VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

DIGITÁLNÍ STOPA

Autor práce: Václav Poláček, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinované

Vedoucí práce: prof. JUDr. Jozef Meteňko, PhD

Katedra: Katedra právních oborů a bezpečnostních studií

2024

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Václav Poláček

Studijní program: Bezpečnostně právní činnost
Forma studia: ~~Prezenční~~ / Kombinovaná
Místo studia: ~~České Budějovice~~ / Příbram

Název bakalářské práce: Digitální stopa

Název bakalářské práce v anglickém jazyce: Digital trace

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): prof. JUDr. Jozef Meteňko, PhD

Datum zadání bakalářské práce (měsíc, rok): 10.2023

Cíl bakalářské práce: Prozkoumat a analyzovat druhy a vytváření digitální stopy v online prostředí. Zhodnotit dopady digitální stopy na soukromí a bezpečnost uživatelů. Navrhnout doporučení pro ochranu osobní digitální stopy a zlepšení povědomí o této problematice.

Student: Václav Poláček, DiS.	30.10.2023 *datum*	*podpis*
Vedoucí práce: prof. JUDr. Jozef Meteňko, PhD	*20231030* *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	9.11.23 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	13.11.2023 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	17.11.2023 *datum*	*podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Zde bych rád poděkoval vedoucímu mé bakalářské práce, panu prof. JUDr. Jozefu Meteňkovi, PhD, za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

POLÁČEK, V. Digitální stopa: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2024. Vedoucí bakalářské práce: prof. JUDr. Jozef Meteňko, PhD

Klíčová slova: Digitální stopa, soukromí, bezpečnost, internet

Tato bakalářská práce se zaměřuje na studium digitální stopy a její vliv na soukromí jednotlivců. Cílem této práce je analyzovat různé aspekty digitální stopy, včetně jejího vzniku, sběru a využití, a zkoumat, jaké důsledky má pro soukromí a bezpečnost uživatelů online prostředí. Dále i jak je digitální stopa chápána z kriminalistického hlediska. V práci bylo využito množství dostupné odborné literatury. Tato práce pomáhá k lepšímu porozumění, co je digitální stopa a zároveň poskytuje doporučení pro uživatele, jak chránit sebe a své soukromí v digitálním prostředí.

ABSTRACT

Poláček, V. Digital trace: Bachelor Thesis. České Budějovice: The College of European and Regional Studies, 2024. Supervisor: prof. JUDr. Jozef Meteňko, PhD

Key words: Digital trace, privacy, security, internet

This bachelor thesis focuses on studying digital trace and its influence on the privacy of individuals. The aim of this work is to analyze various aspects of digital trace, including its origin, collection and use, and examine the consequences for the privacy and safety of users on online environment. Furthermore, how the digital trace is understood from a criminalistic point of view. A lot of available literature was used in the work. This work helps to better understand what is a digital trace while providing recommendations for users how to protect themselves and theirs privacy in a digital environment.

Obsah

Úvod

Základním problémem, který bude řešen v bakalářské práci, je problematika digitální stopy. Digitální stopu zanechává každý, kdo alespoň okrajově využívá technologie v digitálním prostředí. Práce je zaměřena na to, jak jsou data o digitální stopě sbírána, uchovávána a využívána. Dále bude řešen i vliv digitální stopy na soukromí a bezpečí jednotlivců v digitálním prostředí. V práci bude řešena i problematika digitální stopy z kriminalistického hlediska. Této problematice se věnuje více pozornosti z důvodu aktuálnosti a vzrůstajícímu nebezpečí kyberkriminality.

1 Cíl a metodika bakalářské práce

Tato práce se bude zabývat digitální stopou, její komplexní analýzou a zhodnocení dopadů digitální stopy na soukromí a bezpečnost uživatelů. Cílem této práce je zlepšení povědomí uživatelů o digitální stopě a navrhnout doporučení pro ochranu osobní digitální stopy.

Práce bude zaměřena na obecnou rovinu ohledně digitální stopy, identifikaci různých forem a způsobu vytváření digitální stopy a pohled na digitální stopu z pohledu kriminalistického. V práci bude řešena i problematika právních aspektů ohledně ochrany osobní digitální stopy a jakým způsobem je digitální stopa uživatele zajišťována a dále využívána.

V praktické části se autor zaměří na vlastní digitální stopu, kdy v práci uvede jakým způsobem se pohybuje v digitálním prostředí, jak ho využívá a jak vlastní digitální stopu chrání. Dále se autor pokusí zjistit a zálohovat vlastní digitální stopu. V práci bude vyhodnocena osobní digitální stopa autora, jakož i rizika z toho vyplývající.

Metodika práce zahrnuje rešerši odborné literatury a online zdrojů k detailní analýze problematiky digitální stopy.

Výstup této práce má za cíl napomoci jednotlivcům k lepší ochraně své digitální stopy a minimalizaci rizik spojených s online aktivitami. Práce přispěje k pochopení významu digitální stopy v dnešní digitální společnosti a má sloužit jako podklad pro další studie a výzkum v oblasti bezpečnosti a soukromí v online prostředí.

2 Digitální stopa

2.1 Co je to digitální stopa? Obecná definice pojmu.

Digitálním stopy bývají nazývané také jako digitální stíny. Pomocí stop, které za sebou v digitálním prostředí zanecháváme, umožňujeme ostatním, aby nás v tomto prostředí sledovali. Ostatní lidé tak mohou vidět, jaká místa v digitálním světě navštěvujeme, jaké jsou naše cesty, odkud na které místo přicházíme, jaké jsou naše vzorce chování, jaké máme naše nejintimnější konverzace nebo jaké jsou hlavní změny v našich životech[1].V nejširším pojetí je digitální stopa čehokoliv, co je zaznamenáno senzorem. Shromáždění digitálních stop vytváří obrovský soubor dat. Aplikace pro „dolování dat“ vytvářejí slibný nástroj pro komerční sledování a využití k marketingovým účelům. Ze sledování však mohou plynout i četná rizika spojená s ochranou osobních dat a jejich možným zneužitím. Technologie dolování dat založená na digitálních stopách má různé účely. Patří mezi ně soukromé komerční účely, národní bezpečnost a veřejné zájmy[2].

Digitální stopu uživatelé zanechávají tehdy, pokud jsou online. Mezi úkony, které uživatelé během zanechávání pohybu v počítačovém a jiném online prostředí zanechávají patří např. historie při „brouzdání“ na internetu, různá kliknutí, prohlížení webových stránek, vytváření osobních profilů, „lajkování“ na sociálních sítích apod.[3] Mnoho prohlížečů (např. Google), sociálních sítí (např. Facebook, Instagram) či e-shopů (např. Amazon) používá systémy umělé inteligence (AI), mezi které patří algoritmy strojového učení, které slouží ke shromažďování dat a které dále postupují k rozpracování vzorců, které slouží analýze našich preferencí, zájmů a cíl. Cílem těchto algoritmů je realizovat

1 COCQOVÁ, C. Digital Footprints and Narrative Traceability/Narrative Footprints and Digital Traceability [online]. Helsinki: 2021 [cit. 2024-01-22]. eSSN 2659-6881. Dostupné z WWW: <https://dra.revistas.csic.es/index.php/dra/article/view/881/1022>

2 CHENG F. CH, WANG, Y.S. The Do Not Track Mechanism For Digital Footprint Privacy Protection In Marketing Applications. 2018. Journal of Business Economics and Management. Volume 19, Issue 2: 253-267. ISSN 1611-1699 / eISSN 2029-4433

3 LAMBIOTTE, R., KOSINSKI, M. Tracking the Digital Footprints of Personality [online]. 2014, Volume 102, Issue 12 [cit. 2024-01-22]. Dostupné z WWW: https://ieeexplore.ieee.org/document/6939627

takový proces, v kterém dochází k monitorování digitální stopy a kde jsou odvozovány osobní preference, zájmy, cíle aj. Tento proces se nazývá algoritmické sledování.

Podle výzkumníků Zankera et al.[4] a Youyou at al.,[5] během algoritmickém sledování provádějí počítačové systémy „úsudky“, „psychologické závěry“ a „předpoklady o zájmech, cílech a preferencích jednotlivce.“ Podle Burra a Cristianiniho (2019) je tedy možné tvrdit, že algoritmické sledování je založené na základě vzorku pozorovatelného chování subjektu. Podle Peterse[6] může mít algoritmické sledování dva druhy:

- algoritmické sledování,

- psychometrické sledování

Jedním z cílů zkoumání digitální stopy je zvýšení ochrany bezpečnosti uživatelů digitálního prostoru.

Podle Scientific Working Group on Digital Evidence[7] je možné definovat digitální stopu následujícím způsobem: „*Digitální stopa je jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená přenášená v digitální podobě.*

Rak a Porada[8] definují digitální stopu takto: *„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.“*

---

4 ZANKER, M., L. ROOK, a D. JANNACH. 2019. “Measuring the Impact of Online Personalisation: Past, Present and Future.” International Journal of Human-Computer Studies 131: 160–168.

5 YOUYOU, W., M. KOSINSKI, and D. STILLWELL 2015. “Computer-based Personality Judgments are More Accurate than Those Made by Humans.” Proceedings of the National Academy of Sciences of the United States of America, 112(4): 1036–1040.

6 PETERS, U. *Reclaiming Control: Extended Mindreading and the Tracking of Digital Footprint*s. 2022. DOI: 0.1080/02691728.2021.2020366

7 RAK, R., PORADA, V.. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, ročník 16. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf

8 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

Podle pokynů policejního prezidenta se digitální stopou rozumí „*digitální informace nebo jakákoli data přenesená nebo uložená za použití*“.[9]

2.2 Vysvětlení různých forem digitálních stop

Digitální stopy mohou mít různé formy a existují různé způsoby dělení. První představený způsob dělení forem digitální stop bude podle Bemmamiho[10] některou z následujících tří forem:

- záznamy (protokoly): odpovídají dokumentaci události a týkají se konkrétního systému, který je automaticky generovaný v určitém čase. Záznamy generují prakticky všechny softwary. Využití protokolu vyžaduje plný přístup k jádru digitálního nástroje a to za účelem extrahování protokolů.
- tagy: jedná se o prvky informací (jakými jsou záložky webových stránek, počítačové soubory nebo databáze).
- textové prvky. Jedná se o jakékoliv písemné prvky, které se generují prostřednictvím digitálního řešení (např. e-maily, PDF, elektronické knihy apod.)[11]

Další dělení digitální stopy je na aktivní a pasivní. Aktivní digitální stopa je taková, na jejímž zanechání se uživatel aktivně podílí a to tak, že například vytváří profily na sociálních sítích, sdílí fotografie, píšou emaily, vyplňují registrační formuláře apod. Pasivní digitální stopy jsou pak takové, které necíleně vytváříme pouze tím, že používáme internet. Tyto stopy bývají nazývané také jako digitální otisk. Patří sem např. soubory cookies, aktivity na webových stránkách, záznamy IP adres či záznamy používaného

9 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022.

10 BEMMAMI, K-E, GRAZA, L.a COURTIN C.. From digital traces to competences. 2022. IFAC PapersOnLine 55-10 (2022) 1944–1949

11 BEMMAMI, K-E, GRAZA, L.a COURTIN C.. From digital traces to competences. 2022. IFAC PapersOnLine 55-10 (2022) 1944–1949

zařízení apod.[12] Dalším příkladem pasivní digitální stopy jsou různé veřejné seznamy, kde může být každý poměrně lehce dohledatelný.

Peters[13] jmenuje dva druhy algoritmického sledování a těmi jsou jednoduché algoritmické sledování a psychometrické sledování:

Jednoduché algoritmické sledování. Tento způsob používá například Amazon nebo Netflix a slouží k tomu, aby bylo možné sledovat, jaké v minulosti daný uživatel provedl nákupy, hodnocení, jaké si prohlíží položky nebo jak se chová jako uživatel webu. Na základě těchto informací je pak možné vytvořit profil uživatele a najít další podobné uživatele, jejichž hodnocení, nákupy a prohlížené položky jsou podobné. Algoritmy pak fungují tak, že agregují podobné položky od těchto velmi podobných uživatelů a druhému uživateli nabízejí algoritmy takové nákupní položky, jaké již nakoupil první uživatel.[14] Během tohoto jednoduchého sledování algoritmy nepracují s psychologií, pouze sledují podobné chování uživatelů. Cílem práce těchto algoritmů je, aby se maximalizoval počet akcí, které uživatel učiní (lajky, nákupy, apod.). I když jednoduché algoritmy nepracují s psychologií, tak fungují, protože vycházejí z faktů, jak se chovali typologicky podobní uživatelé.[15]

Psychometrické sledování. Jedná se o zpracování, při kterém systémy umělé inteligence měří a explicitně připisují uživatelům webových stránek psychologické rysy včetně osobnostních rysů. Činí tak na základě jejich online chování nebo jiných uživatelských dat.[16]

---

12 TOTALSERVICE. Digitální stopy: co jsou a jak se jich zbavit? Totalservice.cz [online]. 18.2.2022 [cit. 2024-01-23]. Dostupné z WWW: https://www.totalservice.cz/novinky/digitalni-stopy-co-jsou-a-jak-se-jich-zbavit-2022-02-18

13 PETERS, U. *Reclaiming Control: Extended Mindreading and the Tracking of Digital Footprint*s. 2022. DOI: 0.1080/02691728.2021.2020366

14 RICCI, F., ROKACH, L., SHAPIRA, B., a KANTOR, P. B. *Recommender Systems Handbook.* Berlin: Springer, 2011.

15 PETERS, U. *Reclaiming Control: Extended Mindreading and the Tracking of Digital Footprint*s. 2022. DOI: 0.1080/02691728.2021.2020366

16 RUST, J., KOSINSKI, M., STILLWELL, D. *Moderní psychometrie. Věda o psychologickém hodnocení.* Londýn: Routledge, 2021

Metadata. V souvislosti s digitální stopou je třeba neopomenout zmínit ani metadata. Například v případě fotografie to může být metadatem místo, kde byla fotografie pořízena nebo informace o lokalizaci počítače podle IP adresy. Metadata vznikají tedy vedle digitální stopy a „žijí si svým nezávislým životem“.[17]

Vzhledem k běžnému uživateli je možné rozlišit digitální stopy na dobré a špatné. Některé digitální stopy mohou mít pro uživatele přínos a mohou zlepšit jeho čas, který tráví online, protože vyhledávač díky digitální stopě nabízí uživateli pohodlnější a přizpůsobivější fungování. V praxi to vypadá tak, že pokud si uživatel chce například objednat stejné jídlo jako minule, prohlížeč si ho zkrátka zapamatuje. Dalším pozitivním přínosem digitální stopy v osobním životě může být to, že uživatel může vytvářet působivou sebeprezentaci, která bude stavět daného uživatele „do dobrého světla.“ Oproti tomu „špatná“ digitální stopa může přinášet celou řadu negativ a může vést např. spamování nevyžádanými nabídkami, snížením soukromí či krádeží identity.[18]

Digitální stopy se mohou také dělit na:

- veřejnou: informace veřejně dohledatelné na internetu,
- neveřejnou: informace, které mohou dohledat pouze někteří oprávnění uživatelé (např. přátelé na sociálních sítích).
- skryté: technické záznamy o připojení a zařízení nebo cookies [19] (Co jsou to cookies? Jejich úkol je jasný – přiřadit aktivitu na webových stránkách ke konkrétnímu uživateli. Můžete si je představit jako jedinečný řetězec písmen a čísel, který páruje relaci uživatele k příslušným datům a obsahu a zná pohyb uživatele napříč weby. Identifikace uživatele je pak zásadní pro personalizovanou reklamu nebo sledování výkonu inzercí)[20].

