Univerzita Palackého v Olomouci
Právnická fakulta

Denisa Kurková

Kyberkriminalita a její odhalování a vyšetřování

Diplomová práce

Olomouc 2020

Prohlašuji, že jsem diplomovou práci na téma Kyberkriminalita a její odhalování a vyšetřování vypracovala samostatně a citovala jsem všechny použité zdroje.

V Olomouci dne ……..…. 2020 Podpis: ……..

Denisa Kurková

Poděkování

Děkuji touto cestou doc. JUDr. Filipu Ščerbovi, Ph.D. za jeho podněty, odborné rady a připomínky při vedení této práce. Dále bych rovněž ráda poděkovala Krajskému ředitelství policie Olomouckého kraje za poskytnutí spolupráce, odborné konzultace a poskytnutí poznatků z praxe, které mi byly nápomocny při psaní diplomové práce. Rovněž patří velké díky mé rodině, která mi byla velkou oporou nejen při psaní, ale i po dobu celého studia.

Obsah

Seznam použitých zkratek 5
Úvod 6
1 Pojem kybernetické kriminality 9
1.1 Dělení kyberkriminality 10
2 Postup při odhalování a vyšetřování kyberkriminality 12
2.1 Kriminalisticko-taktický postup 12
2.2 Metodika vyšetřování 12
2.3 Metodika vyšetřování kyberkriminality 13
2.3.1 Zvláštnosti prvotních vyšetřovacích a operativně pátracích úkonů 14
2.3.2 Zvláštnosti následné etapy vyšetřování 19
3 Digitální stopa 21
3.1 Pojem stopa 21
3.1.1 Dělení kriminalistických stop 21
3.2 Digitální stopa 22
3.2.1 Vlastnosti digitálních stop 24
3.3 Elektronický důkaz 25
4 Zajištění důkazních prostředků 27
4.1 Domovní prohlídka 27
4.2 Prohlídka jiných prostor a pozemků 32
4.3 Zajištění věci pro důkazní účely 33
4.4 Údaje o telekomunikačním provozu 35
4.5 Okamžité zajištění dat a ustanovení § 7b trestního řádu 40
Závěr 46
Zdroje 48
Abstrakt 58
Abstract 59
Klíčová slova 60
Key words 60

Seznam použitých zkratek

ČR	Česká republika
EU	Evropská unie
ESD	Evropský soudní dvůr
EÚLP	Evropská Úmluva o ochraně základních práv a svobod
ESLP	Evropský soud pro lidská práva
FBI	Federal Bureau of Investigation
KŘP	Krajské ředitelství policie
KÚP	Kriminalistický ústav v Praze
LZPS	Listina základních práv a svobod
OČTŘ	Orgány činné v trestním řízení
OKTE	Odbor kriminalistické techniky a expertiz
PC	Počítač
PČR	Policie České republiky
SPTČ	Skutková podstata trestného činu
TŘ	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
TZ	Zákon č. 40/2009 Sb., trestní zákoník
USA	Spojené státy americké
ÚS	Ústavní soud České republiky
ZEK	Zákon číslo 127/2005 Sb., Zákon o elektronických komunikacích

Úvod

Pokrok vědy a techniky za posledních padesát let výrazně změnil tvář společnosti, způsob života, komunikace a přinesl s sebou i změny v páchání trestné činnosti. V současné době lze najít jen málo oblastí života, které nejsou spojeny s informačními a komunikačními technologiemi. Tyto technologie významným způsobem usnadnily člověku život, ale bohužel je jejich vedlejším produktem i přínos nových způsobů páchání trestné činnosti. Zatímco celková kriminalita v ČR má tendence klesat, u kyberkriminality vidíme opačný efekt, kdy dochází k nárůstu počtu spáchaných trestný činů. V roce 2011 jich PČR zaregistrovala 1502, zatímco v roce 2019 jich bylo 8417[1], což jen potvrzuje to, že rozvoj informačních a komunikačních technologií vytvořil nové možnosti v páchání trestné činnosti, ba dokonce dal jejím pachatelům jakýsi falešný pocit bezpečí a šanci, že pro spáchané skutky nebudou trestně stíháni.

Zákonodárce má tedy nelehký úkol, jímž je povinnost vytvořit právní úpravu, jež bude chránit zájmy společnosti i jednotlivce a zároveň bude efektivně potírat trestnou činnost, kterou lze pojit s fenoménem kyberkriminality.

S významným nárůstem kyberkriminality se zvyšuje i potřeba zabývat se touto oblastí a vytvářet efektivní právní úpravu. Jde o problematiku, která se dynamicky rozvíjí, a proto si myslím, že náměty pro vědecké práce v této oblasti ještě nebyly vyčerpány. Podle mého názoru se česká právní úprava kybernetické kriminalitě prozatím příliš nepřizpůsobila. Pokládám proto za vhodné zabývat se jejími oblastmi souvisejícími s odhalováním a vyšetřováním kyberkriminality, což mě spolu se zájmem o informační a komunikační technologie přivedlo k tématu předkládané diplomové práce.

V rámci této práce se nebudu zaměřovat na hmotněprávní úpravu, jelikož je dle mého názoru této oblasti ze strany autorů odborných prací věnován dostatek pozornosti. Zaměřím se na oblast kriminalistickou a procesněprávní, avšak jen na vybrané části, protože se jedná o oblast velice složitou, přičemž rozsah předkládané práce ji neumožňuje celou obsáhnout. Pro účely této diplomové práce bude užíván pojem kyberkriminalita jako ústřední pojem, který v sobě spojuje jak kyberkriminalitu, tak počítačovou kriminalitu.

Mým primárním cílem je prozkoumat kriminalistický postup při odhalování této trestné činnosti a přiblížit některé postupy při zajišťování důkazních prostředků, popřípadě upozornit

[11] *Kyberkriminalita na vzestupu, oběťmi jsou stále častěji děti. Udělejte si test*. [online]. eurozpravy.cz, 10 února 2020 [cit. 9. 3. 2020]. Dostupné na <https://eurozpravy.cz/domaci/zivot/kyberkriminalita-na-vzestupu-obetmi-jsou-stale-casteji-deti-udelejte-si-test.d47c0d49/ >.

na jejich možné nedostatky, a to za použití právní úpravy ČR a postupy OČTŘ působícími v ČR. Tato práce se pokusí zodpovědět následující výzkumné otázky: Je jednotný názor na pojmenování dané oblasti trestné činnosti a na její dělení? Jaké jsou v současné době metodiky objasňování zabývající se touto problematikou? Měnily se tyto metodiky v čase? Co je to digitální stopa? Má význam definovat v zákonné úpravě pojem elektronický důkaz? Jakým způsobem lze zajišťovat důkazy relevantní pro trestní řízení v souvislosti s kyberkriminalitou?

Jsem si vědoma, že obsah předkládané práce nemá sloužit jako návod pro pachatele trestných činů, a proto se kriminalistickým metodám a postupům nevěnuji příliš podrobně, abych neprozradila citlivé informace a významné know how PČR, které je veřejnosti záměrně utajováno. Během psaní jsem své výsledky a závěry konzultovala s odborníky z praxe, a to z prostředí PČR. Jelikož se tito odborníci podílí na vyšetřování trestné činnosti, je třeba zachovat jejich anonymitu, a proto, pokud cituji jejich názory a poznatky z praxe, užívám v poznámkách pod čarou "Informovaný zdroj z prostředí PČR", přičemž s tímto postupem souhlasí vedoucí práce doc. JUDr. Filip Ščerba, Ph.D.

Pojem vyšetřování užívám ve smyslu kriminalistickém, který je chápán více ze široka než jen jako jedna z oblastí přípravného řízení ve smyslu TŘ. Pokud bude v této práci použit pojem vyšetřování v užším smyslu (dle TŘ), bude to v ní výslovně uvedeno.

Diplomová práce je rozdělena do čtyř kapitol. První kapitola by měla uvést čtenáře do problematiky a pokusit se vystihnout pojem kyberkriminality. Pozornost je zde věnována i nejednotnosti nazývání této oblasti. Dále se první kapitola věnuje dělení kyberkriminality. Druhá kapitola se zaměřuje na postup při jejím odhalování a vyšetřování. Věnuje se zejména metodice vyšetřování a vybraným aspektům, které souvisí s procesním právem. Bohužel zde není prostor pro podrobný rozbor jednotlivých kroků metodiky vyšetřování, jelikož daná oblast by vydala na samostatnou diplomovou práci. Třetí kapitola pojednává o pojmu digitální stopa, poukazuje na klasické stopy, jejich dělení a dále rozebírá digitální stopy a jejich vlastnosti a možnosti definice elektronických důkazů v českém právním řádu. Čtvrtá kapitola se zaměřuje na zajištění důkazních prostředků, avšak zabývá se jen vybranými způsoby z důvodu rozsahu práce. Mým cílem je věnovat pozornost oblastem, v nichž může být právní úprava zaostalá, popřípadě nešetrná k právům jednotlivce. Domovní prohlídkou se zabývám podrobněji hlavně z důvodu, že jsem byla jedné přítomna jako nezúčastněná osoba, a to právě při prohlídce související s vyšetřováním kyberkriminality, a viděla jsem některé postupy v praxi. Za tuto cennou zkušenost mohu poděkovat Krajskému ředitelství policie Olomouckého kraje.

Diplomová práce poukazuje nejen na kriminalistické a procesněprávní aspekty, ale zároveň se pokouší spojit informace získané odborníky z praxe a poznatky kriminalistické vědy

s vybranými procesními instituty TŘ. Význam spatřuji v tom, že informace získané odborníky z praxe jsou schopny poukázat na možné nedostatky právní úpravy, popřípadě nastínit způsob nového vytvoření efektivnější právní úpravy.

1 Pojem kybernetické kriminality

Kybernetická kriminalita je relativně nová oblast trestné činnosti, která se v poslední době rychle a dynamicky rozvíjí, a to z důvodu rozvoje a dostupnosti výpočetní techniky a kyberprostoru. Mohlo by se zdát, že je tento jev fenoménem poslední doby. Nicméně zdání klame, jelikož: *„…kriminalita kopírovala technické i uživatelské možnosti počítačů, zpočátku coby neznámých a obtížně dostupných zařízení. Prvními trestnými činy byly sabotáže, které byly různě motivované – politicky i mstou zaměstnavateli. Pravděpodobně první čistě počítačový zločin se u nás odehrál v sedmdesátých letech, kdy nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách. Tento pracovník byl odsouzen podle neověřených informací za sabotáž podle Části druhé Hlavy prvé tehdejšího trestního zákona.“*[2] Od 70. let minulého století došlo k velkým změnám v oblasti výpočetních a informačních technologií a dnes bychom velice těžce hledali oblast lidského života, která by nějakým způsobem nevyužívala výpočetní techniku či informační technologie. Kromě pojmu kyberkriminalita se ještě můžeme setkat s pojmem počítačová kriminalita či high-tech kriminalita a dalšími označeními této problematiky. Nazývat tuto oblast jako počítačovou kriminalitu není dle mého názoru zcela správné, jelikož to může v současné době zkreslovat představu jedince a evokovat pocit, že se pojem počítačová kriminalita vztahuje pouze na oblast počítačů a notebooků. Rovněž high-tech kriminalita není dle mého názoru zcela vhodný název, jelikož pojem high-tech označuje nejvyspělejší, nejpokročilejší techniku k danému časovému okamžiku a tímto okamžikem je současnost. Je zřejmé, že to, co je považováno dnes za high-tech, již za 2 roky do této kategorie spadat nemusí. V důsledku toho by pak bylo nutné vymezovat další kategorie, které by tuto oblast pokryly. Myslím si, že je vhodnější nazývat tuto oblast jako kybernetickou kriminalitu nebo zjednodušeně kyberkriminalitu. Tento pojem je širší než počítačová kriminalita a zahrnuje i oblasti, které by se hůře řadily do oblasti počítačové kriminality, proto považuji takové označování v současné době za vhodné a výstižné. Nicméně se můžeme setkat s názorem, že pojem kyberkriminalita je podmnožinou počítačové kriminality a není zcela vhodné takto označovat tuto oblast, jelikož slovo kyberkriminalita je odvozeno od slova kyberprostor. Kyberprostor představuje systém tvořený tisíci počítačů, serverů, routerů, přepínačů, optických kabelů apod. Uvedený názor zastává tezi, že kyberkriminalita je

[2] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2 vydání. Plzeň: Aleš Čeněk, 2018. s. 102.

podmnožinou počítačové kriminality, jelikož počítačová kriminalita se může odehrát i mimo tento prostor, zatímco kybernetická nikoli.[3]

Definice pojmu kyberkriminality se mohou lišit a z důvodu dynamického rozvoje této oblasti nelze vytvořit univerzální definici, která by pokryla rozsah tohoto pojmu, jenž se v čase mění. Jedna z možných a dle mého názoru výstižných definic v současnosti je: *„Pod pojmem „počítačová kriminalita" je třeba chápat 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 zájmu této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsána zařízení jako věci movité, nebo b) jako nástroj trestné činnosti."*[4] *„Počítač tedy může být předmětem trestného činu, ale současně také prostředkem ke spáchání trestné činnosti."*[5] Slovo počítač však musí být chápáno sensu lato, tzn. podřadíme pod něj např. chytré hodinky, mobilní telefon, tablet, chytrou ledničku apod. Je však vysoce pravděpodobné, že ani tato definice v čase neobstojí, stane se zastaralou a bude nahrazena novou, výstižnější. Záležet bude na vývoji informačních technologií i na samotném vývoji kyberkriminality.

