POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra managementu a informatiky

Zajišťování digitálních stop v rámci domovní prohlídky

Bakalářská práce

Securing digital evidence during house search

Bachelor thesis

VEDOUCÍ PRÁCE
PhDr. Mgr. Eliška Jonášová, Ph.D.

AUTOR PRÁCE
Ing. Bc. Martina Králíková, DiS.

PRAHA
2024

Poděkování

Na tomto místě bych chtěla upřímně poděkovat paní PhDr. Mgr. Elišce Jonášové, Ph.D. a mjr. Mgr. Karlu Jonášovi za vedení mé bakalářské práce, a především za mimořádnou ochotu a vstřícnost při poskytování cenných rad.

Čestné prohlášení

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

V Praze dne 28.2.2024

……

Ing. Bc. Martina Králíková, DiS.

ANOTACE

Bakalářská práce objasňuje pojem digitální stopa a problematiku zajišťování digitálních stop s akcentem na jejich zajišťování při domovní prohlídce. Samotný pojem digitální stopa je pak dán do kontextu termínu kriminalistické stopy, jsou uvedeny její znaky a charakteristiky. Obdobně pak práce rozpracovává související termíny, které jsou specifické pro virtuální prostředí, v němž je možné digitální stopy vyhledávat. Stěžejní je pak typologie digitálních stop, což odráží následné zpracování metod a postupů zajišťování digitálních stop. V neposlední řadě je doplněno formální nakládání se zajištěnými digitálními stopami, jejich dokumentace, balení, ukládání a samozřejmě protokolace. Finálně je pak předložen reálný případ, na němž lze demonstrovat, jaké digitální stopy lze zajišťovat a jaký mohou mít vliv na průběh trestního řízení.

KLÍČOVÁ SLOVA

domovní prohlídka, digitální stopa, zajištění stop, kyberkriminalita, policie, mobilní zařízení, počítačová technika

ANNOTATION

This bachelor's thesis clarifies the term 'digital trace' and the issue of securing digital traces with a focus on securing these during house searches. The term 'digital trace' is then placed in the context of the forensic trace, and its features and characteristics are discussed. Similarly, the thesis then considers related terms specific to the virtual environment in which digital traces are found. The key part of the thesis is then a typology of digital traces, which is followed by further discussion of the methods and processes in securing digital traces. The penultimate part explains the formal treatment of secured digital traces, including their documentation, packing, storage, and protocol completion. Finally, a case study is presented which demonstrates the types of digital traces that can be secured, and their influence on criminal proceedings.

KEYWORDS

home inspection, digital evidence, securing traces, cybercrime, police, mobile devices, computer technology

Obsah

Úvod

Soudobá společnost se vyznačuje dynamickým vývojem v oblasti technologií, moderní informační a komunikační technologie prostupují do všech sfér lidské činnosti a staly se nedílnou součástí běžného života každého jedince. Moderní přístroje – mobilní telefony, tablety či výpočetní technika, nejsou prostým, jednoúčelovým zařízením, ale mají široké možnosti použití napříč osobními a pracovními životy. Prosakování smart technologií, využívání vysokorychlostního internetu, šifrovacích nástrojů a bezpečné komunikace pomocí aplikací je umožněno právě bleskovým vývojem technologií a přirozeně si takové nástroje osvojili také pachatelé trestné činnosti.

Digitální svět nám přináší řadu nových možností, nový životní styl, zrychluje naši dobu a maže geografickou vzdálenost, avšak je na místě si uvědomit, že se právě díky těmto technologiím může každý člověk stát obětí, terčem pachatelů nových druhů kriminality, může ztratit své informace, uspořené peníze a majetkové hodnoty anebo může být zneužita jeho identita. Každá činnost uživatele v digitálním světě má konsekvence a zanechává v něm otisk, stopy, byť si to uživatel nemusí zcela uvědomovat. Vývoj v oblasti informačních a komunikačních technologií pak vytvoří možnosti, ale i výzvy, pro orgán prosazující právo a je zapotřebí s nimi pracovat, zejména pak při ochraně společnosti před pachateli trestné činnosti, kteří se pohybují v digitálním světě.

Jedním z limitů pro orgány činné v trestním řízení je pomalá reflexe vývoje technologií a následná harmonizace právního systému, tedy získání faktických nástrojů pro zajišťování dat, které mohou být důkazem v trestním řízení, a to jak po stránce technické, tak po stránce právní, neboť pachatelé trestné činnosti jsou v tom ohledu vždy o krok napřed.

V rámci své bakalářské práce se zaměřuji na zajišťování digitálních stop při domovní prohlídce, což považuji za aktuální téma, a to nejen v návaznosti na své služební zařazení na protidrogovém oddělení Služby kriminální policie a vyšetřování Obvodního ředitelství policie Praha I. Práce si klade za cíl předložit čtenáři základní informace o digitálních stopách a způsobech jejich zajišťování, dokumentování a uvedení následných možností jejich zkoumání tak, aby je bylo možné využít při objasňování kriminalisticky relevantních událostí.

Pro plnění cíle této práce byly zvoleny jednotlivé kapitoly tak, aby na sebe navazovaly a poskytovaly čtenáři alespoň elementární vhled do této problematiky, i proto je v teoretické části použita metoda deskripce a analýzy významných definic, odborných publikací a právních předpisů a poté bude pokračováno praktickou částí.

Úvodní kapitola předkládá základní terminologii, se kterou bude pracováno v dalším textu. Zejména má ambici vymezení pojmu digitální stopa v kriminalistice.

V navazující druhé kapitole bude vymezen právní rámec zajišťování digitálních stop, a to pomocí různých trestně právních institutů a navazujícím akcentem na domovní prohlídku.

Třetí kapitola se pak detailně věnuje pojmu digitální stopa, čtenář se dozví o charakteristických vlastnostech digitálních stop, které je odlišují od jiných typů kriminalistických stop.

Metody zajišťování digitálních stop při domovních prohlídkách budou popsány ve čtvrté kapitole, stejně tak budou přiblíženy způsoby zajišťování digitálních stop na paměťových uložištích i ve virtuálním prostředí, blíže budou rovněž popsány způsoby ukládání, balení zajištěných digitálních stop a jejich protokolace pro účely trestního řízení.

Poslední kapitola teoretické části předloží informace o tom, jak může být s digitální stopou dále nakládáno po jejím zajištění. Blíže bude popsáno, jak je odesílat na zkoumání a možnosti jejich zkoumání prizmatem institutů trestního práva – odborné vyjádření, znalecký posudek, ohledání specializovaným pracovištěm.

Kapitola šestá je praktickou aplikovanou částí této práce. Jedná se o skutečnou kauzu, v níž byly zjišťovány informace v kyber prostředí a z provedených úkonů byly zadokumentovány digitální stopy, a to jak během prověřování, tak při provádění domovních prohlídek, kterými byly zajištěny zařízení, které obsahovaly rozhodné digitální stopy pro objasnění trestné činnosti pachatelů.

1. Základní vymezení pojmů

1.1. Kriminalistická stopa

Kriminalistika je samostatná vědní disciplína, jejíž vymezení může být stanoveno pomocí objektů, které jsou zkoumány a které „lze rozdělit do tří skupin: skutek trestného činu a osoba pachatele, stopy trestného činu a nositelé stop, činnost policie, orgánů činných v trestním řízení, odborníků a znalců při odhalování a vyšetřování trestných činů a při zkoumání stop.[1] Odborná literatura již z podstaty pojmu kriminalistika reflektuje termín stopa, resp. kriminalistická stopa. Stejně tak je z odborné literatury zřejmé vymezení předmětu kriminalistiky, které tvoří dvě oblasti:

1. „zákonitosti vzniku, trvání a zániku stop a jiných kriminalisticky relevantních informací o spáchaných trestných činech,

2. zákonitosti vyhledávání, shromažďování a zkoumání stop a jiných kriminalisticky relevantních informací o spáchaných trestných činech.“[2]

Jak tedy vyplývá, tak pojem, resp. kriminalistická stopa je jedním z ústředních termínů v kriminalistice a rovněž pro potřeby této práce je nanejvýš vhodné věnovat se definici kriminalistické stopy a předložit čtenáři vhodné související informace a typologii kriminalistických stop.

Odborná literatura seznává množství více či méně konkrétních anebo obsáhlých definic a někteří autoři pak předkládají definici takřka totožnou a diference mezi nimi lze spatřovat z uchopení jejího dalšího praktického použití a eventuálního akcentu či absence její zjistitelnosti, zajistitelnosti a využitelnosti.

„Kriminalistická stopa je každá změna v materiálním prostředí nebo ve vědomí člověka, která příčinně nebo alespoň místně nebo časově souvisí s vyšetřovanou událostí, obsahuje kriminalisticky nebo trestněprávně relevantní informaci a je zjistitelná a informace z ní je využitelná pomocí přístupných kriminalistických, přírodovědných a technických metod, prostředků a postupů.“[3]

---

[1] MUSIL, KONRÁD, SUCHÁNEK. *Kriminalistika, 2. přepracované a doplněné vydání*, 2004, s. 3. ISBN 80-7179-878-9.
[2] MUSIL, KONRÁD, SUCHÁNEK. *Kriminalistika, 2. přepracované a doplněné vydání*, 2004, s. 4. ISBN 80-7179-878-9.
[3] PORADA, Viktor. *Kriminalistika: (Úvod, technika, taktika).* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2007. s. 56. ISBN 978-80-73-80-038-3.

„Kriminalistická stopa je každá změna v materiálním prostředí nebo ve vědomí člověka, která příčinně nebo alespoň místně nebo časově souvisí s vyšetřovanou událostí, obsahuje kriminalisticky nebo trestněprávně relevantní informaci a je zjistitelná, zajistitelná a informace z ní využitelná pomocí dostupných kriminalistických, přírodovědných a technických metod, prostředků a postupů.“[4]

„Stopou rozumíme v kriminalistice každou změnu, která na místě konkrétního trestného činu nebo na místě přípravy k němu vznikla jednáním osob, zúčastněných na trestném činu, a je v příčinné souvislosti s nastalým nebo zamýšleným výsledkem. Stoupou proto rozumíme nejen změnu způsobenou pachatelem, popřípadě i spolupachatelem, nýbrž i všechny změny přivoděné obětí a jinými osobami na trestném činu nějakým způsobem zúčastněnými, jakož i všechny známky, které jsou následkem událostí na místě trestného činu proběhnuvších.“[5]

Jak bylo shora uvozeno, tak dílčí odlišnosti v definicích kriminalistické stopy jsou v zjistitelnosti, zajistitelnosti a využitelnosti, avšak pro praktický výkon činností policejního orgánu v trestním řízení jde zřejmě o zcela klíčové pojmy, jelikož stopa, která není zjistitelná, tak ze své podstaty nebude orgánům činným v trestním řízení známá a nebude možno s ní jakýmkoliv způsobem dále pracovat v rámci objasňování nějaké kriminalisticky relevantní události, obdobně pokud by nebyla zajistitelná, tak nebude žádný způsob, jak ji použít při objasňování kriminalisticky relevantní události, typicky pak v trestním řízení. Na to bezprostředně navazuje možnost jejího dalšího uchování a využití, pakliže by nebylo možné, tak by mohlo dojít k její nepřezkoumatelnosti a v trestním řízení by nemohla být užita jako relevantní důkaz.

Kriminalistická stopa, jak vyplývá z předložených definic, hraje ústřední roli. Autor této práce, z vlastní kriminalistické praxe, může tomuto pouze přisvědčit, jelikož kriminalistické stopy poskytují významné informace o kriminalisticky relevantní události, a to byť by se stala anebo dílem souvisela s kyberprostorem a lze tak vytěžit rozhodné informace o průběhu kriminalisticky relevantní události,

---

[4] KONDRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika, Teorie, metodologie a metody kriminalistické techniky.* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 54. ISBN 978-80-7380-535-7.

[5] NĚMEC, Bohuslav a kol. *Učebnice kriminalistiky (Kriminalistická technika).* Praha. Vydal Kriminalistický ústav MV-hlavní správy VB, 1959. s. 3.

důvodech a způsobech jednání pachatele a dalších osob a mohou přinést další významné poznatky, které mohou přispět, byť pouze operativně, pro další fáze objasňování kriminalisticky relevantní události. Zejména při prověřování a vyšetřování mohou získané informace dopomáhat policejnímu orgánu seznámit se s osobou pachatele, mechanismu, jak konkrétně při páchání trestného činu postupoval (tělesné pohyby, nástroje, výpočetní technologie a algoritmy), ale případně i jaký měl motiv pro spáchání trestného činu, popřípadě jaký měl vztah k oběti, a v neposlední řadě ho identifikovat. Všechna tato zjištění lze využít ke konstruování vyšetřovacích verzí ke kriminalisticky relevantní události, jejichž podstatou je vytvoření hypotéz a jejich následné potvrzení či vyvrácení.