---

17 BEČVÁŘ, O. Digitální stopa a její rizika [online]. 2022 [cit. 2024-01-23]. Dostupné z WWW: <https://www.ak-becvar.cz/digitalni-stopa-a-jeji-rizika/>

18 MORGAN STANLEY. Strategies to Help Protect Your Digital Footprint [online]. 9.10.2023. [cit. 2024-01-23]. Dostupné z WWW: https://www.morganstanley.com/articles/digital-footprint-protection-strategies

19 INTERNETEM BEZPEČNĚ. Digitální stopa. Internetem bezpecne.cz [online]. 2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

20 Cookies třetích stran končí: Proč je váš e-shop potřebuje? cz [online]. 2024 [cit. 2024-04-05]. Dostupné z https://www.advisio.cz/blog/co-jsou-cookies-tretich-stran-a-jak-jejich-konec-ovlivni-e-shopy/

Nejedná se o dělení stop z kriminalistického hlediska. Dělením stop podle kriminalistického hlediska se autor bude věnovat v dalších částech této práce.

2.3 Identifikace způsobů vytváření digitální stopy

Existuje velké množství zdrojů, které pomáhají digitální stopu utvářet. Podle Chenga a Wanga[21] jsou to veškeré činnosti na internetu, které pomáhají sledovat a zaznamenávat.

Nástroje, kterými je utvářena digitální stopa je možné rozdělit na funkční prvky v online prostoru a na hardwarové vybavení. Nejprve budou představeny funkční prvky v online prostoru.

Cookies. Cookies jsou soubory dat, jenž se ukládají při návštěvě webové stránky. Provozovatelé webů cookies používají z toho důvodu, že jim napomáhají např. v analyzováním toho, jak se chovají uživatelé webu. Sběr dat z cookies je využitelný zejména pro SEO, nastavení správného UX nebo pro online marketing. Díky cookies mohou mít totiž provozovatelé webu získat informace např. o počtu návštěv na webu, jaké URL jsou na webu nejnavštěvovanější a které naopak ne. Pro uživatele mají cookies zase ten přínos, že se jim personalizuje obsah na webu (např. nastavují se jazykové preference nebo způsobí, že se obsah košíku nevymaže, když e-shop opustíme)[22]. Celkově tedy cookies pomáhají k získání přehledu o dění na webu. Ve vztahu k vytváření digitální stopy je výhodou cookies, že je možné se jich poměrně snadno zbavit. Pokud webová stránka cookies používá, musí požádat k svolení k jejich užívání[23].

---

21 CHENG F. CH, WANG, Y.S. The Do Not Track Mechanism For Digital Footprint Privacy Protection In Marketing Applications. 2018. Journal of Business Economics and Management. Volume 19, Issue 2: 253-267. ISSN 1611-1699 / eISSN 2029-4433

22 MARČÍKOVÁ, V. Cookies lišta v roce 2022: Jak si s novelou zákona o elektronické komunikaci poradily velké české weby. In *Aira* [online]. © 2022 [cit. 2024-01-24]. Dostupné z WWW: https://blog.aira.cz/cookies-lista-v-roce-2022-jak-si-s-novelou-zakona-o-elektronicke-komunikaci-poradily-velke-ceske

23 GIVENS, CH. Digitální stopa zařízení a sledování na internetu. In *Avast* [online]. 2.10.2019 [cit. 2024-01-24]. Dostupné z WWW: https://blog.avast.com/cs/fingerprinting-and-the-surveillance-economy

Pro sledování pohybu osob **ve fyzickém prostoru** pak slouží následující prvky:[24]

Bluetooth. Jedná se o protokol pro bezdrátové připojení na krátkou vzdálenost komunikace až 100 metrů pomocí radiových vln. Díky tomu, že jsou chytré telefony všudypřítomné a obvykle mají zapnuté bluetooth, stávají se velmi slibným kandidátem na digitální sledování.

GPS (Global Positioning System). Poskytuje geografické informace o poloze a čase, jak se pohybují zařízení vybavení GPS prostřednictvím sady radioaktivních satelitů GPS. GPS poskytuje prostředky ke sledování každého chytrého telefonu. Pro sledování digitální stopy je to velmi dobrým předpokladem, protože většina smartphonů po celém světě GPS podporuje. Sledování prostřednictvím GPS selhává ve dvou ohledech. Prvním z nich je otázka ochrany soukromí („Jsem sledován?“). Dále je nevýhoda GPS, že selhává v tunelech a ve vnitřních prostorech, kde chybovost určení polohy dosahuje rozmezí až 10 metrů.

WiFi. Jak již bylo řečeno, GPS sledování je možné využít zejména ve venkovních prostorech. Vzhledem k tomu, že lidé tráví přibližně 80 % svého času v interiéru, tak je potřeba najít řešení pro sledování kontaktů v době, kdy se nacházejí uvnitř. Ve většině vnitřních prostor jsou dostupné WiFi sítě. U podnikových WiFi dochází k několika způsobům připojení (Access Points = AP) a uživatelská zařízení se neustále připojují a odpojují a pohybují se mezi jednotlivými AP. Uvnitř podniků většina osob nosí svůj mobilní telefon s sebou. Díky tomu je možné odvodit trajektorii, jakou pracovníci vykonávají. Zároveň je možné pozorovat, jaký čas strávili pracovníci odpojeni od jednotlivých AP.

Akustický rozsah. Zvuk je přítomný stejně jako Bluetooth. Pro sledování digitální stopy je výhodou, že primárním účelem telefonů je vysílat, nahrávat a přenášet zvuk. Základem akustického rozsahu se zakládá na myšlence, že každé zařízení vydává sice náhodný, ale zároveň i jedinečný zvuk. Ten je možné využívat k odvození

---

24 TRIVEDI, A., VASISHT, D. Digital Contact Tracing: Technologies, Shortcomings, and the Path Forward. 2020. DOI: 10.1145/3431832.3431841

vzdálenosti. Na rozdíl od Bluetooth, GPS a WiFi je zvuk mechanickou vlnou, která se pohybuje mnohem pomaleji než radiové vlny. Díky tomu je možné poměrně přesně měřit, jak dlouho potrvá, než dojde zvuk od jednoho zařízení do druhého. Například pokud by zařízení vydalo signál z Telefonu 1 a k Telefonu 2 se dostalo za 4,5 milisekund, lze vypočítat, jaká je jejich vzájemná vzdálenost. I toto zanechávání stopy má své limity. Jedním z limitů je počet zařízení, které mohou ve stejnou chvíli vydávat zvuk. Pokud zvuky zanechávají dva telefony, je sledování ještě poměrně čitelné, při větším počtu telefonů je to však již problém. Druhým limitem je ochrana soukromí. To, aby bylo možné sledovat polohu podle akustického systému, je třeba, aby měly všechny telefony v okolí na nějaký čas „zapnutý“ mikrofon. Dále jde i o aktuální umístění mobilního telefonu, různé překážky v interiéru apod.

Netradiční metody. Mezi relativně tradiční metody vytváření digitální stopy patří již zmíněné GPS, Bluetooth, WiFi. Existuje však i celá další řada dalších kreativních nápadů, jak sledovat digitální stopu. Řadí se sem třeba hybridní multimodální přístup, s kterým pracují nejrůznější aplikace. U tohoto přístupu se využívá různých modalit, jako zvuk a Bluetooth a jejich vzájemné propojení, či naopak zjištění toho, jak to udělat, aby se zvuk a bluetooth nerušili.

Mezi **příklady**, jakým konkrétním způsobem lidé vytvářejí své digitální stopy patří v praxi:

- Online nakupování (Registrace k odběru newsletterů značky, stahování a používání nákupních aplikací, nákup na e-shopech, stahování a používání nákupních aplikací)
- Internetové bankovnictví (Účet kreditní karty, pravidelné platby (Netflix, posilovna), prodej a nákup akcií, používání aplikace mobilního bankovnictví).
- Sociální média (připojení k aplikaci či seznamce, navázání spojení s přáteli a kontakty, přihlášení k jiné webové stránce pomocí údajů na sociální síti).
- Čtení zpráv (Přihlášení k odběru newsletterů, prohlížení článků v zpravodajské aplikaci apod.).

- Sport a zdraví (používání fitness trackerů, registrace pomocí emailu v posilovně, používání aplikací k poskytování zdravotní péče).[25]

Dalším dělením zdrojů pro vytváření digitální stopy jsou hardwarové nástroje, kam patří:

- mobilní telefony,
- elektronické diáře,
- handheldery (osobní počítače do dlaně velikosti krabičky cigaret),
- audio digitální záznamníkové přístroje,
- digitální videokamery a fotoaparáty,
- video a DVD přehrávače nebo rekordéry,
- platební a identifikační karty,
- nejrůznější záznamníková videa (CD, DVD, USB paměti, digitální paměti videokamer, fotoaparátů apod.),
- palubní počítače automobilů, lodí a letadel,
- různá bezpečnostní monitorovací zařízení,
- elektronická identifikace zboží a objektů apod.
- bohaté příslušenství rozmanitých druhů periférií ke všem uvedeným zařízením[26]

Dalším velmi důležitým zdrojem jsou webkamery, které monitorují určitou oblast v reálném čase. Živé záběry si tak může prohlížet kdokoliv s přístupem, a to po celé planetě. Všechna tato uvedená zařízení zaznamenávají z forenzního a kriminalistického pohledu prokazatelné stopy činnosti.[27]

---

25 KASPERSKI. *What is a digital footprint? And how to protect it from hackers* [online]. © 2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

26 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

27 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

2.4 Vliv našich online aktivit na digitální stopu

Uživatel vytváří digitální stopu veškerou činností realizovanou ve virtuálním prostředí. Uživatelská data jsou vysoce ceněným artiklem. Většina uživatelů technologií a internetu si to neuvědomuje, ale je potřeba se zajímat i o to, jakou digitální stopu po sobě zanecháváme, neboť vypovídá o našem digitálním JÁ. Tato data jsou velmi snadno zneužitelná a na jejich základě může zkušený uživatel sestavit podrobnou digitální identitu každého uživatele moderních technologií. V podstatě se jedná o takový digitální otisk prstu.

Digitální stopa zařízení je vytvořena nástroji pro sledování uživatelů na webových stránkách. Obsahuje informace o zařízení, které daný uživatel využívá (značka, model, OS, prohlížeč, nainstalovaný software). Všechny tyto údaje tvoří jedinečnou stopu, podle níž lze uživatele (zařízení) identifikovat na internetu. Jedinečnost hardwarové a softwarové konfigurace přispívá k faktu, že lze dle digitální stopy velmi přesně identifikovat konkrétního uživatele. Pokud se digitální stopa zařízení zkombinuje se záznamy chování a pohybu na webu daného uživatele, dostaneme podrobné informace o celé jeho online historii, preferencích, jeho aktivitách, ale dokonce i o některých důležitých událostech v jeho životě. Běžný uživatel internetu nemá šanci zjistit, které webové stránky sestavují digitální stopu jeho zařízení, kterou poté využívají ke sbírání údajů o uživateli, přičemž s vysokou pravděpodobností tyto data také přeprodávají za vysoké částky třetím stranám. V nejlepším případě tyto třetí strany použijí nasbírané informace k inzertním účelům a přizpůsobení webových stránek dle preferencí uživatele. Mohou se však naskytnout případy vážnějšího zneužití dat. Z mnoha vyberme například situaci, kdy si uživatel vyhledává informace o bolesti na hrudi. Daný vyhledávač prodá historii jeho hledání zdravotní pojišťovně a ta se může domnívat, že uživateli hrozí srdeční choroba a na základě poskytnutých informací uživateli zvýší pojistné sazby. Dalším příkladem může být manipulace s cenami výrobků. Na základě sdílení polohy

uživatele mu firma začne účtovat za zboží více (uživatel bydlí v drahé čtvrti), protože si myslí, že si to uživatel může finančně dovolit.[28]

Aktivní digitální stopu vytváříme sami tím, že o sobě sdělujeme informace sami, viz. profil na sociálních sítích, vyplňování registračních formulářů, e-mailová komunikace, nakupování v e-shopech, interakce na diskusních fórech, fotografie apod. Pasivní stopu naopak vytváříme zcela nezáměrně jen pouhým použitím internetu (cookies, záznamy IP adres, GPS souřadnice apod.)

Digitální stopa je více a více využívána i personalisty. Žadatel o zaměstnání může v dnešní době téměř určitě počítat s tím, že personalista si před samotným pohovorem zjistí k žadateli všechny možné dostupné informace z internetu. Pracovník HR oddělení si takto vypracuje podrobný profil uchazeče za užití digitální stopy žadatele. I to může rozhodnout, zda bude uchazeč úspěšný či nikoliv.

2.5 Využití digitální stopy v oblasti marketingu a reklamy

Digitální stopa uživatele je pro online marketingové účely alfou a omegou. Data o uživatelích sbírají weby či aplikace, které mohou (ale nemusí) nasbírané informace předávat dál (třetím stranám). Třetí strany neboli externí marketingové společnosti, mohou data sbírat buď samy nebo je právě odkoupit od strany první (weby a aplikace). Třetí strany mohou data dál prodávat.