1.1 Dělení kyberkriminality

Dělení kyberkriminality se může lišit v závislosti na jejím pojetí autorem, pojetí právní normou či z jiného relevantního důvodu. Proto v současné době není jednotný názor na její rozdělení. Jedním z možných dělení je klasifikace dle Úmluvy Rady Evropy o kybernetické kriminalitě, která ji spolu s dodatkovým protokolem dělí do 8 kategorií a to: *„1) trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů, 2) trestné činy související s počítačem, 3) trestné činy související s obsahem, 4) trestné činy související s porušováním autorských práv a práv souvisejících, 5) šíření rasistických a xenofobních materiálů pomocí počítačových systémů, 6) rasisticky a xenofobně motivované vyhrožování, 7) rasisticky a xenofobně motivované útoky, 8) popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti."*[6] Odlišný názor na dělení kyberkriminality mají autoři knihy Kriminalistika: Kriminalistická taktika a metodika vyšetřovaní, kde Zdeněk Konrád

[3] KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. *Časopis pro právní vědu a praxi*, 2016, roč. 24, č. 1, s. 5-19.
[4] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. Kriminalistika: Kriminalistická taktika a metodiky vyšetřování. Plzeň: Aleš Čeněk, 2015. s. 334.
[5] Tamtéž.
[6] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016. s. 38.

a kol., uvádějí toto dělení: *„a) neoprávněný zásah do vstupních dat, b) neoprávněné změny v uložených datech, c) neoprávněné pokyny k počítačovým operacím, d) neoprávněné pronikání do počítačů, počítačového systému a jeho databází, e) napadení cizího počítače, jeho programového vybavení a souborů dat v databázích, f) informační trestná činnost.“*[7] Na internetových stránkách PČR nalezneme odlišné dělení: *„1) podvodná jednání, 2) hacking, 3) blagging, 4) podvodné e-shopy, 5) mravnostní trestné činy, 6) trestné činy proti autorskému právu, 7) násilné projevy a hate crime.“*[8] Toto jsou jen některé ze způsobů dělení kyberkriminality, existuje jich mnohem více, ale není důvod, aby tato práce obsahovala výčet všech. Na výše uvedených děleních jsou vidět odlišnosti v pojetí. Zatímco dělení dle Úmluvy Rady Evropy se více zaměřuje na dělení podle skutkových podstat, druhé dělení je pojato více kriminalisticky a zaměřuje se více na předmět útoku. Poslední dělení je velmi zjednodušené a některé trestné činy by se nedaly pod žádnou z těchto kategorií podřadit. To, jak je kyberkriminalita dělena, nehraje až tak zásadní roli, nicméně vhodné dělení je schopno podstatným způsobem ulehčit práci OČTŘ, neboť pro ně bude jednodušší podřadit konkrétní skutek pod určitou výseč trestných činů, aplikovat na něj vhodnou metodiku vyšetřování a užít vhodné procesní instituty, které budou co nejefektivněji sloužit k získání potřebných důkazů.

[7]KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování*. Plzeň: Aleš Čeněk, 2015. s. 336-338.
[8] *Jednotlivé druhy kyberkriminality*. [online]. policie.cz, [cit. 24. 10. 2019]. Dostupné na <https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx?q=cHJuPTE%3d>.

2 Postup při odhalování a vyšetřování kyberkriminality

2.1 Kriminalisticko-taktický postup

Obecně se autoři knih, např. Z. Konrád, V. Porada, J. Straus, J. Musil, I. Svoboda, shodnou na definici kriminalistické taktiky. Kriminalistická taktika je samostatnou částí systému kriminalistiky, která poskytuje vědecky podložené postupy a metody zaměřené především na získávání, dokumentaci a využívání paměťových kriminalistických stop. Poznatky z kriminalistické taktiky se promítají v kriminalistické technice i v metodice jednotlivých druhů trestných činů.[9] I. Svoboda řadí mezi současné kriminalistické taktiky tyto: *„ ...- kriminalistické ohledání; kriminalistická prohlídka; - kriminalistické verze; - výslech; - konfrontace; - prověrka výpovědi na místě; - rekognice; - kriminalistický experiment; - kriminalistická rekonstrukce.“*[10] Úkony jako kriminalistický experiment, kriminalistická rekonstrukce a prověrka výpovědi na místě se v souvislosti s prověřováním a vyšetřováním kyberkriminality využívají v současnosti málokdy.[11] Pokud jde o kriminalistické ohledání, pak nejčastěji půjde o ohledání místa činu, u kriminalistických prohlídek se jedná hlavně o domovní prohlídky, prohlídky jiných prostor a osobní prohlídky. Rovněž se využívají kriminalistické verze se zaměřením na kyberkriminalitu, přičemž obvykle jsou obsahem metodiky vyšetřování. Výslechy se zabývám níže v této kapitole. Rekognice je OČTŘ využívaná s tím, že postupují v souladu s klasickými metodami, postupy, obecnou metodikou a TŘ.[12]

2.2 Metodika vyšetřování

Odborná veřejnost se v zásadě shoduje v tom, co znamená metodika vyšetřování. Proto jsem se rozhodla ve své práci citovat jen několik málo autorů a jejich děl. Obecně uznávaná definice je, že: *„ ...metodika vyšetřování je ta část kriminalistické vědy, která odhaluje a zkoumá zákonitosti vzniku stop a zvláštnosti postupů při vyhledávání, zajišťování a využívání stop, jiných soudních důkazů a kriminalisticky významných informací s ohledem na určitý typ trestného činu a předpokládanou typovou vyšetřovací situaci.“*[13] Pro zjednodušení citované definice si dovolím zmínit názor Jana Musila, který říká: *„ ...metodika vyšetřování jednotlivých druhů trestných činů zkoumá zákonitosti vzniku stop určitého druhu trestných činů a na jejich*

[9] SVOBODA, Ivo a kol. *Kriminalistika*. Ostrava: Key Publishing s.r.o., 2016. s. 32-34.
[10] Tamtéž.
[11] Informovaný zdroj z prostředí PČR.
[12] Informovaný zdroj z prostředí PČR.
[13] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování*. Plzeň: Aleš Čeněk, 2015. taktika s. 166. Shodně v PORADA, Viktor a kol. *Kriminalistická metodika vyšetřování*. Plzeň: Aleš Čeněk, 2007. s. 12.

základě modifikuje obecné metody tak, aby vyhovovaly podmínkám odhalování a vyšetřování a prevence jednotlivých druhů trestných činů."[14] Jde o vědecké poznání, které je adresované praxi, ale zároveň je praxí vytvářeno a ověřeno.[15] Funkce této metodiky je poznávací a formální a Zdeněk Konrád ji ve své knize Kriminalistika doplňuje o funkci kontrolní. Metodika vyšetřování má rovněž své zásady, a to zásady tvorby a zásady aplikace. Tato práce se však primárně nezabývá metodikou vyšetřování, a proto pro bližší informace odkazuji na výše zmiňovanou učebnici.[16]

2.3 Metodika vyšetřování kyberkriminality

Pro každý typový model trestné činnosti je vytvořena samostatná metodika vyšetřování, tedy i pro oblast kybernetické kriminality, přičemž ve starší literatuře se můžeme setkat s jejím označováním jako metodika vyšetřování počítačové kriminality. Takové označování je ale dle mého názoru zastaralé a autoři nových publikací a článků by měli zvážit jeho užití. Metodika vyšetřování se v čase mění, jelikož musí reagovat na změny, které se v souvislosti s aktuálními trendy ve způsobu páchání dané trestné činnosti dějí, popřípadě musí reagovat na změny legislativy či vznik nových kriminalistických metod. A protože kyberkriminalita je dynamicky se rozvíjející oblast, metodika na toto musí reagovat. Je důležité si uvědomit, že metodika vyšetřování je jen jakýsi souhrn doporučení, který pro kriminalisty není nijak závazný. Oni sami musí volit nejvhodnější postup pro vyšetření daného trestného činu.[17] Ve své práci se nebudu podrobně věnovat všem částem metodiky vyšetřování kyberkriminality, protože jde o téma, které by vydalo na samostatnou diplomovou práci, ale podrobněji se zaměřím na části, které se více týkají trestně procesních aspektů věci, a to na zvláštnosti předmětu vyšetřování a dokazování, zvláštnosti prvotních vyšetřovacích a operativně pátracích úkonů a na zvláštnosti následné etapy vyšetřování. Zbylými oblastmi metodiky vyšetřování kyberkriminality se ve své práci nebudu zabývat.

Metodiky vyšetřování by se daly rozdělit na tzv. obecné metodiky vyšetřování, metodiky vyšetřování, které nejsou veřejně přístupné, a metodiky, které PČR vytváří ve spolupráci s dalšími organizacemi pro veřejnost. Níže uvedené podkapitoly budou vycházet

[14] MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. *Kriminalistika*. 2 přepracované a doplněné vydání. Praha: C. H. Beck, 2004. s. 407.
[15] PORADA, Viktor, a kol. *Kriminalistická metodika vyšetřování…. s. 11-12.*
[16] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování*. Plzeň: Aleš Čeněk, 2015. s. 166. srov. PORADA, Viktor, a kol. *Kriminalistická metodika vyšetřování….* s. 11-13. Srov. MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. *Kriminalistika…..* s. 407.
[17] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování*. Plzeň: Aleš Čeněk, 2015. s. 166 – 171.

z tzv. obecných metodik, které nalezneme v učebnicích kriminalistiky, protože tento obecný "základ" se mění minimálně nebo se nemění vůbec, a v některých případech budou obecné metodiky doplněny o poznatky z kriminalistické praxe, které mohou být uveřejněny.

Metodiky vyšetřování nepřístupné veřejnosti jsou takové, které vytváří PČR sama. Jedná se o poznatky z praxe, které jsou využívány tak, aby metodiky reagovaly na aktuální dění ve společnosti a na způsoby páchání kriminality. Metodiku pro oblast kyberkriminality, ale i pro další oblasti kriminality vytváří Úřad služby kriminální policie a vyšetřování, který spadá pod Policejní prezidium České republiky. Tento úřad vydává speciální metodiky, přičemž ne vždy musí být jejich autorem. Pokud dostane podnět z jiných útvarů, tak jejich práci přezkoumá, popřípadě doplní, a poté vydá metodiku pro konkrétní typ trestné činnosti, např. metodika vyšetřování podvodných e-shopů nebo metodika vyšetřování ransomware. Metodiku, kterou tento úřad vydává, může vytvářet buď Národní centrála organizovaného zločinu, a ta se obvykle zaměřuje na čistou kyberkriminalitu, např. týkající se malware, ransomware apod., nebo ji může zpracovat KŘP nebo samotný Úřad služby kriminální policie a vyšetřování. Důvodem, proč tyto metodiky nejsou veřejné, je to, že v nich policie aplikuje své tzv. know how, které by v případě proniknutí na veřejnost zásadně znesnadnilo vyšetřování tohoto druhu trestné činnosti. Mohlo by totiž pachatele upozornit na oblasti, z nichž se dají čerpat významné důkazy pro trestní řízení, popřípadě by mohlo upozornit na možnost, jak páchat trestnou činnost tak, aby byla pro OČTŘ nezjistitelná.[18]

2.3.1 Zvláštnosti prvotních vyšetřovacích a operativně pátracích úkonů

Odborná veřejnost se ve svých názorech v zásadě shoduje na tom, že vzhledem k rozsahu trestné činnosti spadající do kategorie kyberkriminality a k odlišnému charakteru stop, které u jednotlivých druhů trestných činů vznikají, se prvotní operativně pátrací a vyšetřovací úkony mohou lišit. Významným způsobem tyto zvláštnosti ovlivňuje, zda jde o jednání pachatelů vnitřních či vnějších a zda jde o trestnou činnost latentní či zjevnou a další. Rovněž tyto zvláštnosti ovlivňuje i to, zda kriminalisticky relevantní informace (stopy) požívají ochrany státem uznávaného tajemství, a jestliže ano, je nezbytné zajistit souhlas se zajišťováním takovýchto skutečností, popřípadě rozhodnutí o udělení souhlasu příslušného orgánu.[19] Odborná veřejnost se rovněž shoduje na tom, že: *„při vyšetřování počítačové trestné*

[18] Informovaný zdroj z prostředí PČR.
[19]PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality*. Praha: Policejní akademie České republiky, 1998. s. 26. shodně v KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika…* s. 351-356. shodně též v PORADA, Viktor a kol. *Kriminalistika Technické, forenzní a kybernetické aspekty*. Plzeň: Aleš Čeněk, 2016. s. 797 – 799.