V souhrnu je možné konstatovat, že každá kriminalistická stopa nese hodnotu, která má určitý kriminalisticko-technický význam, který znamená, že stopu můžeme zjistit a zajistit vhodnými prostředky a poté jí zkoumat a z výsledků zkoumání pak lze využít pro objasňování kriminalisticky relevantní události a identifikování osob, zvířete či věci, které danou stopu vytvořily[6] a dále se pak nauka o kriminalistických stopách v odborné literatuře i kriminalistické praxi stala důležitým a hodnotným podkladem pro zpracování kriminalistických metod, které reflektují vývoj trestné činnosti, a to mimo jiné i v digitálním světě.

Autor této práce považuje za vhodné předložit čtenáři pro úplnost některé typologie kriminalistických stop vyplývajících z odborné literatury, a to tzv. elementární dělení dle kriminalistických disciplín. Ambicí této práce však není jednotlivé typologie komplexněji popisovat či detailněji předkládat informace k jednotlivým druhům, neboť to není pro zpracování podstatné, vyjma určitého vztahu ke stopám digitálním.

Kriminalistické stopy elementárně dělíme na stopy ve vědomí (paměťové) a stopy materiální (hmotné).[7] Stopy ve vědomí se dají členit dle receptorů lidských smyslů (zraku, sluchu, čichu, chuti a hmatu), kterými jsou vnímány. Prakticky nejčastěji vznik paměťové stopy je pomocí zraku a sluchu. Ostatní smyslové vjemy

[6] KONRAD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika, Teorie, metodologie a metody kriminalistické techniky.* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 71-72. ISBN 978-80-7380-535-7.
[7] MUSIL, KONRÁD, SUCHÁNEK. *Kriminalistika, 2. přepracované a doplněné vydání*, 2004, s. 81. ISBN 80-7179-878-9.

mají v kriminalistice výrazně méně četné použití. Stopy materiální vznikají na nejrůznějších objektech neživé nebo živé přírody.[8]

Klasifikace stop podle oboru zkoumání přímo reflektuje jednotlivé kriminalistické disciplíny daktyloskopie, trasologie, balistika, genetika a biologie, odorologie, mechanoskopie, chemie a další obory.

Shora uvedené členění kriminalistických stop téměř v žádné z kriminalistických odborných publikací zcela nereflektují společenský, technický a technologický vývoj společnosti a její „digitalizaci". Až v posledních letech se tematizuje problematika stop v digitálním/kybernetickém prostředí, jelikož se zcela zjevně jedná o informace, které mají význam pro objasňování a souvisejí s kriminalisticky relevantní událostí a v současné době již jsou možnosti a technologie, jak takové stopy vyhledat, zadokumentovat, vyhodnotit a uchovat. Dynamický vývoj v oblasti informačních a komunikačních technologií tak tvoří nové výzvy jak pro orgány prosazující právo, resp. orgány činné v trestním řízení, tak i pro odbornou veřejnost a znalecká pracoviště.

1.2. Digitální stopa

Obdobně, jako je velké množství definic termínu kriminalistická stopa, tak je i množství definic termínu digitální stopa. Čtenáři bude níže předloženo pět konkrétních definic, které poslouží k obecnému vymezení tohoto pojmu, avšak je z nich patrné, že ve svém jádru jsou poměrně značně rozdílné. Obsahová diference může být přisuzována právě skutečnosti, že se jedná o dynamicky se vyvíjející oblast, v níž se objevují nové nástroje a možnosti lidské činnosti, které vytvářejí různé otisky v nehmotném virtuálním, resp. digitálním prostředí.

„Digitální stopa je informace zanechaná uživatelem v prostředí internetu nebo jako součást souborů."[9]

[8] MUSIL, J., KONRAD, Z., SUCHANEK, J. *Kriminalistika.* 1. vydání. Praha: C.H.Beck, 2001. s. 84. ISBN 80-7179-878-9.
[9] BRECHLEROVÁ, Dagmar. *Digitální stopy a jejich odstraňování*. In: Computerworld. Online. 2016. Dostupné z: https://computerworld.cz/securityworld/digitalni-stopy-a-jejich-odstranovani-53197. [citováno 2024-02-10].

„Digitální stopa je sada informací zanechaná konkrétním uživatelem v síťových i lokálních IT a elektronických zařízeních (serverech, počítačích, telefonech, kamerách apod). Především pak v prostředí internetu.“[10]

„Digitální stopa je záznam všech interakcí s digitálním světem a toho, jak data, která z těchto interakcí zůstávají, mohou být využitá. Digitální stopu sestavují sledovací nástroje na webových stránkách a v prohlížečích. Pohybem na internetu – např. návštěvou stránek, sdílením a lajkováním příspěvků jí každý zanechává. Všechny informace, které se na internetu nashromáždí, pak společně tvoří jedinečnou stopu, podle které lze na internetu poznat prakticky kohokoli (stejně jako je možné identifikovat osobu například pomocí otisků prstů).“[11]

„Digitální stopou je digitální informace nebo jakákoli data přenesená nebo uložená za použití počítačového systému; digitální stopa se zpravidla nachází na magnetickém, optickém nebo polovodičovém médiu nebo v prostředí datových sítí.“[12]

Širokým okruhem specialistů akceptovaná a nejčastěji používaná je definice, která byla již v roce 1999 navržena pracovní skupinou SWGDE – *Scienific Working Group on Digital Evidence*

„Digitální stopa je jakákoli informace s odpovídající hodnotou pro danou relevantní událost, uložená nebo přenášená v digitálním prostředí.“

Pod optikou této konkrétní definice lze subsumovat do jejího vymezení jakoukoli digitální technologii, tedy od počítačů a počítačové komunikace, oblast digitálních přenosů, jako jsou mobilní telefony, videa, audia, digitální fotografie, data z uzavřených kamerových systémů, data elektronických zabezpečovacích systémů, a jakýchkoli dalších technologií potenciálně spojených s Hi-Tech kriminalitou.[13,14]

Moderní praktická kriminalistická činnost se pak navíc mimo uvedené IT oblasti dotýká také oblasti šifrování, kryptoměn a jejich trasování.

---

[10] https://it-slovik.cz/pojem/digitalni-stopa/?utm_source=cp&utm_medium=link&utm_campaign=cp
[11] Online. Dostupné z: https://www.totalservice.cz/novinky/digitalni-stopy-co-jsou-a-jak-se-jich-zbavit-2022-02-18. [citováno 2024-02-10].
[12] Čl. 2 písm. j) pokynu policejního prezidenta č. 100/2021, o kriminalisticko-technické činnosti
[13] Digital Evidence: Standards and Principles. *Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE).* http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm
[14] WHITCOMB C.M.: An Historical Perspective of Digital Evidence: A Forensic Scientist´s View. In: *International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1.* s. 115.

Šifrování pro potřeby praktické kriminalistiky zjevně nespočívá ve snaze prolamovat použité kryptovací algoritmy apod., nicméně význam má zjištění šifrovacího klíče užívaného konkrétním uživatelem v P2P šifrování[15], typicky v rámci používání nějaké komunikační aplikace. Samo o sobě vyhledání a zadokumentování soukromého či veřejného šifrovacího klíče je ve své podstatě získání digitální stopy, která navíc může v souhrnu s dalšími informacemi dát možnost rozpoznat další informace, které mohou být digitální stopou a zjevně pak mohou objasnit kriminalisticky relevantní událost.

Další oblastí, kterou s sebou přinesl vývoj virtuálního světa, jsou kryptoměny[16]. Kryptoměny mohou být digitální stopou zvláště v případě, kdy je fakticky možné trasovat jejich pohyb. Digitální stopou pak z podstaty jsou i informace z blockchain[17], které mohou mít zásadní vliv při objasňování kriminalisticky relevantní události.

Digitální stopou mohou tedy dle shora uvedeného být od obrazových, audio, video souboru na paměťových uložištích či cloudech, logovací údaje do aplikačních rozhraní, do internetu ve všech úrovních (clearnet, deepweb), metadata, software a v něm obsažená data, šifrovací nástroje a individuální šifrovací klíče, kryptoměny a informace o jejich převodech a adresách peněženek, a to v těch případech, kdy je vztah takových dat ke kriminalisticky relevantní události.

1.3. Kyberkrimininalita

V rámci pojmu kyberkriminalita nenajdeme žádnou jednoznačnou definici. V souvislosti s kyberkriminalitou hovoříme o takzvané počítačové či internetové kriminalitě. V obecnější rovině by se tento pojem dal označit jako trestná činnost neboli škodlivé protiprávní jednání, která se odehrává v kyberprostoru, tedy ve virtuálním prostředí.

---

[15] P2P neboli peer to peer šifrování spočívá v tom, že zpráva se u odesílatele zašifruje klíčem, který zná pouze odesílatel a adresát, který pomocí tohoto klíče zprávu dešifruje. Tudíž i při zachycení zprávy není možné ji bez tohoto klíče přečíst, či dešifrovat. Viz. KOLOUCH, Jan. *Cybercrime*. Praha: Edice CZ.NIC, 2016. s. 195. ISBN 978-80-88168-18-8.

[16] Kryptoměna je digitální měna využívající blockchainovou technologii, která umožňuje Peer-to-peer (P2P) transakce. Online. Dostupné z: https://academy.binance.com/cs/articles/what-is-a-cryptocurrency. [citováno 2024-02-25].

[17] Blockchain je distribuovaná databáze, ve které jsou navždy uloženy veškeré záznamy, které jsou do ní vloženy. Online. Dostupné z: https://www.alza.cz/co-je-blockchain. [citováno 2024-02-19].

Zákon o kybernetické bezpečnosti vymezuje pojem kyberprostor jako: *„Kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*[18] Tento prostor můžeme označit za virtuální realitu. Jedná se o prostředí, které je tvořeno propojením informačních a komunikačních systémů (dále jen „ICT“). Kyberprostor můžeme rozdělit do tzv. tří částí, a to Visible Web, Deep Web a Dark Web. Visible web je dostupný široké veřejnosti a lze se v něm pohybovat prostřednictvím klasických webových prohlížečů Seznam, Google apod. Deep Web tvoří podstatnou část celého Internetu, avšak jeho obsah není možné zobrazit klasickým webovým prohlížečem, ale je nutné znát jeho URL nebo mít k jeho zobrazení oprávnění.[19] Poslední část tvoří Dark Web, který je tvořen šifrovanými stránkami, které neobsahují IP adresy. Deep Web stejně jako Dark Web zajišťuje jeho uživatelům buď částečnou nebo úplnou anonymitu. Úplná anonymita vládne především na Dark Webu, jelikož uživatelé tyto stránky navštěvují prostřednictvím šifrovacího softwaru, který zcela maskuje jejich IP adresy, aby nebyla možná jejich identifikace. Typickou činností probíhající jak na Deep Webu, tak Dark Webu, je prodej nelegálního zboží, obchod se zbraněmi, obchod s drogami a pornografií.
Trestná činnost odehrávající se v kyberprostoru by se dala chápat jak v širším, tak i v užším pojetí. V užším pojetí by se cílem útoku stala oblast informačních a komunikačních technologií. Typickým příkladem je tzv. DOS útok neboli **Denial-of-service (DoS)** (česky odepření služby) je typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům. Může k tomu dojít zahlcením obrovským množstvím požadavků či využitím nějaké chyby, která sice útočníkovi neumožní službu ovládnout, ale umožní ji znefunkčnit. Podtypem útoku DoS je tzv. **distributed denial-of-service (DDoS)**, při kterém je pro zahlcení cílové služby požadavky využito velké množství počítačů z různých geografických lokalit.[20]

---

[18] ust. § 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
[19] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ NIC, 2013. s. 35. ISBN 978-80-904248-7-6.
[20] Online. https://www.w3.org/Security/Faq/wwwsf6.html. [citováno 2024-02-11].