Reklama tvoří většinový příjem poskytovatelů webových služeb. 90 % příjmů Googlu přichází z webového marketingu, Facebook je na tom ještě lépe – u něj je to 95 %.[29]

Marketing využívá digitální stopu pro ovlivnění zákazníka / uživatele. Na základě sesbíraných dat lze vytvořit poměrně přesnou digitální identitu uživatele a dle jeho preferencí upravit zobrazovanou reklamu tak, aby cílila co nejvíc do jeho preferencí.

---

28 GIVENS, CH. Digitální stopa zařízení a sledování na internetu. In *Avast* [online]. 2.10.2019 [cit. 2024-01-24]. Dostupné z WWW: https://blog.avast.com/cs/fingerprinting-and-the-surveillance-economy

29 LIEM, C., PETROPOULOS, G. The economic value of personal data for online platforms, firms and consumers . In *Bruegel* [online]. 14.1. 2016 [cit. 2024-03-12]. Dostupné z WWW: https://www.bruegel.org/blog-post/economic-value-personal-data-online-platforms-firms-and-consumers#:~:text=The%20generated%20value%20from%20personal,they%20use%20for%20attracting%20advertisers.

V rámci marketingu a cílené reklamy můžeme mluvit o *retargetingu* a *behaviorálním targetingu.* V retargetingu se jedná o to, že uživatel hledá určitý artikl v jednom či dvou e-shopech a od té doby se mu neustále zobrazuje reklama na daný artikl i na externích stránkách. V rámci behaviorálního targetingu, tak, aby bylo marketingové míření přesné, se sleduje veškerý pohyb uživatele ve virtuálním prostředí; analyzuje se jeho chování na internetu; jaké navštívil webové stránky, jak dlouho na nich strávil, na jaké odkazy klikl, co okomentoval, „olajkoval", o co projevil zájem. Z takto nasbíraných dat se poté vytvoří uživatelský profil, který umožňuje zacílit reklamu na uživatele co nejefektivněji. Tyto údaje jsou vysoce ceněné a obvykle se s nimi na internetu bohatě obchoduje.[30]

Ale pozor, spousta z nás nemá tušení, že kromě sběru běžných digitálních dat o uživatelích prohlížeče sbírají i tzv. behaviorální biometrická data. Google nás dokáže identifikovat tak dokonale, že když zasedneme k počítači a něco hledáme, zhruba po 20 zadaných znacích Google pozná, že jsme to my. Pokud k našemu počítači usedne úplně jiná osoba, která ovšem využívá náš účet, Google dokáže poznat, že to nejsme my a že jde o jiného uživatele. Jak je to možné? Google totiž zaznamenává kromě jiného i způsob práce s klávesnicí (dynamiku úhozu, styl psaní, skladbu slov aj.) Všechny tyto informace jsou zpracovány, propojeny s naší digitální stopou a přiřazeny k nám (jinak řečeno, takto se vytváří celý komplexní profil daného člověka).[31]

V rámci reklamy nelze nezmínit internetového giganta Google, který se svou službou Google Ads vládne online reklamnímu světu. Tady je pár statistických dat z poslední doby podle R. Shewale:[32]

- 80 % všech firem na světě využívá Google Ads
- Google Ads vygeneroval v roce 2023 celkové tržby ve výši 237,855 miliard USD.
- Více než 1,2 milionu firem používá Google Ads k propagaci svých produktů a služeb

---

30 INTERNETEM BEZPEČNĚ. Digitální stopa. Internetem bezpecne.cz [online]. 2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

31 REPKOVÁ, I. M. Nesmazatelná digitální stopa anebo Google nezapomíná. In Stisk online [online]. 17.10.2021 [cit. 2024-03-12]. Dostupné z WWW: https://stisk.online/a/SSxhd/nesmazatelna-digitalni-stopa-aneb-google-nezapomina

32 SHEWALE, R. Google Ads & PPC Statistics 2024 (Revenue & ROI). In Demandsage [online]. 18.2.2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.demandsage.com/google-ads-statistics

- 96 % značek utrácí peníze za Google Ads
- Příjmy z reklamy společnosti Google se za poslední desetiletí zvýšily o téměř 400%

Téměř každý z nás využívá Google search, má nainstalované různé aplikace apod. Digitální stopy, které Google může posbírat o každém uživateli, jsou enormní. Počet uživatelů Googlu potažmo uživatelů, kteří kdy někdy kliknou na reklamu z Google Ads, je enormní také. Bavíme se tu o monopolu na reklamní byznys, který jen tak někdo pravděpodobně v budoucnu nepřekoná. Sumy, které se v tomto byznysu otáčí, jsou gigantické. Tak jen pro představu, kolik dokáže vydělat obchodování s našimi digitálními identitami.[33]

2.6 Bezpečnostní rizika spojená s digitální stopou

Podle M. Černého[34] je potenciálních rizik brouzdání internetem jistě existuje poměrně velké množství. Kybernetická kriminalita. Digitální stopa uživatele se dá zneužít mnoha způsoby. Může se jednat o krádež osobních údajů (informace z kreditních karet, rodné číslo apod.), krádež hesel, e-mailových účtů, profilů na sociálních médiích. Ukradená digitální identita bývá dále využita ke spáchání dalšího protiprávního jednání. Samostatnou kapitolou je pak situace, kdy dochází ke kyberšikaně, zejména u náctiletých, kteří si plně neuvědomují dopad svých činů a aktivit ve virtuálním prostředí.

Černý také potvrzuje, že jedním z nejzásadnějších rizik je zneužití digitální stopy a následná krádež digitální identity. Někdo o nás nasbírá dostatečné množství dat a může si založit falešný profil či blog a jeho prostřednictvím šířit spam či extremistické názory. Zloděj identity se za uživatele také může jednoduše vydávat, aniž by druhá strana, se kterou komunikuje, o tom měla tušení. Toto pachatel může využít ke svému prospěchu – různá podvodná jednání, kdy se vydává za přítele oběti a uvádí, že v nouzi potřebuje peníze.

---

33 SHEWALE, R. Google Ads & PPC Statistics 2024 (Revenue & ROI). In Demandsage [online]. 18.2.2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.demandsage.com/google-ads-statistics

34 ČERNÝ, M. Digitální stopa a digitální identita. In *Metodický portál RVP.CZ [*online]. 26.8.2011 [cit. 2024-03-11]. Dostupné z WWW: https://clanky.rvp.cz/clanek/c/o/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html

Dalším zásadním rizikem je pro Černého absolutní ztráta soukromí. Digitální stopa o nás dokáže prozradit víc, než si dokážeme představit. Druhá strana si o nás může zjistit sebemenší detaily z našeho života – s kým se přátelíme, co děláme, kde pracujeme, kolik a za co utrácíme, co máme rádi, kde jsme všude byli apod.

Mezi další rizika můžeme zařadit situace, kdy jsou naše osobní údaje, které tvoří naši digitální stopu, využity pro manipulaci ve významných celospolečenských událostech. Web Totalservice[35] zmiňuje datový skandál společnosti Facebook a Cambridge Analytica, kdy tato společnost využila data uživatelů Facebooku a prostřednictvím analýzy sociálních médií a digitálních stop milionů a milionů uživatelů sociální sítě ovlivnila volby v USA v roce 2014, volbu amerického prezidenta v roce 2016 a referendum o Brexitu.

35 TOTALSERVICE. Digitální stopy: co jsou a jak se jich zbavit? Totalservice.cz [online]. 18.2.2022 [cit. 2024-01-23]. Dostupné z WWW: https://www.totalservice.cz/novinky/digitalni-stopy-co-jsou-a-jak-se-jich-zbavit-2022-02-18

3 Digitální stopa z pohledu kriminalistického

3.1 Kriminalistická stopa

Vymezení kriminalistiky jakožto samostatného vědního oboru se odvíjí od základního kriminalistického pojmu, jakým je právě kriminalistická stopa. V kriminalistice zkoumáme zákonitosti vzniku, trvání a zániku stop, jejich vyhledávání, zajišťování, zkoumání. Následně jsou tyto poznatky využívány k vypracování kriminalistických metod a postupů. Díky nim se poté stopy snadněji zajišťují a zkoumají a celý vyšetřovací proces tím může být značně efektivnější. Kriminalistické stopy umožňují vyšetřovatelům sestavit komplexní informace o trestném činu (průběh, provedení, pachatel, použité nástroje apod.)[36]

3.2 Klasická teorie kriminalistické stopy

Podstatou kriminalistických stop je exaktně zjištěná skutečnost formulovaná v *obecné teorii odrazu*: [37]

„Působí-li na sebe současně dva nebo více objektů, dochází ke vzájemnému předávání informací o jednotlivých objektech navzájem.“ Přitom je v podstatě lhostejné, jaký je charakter jednotlivých navzájem na sebe působících objektů. Výsledkem vzájemného působení objektů a předávání informací je tzv. odraz, který můžeme považovat za stopu, pokud splňuje následující tři podmínky:

1) *Odraz musí být v souvislosti s kriminalisticky relevantní událostí.* Jakákoliv digitální zařízení shromažďují ohromná množství digitálních záznamů (informací), dokumentující všechno, co se děje se zařízením nebo jakou aktivitu uživatel vykonává. Jedná se o digitální stopy obecně. Abychom nějakou digitální stopu považovali za kriminalistickou, musí být dána do souvislosti s počítačovou nebo kybernetickou kriminalitou.

---

36 KONRÁD, Zdeněk et al. Kriminalistika: teorie, metodologie a metody kriminalistické techniky. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. 318 s. ISBN 978-80-7380-535-7, str. 53

37 RAK, R., PORADA, V. Digital trace, *Booklet from scientific conference "Advances in criminalistics",* Police Academy, Prague, 2004

2) Odraz musí existovat alespoň od svého vzniku do zjištění. Neboli – neexistující odraz nelze využít.

3) *Odraz musí být vyhodnotitelný současnými metodami a prostředky.* Pokud nedokážeme získat z odrazů kriminalisticky relevantní informace, nemají pro nás prakticky význam.

Obecná teorie stop tedy pojednává o stopě jako o výsledku odrazu a v souvislosti s touto teorií také mluvíme o odrážených objektech, prostředcích odrazu a odrážejících objektech a subjektech.

Odráženým objektem chápeme osoby a prostředky, které vyvolávají aktivity. V souvislosti s digitální stopou jsou to tedy uživatelé výpočetní a digitální techniky a samotná digitální technika.

Prostředkem odrazu rozumíme vlastnosti odrážených objektů a objektivní okolnosti. Pokud mluvíme o osobách, pak tyto prostředky odrazu znamenají jejich psychologické vlastnosti, znalosti a dovednosti, které použijí pro výběr softwaru / zařízení a které ukazují úroveň jeho ovládání a využití.

Odrážející objekty a subjekty – vnější materiální prostředí, na které odrážené objekty za pomoci prostředků působí. Kromě toho se stopy o aktivitách odráží i ve vědomí uživatelů – tyto stopy nejsou materiální – nazýváme je paměťovými stopami (v teorii kriminalistických stop, ne digitálních).[38]

Jakékoliv technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechá záznam – a ten je z pohledu kriminalistické teorie stop ODRAZEM jeho činnosti, jak zmiňuje právě Rak a Porada. Tyto záznamy jsou z pohledu kriminalistiky stopami. Dle klasické teorie odrazu člověk / předmět / subjekt spojený s jeho činností aktivuje či upravuje softwarové vybavení či nějak reguluje elektronické

---

38 RAK, R., PORADA, V. Digital trace, *Booklet from scientific conference "Advances in criminalistics",* Police Academy, Prague, 2004

technologie. Tyto činnosti a změny způsobené těmito činnostmi se odráží do materiálního prostředí.

Je také nutné zmínit, že v cizojazyčné literatuře můžeme chápat význam slov stopa a důkaz jinak. Anglické literatura (potažmo angličtina jako jazyk) zmiňuje spojení slov *digitální evidence* (důkaz) ve smyslu *digitální stopy*. Pokud je k práci (neboli ke spáchání trestného činu) použit počítač, získává slovo evidence (důkaz) specifický význam. Jako příklad můžeme uvést situaci, kdy je oficiální dokument zfalšován legálně zakoupeným softwarem (např. Adobe Photoshop). Aplikace, počítač i původní dokument jsou naprosto legální, jediným důkazem o spáchání trestného činu je datový soubor se zfalšovaným dokumentem, uloženým v počítači společně se záznamy, které dokazují, že čin byl proveden určitým programem, v určitý čas, určitou osobou. Žádná jiná škoda nebyla způsobena.

V anglickém jazyce má využití slova *evidence (důkaz)* přednost před *stopou* (ve spojení s forenzní praxí). Slovo stopa, které by bylo vztažené k moderním technologiím, se prostě v cizojazyčné literatuře nepoužívá. Důvodem je, že teorie a praxe cizích zemí se výrazně orientuje na výsledek trestního řízení, tzn., že *stopa* musí být akceptována soudem. Proto je význam těchto dvou pojmů (důkaz a stopa) identický.[39]

Je tomu už docela dávno (v roce 1999), kdy byla vytvořena přijatelná definice pojmu digitální stopa. Definice byla vydána skupinou SWGDE (Scientific Working Group on Digital Evidence). [40]

Koncept digitální stopy chápe jako:

„Jakákoliv změna v hmotném prostředí hardwarové paměti nebo změna zachycená v takovém hardwarovém nosiči pro data, který má kriminalistickou relevanci (související s kriminalisticky relevantní událostí), je zkoumána (hledán, zajišťování, konkrétní zkoumání) kriminalisticko- (forenzní) informatickou (kyber) metodou a na

---

39 RAK, R., PORADA, V. Digital trace, *Booklet from scientific conference "Advances in criminalistics",* Police Academy, Prague, 2004

40 Digital Evidence: Standards and Principles. Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE) [online]. Říjen 1999 [cit. 2024-02-25]. Dostupné z WWW: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

základě jejího zkoumání je možné identifikovat vztah digitálních stop a objektu, který ji vytvořil. Digitální stopa je jakákoliv informace, která má komunikační hodnotu, uložená nebo přenášená v digitální podobě.“[41]

Výše zmíněná definice počítá s jakoukoliv digitální technologií. Pokrývá oblast počítačů, mobilních telefonů, digitální TV, videa, zvuku, fotografií, dat z kamerových systémů, dat elektronických bezpečnostních systémů apod. Digitální stopa musí být použitelná nejen pro kriminalistiku, ale i pro obecné forenzní vyšetřování státních orgánů či pro potřeby nezávislých interních a externích auditů apod. [42]

3.3 Digitální stopy a místo trestného činu

Podle Raka a Porady[43], místo trestného činu většinou není v případě digitálního (kybernetického) trestného činu jasně definovatelné, jako je tomu v případě běžných kriminalistických stop. Naopak může být velice těžko geograficky vymezitelné. V těch nejjednodušších případech lze na místě činu nalézt důkazní materiál ve formě hmotných nosičů digitálních informací, jako např. PC, notebooky či jiná digitální zařízení. Digitální stopy jsou uloženy přímo v těchto zařízeních.

