plk. v. v. Mgr. Jan Čáp, Ph.D.
Policejní akademie České republiky v Praze
Fakulta bezpečnostně právní
Katedra kriminalistiky
plk. Ing. Bc. Lukáš Breu, pplk. Mgr. Zdeněk Prošek
Policie ČR, Národní centrála proti organizovanému zločinu SKPV

Zajišťování, zpřístupňování a vyhodnocování digitálních stop

Úvod

Problematika zajišťování, zpřístupňování a vyhodnocování digitálních stop v posledních letech neustále nabývá na významu. Stále více a více činností a dokumentů se přesouvá do digitálního prostředí, což se logicky odráží i při plnění úkolů policejních orgánů v trestním řízení, které musí na tento trend reagovat a umět s ním pracovat tak, aby bylo možné v tomto prostředí zajišťovat procesně způsobilé důkazy.

Národní centrála proti organizovanému zločinu služby kriminální policie a vyšetřování Policie ČR (dále jen „NCOZ SKPV“) se vzhledem ke své působnosti potkává s problematikou digitálních stop v jejich nejrůznějších podobách poměrně často, a proto zde došlo ke stanovení postupu, jak provádět zajišťování, zpřístupňování a vyhodnocování těchto stop. Postup byl konzultován a následně připomínkován Vrchním státním zastupitelstvím v Praze a Olomouci a Kriminalistický ústavem Policie ČR, a nyní ho předkládáme odborné praxi k případnému využití.

Ředitel NCOZ SKPV rozhodl o zřízení pracovní skupiny, do které byli přizváni zástupci zmíněných Vrchních státních zastupitelství, Kriminalistického ústavu Policie ČR a odborníci z policejní praxe v celém rozsahu dokumentační praxe útvaru (operativec, analytik, IT specialista, specialisté vyšetřující kybernetickou kriminalitu) a legislativní pracovník. Na základě dosavadní policejní a justiční praxe, společných jednání a několika kol připomínkového řízení byl v rámci NCOZ SKPV vytvořen interní akt řízení obsahující metodický postup, dle kterého příslušníci útvaru postupují. V současné době projevil zájem o tento postup i další bezpečnostní sbor a to Celní správa ČR.

Předložený text je zároveň zahrnut jako výstup dílčího výzkumného úkolu realizovaného na Policejní akademii České republiky v Praze pod č. I/3 Aktuální problémy kriminalistické taktiky a metodiky,[1] plněného v rámci Rozvojového programu Policejní akademie České republiky v Praze, jako výzkumné organizace na léta 2017-2023.

Z metodologického hlediska je pro čtenáře na místě uvést, že v rámci výzkumné činnosti bylo především použito **Historické metody**, kdy byla analyzována minulost

[1] *Policejní akademie ČR: Vědeckovýzkumná činnost Policejní akademie ČR v Praze v letech 2017-2023* [online]. Praha: PA ČR, 2021 [cit. 2021-9-8]. Dostupné z: https://www.polac.cz/g2/view.php?o_skole/veda/vvc_17.html

zkoumaného problému, v konkrétních trestních spisech a rozhodnutích ve věci, v letech 2008-2020.

Jako **výzkumné techniky** bylo použito analýzy dokumentů, aplikačních postupů a expertizy založené na řízené diskuzi renomovaných (kompetentních odborníků) – techniky Round table.

Zajišťování digitálních stop

Pro účely vypracování postupu policistů NCOZ SKPV při zajišťování, zpřístupňování a vyhodnocování digitálních stop byl samotný pojem „digitální stopa“ definován tak, že se jedná o

a) 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“) nebo
b) hmotný nosič digitální informace.

Vedle toho je na místě teoreticky vymezit termín počítačové kriminality, kdy se nabízí pojem jednoho ze současných teoretiků této oblasti a to profesora Vladimíra Smejkala,[2] kdy tento druh kriminality vnímá jako páchání trestné činnosti, v níž figuruje určitým způsobem 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 této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité,
b) nebo jako nástroj trestné činnosti,[3]

zároveň je i vymezení české technické normy, kde se můžeme dočíst, že „*počítačový zločin je zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený“.*[4]

Z trestně procesního pohledu je na úvod potřebné říci, že o zajištění digitálních stop rozhoduje hlavní zpracovatel trestního spisu, přičemž digitální stopy se získávají pomocí zajišťovacích institutů podle trestního řádu. Jedná se především o předložení nebo vydání věci podle § 78 trestního řádu, odnětí věci podle § 79 trestního řádu, a to i v rámci výkonu prohlídek (domovní prohlídka, prohlídka jiných prostor a pozemků, osobní prohlídka podle § 82 a násl. trestního řádu) a ohledání podle § 113 trestního řádu (místa činu, věci). Digitální stopy lze zajistit in natura jako digitální data uložená na hmotné nosiče digitální informace (počítač, notebook, server, USB flashdisk apod.) nebo jako digitální data uložená na hmotný nosič digitální informace Policie ČR např. formou provedení bitové kopie nebo prostým zkopírováním digitálních dat (opatřené kontrolním součtem, pakliže je to v daném případě možné), případně snímáním obrazovky monitoru pomocí software nebo foto či video dokumentací např. při zjišťování obsahu webových stránek, on-line komunikátorů, e-mailových zpráv.

[2] prof. Ing. Vladimír Smejkal, CSc. LL.M.
[3] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi, s. 20-21. ISBN 978-80-7380-501-2.
[4] ČSN ISO/IEC 2382-8 (369001). *Informační technologie – Slovník. Část 8: Bezpečnost.*

Samozřejmě při provádění výše uvedených zajišťovacích úkonů musí být splněny zákonné podmínky průběhu úkonů (např. přítomnost nezúčastněné osoby).

