost orgánů činných v trestním řízení z vlastní iniciativy vyhledávat a provádět důkazy tak, aby byl zjištěn skutkový stav věci, o němž nejsou důvodné pochybnosti, a v rozsahu nezbytném pro jejich rozhodnutí.[19] Je tedy na policejním orgánu a státním zástupci, aby zajistili data uložená ve výpočetní technice, je-li to pro trestní řízení relevantní.

Nástroje, které jim k tomu trestní řád nabízí, podrobněji rozebereme v pozdější kapitole. Už na tomto místě je však vhodné předeslat, že aby byl důkaz v trestním

[17] KALVODOVÁ, 2015, op. cit., s. 69.
[18] KALVODOVÁ, 2015, op. cit., s. 74.
[19] KALVODOVÁ, 2015, op. cit., s. 85.

řízení použitelný, musí být získán právně přípustným způsobem. Při zajištění důkazů tak musí být zajištěn soulad se všemi relevantními ustanoveními trestního řádu týkajícími se dokazování, aby se z přípustného důkazu nestal důkaz nepřípustný či neúčinný. Stupka v této souvislosti poukazuje na to, že stávající trestní řád je v tomto ohledu zastaralý a neobsahuje žádná specifická ustanovení pro zajišťování elektronických důkazů. Ty jsou proto zajišťovány prostřednictvím stávajících institutů a to začasto postupem v praxi netestovaným a judikatorně nepodloženým, což s sebou nese riziko, že se takto získaný důkaz může stát v trestním řízení nevyužitelný. Vedle absolutně nepřípustných důkazů[20] mohou být důkazy v trestním řízení absolutně či relativně neúčinné (podle toho, lze-li takovou vadu odstranit) i z jiných důvodů.[21] Stupka k tomu podotýká, že byť jsou z důvodu důrazu na ochranu práv obviněného tyto instituty vykládány poměrně extenzivně, praxe při zajišťování elektronických důkazních prostředků orgány činnými v trestním řízení je značně nejednotná. Využívány jsou různé procesní nástroje s přihlédnutím nejen k charakteru konkrétního důkazního prostředku, ale také v závislosti na zkušenostech konkrétního vyšetřovatele či požadavcích osoby, která má důkazní prostředek poskytnout.[22] Byť tedy situace není jednoznačná a dostatečně podložená judikaturou, v kapitole 3.3 se pokusíme shrnout současný stav a doporučení pro praxi. Situaci by významně prospěla novelizace trestního řádu a přijetí specifících procesních institutů pro zajišťování elektronických důkazů. Ostatně není třeba vynalézat kolo – Česká republika se k přijetí takové právní úpravy zavázala svým přistoupením k tzv. Budapešťské úmluvě.[23]

3.2 Data jako důkaz

Dříve, než se podrobněji zaměříme na jednotlivé procesní prostředky, jejichž prostřednictvím je možné prameny důkazů v podobě dat uložených ve výpočetní technice zajistit, je vhodné prozkoumat, jakou podobu tyto prameny důkazů mohou mít, kde mohou být uložena a v čem mohou být v rámci dokazování v průběhu trestního řízení užitečná.

Data uložená ve výpočetní technice lze kategorizovat jako elektronické prameny důkazů. Stupka podotýká, že ačkoliv pojem elektronické důkazní prostředky v současně platné právní úpravě není nikde definován ani zmíněn, lze pod ním obecně rozumět takové důkazní prostředky, k jejichž převodu do podoby

---

[20] Typicky důkaz získaný nezákonným donucením, viz § 89 odst. 3 trestního řádu.

[21] POLČÁK, Radim a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 572.

[22] KALVODOVÁ, 2015, op. cit., s. 315.

[23] *Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě* [online]. Sbírka mezinárodních smluv č. 104/2013 ze dne 23. 12. 2013 [cit. 12. 12. 2019].

srozumitelné pro člověka je třeba použít nějaké elektronické zařízení.[24] S ohledem na mohutný technický rozmach a začlenění prostředků výpočetní techniky do takřka všech aspektů našich každodenních životů, je zřejmé, že data uložená na těchto zařízeních na nás mohou mnoho prozradit a mohou tak často sloužit i jako velmi výmluvný pramen důkazů.

Pokud jde o různé kategorie dat, Stupka uvádí základní dělení na data, která přímo obsahují nějaké informace (elektronické dokumenty, které obsahují informace aktivně zadané člověkem, jejich metadata a provozní data vytvořená aplikacemi), a aplikace.[25] Jako prameny důkazů mohou obvykle sloužit zejména dokumenty a jejich metadata, případně provozní data aplikací. Aplikace samotné mohou být za určitých okolností také relevantním pramenem důkazů, ovšem to se týká spíše specifických trestných činů.[26] Kothánek uvádí příkladmý výčet toho, jaká data potenciálně relevantní pro trestní řízení lze z výpočetní techniky vytěžit. V současné době se jedná především o komunikaci na internetu, ať už e-mailovou komunikaci, komunikaci skrze chatovací aplikace a aplikace pro instant messaging (ICQ, Google Hangouts, Messanger, Telegraf, Skype aj.) či komunikaci na sociálních sítích (Facebook, Twitter, Instagram aj.).[27] Jako užitečný pramen důkazů mohou sloužit nejrůznější textové dokumenty, tabulky, prezentace v nejrůznějších formátech (dokumenty kancelářských balíků Microsoft Office, Libre Office, Open Office aj.), včetně dokumentů ve formátu PDF. Jako prameny důkazů mohou sloužit také multimediální soubory zvukové (MP3, WAV, WMA, OGG, RMA, FLAC aj.), obrazové (JPG, TIFF, BMP, GIF, DRW, SVG aj.) či video soubory (WMV, MP4, MOV, AVI aj.).[28] Jako užitečná se pro účely dokazování mohou ukázat i data o připojení k internetu a sítím obecně (jako je IP adresa, výchozí brána, název počítače v síti či MAC adresa), která jsou uložena v registrech operačního systému. [29]