Většinou však nastane situace, kdy je počítač (či jiné zařízení) propojen do rozsáhlé podnikové sítě, do prostředí internetu apod. Servery mohou být uloženy mimo instituci, v jakékoliv zemi na druhé straně polokoule (cloudové úložiště).

Další překážkou může být fakt, že vyšetřovatelé čelí profesionálnímu pachateli, který se zmocnil nejvyšších administrátorských práv správce systémů, skryl své stopy a

---

41 Digital Evidence: Standards and Principles. Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE) [online]. Říjen 1999 [cit. 2024-02-25]. Dostupné z WWW: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

42 Whitcomb, C., M. International. An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence* [online]. Spring 2002, Volume 1, Issue 1 [cit. 2024-02-20].Dostupné z WWW: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

43 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

v digitálním prostředí se pohyboval téměř neviditelně. Při kybernetických útocích pak postupoval několikanásobným, řetězovým ovládnutím většího počtu serverů a poškozený pak ani neví, kdo vlastně útočí. Vyšetřovatelé musí odkrýt celý řetězec postupných kroků a tím je místo trestného činu téměř nevymezitelné, neboť se v žádném případě nejedná o malý fyzický prostor.

Digitální stopy také mohou být důsledkem organizované trestné činnosti za účasti vícera zapojených pachatelů, spolupracujících za pomoci různých technologií, sdílejících určité činnosti či prostředky a působících v různých zemích.

Jak již bylo zmíněno, definovat místo trestného činu může být nesmírně složité, pro odvětví kybernetické kriminality, proto dle Porady a Raka vyčleňujeme tyto čtyři oblasti:[44]

- Oblast zájmu – cíl útoku, ve kterém pachatel koná trestnou činnost
- Oblast podpory zájmu – okolní prostředí (servery na přístupových trasách, komunikační cesty, spolupachatelé, prostřednící apod.). Oblast podpory zájmu může být i krycím prostředím, jehož cílem je zahladit stopy a popřít souvislost mezi oblastí zájmu a oblastí pachatele. Někdy může oblast podpory zájmu sloužit jako skutečný prostředek ke spáchání trestného činu.
- Oblast pachatele – je místem, ze kterého pachatel organizuje, koordinuje aktivity směrované do oblasti jeho zájmu. Zajištění digitálních stop v této oblasti často vede k odhalení celé složité organizační struktury či technologických kanálů a prostředků pro realizaci útoku. V této oblasti lze nalézt klíčové důkazy, neboť v ní můžeme dokázat přímou vazbu mezi pachatelem a jeho činnostmi.
- Oblast zázemí pachatele – bezprostřední oblast, ve které pachatel působí, pro něj není bezpečná z hlediska potenciálního vyšetřování. Zřídkakdy do ní tedy pachatel ukrývá cokoliv, co by mohlo vést k jeho prozrazení. Pachatel proto využívá různé způsoby skrývání své trestné činnosti. Může se jednat o uložení citlivých informací na speciální místo či speciální datový nosič, ukrytý někde

---

44 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

mimo logickou strukturu zázemí pachatele. Aktivita trestného činu (peníze, datové nosiče apod.) může být skryta i v trezoru v bance (samozřejmě ne v té, kterou pachatel běžně využívá).

3.4 Kriminalistický pohled na digitální stopy

Digitální stopy se stále častěji využívají jako důkazy v trestním řízení. Dokáží prozradit až neuvěřitelně mnoho detailů o podezřelém. Digitální stopy z mobilních telefonů, jako např. e-maily, SMS zprávy či ukládání polohy a pohybu uživatele se jako důkazy používají již docela dlouho. S přibýváním digitalizace a „chytrých přístrojů" v domácnosti také přibývá zařízení, která ukládají naše další digitální stopy (a která mohou v případě potřeby sloužit jako důkazy). Jako typický příklad můžeme uvést případ, kdy podezřelý ve Velké Británii tvrdil, že v době spáchání trestného činu byl doma a pral prádlo. Nicméně digitálnímu forenznímu týmu se podařilo prokázat z dat z jeho chytré pračky, že byla aktivována telefonem z místa činu. Aplikace pro zapnutí chytré pračky měla práva pro využívání lokalizace polohy. Data z chytrých hodinek nám mohou taktéž prozradit mnoho užitečných informací o jejich nositeli z doby spáchání trestného činu, na základě měření srdečního tepu nebo sledování pohybů. Pokud má někdo doma chytré elektroměry, které zaznamenávají spotřebu ve vteřinovém rozlišení, z jejich dat můžeme vyčíst, že někdo v určitou chvíli zapnul světlo nebo otevřel ledničku.[45]

V současné době jsou digitální stopy všudypřítomné. Osobní počítače můžeme brát jako rozsáhlý archiv lidského počínání, který dokáže prozradit o člověku nesmírné množství intimních informací (co kdy děláme, kde nakupujeme, co jsou naše slabosti, co máme rádi atp.). Z digitálních stop lze vyčíst o člověku (pachateli nebo oběti) tolik, až to můžeme považovat za hluboký psychologický náhled do duše (pachatele nebo oběti).

V dnešní době se mnoho z lidské činnosti digitalizuje, což představuje výzvu i pro policejní orgány, které se musí tomuto aktuálnímu trendu přizpůsobit a umět vyhodnocovat celou komplexní problematiku digitálních stop (ve smyslu, kdy digitální stopa slouží jako důkaz nebo jako objekt trestné činnosti). Je potřeba mnoha specialistů, kteří dokážou vyvozovat relevantní závěry využitelné pro orgány činné v trestním řízení. Existuje jasný postup, jak provádět zajišťování, zpřístupňování a vyhodnocování těchto

45 ZANDL, P. *Mýty a naděje digitálního světa*. Vyd. 1. Brno: Jan Melvil Publishing, 2022. ISBN 978-80-7555-175-7

stop. Aby byl tento postup validní a obecně aplikovatelný, bylo potřeba jasně definovat některé pojmy. Pokud tedy hovoříme o ***digitální stopě*** z pohledu kriminalistiky, jedná se o:

1) digitální informace nebo jakákoliv data přenesená nebo uložená za použití počítačového systému, která se zpravidla nachází na magnetickém, optickém nebo polovodičovém médiu v prostředí datových sítí (souhrnně „digitální data“)

2) hmotný nosič digitální informace[46]

Další důležitý pojem **je zajišťování digitálních dat,** kterým v kriminalistice rozumíme:

Úkon trestního řízení, který není výslovně upravený v zákoně č. 141/1961 Sb., o trestním řízení soudním (trestním řádu), a který spočívá v pořízení kopie digitálních dat označených zpracovatelem spisu za věc důležitou pro trestní řízení (§ 77b trestního řádu) a pokud to z technických důvodů není možné, v pořízení multimediálního záznamu zobrazení takových digitálních dat na jiném zařízení.[47]

Je také třeba si definovat **zpřístupňování zajištěných digitálních dat.** Definici podle Čápa a kol [48]můžeme formulovat nějak takto:

Úkon trestního řízení, jenž není výslovně upravený v trestním řádu a spočívá v přípravě zajištěných digitálních dat do technické podoby, která je vhodná pro účely následného vyhodnocování a respektuje zásady kybernetické bezpečnosti.

---

46 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

47 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

48 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

Dalším důležitým základním pojmem je **vyhodnocování zajištěných a zpřístupněných digitálních dat:**

Úkon trestního řízení, který není výslovně upravený v trestním řádu a spočívá buď v analýze digitálních dat (hledání informací relevantních k příslušné trestní věci) nebo syntéze digitálních dat (přiřazení nalezené informace do kontextu s trestní věcí).

Kromě výše zmíněných pojmů je důležité zmínit i několik dalších, které definuje Rak a Janíček:[49]

Zabavení/zajištění digitálních stop – proces začínající v momentu, kdy jsou zjištěny informace o zařízení nebo je zařízení nalezeno uložené za účelem zabavení a prozkoumání. Fyzické a datové objekty se stanou důkazem za předpokladu, že jsou shledány přijatelnými orgány činnými v trestním řízení.

Datové objekty – jsou buď objekty nehmotné podstaty nebo informace mající důvěryhodnou komunikační hodnotu, přičemž jsou spojeny s prvky hmotné podstaty, jichž se dokážeme dotknout. Datovými objekty mohou být databáze, adresáře, soubory, obsahy virtuálních pamětí, digitální video nebo audio záznamy a další.

Fyzické objekty – média, kde jsou datové objekty uloženy a prostřednictvím kterých jsou přenášeny. Mohou to být pevné disky, diskety, CD a DVD, paměťové karty, flashdisky apod. V širším smyslu chápeme fyzické objekty jako celá zařízení (počítače, tiskárny, síťové komponenty a další), obsahující kromě digitálních stop i jiné informace důležité pro vyšetřovatele (sériová čísla, mechanické nebo biologické stopy a další stopy), které mohou prokázat logickou souvislost mezi fyzickým zařízením (vlastník, uživatel, čas a další) a jeho uživatelem (pachatelem) a trestným činem nebo jinou aktivitou, která je předmětem vyšetřování.

Originál digitální stopy – fyzický či datový objekt zadržený pro potřeby znaleckého nebo forenzního zkoumání. Originály jsou základním důkazním materiálem. Vyšetřovatelé si pro pracovní účely vytvářejí duplikáty či kopie originálních digitálních stop, pčičemž samozřejmě nedochází k žádné změně informací. Duplikovaný materiál má stejnou informační hodnotu jako originál a vytváří se především pro potřebu

---

49 RAK R., JANÍČEK P. Identification in criminalistic and security practice supported by computer technology, Expertise n. *3/2000*, volume V, p. 30-38, 2000

opakovaného vyšetřování nebo v případech, kdy samotný fyzický objekt nelze z jakýchkoliv důvodů zajistit pro potřeby orgánů činných v trestním řízení (např. firemní PC).

Kopie digitální stopy – kopií rozumíme přesnou reprodukci informací z původního fyzického objektu na jiné, fyzicky nezávislé datové médium. Vytvořením kopie vytvoříme datový objekt se stejnými informacemi za použití fyzického objektu, který může být jiného typu. Kopie obsahují pouze část datových objektů z původního fyzického objektu, informační hodnota se ale oproti originálu nemění.

3.5 Zajištění digitální stopy

Zajištění digitálních stop je určeno hlavním zpracovatelem trestního spisu. Stopy se získávají pomocí zajišťovacích institutů podle trestního řádu (předložení nebo vydání věci podle § 78 trestního řádu, odnětí věci podle § 79 trestního řádu a ohledání podle § 13 trestního řádu). Zajištění digitálních stop lze realizovat jako zajištění digitálních dat uložených na hmotném nosiči digitální informace (PC, notebook, server, USB flashdisk atd.). Policie ČR může data buď zkopírovat nebo provést bitovou kopii, popřípadě může provést snímání obrazovky monitoru za pomoci vhodného softwaru, foto nebo video dokumentaci.

Kdo provádí zajišťování digitálních stop:

a) policista (oprávněn zajišťovat pouze hmotné nosiče digitální informace)

b) kriminalistický technik (zajištění hmotných nosičů a foto a video dokumentace)

c) kriminalistický IT specialista (kromě výše zmíněných oprávnění také může zajišťovat data ve formě bitových kopií, obsahu datových úložišť, obsahu internetových stráněk, sociálních sítí, virtuálních měn, e-mailových adres apod.)

d) znalec (poskytuje metodickou pomoc pro zajištění digitálních stop výše zmíněným osobám a znalecké zkoumání digitálních stop zajištěných v trestním řízení)[50]

Jak se digitální stopa zajišťuje:

Tento úkon je upraven interním aktem řízení (pokyn ředitele Kriminalistického ústavu č.34/2019).

Je také nutné teoreticky vymezit termín počítačová kriminalita. Často se uvádí pojem jednoho ze současných teoretiků tohoto tématu, profesora Vladimíra Smejkala. Ten chápe počítačovou kriminalitu jako páchání trestné činnosti, v níž určitým způsobem figuruje počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď:

a) jako předmět trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité

b) jako nástroj trestné činnosti[51]

Zajištění digitální stopy může být provedeno jakoukoliv osobou, která je k této činnosti oprávněna (policista zařazený v organizačním článku útvaru, který vede trestní řízení), popř. tato osoba může vhodný postup konzultovat s dalšími osobami (kriminalistický technik nebo IT specialista, znalec). Digitální stopy se získávají za pomoci zajišťovacího institutu podle trestního řádu (předložením či vydáním věci, odnětím věci, a to i v rámci uskutečnění domovních prohlídek, osobních prohlídek či prohlídek jakýchkoliv jiných prostor, a ohledáním místa, činu či věci).[52]

---

50 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

51 SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi, s. 20-21. ISBN 978-80-7380-501-2

52 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

Čáp a kol.[53] také ve svém textu tvrdí, že originální hmotný nosič digitální informace by měl být uchováván v zapečetěném obalu, který smí být rozpečetěn pouze v rámci procesního úkonu za zákonem stanovených podmínek či v rámci znaleckého zkoumání.

V případech, kdy nelze zajistit originální hmotný nosič digitální informace, digitální stopa může být zajištěna vytvořením její kopie na technologický hmotný nosič digitální informace. Kopie by měla být opatřena kontrolním součtem (pro ověření autenticity), který je nutné zaprotokolovat. Pokud tento úkon nelze vykonat, je nutné nosič uložit do zapečetěného obalu a nakládat s ním stejným způsobem jako v případě originálního nosiče.

Ohledání zajištěné techniky (originál nebo kopie bez vytvořeného kontrolního součtu) probíhá dodatečně. Úkon vždy musí splnit všechny zákonné podmínky. Provádí ho kriminalistický IT specialista podle postupů stanovených Kriminalistickým ústavem (pokyn ředitele Kriminalistického ústavu 34/2019). O provedeném úkonu se musí sepsat protokol o ohledání (podle § 55 trestního řádu). Toto dodatečné zajištění digitálních dat slouží prvoplánově k tomu, aby digitální data nebyla již nadále vázána na svůj konkrétní hmotný nosič digitální informace (tudíž se nemusí jejich autenticita zajišťovat zapečetěným obalem) – to dává vyšetřujícím možnost vytvoření identické pracovní kopie digitálních dat, kterou lze nadále kopírovat a tím může být najednou vyhodnocována více orgány. Originální hmotný nosič digitální informace také může být vrácen majiteli, pokud to situace vyžaduje a jeho dlouhodobě zajištění by mohlo způsobit materiální škody či způsobit ohrožení.