činnosti je potřebné od samého počátku postupovat rychle, uvážlivě, protože pachatelé této trestné činnosti jsou zpravidla velmi kvalifikovaní a znalí počítačových operací, které obvykle přesahují znalosti policejních orgánů a vyšetřovatelů. Je proto nezbytné, aby policejní orgány a vyšetřovatelé, ale i pracovníci služby kriminální policie od počátku objasňování spolupracovali s počítačovými experty."[20] Za hlavní úkol při prvotních úkonech lze označit zabránění výmazu dat, obnovení vymazaných dat a informací, popřípadě zabránění šíření viru. *„Mezi prvotní a neodkladné úkony v počátečních fázích realizace vyšetřování počítačové kriminality patří zejména: - přijetí oznámení o trestném činu, - vyžádání potřebných vysvětlení, - vydání a odnětí věci důležitých pro trestní řízení, ohledání místa činu, ale zejména domovní prohlídky a prohlídky jiných prostor, - vyžádání expertíz z oboru výpočetní techniky, účetnictví a provedení zajišťovacích úkonů pro tyto expertízy, - vyhledávání elektronických (počítačových stop) stop a důkazů, - posouzení rozsahu informace pro media a veřejnost apod."*[21] V této kapitole se budu podrobněji věnovat jen institutu konzultanta, technika a znalce. Domovní prohlídce a prohlídce jiných prostor se věnuji ve čtvrté kapitole. Pokud se v této kapitole mluví o vyšetřování, je třeba jej chápat v širším významu, a nejde jen o část trestního řízení po zahájení trestního stíhání.

Jelikož se jedná o velice specifický druh kriminality a je potřeba mít rozsáhlé znalosti v této oblasti, OČTŘ musí již během počátku trestního řízení obvykle využívat odborné vyjádření od příslušných orgánů, znalecké posudky apod. Mezi tyto odborníky se řadí experti v oboru, odborné firmy, vědecko-výzkumné a univerzitní instituce, zájmová sdružení, popřípadě další subjekty, které jsou schopny odpovědět na odborné otázky. Tito odborníci jsou v postavení konzultanta policejního orgánu, znalce nebo poskytovatele odborného vyjádření.[22]

2.3.1.1 Konzultant

Přibrání konzultanta je umožněno ustanovením § 157 odst. 3 TŘ. Tuto možnost má jak státní zástupce, tak policejní orgán, přičemž se dá využít jen v případě, že se jedná o věc závažnou nebo skutkově složitou. V případě využití konzultanta musí mít OČTŘ na paměti, že tento institut má své limity a je nutné odlišovat funkci konzultanta od funkce znalce či od funkce konzultanta znalce. Konzultant totiž může být zapsán v seznamu znalců pro konkrétní obor.

[20]PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování*... s. 26.
[21] PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování*... s. 26. shodně v KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika*... s. 351-356. shodně též v PORADA, Viktor a kol. *Kriminalistika Technické, forenzní*.... s. 797 – 799. srov. s PORADA, Viktor, a kol. *Kriminalistická metodika*… s. 190-193.
[22] SMEJKAL, Vladimír. *Kybernetická kriminalita*... s. 724-725.

Pokud je znalec požádán OČTŘ, aby vystupoval v trestním řízení jako konzultant, pak již v dané věci nemůže podat znalecký posudek, jelikož by byl vyloučen z důvodu ustanovení § 105 odst. 2 TŘ, a to pro svůj vztah k projednávané věci.[23] Tento znalec je rovněž ze stejného důvodu vyloučen z podání odborného vyjádření k projednávané věci ze stejného důvodu, z jakého je vyloučen z podání znaleckého posudku.[24] K dané problematice se vyjadřoval Vrchní soud v Olomouci a ve svém usnesení uvádí: *„Smyslem činnosti konzultanta je poskytnout pomoc orgánu činnému v trestním řízení v závažných a skutkově složitých věcech zejména v tom, aby se z hlediska odborných znalostí náležitě orientoval ve skutkových okolnostech a mohl zaměřit dokazování správným směrem. Přibráním konzultanta podle § 157 odst. 3 tr. ř. a § 183 odst. 2 tr. ř. však nelze nahrazovat postup podle § 105 a násl. tr. ř. Pokud se i v důsledku činnosti konzultanta ukáže potřeba odborných znalostí k objasnění některé skutečnosti důležité pro trestní řízení, pak příslušný orgán činný v trestním řízení vyžádá buď odborné vyjádření, anebo pro složitost posuzované otázky přibere znalce (popř. znalecký ústav), neboť samotná činnost konzultanta ani její výsledek nemůže sloužit jako důkaz.“*[25] V. Smejkal považuje využívání konzultanta *„jako poměrně problematické, neboť mnohdy dochází k excesům v tom smyslu, že jeho působení ovlivňuje průběh trestního řízení neadekvátním způsobem (typicky, když je konzultantem zaměstnanec poškozeného subjektu), či dokonce může způsobit jeho nezákonnost).“*[26]

Otázku přibírání konzultantů jsem řešila s odborníky z praxe, kteří mi sdělili informace týkající se využívání tohoto institutu. V současné době institut konzultanta v souvislosti s trestnou činností spadající do oblasti kyberkriminality není využíván. PČR má své vyškolené a certifikované techniky, kteří sice nejsou znalci, ale jsou schopni na méně složité situace reagovat. V případě složitých otázek je přibírán opatřením znalec pro oblast kybernetiky dle § 105 TŘ, který si pak sám může přibrat konzultanta pro některé otázky.[27]

2.3.1.2 Certifikovaný technik působící u PČR

Certifikovaní a vyškolení technici z PČR jsou osoby, které působí v rámci PČR a jsou řazeni jako technici pod oddělením kyberkriminality pod KŘP. Tito technici jsou povoláni k zajištění dat, a to buď na místě činu, nebo v případě domovní prohlídky, popřípadě mohou

[23] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. *Trestní řád II., komentář.* 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1899. (ustanovení § 157 TŘ)
[24] ŠÁMAL, Pavel. In ŠÁMAL, Pavel a kol. *Trestní řád I., komentář.* 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1566 (ustanovení § 105 TŘ)
[25] usnesení Vrchního soudu v Olomouci ze dne 2. 1. 2014, sp. zn. 6 To 94/2013.
[26] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 726.
[27] Informovaný zdroj z prostředí PČR.

provést základní úkony, ke kterým není potřeba přibrání znalce, např. pokud je potřeba z komunikace vyselektovat e-maily nebo pokud je potřeba vyselektovat z harddisku závadový materiál v podobě dětské pornografie apod. Pokud například technik zajistí při domovní prohlídce nebo na místě činu harddisk a potřebuje udělat tzv. image disku, přizve si na své pracoviště podezřelého a v případě, že je zastoupen obhájcem, tak i jeho obhájce, popřípadě se účastní jen obhájce. Za jejich přítomnosti vezme technik zajištěný harddisk a připojí ho na speciální přístroj Falcon Forensic NEO, od výrobce Logicube Inc., na nějž se připojí i další harddisk, na který se bude dělat tzv. image disku[28] tohoto zajištěného harddisku. Tento přístroj se i s harddisky vloží do tzv. Rackovy skříně,[29] která se za přítomnosti podezřelého, obhájce, popřípadě obou, zapečetí a pečeť se vyfotografuje. Pak se čeká několik hodin, než se vytvoří image disku. Poté se znovu přizve podezřelý či jeho obhájce, popřípadě oba, tato skříň se rozpečetí a harddisky se i s přístrojem ze skříně vyjmou a odpojí. Image disku pak technik dále využívá při svém zkoumání. Výstupem jejich práce je protokol o ohledání dat nebo protokol o zajištění dat v souladu s ustanovením § 55 TŘ. Pokud je však potřeba provést složitější zkoumání, musí OČTŘ přibrat znalce. Tito technici k tomu, aby mohli provádět zajišťování dat, potřebují získat certifikaci. Tu získávají u Útvaru policie pro vzdělávání a služební přípravy, jde např. o školící centra v Pardubicích, Holešově a další. Výuku obvykle vedou znalci, kteří působí u KÚP. Po dokončení získávají technici certifikát, jímž je osvědčení k provádění kriminalisticko-technických úkonů při zajišťování výpočetní techniky a digitálních dat na místě jejich nálezu. Tito technici začali být využíváni přibližně od roku 2011. Umožnily to finance určené pro potírání kyberkriminality, díky kterým získala PČR lepší software a hardware vybavení. Dalším důvodem jejich využívání jsou nemalé finance, které stojí znalecké posudky, a také časová vytíženost OKTE a KÚP.[30]

Digital Evidence First Responder (DEFR) *„…je osoba, která je oprávněná, vyškolena a kvalifikována ke sběru a hledání digitálních důkazů na místě činu.“*[31] Jedná se o pojem, obsažený v normě z roku 2012, kterou Úřad pro technickou normalizaci vyhlásil jako českou technickou normu ČSN EN ISO/IEC 27037 s názvem Informační technologie - Bezpečností techniky - Směrnice pro identifikaci, sběr, získávání a uchovávání digitálních důkazů, která

[28] Image harddisku je soubor nebo několik souborů, který obsahuje přesnou kopii pevného disku, ze kterého byl tento image vyroben, včetně funkčního operačního systému (pokud byl na disku, ze kterého image pochází), instalovaných programů, uživatelských nastavení a dat.
[29]Rackova skříň je standardizovaný systém umožňující přehlednou montáž a propojování různých elektronických a elektrických zařízení (např. harddisky, mobilní telefony, switche, počítačové servery apod.). Rovněž označován jako stojanový rozvaděč.
[30] Informovaný zdroj z prostředí PČR.
[31] SMEJKAL, Vladimír. *Kybernetická kriminalita…..* s. 700-701.

vešla v účinnost v únoru roku 2017. Hlavním úkolem DEFR je postupovat při zajišťování digitálních důkazů způsobem, který zajistí zachování integrity a spolehlivosti digitálních stop.[32] Jeho činnost v současné době provádí zejména certifikovaní technici působící v rámci PČR.

2.3.1.3 Znalec

Znalec je osoba, která má v trestním řízení objasnit určitou skutečnost, jež je pro dané řízení nezbytná. Znaleckou činnost vykonává soudní znalec, který je zapsán v seznamu soudních znalců, nebo ji může vykonávat znalecký ústav.[33] Nejčastěji se jedná o znalce z oboru kybernetika, odvětví výpočetní technika, nebo kybernetická odvětví různá.[34] Při vyšetřování kyberkriminality ovšem mohou nastat situace, kdy bude potřeba znalecký posudek z jiných oblastí, např. z oblasti ekonomie, psychologie, psychiatrie apod. OČTŘ by měly při vybírání znalce brát zřetel na jeho obor a odvětví, kterým se zabývá, a zjistit, jestli položené otázky spadají pod jeho zaměření a zdali je dostatečně kvalifikovaný, aby na jimi položené otázky odpověděl. Rovněž by měly zjistit časovou flexibilitu znalce a jeho možnost vypracovat znalecký posudek v potřebném čase. Podle názoru V. Smejkala by OČTŘ měly brát i ohled na renomé znalce.[35]

Znalecký posudek je výstupem znalce, který byl přibrán OČTŘ opatřením dle ustanovení § 105 an. TŘ, popřípadě výsledkem jeho činnosti na základě zadání od poškozeného či podezřelého, obviněného apod. Osoba, jež znalecký posudek zadává, formuluje otázky, na které má znalec odpovědět. Nejčastěji kladené otázky znalcům ze strany OČTŘ při vyšetřování kyberkriminality se týkají složitější analýzy dat, analýzy řetězců dat, dohledání škodlivého software na přístroji (např. malware, trojský kůň), hardwarové struktury dat nebo zda došlo ke smazání nějakých dat. Dále jsou přibíráni znalci z odvětví ekonomie, a to typicky pro objektivizaci škody, objektivizaci ceny obvyklé u přístroje, softwaru apod. V případě vyšetřování mravnostních trestných činů páchaných v oblasti kyberkriminality se často přibírají znalci z oblasti psychologie a psychiatrie, kteří zkoumají příčetnost pachatele, jeho rozumovou a mravní vyspělost apod. Znalecké posudky čistě z oblasti kyberkriminality provádí pro OČTŘ nejčastěji KÚP nebo OKTE, popřípadě soukromý znalec. KÚP je využíván pro velmi složité otázky, OKTE se využívá dle spádovosti KŘP, takže např. KŘP Olomouckého kraje musí přednostně využívat OKTE ve Frýdku-Místku. Ale v případě, že je toto pracoviště přetížené

[32] SMEJKAL, Vladimír. *Kybernetická kriminalita…* .s. 700-701.
[33] KOLOUCH, Jan. *CyberCrime…* . s. 451-452.
[34] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 732.
[35] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 735.

a vypracování znaleckého posudku by trvalo příliš dlouho, lze domluvit i jiné než spádové OKTE např. pro KŘP Olomouckého kraje by takovým mohlo být OKTE v Hradci Králové. Znalci ze soukromého sektoru jsou využíváni v případě, kdy jsou výše uvedené ústavy přetížené, nebo pokud je znalec zkušenější, má v dané oblasti větší přehled a je schopen znalecký posudek zpracovat v relativně rychlém časovém období.[36] Znalecký posudek má velmi významné místo v rámci dokazování v trestním řízení. Ústavní soud však již několikrát judikoval, že znaleckému posudku nelze přikládat větší sílu než jiným důkazům jen z důvodu, že se jedná o znalecký posudek, i tento musí být podroben volnému hodnocení důkazu, a to se tejnou pečlivostí, jakou soud hodnotí jiné důkazy. Dále klade důraz na to, že je potřeba hodnotit celý proces vytváření znaleckého posudku.[37]

2.3.2 Zvláštnosti následné etapy vyšetřování

Hlavní zvláštnost následné etapy vyšetřování spočívá v její specifické oblasti, která je předmětem trestního řízení. V této etapě vyšetřování OČTŘ prověřují jimi vytyčené vyšetřovací verze a v průběhu takového prověřování využívají typicky následující vyšetřovací úkony: výslech podezřelého v trestní věci, výslechy svědků, vyžádání si znaleckých posudků zpracovávaných v různých oborech nezbytných k objasnění trestného činu.[38] V této podkapitole se budu podrobněji zabývat výslechem podezřelého a svědků.