Při vyžadování součinnosti na místě úkonů trestního řízení od znaleckého ústavu Policie ČR je nutno vzít v úvahu, že pracovník tohoto ústavu je oprávněn ke kriminalisticko-technické činnosti v rozsahu svého znaleckého oprávnění (příloha č. 2 písm. k) pokynu policejního prezidenta č. 177/2018, kterým se upravuje věcná, funkční a místní příslušnost znaleckých ústavů Policie České republiky). Současně je nezbytné si uvědomit, že v případě zajištění digitálních dat nebo hmotného nosiče digitální informace či techniky in natura lze ke znaleckému zkoumání zajištěných věcí přibrat znalecký ústav Policie ČR, kde je pracovník, který zajištění prováděl, služebně zařazen; tento konkrétní pracovník však nesmí provádět znalecké zkoumání a je nutné na toto upozornit v opatření o přibrání znaleckého ústavu podle § 110 trestního řádu; analogicky platí u odborného vyjádření podle § 105 trestního řádu.

K vlastnímu obsahu vytvořené sjednocující metodiky postupu, zobrazené v interním aktu řízení:

1. Předmět úpravy a výklad pojmů

Z metodologického a legislativního hlediska bylo při vypracování interního aktu řízení k postupu při zajišťování, zpřístupňování a vyhodnocování digitálních stop přistoupeno v následující struktuře:

1.1. Předmět úpravy

Dokument obsahuje vybraná pravidla a aktuální postupy při zajišťování digitálních dat, následných činnostech se zajištěnými digitálními daty a nakládání s hmotnými nosiči digitální informace pro účely řádného plnění úkolů trestního řízení v podmínkách Národní centrály proti organizovanému zločinu služby kriminální policie a vyšetřování (dále jen „útvar“).

1.2. Výklad pojmů

Pro účely tohoto dokumentu se rozumí

a) digitální stopou[5)]

1. digitální informace nebo jakákoli data přenesená nebo uložená za použití počítačového systému; digitální stopa se zpravidla nachází na magnetickém, optickém nebo polovodičovém médiu nebo v prostředí datových sítí (dále jen „digitální data“),
2. hmotný nosič digitální informace mající souvislost s trestním řízením,

b) zajišťováním digitálních dat

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[6)] a pokud to z technických důvodů není možné, v pořízení multimediálního záznamu zobrazení takových digitálních dat na jiném zařízení; úkon po procesní

[5] Čl. 2 písm. j) pokynu policejního prezidenta č. 100/2018, o kriminalisticko-technické činnosti.
[6] § 77b trestního řádu.

i technické stránce se provede tak, aby v dalším řízení nebyly pochybnosti o správnosti jeho provedení,

c) zpřístupňováním zajištěných digitálních dat

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,

d) vyhodnocováním zajištěných a zpřístupněných digitálních dat

úkon trestního řízení, který není výslovně upravený v trestním řádu a spočívá

1. v analýze digitálních dat, hledání informací relevantních k příslušné trestní věci,
2. v syntéze, přiřazení nalezené informace do kontextu s trestní věcí,

e) vyhodnocenými relevantními digitálními daty

digitální data, která byla v rámci vyhodnocení zajištěných a zpřístupněných digitálních dat označena za relevantní ke konkrétní trestní věci a mohou sloužit pro důkazní účely,

f) zpracovatelem spisu

příslušník Policie České republiky (dále jen „policista“), jemuž byla v rámci útvaru přidělena k vyřízení konkrétní trestní věc (hlavní zpracovatel), nebo policista přidělený v konkrétní trestní věci k provedení dílčích úkonů (vedlejší zpracovatel),

g) kriminalistický IT specialista[7]

policista oprávněný na základě platného osvědčení provádět kriminalisticko-technické úkony při zajišťování výpočetní techniky a digitálních stop,

h) znalec

1. znalecký ústav Policie České republiky (Kriminalistický ústav, odbor kriminalistické techniky a expertiz krajského ředitelství Policie České republiky),[8]
2. znalec (fyzická osoba) a znalecký ústav,[9]

i) zásadami kybernetické bezpečnosti

obecné zásady kybernetické bezpečnosti a zásady kybernetické bezpečnosti stanovené interními akty řízení.[10]

2. Fáze zajišťování digitálních stop

Zajišťování digitálních stop zabezpečuje policista zařazený v organizačním článku útvaru, který vede trestní řízení. O zajišťování digitálních stop rozhoduje zpracovatel spisu, či jím pověřená osoba podílející se na dokumentaci trestní věci.

[7] Čl. 2 písm. c) pokynu policejního prezidenta č. 100/2018.
[8] Čl. 2 písm. a) bod 1 pokynu policejního prezidenta č. 100/2018.
[9] Zákon č. 36/1967 Sb., o znalcích a tlumočnících.
Čl. 52 odst. 3 pokynu policejního prezidenta č. 103/2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení.
[10] Např. pokyn policejního prezidenta č. 235/2014, o využívání datové sítě intranet Ministerstva vnitra Hermes, pokyn policejního prezidenta č. 236/2014, o využívání celosvětové sítě internet.

Digitální stopy se získávají pomocí zajišťovacích institutů podle trestního řádu, především předložením nebo vydáním věci, odnětím věci, a to i v rámci výkonu prohlídek (domovní prohlídky, osobní prohlídky, prohlídky jiných prostor a pozemků)[11] a ohledání (místa činu, věci).[12] Digitální stopy se zajišťují dílem in natura jako digitální data uložená na hmotné nosiče digitální informace či techniku (PC, notebook, server, USB flashdisk apod.) dotčených subjektů (podezřelý, obviněný, svědek apod.) a dílem jako digitální data uložená na technologické hmotné nosiče digitální informace Policie České republiky např. formou provedení bitové kopie nebo prostým zkopírováním digitálních dat (opatřené kontrolním součtem, pakliže je to v daném případě možné), případně snímání obrazovky monitoru pomocí software nebo foto či video dokumentací např. při zajišťování obsahu webových stránek, on-line komunikátorů, e-mailových zpráv. Při výše uvedených zajišťovacích úkonech musí být splněny zákonné podmínky průběhu úkonů, především účast nezúčastněné osoby, obhájce, popř. dalších povinných subjektů.