Existují i specifické případy zajišťování digitálních dat, které se nenacházejí na žádném hmotném nosiči. Mezi tyto případy patří např. zajištění obsahu webových stránek, e-mailových schránek či profilů sociálních sítí. Obsah z těchto platforem lze zajistit několika způsoby. Za pomoci speciálních programů či doplňků webových prohlížečů lze transformovat kompletní obsah do podoby off-line zálohy. Také lze využít programy na snímání obrazovky nebo provedení foto či video dokumentace obrazovky

53 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

monitoru (nebo displeje), na kterém je webová stránka (nebo profil sociální sítě nebo cokoliv jiného) zobrazena. [54]

3.6 Zpřístupňování zajištěných digitálních dat

Jakákoliv následná činnost prováděná s digitálními daty musí zaručit jejich neměnnost, jejich důkazní hodnota a přezkoumatelnost, a to v jakékoliv fázi trestního řízení. K této záruce dochází většinou tím, že jsou jakékoliv úkony s digitálními daty prováděny na pracovních kopiích opatřených kontrolními součty, které jsou před jednotlivými úkony a při kopírování dat verifikovány.

Na zpřístupňování zajištěných dat spolupracuje kriminalistický IT specialista specializovaného pracoviště útvaru společně se zpracovatelem spisu. Podle autorů Čápa, Breu a Proška[55], zpřístupňování dat probíhá v následujících bodech:

a) zpřístupňování se vždy děje na kopii zajištěných digitálních dat opatřených kontrolním součtem zajišťujícím autenticitu. Vlastní práce se zajištěnými daty při procesu jejich zpřístupňování probíhá zásadně na tzv. pomocné pracovní kopii. Pomocnou pracovní kopii si kriminalistický IT specialista vytvoří před začátkem procesu z pracovní kopie.

b) za pomoci speciálního software (forenzně-analytické nástroje, nástroje pro obnovu digitálních dat, indexačně-analytické nástroje apod.) začne kriminalistický IT specialista proces zpřístupňování na základě konkrétních požadavků. Může se také spolupodílet na vyhodnocování zajištěných digitálních dat.

---

54 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

55 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

c) výstupy procesu zpřístupňování zajištěných dat mohou být:

- Selekce souborů podle typu či podle klíčových slov včetně obnovy smazaných souborů
- Selekce e-mailové komunikace včetně obnovy smazané komunikace
- Výpisy z historie webových prohlížečů
- Výpisy z registru informačních systémů
- Vytvoření časové osy či provázanosti ve vztahu ke konkrétním souborům a osobám zúčastněným v dané trestní věci

d) dochází k redukci množství digitálních dat, která budou předána k procesu vyhodnocování, popř. budou využita jako důkazní materiál. V této části lze tímto postupem separovat digitální data a techniku nepotřebnou pro účely trestního řízení a lze ji vrátit majiteli

e) lze provést proces zpřístupňování digitálních dat provedením ohledání (podle § 113 trestního řádu). Je nutné provést kontrolu autenticity dat pomocí kontrolního součtu – ohledání je totiž nutno provést na původních a nezměněných zajištěných digitálních datech

f) je sepsán protokol o zpřístupnění zajištěných digitálních dat, případně protokol o ohledání

g) výstupem procesu zpřístupňování je protokol o provedeném úkonu. Ten obsahuje list souborů a adresářů dat s kontrolními součty. Přílohou protokolu je hmotný nosič digitálních informací se zpřístupněnými daty, případně lze přidat i tištěnou podobu jednotlivých souborů.

3.7 Vyhodnocování zajištěných a zpřístupněných digitálních dat

Vyhodnocení provádí zpracovatel spisu (obeznámený s podstatou trestní věci) společně s analytiky útvaru, popřípadě s kriminalistickými IT specialisty specializovaného pracoviště útvaru. Vyhodnocení je prováděno za pomoci analytických

nástrojů, informačních systémů Policie ČR případně jiných externích zdrojů. Dále je sepsán protokol o vyhodnocení zajištěných a zpřístupněných digitálních dat –

- (s náležitostmi podle § 55 trestního řádu). Vyhodnocená data jsou součástí originálu trestního spisu.[56]

3.8 Dokazování, vrácení věci

Je nutné zachovat hmotné digitální nosiče, které budou sloužit jako důkazní materiál před soudem. K vrácení lze přistoupit jen tehdy, není-li věc důležitá pro trestní řízení. Nicméně v praxi to není tak jednoduché. Z technických i časových důvodů je často předvedení důkazu z originálního hmotného nosiče nemožné a je nutné vytvořit kopii materiálů na jiný technologický hmotný nosič digitální informace, samozřejmě za předpokladu dodržení doporučených postupů při zajišťování.[57]

56 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

57 SMEJKAL, V. *Kybernetická kriminalita.* 3 vydání. Plzeň Aleš Čeněk, 2022. ISBN 978-80-7380-849-5

4 Forenzní analýza digitálních stop

Forenzní analýza je soubor postupů dokazování v široké řadě oborů; v chemickém, medicínském, počítačovém apod. Tyto postupy mají za úkol zajistit, aby prováděné zkoumání bylo realizováno s ohledem na legislativní požadavky dokazování v soudně-právní rovině. V počítačovém odvětví plní forenzní analýza specifickou roli využitím specifických přístupů, kterými zajišťuje správné získávání důkazů.

Forenzní analýza nemůže existovat sama o sobě bez předchozího forenzního hodnocení; jsou to navazující postupy. Hodnocení předchází následujícím analytickým postupům, extrahuje data a připravuje je k následné analýze.[58]

Lehce pochopitelnou definici, co to vlastně forenzní analýza dat je, nám podává webová stránka firmy zaměřující se na zajišťování digitálních dat RiskAnalysisConsultants:[59]

„Digitální forenzní analýza je věda i schopnost získávání, vyhledávání a interpretace digitálních dat pro trestní, obchodní nebo soukromé soudní procesy nebo soukromé účely. Výsledky analýzy by mohly být důkazem o trestné činnosti, porušení vnitřních předpisů nebo by mohly být důležité z různých důvodů a za standardních podmínek nepřístupné.“

Laicky řečeno, jedná se o analýzu jakýchkoliv digitálních dat za účelem zjištění, co, kdy a jak se co stalo a kdo je zainteresovaný.

Digitální forenzní analýza se dá analogicky přirovnat k běžné vyšetřovací metodice. Pokud se stane např. vražda, bude nutné ohledat místo činu za účelem rekonstrukce toho, co se stalo, za účelem nalezení pachatele a ke sběru důkazů. Podobná rekonstrukce probíhá i v případě, kdy je potřeba prozkoumat digitální zařízení či data. A to právě zkoumá digitální forenzní analýza. Digitální data jsou nicméně oproti hmotným důkazům na místě činu velmi nestálá – tomuto faktu by se mělo přizpůsobit nakládání s daty, jejich sběr, transport a uchovávání.

---

58 CASEY, Eoghan. Handbook of digital forensics and investigation. Boston: Academic, c2010. ISBN 978-0-12-374267-4, s. 38

59 Risk Analysis Consultants. Digitální forenzní analýza [online]. 2021 [cit. 2024-03-12]. Dostupné z WWW: https://www.rac.cz/cs/digitalni-forenzni-institut/digitalni-forenzni-analyza/

4.1 Zajišťování digitálních stop ve forenzní analýze

Nyní se bude práce věnovat způsobu, jak dochází k zajišťování digitální stop ve forenzní analýze digitálních stop. Samotné zajišťování digitálních dat patří mezi úkony trestního řízení. To spočívá v tom, že je pořízená kopie digitálních dat. Ta označí zpracovatel spisu za důležité pro trestní řízení, případně pořízením multimediálního záznamu zobrazení takových digitálních dat na jiném zařízení. K zajišťování digitálních stop jsou oprávněné následující subjekty:

- policista bez speciálních znalostí: je oprávněný zajišťovat pouze hmotné nosiče digitální informace;

- kriminalistický technik (je vázán 3 Čl. 2 písm. b) pokynu policejního prezidenta č. 100/2018)

- kriminalistický IT specialista: smí např. zajišťovat data ve formě bitových kopií hmotných nosičů digitální informace, zjišťovat obsah datových úložišť, obsah webových stránek a sociálních sítí, dále pak on-line komunikátorů, e-mailových schránek či virtuálních měn.

- znalec: představuje metodickou pomoc na místě úkonů trestního řízení; provádí znalecké zkoumání digitálních stop, které byly zajištěné v trestním řízení (smí extrahovat e-mailovou komunikaci, obnovovat smazané soubory apod.)[60]

Mezi tři základní pojmy, které se řadí k úkonům forenzní analýzy patří:[61]

- model: jedná se o soubor aktivit, které jsou aplikované během vyšetřování digitálních stop,

- fáze: jedná se o nejvyšší komponentu během členění na menší strukturní celky.

- úloha: seznam jednotlivých úkonů, které je třeba provést.

---

60 ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf

61 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1

Mezi postupy forenzní analýzy digitálních stop patří následující:

CFIP (Computer Forensic Invstigative Process). Jedná se o model z roku 1984. Postup analýzy je zde rozdělen do čtyř fází: zajištění (obvykle sestává ze zajištění paměťových médií, hardwaru apod.), identifikaci (získání stop ze zajištěných zařízení a převod na srozumitelnou prezentaci), ocenění (posuzování relevantnosti k vyšetřovanému činu) a prezentaci (prezentace příslušným orgánům). V první fázi se tedy provádí zajišťování důkazů, v nichž budou dále vyhledávány digitální stopy (v souladu s principy a postupy forenzního institutu. Laicky řečeno, první fáze se věnuje např. zajišťováním hardwaru, paměťových médií apod. V druhé fázi se provádí získávání digitálních dat ze zajištěných zařízení, data (digitální stopy) se dále převádí do srozumitelné prezentace. Ta se ve třetí fázi posuzuje z hlediska relevantnosti k vyšetřovanému trestnému činu a také musí být rozhodnuto, zda jsou získaná data legitimním důkazem. V poslední fázi dochází k prezentaci legitimních důkazů příslušným orgánům.[62]

DFRWS (Digital Forensic Research Workshop) Investigative Model. Používá se od roku 2001. Metodika vyšetřování sestává ze 6 fází vyšetřování. Fáze jsou specifické tím, že se řídí podle vodopádového modelu a každá fáze začne až po skončení předchozí.

Fázemi zde jsou:

- identifikace – tato fáze má za úkol ohledat místo činu, monitorovat relevantní digitální zařízení, určovat uživatelské profily, analyzovat s cílem stanovit základní parametry činu
- uchování – stanovení způsobu uchování zajištěných digitálních dat, aby nedošlo během jejich zkoumání k jejich kontaminaci či poškození
- sběr – získání relevantních dat ze zajištěných zařízení prostřednictvím schválené metodiky
- zkoumání – probíhá zde data mining – vytěžování dat, zviditelnění dat včetně obnovení dat, která byla uživatelem smazána a následné dešifrování a sledování procesů, jak data vznikla

---

62 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. S. 197-199. ISBN 978-80-87236-16-1

- analýza – probíhá nastejno s fází zkoumání. Dochází ke stanovení posloupnosti vzniku dat, posouzení validity dat a dochází k dalším aktivitám, pomocí kterých se vyhodnocují důkazy. Cílem je poskytnout vyšetřovateli komplexní obraz o aspektech spáchaného trestného činu
- Prezentace – prezentace dokumentace výstupů analýzy ve formě schválené rozhodčím orgánem[63]

ADFM (**Abstract Digital forensic Model**). Používá se od roku 2002 a rozšiřuje metodiku DFRWS. Jednotlivé kroky se zde člení následujícím způsobem a doplňují tak zmíněnou metodiku DFRWS: identifikace, příprava, strategie přístupu. Stanovení přístupů, které se použijí při následném ohledání důkazů, uchování, sběr, zhodnocení, analýza, prezentace, vrácení důkazů (doplňuje DFRWS, důkazní materiály jsou předány k archivaci nebo navráceny majiteli).[64]

IDIP (**Integrated Digital Investigation Process**). Používá se od roku 2003. Jeho cílem je integrovat všechny předchozí postupy. Sestává z 5 fází: připravenost (dochází k naplnění podmínky připravenosti a to pomocí zajištění nástrojů nutných pro vyšetřování – technologie, metodika, infrastrukturní připravenost v podobě zajištění lidských zdrojů), rozvinutá fáze (probíhá analýza vzniku potenciálních incidentů, jenž mohli vést k trestnému činu), fyzické vyšetřování trestného činu (samotné ohledání místa trestného činu, zajištění digitálních stop a jejich forenzní zkoumání, transport dat na expertní pracoviště), digitální vyšetřování trestného činu (specializované vyšetřování digitálních stop a stanovení výstupů vyšetřování, které se integrují do fáze fyzického vyšetřování), zhodnocení (probíhá interní diskuze všech výsledků vyšetřování).[65]

---

63 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1, s. 200.
64 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1, s. 201.
65 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1, s. 202-203.

EFIP (**Enhanced Digital Investigation Process**). Používá se od roku 2004 a navazuje na IDIP.[66]

CFFTP (**Computer Forensic Field Triage Process**). Používá se od roku 2006 a snaží se pokrýt veškeré oblasti, které zasahují do digitálního místa činu. Zaměřuje se nejen na uchování dat ze zařízení, které bylo nalezené na místě činu, ale také na data mining – vytěžování dat, a na trasování informací, které je možné ze zařízení získat. Probíhá zde 6 fází: plánování, třídění a prioritizace, vytvoření uživatelského profilu, časová posloupnost (zrekonstruování vzniku a užití jednotlivých datových stop), internet (dochází ke zkoumání aktivit uživatele v síti), specifičnost případu (dochází ke komparaci zjištěných skutečností všech digitálních stop a jejich přiřazení k podstatě trestného činu).[67]

DFMMIP. Používá se od roku 2009, vychází z malajské vyšetřovací praxe a skládá se ze 7 fází: plánování, identifikace, průzkum (primární zajišťování digitálních stop na zapnutých zařízení. Pokud by došlo k vypnutí zařízení, může se stát, že dojde ke ztrátě neuložených dat, např. rozepsaného emailu nebo k automatickému odhlášení chráněného heslem), doprava a uložení, analýza, potvrzení důkazů, archivace.[68]

Pokud by se měly shrnout výše uvedené modely, je možné odvodit základní univerzální metodiku forenzní analýzy digitálních stop. Z tohoto obecného pohledu je možné členit metodiku do pěti obecných fází. Ty mohu být podle potřeby rozšiřovány, proto můžeme o následujících pěti fázích hovořit jako o generickém modelu:

- pre-process,
- zajištění a uchování,
-analýza,

---

66 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1, s. 203.