Výslech podezřelého má pro objasnění trestného činu význam, jelikož ten by měl mít nejlepší poznatky o způsobu jeho spáchání, o průběhu páchání trestného činu apod., a to za předpokladu, že podezřelý vypovídá pravdu. Výslech podezřelého je proto typický vyšetřovací úkon, který OČTŘ provádí při vyšetřování jakéhokoli spáchaného trestného činu a v oblasti kyberkriminality tomu není jinak. [39] Vede se v souladu s ustanovením § 92 an. TŘ. Avšak často se stává, že podezřelý využije svého zákonného práva a odmítne v dané věci vypovídat. Pokud však podezřelý vypovídá, měla by být osoba, která vede výslech, řádně připravená, jelikož v případě podezřelého se obvykle jedná o osobu s vysoce kvalitními znalostmi v oblasti informačních a komunikačních technologií, a dá se předpokládat, že v počátečních etapách vyšetřování bude celou věc bagatelizovat a popírat. Proto je pro vedení takového výslechu nezbytná příprava, kterou je nutné v případě potřeby doplňovat. Čím více je věc skutkově složitá z hlediska odborných znalostí informačních a komunikačních technologií, tím je

[36] Informovaný zdroj z prostředí PČR.
[37] nález Ústavního soudu ze dne 30. 4. 2007, sp. zn. III ÚS 299/06.7 shodně v nálezu Ústavního soudu ze dne 24. 7. 2013, sp. zn. I. ÚS 4457/12.
[38] PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování…* s. 36.
[39] Tamtéž.

nezbytnější přibrání znalce či konzultanta z příslušného oboru, a to nejprve ke konzultacím, a popřípadě i k výslechům obviněného.[40] J. Kolouch doporučuje: *„…je vhodné zaměřit se na zjištění těchto skutečností: - osobní, majetkové, výdělkové poměry a předchozí tresty; - informace vztahující se k úmyslu spáchat trestný čin; - informace o podílu osoby na trestném činu, případně existenci spolupachatelů (jejich podíl na trestné činnosti); - informace o způsobu spáchaní trestného činu (otázky týkající se utajení trestné činnosti, vlastního postupu pachatele, atd.); - využití sociálního inženýrství či jiných netechnických prostředků; - popis mechanismů zásahu do počítačového systému či programového vybavení počítačového systému (následky toho zásahu – jaká data byla pozměněna, potlačena, odstraněna, atd.); - jakým způsobem se pachatel dozvěděl, kterou činnost je třeba v rámci kybernetického útoku provést, či zda jde o jeho vlastní invenci; - jakým způsobem maskoval svoji činnost aj; - informace o tom, co bylo trestným činem získáno (finanční prostředky, informace, nelegální materiály – např. dětská pornografie aj.) a jak byl tento zisk využit.“*[41]

Výslech svědků je rovněž typickým vyšetřovacím úkonem, který OČTŘ taktéž využívají při vyšetřování trestných činů. J. Kolouch rozděluje svědky do dvou skupin, a to na svědky odborníky a svědky neodborníky.[42] Rovněž je při výslechu svědků nezbytné, aby vyslýchající osoba byla řádně připravená, obzvlášť v případě výslechu svědků odborníků. I zde je namístě v určitých případech zvažovat přibrání znalce. Výslech svědka se řídí ustanovením § 99 an. TŘ.

[40] PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování…* s. 37-38. shodně v PORADA, Viktor, a kol. *Kriminalistická metodika vyšetřování….* s. 194. shodně v PORADA, Viktor a kol. *Kriminalistika Technické, forenzní….* s. 360. srov. s KOLOUCH, Jan. *CyberCrime…* s. 408-409.
[41] KOLOUCH, Jan. *CyberCrime…* s. 409.
[42] Tamtéž.

3 Digitální stopa

Po prostudování většího množství literatury docházím k závěru, že učebnice kriminalistiky se shodují až na mírné odlišnosti na vymezení pojmu stopa, na jejím dělení a vlastnostech. Proto jsem se rozhodla citovat názory z jednoho zdroje, který se shoduje s ostatními publikacemi. Navíc autoři, kteří se k této problematice vyjadřují v ČR, jsou stále stejní a novější publikace obsahují jen nepatrné doplnění, přičemž ale základní vymezení pojmu stopa a její dělení zůstává stejné.

3.1 Pojem stopa

Pojem stopa má více významů. Můžeme je dělit na stopy kriminalistické, stopy forenzní a jinak využitelné stopy. Z kriminalistického hlediska se jedná o: „*jakoukoli změnu v materiálním prostředí nebo ve vědomí člověka, která je zjistitelná, zajistitelná a využitelná současnými metodami, prostředky a postupy mající příčinnou, prostorovou nebo časovou souvislost s kriminalisticky relevantní událostí.*“[43] V odborné literatuře se lze setkat s řadou definic stopy, ale všechny se shodují ve třech podmínkách, které musí stopa splnit, aby byla kriminalisticky relevantní. Jde o tyto podmínky: stopa musí vzniknout v souvislosti s kriminalisticky relevantní událostí, přičemž jde o souvislost místní, časovou a zejména musí existovat příčinná souvislost. Dále stopa musí existovat od svého vzniku do zajištění. A poslední podmínkou je, že stopa musí být vyhodnotitelná současnými kriminalistickými metodami.[44] Typickým příkladem jsou stopy bipedální lokomoce ve sněhu, přičemž tyto stopy jsou vysoce nestálé a jejich zjistitelnost a zajistitelnost je vysoce závislá na vnějších vlivech, např. na počasí. *„Z pojmu kriminalistické stopy lze tedy vyvodit tyto obligatorní znaky: změnu (materiální i ve vědomí člověka), změnu v příčinné, časové nebo místní souvislosti s kriminalisticky významnou událostí, změnu, kterou lze vyhledat, fixovat, zajistit a informaci dekódovat.*“[45]

3.1.1 Dělení kriminalistických stop

Podle základního dělení lze rozlišit stopy paměťové - ve vědomí a stopy materiální. Paměťové stopy je možné dále dělit na paměťové stopy dle počitků (zrak, chuť, sluch, čich, hmat) a stopy dle doby uchovávání v paměti osoby (krátkodobá, střednědobá, dlouhodobá).

[43] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, 2012. s. 58.
[44] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy…* s. 57- 58.
[45] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy….* s. 58.

Materiální stopa se dále dělí na stopy odrážející vnější struktury působícího objektu, stopy odrážející vnitřní struktury působícího objektu, stopy odrážející funkční struktury působícího objektu a stopy kombinované. Dále zná kriminalistika ještě dělení z hlediska praxe, a to podle mechanismu vzniku (např. stopy chemické, tepelné, hnilobné, biologické, pachové, atd.), podle oboru kriminalistické expertní činnosti (daktyloskopické, trasologické, balistické, atd.) a podle druhu informace, kterou stopa přináší o objektu, jenž ji zanechal, tzn. stopy paměťové a materiální, jak již bylo výše uvedeno.[46] V návaznosti na to je třeba uvést názor V. Porady a J. Strause, kteří uvádí: *„je vhodné připomenout, že neexistují žádné všeobecně uznávané systémy dělení kriminalistických stop, které by měly obecnou platnost. V minulosti takovéto snahy existovaly, ale jejich výsledek byl neuspokojivý. Pro kriminalistickou praktickou činnost není totiž důležité určení (taxativní výčet) kriminalistických stop, ale potřeba se zabývat všemi kriminalistickými stopami, které byly ke konkrétní události nalezeny.“*[47] Každá kriminalistická stopa má svoji kriminalisticko–technickou a kriminalisticko–taktickou důkazní hodnotu (význam). Kriminalisticko–technická hodnota spočívá v kvalitě stopy a možnosti jejího využití pro účely kriminalistické identifikace, a to především individuální identifikace objektu, který stopu vytvořil. Kriminalisticko–taktická hodnota spočívá v míře pravděpodobnosti, že stopa pochází od pachatele, a v kriminalistickém využívání způsobu páchání trestné činnosti. To nám umožňuje předvídat fyzické a psychické vlastnosti a schopnosti pachatele, jeho dovednosti a znalosti. Důkazní hodnota spočívá v možnosti využití stopy v trestním řízení jako důkazu dle postupu podle TŘ.[48]

3.2 Digitální stopa

Digitální stopa navazuje na kriminalistické učení o stopách a doplňuje jej o vlastnosti, které jsou charakteristické pro oblast kyberkriminality. V. Smejkal ve své knize Kybernetická kriminalita definuje digitální stopu takto: *„Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává záznamy (odrazy) o své činnosti. V oblasti IS/IT jsou tedy především digitální stopy, které lze definovat podle SWGDE (Scientific Working Group on Digital Evidence) jako jakékoliv informace s vypovídající hodnotou, uložené nebo přenášené v digitální podobě.“*[49] Autoři knihy Kriminalistika: Kriminalistická taktika a metodika vyšetřovaní, Zdeněk Konrád a kol., nepoužívají pojem digitální stopa, ale

[46] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy….* s. 59-61.
[47] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy….* s. 60.
[48] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy….* s. 61-63.
[49] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 697-698.

počítačová stopa, kterou definují jako: *„informaci nebo změnu na materiálním nosiči, vzniklou v souvislosti s trestným činem, při jehož spáchání byla využita výpočetní technika, a která je zjistitelná a využitelná pomocí současných metod, prostředků, postupů a operací.“*[50] Dle mého názoru je definice V. Smejkala vhodnější, jelikož je obecnějšího rázu a za digitální stopu považuje i stopy, které nutně nesouvisí s trestnou činností. Navíc Z. Konrád používá pojem počítačová stopa, přičemž můžeme toto pojmenování označit za nesprávné či nepřesné, jelikož není schopno pojmout širokou škálu a rozmanitost výpočetních technologií, které v současné době zanechávají stopy a které jsou svou strukturou a obsahem srovnatelné s počítačovými stopami. Opět by tento pojem mohl evokovat, že se daná stopa, která nebyla vytvořena počítačem nebo notebookem, nedá pod tento pojem podřadit. Proto je dle mého názoru vhodnější užívat v souvislosti s kyberkriminalitou pojem digitální stopa. Tento pojem v kriminalistickém smyslu je nutné odlišit od obecného pojmu digitální stopy, kdy se jedná o zanechávání informací o uživateli na internetu při obyčejném užívání internetu (surfování) či používání sociálních sítí nebo nakupování. Mohou to být například příspěvky do různých diskuzí či nahrávání fotek na sociální sítě, ale rovněž informace o IP adrese či poskytovateli připojení.[51] Tyto digitální stopy mohou být rovněž relevantní pro kriminalistické zkoumání. Oba pojmy se částečně překrývají, ale nejde o synonyma, protože kriminalistické pojetí digitální stopy je širší, zatímco obecné pojetí souvisí s používáním internetu.