Soubory, které mohou být důležité pro konkrétní trestní řízení a jsou proto předmětem zajištění a následné forenzní analýzy a dokazování, se nazývají zájmové soubory. Kothánek podotýká, že rozsah zájmových souborů se liší případ od případu v závislosti na řešené trestné činnosti. V případě hospodářské trestné činnosti budou typicky důležité soubory, které mohou obsahovat účetnictví či faktury, a dále e-mailová komunikace a internetová historie se zaměřením na finanční transakce v internetovém bankovnictví. Naopak při řešení případů dětské pornografie budou

[24] KALVODOVÁ, 2015, op. cit., s. 312.

[25] KALVODOVÁ, 2015, op. cit., s. 313.

[26] Např. trestná činnost související s hackingem či porušováním autorských práv.

[27] V případě chytrých mobilních telefonů (které samozřejmě také spadají do kategorie výpočetní techniky) lze navíc zmínit i SMS a MMS zprávy či zprávy typu iMessage aj.

[28] S ohledem na nepřeberné množství typů souborů je zpravidla do forenzní analýzy nutno zahrnout veškeré známé formáty, aby došlo ke komplexní analýze.

[29] KOTHÁNEK, Jakub. Vytěžování důkazů z výpočetní techniky [online]. Brno, 2014 [cit. 10. 10. 2019]. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA. s. 39an.

zájmovými soubory především fotografie a videa a dále pak veškerá komunikace. Při vyhledávání se přitom nelze spoléhat na ruční vyhledávání například pomocí přípony souboru. Existuje totiž velké množství různých formátů a navíc příponu souboru lze jednoduše měnit. Pro vyhledávání se proto používají speciální forenzní nástroje, které soubory prohledávají pomocí jejich typických příznaků.[30]

Dalším aspektem je pak otázka, kde jsou data uložen – mohou se nacházet buď přímo v paměti počítače či jiného obdobného elektronického zařízení, jako jsou chytré mobilní telefony či například fotoaparáty. V případě počítačů se bude typicky jednat o pevné disky typu HDD či SSD, v případě jiných elektronických zařízení o jistý typ integrované paměti (obvykle paměti na bázi technologie Flash). Data se rovněž mohou nacházet na nejrůznějších přenosných paměťových médiích, ať už jde o optické disky (CD, DVD, Blu-Ray), paměti typu flash (USB klíčenky, paměťové karty), či některé staré typy paměťových médií, jako jsou diskety. Vedle toho mohou jako přenosná paměťová média složit i externí pevné disky typu HDD či SSD. V dnešní době rovněž narůstá význam ukládání dat tzv. v cloudu, tedy na infrastruktuře třetích stran prostřednictvím sítě Internet. Místo uložení zájmových souborů také ovlivňuje volbu procesního nástroje pro jejich zajištění. V případě dat uložených na paměťových médiích je obvykle nezbytné fyzicky zajistit přímo předmětný nosič dat. V případě dat cloudu či dat uložených na zařízeních připojených k síti Internet je za určitých okolností možné data zajistit i vzdáleným způsobem, popřípadě od poskytovatele služby. Stupka[31] uvádí, že v případě počítačů mohou jako prameny důkazů posloužit i vstupní a výstupní zařízení, procesor, paměť RAM či systémový a aplikační software. Tuto problematiku podrobněji prozkoumáme v následující kapitole.

3.3 Způsob zajištění dat

Stupka[32] uvádí možné způsoby získání počítačových dat: zajištění zařízení nebo datových nosičů, získání přístupu k počítačovým datům, anebo získání dat od poskytovatelů služeb. Jednou možností je tedy získání samotného zařízení výpočetní techniky jako takového, popřípadě paměťových médií. V případě dat uložených v chytrých mobilních telefonech či na tabletech může být alternativou i získat přístup k zařízení, se kterým se toto mobilní zařízení synchronizuje. Další možností je vzdálené získání dat, která zařízení uložilo nebo vytvořilo – ať už přímo ze samotného zařízení jako takového, anebo třeba z připojeného cloudového

[30] KOTHÁNEK, 2014, op. cit., s. 54.

[31] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 83.

[32] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 101.

úložiště. Do této kategorie spadá odposlech. Poslední možností je získání požadovaných dat od operátora či poskytovatele dané služby.

Jak už bylo zmíněno výše, literatura obecně akcentuje problematičnost stávajícího stavu, kdy trestní řád neobsahuje žádná ustanovení týkající se zajišťování elektronických důkazních prostředků a orgány činné v trestním řízení jsou odkázání na užití obecných procesních postupů.[33] Stupka přitom upozorňuje na problematičnost stávajícího postupu, kdy je existující doktrína pro zajišťování hmotných důkazních prostředků analogicky aplikována na vyšetřování trestných činů založených na využití prostředků informačních a komunikačních technologií. Podotýká, že v mnoha případech je dokazování znemožněno nebo znesnadněno, zatímco v jiných ohledech je vyšetřování naopak limitováno nedostatečně a jsou tak ohrožena práva občanů.[34] Tento stav s sebou nese i nejednotnost aplikace stávajících procesních prostředků. Kothánek například uvádí, že se na základě konzultací s policisty dozvěděl, že e-mailová komunikace bývá někdy zajišťována také dle § 158d trestního řádu upravujícího sledování osob a věcí. Obdobná situace je dle Kothánka i na soudech, kdy například v Praze některé obvodní soudy vydávají povolení na základě § 88a trestního řádu a některé právě na základě zmíněného § 158d trestního řádu.[35] Tato nejednotnost je samozřejmě nežádoucí. Kothánek v této souvislosti upozorňuje na skutečnost, že Česká republika dne 22. srpna 2013 ratifikovala budapešťskou Úmluvu o počítačové kriminalitě a český právní řád by proto měl být s touto úmluvou uveden do souladu a měla by být zavedena procesní ustanovení týkající se specifik počítačových dat.[36]