2.1. Oprávnění v souvislosti s digitálními stopami

Oprávnění v souvislosti s digitálními stopami:

a) policista (bez speciálních znalostí) – pouze zajišťování hmotných nosičů digitální informace in natura, např. USB flashdisk, USB přenosný HDD, PC, notebook, síťové úložiště NAS,
b) kriminalistický technik[13] – kromě oprávnění podle písmene a) dále foto či video dokumentace,
c) kriminalistický IT specialista – oprávnění podle písmene a) a b), dále např. zajišťování digitálních dat ve formě bitových kopií hmotných nosičů digitální informace, obsahu datových úložišť, obsahu webových stránek, sociálních sítí jako např. Facebook, Instagram, YouTube, on-line komunikátorů, virtuálních měn, e-mailových schránek,
d) znalec
    1. metodická pomoc na místě úkonů trestního řízení pro potřeby řádného zajištění digitálních stop výše uvedenými osobami,
    2. znalecké zkoumání digitálních stop zajištěných v trestním řízení[14] (např. dokumentace digitálních dat z techniky zajištěné in natura, obnova smazaných souborů, extrakce e-mailové komunikace).

Při vyžadování součinnosti na místě úkonů trestního řízení od znaleckého ústavu Policie České republiky (Kriminalistický ústav, odbor kriminalistické techniky a expertiz krajského ředitelství Policie České republiky) je nutné vzít v potaz následující možnosti:

a) pracovník znaleckého ústavu Policie České republiky provádí kriminalisticko-technickou činnost

[11] Např. § 78, 79 a 82 trestního řádu.
[12] § 113 trestního řádu.
[13] Čl. 2 písm. b) pokynu policejního prezidenta č. 100/2018.
[14] Např. § 105, 107 a 110 trestního řádu.

1. v žádosti o součinnost je nutné uvést, že je požadována kriminalisticko-technická činnost,
2. pracovník znaleckého ústavu Policie České republiky je oprávněn ke kriminalisticko-technické činnosti v rozsahu znaleckého oprávnění (příloha č. 2 písm. k) pokynu policejního prezidenta č. 177/2018, kterým se upravuje věcná, funkční a místní příslušnost znaleckých ústavů Policie České republiky),
3. v případě zajištění digitálních dat nebo hmotného nosiče digitální informace či techniky in natura lze ke znaleckému zkoumání zajištěných věcí[10)] přibrat znalecký ústav Policie České republiky, kde je pracovník, který zajištění prováděl, služebně zařazen; tento konkrétní pracovník však nesmí provádět znalecké zkoumání a je nutné na toto upozornit v opatření o přibrání znaleckého ústavu podle § 110 trestního řádu; analogicky platí u odborného vyjádření podle § 105 trestního řádu,

b) pracovník znaleckého ústavu Policie České republiky je v místě úkonů trestního řízení v roli znalce
   1. žádost o součinnost doplnit o opatření o přibrání znalce,[10]
   2. v případě zajištění digitálních dat nebo hmotného nosiče digitální informace či techniky in natura je nutné tyto předat ke znaleckému zkoumání tomuto pracovníkovi/pracovišti;[10] pro předání přímo na místě úkonů trestního řízení se použije záznam o předání a převzetí stop.[15]

2.2. Základní možnosti zajišťování digitálních stop

Zajišťování počítačových systémů a komunikační techniky je upraveno interním aktem řízení.[16]

2.2.1. Zajištění hmotného nosiče digitální informace in natura

Zajištění hmotného nosiče digitální informace in natura může provést jakákoli osoba, která je oprávněná zajišťovat věci důležité pro trestní řízení.[2] V případě potřeby konzultuje vhodný způsob zajištění s kriminalistickým technikem, kriminalistickým IT specialistou nebo znalcem. Autenticita digitálních dat uložených na zajištěném originálním hmotném nosiči digitální informace je zajištěna pomocí zapečetěného obalu. Aby nemohlo dojít ke zpochybnění autenticity digitálních dat, může být zapečetěný obal rozpečetěn pouze v rámci procesního úkonu za zákonem stanovených podmínek nebo v rámci znaleckého zkoumání.

2.2.2. Kopie digitálních dat na technologický hmotný nosič digitální informace

V případech, kdy na místě provádění úkonů trestního řízení není možné zajistit digitální stopu včetně originálního hmotného nosiče digitální informace (např. objekty kritické infrastruktury, nemocnice, letiště, ústřední orgány státní správy, dále pak např. obsah webové stránky, on-line komunikátorů) nebo by tento způsob zajištění výrazným

[15] Příloha č. 1 k pokynu policejního prezidenta č. 100/2018.
[16] Pokyn ředitele Kriminalistického ústavu č. 34/2019, k vybraným kriminalisticko-technickým činnostem.

způsobem poškodil jejich majitele, jsou digitální stopy zajišťovány vytvořením jejich kopie na technologický hmotný nosič digitální informace.

Pokud je to možné, je pořízená kopie digitálních dat opatřena kontrolním součtem, pomocí kterého je možné kdykoli ověřit jejich autenticitu. Tento kontrolní součet je nutné zaprotokolovat. Pokud není vytvoření kontrolního součtu z nějakého důvodu možné, je nutné technologický hmotný nosič digitální informace s pořízenou kopií digitálních dat zajistit do zapečetěného obalu a dále se k němu chovat stejným způsobem jako v případě zajištění originálního hmotného nosiče digitální informace in natura.