Digitální stopy rovněž vykazují tři základní vlastnosti (obligatorní znaky), které musí vykazovat každá kriminalistická stopa, tzn. stopa vznikla v souvislosti s kriminalisticky relevantní událostí, existuje od svého vzniku do zajištění a je vyhodnotitelná současnými kriminalistickými metodami. *„Odráženými objekty v této souvislosti jsou osoby a prostředky, které působí nebo vyvolávají aktivity. V souvislosti s digitálními stopami jsou typickým příkladem uživatele výpočetní a digitální techniky a tato technika samotná. Prostředek odrazu jsou vlastnosti odrážených objektů a objektivní okolnosti (např. vlastnosti, znalosti a dovednosti osoby, které se odrážejí výběrem softwaru nebo zařízení pro činnost, úroveň jeho ovládání atd.). Odrážející objekty a subjekty je vnější materiální prostředí a vědomí lidí, na které odrážené objekty za pomoci prostředku odrazu působí (např. technologie v konečném důsledku působí na záznamové médium, na které se ukládají data).*[52] Kromě výše uvedených digitálních stop můžeme v rámci trestné činnosti související s kyberkriminalitou narazit na stopy paměťové (ve

[50] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika…* s 342.
[51] *Digitální stopa*. [online]. internetembezpecne.cz, [cit. 27. 11. 2019]. Dostupné na < https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/>.
[52] PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy…* s 294.

vědomí osob, které trestnou činnost vnímaly) a samozřejmě i na klasické stopy (daktyloskopické, mechanoskopické atd.).

3.2.1 Vlastnosti digitálních stop

Digitální stopy mají základní vlastnosti stop, ale i další vlastnosti, které jsou odlišné od klasických stop. Proto je nezbytné a důležité, aby se během jejich zjišťování a zajišťování dbalo na dodržování správných postupů, aby stopy byly získány legálním způsobem, řádně se zadokumentovaly, aby mohly být případně použity v řízení před soudem. Zvláštní vlastnosti těchto stop bohužel často negativním způsobem ovlivňují práci OČTŘ. *„Patří sem zejména: a) nehmotnost digitálních stop, b) latentnost digitálních stop, c) časová trasovatelnost digitálních stop, resp. manipulovatelnost s časem v počítačových systémech, d) informační hodnota digitálních stop, e) velmi nízká životnost digitálních stop, f) uchování a kvalita archivních záznamů, g) velké objemy digitálních dat, h) vysoká datová hustota digitálních záznamů, i) dynamika vývoje digitálních technologií, j) dynamika činnosti informačních systémů, k) komplexnost prostředí, l) velký geografický rozsah prostoru s digitálními stopami, m) dostupnost kvalitní ochrany digitálních dat, n) možnost automatizace při identifikaci digitálních stop, o) možnosti změny identity pachatele v kyberprostoru, p) obnovitelnost digitálních stop, q) problém originality důkazů, r) nedůvěra v důkazní sílu digitálních stop.“*[53] Díky těmto vlastnostem musely OČTŘ reagovat na vývoj informačních a telekomunikačních technologií a naučit se vyhledávat takové stopy, zajišťovat je a vyvinout vhodné metody a postupy při jejich zkoumání tak, aby tyto stopy nebyly znehodnocovány a mohly být upotřebitelné v soudním řízení. Proto musí být striktně dodržovány zásady při vyhledávání a zajišťování digitálních stop. *„Klíčovou je právě otázka prokazatelnosti, že se stopa nacházela na určitém místě a že v procesu od jejího zajištění do ukončení znaleckého zkoumání nebyla žádným způsobem modifikována.“*[54] Proto se zajišťované digitální stopy označují kontrolní sumou,[55] aby následně pachatel trestného činu nemohl tvrdit, že se stopou bylo během zkoumání manipulováno a byl do ní vložen další obsah.[56]

[53] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 698.
[54] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 706.
[55] Kontrolní suma je elektronická pečeť, která je jedinečným identifikátorem, v případě, že dojde ke změně dat, nikdy nemůže být stejná.
[56] Informovaný zdroj z prostředí PČR.

3.3 Elektronický důkaz

Česká právní úprava nepracuje s pojmem elektronický důkaz. V TŘ nalezneme ustanovení § 89 odst. 2 TŘ, které konstatuje, že: *„…za důkaz může sloužit vše, co může přispět k objasnění věci….“* Dále věta pokračuje demonstrativním výčtem možných důkazních prostředků. Pod toto ustanovení lze bez problému podřadit i elektronické důkazy.

Na první pohled by se mohlo zdát, že není potřeba pro trestní řízení samostatně upravovat a definovat pojem elektronický důkaz v právním řádu, jelikož současná právní úprava tento pojem zahrnuje v ustanovení § 89 odst. TŘ.

Avšak můj názor je takový, že definování tohoto pojmu v právním řádu by bylo přínosem pro zákonodárce a OČTŘ. Nepovažuji jeho definování za nadbytečné, mělo by vést k zefektivnění potírání a objasňování trestné činnosti a zjednodušit tak práci zákonodárce.

S pojmem elektronický důkaz pracuje například Úmluva o počítačové kriminalitě ze dne 23. 11. 2001, která v čl. 14. odst. 2 stanoví, že pravomoci a postupy z této Úmluvy lze užít na zajištění důkazů o trestném činu, které jsou v elektronické formě. Toto ustanovení ovlivňuje procesní postupy, které byly do českého právního řádu implementovány z této Úmluvy. Zajímavý dopad by definování tohoto pojmu mohlo mít v případě ustanovení § 7b TŘ, které by se tak dalo užít na všechny elektronické důkazy. Problematice ustanovení § 7b TŘ se podrobněji věnuje čtvrtá kapitola. S tímto pojmem dále pracuje i unijní úprava, například v návrhu Nařízení Evropského Parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech. Toto nařízení má usnadnit, zjednodušit a zrychlit obstarávání elektronických důkazů, které jsou dnes získávány dle evropského vyšetřovacího příkazu.[57] Tato unijní úprava by mohla značně zrychlit spolupráci na mezinárodní úrovni, ale to, že česká právní úprava nepracuje s pojmem elektronický důkaz, může dle mého názoru činit značné obtíže při vykládání toho, na co vše půjde výše uvedená unijní úprava užít, co vše ještě pod pojem elektronický důkaz spadá a co již za elektronický důkaz považovat nemůžeme. Proto si myslím, že by česká právní úprava měla s tímto pojmem pracovat a nevidím v jeho definování v právním řádu nadbytečnost, spíše naopak potřebu.

Myslím si, že zakotvení pojmu elektronického důkazu do právního řádu může usnadnit práci zákonodárce, který pak nebude muset u některých procesních institutů složitě vyjmenovávat, na které trestné činy jej lze užít. V případě zakotvení tohoto institutu v zákoně se takovému zdlouhavému vysvětlování může předejít.

[57] *Bezpečnostní unie: Komise usnadňuje přístup k elektronickým důkazům*. [online]. ec.europa.eu, 17. duben 2018 [cit. 28. 3. 2020]. Dostupné na < https://ec.europa.eu/commission/presscorner/detail/cs/IP_18_3343>.

Co si tedy lze představit pod pojmem elektronický důkaz? Dle definice zmíněné v knize Digital Evidence and Computer crime je elektronický důkaz jakýkoli důkaz uložený nebo přenášený v digitální podobě.[58] Evropská Komise na svých internetových stránkách pojem elektronický důkaz vysvětluje jako různé typy dat v elektronické formě, které jsou relevantní pro trestní řízení a zahrnují data jako e-maily, textové zprávy, fotografie, videa a další kategorie dat.[59]

Definice elektronického důkazu by měla do značné míry vycházet z definice digitální stopy, měla by reflektovat vlastnosti digitálních stop, zejména to, že mají nestálou povahu. Dle mého názoru lze pojem elektronického důkazu definovat takto: *Elektronický důkaz jsou jakákoli data, která jsou způsobilá přispět k objasnění věci.* Přičemž záměrně zde volím slovo data, jelikož je vhodnější než užití pojmu "informace v digitální podobě", a to z důvodu, že pojem data zahrnuje data jak ve formě digitální, tak i ve formě analogové.[60]

[58] CASEY, Eoghan. *Digital evidence and Computer crime.* Third Edition. London: Elsevier Books, 2011.. s 7.
[59] *Frequently Asked Questions: New EU rules to obtain electronic evidence*. [online]. ec.europa.eu, ze dne 17. května 2017 [cit. 30. 3. 2020]. Dostupné na < https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345>.
[60] CASEY, Eoghan. *Digital evidence and Computer crime….* s. 7.

4 Zajištění důkazních prostředků

4.1 Domovní prohlídka

Ochrana soukromí a nedotknutelnost obydlí je zaručena ústavním právem a je zakotvena v LZPS, a to v článcích 2, 7 a 12, které tuto ochranu garantují. Tato práva jsou rovněž zakotvena v Listině základních práv EU, a to v článku 7. Domovní prohlídka proto znamená podstatný zásah do těchto základních práv, a to zejména do osobní a domovní svobody, a připouští se jen v zákonem stanovených případech za dodržení litery zákona. Z judikatury ÚS vyplývá, že: *„domovní svoboda jako ústavní zaručené právo plynoucí z čl. 12 Listiny základních práv a svobod svou povahou a významem spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní a dalšími ústavně zaručenými základními právy dotváří osobnostní sféru jedince, jehož individuální integritu, jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec, je nutno respektovat a důsledně chránit. Jestliže ústavní pořádek České republiky připouští průlom této ochrany, děje se tak toliko a výlučně v zájmu ochrany demokratické společnosti jako takové, případně v zájmu ústavně zaručených základních práv a svobod jiných. Přípustnost domovní prohlídky v obydlí (jiných prostorách) pachatele nebo důvodně podezřelého (§ 82 a násl. TrŘ) je však třeba chápat jako výjimku, která nadto vyžaduje restriktivní interpretaci zákonem stanovených podmínek její přípustnosti.“*[61] Tuto judikaturu ÚS potvrzuje a rozvíjí ve svých dalších nálezech, např. I. ÚS 2787/13, I. ÚS 1466/15, I. ÚS 2024/15 atd.

Rovněž sama LZPS v čl. 12 odst. 2 stanoví, že domovní prohlídka je přípustná jen pro účely trestního řízení a dále odkazuje na zákon.

Tento procesní institut patří mezi zajišťovací úkony. Jedná se o úkony, které směřují k zajištění osob či věcí důležitých pro trestní řízení. Domovní prohlídku lze provádět buď v klasickém režimu, nebo jako neodkladný nebo neopakovatelný úkon. Jako neodkladný a neopakovatelný úkon se z hlediska praxe provádí domovní prohlídka častěji, jelikož potřeba zajistit věci nebo osoby důležité pro trestní řízení často nastává již v době, kdy ještě není nikdo osobou obviněnou a nebylo zahájeno trestní stíhání. V případě, že je domovní prohlídka prováděna jako neodkladný nebo neopakovatelný úkon, musí být v příkazu domovní prohlídky uvedeno odůvodnění neodkladnosti či neopakovatelnosti takového úkonu.[62] Při provádění

[61] nález Ústavního soudu ze dne 22. 5. 1997, sp. zn. III ÚS 287/96.
[62] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. Trestní řád I., komentář. 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1111. (ustanovení § 82 TŘ).

domovní prohlídky jako neodkladného nebo neopakovatelného úkonu pravděpodobně nedojde k předchozímu výslechu podezřelého či obviněného. V takovém případě by měly OČTŘ po zajištění prostoru vyslechnout podezřelého nebo obviněného, zjistit, zda nevydá hledané věci či osoby dobrovolně, a pokud ne, pak teprve přistoupit k provedení domovní prohlídky.[63]

Domovní prohlídka může být zákonně provedena jen v obydlí subjektu, který je v příkazu k ní řádně označen.[64] Je možné, že se v jedné nemovitosti nachází více obydlí, ale v katastru nemovitostí nejsou zapsány žádné samostatné jednotky určené k bydlení. Nelze proto v takovém případě bez dalšího říci, že se v domě nenachází vícero obydlí. Z judikatury vyplývá, že policejní orgán má vyslechnout osobu, u níž bude provedena domovní prohlídka, a dozvědět se tak, jaké jsou poměry v domě. Výslechem mohou OČTŘ zjistit, zda se v domě nachází osoba či věc důležitá pro trestní řízení, popřípadě získat dobrovolné vydání věci.[65]

Principy a postupy, které se uplatňují u domovní prohlídky, se obdobně užijí pro prohlídku jiných prostor a pozemků.