67 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1, s. 205-206.

68 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1, s. 206-207.

-prezentace,

-následný proces[69]

V knize Handbook of digital forensics and investigation[70] se říká, že metody forenzní analýzy digitálních dat se zakládají na 4 fázích, které zahrnují:

1. Sběr informací a pozorování aneb forenzní hodnocení. Tato fáze ověřuje autenticitu digitálních důkazů a ukládá si za cíl realizovat šetření a posouzení co nejefektivněji a také s ohledem na nástroje, které lze uplatnit v dalším postupu. Často se v této fázi využívá vyhledávání za pomoci klíčových slov a dochází k prvotnímu posuzování konfigurace systémových komponent.

2. Formulace hypotézy – tato fáze má za úkol objasnit a vysvětlit pozorované jevy, uplatňuje se zde snaha sdružit posbírané důkazy do určitých vztahových celků s cílem vytvořit potenciální obraz kriminálního činu.

3. Evaluace hypotézy – v této fázi dochází k verifikaci hypotéz stanovených ve druhé fázi analýzy. Verifikace probíhá na základě znovu-zhodnocení všech informací.

4. Tvorba závěrů a komunikace výstupů – po verifikaci a důkladném posouzení je znění hypotézy nutno opravit do takové formy, v jaké je možné ji komunikovat směrem k příslušnému rozhodčímu orgánu.

---

69 RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1

70 CASEY, Eoghan. Handbook of digital forensics and investigation. Boston: Academic, c2010. ISBN 978-0-12-374267-4, s. 23-24

5 Ochrana a správa digitálních stop

Otázka ochrany soukromí na internetu je v posledních letech předmětem velkého množství sporů a diskusí. Za zmínku zde stojí dva technické důvody. Prvním z nich je obtížnost vyšetřování údajných porušení ochrany osobních údajů, protože bývají chráněny také údajů uživatelů, kteří potenciálně dat zneužili. Druhým problémem je přeshraniční povaha zveřejněných údajů, které brání vyšetřování a případné postihnutí pachatele a uplatňování zákonů ve fyzickém světě.[71]

5.1 Strategie pro ochranu osobní digitální stopy

Způsoby, jak chránit digitální stopu, mohou být podle M. Stanleyho[72] následující:

1. Uživatel by se měl aktivně snažit o ochranu své digitální stopy. Pokud uživatel začne sám pátrat po své digitální stopě, může být snadno velmi nemile překvapen tím, co odhalí. Jeho zjištění mohou být alarmují, protože zjistí, že odhaluje data, která vůbec nechce zveřejnit. V případě, že uživatel odhalí data, která si nepřeje zveřejnit (jsou citlivá, nesprávná, zavádějící nebo nevhodná), měl by uživatel kontaktovat správce daného webu a požádat o odstranění, případně data odstranit sám, pokud je to možné.[73]

71 CHENG F. CH, WANG, Y.S. The Do Not Track Mechanism For Digital Footprint Privacy Protection In Marketing Applications. 2018. Journal of Business Economics and Management. Volume 19, Issue 2: 253-267. ISSN 1611-1699 / eISSN 2029-4433

72 MORGAN STANLEY. Strategies to Help Protect Your Digital Footprint [online]. 9.10.2023. [cit. 2024-01-23]. Dostupné z WWW: https://www.morganstanley.com/articles/digital-footprint-protection-strategies

73 MORGAN STANLEY. Strategies to Help Protect Your Digital Footprint [online]. 9.10.2023. [cit. 2024-01-23]. Dostupné z WWW: https://www.morganstanley.com/articles/digital-footprint-protection-strategies

2. Využití nástrojů na ochranu digitální stopy. V dnešní době již existují dostupné online nástroje, které chrání soukromí uživatele. Jedná se zejména o placené online nástroje (např. Kamo[74], AntiTrack[75] aj.)

3. Nastavení přísnějšího nastavení ochrany soukromí. Poskytovatelé sociálních sítí, e-shopů, e-mailu, webových prohlížečů, online setkání apod. dávají svým uživatelům často na výběr, jak spravovat nastavení zabezpečení svého účtu. Zde by se měl uživatel rozhodnout mezi přísností nastavení ochrany a mezi uživatelským pohodlím, protože při velmi striktním nastavení může klesnout použitelnost webu nebo vést k různým nevýhodám.

4. Opatrnost na sociálních sítích. Zde je velkým rizikem to, že nikdy není zřejmé, kdo bude obsah, který uživatel zveřejní, sdílet a na základě čehož to bude opět sdílet někdo dále. Následně to, co jsme zveřejnili v dobré víře může být proti nám zneužito. Velké riziko v tomto ohledu je zcela určitě kyberšikana.

5. Omezení oprávnění mobilní aplikace. Pokaždé, když uživatel udělí mobilním aplikacím souhlas se zpřístupněním k poloze, fotoaparátu, kontaktům či fotografiím, zpřístupňuje tyto údaje i poskytovateli aplikace. Ten tyto informace může předávat dál nebo je uchovávat pro vlastní potřebu. Uživatel musí více přemýšlet o tom proč např. videoherní mobilní aplikace vyžaduje přístup k jeho poloze, kontaktům apod.

6. Omezení online účtů. Čím větší počet účtů daný uživatel má, tím větší produkuje digitální stopu. K jejímu snížení může pomoci deaktivace účtů, které uživatel již nepotřebuje. Uživatel by si měl klást otázky? Skutečně potřebuji několik emailových adres, které nepoužívám?

7. Využití správce hesel. Správce hesel je softwarový nástroj, jehož úkolem je bezpečně šifrovat a vytvářet jedinečná a složitá hesla.

8. Dvoufázové ověřování. Někdy se také nazývá jako dvou faktorové

ověřování. Je vhodné pro maximalizaci ochrany uživatelských účtů.

---

74 KAMO. Kamo zastaví online sledování a ochrání vaše soukromí. Ccleaner.cz [online]. © 2005-2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.ccleaner.com/cs-cz/kamo

75 GIVENS, CH. Digitální stopa zařízení a sledování na internetu. In *Avast* [online]. 2.10.2019 [cit. 2024-01-24]. Dostupné z WWW: https://blog.avast.com/cs/fingerprinting-and-the-surveillance-economy

9. Propojení účtů. Někteří poskytovatelé služeb umožňují propojit některé účty a umožňují, aby se uživatelé přihlásili např. přes Facebook nebo Google. Tímto způsobem uživatel zvyšuje možnost potenciálního sledování.

10. použití VPN (virtuální privátní síť). Ta skryje IP adresu a tím se částečně zakryje i digitální stopa. Díky VPN je také možné vést anonymní online komunikaci za pomoci šifrování. Také zabraňuje třetím stranám, aby shromažďovali historii vyhledávání.

11. Požádat o smazání údajů.

12. Deaktivace účtů, které nepoužíváme.

13. Nevyužívat služeb veřejné Wi-Fi sítě. Pokud ji využíváme, ostatní mohou odposlouchávat konverzace, krást hesla či zachytit nešifrovaná data. Při užívání veřejné Wi-Fi sítě vždy užívat anonymní prohlížení a VPN.

14. Anonymní režim prohlížeče. Vymazává mezipaměť, historii prohlížeče a cookies.

15. Používat bezpečnostní software – antivirové programy (některé již obsahují další aplikace proti sledování, zabezpečené platby, VPN apod.)

16. Zabezpečit účty silnými hesly

17. Nesdílet soukromé informace, osobní údaje či přihlašovací údaje v e-mailu či chatu

18. Zveřejňovat pouze informace nezbytné pro používání aplikace

19. Nastavit soukromí svých profilů na sociálních sítích, aby byly informace viditelné jen pro přátele

20. Zrušit účty u všech služeb, které uživatel nepoužívá

21. Vypnout sledování polohy v aplikacích, zapínat jen v nutných případech

22. Pro každou službu nastavit jiné heslo

23. Bezpečnostní software nainstalovaný na každé zařízení připojené k internetu

24. Mazat historii alespoň jednou za 3 měsíce

25. Vypnout sledování polohy

26. Použití nástroje proti sledování (DuckDuckGo, Privacy Badger, TrackOFF aj.)

27. Odmítat cookies, kdykoliv to lze

28. Být opatrný se stahováním aplikací, neboť každé aplikaci automaticky udělíme určitá oprávnění ke shromažďování dat – kontrolovat, povolovat jen to nejnutnější, při delším nepoužívání aplikaci uspat nebo odinstalovat.

29. Použít prohlížeč Tor (název softwarového systému zajišťujícího anonymizaci uživatele při pohybu na Internetu)

30. Nepoužívat veřejnou wifi síť[76] [77]

5.2 Právní aspekty spojené s digitální stopou

Problematika zajišťování, zpřístupňování a vyhodnocování digitálních stop nabývá v posledních letech na významu i z pohledu odhalování kriminálních činů. Národní centrála proti organizovanému zločinu kriminální policie a vyšetřování Policie ČR („dále jen NCOZ SKPV“) proto stanovila postup, jak provádět zajišťování, zpřístupňování a vyhodnocování těchto stop.

K popisu zajišťování digitálních stop je třeba nejprve vymezit pojem „počítačová kriminalistika“. Jedná se o pojem profesora Vladimíra Smejkala[78]. Ten vnímá počítačovou kriminalistiku jako trestnou činnost, v které nějakým způsobem figuruje počítač (či více počítačů) a souhrn programového a technického programového vybavení včetně všech dat. Za počítačový zločin se pak považuje takový zločin, který „*je spáchaný za pomocí zpracování dat nebo počítačové sítě nebo přímo s nimi spojený*“. (ČNS ISO/IEC 2382-8). Rak a Porada[79] zase jmenují pojem „*počítačová kriminalita*“, přičemž podle nich tento pojem vznikl již v době prvních a sálových počítačů. Je zřejmé, že v dnešní době má pojem „počítačová“ kriminalita mnohem širší význam a již není chápána pouze ke vztahu k počítači.

---

76 TOTALSERVICE. Digitální stopy: co jsou a jak se jich zbavit? Totalservice.cz [online]. 18.2.2022 [cit. 2024-01-23]. Dostupné z WWW: https://www.totalservice.cz/novinky/digitalni-stopy-co-jsou-a-jak-se-jich-zbavit-2022-02-18

77 ETECHBLOG. Zmenšete svou digitální stopu pomocí těchto 6 nástrojů [online]. 27.9.2022 [cit. 2024-03-09]. Dostupné z WWW: https://etechblog.cz/zmensete-svou-digitalni-stopu-pomoci-techto-6-nastroju/

78 SMEJKAL, V. *Kybernetická kriminalita.* 3 vydání. Plzeň Aleš Čeněk, 2022. ISBN 978-80-7380-849-5

79 RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

Z právního a kriminalistického hlediska digitální stopa celou řadu vlastností a individuálních charakteristik- Z pohledu trestního řízení mají tyto vlastnosti jak pozitivní, tak i negativní aspekty. Podle Raka a Porady[80] mezi ně patří:

- nehmotnost: digitální stopa nemá hmatatelnou podobu a aby ji bylo možné uložit, je třeba, aby měla hmotné prostředí. Médium, na kterém je uchována digitální stopa, se považuje za věcný důkaz. Média však mají vysokou variabilitu a je potřeba nalézt vhodné zařízení, které bude schopné toto médium přečíst.
- časová trasovatelnost: velké množství digitální stopy prokazatelně disponuje spojením s velmi přesným časovým údajem. Problém však může nastat, pokud je uživatel zkušený a jakýmkoliv způsobem získá administrátorská oprávnění, a tak dokáže pozměnit systémový čas.
- latentnost: bez technologií je digitální stopa pro lidské smysly nezaznamenatelná. Toho lze využít v situacích, kdy uživatel (podezřelý) zanechává digitální stopy bez uvědomění.
- vysoká obsažnost: digitální stopa disponuje vysokou informační hodnotou; informace jsou většinou multimediálního charakteru. Jako pozitivum lze v tomto případě vidět fakt, že máme k dispozici velké množství informací potřebných ke kriminalistickým šetřením. Na druhou stranu však tento fakt může mít úplně opačný účinek – příliš mnoho informací nás může zahltit a relevantní informace mohou být přehlédnuty.
- velmi nízká životnost: komunikační systémy a záznamy mohou být přepsané jinými nebo smazány. K tomu může dojít jak na základě samotné vlastnosti ICT technologie anebo i pachatelem samotným.
- uchování a kvalitu ovlivňuje celá řada subjektivních faktorů: mezi tyto faktory patří omezení v podobě legislativních či interních předpisů, institucionální kultura úrovně informační bezpečnosti apod.

---

80 RAK, R., PORADA, V.. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, ročník 16. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf

- velký objem dat – jak je již uvedeno výše – paměťová média pojmou vysoké množství informací, které mohou sloužit jako důkazní materiál. Negativní stránkou věci může být vysoký nárok na čas pro zpracování všech dat a také přehlcenost informacemi, které může vést k informačnímu přesycení a přehlédnutí důležitých důkazů.
- datová hustota v čase a s rozvojem nových technologií neustále klesá: digitální stopy se stále hůře nalézají. Důvodem je ukládání stále většího množství dat, což se děje také v důsledku rozvoje velkokapacitních datových médií a intenzivního využívání výpočetní techniky.
- extrémní dynamičnost prostředí – provoz klíčových informačních systému v jakémkoliv podniku nelze jen tak přerušit – tím by majiteli mohly vzniknout značné ekonomické ztráty. Za plného provozu však některé digitální stopy nelze nalézt a také zde hrozí riziko, že stopy budou důsledkem provozu informačních systémů znehodnoceny nebo dokonce zničeny.
- komplexnost a heterogennost prostředí –zpracování informací probíhá běžně skrze integrované celky, které jsou tvořeny právě heterogenními systémy – to přináší výhodu v tom, že potřebný důkazní materiál lze nalézt v každé části složitého komplexu, ačkoliv v jiné části chybí nebo byl zničen. Nicméně hledat digitální stopy v takto komplexních systémech je časově velmi náročné a vyžaduje velké množství vysoce kvalifikovaných specialistů.
- velký geografický rozsah prostoru: z pohledu geografického prostředí výpočetní technika nezná hranic. Kyber-útoky mohou být prováděny přes několik serverů v různých cizích zemích. Velkou nevýhodou této vlastnosti je komplikace v rozdílné legislativě v různých zemích a také v rozdílných způsobech a postupech vyšetřování a zajišťování digitálních stop.
- vysoký stupeň ochrany některých činí práci s některými digitálními stopami nesnadnou a někdy i nemožnou. Data mohou být zakódována, zašifrována a v této formě neposkytují vyšetřování žádné použitelné informace. Dekódovat data je často nemožné, popřípadě časově velmi náročné.
- Kvalifikovaní pachatelé dokáží mistrně zahladit digitální stopy. Tito pachatelé, tedy lidé s vysokou odborností v ICT mají také předpoklad způsobit největší škody. V detailně promyšleném, kvalifikovaným pachatelem spáchaném

digitálním trestném činu, bude velice obtížné a komplikované nalézt a zajistit digitální stopy.