2.3. Ohledání zajištěné techniky in natura a digitálních dat bez kontrolního součtu za využití § 113 trestního řádu

Ohledání zajištěné techniky in natura a digitálních dat bez kontrolního součtu za využití § 113 trestního řádu:

a) probíhá dodatečně z již zajištěného hmotného nosiče digitální informace in natura (bod 2.2.1) nebo kopie digitálních dat, která z nějakého důvodu nemohla být opatřena kontrolními součty (bod 2.2.2),
b) musí se vždy jednat o procesní úkon za splnění všech zákonných podmínek (vyrozumění o úkonech dotčených osob podle aktuálního procesního postavení a aktuální procesní situace trestní věci),
c) provádí kriminalistický IT specialista podle postupů stanovených Kriminalistickým ústavem[12)] – např. provedení bitové kopie či prosté vykopírování souborů za použití opatření, aby nebyl možný zásah do originálních digitálních dat (např. HW blokátory, práce pod operačním systémem LINUX),
d) cílem je zajištění digitálních dat na technologický hmotný nosič digitální informace včetně opatření kontrolních součtů těchto digitálních dat (např. MD5, SHA1, SHA256 nebo jejich kombinacemi),
e) o provedeném úkonu se sepíše protokol o ohledání (zajištění digitálních dat) s náležitostmi podle § 55 trestního řádu, zejména pak:
    1. datum, čas a místo provádění úkonu ohledání a spisová značka, pod kterou je věc vedena,
    2. pojmenování policejního orgánu provádějícího úkon a předmět úkonu,
    3. informace o osobách, které byly u úkonu přítomny – pracovníci provádějící úkon (kriminalistický IT specialista, zpracovatel spisu), nezúčastněná osoba, další přítomné osoby,
    4. informace o vyrozumění dotčených osob o prováděném úkonu a jejich přítomnosti u prováděného úkonu (obhajoba, obviněný apod.),
    5. soupis zajištěných věcí (techniky, z níž jsou digitální data zajišťována) z předchozích úkonů trestního řízení (např. domovní prohlídka, prohlídka jiných prostor a pozemků), které se tímto úkonem ohledávají, včetně označení data a místa zajištění, realizační skupiny, číslo jednací spisového materiálu, pod kterým byly úkony prováděny, identifikace jednotlivých digitálních stop a jejich technický popis (značka, model, sériové číslo, stav apod.),
    6. informace o stavu (neporušenosti) zapečetěného obalu a o provedené fotodokumentaci,

7. informace o uživateli zařízení a přístupových kódech a heslech, pokud jsou známé,
8. popis, jakým způsobem, jakým SW či HW nástrojem bylo zajištění digitálních dat provedeno,
9. označení výsledku zajištění digitálních dat – souborů nebo adresářů se zajištěnými digitálními daty včetně kontrolních součtů,
10. případná vyjádření, námitky a požadavky zúčastněných k průběhu úkonu,

f) výsledkem úkonu by měla být zajištěná digitální data opatřená kontrolním součtem, který je uveden v protokolu o provedení úkonu,

g) motivace k dodatečnému zajištění digitálních dat spočívá zejména v tom, že od té chvíle již nejsou digitální data vázána na konkrétní hmotný nosič digitální informace a není nutné jejich autenticitu zajišťovat zapečetěným obalem; tím také vzniká možnost vytvoření identické pracovní kopie digitálních dat, kdy např. jednu kopii může vyhodnocovat samostatně policejní orgán a druhá kopie může být současně předána znalci; dalším důvodem pak může být také možnost vrácení techniky či hmotných nosičů digitální informace zajištěné in natura zpět jejímu majiteli v případech, že by její dlouhodobé zajištění mohlo způsobit vysoké materiální škody nebo ohrožovat nějaký důležitý zájem,

h) z důvodu velké časové náročnosti této operace a možnosti velkou část úloh automatizovat je možné volit i takový postup, že za přítomnosti všech zákonem požadovaných osob je příslušná operace spuštěna a technika následně zapečetěna tak, aby po dobu automatizovaného zpracování nemusel být tomuto procesu nikdo přítomen; při následném rozpečetění a zadokumentování výsledků této automatizované operace je nutné, aby byly opět přítomny všechny zákonem požadované osoby jako před jejím spuštěním; k tomuto účelu je možné použít např. RACK skříň nebo samostatnou k tomuto účelu určenou místnost, která se po spuštění operace uzavře a opatří pečetí,

i) alternativním řešením ve smyslu požadavku na zajištění digitálních dat z techniky nebo hmotných nosičů digitální informace, které byly při úkonech trestního řízení zajištěny in natura nebo digitálních dat bez kontrolních součtů na technologických hmotných nosičích digitální informace v zapečetěných obalech (bod 2.2.2), je předání takové techniky nebo hmotných nosičů digitální informace znalci.

2.4. Specifické případy zajišťování digitálních dat

V rámci zajišťování dat z on-line prostředí je třeba vždy dbát na kompletní dokumentaci zařízení (HW i SW včetně verzí použitého SW a jeho nastavení – zejména nastavení webového prohlížeče, místní nastavení OS a IP adresa), ze kterého je záloha prováděna.

2.4.1. Zajišťování obsahu webových stránek, uživatelských profilů sociálních sítí, např. Facebook, Instagram, YouTube, on-line komunikátorů, e-mailových schránek apod.

Obecně lze obsah webových stránek, profilů sociálních sítí (např. Facebook, Instagram, YouTube, on-line komunikátorů, e-mailových schránek) zajišťovat několika způsoby, zejména pak:

a) zajištění kompletního obsahu jednotlivých webových stránek, konverzací sociálních sítí, mediálních kanálů apod. do podoby off-line zálohy za pomoci speciálních programů či doplňků (tzv. „add-on“) webových prohlížečů; čím obsáhlejší je požadavek (úroveň hloubky zálohy), tím obsáhlejší je výstup a záloha bude trvat déle; lze se setkat i s výstupy o velikosti několik desítek GB; k provádění záloh lze využít různorodé programy, neboť každá jedna webová stránka vypadá po zajištění více různými programy různě a málokdy se podaří zajistit podobu, která je identická s on-line verzí webové stránky,
b) v případě potřeby rychlého a jednoduchého zajištění zájmové webové stránky nebo jen její části lze využít i programy na snímání obrazovky; existují placené programy nebo lze využít i bezplatné „free“ alternativy nebo funkce přímého ukládání webové stránky do obrázku ve webovém prohlížeči, případně funkce tisku (do PDF) a doplňků (tzv. „add-on“) webového prohlížeče,
c) další možností může být provedení foto či video dokumentace obrazovky monitoru či displeje zařízení, na němž jsou webová stránka nebo profil sociální sítě (např. Facebook, Instagram, YouTube, on-line komunikátor) zobrazeny.