V současné době jsou použitelnými důkazními prostředky pro získání pramene důkazu vydání[37] či odnětí[38] věci pro důkazní účely, domovní či osobní prohlídka či prohlídka pozemků a prostor nesloužících k bydlení.[39] Tímto způsobem lze získat přímo zařízení, na kterém jsou data uložena, popřípadě i jiné nosiče nebo zařízení, která mohou zájmová data buď přímo obsahovat, nebo k nim umožňovat přístup (např. ke cloudovému úložišti). Takto získaný pramen důkazu je pak následně

[33] POLČÁK, Radim; Jiří ČERMÁK; Zbyněk LOEBL, a kol. *Cyber law in the Czech Republic*. 2. vyd. Alphen aan den Rijn : Kluwer Law International, 2015. s. 223.

[34] KALVODOVÁ, 2015, op. cit., s. 311.

[35] KOTHÁNEK, 2014, op. cit., s. 11.

[36] KOTHÁNEK, 2014, op. cit., s. 60.

[37] Viz § 78 trestního řádu.

[38] Viz § 79 trestního řádu.

[39] Viz § 82 až 85b trestního řádu.

podroben ohledání,[40] popřípadě znaleckému zkoumání či odbornému vyjádření.[41] Data je však možné získat i nepřímo, a to především pomocí operativně pátracího prostředku sledování osob a věcí,[42] nebo institutu odposlechu a záznam telekomunikačního provozu[43] či vyžádání údajů o uskutečněném telekomunikačním provozu.[44] Jednotlivým procesním institutům se budeme podrobněji věnovat níže.

Použití výše uvedených důkazních prostředků samozřejmě představuje zásadní zásah do práv a svobod. Polčák k tomu uvádí, že schizofrenní je role státu, „*který má na jedné straně chránit člověka před negativními důsledky přirozeného, avšak poněkud překotného technického vývoje, majícího za následek bezprecedentní expozici soukromí a na straně druhé má implicitní povinnost využít nově dostupných dat k tomu, aby plnil své základní funkce (tj. chránil člověka a společnost před chaosem).“*[45] Proto je zásadní při použití důkazních prostředků striktně zajistit zákonnost v zájmu zajištění práva na spravedlivý proces. Trestní řád dokonce v § 89 odst. 3 výslovně stanoví, že důkaz získaný nezákonným donucením nebo hrozbou takového donucení nesmí být v řízení použit. Púry[46] uvádí, že nepřípustný je i důkaz opatřený při provádění nezákonného procesního úkonu (např. získání věci při nepovolené domovní prohlídce). Pro zajištění pramene důkazu tak musí být použit správný procesní postup (správný důkazní prostředek), neboť podstatné vady řízení[47] mohou mít za následek absolutní nebo relativní neúčinnost důkazu.[48]

3.3.1 Přímý přístup k datům (fyzické získání)

Samotnou výpočetní techniku, či datové nosiče (paměťové karty, disky počítače se zálohou) a simkarty, lze zajistit vydáním nebo odejmutím, popřípadě v rámci domovní či osobní prohlídky či prohlídky nebytových prostor.[49] Stupka uvádí, že tímto způsobem lze získat přístup k zařízení nebo datovému nosiči jako takovému,

---

[40] Viz § 113 trestního řádu.

[41] Viz § 105 až 111 trestního řádu.

[42] Viz § 158d trestního řádu.

[43] Viz § 88 trestního řádu.

[44] Viz § 88a trestního řádu.

[45] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 19.

[46] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 61.

[47] Viz § 258(1)(a) trestního řádu, který hovoří o podstatných vadách řízení, „*které rozsudku předcházelo, zejména proto, že v tomto řízení byla porušena ustanovení, jimiž se má zabezpečit objasnění věci nebo právo obhajoby, jestliže mohly mít vliv na správnost a zákonnost přezkoumávané části rozsudku*“.

[48] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 100.

[49] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 101.

ale také k v nich obsaženým datům[50] nebo jen k listinným důkazům vytvořeným na jejich základě.[51, 52] Pejčochová a Elbert[53] uvádějí, že výpočetní technika (a veškerá data na ní uložená) je v rámci trestního řízení vnímána jako jakékoliv jiné věci, přičemž orgány činné v trestním řízení mohou data uložená v zajištěné výpočetní technice v okamžiku zajištění vytěžit a použít k provedení důkazů, aniž by k tomu potřebovaly svolení soudu.[54] To se samozřejmě týká i jiných věcí, které mohou nést uložená data (např. záloha mobilního komunikačního zařízení na počítači nebo SD karta, která byla s mobilním komunikačním zařízením použita). Podmínkou však je, že dané předměty nesmějí mít povahu zpráv uchovávaných v soukromí. Stupka tak upozorňuje na specifickou situaci dat, která jsou předmětem komunikace, jako je třeba textová nebo emailová zpráva nebo vzkaz na Skypu či ICQ.[55] Jednorázové zajištění těchto dat se realizuje prostřednictvím operativně pátracího prostředku sledování věci dle § 158d odst. 3 trestního řádu, zatímco ke sledování další komunikace, která se uskuteční teprve v době po zajištění, je třeba souhlas s nasazením odposlechu a záznamu telekomunikačního provozu ve smyslu § 88 trestního řádu.