Domovní prohlídky jsou významným nástrojem z hlediska opatřování důkazů potřebných pro trestní řízení týkající se kyberkriminality. Obvykle jsou prováděny jako prvotní úkony. V rámci této prohlídky se zajišťují např. počítače, mobily, harddisky, cloudová úložiště apod. U domovních prohlídek souvisejících s kyberkriminalitou se musí aplikovat klasické metodické zásady pro provedení domovní prohlídky, které byly vytvořeny kriminalistickou praxí. V souvislosti s touto kriminální oblastí je potřeba vhodně zvolit taktiku jejího provedení, jež je závislá na charakteru, rozsahu specifických zvláštností prověřovaného objektu a rovněž na charakteru hledaných věcí či osob. Prohlídka musí být důkladně naplánovaná a promyšlená do detailů z důvodu možnosti rychlého odstranění, zničení či zašifrování stop důležitých pro trestní řízení. Ustanovení upravující domovní prohlídky a způsob jejich provedení nalezneme v § 82 – 85c TŘ. „*Nařídit domovní prohlídku je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Domovní prohlídku provádí policejní orgán.*“ Příkaz k domovní prohlídce má povahu rozhodnutí sui generis a nejsou proti němu přípustné opravné prostředky (stížnost, odvolání atd.).[66] *„Příkaz k domovní prohlídce musí být písemný a odůvodněn. Doručí se uživateli obydlí nebo dotčených prostor nebo pozemků, a nebyl-li*

[63] Rozsudek Nejvyššího soudu ze dne 29. 3. 2000, sp. zn. 5 Tz 32/2000.
[64] nález Ústavního soudu ze dne 14. 11. 2012, sp. zn. IV. ÚS 2227/12.
[65] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. Trestní řád I., komentář. 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1112–1121. (ustanovení § 82 TŘ).
[66] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. Trestní řád I., komentář. 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1112–1121. (ustanovení § 82).

zastižen při prohlídce, bezprostředně po odpadnutí překážky, která doručení brání.“[67] Pokud je zde reálná možnost, že dojde k zajišťování dat ze vzdáleného úložiště (cloudu), je vhodnější do příkazu k domovní prohlídce tuto skutečnost rovněž uvést. Cloudová úložiště se zajišťují při domovních prohlídkách, jelikož je to nejlepší cesta, jak se k datům na nich uložených dostat. Pokud se např. cloudové úložiště nachází v USA, jedná se o složitý a finančně náročný proces jeho zajištění. V případě zajištění těchto dat formou mezinárodní právní pomoci či evropského vyšetřovacího příkazu, který by se mohl kombinovat s § 7b TŘ, jde o zdlouhavý proces, kdy mohou být data odstraněna či znehodnocena. Proto pokud je možné při domovní prohlídce zajistit cloudové úložiště (nebrání tomu např. šifrování, heslo apod.), jedná se o nejlepší způsob, jelikož je zachován moment překvapení a podezřelá osoba či další osoby nestihnou s tímto úložištěm manipulovat. Při zajišťování těchto dat se vytvoří datový otisk, který se opatří tzv. kontrolní sumou[68], aby bylo patrné, že s ním nikdo nemanipuloval.[69]

V rámci problematiky domovních prohlídek je velmi významný pojem obydlí. Tento pojem nalezneme mimo jiné v § 82 TŘ, kde se stanoví, že se jedná o prostor: *„v bytě, nebo jiné prostory sloužící k bydlení nebo v prostorách k nim náležející (obydlí) atd.“* Definici pojmu obydlí nalezneme v TZ, a to v ustanovení § 133 a z komentářové literatury vyplývá, že: *„pojem obydlí zahrnuje mimo obytných domů a bytů i obytné chaty, hotelové domy, ubytovny, vysokoškolské koleje apod., tedy veškeré prostory sloužící k bydlení lidí. Rozhodný je faktický stav bydlení, ať už jeho právním důvodem je jakýkoli titul, např. vlastnictví nemovitosti, nájemní či podnájemní vztah, anebo faktické bydlení na základě rodinných i jiných vztahů.“*[70] Příslušenstvím domu dle komentářové literatury: *„může být např. půda, sklep, uzavřený dvůr či ohrazená zahrada přiléhající k domu (R 16/1993-II.). Naproti tomu domem ani příslušenstvím k němu ve smyslu tohoto ustanovení nejsou např. kůlny, stodoly, volné přístřešky, altánky a rovněž tak domy neobydlené, opuštěné. Příslušenstvím bytu je např. uzamykatelná sklepní kóje, komora, půda.“*[71] *„Osoba, u níž má být provedena domovní prohlídka, prohlídka jiných prostor a pozemku, osobní prohlídka nebo vstup do obydlí, je povinna tyto úkony strpět.“*[72]

---

[67] POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub, a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, Právnická fakulta 2015. s. 75.
[68] Kontrolní suma je elektronická pečeť, která je jedinečným identifikátorem, v případě, že dojde ke změně dat, nikdy nemůže být stejná.
[69] Informovaný zdroj z prostředí PČR.
[70] JELÍNEK, Jiří a kol. Trestní zákoník a trestní řád s poznámkami a judikaturou. 6. aktualizované vydání podle stavu k 1. 2. 2016. Praha: Leges, 2016. s. 191.
[71] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. Trestní řád I., komentář. 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1112–1121. (ustanovení § 82 TŘ).
[72] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. Trestní řád I., komentář. 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1148. (ustanovení § 85a TŘ).

OČTŘ provádějící prohlídku by měly zjistit, kolik osob obývá danou nemovitost, jestli je tam možnost více obydlí, a co nejpřesněji tyto informace specifikovat v příkazu k domovní prohlídce. Jelikož je v souvislosti s kyberkriminalitou prováděná domovní prohlídka často označována jako neodkladný úkon, je potřeba neodkladnost řádně zdůvodnit, a právě u rodinných domů, které nemají v katastru nemovitostí vymezeny jednotky a je zde možnost více obydlí, zjistit alespoň osoby, které v místě mají bydliště. Proto musí OČTŘ před provedením domovní prohlídky zjišťovat co nejvíce informací o podezřelé osobě, kolik osob s ní žije v domácnosti, jestli se v obydlí nachází nějaké děti, zvířata, zbraně, speciální technické vybavení atd., a tomu přizpůsobit provedení domovní prohlídky. Pokud v průběhu provádění domovní prohlídky OČTŘ zjistí, že se v domě nachází další obydlí, které nebylo specifikováno v příkazu k domovní prohlídce a osoba, jíž toto obydlí náleží, nedala k provedení domovní prohlídky souhlas, provedou OČTŘ domovní prohlídku v té části, která je označena v příkazu k domovní prohlídce. V části nespecifikované v příkazu k domovní prohlídce zajistí, aby daný prostor zůstal nedotčen a aby do něj nemohly vstupovat další osoby. Poté si OČTŘ zajistí dodatečný příkaz k této části a provede zbytek domovní prohlídky. Je potřeba dodržet literu zákona v průběhu provádění domovní prohlídky, jinak by se mohly OČTŘ začít pohybovat na hraně zákonnosti takto získaných důkazů.[73]

Rovněž je potřeba zajistit příslušný počet osob s ohledem na velikost nemovitosti. Prostor musí být zajištěn tak, aby nebylo nikomu umožněno jej opustit bez svolení policejního orgánu vykonávajícího domovní prohlídku, popřípadě ovlivňovat průběh prohlídky. Rovněž je nutné sledovat chování těchto osob a znemožnit jim ničení důkazů důležitých pro trestní řízení, jelikož pachatelé kyberkriminality často mají rozsáhlé znalosti a schopnosti týkající se výpočetní techniky a jsou schopni během pár kliknutí smazat či zašifrovat důležitá data či jiné informace související s domovní prohlídkou. Rovněž by se domovní prohlídky měl účastnit i tzv. DEFR, *„který by měl postupovat tak, aby zajistil zachování integrity a spolehlivost digitálních stop.“*[74] V rámci těchto domovních prohlídek by mělo být spíše preferováno zajištění dat tzv. bitovou kopií opatřenou kontrolní sumou před zabavením celých zařízení s ohledem na zásadu přiměřenosti. Policejní orgán by se měl snažit zasahovat do subjektivních práv osob jen v nezbytném rozsahu, jelikož obrácený přístup by mohl vést k požadování náhrady škody vůči státu.[75]

[73] Informovaný zdroj z prostředí PČR.
[74] SMEJKAL, Vladimír. *Kybernetická kriminalita…* s. 701.
[75] Informovaný zdroj z prostředí PČR.

Příkaz k domovní prohlídce obsahuje automaticky i výzvu k vydání věci doličné a zároveň i příkaz k odnětí věci. Pokud nedojde k dobrovolnému vydání, obsahuje také příkaz k vydání dat z cloudu přístupného z prostoru prohlídky a v případě potřeby stažení dat z cloudu, pokud se domovní prohlídka vztahuje i na vzdálená uložiště.[76]

„Vzhledem k vysokému stupni používání internetu je nezbytná spolupráce s poskytovateli služeb a sítí elektronických komunikací – ISP providery, provozovateli serveru, poštovních služeb (freemailových – seznam.cz apod.), odkud na základě zákonného zmocnění lze získat důležité informace o struktuře a případně obsahu elektronické komunikace.“[77]

V případě provádění domovní prohlídky nebo prohlídky jiných prostor, v nichž advokát vykonává svou činnost, je nezbytná součinnost ze strany České advokátní komory, spočívající v tom, že zajistí zástupce komory, který je účasten na prohlídce. Tento zástupce uděluje souhlas k tomu, aby se OČTŘ mohly seznámit s obsahem listin, jež obsahují informace, na něž se vztahuje povinnost mlčenlivosti advokáta. Blíže viz ustanovení § 85b TŘ.

Pokud OČTŘ v případě domovní prohlídky, která není zaměřená na vyšetřování kyberkriminality, naleznou předměty výslovně neoznačené v příkazu k domovní prohlídce, jsou tyto předměty zajištěny také. K této problematice se vyjadřoval ÚS, kdy ve svém usnesení konstatoval: „*...ani v případě odůvodnění příkazů k domovním prohlídkám ani v případě postupu dle ustanovení § 78 odst. 1 tr. řádu nelze s ohledem na podstatu věci po orgánech činných v trestním řízení vyžadovat, aby a priori naprosto přesně specifikovaly všechny věci důležité z hlediska trestního řízení, jejichž existence a význam teprve vyjde najevo při faktickém provádění prohlídky. Z hlediska požadavků trestního řádu i kautel práva ústavního je dostačující, jsou-li uvedené věci následně konkretizovány v pořízených protokolech dle ustanovení 85 odst. 3 ve spojení s ustanovením § 79 odst. 5 tr. řádu, zatímco v příkazu k provedení prohlídky postačí uvést toliko určité kategorie věcí, resp. důkazů. Stejně tak nelze v dané fázi řízení s naprostou jistotou určit, zda a které z nalezených věcí skutečně souvisejí s projednávanou trestnou činností a lze vyžadovat toliko pravděpodobnost, že taková věc bude pro vyšetřování potřebná.“*[78] Postup OČTŘ je tedy takový, že tyto předměty zajistí, i když nebyly výslovně označeny, jelikož se jedná o předměty důležité pro trestní řízení. Přitom není podstatné, zda byly výslovně uvedeny v příkazu k domovní prohlídce, protože se dají podřadit

[76] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*, 2019, roč. 18, č. 3, s. 66-71.
[77] KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: Kriminalistická taktika… s.* 355-356.
[78] usnesení Ústavního soudu ze dne 13. 12. 2007, sp. zn. III. ÚS 1033/07. shodně v usnesení Ústavního soudu ze dne 28. 2. 2008, sp. zn. III. ÚS 1578/07.

pod klauzuli „*věc důležitá pro trestní řízení*“ a v souladu s ustanovením § 78 TŘ a § 79 TŘ je OČTŘ mohou v rámci domovní prohlídky odebrat a nepotřebují výslovný souhlas soudu či státního zástupce, jelikož příkaz k domovní prohlídce již tento souhlas obsahuje.[79]

4.2 Prohlídka jiných prostor a pozemků

„Po novele č. 459/2011 Sb. se na nařízení a provedení prohlídky jiných prostor a pozemků obdobně užije § 83 odst. 1 a 2.“[80] Tato novela reagovala na rozhodnutí pléna ÚS ze dne 8. 6. 2010, které rušilo ustanovení § 83a odst. 1 části věty první a věty druhé TŘ, jelikož znění tohoto ustanovení plénum nepovažovalo za ústavně konformní. Původní znění zákona umožňovalo prohlídku jiných prostor a pozemků nařídit se souhlasem předsedy senátu a v přípravném řízení ji mohl nařídit státní zástupce nebo policejní orgán, který k tomu potřeboval předchozí souhlas státního zástupce. ÚS ve svém rozhodnutí dovodil, že o příkazu k prohlídce jiných prostor a pozemku by měl rozhodovat nezávislý a nestranný orgán.[81] Dle názoru ÚS původní znění výše zmiňovaného ustanovení: „*zřetelně porušovaly v odůvodnění nálezu naznačené ústavněprávní limity (čl. 12 odst. 1 Listiny, čl. 8 odst. 1 Úmluvy o ochraně lidských práv a základních svobod a čl. 17 Mezinárodního paktu o občanských a politických právech), které je zcela nezbytné při zákonné konstrukci (stejně jako při užití) nástrojů trestního procesu omezující základní práva a svobody jednotlivců respektovat.*“[82] Po výše zmiňovaném rozhodnutí ÚS a následné novele zákona je potřeba předchozího souhlasu předsedy senátu a v přípravném řízení na návrh státního zástupce souhlas soudce.