Běžným chápáním kyberkriminality je tzv. širší pojetí, kdy se jedná o prakticky jakoukoli trestnou činnost, která je páchána prostřednictvím informačních a komunikačních technologií, případně tyto technologie tvoří významnou součást trestné činnosti.[21] Typickým příkladem takové činnosti je počítačové pirátství. Porušování práva duševního vlastnictví, tedy práv autorských a průmyslových spočívá v tom, že pachatel neoprávněně umístí dílo do kyberprostoru a tímto činem ho rozšíří pro veřejnost. Na internetu dnes můžeme nalézt různá fóra, jejichž prostřednictvím se nelegální kopie šíří rychleji, jde na nich získat kompletní filmy, cracky a také hudbu. Fóra jsou postižitelná stejně jako jiné porušení autorských práv podle ust. § 270 Porušení autorských práv, práv souvisejících s právem autorským a práv k databázi či § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému jiných takových dat zákona č. 40/2009 Sb., trestního zákoníku. Pachatele, který se dopustil určitého protiprávního jednání v rámci kyberprostoru, je však mnohdy obtížné dopadnout, protože se umí v tomto prostředí volně, rychle a nenápadně pohybovat, umí prolomit hesla, získat vzdálený přístup a plně manipulovat se zařízením, měnit identity či je umí nechat úplně zmizet. To znamená, že po sobě nemusí zanechat žádné stopy. Nelze stoprocentně spoléhat pouze na kvalitní software či antivirový program, proto by především sami lidé měli znát rizika při používání těchto technologií, dbát zvýšené opatrnosti při práci s nimi a důkladně si promyslet, jaké do kybernetického prostoru ukládají informace.

1.4. Integrita digitálních dat

Integrita digitálních dat je termín pro označení celistvosti, úplnosti a neporušenosti dat, která jsou zajištěna jako důkazní prostředek, resp. obsahují informace mající potenciální důkazní relevanci. Úplná, neporušená, celistvá data legálně zajištěná policejním orgánem některým z procesních úkonů podle trestního řádu, do nichž nebyl proveden neautorizovaný zásah, změna či úprava jejich obsahu, mohou být použita v trestním řízení jako důkaz a jsou tak přezkoumatelná.

[21] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. s. 541. ISBN 978-80-7598-045-8.

Integrita dat je tedy nezbytným parametrem při zajišťování digitálních stop pro účely trestního řízení.[22]

1.5. Bitová kopie

Bitová kopie nebo také diskový obraz, image nebo otisk obsahuje komplexní zálohu veškerých dat, které se nacházejí na nosiči dat (např. interní paměť telefonu, flashdisk či jiné externí paměťové zařízení). Nejedná se pouze o samotné soubory, ale taktéž o metadata souborového sytému jako je (operační systém, nainstalované programy, nastavení, ovladače a podobně). V případě, že by došlo k selhání pevného disku nebo poškození kritických souborů operačního systému, je možné obnovit všechny soubory právě pomocí bitové kopie. V případě, že se jedná o zajišťování důkazních prostředků, jde o způsob, jak vyhodnotit obsah zajištěných nosičů na jiném zařízení bez zásahu do obsahu původního nosiče.[23]

1.6. Hashovací funkce, hash

Hashovací funkce je jednosměrná matematická funkce, pomocí které lze převést jakákoli libovolná vstupní data (různé druhy a velikosti) do řetězce znaků definované velikosti, tedy do relativně malého čísla. Vstupní data mohou být v jakékoli velikosti a mohou mít jakoukoli formu. Výstupní data budou mít formát vždy stejně dlouhé řady znaků, která tvoří kontrolní součet (taktéž nese označení kontrolní suma nebo hash). Délka vzniklého řetězce vždy závisí na použitém algoritmu nikoli na velikosti vstupních dat.[24]

---

[22] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách.* Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

[23] Online. Dostupné z: https://www.linnetdesign.cz/app4/743/co-je-bitova-kopie-disku. [citováno 2024-02-11].

[24] Mulvey, Bret. Pluto Scarab - Hash Functions. Hash Functions. Online. 2007. Dostupné z: http://home.comcast.net/~bretm/hash/. [Citováno 11.2.2024.]

1.7. Metadata

V digitálním světě, který je plný obrovského množství informací, jsou metadata klíčovým pojmem. Metadata jsou data, která poskytují informace o jiných datech. Jednoduše řečeno, jsou to popisy, které nám pomáhají pochopit a organizovat obsah, který se skrývá uvnitř souborů, dokumentů, obrázků nebo jiných digitálních entit. S trochou fantazie je lze přirovnat k mapě k pokladu. Samotná mapa představuje metadata (informace o datech) a poklad symbolizuje data (soubor, fotku). Metadata hrají důležitou roli ve správě dat, vyhledávání informací a organizování digitálního obsahu.

Existuje mnoho různých typů metadat, která se liší v závislosti na kontextu a použití. Některé z nejčastějších typů metadat zahrnují:

- **Popisná metadata:** Tato metadata slouží k popisu obsahu a poskytují informace jako název, autor, datum vytvoření, popis a klíčová slova. Jsou důležitá pro identifikaci a vyhledávání konkrétních souborů nebo dokumentů.
- **Technická metadata:** Zaměřují se na technické informace o digitálním obsahu. Mohou zahrnovat formát souboru, rozlišení obrázku, délku a kodeky videa nebo zvukového souboru. Technická metadata jsou klíčová pro správu a optimalizaci digitálních souborů.
- **Administrativní metadata:** Zabývají se správou a organizací digitálního obsahu. Zahrnují informace o vlastnictví, přístupových právech, oprávněních a životním cyklu dat. Administrativní metadata pomáhají určit, kdo má právo přistupovat k určitému obsahu a jakým způsobem může být spravován.
- **Kontextová metadata:** Tato metadata přidávají do digitálního obsahu informace o jeho kontextu. Mohou zahrnovat geografickou polohu, historické informace, odkazy na související dokumenty nebo události. Kontextová metadata pomáhají uživatelům lépe porozumět obsahu a jeho vztahům k ostatním informacím.[25,26]

[25] BRATKOVÁ, Eva. *Metadata jako nový nástroj pro komunikaci webovských informačních zdrojů.* Národní knihovna, 1999, 10(4), s. 178-195. ISSN 0832-7487.
[26] BRATKOVÁ, Eva a Helena KUČEROVÁ. *K otázkám metadatového popisu systémů organizace znalostí.* Knihovna: knihovnická revue, 2015, 26(1), s. 5-36. ISSN 1801-3252.

2. Právní aspekty zajišťování digitálních stop

Digitální stopou, která může být důležitou pro objasňování kriminalisticky relevantní události, lze pro potřeby trestního řízení zajistit několika instituty v souladu se zákonem č. 141/1961 Sb., o trestním řízení soudním (dále jen trestní řád), což v zásadě koresponduje s běžným zajišťováním věcí pro potřeby trestního řízení:

- **datafreezing** dle ust. § 7b trestního řádu
- **vyžádání informací** dle ust. § 8 odst. 1 trestního řádu
- **vyžádání informací** dle ust. § 8 odst. 2 trestního řádu
- **vyžádání informací** dle ust. § 8 odst. 5 trestního řádu
- **vydání a předložení věci** dle ust. § 78 trestního řádu
- **odnětí věci** dle ust. § 79 trestního řádu
- **domovní prohlídka, prohlídka jiných prostor a pozemků** dle ust. § 82 a následující trestního řádu
- **vyžádání informací o telekomunikačním provozu** dle ust. § 88a trestního řádu
- **odposlech a záznam telekomunikačního provozu** dle ust. § 88 trestního řádu
- **ohledání** dle ust. § 113 trestního řádu
- **předstíraný převod** dle ust. § 158c trestního řádu
- **sledování osob a věcí** dle ust. § 158d odst. 3 trestního řádu

Přestože není pro tuto bakalářskou práci zásadní detailně popisovat shora uvedené zajišťovací instituty, autor považuje za vhodné rámcově vymezit typový okruh digitálních stop, které mohou být jednotlivými instituty získány v trestním řízení, jelikož mohou mít zásadní vliv při objasňování kriminalisticky relevantní události, a to zvláště při jejich komparaci či souvislosti s digitálními stopami zajištěnými při domovní prohlídce anebo prohlídce jiných prostor a pozemků.

Datafreezing je instrument k zajištění dat v čase u poskytovatele služeb v digitálním prostředí, může se jednat o providera konektivity, provozovatele webových rozhraní a databází apod. „Zmražená“ data pak jsou policejním orgánem vyžadována podle svého charakteru dalšími níže uvedenými instituty.

Vyžádání informací dle ust. § 8 odst. 1 trestního řádu je prosté vyžádání informací od fyzických či právnických osob, které mohou nést informace, které jsou de facto digitální stopou. Typickým příkladem je vyžádání logovacích údajů do klientských rozhraní, a to od provozovatelů internetových služeb, například Seznam.cz a.s., který poskytuje logovací údaje o službách používaných konkrétním uživatelem – email, Sbazar, mapy atd. Policejní orgán takové informace (digitální stopy z databází poskytovatele služeb) může získat bez použití jiných institutů.

Další podobné informace, resp. digitální stopy mohou být získány od bankovních domů, zejména logovací údaje do uživatelského rozhraní internetového bankovnictví, nicméně se jedná o informace, které jsou předmětem bankovního tajemství, a tudíž je pro potřeby trestního řízení může vyžádat v přípravném řízení „státní zástupce a po podání obžaloby nebo návrhu na potrestání předseda senátu.“[27]

Logovací údaje a související informace, které mohou být digitální stopou, která může souviset s objasňováním kriminalisticky relevantní události, lze získat mimo jiné od poskytovatelů doručovacích a poštovních služeb ve smyslu zákona č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů. Takové informace jsou ovšem chráněny poštovním tajemstvím a pro potřeby trestního řízení je lze vyžadovat pouze po předchozím souhlasu soudce.[28]

Vydání a odnětí věci dle ust. § 78, resp. § 79 trestního řádu je institut, kterým lze pro potřeby získat digitální stopy od osoby, která je má v „držení“. Může se jednat o vydání prostých digitálních dat, eventuálně nosiče, na němž jsou data uložena, pak by došlo k jejich zadokumentování dalšími procesními úkony, čemuž se blíže věnuje kapitola 4.

Informace o telekomunikačním provozu a **odposlech a záznam telekomunikačního provozu** jsou procesní úkony, kterými mohou být zajištěny a zadokumentovány takové skutečnosti, které v zásadě tvoří digitální stopu, typicky pak logovací údaje v rámci internetového provozu v telekomunikační síti operátorů, ale dále také MMS zprávy, v nichž může být obrázek anebo zvukový záznam, které pak mohou zároveň obsahovat metadata.

---

[27] § 8 odst. 2 zákona č. 141/1961 Sb., o trestním řízení soudním
[28] § 8 odst. 5 zákona č. 141/1961 Sb., o trestním řízení soudním

Ohledání je procesní úkon, kterým lze zajistit a zadokumentovat digitální stopu. V praxi je ale tento procesní úkon v podstatě formální, neboť se jím zadokumentuje například obsah mobilního telefonu či datového uložiště a v protokolaci jsou uvedeny forenzní nástroje, číslo oprávnění specializovaného kurzu vydaného Kriminalistickým ústavem konkrétnímu policistovi-technikovi provádějícím ohledání. Blíže bude ohledání, jako způsob dokumentace v této práci, zpracován v kapitole 4.

Přestože je **předstíraný převod** operativně pátracím prostředkem, je nutné konstatovat, že při jeho provádění mohou být zjištěny a zadokumentovány takové informace, které svým charakterem jsou digitální stopou a zřejmě by mohly být využitelné při objasňování kriminalisticky důležité události. Zcela ukázkovým příkladem je předstíraný převod, jež je uskutečněn v prostředí darknetu[29] ve virtuálním tržišti, kde je předmětem předstíraného převodu omamná nebo psychotropní látka (dále jen OPL). Během převodu může být zjištěn veřejný a soukromý šifrovací klíč a také údaje k zaslání platby za OPL skrze kryptopeněženku.

Další operativně pátrací prostředek, kterým lze zjistit a zadokumentovat digitální stopy je bezesporu **sledování osob a věcí**, kterým je získán obsah databází, které nelze zajistit pro účely trestního řízení některým ze shora uvedených institutů. Naprosto charakteristickým je zajištění obsahu emailové schránky od poskytovatele emailových služeb jako je Seznam.cz a.s. Sledováním, kterým je *„zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, lze je uskutečnit jen na základě předchozího povolení soudce.“*[30]

Obecně lze konstatovat, že většina digitálních informací, které by mohly být považovány za digitální stopu, jež jsou v rámci trestního řízení zajištěné shora uvedenými instituty, tak lze vhodně využít v souhrnu, komparaci či souvislosti s dalšími zajištěnými digitálními stopami právě zajištěných při domovní prohlídce

[29] Součástí kyberprostoru. Darknet není separátní fyzickou sítí, jedná se o aplikační vrstvu v rámci existujících sítí a služeb. blíže viz. KOLOUCH, Jan. *Cybercrime*. Praha: Edice CZ.NIC, 2016. s. 48. ISBN 978-80-88168-18-8.

[30] § 158 odst. 3 zákona č. 141/1961 Sb., o trestním řízení soudním

a prohlídce jiných prostor a pozemků, ostatně tam může být kupříkladu bitová kopie digitální stopy či zdrojový soubor/uložiště/nezměněná podoba.