Při provádění zajištění výpočetní techniky, zejména v případě využití institutu domovní prohlídky, je dle Kothánka nezbytné postupovat rychle, aby nedošlo ke ztrátě důkazů, přičemž taková prohlídka vyžaduje speciální přípravu, aby se předešlo poškození nebo dokonce vymazání dat. Počítač může být nastaven tak, že zmáčknutím jediné klávesy vymaže všechna uložená data, popřípadě v hrozí nebezpečí manipulace s daty z vnějšku prostřednictvím vnitřní sítě nebo sítě Internet. Zajištění výpočetní techniky by proto měl být přítomen specialista, který všechny úkony pečlivě zdokumentuje,[56] aby postup nemohl být následně napadnut a autenticita dat či odborná manipulace zpochybněna.[57] Konkrétní postupy, jak digitální techniku zajistit, aby nedošlo k poškození důkazního materiálu, se liší

[50] V takovém případě nemusí dojít k zajištění zařízení nebo nosiče, ale je pouze vytvořena tzv. bitová kopie zájmových dat.

[51] Listinné důkazy v podobě výtisků e-mailových zpráv, nebo fotografií zachycujících obsah e-mailové zprávy na monitoru.

[52] KALVODOVÁ, 2015, op. cit., s. 316.

[53] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 210.

[54] Okamžikem doručení zprávy příjemci totiž zpráva přestává požívat zvýšené ochrany přenášené zprávy podle čl. 13 Listiny základních práv a svobod. Viz Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky. In: *Zákony pro lidi* [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019].

[55] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 105.

[56] Dokumentace by měla zahrnovat veškeré detaily, jako např. zapojení techniky do sítě, zapojení disků, připojení dalších zařízení apod. Viz KOTHÁNEK, 2014, op. cit., s. 11.

[57] KOTHÁNEK, 2014, op. cit., s. 24.

s ohledem na konkrétní okolnosti případu a nelze vždy dodržet všechny požadavky a poučky. Kothánek jako příklad uvádí, že v případě hackerského útoku na počítačový systém či v případě zajištění šifrovaného disku je přednější zajistit informace z operační paměti pomocí vytvoření bitových kopií pamětí RAM, než dostát požadavku, že data by neměla být nijak modifikována. Stejně tak neexistuje jednoznačné pravidlo, jak zajistit spuštěnou techniku. V jednom případě je vhodné digitální techniku odpojit od elektrické energie, v jiném případě ji standardně vypnout. U mobilních telefonů existuje riziko, že pokud jej necháme zapnutý, pachatel může dálkově smazat data. Pokud jej však vypneme, bez znalosti přístupových kódů riskujeme, že se k informacím v něm uloženým již nemusíme dostat.[58] Svetlík[59] podotýká, že v dnešní době nelze zajistit nepozměnění originální datové stopy, neboť v podstatě neexistuje způsob, jak z výpočetní techniky zajistit data, aniž by na zařízení došlo k nějakým změnám. Provedení minimálních a dobře zdokumentovaných a odůvodněných změn ovšem nemusí být s požadavkem zachování integrity digitální stopy nutně v rozporu.[60] Z tohoto důvodu je naprosto klíčové klást důraz na nezávislost a profesionalitu osoby, která digitální stopy z mobilního komunikačního zařízení zajišťuje. V opačném případě je totiž riziko, že důkaz nebude připuštěn jako dovolený z důvodů narušení principu legality, popřípadě že pro své nedostatky neprojde sítem volného hodnocení důkazů.

3.3.2 Vzdálený přístup

Další možností, jak získat přístup k datům generovaným výpočetní technikou či v ní uloženým, popřípadě datům týkajícím se takové techniky, je získat je prostřednictvím vzdáleného přístupu k datům. V takovém případě je třeba rozlišovat mezi přístupem k datům volně dostupným a datům, která volně dostupná nejsou.[61] Volně dostupná data lze v rámci dokazování využít bez omezení.[62] Kothánek uvádí, že při zajišťování veřejně přístupných dat ze sítě Internet lze tato data standardním způsobem zajistit s využitím speciálního programového vybavení, které simuluje a dokumentuje prohlížení internetových stránek. Zadokumentována jsou však pouze data, která jsou prezentována internetovým prohlížečem na lokální stanici uživatele, nikoliv veškerá data uložená na daném serveru. Ten přitom může obsahovat data, která nemusí být veřejně přístupná, případně mohou být maskována takovým způsobem, aby byl k nim byl omezen

[58] KOTHÁNEK, 2014, op. cit., s. 34.

[59] SVETLÍK, Marián. Analýza mobilních zařízení s důrazem na využití JTAG. *Digital forensic review* [online]. 2017, roč. 1, č. 1 [cit. 6. 8. 2018]. ISSN 2570-5059.

[60] SVETLÍK, 2017, op. cit., s. 17.

[61] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 104.