Procesní stránka zajišťování obsahu webových stránek, profilů sociálních sítí (např. Facebook, Instagram, YouTube, on-line komunikátorů, e-mailových schránek):

a) pokud bude potřeba zajistit obsah webové stránky, e-mailové schránky, uživatelský účet na sociální síti nebo archiv účtu procesně (důkaz v trestním řízení), realizuje se v rámci úkonů trestního řízení např. § 78 trestního řádu, domovní prohlídka, prohlídka jiných prostor a pozemků, případně v rámci úkonu ohledání podle § 113 trestního řádu, přičemž veškeré úkony je nutno zaprotokolovat včetně identifikace příloh obsahujících zajištěné zálohy digitálních dat (zajištěné digitální stopy), např. screeny (snímky obrazovky), archiv profilu nebo jiné zálohy (off-line HTML), případně soubor s foto či video dokumentací průběhu úkonu pořízenou snímáním obrazovky monitoru např. speciálním programem; digitální data jsou zajištěna na technologický hmotný nosič digitální informace a opatřena kontrolním součtem, případně je jejich autenticita zajištěna uložením technologického hmotného nosiče digitální informace do zapečetěného obalu (bod 2.2),
b) v případě zajišťování takových digitálních dat prostřednictvím vydání věci podle § 78 trestního řádu, např. když poškozený Policii České republiky sám donese hmotný nosič digitální informace (CD, DVD, USB flashdisk apod.) se zálohou zájmových digitálních dat (např. archivem svého uživatelského účtu), měl by být takový nosič řádně označen a nesmazatelně podepsán vydávajícím; doporučuje se vydání na nepřepisovatelném paměťovém médiu, v případě přepisovatelných médií (např. USB flashdisk nebo paměťová karta) je nutno učinit opatření proti možnému přepisu či znehodnocení poskytnutých digitálních dat (např. umístění hmotného nosiče digitální informace v zapečetěném obalu nebo opatření digitálních dat kontrolními součty s jejich uvedením do protokolu o vydání věci),
c) provádět procesní zálohy digitálních dat z uživatelských účtů lze jak po sdělení přihlašovacího jména a hesla, tak i bez jejich znalosti (vše, co může vidět každý bez nutnosti přihlášení ke konkrétnímu zájmovému účtu – veřejné informace bez omezení); toto platí všeobecně o jakékoliv webové stránce, uživatelském účtu, profilu sociální sítě např. Facebook, Instagram, Snapchat, Lide.cz, Libimseti.cz, X-Chat, on-line inzerci, webovém úložišti; pokud je potřeba získat obsah, který je krytý přihlašovacími údaji a tyto údaje Policie České republiky nezíská dobrovolně

od oprávněného držitele, lze vyžádat vydání digitálních dat od společnosti, která službu provozuje; požadovat lze obecně cokoliv, co oprávněný uživatel účtu vidí, obsluhuje, nastavuje, sdílí apod.; pro procesní získání obsahu uživatelských digitálních dat je nutný příkaz soudu podle § 158d odst. 3 trestního řádu (u českých poskytovatelů služeb) nebo mezinárodní právní pomoc (u zahraničních subjektů),

d) podrobnosti, návody, metodika a další užitečné informace k uvedené problematice jsou zpracovány na metodickém portálu sekce kybernetické kriminality útvaru.

2.4.2. Zajišťování virtuálních měn

Zajišťování virtuálních měn je zpracováno v metodice, která je uveřejněna na metodickém portálu sekce kybernetické kriminality útvaru a její aktuální podoba je vyučována v rámci vzdělávacího programu pro kriminalistické IT specialisty P2/0279 – Provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a digitálních dat na místě jejich nálezu.

2.4.3. Zajišťování obsahu vzdálených úložišť propojených datovými službami a digitálních dat bez teritoriálního ohraničení (dále jen „vzdálené úložiště“)

Podle současných poznatků Kriminalistický ústav doporučuje: digitální data vzdálených úložišť propojených datovými službami a digitální data bez teritoriálního ohraničení dostupná prostřednictvím výpočetní techniky vyskytující se na místě činu je možné prostřednictvím této výpočetní techniky zadokumentovat.

Proces zajištění digitálních dat ze vzdálených úložišť při úkonech trestního řízení (např. § 78 trestního řádu, domovní prohlídka, prohlídka jiných prostor a pozemků) v případě neveřejně přístupných digitálních dat, z pohledu aktuálního stavu přihlášení a případné spolupráce dotčené osoby:

a) výpočetní technika je zapnutá, vzdálené úložiště je dostupné a viditelné – digitální data je možné zajistit v rámci daného úkonu trestního řízení,
b) výpočetní technika je zapnutá/vypnutá, vzdálené úložiště je viditelné, ale veřejně nedostupné bez přihlášení:
    1. dotčená osoba poskytne potřebnou součinnost pro zpřístupnění obsahu vzdáleného úložiště – možno zajistit v rámci dobrovolného vydání (§ 78 trestního řádu, domovní prohlídka, prohlídka jiných prostor a pozemků),
    2. dotčená osoba neposkytne potřebnou součinnost pro zpřístupnění obsahu vzdáleného úložiště – v případě, že je v příkazu k provedení domovní prohlídky či prohlídky jiných prostor a pozemků specifikováno, že se vztahuje i na zajištění dat z virtuálního prostředí, pak připadá v úvahu možnost využít veškerých dostupných možností pro získání přístupu k digitálním datům (např. použít nalezená a zjištěná hesla), případně postup podle § 158d odst. 3 trestního řádu, nebo cestou mezinárodní spolupráce podle konkrétní situace trestní věci.