2.1. Domovní prohlídka

Domovní prohlídka je procesní úkon, který je společně s osobní prohlídkou a prohlídkou jiných prostor a pozemků upraven v oddílu pátém zákona č. 141/1961 Sb., o trestním řízení soudním (dále jen trestní řád), přičemž „domovní prohlídku lze vykonat, je-li důvodné podezření, že v bytě nebo v jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících (obydlí) je věc nebo osoba důležitá pro trestní řízení.“[31] Ze stejných důvodů pak „lze vykonat i prohlídku prostor nesloužících k bydlení (jiných prostor) a pozemků, pokud nejsou veřejně přístupné“[32], přičemž provést domovní prohlídku lze pouze na základě příkazu k provedení domovní prohlídky, která je nařízená v řízení před soudem předsedou senátu a v přípravném řízení pak soudcem příslušného soudu, a to na návrh státního zástupce.[33] Analogicky pak je možné nařídit, resp. provést prohlídku jiných prostor a pozemků, přičemž navíc lze tento úkon provést i v situaci, kdy „vydání příkazu nelze předem dosáhnout a věc nesnese odkladu. Policejní orgán je však povinen si bezodkladně dodatečně vyžádat souhlas orgánu oprávněného k vydání příkazu; v přípravném řízení tak činí prostřednictvím státního zástupce. Pokud oprávněný orgán souhlas dodatečně neudělí, nelze výsledek prohlídky použít v dalším řízení jako důkaz.“[34]

Provádění domovní prohlídky, osobní prohlídky a prohlídky jiných prostor a pozemků je vždy citelný zásah do soukromí osob, ale i do jejich práv a svobod. Z tohoto důvodu je vždy zcela nezbytný výslech osob, kterých se tento úkon bude týkat. Tato povinnost je specifikována v § 84 trestního řádu. V případě, že během výslechu osoba vydá věc důležitou pro trestní řízení, nelze již domovní prohlídku provést. Předchozí výslech není nutný v případě, že celá věc nesnese odkladu a hrozí nebezpečí z prodlení. Při provádění domovní prohlídky a prohlídky jiných prostor a pozemků musí být vždy přítomna nezúčastněná osoba a také orgán,

[31] ust. § 82 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním
[32] ust. § 82 odst. 2 zákona č. 141/1961 Sb., o trestním řízení soudním
[33] ust. § 83 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním
[34] ust. § 83a odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním

který prohlídku provádí. Policejní orgán nemůže neumožnit účast osoby, u které bude prohlídka prováděna.[35]

Pojem domovní prohlídky je dále pro orgány činné v trestním řízení upraven v závazném pokynu policejního prezidenta č. 30/ 2009 o plnění úkolů v trestním řízení. Provádění domovní prohlídky taktéž nalezneme v čl. 62a pokynu policejního prezidenta č. 48/2019 o plnění některých úkolů policejního orgánu Policie České republiky v trestním řízení.

V rámci interních aktů řízení:

- závazný pokyn policejního prezidenta č. 100/2001 ke kriminalisticko-technické činnosti Policie České republiky
- metodický pokyn ředitele KÚP č. 7/2001, kterým se upravuje činnost orgánů Policie České republiky při zajišťování výpočetní techniky a dat pro účely následného znaleckého zkoumání
- závazný pokyn policejního prezidenta č. 77/2009, kterým se upravuje věcná, funkční a místní příslušnost znaleckých pracovišť Policie České republiky
- pokyn policejního prezidenta č. 48/2019 o plnění některých úkolů policejního orgánu Policie České republiky.

[35] FENYK, Jaroslav, HÁJEK, Roman, STŘÍŽ, Igor, POLÁK, Přemysl. *Trestní zákoník a trestní řád, průvodce trestněprávními předpisy a judikaturou, 1. díl – Trestní zákoník.* 1. vydání. Praha: Linde Praha, a.s., 2010. Edice Komentované zákony. ISBN 978-80-7201-802-4.

3. Digitální stopy

3.1. Charakteristické vlastnosti digitálních stop

V rámci jednotlivých kriminalistických oborů jako jsou například daktyloskopie, mechanoskopie či balistika při zkoumání kriminalisticky relevantních stop musíme dodržovat pevné zákonitosti a pravidla pro jejich zkoumání. Stejně tak je tomu i u digitálních stop, které jsou zajištěny během trestního řízení některým se shora uvedených procesních úkonů, a to bez ohledu, zda jsou získány od prověřovaných osob, svědků, poškozených či jiných osob, které disponují informacemi důležitými pro trestní řízení, jako například provideři konektivity, poskytovatelé telekomunikačních služeb či jiných digitálních služeb a aplikací.

Obdobně jako u „konvenčních" kriminalistických stop, tak i u digitálních stop jsou specifická pravidla a zákonitosti, která musí být policejním orgánem akceptována a musí být reflektovány při jejich zajišťování tak, aby nedošlo k porušení či nevratnému poškození digitální stopy a nebylo by jí možné použít jako relevantní důkazní prostředek v trestním řízení. Pokud by došlo k porušení, poškození či ztrátě digitální stopy, jedná se jednoznačně o nežádoucí jev, který by mohl mít negativní důsledek na objasňování kriminalisticky relevantní události, v trestním řízení by pak mohl způsobit, že by nedošlo ke zjištění pachatele trestného činu či by se nepodařilo rozkrýt celý rozsah trestné činnosti a byl by tak ohrožen účel trestního řízení jako takový. V následných bodech jsou popsané charakteristické vlastnosti digitálních stop, a to včetně jejich pozitivního a negativního využití.

3.1.1. Nehmotnost digitální stopy

Při práci s digitálním daty je potřeba mít na paměti, že se jedná o data, která jsou velmi citlivá na změnu obsahu a integrity zájmových dat. Data, informace jako takové jsou nehmotné. Vše, co je uloženo na datovém uložišti, jako je pevný disk počítače, serveru či jiném přepisovatelném záznamovém zařízení typu CD, DVD, BlueRay, flashdisk anebo externí paměťová média, je relevantně snadno pozměnitelné a manipulovatelné. Z výše uvedeného důvodu je vždy nezbytné ukládaní takovýchto nehmotných dat na nepřepisovatelné médium a pro zajištění jejich integrity připojit tzv. hash, nebo-li kontrolní součet (**MD5** – 128 bitů, **SHA-1** –

160 bitů, **SHA-2** – 224, 256, 384, 512 bitů). Datová stopa má reálný fyzikální význam. Médium se zachovanými datovými stopami je věcným důkazem. Negativní využití digitální stopy spočívá ve vysoké variabilitě různých druhů medií. K médiu musí existovat zařízení, které je schopno data číst. S postupem času se schopnost přečíst médiu snižuje.[36]

3.1.2. Latentnost digitální stopy

Latentnost digitální stopy je jedna ze základních charakteristických vlastností. Data ve formě záznamů jsou uchována ve virtuálním prostředí anebo na paměťovém médiu a nejsou viditelné pouhým okem, jako je tomu u některých kriminalistických stop v materiálním prostředí. Různé druhy a typy systémových záznamů nebo souborů jsou taktéž pro běžného uživatele neviditelné, pokud není držitelem zvláštních administrativních práv, bez nichž je nelze zjistit a dále je zpracovávat a poskytnout je orgánům činným v trestním řízení. Jistě je na místě konstatovat, že smazané či přepsané soubory na datových nosičích, přeformátované disky, nebo jinak poškozená či pozměněná datová media jsou také digitálními stopami s vysokou mírou latence.

Pozitivní využití spočívá hlavně v tom, že pokud se jedná o neznalého uživatele, zanechává digitální stopy, aniž by si to sám uvědomoval. Pro zpřístupnění latentních dat je potřeba, jak již bylo uvedeno, buď zvláštní administrativní práva či specializovaný software nebo vybavení.[37] Drobnou odchylkou jsou pak metadata, která jsou latentní a mohou je obsahovat „běžné“ soubory jako fotografie, zvukové nahrávky či videa a alespoň částečně je lze zjistit základními uživatelskými znalostmi práce s výpočetní technikou.

---

[36] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách*. Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

[37] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách*. Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

3.1.3. Časová trasovatelnost digitální stopy

Velké množství datových stop je ve výpočetních a komunikačních systémech prokazatelně spojeno s velmi přesným časovým údajem. Téměř každá digitální stopa je nositelem tzv. časové trasovatelnosti, díky které je možné prostřednictvím forenzních analýz určit přesnou časovou posloupnost dané události. Každý psaný text, audiozáznam, fotografie či dokument s sebou nese informace o času vytvoření, čase poslední změny, počtu úprav, o svém původu. Každé digitální zařízení je nositelem systémového času, což není nic jiné než vnitřní hodiny daného zařízení. Každá provedená operace pomocí aplikačního nebo systémového vybavení je opatřena „časovou známkou“. Díky tomuto časovému údaji je možné určit, kdy proběhlo poslední přihlášení do počítače nebo kdy došlo ke vzniku či pozměnění zájmového dokumentu. Negativním využitím se zde jeví hlavně znalost uživatele, který s příslušnými administrativními oprávněními může pozměnit neboli antidatovat systémový čas nebo změnit časové značky.[38] Podle charakteru dat je možné některé časové údaje zjistit z metadat, v některých případech pak k tomu musí být adekvátní softwarové vybavení.

3.1.4. Vysoká obsažnost digitální stopy

Digitální stopy teoreticky obsahují velmi vysokou informační hodnotu. Informace ve virtuálním prostředí tedy i digitální stopy mají dnes multimediální charakter. Jsou nositelem dostatečného množství informací relevantních ke kriminalistickým nebo forenzním zkoumáním a nad to obsahují informace o uživateli (který může být i pachatelem prověřované kriminalisticky relevantní události), ale mohou obsahovat i další související informace o soukromém životě, volnočasových aktivitách, stylu života, taktéž ale může býti nositel informace o pohybu pachatele ve virtuálním prostředí, o jeho posledních aktivitách na internetu, o posledních připojených datových nosičích, nebo o používaných aplikacích či službách a v neposlední řadě také informace o uložených heslech.

[38] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách.* Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

Negativním využitím ve vysoké obsažnosti dat může dojít k přesycení a kriminalisticky relevantní údaje mohou být přehlédnuty nebo nedoceněny.[39]

3.1.5. Uchování a kvalita je ovlivněna řadou subjektivních faktorů

Determinujícím faktorem jsou legislativní a interní předpisy, odbornost administrace ICT a institucionální kultura úrovně informační bezpečnosti. Při správně nastavených parametrech auditovatelnosti informačních systémů a jejich praktické realizace jsou v ICT systémech zachovány požadované informace, využitelné jako datové stopy. Jedná se o zcela stejný princip, ze kterého vychází samotná definice *„kriminalistické stopy, která je využitelná pomocí přístupných kriminalistických, přírodovědných a technických metod, prostředků a postupů*.“[40] V případě, že nebudou dodržována základní pravidla je praktická použitelnost digitálních stop zpravidla nízká. Není-li možné digitální stopu uchovat, není v podstatě její možnost jí využít jako důkaz v trestním řízení.

3.1.6. Heterogennost a komplexnost prostředí

Prostředí výpočetních a komunikačních technologií v institucích bývá velmi rozmanité a heterogenní. Heterogenní systém často tvoří integrované celky, napříč kterými probíhá zpracování informací. V každé části složitých komplexů je možné tak najít důkazní materiál, i když by v jiných částech nebyl nebo by byl zničen. Pro vyhledávání, fixaci a analýzu digitálních stop je často potřebné velké množství vysoce kvalifikovaných specialistů. Tyto procesy jsou často velmi časově náročné a vyžadují velké množství nejrůznějších zdrojů.[41]

---

[39] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách.* Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

[40] PORADA, Viktor. *Kriminalistika: (Úvod, technika, taktika).* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2007. ISBN 978-80-73-80-038-3. s. 56.

[41] RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách*. Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

3.1.7. Komplexnost digitální stopy

Kvalita a rychlost zajišťováni digitálních stop hraje zásadní roli při prověřování a vyšetřování trestných činů a pro další vedení trestního řízení a provádění dalších procesních úkonů je pak důležitá komplexnost prostředí, ve kterém byly digitální stopy zajištěny. Je nezbytné rozlišovat, zda se jedná o zajištění digitální stopy jako celku (notebook, tablet, stolní PC nebo mobilní telefon), reálně tedy věcné stopy zajištěné v trestním řízení, která obsahuje data, jež mají vztah ke kriminalisticky relevantní události a jsou digitální stopou nebo zda-li se jedná o stopu, která bude představovat prostá data uložená v informačních systémech a uložištích providera konektivity či poskytovatele internetových služeb.