Nařízení a podmínky jsou obdobné jako u domovní prohlídky. Příkaz musí obsahovat obdobné náležitosti jako příkaz k domovní prohlídce.[83] Tento procesní postup řadíme rovněž mezi zajišťovací úkony TŘ. Jde tedy o případy, kdy má policejní orgán důvodné podezření, že se v prostorech nesloužících k bydlení nebo na pozemcích, které nejsou veřejně přístupné, nachází osoby nebo věci důležité pro trestní řízení. V případě kyberkriminality se tento institut využívá, když jde o prostory, které neslouží k bydlení, např. živnostenské provozovny, sídla právnických osob, prodejny a servisy výpočetní techniky, kanceláře apod. Hledány jsou zejména věci informačních technologií či výpočetní techniky. Zajištění těchto věcí by stejně jako u domovní prohlídky měla provádět odborně vyškolená osoba DEFR, rovněž jako

[79] Informovaný z prostředí PČR.
[80] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. *Trestní řád I., komentář.* 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1126. (ustanovení § 83a TŘ).
[81] nález Ústavního soudu ze dne 8. 6. 2010 sp. zn. Pl. ÚS 3/09.
[82] Tamtéž.
[83] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. *Trestní řád I., komentář.* 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s. 1126. (ustanovení § 83a TŘ).

u domovní prohlídky, kde by totiž neodborné zacházení se zajišťovanými věcmi mohlo zmařit účel prohlídky. Prohlídka jiných prostor a pozemků by měla být dobře naplánovaná (obdobný postup jako u domovní prohlídky) s tím, že by se osobám využívajícím tento prostor či pozemky mělo znesnadnit, nejlépe zamezit, v ničení či pozměňování důkazů. Rovněž i zde by měl policejní orgán postupovat v souladu se zásadou přiměřenosti.[84] ÚS navíc ve své judikatuře zdůrazňuje, že v případě, kdy probíhá prohlídka jiných prostor a pozemků jako neodkladný a neopakovatelný úkon, je potřeba, aby OČTŘ měly dostatek informací a důkazů, které jsou podkladem pro důvodné podezření, jež by mělo být objektivní, tzn. skutečnosti by měly nasvědčovat tomu, že byl spáchán trestný čin.[85]

4.3 Zajištění věci pro důkazní účely

Zajištění věci pro důkazní účely je jeden z procesních nástrojů, kterým lze získat důkazy o spáchaném trestném činu. Způsob jeho provedení upravuje ustanovení § 78 a § 79 TŘ. Tento institut je využíván i při vyšetřování kyberkriminality. Během vyšetřování můžou OČTŘ narazit na věci, které jsou zaheslovány nebo zašifrovány či je k jejich odemčení potřeba užití biometrických údajů, např. odemykání mobilního telefonu pomocí otisku prstu nebo pomocí obličeje. K tomu, aby se takováto věc dala odemknout, je tedy nezbytné získat heslo, otisk prstu apod. To, jakým způsobem je odemčení dosaženo, úzce souvisí se zásadou zákazu sebeobviňování.

Zákaz sebeobviňování *(Nemo tenetur se ipsum accusare)* je jednou ze zásad trestního řízení a vychází jak z EÚLP, kde není vyjádřena výslovně, ale je dovozena judikaturou ESLP. Rovněž je tato zásada zakotvena v LZPS v čl. 37 odst. 1, který stanoví právo odepřít výpověď, a v čl. 40, který stanoví, že práva odepřít výpověď se nelze vzdát. Tato zásada se promítá nepřímo např. v ustanoveních § 66 TŘ, § 78 odst. 3 TŘ, § 114 TŘ atd. Několikrát se k této zásadě vyjadřoval ÚS (např. v sp. zn. Pl. ÚS 29/2000, I. ÚS 677/03, III. ÚS 451/04 I. ÚS 671/05 atd.), ale i ESLP, např. Allan versus Spojené království z roku 2012 atd.[86]

V kontextu s touto zásadou je zajímavý případ, který se stal v USA v srpnu roku 2018. FBI dostala povolení k domovní prohlídce z důvodu podezření, že podezřelá osoba vyhledává a drží dětskou pornografii. Během této prohlídky vyšetřovatel donutil podezřelou osobu, aby nastavila obličej před svůj iPhone, který byl zabezpečený heslem a dal se otevřít pomocí

[84] KOLOUCH, Jan. *CyberCrime…* s 429-431.
[85] nález Ústavního soudu ze dne 7. 6. 2016, sp. zn. III. ÚS 905/13.
[86] MATES, Pavel, PÚRY, František. Zákaz nucení k sebeobviňování. *Bulletin advokacie*, 2019, roč. 49, č. 3, s. 7-13.

obličeje. Telefon se odblokoval a policie jej mohla prověřit. Dle zdroje, který tuto zprávu uveřejnil, se podezřelá osoba aktivně nebránila a tento odemčený telefon údajně výrazně nepomohl vyšetřování případu.[87] V souvislosti s touto problematikou je důležité si uvědomit, že dostat se do iPhonu, popřípadě jiných smartphonů, je v současnosti náročné a v některých případech kriminalisté nedokáží takovéto zabezpečení překonat.[88] Myslím si, že je tento případ zajímavý, zvláště pokud se na něj zaměříme optikou českého trestního práva v souvislosti se zásadou zákazu sebeobviňování.

Odhlédneme-li od okolností, že se podezřelý aktivně nebránil a že odemčení mobilního telefonu nepomohlo vyšetřování případu (existovaly další usvědčující důkazy), je možné, že by takovýto postup OČTŘ mohl být posuzován jako možné porušení zásady zákazu nucení k sebeobviňování. Obdobně by mohl být posuzován případ, kdy OČTŘ přinutí podezřelou osobu otevřít mobilní telefon pomocí otisků prstů, přičemž tato osoba jej není ochotna dobrovolně otevřít a OČTŘ ji samy vedou ruku či jiným způsobem ji přinutí.

ÚS ve své judikatuře uvádí, že zásadu zákazu sebeobviňování nelze považovat za bezbřehou a neshledal za protiústavní postup, při kterém dochází k provedení bukálního stěru, odběru vzorku vlasů apod., i když se tak děje proti vůli obviněného. Rovněž neshledal za nezákonný postup, pokud bylo tohoto cíle dosaženo za pomoci donucení. Konstatoval však, že se nesmí jednat o invazivní zákrok proti tělu osoby, což je podrobněji rozebráno v Pl. ÚS-st. 30/10 či II ÚS 2369/08. Tato judikatura se dle mého názoru vztahuje hlavně k ustanovení § 114 TŘ a cílem tohoto ustanovení je odběr biologického materiálu. V ustanovení § 114 odst. 2 TŘ se výslovně uvádí, že jde o: *„zkoušku krve nebo jiný obdobný úkon.“* Tuto judikaturu však na výše zmiňovaný případ nelze užít, jelikož se dle mého názoru jedná o povinnost vydání věci (popřípadě vydání hesla), kterou upravuje ustanovení § 78 TŘ. Judikatura ÚS týkající se vydání věci uvádí v rozhodnutí III. ÚS 255/05, že obviněný či podezřelý nesmí být nucen pořádkovou pokutou k vydání věci. V odstavci 3. ustanovení § 78 TŘ zákonodárce výslovně stanoví, že: *„Nikoho nelze nutit, aby předložil nebo vydal věc, jež v době, kdy je požádáno o její předložení nebo vydání, může sloužit jako důkaz proti němu nebo proti jeho osobě blízké; tím nejsou dotčena ustanovení o odnětí věci, domovní prohlídce, prohlídce jiných prostor a pozemků a osobní prohlídce.“* Na základě výše uvedeného dospívám k názoru, že tento hypotetický

[87] OMA. *Odmítl odemknout svůj iPhone, poslali ho na půl roku za mříže*. [online]. iDnes.cz, 16. července 2018 [cit. 8. 1. 2020]. Dostupné na < https://www.idnes.cz/mobil/tech-trendy/ipho ne-heslo-policie-vazba.A180716_134953_mob_tech_oma?>.
[88] NOVÁK, Adam. *Zločinci se radují, FBI umí prolomit jen zlomek smartphonů*. [online]. iDnes.cz, 25. května 2018 [cit. 9. 1. 2020]. Dostupné na < https://www.idnes.cz/mobil/tech-trendy/fbi-prolomeni-zabezpeceni-smartphonu.A180523_230608_mob_tech_ada?>.

postup OČTŘ by měl být hodnocen jako zásah do zásady zákazu nucení k sebeobviňování a takto získané informace a důkazy by neměly být v souladu s ustanovením § 89 odst. 3 TŘ použity v trestním řízení. Na podporu svých tvrzení si dovolím citovat úryvek z článku Pavla Matese a Františka Púry, kteří zastávají názor, že z judikatury ESLP a ÚS vyplývá, že: *„ …obviněného (resp. podezřelého) lze nutit k tomu, aby pasivně strpěl určité úkony trestního řízení, jejichž výsledek ho může usvědčovat ze spáchání trestného činu, a to včetně tzv. neinvazivních zásahů (viz např. § 114 odst. 2 až 4 tr. řádu), ale nelze ho nutit k tomu, aby aktivně poskytoval orgánům činným v trestním řízení důkazní prostředky, které by ho mohly usvědčit ze spáchání trestného činu. Na druhé straně obviněnému nic nebrání v tom, aby dobrovolně poskytl i důkazní prostředek, k němuž jinak nemůže být nucen, pokud se domnívá, že je to v jeho prospěch, resp. může tak učinit, i když se tím dobrovolně usvědčí ze spáchaného trestného činu [např. z důvodu získání dobrodiní polehčující okolnosti podle § 41 písm. l) tr. zákoníku].“*[89]

Nejde ovšem o zcela jasnou a najisto postavenou problematiku a pravděpodobně konečné slovo by v této věci musel vyjádřit Nejvyšší nebo Ústavní soud ČR.

4.4 Údaje o telekomunikačním provozu

Institut údaje o telekomunikačním provozu byly jakožto institut do právního řádu ČR zakotven novelou TŘ č. 265/2001 Sb., a to v reakci na dosavadní vývoj judikatury ÚS. Zejména jde o nálezy pod sp. zn. II. ÚS 502/2000, IV. ÚS 536/2000, IV. 78/2001. Ustanovení § 88a TŘ upravuje podmínky získání „*údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat.“* Dle komentářové literatury: *„provozními a lokalizačními údaji jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace. Rozsah provozních a lokalizačních údajů uchovávaných, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis.“*[90] Pod těmito údaji si můžeme představit např. datum a čas komunikace, IP adresu a číslo portu, odkud bylo připojení uskutečněno, telefonní číslo volajícího a volaného a další. Provozní a lokalizační údaje rovněž definuje ustanovení § 90 a § 91 ZEK. Provozní a lokalizační údaje

[89] MATES, Pavel, PÚRY, František. Zákaz nucení k sebeobviňování. *Bulletin advokacie*, 2019, roč. 49, č. 3, s. 7-13.
[90] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. In ŠÁMAL, Pavel a kol. Trestní řád I., komentář. 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. s 1222. (ustanovení § 88a TŘ).

bývají také označovány jako tzv. metadata. Institut uchovávání provozních a lokalizačních údajů bývá v odborné literatuře označován jako data retention. Zjednodušeně se tedy dá říci, že postupem dle § 88a TŘ lze zjistit informace o komunikaci. Nejde o zjišťování vlastního obsahu komunikace, přičemž tyto informace je povinen vydat OČTŘ jejich držitel jako např. operátor, poskytovatel internetu apod. s tím, že vydává informace o již proběhlé komunikaci.[91] Osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací jsou povinny uchovávat tyto informace šest měsíců, pak je musí zlikvidovat, viz ustanovení § 97 odst. 3 a odst. 4 ZEK. Z výše uvedeného vyplývá, že jde o uchovávání informací o jedinci, který nějak využívá informační technologie. Z těchto informací se sice nedá zjistit obsah proběhlé komunikace, přesto jsou schopny poskytnout významné údaje o životě jedince. Např. budeme-li sledovat provozní a lokalizační údaje o konkrétním jedinci, jsme schopni určit v konkrétní den místa, která v určitý čas navštívil. Je tedy nepochybné, že uchovávání těchto informací je schopno podstatně zasáhnout do soukromí jednotlivce, jelikož je skrze ně možno podrobně mapovat jeho způsob života. Ústavní soud se zabýval výše uvedenou problematikou a konstatoval, že: *„…právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popřípadě v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný čl. 10 odst. 3 LPS.“*[92] Není divu, že tento institut je často předmětem diskuzí ze strany odborné veřejnosti, a to jak na vnitrostátní úrovni, tak i na mezinárodní úrovni. Několikrát se touto problematikou zabýval ESD, např. v Digital Rights Ireland Ltd, C-293/12 a C-594/12, či Tele2 Sverige AB a Watson, C-203/15 a C-698/15.