2.4.4. Zajišťování digitálních dat z komunikační techniky

Vydaná osvědčení kriminalistických IT specialistů aktuálně nezahrnují oprávnění k zajišťování digitálních dat z komunikačních zařízení. Zpracovatel spisu může přibrat kriminalistického IT specialistu k zajištění digitálních dat z komunikačních zařízení v případě, že takto získané údaje využije pro operativní účely, nebo s možným rizikem, že takto získané údaje nebude možné použít jako důkaz pro trestní řízení.

K zajištění digitálních dat z komunikačních zařízení v případě, že takto získané údaje bude možné použít jako důkaz pro trestní řízení, musí zpracovatel spisu přibrat znalce.

2.4.5. Zajišťování digitálních dat z rozsáhlých serverových systémů a diskových polí

Při zajišťování digitálních dat z rozsáhlých serverových systémů a diskových polí je vhodné přibrat znalce.

Může být účelné k takovým případům zajišťování techniky a digitálních dat zainteresovat místního administrátora nebo pracovníka externí společnosti, která zajišťuje správu a administraci předmětných informačních systémů, je však třeba brát v potaz možné riziko ohrožení úkonů zajišťování digitálních dat.

3. Činnosti se zajištěnými digitálními daty

Veškerá činnost policejního orgánu s digitálními daty zajištěnými v rámci úkonů trestního řízení se vždy provádí tak, aby byla zajištěna neměnnost zajištěných digitálních dat, jejich důkazní hodnota a přezkoumatelnost v kterékoliv fázi trestního řízení. Toto je zaručeno zejména tím, že jsou úkony zpřístupňování a vyhodnocování digitálních dat prováděny na pomocných pracovních kopiích digitálních dat opatřených kontrolními součty, přičemž ty jsou před jednotlivými úkony a při přesouvání či kopírování digitálních dat verifikovány. Následující postupy se týkají převážně činností se zajištěnými digitálními daty (body 2.2 a 2.3).

3.1. Zpřístupňování zajištěných digitálních dat

Kriminalistický IT specialista specializovaného pracoviště útvaru pracuje při zpřístupňování zajištěných digitálních dat v součinnosti se zpracovatelem spisu na základě konkrétních požadavků (např. zadání spolupráce v informačním systému ETŘ, plán prověřování/vyšetřování):

a) při zpřístupňování zajištěných digitálních dat se vždy pracuje s kopií zajištěných digitálních dat, která byla opatřena kontrolním součtem zajišťujícím jejich autenticitu (nepracuje se na technice nebo hmotných nosičích digitální informace zajištěných in natura či na digitálních datech bez kontrolních součtů); možnosti zajištění pracovní kopie digitálních dat jsou podrobně zpracovány v bodech 2.2 a 2.3; vlastní práce se zajištěnými digitálními daty při procesu jejich zpřístupňování probíhá zásadně na tzv. pomocné pracovní kopii, kterou si kriminalistický IT specialista specializovaného pracoviště útvaru pro tento účel vytvoří před začátkem procesu zpřístupňování zajištěných digitálních dat z pracovní kopie,
b) kriminalistický IT specialista specializovaného pracoviště útvaru na základě konkrétních požadavků podle konkrétního spisového materiálu provádí za pomoci speciálního software (forenzně-analytické nástroje, nástroje pro obnovu digitálních dat, indexačně-analytické nástroje apod.) proces zpřístupňování zajištěných digitálních dat, případně se následně spolupodílí na vyhodnocování zajištěných digitálních dat ve vztahu k dokumentované trestní věci, které je prováděno zpracovatelem spisu, či jím pověřenou osobou (bod 2.2),
c) výstupem procesu zpřístupňování zajištěných digitálních dat kriminalistickým IT specialistou specializovaného pracoviště útvaru může podle konkrétního požadavku být např.:

1. selekce souborů podle typu či podle klíčových slov včetně obnovy smazaných souborů,
2. selekce e-mailové komunikace včetně obnovy smazané komunikace,
3. výpisy z historie webových prohlížečů,
4. výpisy z registrů informačních systémů,
5. vytvoření časové osy či provázaností ve vztahu ke konkrétním souborům a osobám zúčastněným v dané trestní věci včetně příslušného grafického znázornění apod.

(dále jen „zpřístupněná digitální data“),

d) na základě provedení procesu zpřístupňování digitálních dat dojde k výraznému zredukování množství dat, která budou následně podrobena procesu vyhodnocování a případně budou moci být použita jako důkaz; zároveň je možné tímto postupem separovat digitální data a techniku pro účely trestního řízení nepotřebnou a tuto následně případně vrátit majiteli (typicky např. dětské počítače, multimediální disková úložiště s rodinnými fotografiemi),

e) v případě potřeby je možné provést proces zpřístupňování digitálních dat formou provedení ohledání v rámci procesního úkonu podle § 113 trestního řádu; na začátku tohoto ohledání by měla proběhnout kontrola autenticity digitálních dat pomocí kontrolního součtu, aby bylo nezpochybnitelné, že toto ohledání je prováděno na původních nezměněných zajištěných digitálních datech; za procesní stránku věci je po celou dobu odpovědný zpracovatel spisu, který provádí veškeré úkony s tím spojené, jako je protokolování, vyrozumění oprávněných subjektů o úkonu apod.,