Zajištění digitálních stop uložených v zařízení má svůj význam, jelikož se tak stane bez zřejmého porušení integrity dat a lze nosič takových informací odeslat na další znalecká zkoumání, čímž budou informace procesně zajištěny a zadokumentovány pro účely dalšího dokazování v trestním řízení. Takové stopy je možné zajistit i bez přítomnosti specializovaného pracovníka. V případě jde-li o zajištění digitálních stop z tzv. živého systému, nebo bude potřeba data získat z uložišť, je účast specializovaného pracovníka znalého v oboru při tomto úkonu nezbytná.[42]

[42] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 214. ISBN 978-80-7380-589-0.

4. Metody a postupy zajišťování digitálních stop

V rámci provádění domovní prohlídky je vždy zcela stěžejní výběr správné metody pro zajištění všech upotřebitelných digitálních stop na místě činu. Stanovení správného technicky taktického postupu představuje klíčový okamžik, který může velmi zásadně ovlivnit možnost nalezení a vyhledání digitální stopy, její zajištění a následně také její využitelnost a vytěžitelnost.

4.1. Metody zajišťování digitálních stop při domovní prohlídce

Předně je vhodné zdůraznit, že pro potřeby této kapitoly bude pracováno s pojmem domovní prohlídka, byť jsou v praxi velmi podobné, případně zcela totožné, postupy a metody při provádění prohlídek jiných prostor a pozemků, proto není nezbytně nutné vymezovat se v dalším textu vůči prohlídce jiných prostor a pozemků.

Samotný proces zajišťování výpočetní a komunikační techniky při domovní prohlídce je pro vytěžitelnost a využitelnost získaných stop jedním z klíčových okamžiků. Zajišťování takovéto techniky by nemělo být prováděno policisty bez příslušné specializace s platným osvědčením[43], nad to je pak vhodná součinnost znalce z příslušného oboru, zvláště pak v případech, kdy jsou zajišťovány digitální nosiče a data či výpočetní technika v aktivním provozu. Přítomnost znalce či policisty se specializací na zajišťování výpočetní techniky je vhodným postupem policejního orgánu při provádění domovní prohlídky k zajištění dané stopy podle doporučených technologických a technických postupů, ale také se bude jednat o postupy, které jsou v rámci trestního řízení procesně správné a přezkoumatelné v řízení před soudem, a tudíž získané informace mohou obstát jako relevantní důkaz v trestním řízení.

V následujících podkapitolách budou čtenáři předestřeny nejčastější metody využívané při provádění domovních prohlídek k zajišťování digitálních stop:

- zajištění stopy in natura

[43] Čl. 2 písm. c) pokynu policejního prezidenta č. 100/2021, o kriminalisticko-technické činnosti

- zajištění digitální stopy prostřednictvím jednoúčelového technického zařízení
- zajištění digitální stopy pomocí zkoumaného zařízení
- zajištění digitální stopy ze spuštěného zkoumaného zařízení

4.1.1. Zajištění digitální stopy „in natura“

Zajištění stopy in natura je běžný pojem v kriminalistice, kterým se rozumí zajištění stopy v její skutečné materiální podobě tak, jak byla vyhledána na místě kriminalisticky relevantní události. V případě zajišťování digitálních stop při domovní prohlídce pak je takovým postupem docíleno toho, že nedojde k zásahu do integrity stopy. Přirozeně pak v případě zajištění in natura nesmí dojít k žádnému zálohování či předběžnému zkoumání.

Stopa se při domovní prohlídce označí číslem dle protokolu a provede se její fotodokumentace. Zadokumentovaná stopa se následně zabalí do vhodného obalu, tak aby nedošlo k jejímu poškození. Po zabalení se stopa značí zpravidla číslem jednacím trestního spisu a podpisem osoby, které její zabalení provedla. Následné zkoumání stopy je prováděno na specializovaném pracovišti např. v laboratorních prostorách Kriminalistického ústavu, Odboru kriminalistické techniky a expertíz nebo u soudního znalce. Tato metoda se nejvíce aplikuje při zajištění komunikační a mobilní techniky, jelikož její samotné zkoumání je velmi časově náročné a vyžaduje určité technologické vybavení. Případně se tato metoda používá, pokud je potřebné provést komplexní zkoumání zajištěné stopy, u které provedení zálohy či bitové kopie vyžaduje nestandartní technické vybavení.[44] Tento způsob zajištění se volí u stolních počítačů, mobilních telefonů a jiné komunikační techniky, zvláště v těch případech, kdy zařízení nejsou spuštěná a aktivní.

4.1.2. Zajištění digitální stopy jednoúčelovým technickým zařízením

Nejčastějším a nejpoužívanějším způsobem, jak zajistit digitální stopu a pořídit její bitovou kopii, je prostřednictvím jednoúčelového technického zařízení. Pod

[44] PORADA, Viktor. *Kriminalistika: (Úvod, technika, taktika).* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 114-145. ISBN 978-80-7380-490-9.

takovým zařízením si můžeme představit „speciálně upravený počítač“, který je používán výhradně k tomuto účelu. Často se jedná o desktop[45], který je osazen dostatečným počtem SATA kabelů pro připojení pevných disků (je vhodné, vzhledem k rozvoji doby, aby takové zařízení obsahovalo i starší typy konektorů). Standardně je pak v počítačích s forenzními nástroji a softwarem používán operační systém GNU/Linux.

Uzpůsobení a nastavení techniky je nutné k zajištění ochrany integrity dat tím, že v případě zapojení jakéhokoli média k tomuto technickému forenznímu počítači nedojde k automatickému „nabootování“ tohoto média a k neautorizovanému zápisu systémových informací. Tato funkce je zásadní, neboť by v opačném případě došlo k systémovému zápisu a nedalo by se s takovou digitální stopou dále pracovat a digitální stopa by se stala stopou znehodnocenou a nebylo by možné jí použít jako důkaz v trestním řízení.

V případě, jeli specializovaný pracovník vybaven specializovaným forenzním zařízením pro vytváření bitových kopii, je vytvoření bitové kopie USB disku, paměťové karty snadné. Zařízení samotné je vybaveno vlastním operačním systémem, kde je zajištěna ochrana proti zápisu.[46]

Dlužno dodat, že se pro účely zajištění stop jedná o nejčastější a nejpoužívanější metodu, nicméně ne vždy ji lze realizovat již během provádění domovní prohlídky. Výpočetní technika by byla nejprve zajištěna in natura a poté by byla zkoumána touto metodou na specializovaném pracovišti KÚ, OKTE anebo u soudního znalce.

4.1.3. Zajištění digitální stopy pomocí zkoumaného zařízení

Při provádění domovní prohlídky může nastat situace, kdy není možné zajistit digitální stopy, resp. pořídit bitovou kopii za pomocí technologického počítače s forenzními nástroji či jiného jednoúčelového zařízení. Takový specifický případ je řešen specialistou přímo na místě domovní prohlídky tím, že je vytvořena bitová kopie přímo v zajištěném zájmovém zařízení. Typickým příkladem takového

---

[45] Desktop z anglických slov desk „stůl“ a top „na vrchu“ je typ počítače, který je nejvíce rozšířen a každý ho zná, tzv. stolní počítač. Online. Dostupné z: https://it-slovnik.cz/pojem/desktop. [citováno 2024-02-25].

[46] KOTHÁNEK, Jaroslav. *Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení.* Policie ČR, Praha, 2008.

postupu je v případě, kdy není možné z počítače zajistit bezpečné vyjmutí pevného disku, což nezřídka nastává u moderní výpočetní techniky typu netbook nebo ultrabook popřípadě u zařízení zn. Apple iMac, kdy je hardware počítače umístěn za monitorem.

Pokud v rámci domovní prohlídky dospěje specialista k závěru, že pořízení bitové kopie bude provedeno prostřednictvím zajištěného zájmového zařízení, je další postup zcela totožný s postupem, který by byl použit pro vytvoření bitové kopie za pomocí technického počítače či jednoúčelového technického počítače. V tomto případě musí dojít k zavedení námi zvolené distribuce systému GNU/Linux. Pokud by došlo k zavedení operačního systému, který je v zařízení nainstalován, došlo by k nevratnému poškození informací zaznamenaných na disku počítače.[47]

4.1.4. Zajištění digitální stopy ze spuštěného zájmového zařízení

V posledních několika letech dochází ke značnému rozšíření úkonu zajišťování digitálních stop ze spuštěného zájmového zařízení, neboť se rozšiřují možnosti související se šifrováním dat a využívání šifrovacích programů. Zajištění takové bitové kopie není v dnešní době z pohledu kriminalistické praxe nic neobvyklého. Pokud existuje relevantní podezření, že by se v zájmovém zařízení mohl nacházet nějaký program, který využívá šifrování, je vhodné, aby bylo zařízení v zapnutém stavu a eventuálně lze data dokumentovat, jelikož nebudou opatřena šifrováním.

U zapnutého počítače lze zájmová data zajistit pouhým kopírováním na pevný disk, avšak je nezbytné brát zřetel na kompletní zkopírování dat s verifikací jejich neporušenosti. Pořízení bitové kopie disku společně s otiskem RAM paměti vždy přinese komplexní data a zřejmě bude jejich vyšší míra využitelnosti v trestním řízení než jen prosté kopírování disku. Vytvoření bitové kopie ze spuštěného zájmového zařízení je velmi důležité i pro zajištění digitálních dat umístěných na serverových uložištích. Tento způsob zajištění může být proveden výhradně policistou s příslušnou specializací a platným osvědčením nebo osobou znalce.[48]

---

[47] KOTHÁNEK, Jaroslav. *Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení*. Policie ČR, Praha, 2008.
[48] KOTHÁNEK, Jaroslav. *Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení.* Policie ČR, Praha, 2008.

4.2. Druhy zajišťovaných digitálních stop

Bezprostředně v návaznosti na metody zajišťování digitálních stop je na místě uvést druhy digitálních stop, které mohou být zajišťovány během trestního řízení, tedy i při provádění domovní prohlídky. Některé se shoda uvedených metod pak budou pro určitou skupinu digitálních stop zcela typicky používané a korespondují s formou dat a možnosti je z nositele digitální stopy získat pro účely trestního řízení.

Existují dvě skupiny nositelů digitálních stop, a to technika, která obsahuje digitální stopy a prostá data obsahující digitální stopu. Pro dokreslení je možné čtenáři více specifikovat tyto dvě oblasti.

Zajištění techniky, která obsahuje digitální stopy

- osobní počítače, servery, notebooky, netbooky, tablety
- datová média – HDD, flash disky, výměnná média, CD a DVD, paměťové karty
- mobilní telefony a jiné komunikátory, kapesní počítače, diáře, databanky
- aktivní síťové prvky – routery, firewaly, NAS servery
- ostatní elektronika, která může obsahovat datové stopy

Zajištění dat, které jsou digitální stopou

- zajištění emailové komunikace
- zajištění www stránek a serverů
- zajištění databází
- zajištění účetních dat
- zajištění ostatních dat podle spáchaného trestného činu

- zajištění tiskových a obrazových výstupů, popř. audio či video záznamů, které byly pořízeny nebo zpracovány výpočetní technikou
- zajištění písemné dokumentace, která má vztah k digitálním stopám (listinné důkazy, faktury, objednávky)

4.2.1. Zajištění počítače ve vypnutém stavu

Zajišťuje se pouze samotná skříň počítače. Počítače, notebooky, netbooky a jiné vždy musíme zajišťovat jako celek, to znamená včetně napájecích kabelů a nezbytných periférií. Podle konkrétních okolností je možné zajištění pouze samotných pevných disků. Takovéto řešení se nedoporučuje u serverů nebo zařízení s RAID polem. Zajištěný počítač se musí řádně zabalit a zapečetit. Musíme zajistit, aby nedošlo k žádné neautorizované manipulaci. V rámci protokolu, do kterého zaznamenáváme zajištění objektu je potřeba uvést přesný popis zajištěného objektu, typ, stav, výrobní číslo.

4.2.2. Zajištění počítače v zapnutém stavu

Nejlepším postupem při zajišťování počítače v zapnutém stavu je jednoznačně vytvoření bitové kopie viz. Shora uvedené metody. V rámci prvotních kroků je nutné ohledat zajišťovaný počítač či server. Ohledání spočívá ve zjištění informací o spuštěných aplikacích, přítomnosti šifrovacího nástroje či jaké a zda jsou připojeny síťové disky. V případě zajišťování aktivní zapnuté techniky je vhodné vyslechnout jejího majitele ke způsobu používání zařízení či sdělení hesel, zejména v případech, kdy osoba, u níž jsou věci zajišťované spolupracuje s policejním orgánem. Jakékoli další informace ze strany majitele k předmětnému zařízení mohou usnadnit další dílčí úkony trestního řízení při dokumentaci, zpracování a vyhodnocování získaných informací.