- některé digitální stopy jsou restaurovatelné: některé zničené údaje je možné restaurovat, např. „z košů“, datových nosičů, archivních médií apod. U jiných druhů kriminálních stop tuto vlastnost nenajdeme.
- Originálnost digitálních stop – u digitálních stop lze často snadno vytvářet duplikáty, aniž by se změnila kvalita obsahu či došlo ke změně vlastností stop. Tato vlastnost je výhodná v tom, že lze původní data zachovat nezměněna i v případě poškození originálního nosiče. I to s sebou ale nese negativní výzvu – může docházet k podvrhům a padělkům se změněným obsahem, přičemž originalita datového nosiče se v soudním procesu velmi těžko dokazuje.

Jedním ze zdrojů vytváření digitální stopy jsou cookies. Ty budou nyní speciální zmíněné, ačkoliv představují pouze jeden ze způsobů, jak vzniká digitální stopa. Důvodem je, že cookies se staly v roce předmětem novely zákona v roce 2022. Na cookies může být nahlížen ně ze dvou pohledů. Prvním z nich je pohled ze strany poskytovatele elektronických služeb a druhým z nich je pohled ze strany pohledu ochrany osobních údajů. Oba tyto pohledu jsou ovlivněné jak naší legislativou, tak legislativou EU. Cookies jsou z pohledu českého práva definovány jako "*jakákoli informace týkající se určeného či určitelného subjektu údajů, tj. lze-li takový subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*". Z pohledu českého práva se neoznačují cookies ani jiné technické identifikátory za osobní údaje. Za osobní údaje by cookies byly považované za osobní údaje pouze tehdy, pokud by správce osobních údajů (provozovatel webu) byl schopný na základě údajů, které má k dispozici identifikovat konkrétní osobu.[81]

V souvislosti s cookies a legislativou je třeba zmínit novelu cookies zákona s účinností k 1.1.2022. Podle této novely zákona o elektronických komunikacích došlo k podstatným změnám pravidel, která jsou pro české provozovatele webových stránek závazná při práci s cookies. Hlavní změnou, kterou novela přinesla je, že je nutné změnit

81 SDRUŽENÍ PRO INTERNETOVOU REKLAMU. Cookies v České republice [online]. 2022 [cit. 2024-01-21]. Dostupné z WWW: https://www.thmu.cz/data/cookies.pdf

případný nevyhovující způsob shromažďování souborů cookies. Novela se týká každého provozovatele webu nebo mobilní aplikace.[82] IP adresa je oproti tomu považována za osobní údaj, a to nejen v ČR, ale také ve většině členských států EU.[83]

82 SCHEJBAL, M. Novela cookies zákona: od 1.1.2022 došlo k velkým změnám při ukládání cookies. In Kropáček Legal [online]. 7.4.2022 [cit. 2024-01-24]. Dostupné z WWW: https://www.pravopropodnikatele.cz/novela-cookies-zakon

83 SDRUŽENÍ PRO INTERNETOVOU REKLAMU. Cookies v České republice [online]. 2022 [cit. 2024-01-21]. Dostupné z WWW: https://www.thmu.cz/data/cookies.pdf

6 Praktická část: Vlastní digitální stopa autora

6.1 Jak zjistit svou digitální stopu?

Asi nejjednodušším způsobem, jak zjistit, co o člověku internet ví, je zadat si své jméno do Google vyhledávače. Každý z nás to určitě minimálně jednou v životě udělal. Myslíme si, že toho internet o nás moc neví, protože na první stránce vyhledávání se téměř neobjevujeme? Nenechme se mýlit, nejsme neviditelní. Jen se na prvních místech ve vyhledávání objevují více aktivní profily či hledanější jmenovci. Naší digitální stopu však lze zjistit i skrze jakékoliv další osobní informace, od vyhledávání podle data narození, bydliště, fotka apod.

Dalším způsobem, jak zjistit něco o své digitální stopě, je export dat z Googlu účtu přes takeout.google.com, kde nalezneme všechna data, která o nás Google má. Také na Google Dashboard (myaccount.google.com/dashboard) nalezneme veškeré služby, které skrz Google využíváme (Youtube, Gmail, Drive, Google Play, Keep Notes, Kontakty, Payments, Maps aj. Klik nutím na jednotlivou službu (Download) si můžeme informace z této dané služby stáhnout. Většina lidí používá svůj mobilní telefon právě přes Google Account. Asi není potřeba detailněji rozepisovat, kolik toho o nás může Google vědět.

Kde všude jsme na internetu zmíněni můžeme zjistit přes index Google upozornění (google.com/alerts). Historii napříč Googlem zjistíme přes myactivity.google.com, kde můžeme také spravovat, u čeho chceme historii zaznamenávat. Pokud má někdo odkliknuto „ON“, tedy zapnuto, u všech nabízených možností, Google zaznamenává a uchovává veškerou historii (webovou aktivitu, aplikace, poloha apod.).

Pokud chceme zjistit, jaké informace o nás nashromáždil Facebook, můžeme to zjistit pomocí stáhnutí svého profilu díky Facebook information Download (složka Nastavení – Obecné nastavení – Stáhnout kopii mých dat – spustit archivaci).

6.2 Chování autora v digitálním prostředí

Autor této práce si je velice dobře vědom skrytých nebezpečí číhajících za zdánlivě nevinným brouzdáním po vlnách internetu. Je třeba vyzdvihnout fakt, že se na internetu chová velice opatrně a vědomě. Co se týče sociálních sítí, využívá je, co nejpasivněji to jde. Používá pouze Facebook a Instagram. Místo reálného jména používá alias, nevyplňuje datum svého narození ani žádné jiné osobní informace, nevkládá žádné osobní fotografie. Facebook pravděpodobně zná jeho domácí polohu a autorovi se tento fakt nikdy nepodařil změnit. Google nemá povolení zaznamenávat jeho polohu; tato funkce je vypnuta. Dále pak využívá ochranu VPN a také antitrack – ten mu pomáhá v tom, že neustále mění jeho digitální stopu. Díky antitracku jsou automaticky odmítány cookies, které jsou jím následně i pozměněny. Antitrack také pravidelně pozměňuje a maže historii prohlížení. Mezi aktivně a každodenně využívané platformy patří YouTube a YouTube music a aplikace Discord – komunikační platforma, alternativa TeamSpeaku, Skype apod. Autor je také aktivním hráčem videoher, kdy i na těchto platformách (Steam, Battlenet) se chová velmi opatrně – nikdy nezadává své pravé jméno ani bydliště. Veškeré transakce platí jednorázovou – virtuální platební kartou, čímž snižuje svou digitální stopu a riziko zneužití pravé platební karty.

6.3 Popis a způsob stažení vlastní digitální stopy

V rámci této práce se autor rozhodl si stáhnout svou digitální stopu, kterou zanechal užíváním služeb společností Google, Instagram a Facebook. Každá z těchto společností uchovává trochu jiná data o svých uživatelích, kdy tyto zjištěné informace užívají dále dle svých individuálních potřeb. Ať už se jedná o cílené reklamy, nabízení dalších placených služeb, hudebních koncertů poblíž bydliště uživatele apod.

Záloha dat z Google je uživatelsky poměrně jednoduchá. Nejprve si autor přes svůj internetový prohlížeč vyhledal www.google.com. Následně za využití svých přihlašovacích údajů přihlásil do svého google účtu. Poté již stačilo kliknout na svůj profilový obrázek, vybrat „Účet“, čímž se autor dostal do nastavení. V nastavení účtu si vyhledal „Data a ochrana soukromí“. Zde se i autor mohl prohlédnout veškeré nastavení týkající se kontroly ochrany soukromí. Jak je uvedeno výše, tak autor si moc dobře uvědomuje nebezpečí týkající se digitální stopy a veškeré nastavení týkající se uchovávání polohy, historie vyhledávání, dat sdílených s dalšími uživateli, aktivitu na

webu a aplikacích a dále i personalizované reklamy mý vypnuté. Autor si dále vybral kolonku „Stažení nebo smazání dat“. Následně byl autor odkázán na web https://takeout.google.com/?hl=cs. Zde si autor mohl vybrat stáhnutí až 53 položek s informacemi, které jsou o uživateli uchovávány. Autor si vybral všechny položky. Autorovi po několika dnech přišel e-mail s upozorněním o dokončeném zálohování těchto souborů.

K zajištění dat ze sociální sítě Instagram autor postupoval dle Centra nápovědy. Vše proběhlo za užití internetového prohlížeče na PC. Autor zadal své přihlašovací údaje k účtu, přihlásil se a vyhledal nastavení. Následně se přes Centrum účtů dostal na Vaše informace a oprávnění. Vybral si svůj aktivní Instagram profil. Následně klikl na Stažení vašich informací, poté Stáhnout nebo přenést informace. Opět vybral vlastní aktivní profil. Následně vybral stažení všech dat do vlastního zařízení – PC. Stažení všech informací může dle Instagramu trvat až 30 dní. Stažení informací autora proběhlo v rámci několika dní, kdy na autorův e-mail přišel s odkazem ke stažení vyžádaných dat.

Následovalo zajištění dat ze sociální sítě Facebook. Tam si autor rozklikl svůj profil, nastavení, nastavení a soukromí a následně vybral položku „Stažení vašich informací“. Autor měl možnost vybrat si stažení dat z účtu na Facebooku nebo na Instagramu. Autor si zvolil možnost stáhnout si informace z aktivního účtu na Facebooku a zvolil „dostupné informace“, stáhnout do zařízení a data za celou dobu aktivity na Facebooku. Stažení všech informací může trvat až 4 dny. Za 2 dny přišel autorovi e-mail s upozorněním, že požadovaná data jsou již k dispozici.

6.4 Zjištěná data a jejich analýza

Autor zajištěním dat z účtu u společnosti Google, a jejich analýzou o sobě zjistil, že Google, dle nastavení autora, nemá přístup k jeho časové ose a poloze (autor toto vypl dle informací dne 01.07.2023). Dále měl autor zapnuté automatické mazání informací o jeho poloze, a to každé 3 měsíce. Google o autorovi shromažďuje informace z jeho oblasti zájmů, historie vyhledávání, jméno, příjmení, pohlaví, telefonní číslo a ovládané

jazyky[84]. Autor měl vypnutá i další nastavení, včetně personalizované reklamy a evidování aktivity na webu a aplikacích. U těchto nastavení nejde nastavit automatické mazání, protože tuto aktivitu Google u autora vůbec neeviduje. Autor se o sobě dále dozvěděl pouze jeho historii vyhledávání a to na Youtube, kdy tyto informace nebyly aktuální. Poslední relevantní informace byla ze dne 03.12.2023, poté následovaly informace až z března roku 2021. Více relevantních informací se o sobě autor nedozvěděl. Vzhledem k tomu, že autor využívá služeb i dalších společností a to prostřednictvím svého Google účtu, se rozhodl využít služeb aplikace *Saymineapp*[85]. Jedná se o aplikaci, která z informací poskytnutých žadatelem – Jméno, příjmení, e-mailové adresy a národnosti, sestaví digitální stopu žadatele a zjistí společnosti, které disponující informacemi o jeho digitální stopě. Autor se dozvěděl, že za jeho působení v digitálním prostředí o něm uchovává informace nejméně 72 společností. Jedná se o společnosti u kterých někdy autor nakupoval, využíval jejich služeb nebo se u nich jen prostě registroval. Dále u těchto společností bylo evidováno nejméně 12 firem, které měly k dispozici i finanční údaje, např. o jeho debetní kartě, případně informace zda je bonitní.

Zajištěním a vyhodnocením dat ze sociální sítě Instagram[86] se o sobě autor dozvěděl jeho falešné alias. Dále případné vložené komentáře /autor nic nekomentoval, sociální sítě využívá pasivně/, jeho aktivitu – oblíbené příspěvky, sledované profily a profily sledujících jeho profil, reklamy které shlédnul, reakce na komentáře apod. Autor na tuto síť nevkládá žádné osobní údaje ani fotografie. Síť využívá pouze ke sledování krátkých videí a sledování oblíbených osob a tvůrců obsahu. Instagram o autorovi neuchovává žádné relevantní skutečnosti.

Dále autor vyhodnotil zajištěná data ze sociální sítě Facebook[87]. Na Facebooku jsou informace poskytnuté autorem – falešná profilová fotografie, alias /falešné příjmení a pozměněné křestní jméno/. Autor má na profilu několik hromadných fotografií, kdy veškeré nastavení soukromí je nastavené na "pouze přátelé" a "nikdo". Facebook u autora vede jeho primární polohu – jedná se o domácí město autora. Tuto informaci se již

---

[84]Dostupné online z https://myaccount.google.com/data-and-privacy?hl=cs&utm_source=google&utm_medium=pref-page#things-you-do [citováno 2024-04-04].

[85] Dostupné online z https://saymineapp.com/overview [citováno 2024-04-04].