f) o provedeném úkonu se sepíše protokol o zpřístupnění zajištěných digitálních dat případně protokol o ohledání (zpřístupnění digitálních dat) věci podle § 113 trestního řádu s náležitostmi podle § 55 trestního řádu, zejména pak:
   1. datum, čas a místo provádění úkonu ohledání a spisová značka, pod kterou je věc vedena,
   2. pojmenování policejního orgánu provádějícího úkon a předmět úkonu,
   3. informace o osobách, které byly u úkonu přítomné – pracovníci provádějící úkon (kriminalistický IT specialista, zpracovatel spisu), nezúčastněná osoba, další přítomné osoby,
   4. informace o vyrozumění dotčených osob o prováděném úkonu a jejich přítomnosti u prováděného úkonu (obhajoba, obviněný apod.),
   5. identifikace zpřístupňovaných digitálních dat, případně předmět ohledání – popis zajištěné věci (kopie digitálních dat) z předchozích úkonů trestního řízení (např. domovní prohlídka, prohlídka jiných prostor a pozemků) včetně označení data a místa zajištění, realizační skupiny, číslo jednací spisového materiálu, pod kterým byly úkony prováděny, identifikace stopy a její technický popis,
   6. informace o aktuální verifikaci kontrolního součtu,
   7. popis, jakým způsobem a metodami a za pomoci jakých SW či HW nástrojů byl úkon proveden,
   8. označení výsledku – např. soupis souborů nebo adresářů se zajištěnými digitálními daty včetně kontrolních součtů,
   9. případná vyjádření, námitky a požadavky zúčastněných k průběhu úkonu,

g) výstupem procesu zpřístupňování zajištěných digitálních dat je zpravidla protokol o provedeném úkonu obsahující seznam souborů a adresářů zpřístupněných digitálních dat s kontrolními součty, jehož přílohou je technologický hmotný nosič digitální informace se zpřístupněnými digitálními daty a v případě potřeby i s tištěnou podobou jednotlivých souborů (např. smlouvy či e-mailová komunikace),

h) motivací a cílem procesu zpřístupňování zajištěných digitálních dat vlastními silami, kriminalistickými IT specialisty specializovaného pracoviště útvaru, je zejména možnost přímé spolupráce se zpracovatelem spisu, zrychlení celého procesu zpřístupňování a vyhodnocování zajištěných a zpřístupněných digitálních dat a celého trestního řízení a v neposlední řadě snaha o úspory finančních prostředků vynakládaných za znalecké zkoumání znalcům,

i) veškerá činnost kriminalistických IT specialistů specializovaného pracoviště útvaru při procesu zpřístupňování zajištěných digitálních dat je prováděna na pomocných pracovních kopiích zajištěných digitálních dat, která byla opatřena kontrolním součtem zajišťujícím jejich autenticitu, přičemž originální zajištěná digitální data zůstávají neměnná a není tedy narušena možnost případného znaleckého zkoumání zajištěných digitálních dat.

3.2. Vyhodnocování zajištěných a zpřístupněných digitálních dat

Po provedení zajištění digitálních dat v čitelné a zpracovatelné podobě případně po provedení zpřístupnění digitálních dat nastává fáze vlastního vyhodnocování digitálních dat zpracovatelem spisu.

Zpracovatel spisu, obeznámený s podstatou trestní věci, při vyhodnocování spolupracuje s analytiky útvaru, případně s kriminalistickými IT specialisty specializovaného pracoviště útvaru. Za použití analytických nástrojů, informačních systémů Policie České republiky, případně externích zdrojů, je provedeno vyhodnocení zajištěných a zpřístupněných digitálních dat včetně dalších souvisejících vztahových a časových analýz s případným propojením a návaznostmi do jiných trestních věcí.

Osoba provádějící úkon vyhodnocení zajištěných a zpřístupněných digitálních dat sepíše protokol o vyhodnocení zajištěných a zpřístupněných digitálních dat s náležitostmi podle § 55 trestního řádu, především:

a) datum, čas a místo provádění úkonu a spisová značka, pod kterou je věc vedena,

b) pojmenování policejního orgánu provádějícího úkon, místo, čas, předmět úkonu, jméno a příjmení osoby provádějící úkon,

c) identifikace zpřístupněných digitálních dat, popis metod a způsobů vyhodnocení zpřístupněných digitálních dat, popis zjištěných skutečností v kontextu s trestní věcí,

d) pokud je to technicky možné, přílohou protokolu je technologický hmotný nosič digitální informace s vyhodnocenými relevantními digitálními daty, v opačném případě protokol obsahuje informaci, kde se taková digitální data nachází.

Vyhodnocená relevantní digitální data jsou součástí originálu trestního spisu.

3.3. Přibrání znalce

Znalecké zkoumání zajištěných digitálních stop (všechny možnosti zajištění dat – bod 2.2) je možné provádět znalcem na základě opatření o přibrání znalce podle § 105 trestního řádu, znaleckého ústavu podle § 110 trestního řádu a v jednodušších případech formou odborného vyjádření podle § 105 trestního řádu (např. odbory kriminalistické technicky a expertiz krajských ředitelství Policie České republiky).

Výstupem znaleckého zkoumání je zpravidla znalecký posudek, ve kterém jsou mimo jiné zadokumentovány metody a postupy znaleckého zkoumání a v neposlední řadě zpřístupněná digitální data ze zajištěných digitálních stop.

Na zajištěných digitálních datech zpřístupněných znaleckým zkoumáním se následně provede vyhodnocování podle bodu 3.2.

4. Nakládání s hmotnými nosiči digitální informace

4.1. Optimalizace a uložení zajištěných digitálních dat

Optimalizace datového prostoru na technologických hmotných nosičích digitální informace je možná pouze v případě, že jsou tato digitální data opatřena kontrolními součty.

Při každé manipulaci s digitálními daty je nutné verifikovat tato data pomocí kontrolních součtů.

Po provedených úkonech trestního řízení, při nichž jsou zajištěna digitální data na technologické hmotné nosiče digitální informace, je nutné provést vyhodnocení zaplněnosti těchto nosičů, na jehož základě dojde k případné optimalizaci využití jejich datové kapacity.

Pro potřeby zpřístupňování zajištěných digitálních dat, popřípadě zadání znaleckého zkoumání zajištěných digitálních dat a následného vyhodnocování zajištěných a zpřístupněných digitálních dat kriminalistický IT specialista vytvoří v součinnosti se zpracovatelem spisu pomocnou pracovní kopii zajištěných digitálních dat, se kterou se bude nadále pracovat, přičemž originály zajištěných digitálních dat zůstanou bezpečně zálohovány podle aktuálních technických možností útvaru. Tímto postupem je zaručena neměnnost zajištěných digitálních dat a zachování jejich důkazní hodnoty.