V případě zjištění skutečnosti, že na zařízení není použit žádný šifrovací nástroj nebo jiná překážka, tak je možné zařízení standardně vypnout. V opačném případě by mohlo dojít k nevratné ztrátě dat, a tudíž je potřebné zajištění dat z tzv. „živého“ systému. V takovémto případě se vytvoří bitové kopie z nezašifrovaného systému nebo samotné vykopírování dat. Jak již bylo zmíněno, u vykopírování dat nemusí dojít k zajištění kompletního obsahu zařízení, ovšem zajištění tímto způsobem je vždy lepší, než nemít data žádná. Ze strany znalce je možné provedení forenzní analýzy přímo na místě domovní prohlídky.[49]

[49] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet.* 3rd ed. Waltham, MA: Academic Press, c2011. s. 38. ISBN 978-0-12-374268-1.

4.2.3. Zajištění pevných disků

Prvotním úkonem je vyjmutí pevného disku ze zařízení, které by měl provádět znalec či IT specialista. Externí neboli výměnné disky se zajišťují vždy jako celek včetně příslušenství a napájecích zdrojů. Ideální je uložení takové disku do antistatického obalu a následně do bublinkového obalu či sáčku ORGATECH. Vždy musí dojít k jeho zapečetění.

4.2.4. Zajištění výměnných datových médií

Do této kategorie spadají CD, DVD, BlueRay, datové pásky, flashdisky, paměťové karty. Nezajišťujeme lisované disky CD-ROM/DVD-ROM tovární výroby. Při zajišťování takovýchto médií musíme dbát na jejich roztřídění dle typů a míst, na kterých byly v rámci domovní prohlídky nalezeny. Stejné typy datových medií můžeme uložit do jednoho obalu. Akcent u zajišťování flashdisků je nutné klást na jejich vyhledání, neboť jsou v současné době tyto datová uložiště konspirována a mají různé podoby (např. podoba hračky, nože, nábojnice, klíče aj.).

4.2.5. Zajištění mobilních telefonů a jiných komunikátorů

Při zajišťování mobilních telefonu při domovní prohlídce musí dojít k jejich zajištění s napájecím adaptérem. V případě, že se jedná o mobilní telefony opatřeny heslem či gestem je žádoucí takové to informace získat od jejich majitele a řádně hesla či gesta zaznamenat. V případě, že je mobilní telefon zapnutý, nemělo by dojít k jeho vypnutí, ale pokud je to možné, tak ho přesunout do režimu letadlo, abychom zamezili připojení na internet a případné ztrátě, resp. smazání dat na dálku. Vzhledem k tomu, že je v dnešní době řada mobilních telefonu opatřena tzv. FaceID, je nutné dbát na to, aby mobilní telefon nenačetl obličej kriminalistů provádějících domovní prohlídku, neboť by zařízení mohlo detekovat „neoprávněnou osobu“ a v důsledku by mohlo dojít k zašifrování potřebných dat anebo jejich smazání, tudíž by k nim byl znemožněn přístup a nebylo by možné je zadokumentovat. Pokud je telefon ve vypnutém stavu platí obecné doporučení ho nezapínat či jej jakýmkoli způsobem rozebírat. Do protokolu zaznamenáme stav

mobilního zařízení, jeho typ a zabalíme předepsaným způsobem. Takto zajištěné mobilní zařízení dopravíme ke znalci.[50]

4.2.6. Zajištění aktivních síťových prvků

Mezi aktivní síťové prvky řadíme routery, firewally, bezdrátové access pointy apod. Z takových zařízení se zajišťují jen jejich provozní data a nastavení. Na začátku provádění ohledání anebo zajišťování je potřeba stanovit, zda bude zařízení zajišťováno in natura anebo bude vykopírován obsah s provozními informacemi.

V případě, že by došlo k vypnutí dojde k nezvratné ztrátě dat. Při zajišťování dat na místě je potřeba provést administraci pomocí síťového připojení, které často síťové prvky nabízí. Tímto způsobem může být zjištěno, odkud jsou síťové prvky spravovány. Při tomto úkonu je nutná spolupráce správce sítě pro prohlášení do aktivního síťového prvku, přičemž takový postup lze v ideálních podmínkách dokumentovat pořízením videozáznamu anebo alespoň fotograficky. V případě, že by bylo nutné zajištění celého zařízení aktivního síťového prvku, zajišťuje se standartním způsobem.

4.2.7. Zajištění ostatní elektroniky

Jiná elektronická zařízení anebo zařízení, která by mohla mít vlastní paměťové uložiště, zřejmě netvoří a priori okruh předmětů, v nichž lze očekávat přínos pro trestní řízení, nicméně mohou představovat významný zdroj informací, které budou důležité pro objasnění kriminalisticky relevantní události. Typicky se může jednat o fotoaparáty, kamery, MP3 přehrávače, satelitní přijímače, smart zařízení jako TV, hi-fi panely a další.

Dle konkrétních okolností na místě souvisejících s konkrétní prověřovanou trestnou činností je ovšem vhodné zvážit jejich přínos a následně je zajišťovat zpravidla in natura za účelem jejich dalšího zkoumání.

4.2.8. Zajištění www stránek a www serverů

Zajišťování webových stránek je jedním z nejčastějších úkonů prováděných v rámci trestního řízení. Jedná se o zajištění dat z internetového nebo

[50] VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů*. Zlín, 2013. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

intranetového prostřední společností. Buď můžeme provést tzv. přímé stažení stránek pomocí nástroje HTTrack Website Copier nebo prosté snímky obrazovky za pomocí modulu FireShot pro Mozzila Firefox, Maxthon, další eventualitou je prosté vyexportování v prohlížeči jako náhled k tisku v *.PDF. Při zajištění ovšem vždy musí dojít k vytvoření kontrolního otisku HASH (MD5, SHA-1, SHA-2), který bude uložen na datovém médiu a bude součástí spisového materiálu.

Rozsah zajištěných dat z www stránek může být různý:

- zajištění jednotlivých www stránek, kdy se může jednat o stránku z diskuse, popřípadě profil na sociální síti.
- zajištění všech www stránek příslušné domény např. e-shop
- zajištění všech dat určitého www serveru – takové zajištění vždy probíhá přímo u samotného provozovatele serveru, všechna data musí být zajištěna spolu se zdrojovými kódy a scripty, databází i grafikou[51]

4.2.9. Zajišťování emailových zpráv

Zajišťování emailových zpráv v rámci domovní prohlídky, popřípadě zajišťování emailových zpráv u poskytovatelů emailových služeb provádí IT specialista policie. Zajištění u poskytovatelů emailových služeb pak policista, avšak by se nejednalo o úkony související s domovní prohlídkou a zpravidla by bylo provedeno operativně pátracím prostředkem sledování osob a věcí dle ust. § 158d odst. 3 trestního řádu. Při zajišťování emailových zpráv musíme dodržovat předepsané postupy, emailové zprávy se zajišťují přímo v zájmovém emailovém účtu prostřednictvím uživatelského rozhraní, do nějž musí být uživatel v době provádění domovní prohlídky přihlášen, jinak by bylo opět nezbytné postupovat v návaznosti na uvedený operativně pátrací prostředek. Zprávy se zajišťují vždy ve formátu eml nebo msg. V případě, že by to nebylo možné, je potřeba zajistit email s jeho hlavičkou neboli záhlavím zprávy. Emailové zprávy se zajišťují výhradně v elektronické podobě.

Pokud to situace na místě umožňuje, je vhodné zajistit původní emailovou zprávu, která bude obsahovat tzv. hlavičku emailu, která je relevantním zdrojem digitálních stop. Taková zpráva obsahuje veškeré informace o přijatém emailu, které jsou

[51] KOLOUCH, Jan. *Cybercrime*. Praha: Edice CZ.NIC, 2016. s. 85-135. ISBN 978-80-88168-18-8.

hlavně IP adresa, ze které byl email odeslán, díky které je možné ustanovit konkrétní osobu uživatele, informace o celé cestě emailu internetem (přesné datum a čas odeslání, přes jaký poštovní server došlo k odeslání, komu byl dále adresován), a další informace.[52]

4.2.10. Zajišťování databází

Při zajišťování databází je vždy potřeba spolupráce se správcem databázového serveru a zpravidla se k tomu provádí videodokumentace a fotodokumentace, eventuálně pak snímkování obrazovky. Pokud není jiná možnost, zajistí se celý databázový server nebo počítač, na kterém databáze běží. Databáze můžeme rozdělit na tzv. **lokální databáze**, mezi které patří Microsoft Office Access, Fox Pro a na **DB server** nazývaný taktéž SQL server, který může být umístěn dokonce na zcela jiném místě. Jednotlivé operace s těmito typy serverů se provádí pouze dálkově před administrativní rozhraní databáze.

Zajištění lokální databáze se provádí tím způsobem, že se při provádění domovní prohlídky v aktivním počítači vyhledá její umístění a poté se zájmové soubory vykopírují na datové médium. V případě zajištění databází, které jsou umístěny na datových serverech, je postup pro jejich zajištění složitější. Nejdříve je nutné zjistit typ a verzi DB serveru a platformy, na které je spuštěn, následně kde a v jaké formě jsou umístěna data zajišťované databáze a zjistit přihlašovací údaje a heslo. Přihlášení do DB serveru je možné pouze za spolupráce s administrátorem přes administrátorské rozhraní. Pokud se nám tento krok povede, dojde k vytvoření úplné zálohy zajišťované databáze. Zajištěná data musí být opatřena kontrolním otiskem HASH (MD5, SHA-1, SHA-2). Celý tento úkon musí být zaznamenán do protokolu.[53]

4.3. Ukládání a balení zajištěných digitálních stop

Všechny stopy, zajištěné při domovní prohlídce, je nutné ochránit před poškozením, a zvláště v případě digitálních stop pak rovněž proti neoprávněnému, neautorizovanému zásahu do jeho integrity. Nevhodné nakládání se stopami

---

[52] BRADÁČ, Albert, KLEDUS, Miroslav a KREJČÍŘ, Pavel. *Soudní znalectví*. Brno: Akademické nakladatelství CERM, 2010. s. 95-126. ISBN 978-80-7204-704-8.
[53] KOLOUCH, Jan. *Cybercrime*. Praha: Edice CZ.NIC, 2016. s. 138. ISBN 978-80-88168-18-8.

a jejich „narušení“, ztráta či poškození snižuje jejich potenciální využitelnost v trestním řízení, protože by tím mohlo dojít ke zmaření důkazu, který obsahují. Narušení integrity digitálních dat, viz podkapitola 1.4, pak obdobně značí využitelnost takových informací v trestním řízení, a proto je nutné při manipulaci, ukládání a balení provádět profesionálně, k čemuž je zpravidla určen právě policista s platným osvědčením, který postupuje vždy v souladu s interními akty řízení, zvlášť pak:

- závazný pokyn policejního prezidenta č. 100/2001, ke kriminalisticko-technické činnosti Policie České republiky,
- metodický pokyn ředitele KÚP č. 7/2001, kterým se upravuje činnost orgánů Policie České republiky při zajišťování výpočetní techniky a dat pro účely následného znaleckého zkoumání.

Pro úplnost je na místě doplnit formální souvislosti při balení, zabezpečení a označování stop zajištěných při domovní prohlídce.

Balení stop usnadňuje jejich přenášení a alespoň částečně je chrání před poškozením, přičemž obecně jsou používané – transparentní sáčky PČR (tzv. ORGATECH, debasafe) v různých velikostech, silnostěnné plastové či papírové pečetící pytle, případně krabice. Pokud je to pro ochranu předmětu (zajištěné stopy) vhodnější, je použit původní obal od výrobku.

Zabalené stopy musí být označeny číslem jednacím trestního spisu, číslem stopy, musí být uvedeno místo zajištění a eventuálně pak stručný popis, a to z důvodu zamezení záměny stop, zvláště v případech, kdy je v rámci realizace trestního spisu prováděno více domovních prohlídek a prohlídek jiných prostor a pozemků a jsou při nich zajišťovány stopy obdobného charakteru.

Zabezpečení před neoprávněným zásahem do integrity stopy je proveden již vhodným balením stopy, neboť se zpravidla jedná o obalový materiál, který disponuje pečetící anebo zalepovací plochou, jejíž mechanické otevření není možné bez poškození obalu jako celku. Případy, kdy jsou použity jiné obalové materiály, kupříkladu původní obaly, jsou pro zajištění integrity kompenzovány použitím pečetících pásek a opatřováním podpisů nezúčastněné osoby. Zabalené a zabezpečené stopy jsou rovněž dokumentovány fotograficky a je to rovněž poznamenáno do protokolu, viz další podkapitola.