[62] Například informace z fotografie uložené na veřejném profilu na sociální síti.

přístup policii či například z určitého státu.[63] Pokud jde o data, která volně dostupná nejsou,[64] ta jsou považována za záznamy uchovávané v soukromí ve smyslu § 158d odst. 3 trestního řádu a mohou být jako důkaz použity pouze v případě, že soudce udělil souhlas k užití operativně pátracího prostředku sledování věci dle § 158d odst. 3 trestního řádu (popřípadě se souhlasem osoby, do jejíchž práv a svobod je tímto zasahováno).[65, 66] I v takovém případě je třeba rozlišovat mezi zprávami doručenými a nedoručenými v okamžiku zajištění, přičemž ve druhém případě se uplatní postup dle § 88 trestního řádu.[67]

Ve vztahu k zajišťování dat uložených ve výpočetní technice je třeba podotknout, že institut odposlechu telekomunikačního provozu se netýká čistě jen hlasové komunikace,[68] ale veškeré komunikace uskutečňované prostřednictvím telekomunikačních sítí a sítí elektronických komunikací mezi konečným počtem uživatelů.[69] Prostřednictvím odposlechu tak lze zachytit jakákoliv data přenášená prostřednictvím telekomunikačních sítí a sítí elektronických komunikací. S ohledem na skutečnost, že se jedná o velmi výrazný zásah do soukromí odposlouchávaných osob ústavně garantované práva na ochranu poštovního tajemství a tajemství přepravovaných zpráv, je takový zásah možný jen za podmínek a v mezích stanovených zákonem.[70] Použití odposlechu a záznamu telekomunikačního je tak přípustné pouze v případě závažnější trestné činnosti[71] a to pouze na základě principu subsidiarity, tedy nelze-li požadovaných výsledků dosáhnout jiným způsobem. Odposlech nařizuje předseda senátu a v přípravném řízení na návrh státního zástupce soudce.[72]

---

[63] KOTHÁNEK, 2014, op. cit., s. 37.

[64] A je irelevantní, zda se jedná o zajištění heslem, anebo jsou tyto údaje uloženy mimo mobilní telefon v cloudové službě. Pouhá skutečnost, že je mobilní komunikační zařízení k účtu cloudové služby přihlášen, neopravňuje orgány činné v trestním řízení tyto údaje bez dalšího vytěžovat. Srov. POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 213.

[65] To platí i v případě, že orgány činné v trestním řízení získají přístupové údaje jiným způsobem, např. nálezem nebo prolomením. POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 104.

[66] Kothánek uvádí, že v případě neveřejných dat lze také využít institutu dožádání dle § 8 odst. 1 trestního řádu a požádat poskytovatele služby o zadokumentování stavu serveru k dalšímu opatření. Viz KOTHÁNEK, 2014, op. cit., s. 37.

[67] Srov. POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 214.

[68] Typicky prostřednictvím telefonu či vysílaček.

[69] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 183an.

[70] KALVODOVÁ, 2015, op. cit., s. 223.

[71] Výčet trestných činů je obsažen v § 88 odst. 1 trestního řádu.

[72] Srov. § 88 odst. 2 trestního řádu.

3.3.3 Získání od třetí osoby

Posledním způsobem je získání požadovaných dat od poskytovatelů služeb. Dle Stupky[73] je třeba rozlišovat jednak mezi různými typu poskytovatelů služeb, a jednak i s ohledem na charakter žádaných dat. Rozdílný režim se uplatní v případě poskytovatelů telekomunikačních služeb,[74] kteří poskytují infrastrukturu veřejné komunikační sítě nebo poskytují připojení k takové síti, a poskytovatelů služeb informační společnosti,[75] kteří elektronickými prostředky a prostřednictvím infrastruktury a připojení poskytovatelů telekomunikačních služeb poskytují na individuální žádost uživatele konkrétní služby. Obecně platí, že data, která nepodléhají povinnosti mlčenlivosti mohou být dožádána prostřednictvím § 8 odst. 1 trestního řádu. Jestliže ale předmětná data mají charakter záznamů uchovávaných v soukromí (například proto, že jsou chráněna heslem), je třeba postupovat podle § 158d odst. 3 trestního řádu. Zvláštní právní úprava se pak uplatní v případě poskytovatelů telekomunikačních služeb, kteří mají povinnost uchovávat tzv. provozní a lokalizační údaje.[76] Tyto provozní a lokalizační údaje[77] je možné za specifických podmínek získat postupem dle § 88a trestního řádu. Pokud jde o data tvořící obsah komunikace prostřednictvím sítě elektronických komunikací, je k jejich odposlechu nebo zachytávání v průběhu jejich přenosu, stejně jako v případě zpráv došlých po zajištění mobilního komunikačního zařízení, třeba postupovat podle § 88 trestního řádu. Postupem dle § 88 a 88a trestního řádu lze navíc postupovat jen při stíhání určitých trestných činů.

Pokud jde o posledně dva jmenované instituty, je třeba poznamenat, že povahu metadat mají především provozní a lokalizační údaje ve smyslu § 88a trestního řádu. Na druhou stranu metadata mohou být i předmětem odposlechu komunikace ve smyslu § 88 trestního řádu, jestliže se jedná o metadata, která tvoří součást přenášené komunikace (z hlediska poskytovatele telekomunikačních služeb se jedná o obsahová data, zatímco z hlediska uživatele se může jednat o metadata). V této souvislosti je třeba upozornit, že dle některých výkladů lze pod údaje o

---

[73] POLČÁK, 2015, *Elektronické důkazy v trestním řízení,* op. cit., s. 106.

[74] Ve smyslu zákona č. 127/2005 Sb., č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů. In: Zákony pro lidi [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019].

[75] Ve smyslu zákona č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů. In: Zákony pro lidi [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019].