4.2. Pravidla při kopírování zajištěných dat

V situaci,

a) kdy jsou zajištěná digitální data opatřena kontrolními součty, je nutné při každém jejich kopírování či přesouvání tyto kontrolní součty ověřovat,
b) kdy nejsou zajištěná digitální data opatřena kontrolními součty, je možné tato data kontrolními součty opatřit dodatečně v rámci procesního úkonu ohledání podle § 113 trestního řádu nebo v rámci znaleckého zkoumání. V případě, že při tomto úkonu není technicky možné kontrolní součty provést, je nutné zajištěný originál i případnou kopii digitálních dat uložit v zapečetěném obalu pro zaručení neměnnosti zajištěných digitálních dat a zachování jejich důkazní hodnoty.

4.3. Dokazování, vrácení věci

Dokazování je prováděno před soudem, proto musí být zachovány hmotné nosiče digitální informace, které jsou považovány podle práva za věc. K vrácení věci může dojít jen tehdy, pokud není důležitá pro trestní řízení.

Ne vždy lze však zajistit techniku in natura (např. webové stránky, síťová úložiště, rozsáhlé servery v nadnárodních společnostech) a ponechat si ji pro účely trestního řízení po celou dobu tohoto řízení. Zároveň není vyloučená situace, že při zajištění techniky in natura, vzhledem k jejímu možnému stáří a stavu této zajištěné techniky a mnohdy i délce trestního řízení, dojde k nefunkčnosti zajištěné techniky a tedy i následné nemožnosti dokazování před soudem.

Ve zvlášť odůvodněných a výjimečných případech pak mohou být původně in natura zajištěné hmotné nosiče digitální informace po vytvoření kopie jejich obsahu přednostně vráceny zpět. Jedná se o případy, kdy by jejich dlouhodobé zajištění mohlo způsobit vysoké materiální škody nebo ohrožovat nějaký důležitý zájem. Uvedený postup je možný pouze na základě rozhodnutí dozorujícího státního zástupce nebo výlučně s jeho souhlasem.

Provedení důkazu z originálního hmotného nosiče digitální informace před soudem je často z technických i časových důvodů nerealizovatelné a je vhodné vytvořit kopii elektronických důkazních materiálů na technologický hmotný nosič digitální informace při dodržování doporučených postupů při zajišťování digitálních stop.

Závěr

Policie ČR, ale i jiné bezpečnostní sbory jsou již delší dobu zahlcené přemírou interních aktů upravujících jejich činnost a autoři si jsou vědomy i averze vůči každému novému předpisu, který „svazuje“ činnost příslušníků v přímém výkonu služby, nicméně tento interní akt ředitele NCOZ SKPV si tuto ambici v žádném případě nenese, neboť **je postaven na základní filozofii** metodicky sjednotit a upřesnit výkon služby v této oblasti tak, aby nedocházelo k zbytečné ztrátě hodnoty zajištěných důkazů. Tak jak uvedeno v úvodu článku, obsah předkládáme odborné praxi, k případné využitelnosti i v rámci jejich bezpečnostní praxe, přičemž se nebráníme případným připomínkám. Provedená výzkumná zjištění budou spoluautorem /řešitelem zmíněného výzkumného úkolu DVVÚ I/3/ zahrnuta do výuky kriminalistické taktiky a metodiky tak, aby byly aktuální postupy praxe přeneseny na studenty bezpečnostní praxe, přičemž v součinnosti s odborníky z praxe bude nadále sledován vývoj kriminalistické praxe a usměrňován tak teoretický a praktický pohled na věc, a to **v rámci aplikovaného výzkumu**.

Literatura

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

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-807-3807-207.

ČSN ISO/IEC 2382-8 (369001). *Informační technologie – Slovník. Část 8: Bezpečnost*

Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

Zákon č. 36/1967 Sb., o znalcích a tlumočnících.

Zákon č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech.

Pokyn ředitele Kriminalistického ústavu č. 34/2019, k vybraným kriminalisticko-technickým činnostem.

Pokyn policejního prezidenta č. 103/2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení.

Pokyn policejního prezidenta č. 235/2014, o využívání datové sítě intranet Ministerstva vnitra Hermes, pokyn policejního prezidenta č. 236/2014, o využívání celosvětové sítě internet.

Pokyn policejního prezidenta č. 100/2018, o kriminalisticko-technické činnosti.

R E S U M É

Současná policejní praxe přináší, v rámci dokumentace protiprávního jednání, čím dál tím více nutnost ze strany příslušníků bezpečnostních sborů, kteří zajišťují, zpřístupňují a vyhodnocují digitální stopy, dovednosti jak technického, tak procesně právního rázu. Dovednosti byly ze strany pracovní skupiny Národní centrály proti organizovanému zločinu SKPV Policie ČR shrnuty do interního aktu řízení, který předkládáme odborné veřejnosti, k případnému posouzení.

Klíčová slova: zajišťování, vyhodnocování digitálních stop, kriminalistická taktika, ohledání, důkaz, znalec, kriminalistický IT specialista.

S U M M A R Y

ČÁP, Jan; BREU, Lukáš; PROŠEK, Zdeněk: PROVISION, DISCLOSURE AND EVALUATION OF DIGITAL FOOTPRINTS

In the context of documenting illegal behaviour, the current nature of police work puts further emphasis on technical and law processing abilities of involved security services that provide access and evaluate digital traces. Those competences were conceptualized by The National Centre against Organised Crime of the Criminal Police and Investigation Service, Police of the Czech Republic and are presented in an internal managerial act, which we bring forward to be assessed by the expert community.

Keywords: securing, evaluation of digital footprints, criminal tactics, examination, proof, expert, forensic IT specialist.