Specifickým případem je ovšem zajišťovaní zařízení v případech, kdy je potřeba zajistit jeho dobíjení. Způsob balení a zabezpečení je velmi podobný, avšak lepení obalového materiálu a pečetění je provedeno tak, aby k zařízení vedl napájecí kabel, kterým je možné jej dobíjet.

4.4. Protokolace zajištěných digitálních stop

Každý úkon trestního řízení musí být v rámci trestního spisu řádně protokolován, bez výjimky tedy i skutečnosti, jak policejní orgán pro účely trestního řízení získal či zajistil digitální stopy. Obecně je možné konstatovat, že je v konkrétních případech zpracován:

- **Protokol o odnětí věci**, podle ust. § 79 trestního řádu,
- **Protokol o vydání věci**, podle ust. § 78 trestního řádu,
- **Protokol o provedení domovní prohlídky, prohlídky jiných prostor a pozemků**, podle ust. § 82 trestního řádu,
- **Protokol o ohledání místa činu**, podle ust. § 113 trestního řádu,
- **Protokol o zajištění dat** § 88, § 88a, § 158c, § 158d odst. 3 trestního řádu,
- eventuelně pokud jsou informace obsažené v digitální stopě získané postupem dle § 8 odst. 1, odst. 2, odst. 5 trestního řádu, je k tomu zpracován úřední záznam s vyhodnocením.

Protokolace tedy koresponduje s použitými instituty, viz kapitola 2, a je prováděna obligatorně písemnou formou, která má formální náležitosti – označení policejního orgánu provádějícího úkon, datum, čas a místo provedení úkonu, označení policisty provádějícího úkon a dále signaturu osob přítomných úkonu. Typicky u protokolu o provedení domovní prohlídky je to mimo policisty policejního orgánu rovněž kriminalistický technik, policejní specialista k zajišťování výpočetní techniky a digitálních stop, nezúčastněná osoba, osoba u níž se domovní prohlídka provádí, pokud je přítomna, prověřovaná osoba, pokud je úkonu přítomna a právní zástupce, případně jiné osoby, pokud je jejich přítomnost u domovní prohlídky nutná (příkladem specialista Hasičského záchranného sboru v potenciálně nebezpečných prostorech nelegálních laboratoří na výrobu

omamných a psychotropních látek, který detekuje obsah nebezpečných látek v prostředí).

Nad rámec písemné protokolace je pak pořizována videodokumentace, nanejvýš vhodné je již natáčení zahájení domovní prohlídky, včetně rozpečetění zájmového obydlí (vstupní dveře apod.), prvotní obhlídka prostor obydlí a zachycení stavu obydlí, což může mít význam například u výpočetní techniky, která je aktivní, dále také specifické kroky u zajišťování stop (viz některé způsoby zajišťování) a v neposlední řadě ukončení domovní prohlídky. Obdobně je pak pořizována fotodokumentace, a to zejména s akcentem na vyfocení jednotlivých zajišťovaných stop a jejich bezpečné, transparentní zabalení.

V užším pojetí, vztaženo na zajišťování digitálních stop během domovní prohlídky, je pak nutné vždy dokumentovat:

- identifikace zajištěných zařízení a paměťových médií, a jejich stav, markanty a poškození,
- podrobný popis, aby nemohlo dojít k záměně,
- počet jednotlivých typů objektů, zaznamenat místa, kde byly nalezeny nebo odkud byly vyjmuty,
- zapojení výpočetní techniky a také nestandartní zapojení,
- co a jakým způsobem bylo zajišťováno, použité nástroje, do jakého obalu byla zajištěná technika zabalena,
- fotodokumentace – celek, výrobní štítek – sériové a výrobní čísla, typ a model zařízení a podobně.

5. Analýza digitálních stop zajištěných při domovní prohlídce

Pro úplnost je na místě uvést, že digitální stopy zajištěné při domovní prohlídce musí být podrobeny dalšímu zkoumání a vyhodnocení, z čehož mohou být získány konkrétní informace, důkazy, které mohou rozkrýt celý rozsah prověřované trestné činnosti, případně bude zjištěn modus operandi, účast dalších osob – spolupachatelů apod. Zkoumání digitálních stop zajištěných při domovní prohlídce je v následných úkonech trestního řízení prováděno formou:

- odborného vyjádření
- znaleckého posudku
- analýzy specializovaným pracovištěm, typicky oddělení analytiky a kybernetické kriminality na územních odborech.

Odborné vyjádření

Odborné vyjádření je prováděno na základě žádosti o provedení odborného vyjádření a nejčastěji je směřováno na Kriminalistický ústav anebo Odbor kriminalistické techniky a expertíz, na pracoviště z oboru elektrotechnika, odvětví analýza dat a zkoumání nosičů dat. Kriminalistický ústav i OKTE jsou znaleckým pracovištěm ve smyslu § 7 zákona č. 245/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech, zapsány v oboru kriminalistika podle § 48 zákona č. 254/2019 Sb., téhož zákona a mohou podle ust. § 105 odst. 1 trestního řádu zpracovat odborné vyjádření a znalecký posudek.

Žádost o odborné vyjádření musí přirozeně obsahovat identifikační údaje trestního spisu, popis prověřované trestné činnosti a její právní kvalifikaci, specifikace odesílaných stop ke zkoumání a zásadní jsou pak otázky, které mají být odborným vyjádřením zodpovězené. V návaznosti na zkoumání digitálních stop je nejčastější vytváření bitové kopie z paměťových uložišť a zařízení (mobilní telefony, pevné disky, paměťové karty, flashdisky aj.)

Vzor otázek:

1. Vytvořte identickou bitovou kopii pevných disků předloženého zařízení

2. Data nalezená při zkoumání nosičů zpřístupněte dožadujícímu orgánu a vybraná data vhodným způsobem zadokumentujte

3. Další, dle uvážení znalce

Bitové kopie či jiné výstupy z odborných zkoumání jsou poté vyhodnocovány policejním orgánem a je zjišťována jejich relevance a důkazní hodnota, tudíž jejich další použitelnost v trestním řízení.

Znalecký posudek

Znalecký posudek provádí Kriminalistický ústav, Odbor kriminalistické techniky a expertíz či soudní znalec, vždy podle potřebné specializace, a to na základě opatření o přibrání znalce v souladu s ust. § 105 odst. 1 trestního řádu. Opatření formálně obsahuje identifikační údaje trestního spisu, popis prověřované trestné činnosti a její právní kvalifikaci, specifikace odesílaných stop ke zkoumání a zásadní jsou pak otázky, které mají být znalcem zodpovězeny. Obecně platí, že je v trestním řízení přibrán znalec, místo vyžadovaného odborného vyjádření, v případech, kdy je nutno zodpovědět právně, technicky či jinak odborně složitější otázky, eventuálně je nutné použití speciálních technologií, forenzních nástrojů atd. V případě znaleckého zkoumání a odborných vyjádření v oblasti kybernetiky, výpočetní techniky anebo chemie, jsou pracoviště Kriminalistického ústavu a OKTE plně vybavené a jde zejména o rozsah a složitost otázek ke konkrétnímu zkoumání. Zvláště v oblasti kybernetiky a výpočetní techniky disponují tyto dvě pracoviště v zásadě nejlepšími forenzními nástroji, oproti soukromým znalcům, neboť někteří vývojáři forenzního softwaru poskytují software a jeho aktualizace pouze pro „law enforcement“ instituce, což bezesporu tato pracoviště jsou.

Vzor otázek (znalecký posudek na mobilní telefon)

1. Popsat zajištěné mobilní telefony a všechny datové nosiče, které jsou jejím příslušenstvím (SIM karty, paměťové karty).

2. Pořídit kopii uživatelských souborů, provést rekonstrukci a kopii vymazaných uživ. souborů na uvedené technice (včetně příslušenství)

a zkoumat získaná data s přihlédnutím k možné souvislosti s vyšetřovanou věcí.

3. Zadokumentovat komunikaci ze sociálních komunikátorů (Whatsapp. Signál, Threema, Mesenger, Wickerme a pod).

4. Další skutečnosti, které vyplynou v průběhu zkoumání.

Analogicky, jako u výstupů z odborných vyjádření, jsou i informace získané znaleckým zkoumáním, zejména bitové kopie a obnovená „smazaná“ data apod. podrobeny dalšímu vyhodnocení policejním orgánem k zjištění jejich důkazní relevance pro trestní řízení.

Analýzy specializovaných dat

Možnost analýzy zajištěného zařízení v rámci trestního řízení, které je policejním orgánem odesláno na pracoviště k vytvoření bitové kopie z paměťového uložiště, lze provést výhradně u takových zařízení, do jejichž systému je umožněn přístup – nejsou zaheslované anebo oprávněný uživatel dal policejnímu orgánu heslo/kód/gesto k přístupu. Typicky jsou takto zkoumány zejména mobilní telefony a tablety, případně pevné disky či flashdisky. Pokud by zařízení byla jakýmkoliv způsobem chráněna proti přístupu heslem či šifrováním, tak není možné takto zajistit data pro potřeby trestního řízení.

Provedení analýzy s vytvořením bitové kopie je podmíněno tím, že jej realizuje policista s platným certifikátem, a to na pracovišti, které disponuje forenzním softwarem jako je MobilEdit apod. Formální výstup do trestního řízení pak tvoří protokol o ohledání ve smyslu ust. § 113 trestního řádu.

6. Kazuistika

Pro dokreslení shora uvedených informací o digitálních stopách bude čtenáři předestřen trestní spis, který byl prověřován a následně realizován v rámci součinnostní operace protidrogového oddělení Služby kriminální policie a vyšetřování Obvodního ředitelství policie Praha I a oddělení pátrání 757.5 odboru pátrání Generálního ředitelství cel. Jména a jiné identifikační údaje byly změněny.

Operace „Racek“

Kvalifikace:

- nedovolená výroba a jiné nakládání s omamnými a psychotropními látkami a s jedy dle ustanovení § 283 odst. 1, odst. 2 písm. c) ve formě spolupachatelství dle ustanovení § 23 trestního zákoníku

Trestná činnost obviněných spočívala v tom, že ačkoli nedisponovali oprávněním jakkoliv nakládat s omamnými a psychotropními látkami, tj. že jednali v rozporu s ustanovením § 3 odst. 2 a § 4 zákona č. 167/1998 Sb., o návykových látkách, ve znění pozdějších předpisů, přesto však přinejmenším od roku 2018, kdy si vytvořili profily na virtuálních tržištích v latentní síti internet, nabízeli k prodeji a následně distribuovali do různých zemí omamné a psychotropní látky, zejména marihuanu, která osahuje psychoaktivní látku delta-9-tetrahydrocannabinol (THC), který je uveden v příloze č. 4 k nařízení vlády č. 463/2013 Sb., o seznamech návykových látek, ve znění pozdějších předpisů, jako látka psychotropní a rovněž pak kokain, který je uveden v příloze č. 1 k nařízení vlády č. 463/2013 Sb., o seznamech návykových látek, ve znění pozdějších předpisů, jako látka omamná.

Celá trestná činnost byla páchána ze zištných důvodů, a to maximalizovat finanční prospěch z prodeje drog, k čemuž využívali relativní anonymitu kyberprostoru v latentní síti darknet.

Kriminalisté policejního orgánu vlastním šetřením v latentních sítích identifikovali závadový moniker[54] **AAA**, který na různých tržištích nabízel vyšší množství omamných a psychotropních látek k prodeji. Zjištěná tržiště

[54] Moniker je uživatelské jméno, synonymem v kyberprostoru je též nickname čili přezdívka

CANNAZON, dark0de, WHITEHOUSE MARKET. Nabídka sortimentu prodejce AAA spočívala zejména v látkách kokain a marihuana, a to v různých množstvích v objednávce (1g, 5g, 10g apod.), přičemž ze strany prodejce bylo deklarováno zasílání pouze po zemích Evropské unie.

Šetřením kriminalistů byl zjištěn tzv. PGP key (jedná se o šifrovací program, který je založený na algoritmu RSA pro asymetrickou kryptografii, tzv. šifrovací klíč skládající se ze soukromého a veřejného klíče), který je užíván k šifrování komunikací a zpráv. Veřejný PGP klíč může být předán komukoliv, kdo s konkrétním „držitelem“ vzejde v kontakt, který je zcela individuální pro konkrétní subjekt (osobu či osoby, v daném kontextu tedy ty, kteří zajišťují aktivitu na daném profilu na tržištích v darknetu).