[76] Ve smyslu § 90 a 91 zákona č. 127/2005 Sb., o elektronických komunikacích.

[77] Podrobněji k pojmům provozní a lokalizační údaj v souvislosti s institutem data retention viz MYŠKA, Matěj. *Právní aspekty uchovávání provozních a lokalizačních údajů* [online]. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2013, 136 s. [cit. 2. 1. 2020].

telekomunikačním provozu dle § 88a trestního řádu zahrnout i obsah e-mailových zpráv.[78] Autor se však domnívá, že takový výklad je nepřípustně extenzivní a vzhledem ke skutečnosti, že emailové zprávy mají povahu zpráv uchovávaných v soukromí, je žádoucí trvat na uplatnění právní úpravy odposlechu podle § 88 trestního řádu.

3.4 Co dál – zpracování, analýza, dokazování

Jakmile jsou data jako prameny důkazů některým z výše uvedených způsobů zajištěna, lze přistoupit k jejich praktickému využití k zamýšlenému účelu, tedy poskytnutí informace důležité pro rozhodování v trestním řízní – za tímto účelem je třeba důkazy před soudem provést. V případě elektronických důkazů se nabízí několik možností jejich provedení – v jednodušších případech je lze provést jako věcné či listinné důkazy,[79] ve složitějších případech je možné vyžádat si odborné vyjádření[80] či přibrat znalce.[81] S ohledem na klíčový rys elektronických důkazů – tedy že nejsou pro člověka bez dalšího srozumitelné a přímo vnímatelné – je nezbytné zajistit jejich převod do pro člověka smyslově vnímatelné podoby Pro získávání důkazu z elektronického důkazního prostředku je třeba zvolit vhodné prostředky, jejichž prostřednictvím získáme veškeré údaje, které mohou být pro trestní řízení relevantní. Stupka jako příklad uvádí provedení věcného důkazu zobrazením webové stránky prostřednictvím webového prohlížeče na straně jedné a použití pouhého výtisku takto interpretované webové stránky jako důkazu listinného. Ve druhém případě přicházíme o možná relevantní informace obsažené ve zdrojovém kódu nebo v metadatech.[82]Navíc je třeba podotknout, že ani provedení věcného důkazu nemusí být samo o sobě dostatečné. V některých případech je vhodné vyžádat si odborné vyjádření, anebo znalecký posudek. Dle Kothánka je odborné vyjádření základním institutem trestního řádu pro odborné otázky, přičemž znalec má být přibrán pouze v případě, kdy odborné vyjádření není s ohledem na složitost věci dostačující.[83] Znalecký posudek může být poskytnut znalcem jmenovaným Ministerstvem spravedlnosti nebo předsedou krajského soudu, popřípadě znaleckým ústavem. Znalec může poskytnout posudek typicky ohledně autenticity, integrity zajištěných dat a způsobu, jakým s nimi bylo nakládáno, popřípadě zda s nimi nebylo nezákonně manipulováno.[84] Svetlík

[78] KALVODOVÁ, 2015, op. cit., s. 316.
[79] Dle § 112 trestního řádu.
[80] Dle § 105 trestního řádu.
[81] Dle § 105 trestního řádu.
[82] KALVODOVÁ, 2015, op. cit., s. 314.
[83] KOTHÁNEK, 2014, op. cit., s. 27.
[84] POLČÁK, 2015, *Cyber law in the Czech Republic*, op. cit., s. 225.

vypočítává základní aspekty činnosti soudního znalce – provádění forenzní analýzy[85] – jako nezávislost, profesionalita, opakovatelnost, přezkoumatelnost, integrita, legalita a dokumentace. To jsou všechno aspekty, které je třeba brát v úvahu v zájmu zajištění toho, aby důkaz mohl být u soudu účinně použit.

[85] SVETLÍK, Marián. Základní atributy forenzní analýzy. *Digital forensic review* [online]. 2018, roč. 2, č. 4, s. 5-13 [cit. 6. 8. 2018].

4 Shrnutí získaných poznatků a návrh doporučení

Z výše uvedeného je zřejmé, že pro zdárný průběh trestního řízení je naprosto klíčové, aby byla ve všech fázích získávání pramenů důkazů a provádění důkazů striktně zajištěna zákonnost. Zajišťování pramenů důkazů totiž často představuje významný zásah do práv a svobod. Aby byl důkaz v trestním řízení použitelný, musí být získán právně přípustným způsobem. Problematické je, že stávající trestní řád neobsahuje žádná specifická ustanovení pro zajišťování elektronických důkazů a ty jsou proto zajišťovány na základě analogické aplikace stávajících důkazních prostředků. Současná praxe je však roztříštěná a jsou využívány různé procesní nástroje s přihlédnutím nejen k charakteru konkrétního důkazního prostředku, ale také v závislosti na zkušenostech konkrétního vyšetřovatele a jiných okolnostech.

Orgány činné v trestním řízení si musí být vědomi, kde jsou nebo mohou být data uložena – ta se mohou nacházet buď přímo v paměti počítače či jiného obdobného elektronického zařízení, jako jsou chytré mobilní telefony či například fotoaparáty, na nejrůznějších přenosných paměťových médiích, ať už jde o optické disky (CD, DVD, Blu-Ray), paměti typu flash (USB klíčenky, paměťové karty), či některé staré typy paměťových médií, jako jsou diskety, dále pak externí pevné disky typu HDD či SSD a v dnešní době rovněž tzv. v cloudu, tedy na infrastruktuře třetích stran přístupné prostřednictvím sítě Internet. Místo uložení zájmových souborů ovlivňuje volbu procesního nástroje pro jejich zajištění.