[86] Dostupné online z https://www.instagram.com/ [citováno 2024-04-04]

[87]Dostupné online z https://www.facebook.com/privacy/center/?entry_point=facebook_bookmarks

autorovi nepodařilo změnit. Dále zjistil, že Facebook využívá jeho známou polohu k nabízení služeb v okolí – autor se zajímal o nové auto, kdy Facebook mu nabídl blízký autobazar. Tyto informace lze dohledat na Facebooku v nastavení soukromí – "jak jsme použili vaši polohu". U těchto informací dále Facebook píše, že když v nastavení zařízení zapnete "Polohové služby", může společnost Meta (Facebook a další spol.), mít přístup k vaší GPS poloze, bluetooth, Wi-Fi připojení a dalším informacím o přesné poloze. Autor dále zjistil, že Facebook eviduje veškerou jeho aktivitu a to včetně zaznamenávání „chatu" s dalšími uživateli, "lajkování" příspěvků, komentářů, sdílení, vyhledávání profilů dalších uživatelů, aktivity na Marketplace a další.

6.5 Rizika zjištěná analýzou vlastních dat

Autor vyhodnocením vlastní digitální stopy zjistil, že i přes to, že se považuje za velmi opatrného uživatele internetu, sociálních sítí a celkově i za relativně zběhlého v digitálním prostoru zjistil, že i on je jako většina populace ohrožen a vystaven riziku vyvstávajícího z používání výše uvedeného. Existují desítky, ne-li stovky společností evidující o autorovi jeho osobní údaje, včetně adresy, telefonního čísla, data narození a dalších údajů. Každá z těchto společností je i potencionální obětí kyberkriminality, kdy může dojít k odcizení údajů jejich uživatelů. Tyto údaje mohou následně být využity k páchání dalšího protiprávního jednání. Může se jednat o krádež identity, zneužití platební karty, založení účtů u bankovních i nebankovních společností a podobné. Autor dále zjistil, že i přes to, že se na internetu aktivně chrání tím, že nesděluje pravé osobní údaje a využívá aktivní ochranu VPN, antitrack apod, tak některé společnosti i přes to evidují jeho pravděpodobnou polohu, ať už na základě nákupů, recenzí nebo okruhu přátel. Tyto informace následně mohou být a jsou využívány, ať už pro reklamní účely nebo prodejem těchto informací dalším společnostem.

Závěr

Tahle práce měla za cíl prozkoumat a analyzovat druhy digitálních stop v online prostředí. Zhodnotit dopady digitální stopy na soukromí a bezpečnost uživatelů a zároveň navrhnout doporučení pro ochranu osobní digitální stopy a zlepšit povědomí o této problematice.

Každý uživatel, byť opatrný, za sebou nechává digitální stopu. Je na vlastním uvážení každého, jak velkou digitální stopu za sebou zanechá a kolik toho o sobě v digitálním prostředí prozradí. I přes veškerou snahu se v dnešní době nelze zcela vyhnout určitému druhu sledování, pokud člověk chce zůstat aktivním uživatelem internetu a všeho co nabízí . Tato práce ve své teoretické části navrhuje možné způsoby jak se lze před sledováním osobní digitální stopy chránit. Dále práce ukazuje jakou digitální stopu za sebou průměrný uživatel nechává a s tím i další data jako jsou osobní údaje, věk, pohlaví, bydliště, zdravotní stav, zájmy, finanční situaci a další. Většina lidí by v soukromém životě tyto údaje sdělovala jen blízkým osobám, ale mnohdy jsou tato data o osobách dostupné na internetu pro kohokoli.

Autor se věnoval digitální stopě i z kriminalistického hlediska. Je zřejmé jak obtížné je v dnešní době odhalovat pachatele kyberkriminality, kteří jsou mnohdy profesionálové a používají pokročilé technologie a hardware. Kyberkriminalita je velmi složitá a náročná na vědomosti odborníků, ale i na technologie. Zároveň je velmi nebezpečná tím, že tuto protiprávní činnost může páchat kdokoliv a odkudkoliv na světě.

Závěrem zbývá jen uvést, aby každý vedl v opatrnosti svůj online život. Žijeme v digitálním věku a vše co dnes uděláme bude o nás dohledatelné i za několik desítek let. Toto bude platit i o našich dětech, kterým je kolikrát vytvářena digitální stopa již dnem jejich narození, kdy se šťastní rodičové nezřídka pochlubí fotografií novorozeněte na sociální síti. Z jedné fotografie velmi často víme jméno, příjmení, datum a místo narození osoby. Neopatrní uživatelé následně mohou celé roky vkládat na sociální sítě fotografie dítěte a tím pro digitální prostředí evidovat téměř celý jeho život. Stejně jako se staráme o soukromí v osobním životě, starejme se i o naše soukromí v prostředí digitálním.

Seznam použitých zdrojů

Literární zdroje

1. BURR C., and N. CRISTIANINI. 2019. "Can Machines Read Our Minds?" Minds & Machines 29(3): 461–494.
2. BEMMAMI, K-E, GRAZA, L.a COURTIN C.. From digital traces to competences. 2022. IFAC PapersOnLine 55-10 (2022) 1944–1949
3. CASEY, Eoghan. Handbook of digital forensics and investigation. Boston: Academic, c2010. ISBN 978-0-12-374267-4.
4. ČSN ISO/IEC 2382-8 (369001). Informační technologie – Slovník. Část 8: Bezpečnost.
5. CHENG F. CH, WANG, Y.S. The Do Not Track Mechanism For Digital Footprint Privacy Protection In Marketing Applications. 2018. Journal of Business Economics and Management. Volume 19, Issue 2: 253-267. ISSN 1611-1699 / eISSN 2029-4433
6. KONRÁD, Zdeněk et al. Kriminalistika: teorie, metodologie a metody kriminalistické techniky. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014. 318 s. ISBN 978-80-7380-535-7, str. 53
7. METEŇKO, J. a kol. *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*. 1. vyd. Bratislava 2004, Katedra kriminalistiky a forenzných disciplín, Akadémia PZ v Bratislave. s. 356., ISBN: 80-8054-336-4
8. METEŇKO, J., METEŇKO, M., HEJDA J., *Digital trace*. 7th INTERNATIONAL SYMPOSIUM ON FORENSIC SCIENCES Sep 29th - Oct 1st, 2005, Častá - Slovak republic. KEU PZ PPZ. Bratislava 2005. (s.182) ISBN 80-969363-2-8. EAN 9788096936325. s. 55-79.
9. PETERS, U. *Reclaiming Control: Extended Mindreading and the Tracking of Digital Footprint*s. 2022. DOI: 0.1080/02691728.2021.2020366
10. PORADA, V. a kol. Kriminalistika. Brno: Akademické nakladatelství CERM, 2001. 737 s.

11. RAK R., JANÍČEK P. Identification in criminalistic and security practice supported by computer technology, Expertise n. *3/2000*, volume V, p. 30-38, 2000.

12. RAK, R. a PORADA, V. . Praha [i.e. Karlovy Vary]: Vysoká škola Karlovy Vary, 2013. ISBN 978-80-87236-16-1

13. RAK, R., PORADA, V. Digital trace, *Booklet from scientific conference "Advances in criminalistics",* Police Academy, Prague, 2004.

14. RICCI, F., ROKACH, L., SHAPIRA, B., a KANTOR, P. B. *Recommender Systems Handbook.* Berlin: Springer, 2011.

15. RUST, J., KOSINSKI, M., STILLWELL, D. *Moderní psychometrie. Věda o psychologickém hodnocení.* Londýn: Routledge, 2021

16. SMEJKAL, V. *Kybernetická kriminalita.* 3 vydání. Plzeň Aleš Čeněk, 2022. ISBN 978-80-7380-849-5

17. TRIVEDI, A., VASISHT, D. Digital Contact Tracing: Technologies, Shortcomings, and the Path Forward. 2020. DOI: 10.1145/3431832.3431841

18. YOUYOU, W., M. KOSINSKI, and D. STILLWELL 2015. "Computer-based Personality Judgments are More Accurate than Those Made by Humans." Proceedings of the National Academy of Sciences of the United States of America, 112(4): 1036–1040.

19. ZANKER, M., L. ROOK, a D. JANNACH. 2019. "Measuring the Impact of Online Personalisation: Past, Present and Future." International Journal of Human-Computer Studies 131: 160–168.

20. ZANDL, P. *Mýty a naděje digitálního světa*. Vyd. 1. Brno: Jan Melvil Publishing, 2022. ISBN 978-80-7555-175-7.

Elektronické zdroje

1. BEČVÁŘ, O. Digitální stopa a její rizika [online]. 2022 [cit. 2024-01-23]. Dostupné z WWW: <https://www.ak-becvar.cz/digitalni-stopa-a-jeji-rizika/>
2. COCQOVÁ, C. Digital Footprints and Narrative Traceability/Narrative Footprints and Digital Traceability [online]. Helsinki: 2021 [cit. 2024-01-22]. eSSN 2659-6881. Dostupné z WWW: <https://dra.revistas.csic.es/index.php/dra/article/view/881/1022>
3. ČÁP J, a kol. POLICEJNÍ AKADEMIE ČR V PRAZE. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. Bezpečnostní teorie a praxe 1/2022 [online]. [cit. 2024-01-22]. Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf
4. ČERNÝ, M. Digitální stopa a digitální identita. In *Metodický portál RVP.CZ* [online]. 26.8.2011 [cit. 2024-03-11]. Dostupné z WWW: https://clanky.rvp.cz/clanek/c/o/12943/DIGITALNI-STOPY-A-DIGITALNI-IDENTITA.html
5. Digital Evidence: Standards and Principles. Report of Scientific Working Group on Digital Evidence (SWGDE) and International Organization on Digital Evidence (IOCE) [online]. Říjen 1999 [cit. 2024-02-25]. Dostupné z WWW: https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm
6. ETECHBLOG. Zmenšete svou digitální stopu pomocí těchto 6 nástrojů [online]. 27.9.2022 [cit. 2024-03-09]. Dostupné z WWW: https://etechblog.cz/zmensete-svou-digitalni-stopu-pomoci-techto-6-nastroju/
7. GIVENS, CH. Digitální stopa zařízení a sledování na internetu. In *Avast* [online]. 2.10.2019 [cit. 2024-01-24]. Dostupné z WWW: https://blog.avast.com/cs/fingerprinting-and-the-surveillance-economy
8. INTERNETEM BEZPEČNĚ. Digitální stopa. Internetem bezpecne.cz [online]. 2024 [cit. 2024-01-24]. Dostupné z WWW:

https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

9. KAMO. Kamo zastaví online sledování a ochrání vaše soukromí. Ccleaner.cz [online]. © 2005-2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.ccleaner.com/cs-cz/kamo

10. KASPERSKI. *What is a digital footprint? And how to protect it from hackers* [online]. © 2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

11. LAMBIOTTE, R., KOSINSKI, M. Tracking the Digital Footprints of Personality [online]. 2014, Volume 102, Issue 12 [cit. 2024-01-22]. Dostupné z WWW: https://ieeexplore.ieee.org/document/6939627

12. LIEM, C., PETROPOULOS, G. The economic value of personal data for online platforms, firms and consumers . In *Bruegel* [online]. 14.1. 2016 [cit. 2024-03-12]. Dostupné z WWW: https://www.bruegel.org/blog-post/economic-value-personal-data-online-platforms-firms-and-consumers#:~:text=The%20generated%20value%20from%20personal,they%20use%20for%20attracting%20advertisers.

13. MARČÍKOVÁ, V. Cookies lišta v roce 2022: Jak si s novelou zákona o elektronické komunikaci poradily velké české weby. In *Aira* [online]. © 2022 [cit. 2024-01-24]. Dostupné z WWW: https://blog.aira.cz/cookies-lista-v-roce-2022-jak-si-s-novelou-zakona-o-elektronicke-komunikaci-poradily-velke-ceske

14. MORGAN STANLEY. Strategies to Help Protect Your Digital Footprint [online]. 9.10.2023. [cit. 2024-01-23]. Dostupné z WWW: https://www.morganstanley.com/articles/digital-footprint-protection-strategies

15. RAK, R., PORADA, V.. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, ročník 16. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf

16. RAK, R., PORADA, V. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2006, ročník 17. [cit. 2024-01-22]. Dostupné z WWW: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf

17. REPKOVÁ, I. M. Nesmazatelná digitální stopa anebo Google nezapomíná. In Stisk online [online]. 17.10.2021 [cit. 2024-03-12]. Dostupné z WWW: https://stisk.online/a/SSxhd/nesmazatelna-digitalni-stopa-aneb-google-nezapomina

18. Risk Analysis Consultants. Digitální forenzní analýza [online]. 2021 [cit. 2024-03-12]. Dostupné z WWW: https://www.rac.cz/cs/digitalni-forenzni-institut/digitalni-forenzni-analyza/

19. SDRUŽENÍ PRO INTERNETOVOU REKLAMU. Cookies v České republice [online]. 2022 [cit. 2024-01-21]. Dostupné z WWW: https://www.thmu.cz/data/cookies.pdf

20. SCHEJBAL, M. Novela cookies zákona: od 1.1.2022 došlo k velkým změnám při ukládání cookies. In Kropáček Legal [online]. 7.4.2022 [cit. 2024-01-24]. Dostupné z WWW: https://www.pravopropodnikatele.cz/novela-cookies-zakon

21. SHEWALE, R. Google Ads & PPC Statistics 2024 (Revenue & ROI). In Demandsage [online]. 18.2.2024 [cit. 2024-01-24]. Dostupné z WWW: https://www.demandsage.com/google-ads-statistics

22. TOTALSERVICE. Digitální stopy: co jsou a jak se jich zbavit? Totalservice.cz [online]. 18.2.2022 [cit. 2024-01-23]. Dostupné z WWW: https://www.totalservice.cz/novinky/digitalni-stopy-co-jsou-a-jak-se-jich-zbavit-2022-02-18

23. Whitcomb, C., M. International. An Historical Perspective of Digital Evidence: A Forensic Scientist's View. *International Journal of Digital Evidence* [online]. Spring 2002, Volume 1, Issue 1 [cit. 2024-02-20].Dostupné z WWW: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf

24. https://myaccount.google.com/data-and-privacy?hl=cs&utm_source=google&utm_medium=pref-page#things-you-do [cit. 2024-04-04].

25. https://saymineapp.com/overview [cit. 2024-04-04].

26. https://www.facebook.com/privacy/center/?entry_point=facebook_bookmarks [cit. 2024-04-04]

27. Cookies třetích stran končí: Proč je váš e-shop potřebuje? cz [online]. 2024 [cit. 2024-04-05]. Dostupné z https://www.advisio.cz/blog/co-jsou-cookies-tretich-stran-a-jak-jejich-konec-ovlivni-e-shopy/

Seznam zkratek

Access Points = AP

AI = umělá inteligence

Seznam tabulek a grafů

Seznam příloh

Přílohy