Informace o možné distribuci omamných a psychotropních látek, osobou vystupující jako AAA, se navazujícími úkony, i pomocí identifikace PGP klíče, podařilo spolehlivě ověřit. Došlo k provedení kontrolního nákupu, při kterém byla v zakoupené látce zjištěna pozitivní detekce na přítomnost kokainu, posléze byl proveden na platformě virtuálního tržiště VERSUS další kontrolní nákup, kde byla rovněž identifikována pozitivní detekce na kokain. Ve spojitosti s tímto kontrolním nákupem se podařilo zjistit podací poštu doručované zásilky, díky které se podařilo ustanovit prvního z pachatelů výše uvedené trestné činnosti. Posléze došlo k ustanovení i druhého z pachatelů, a vyšlo najevo, že se jedná o osoby, které společně figurují ve strukturách jedné obchodní společnosti.

Aktualizací šetření k uživatelskému účtu AAA bylo zjištěno, že pachatelé expandují na další virtuální tržiště v latentní síti internet, i v návaznosti na PGP klíče, vyšly najevo další nelegální aktivity na tržištích Bohemia, WallStreetMarket, DreamMarket, TorrezMarket, Dark0deReborn. Všechny profily prodejce AAA dostupné na virtuálních tržištích, které nebyly v dané době zrušeny, byly kriminalisty protidrogového oddělení dohledány. Ze strany kriminalistů došlo ke zpracování podrobné analýzy aktivit obviněných, které vyvíjeli na virtuálních tržištích a byl zjištěn a částečně zadokumentován rozsah trestné činnosti. Analýzy detailně popisovaly dobu, po níž byli obvinění na konkrétních tržištích aktivní, stejně tak počty uskutečněných prodejů omamných a psychotropních látek a množství tzv. feedbacků (jedná se o zpětnou vazbu nakupujícího k uskutečněné koupi drogy, k němuž policejní orgán konstatoval, že počet feedbaků udělených

prodejci – konkrétnímu monikeru je stěžejní ukazatel kvality prodávajícího, v zásadě se jedná o kladnou referenci. Každý dealer ve virtuálním tržišti se snaží mít co největší množství pozitivních feedbaků, což funguje de facto jako punc kvality pro dalšího potencionálního zájemce o koupi drogy).

Z analýz a zjištěných a zadokumentovaných informací vyplynulo, že obvinění skrze virtuální tržiště prodali omamné a psychotropní látky celkem v minimálně 486 individuálních případech, a to v množství minimálně 6.069 gramů marihuany a minimálně 383,6 gramů kokainu. Dlužno podotknout, že z virtuálních tržišť WallStreetMarket a DreamMarket již nebyly dostupné informace o konkrétních omamných a psychotropních látkách, které obvinění distribuovali, ale jednalo se celkem o 654 individuálních prodejů, tedy násobně víc, než jak tomu bylo u zbylých tržišť, kde se data podařilo získat a zadokumentovat.

Při realizaci protidrogové operace RACEK byly provedeny dvě domovní prohlídky a dvě prohlídky jiných prostor a pozemků. Podařilo se zajistit několik mobilních telefonů, notebook a stolní počítač. Zajištěná zařízení následně byla odeslána ke znaleckému zkoumání a z vytvořených bitových kopií byly zjištěny relevantní digitální stopy, které plně korespondovaly s informacemi získanými prováděnými úkony prověřování. Zejména se jednalo o zájmové komunikace mezi pachateli, kteří mezi sebou řešili objemy prodejů na jednotlivých tržištích, migraci na nová tržiště po ukončení činnosti WallStreetMarketu a DreamMarketu, v čemž viděli potenciál pro svůj další „ekonomický růst“, několik fotografií zasílaných zásilek a omamných a psychotropních látek. Dále byl v notebooku vyhledán konkrétní PGP klíč, šifrovací software Kleopatra a software k přístupu do darknetu - TOR broswer.

Bohužel se nepodařilo vyhledat a zajistit všechny informace k platbám za prodané omamné a psychotropní látky, které byly vždy provedeny v kryptoměně a rovněž se nepodařilo zajistit všechny identifikační údaje k peněženkám na kryptoměnu. Vyhodnocením bitových kopií všech zajištěných zařízení byly zjištěny zásadní skutečnosti, které v součtu a při porovnání s informacemi získanými procesními úkony v prověřování přinesly dostatečně odůvodněný závěr, že si pachatelé během několika let vydělali prodejem nelegálních omamných a psychotropních látek na virtuálních tržištích v latentní síti – darknetu minimálně uvedených 6.069 gramů marihuany za částku 41.021,89 € a 4.504 $, což je

v součtu (a dle nejnižšího kurzu za prověřované období) 1.092.086,- Kč a minimálně 383,6 gramů kokainu za částku 4.061,60 € a 34.237,75 $, což je v součtu (a dle nejnižšího kurzu za prověřované období) 812.011,30 Kč.

Policejní orgán si byl bez dalších pochyb zcela vědom, že pachatelé zjevně provedli násobně více prodejů omamných a psychotropních látek, než kolik bylo prověřováním a vyšetřováním důkazně spolehlivě zadokumentováno, absence digitálních stop z uzavřených virtuálních tržišť WallStreetMarket a DreamMarket jim zcela jistě pomohla. Nebylo je možné stíhat pro celý rozsah spáchané trestné činnosti.

Na druhou stranu relativně komplexní informace z prověřování, které významně korespondovaly s digitálními stopami v jejich zařízeních, pak vzaly pachatelům možnost jakkoli fabulovat. Zadokumentované komunikace mezi nimi o objemech prodeje omamných a psychotropních látek a jejich činnost na konkrétních virtuálních tržištích, fotografie drog a zásilek (které byly pořízené jejich vlastními zařízeními a některé obsahovaly i polohové údaje v metadatech) v důsledku zapříčinilo, že se oba pachatelé doznali v zadokumentovaném rozsahu.

Trestní spis byl ukončen návrhem na podání obžaloby na oba pachatele, kteří během necelých tří let vydělali distribucí marihuany a kokainu minimálně 1.904.097,30 Kč. Pod tíhou důkazních prostředků pak cestou svých obhájců navrhovali státnímu zástupci dohodu o vině a trestu, která byla později uzavřena a posléze byla i dohoda o vině a trestu schválena soudem.

Závěr

Smyslem této bakalářské práce bylo zpracování a předložení základních informací o digitálních stopách a způsobech jejich zajišťování, dokumentování, protokolace s akcentem na jejich zajišťování při domovních prohlídkách, a to celé zasazeno do právního rámce, jehož pramenem je trestní řád a v návaznosti na to pak interní akty řízení pro fyzickou činnost policejního orgánu, resp. specialistů provádějících zajišťování, což se neobešlo do zasazení pojmu digitální stopy do reálii kriminalistiky, zejména kriminalisticko-technické a kriminalisticko-taktické činnosti.

Výčet možností, jak zajišťovat informace v digitálním světě jistě není konečný a dalším vývojem virtuálního světa a informačních a komunikačních technologií se budou objevovat nové oblasti, kde bude možné získávat kriminalisticky relevantní informace. Kupříkladu jako tomu bylo v posledních cca deseti letech, kdy doznala dynamického rozvoje oblast kryptoměn, která poté přinesla možnosti jejich trasování a identifikace konkrétních plateb, peněženek a v návaznosti na to i jejich držitelů.

Závěrem bych konstatovala, že jsem při práci s odbornou kriminalistickou literaturou i právními předpisy zjistila, že není zcela jednoznačně definován pojem digitální stopa. Nedostatek obsahu v pojmu digitální stopa bude možná narovnáno budoucí změnou, novelizací trestního řádu či zcela novým trestně procením zákonem, který by mohl více reflektovat digitalizaci činností člověka. Ovšem nenaplněnost pojmu digitální stopa pak je výzvou i pro kriminalistiku, která se stále opírá zejména o materiální svět a vědomí člověka, nikoli však o virtuální prostředí, v němž se člověk pohybuje, zanechává stopy a v němž vlastní nehmotné majetkové hodnoty, které mohou být cílem pro pachatele trestné činnosti.

Seznam použité literatury

Monografie

BRATKOVÁ, Eva. *Metadata jako nový nástroj pro komunikaci webovských informačních zdrojů.* Národní knihovna, 1999, 10(4), s. 178-195. ISSN 0832-7487

BRATKOVÁ, Eva a Helena KUČEROVÁ. *K otázkám metadatového popisu systémů organizace znalostí.* Knihovna: knihovnická revue, 2015, 26(1), s. 5-36. ISSN 1801-3252.

BRADÁČ, Albert, KLEDUS, Miroslav a KREJČÍŘ, Pavel. *Soudní znalectví*. Brno: Akademické nakladatelství CERM, 2010. s. 95-126. ISBN 978-80-7204-704-8.

CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet.* 3rd ed. Waltham, MA: Academic Press, c2011. s. 38. ISBN 978-0-12-374268-1.

FENYK, Jaroslav, HÁJEK, Roman, STŘÍŽ, Igor, POLÁK, Přemysl. Trestní zákoník a trestní řád, průvodce trestněprávními předpisy a judikaturou, 1. díl – Trestní zákoník. 1. vydání. Praha: Linde Praha, a.s., 2010. Edice Komentované zákony. ISBN 978-80-7201-802-4.

KOLOUCH, Jan. *Cybercrime*. Praha: Edice CZ.NIC, 2016. s. 85-135. ISBN 978-80-88168-18-8.

KONDRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika, Teorie, metodologie a metody kriminalistické techniky.* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 54. ISBN 978-80-7380-535-7.

KOTHÁNEK, Jaroslav. *Zajišťování výpočetní techniky a dat pro potřeby důkazního řízení.* Policie ČR, Praha, 2008.

MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ NIC, 2013. s. 35. ISBN 978-80-904248-7-6.

MUSIL, J., KONRAD, Z., SUCHANEK, J. *Kriminalistika.* 1. vydání. Praha: C.H.Beck, 2001. s. 84. ISBN 80-7179-878-9.

MUSIL, KONRÁD, SUCHÁNEK. *Kriminalistika, 2. přepracované a doplněné vydání*, 2004, s. 3. ISBN 80-7179-878-9.

NĚMEC, Bohuslav a kol. *Učebnice kriminalistiky (Kriminalistická technika).* Praha. Vydal Kriminalistický ústav MV-hlavní správy VB, 1959. s. 3.

POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. s. 541. ISBN 978-80-7598-045-8.

PORADA, Viktor. *Kriminalistika: (Úvod, technika, taktika).* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2007. s. 56. ISBN 978-80-73-80-038-3.

PORADA, Viktor. *Kriminalistika: (Úvod, technika, taktika).* Plzeň. Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 114-145. ISBN 978-80-7380-490-9.

PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. s. 214. ISBN 978-80-7380-589-0.

WHITCOMB C.M.: An Historical Perspective of Digital Evidence: A Forensic Scientist´s View. In: *International Journal of Digital Evidence, Spring 2002 Volume 1, Issue 1.* s. 115.

Časopisecké články

RAK, R., PORADA, V. *Digitální stopy v kriminalistice a forenzních vědách.* Soudní inženýrství: časopis pro soudní znalectví v technických a ekonomických oborech. 2005. Online. Policejní akademie České republiky v Praze. http://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf. [citováno 2024-02-11].

Zákonná úprava a IAŘ (interní akty řízení)

zákon č. 141/1961 Sb., o trestním řízení soudním

zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

PPP č. 100/2021 o kriminalisticko-technické činnosti, ze dne 7. prosince 2001

Kvalifikační práce

VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů*. Zlín, 2013. Diplomová práce. Univerzita Tomáše Bati ve Zlíně

Internetové zdroje

BRECHLEROVÁ, Dagmar. *Digitální stopy a jejich odstraňování*. In: Computerworld. Online. 2016. Dostupné z: https://computerworld.cz/securityworld/digitalni-stopy-a-jejich-odstranovani-53197. [citováno 2024-02-10]

Mulvey, Bret. Pluto Scarab - Hash Functions. Hash Functions. Online. 2007. Dostupné z: http://home.comcast.net/~bretm/hash/. [Citováno 11.2.2024.]

Digital Evidence: Standards and Principles. *Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE).* http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

Blockchain. Online. Dostupné z: https://www.alza.cz/co-je-blockchain. [citováno 2024-02-19]

Desktop. Online. Dostupné z: https://it-slovnik.cz/pojem/desktop. [citováno 2024-02-25]

Kryptoměna. Online. Dostupné z: https://academy.binance.com/cs/articles/what-is-a-cryptocurrency. [citováno 2024-02-25]

Online. https://www.w3.org/Security/Faq/wwwsf6.html. [citováno 2024-02-11]

Online. Dostupné z: https://www.linnetdesign.cz/app4/743/co-je-bitova-kopie-disku. [citováno 2024-02-11]

Online. Dostupné z: https://www.totalservice.cz/novinky/digitalni-stopy-co-jsou-a-jak-se-jich-zbavit-2022-02-18. [citováno 2024-02-10]

https://it-slovik.cz/pojem/digitalni-stopa/?utm_source=cp&utm_medium=link&utm_campaign=cp