Pokud jde o možné způsoby získání počítačových dat, orgány činné v trestním řízení mohou zajistit zařízení nebo datové nosiče jako takové, získat přístupu k počítačovým datům vzdáleným způsobem, popřípadě je získat od poskytovatelů služeb.

V případě přímého získání počítačových dat uložených na zařízeních či médiích jsou použitelnými důkazními prostředky instituty vydání či odnětí věci pro důkazní účely, domovní či osobní prohlídka či prohlídka pozemků a prostor nesloužících k bydlení. Tyto instituty zajišťují přístup nejen k zařízení nebo datovému nosiči jako takovému, ale také k v nich obsaženým datům nebo k listinným důkazům vytvořeným na jejich základě. To však platí pouze v případě, že dané předměty nemají povahu zpráv uchovávaných v soukromí. Data, která jsou předmětem komunikace, jako třeba textová nebo emailová zpráva nebo vzkaz na Skypu či ICQ, mají povahu zpráv uchovávaných v soukromí a jejich jednorázové zajištění se realizuje prostřednictvím operativně pátracího prostředku sledování věci, zatímco ke sledování další komunikace, která se uskuteční teprve v době po zajištění, je třeba souhlas s nasazením odposlechu a záznamu telekomunikačního provozu.

V případě získání dat vzdáleným způsobem je třeba rozlišovat mezi přístupem k datům volně dostupným a datům, která volně dostupná nejsou. Volně dostupná data lze v rámci dokazování využít bez omezení, avšak data, která volně dostupná nejsou,

jsou považována za záznamy uchovávané v soukromí a mohou být jako důkaz použity pouze v případě, že soudce udělil souhlas k užití operativně pátracího prostředku sledování věci. Opět je pak třeba rozlišovat mezi zprávami doručenými a nedoručenými v okamžiku zajištění, přičemž ve druhém případě se uplatní postup určený pro odposlech telekomunikačního provozu. Institut odposlechu telekomunikačního provozu se přitom netýká čistě jen hlasové komunikace, ale veškeré komunikace uskutečňované prostřednictvím telekomunikačních sítí a sítí elektronických komunikací mezi konečným počtem uživatelů. Prostřednictvím odposlechu tak lze zachytit jakákoliv data přenášená prostřednictvím telekomunikačních sítí a sítí elektronických komunikací. či vyžádání údajů o uskutečněném telekomunikačním provozu.

Třetí možností je získání zájmových dat od poskytovatelů služeb. Data, která nepodléhají povinnosti mlčenlivosti mohou být dožádána**.** Naopak v případě záznamů uchovávaných v soukromí – například chráněných heslem – je třeba postupovat prostřednictvím operativně pátracího prostředku sledování osob a věci. Zvláštní právní úprava se pak uplatní v případě poskytovatelů telekomunikačních služeb, kteří mají povinnost uchovávat tzv. provozní a lokalizační údaje.

Při provádění zajištění výpočetní techniky, zejména v případě využití institutu domovní prohlídky, je nezbytné postupovat s patřičnou odborností a je proto žádoucí přizvat k úkonu odborně způsobilou osobu – ať už vyškoleného policistu, anebo znalce v oboru výpočetní techniky. Je třeba postupovat rychle a po pečlivé přípravě, aby nedošlo ke ztrátě či poškození důkazů, a veškeré korky dokumentovat.

Pro samotné získávání důkazu z elektronického důkazního prostředku je třeba zvolit vhodné prostředky, jejichž prostřednictvím získáme veškeré údaje, které mohou být pro trestní řízení relevantní. Provedení věcného důkazu nemusí být samo o sobě dostatečné. V některých případech je vhodné vyžádat si odborné vyjádření, anebo znalecký posudek.

Obecně lze říct, že ačkoliv současná právní úprava implicitně umožňuje zajišťování elektronických pramenů důkazů uložených ve výpočetní technice, situaci by významně prospěla novelizace trestního řádu a přijetí specifických procesních institutů pro zajišťování elektronických důkazů. Česká republika se přitom k přijetí takové právní úpravy zavázala svým přistoupením k tzv. Budapešťské úmluvě o počítačové kriminalitě a český právní řád by proto měl být s touto úmluvou uveden do souladu a měla by být zavedena procesní ustanovení týkající se specifik počítačových dat.

5 Závěr

V této stati jsme se zabývali problematikou zajišťování dat uložených ve výpočetní technice v rámci trestního řízení. Ukázali jsme, že s ohledem na mohutný technický rozmach a začlenění prostředků výpočetní techniky do takřka všech aspektů našich každodenních životů na nás mohou data uložená na těchto zařízeních mnoho prozradit, a to mimo jiné i v rámci procesu dokazování v rámci trestního řízení. Rozebrali jsme, jakou podobu mohou prameny důkazů uložené ve výpočetní technice mít, kde mohou být uloženy a v čem mohou být v rámci dokazování v průběhu trestního řízení užitečné. S ohledem na zajištění zákonnosti a práva na spravedlivý proces jsme rozebrali, na základě kterých institutů trestního řádu mohou orgány činné v trestním řízení prameny důkazů spočívající v datech uložených ve výpočetní technice za účelem získání důkazu o nějakém tvrzení relevantním pro trestní řízení opatřit a nakládat s nimi. Argumentovali jsme zároveň, že ačkoliv současná právní úprava implicitně umožňuje dokazování za užití elektronických pramenů důkazů, děje se tak pouze na základě analogické aplikace obecných institutů, které nejsou specifickým vlastnostem elektronických pramenů důkazů přizpůsobeny. Uvedli jsme, že by bylo vhodné českou právní úpravu novelizovat tak, aby odrážela specifické důkazní prostředky pro nakládání s elektronickými prameny důkazů. Vhodné by v tomto ohledu bylo implementovat procesní ustanovení budapešťské Úmluvy o počítačové kriminalitě.

Summary

Given the massive technical boom and the incorporation of information technology into almost every aspect of our daily lives, it is clear that the data stored on these devices can tell a lot about us. This may prove true, inter alia, in the context of criminal proceedings where data stored in information technology can serve as eloquent sources of evidence, enabling law enforcement authorities to reconstruct the facts of the crime to the extent required by the law for a substantive decision on guilt and punishment or for claims of the victim. Criminal law enforcement authorities can obtain sources of evidence and handle them through institutes of criminal law for taking evidence. In order to be usable in criminal proceedings, evidence must be obtained in a legally permissible manner. Thus, in obtaining evidence, compliance with all relevant provisions of the Code of Criminal Procedure concerning the taking of evidence must be ensured, so that admissible evidence does not become inadmissible or ineffective. However, the current legislation is obsolete in this respect and does not contain any specific provisions for the securing of electronic evidence. These are therefore ensured through the existing institutes, often by a procedure that has not been tested in practice and unfounded in law, which carries the risk that the evidence thus obtained may become unusable in criminal proceedings. This paper focuses on the issue of securing data stored in information technology for the purpose of providing evidence in criminal proceedings.

Použité zdroje

Monografie

- KALVODOVÁ, Věra; HRUŠÁKOVÁ, Milana a kol. *Dokazování v trestním řízení – právní, kriminologické a kriminalistické aspekty* [online]. 1. vyd. Brno : Masarykova univerzita, Právnická fakulta, 2015, 503 s. [cit. 12. 10. 2019]. ISBN 978-80-210-8072-0. Dostupné z: http://science.law.muni.cz/knihy/monografie/Kalvodova_Dokazovani.pdf

- POLČÁK, Radim; PÚRY, František, HARAŠTA, Jakub a kol. *Elektronické důkazy v trestním řízení* [online]. 1. vyd. Brno: Masarykova univerzita, 2015, 253 s. [cit. 3. 10. 2019]. ISBN 978-80-210-8073-7. Dostupné z: http://science.law.muni.cz/knihy/monografie/Polcak_Elektronicke_dukazy.pdf

- POLČÁK, Radim; Jiří ČERMÁK; Zbyněk LOEBL, a kol. *Cyber law in the Czech Republic.* 2. vyd. Alphen aan den Rijn : Kluwer Law International, 2015. 236 s. ISBN 978-90-411-6076-8.

- POLČÁK, Radim a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018. 640 s. ISBN 978-80-7598-045-8.

- MYŠKA, Matěj. *Právní aspekty uchovávání provozních a lokalizačních údajů* [online]. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2013, 136 s. [cit. 2. 1. 2020]. ISBN 978-80-210-6462-1. Dostupné z: http://science.law.muni.cz/knihy/monografie/Pravni_aspekty_Myska.pdf

Články

- SVETLÍK, Marián. Základní atributy forenzní analýzy. *Digital forensic review* [online]. 2018, roč. 2, č. 4, s. 5-13 [cit. 6. 8. 2018]. ISSN 2570-5059. Dostupné z: https://issuu.com/digitalforensicreview/docs/dfr_2_2018

- SVETLÍK, Marián. Analýza mobilních zařízení s důrazem na využití JTAG. *Digital forensic review* [online]. 2017, roč. 1, č. 1, s. 17-23 [cit. 6. 8. 2018]. ISSN 2570-5059. Dostupné z: https://issuu.com/digitalforensicreview/docs/dfr_1-2017

Prezentace

- PÚRY, František. *Dokazování v trestním řízení. Elektronické důkazy* [prezentace]. Brno: Právnická fakulta Masarykovy univerzity, 14. 4. 2018, 42 s. [cit. 14. 4. 2018]. Dostupný z: https://is.muni.cz/auth/el/1422/jaro2018/LI203Zk/um/JUDr._Pury_-_Dokazovani_a_el._dukazy_v_TR-PrF_MU_-_upravene.ppt

Právní předpisy

- Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky. In: *Zákony pro lidi* [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019]. Dostupný z: https://zakonyprolidi.cz/cs/1993-2
- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In: *Zákony pro lidi* [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019]. Dostupný z: https://www.zakonyprolidi.cz/cs/1961-141
- Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů. In: *Zákony pro lidi* [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019]. Dostupný z: https://zakonyprolidi.cz/cs/2004-480.
- Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů. In: *Zákony pro lidi* [právní informační systém]. AION CS, s.r.o. [cit. 17. 12. 2019]. Dostupný z: https://zakonyprolidi.cz/cs/2005-127
- *Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě* [online]. Sbírka mezinárodních smluv č. 104/2013 ze dne 23. 12. 2013 [cit. 12. 12. 2019]. Dostupný z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6571

Kvalifikační práce

- KOTHÁNEK, Jakub. *Vytěžování důkazů z výpočetní techniky* [online]. Brno, 2014. 97 s. [cit. 10. 10. 2019]. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA. Dostupné z: https://is.muni.cz/th/d3pt3/Diplomova_prace_-_Kothanek__Jakub.pdf
- ŠMÝD, Patrik. *Dokazování metadaty z mobilního komunikačního zařízení.* Brno, 2018. 25 s. Modulová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Marián SVETLÍK.