Rovněž i ÚS se již několikrát vyjadřoval k této problematice. Významným rozhodnutím je výše zmíněný nález ÚS Pl. ÚS 24/10, kdy došlo ke zrušení ustanovení § 97 odst. 3 a 4 ZEK v tehdejším znění a vyhlášky Ministerstva informatiky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání. ÚS v souvislosti s nálezem Pl. ÚS 24/10 v nálezu sp. zn. Pl. ÚS 24/11 také zrušil ustanovení § 88a TŘ, a to z důvodu vágnosti a neurčitosti (v předchozím nálezu jej nemohl zrušit, jelikož nebyl obsahem návrhu). Nová právní úprava data retention byla přijata novelou ze dne 18. 7. 2012 zákon č. 273/2012 Sb., kterou se mění zákon 127/2005

[91] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*, 2019, roč. 18, č. 3, s. 66-71.
[92] nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů a některé další zákony. Tato nová právní úprava reflektovala výše uvedená rozhodnutí ÚS a zároveň do značné míry vycházela ze Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. 3. 2006. Tato směrnice byla dne 8. 4. 2014 zrušena rozhodnutím ESD ve věci Digital Rights Ireland Ltd.

Naposledy se ÚS k této problematice vyjadřoval v nálezu sp. zn. Pl. ÚS 45/17, kdy zamítl návrh skupiny poslanců na zrušení ustanovení § 97 odst. 3 a 4 ZEK a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, § 88a TŘ, ve znění pozdějších předpisů, § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii České republiky, a vyhlášky č. 357/2012 Sb., o uchování, předávání a likvidaci provozních a lokalizačních údajů. Během ústního jednání ve věci samé bylo provedeno dokazování výslechem informovaných osob z řad odborné veřejnosti a osob z praxe. Dle ÚS z dokazování vyplynulo, že i v případě, kdy zanikne povinnost uchovávat metadata, budou provozní a lokalizační údaje při vyšetřování OČTŘ využívány, ale změní se způsob jejich získávání. Toto vedlo ÚS k závěru, že pokud by došlo k absenci úpravy povinnosti uchovávat metadata, došlo by k menší transparentnosti postupu OČTŘ při vyšetřování a zvýšilo by se riziko zneužití informací, které má držitel (např. operátor) o uskutečněném telekomunikačním provozu k dispozici. Zároveň nelze zaručit, že v případě absence provozních a lokalizačních údajů zvolí OČTŘ z hlediska zásahu do soukromí invazivnější vyšetřovací metody, které zasáhnou do soukromí jednice výrazněji.

Závěr ÚS je takový, že právní úprava je ústavně konformní, přesto však uvádí: *„ …přestože neshledal důvody pro zrušení právní úpravy data retention a přestože od vyhlášení nálezu sp. zn. Pl. ÚS 24/10 a přijetí zákona č. 273/2012 Sb. uplynulo jen několik let, neměl by zákonodárce v době překotného vývoje moderních technologií „usínat na vavřínech“. Současná právní úprava nereflektuje aktuální technologický vývoj a společenský trend co do způsobu a forem využívání elektronické komunikace, např. vymezení okruhu povinných subjektů, neodpovídá dnešnímu způsobu využívání služeb elektronické komunikace – povinnost data retention se nevztahuje na poskytovatele tzv. OTT služeb (např. Facebook, WhatsApp, Skype), které již víceméně klasický telekomunikační provoz začínají nahrazovat.“*[93]

Odlišné stanovisko zaujala soudkyně Kateřina Šimáčková, která je názoru, že česká právní úprava data retention je nedostatečná a z ústavněprávního podhledu neobstojí, protože dostatečně nechrání práva jednotlivce. Má za to, že současná právní úprava neposkytuje

[93] SEDLÁČKOVÁ, Miroslava. *Současná právní úprava data retention je ústavně konformní.* [online]. usoud.cz, 22. května 2019 [cit. 19. 2. 2020]. Dostupné na <https://www.usoud.cz/aktualne/soucasna-pravni-uprava-data-retention-je-ustavne-konformni/>.

potřebné záruky před zneužitím těchto dat, jelikož nekontroluje adekvátním způsobem, co se s metadaty u soukromých subjektů děje a jakým způsobem jsou poskytovány. Dále kritizuje nemožnost jedince kontrolovat, v jakém rozsahu jsou tato data využívána ze strany veřejné moci, a že nemá možnost se proti takovému zásahu bránit. Ve svém odlišném stanovisku dále upozorňuje na výpověď R. Polčáka, který v této výpovědi konstatuje, že v zemích EU je právní úprava odlišná, a přesto je schopna plnit potřebný cíl se stejnou efektivitou. Navrhuje možné řešení této situace, a to kratší uchovávání metadat v kombinaci s tzv. „zmrazovacím příkazem" (též označován jako "zmrazení dat"), popřípadě uchovávat po dobu šesti měsíců pouze některá metadata v omezenějším rozsahu, než je tak činěno v současné době. Dále navrhuje rozlišit a odstupňovat přístup k metadatům dle cíle, který OČTŘ sledují.[94]

K tomuto nálezu ÚS se také kriticky vyjadřoval M. Kokeš. Ten ve svém článku upozorňuje na postup ÚS, který podle něho srovnával současnou právní úpravu a předchozí právní úpravu, jež byla výše zmiňovanou judikaturou zrušena, nikoli však aktuální vývoj právní úpravy této problematiky na unijní úrovní, ani nekomparoval právní úpravu z členských států a nevycházel z kontextu požadavků judikatury ESD či ESLP (např. rozsudek ESD ze dne 13. 5. 2014, Google Spain a Google, sp. zn. C-131/12, rozsudek ESD ze dne 6. 10. 2014, Schrems v. Facebook, sp. zn. C-362/14, rozsudek ESLP ze dne 13. 9. 2018, č. 58170/13, 62322/14 a 24960/15, Big Brother Watch proti Spojenému království), o níž však musel mít povědomí, neboť ji rekapituloval v obecném části odůvodnění k nálezu. Autor je rovněž názoru, že se ÚS nedostatečně zabýval otázkou možného zneužití ze strany soukromých subjektů, které tato metadata uchovávají. Dále poukazuje na nedůkladné zkoumání ze strany ÚS toho, zda samotná úprava poskytuje dostatečné a efektivní záruky před zneužitím, jež vyžaduje judikatura ESD. Závěrem autor konstatuje, že ÚS zaostal za vývojem současné judikatury ESD či ESLP i vývojem v unijní úpravě posilující ochranu soukromí jednotlivce v prostředí elektronické komunikace, a to jak proti zneužití ze strany veřejné moci, tak proti zásahům ze strany soukromých subjektů.[95]

Úřad pro ochranu osobních údajů se k nálezu ÚS rovněž vyjadřoval. Konstatoval, že si lze představit právní úpravu, která je šetrnější, to však je úkolem zákonodárce, nikoli ÚS. Dále upozornil na úpravu jiných evropských zemí a závěrem uvedl, že současná právní úprava je koncipována dosti široce, a tak zvyšuje nároky na všechny účastníky procesu uchovávání

[94] nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.
[95] KOKEŠ, Marian. Judikatura ÚS: ochrana soukromí v tzv. době internetové. *Soudní rozhledy*, 2019, roč. 25, č. 6, s. 182-188.

provozních a lokalizačních údajů a přístupu k nim. Dále upozornil na potřebu vhodných technických a organizačních opatření.[96]

Na to, že současná právní úprava není zcela korektní, již dříve upozorňovala autorka komentáře k ZEK. Ta v komentovaném ustanovení § 97 ZEK poukazuje na to, že současná právní úprava do značné míry vychází ze zrušené směrnice 2006/24 a zákonodárce na to prozatím nikterak nereagoval. Proto autorka komentáře klade důraz na to, že by soudy měly postupovat v souladu s nutností eurokonformního výkladu právních předpisů a v souladu s tímto výkladem užívat ustanovení § 97 ZEK.[97]

ÚS ve svém nálezu konstatoval, že současná právní úprava data retention se dá vykládat ústavněkonformně s tím, že v současné době není v ČR znám lepší způsob, jenž by zasahoval do práv jedince méně, a zrušení tohoto ustanovení by znamenalo užívání alternativ, které by nebyly tak transparentní jako současný způsob provedení. Tento institut je z hlediska objasňování kyberkriminality, ale i dalších trestných činů velice významný nástroj, jejž lze v současné době obtížně nahradit jiným institutem, který bude do práv a svobod jedince zasahovat méně. Zrušení tohoto institutu by znamenalo značné obtíže pro OČTŘ. Je nutné uvědomit si, že ÚS není povolán k tomu, aby měnil právní úpravu, ale aby hlídal soulad právní úpravy s ústavním pořádkem ČR. Současná právní úprava data retention není natolik rozporná či nešetrná, aby dosáhla takové míry intenzity zásahu do práv a svobod jedince, že by byla potřeba právní úpravu zrušit nálezem ÚS.

Dle mého názoru by úplné zrušení tohoto institutu znamenalo krok zpět a vzhledem k současnému stavu techniky a jejímu očekávanému rozvoji by značným způsobem ztížilo a mělo negativní dopady na objasňování kriminality. Během páchání trestných činů jsou často využívány komunikační prostředky. Avšak z výše uvedeného vyplynulo, že je zde potřeba se touto právní úpravou zabývat a zákonodárce by se měl snažit ji přizpůsobit aktuálnímu stavu společnosti a způsobu využívání komunikačních technologií a efektivně reagovat na tento stav vhodnou právní úpravou. Například v Německu umožňuje legislativa uchovávat data retention v období deseti týdnů pro provozní údaje a čtyř týdnů pro lokalizační údaje.[98] V Polsku se data retention uchovávají po dobu dvou let.[99] Dle mého názoru by se zákonodárce měl zamyslet nad

[96] Vláda: ÚOOÚ: Vyjádření k nálezu Ústavního soudu ve věci data retention. *Právní rozhledy*, 2019, roč. 27, č. 12, s. III.
[97] VLACHOVÁ, Barbora. In VLACHOVÁ, Barbora. Zákon o elektronických komunikacích, komentář. 1. vydání. Praha: C. H. Beck, 2017. s. 313. (ustanovení § 97 ZEK).
[98] JAMES, Rebecca. *Germany Mandatory Data Retention Directives*. [online]. privacysniffs.com, 18. července 2019 [cit. 16. 2. 2020]. Dostupné na <https://privacysniffs.com/data-retention-law/germany/>.
[99] CRAIG, Christina. *Poland Surveillance Law*. [online]. nordvpn.com, 12. února 2016 [cit. 26. 2. 2020]. Dostupné na <https://nordvpn.com/blog/poland-surveillance-law/>.

samotným závěrem ÚS, argumenty soudkyně K. Šimáčkové, M. Kokeše, doporučeními R. Polčáka, či vyjádřením Úřadu pro ochranu osobních údajů, ale zároveň i samotným vyjádřením OČTŘ k využívání a významu těchto údajů. Již komentářová literatura konstatuje, že právní úprava, která je v současné době platná a účinná, do značné míry vychází ze zrušené směrnice č. 2006/4 a je potřeba vykládat ji eurokonformně. V řízení před ÚS týkající se nálezu PL sp. zn. Pl. ÚS 45/17 vyšlo najevo, že OČTŘ využívají data retention starší tří měsíců pouze v omezené míře. ÚS sám zdůrazňuje, že současná právní úprava nereflektuje uchovávání provozních a lokalizačních údajů společnostmi jako jsou Facebook, Skype, Wiber apod. Myslím si, že je důležité, aby zákonodárce při vytváření nové právní úpravy komunikoval s odborníky, a to jak z oblasti telekomunikací, tak i ze strany OČTŘ a odborné právní veřejnosti. Dle mého názoru by nová právní úprava mohla zkrátit povinnost uchovávání některých provozních a lokalizačních údajů (např. jméno a příjmení zákazníka, adresa zákazníka, typ telefonní služby apod.) na období délky tří měsíců, kdy po uplynutí této doby bude muset jejich uchovavatel prokázat Českému telekomunikačnímu úřadu, že došlo ke zničení těchto údajů. Naopak u některých provozních a lokalizačních údajů (např. identifikátor IMSI[100], identifikátor IMEI[101], IP adresa[102] a číslo portu, označení přístupového bodu u bezdrátového připojení) by se měla prodloužit povinnost jejich uchovávání na délku jednoho roku s tím, že tyto provozní a lokalizační údaje by si mohl vyžádat jen OČTŘ, a to v případě objasňování trestného činu, pro který stanoví trestní zákon trestní sazbu ve výši např. alespoň pěti let. Dalo by se zde uvažovat i o vyšší trestní sazbě a výčtu trestných činů, které do této sazby nezapadnou, ale bylo by vhodné z důvodu efektivního objasňování těchto trestných činů, aby zde byly zařazeny. Je možné zvažovat i to, že by požadování provozních a lokalizačních údajů, které by se uchovávaly v délce jednoho roku, musel schválit soud. Rovněž by se tento institut měl vhodně kombinovat s institutem zmrazení dat, kdy může poskytnout OČTŘ další čas.

4.5 Okamžité zajištění dat a ustanovení § 7b trestního řádu

Okamžité zajištění dat a ustanovení § 7b TŘ se objevuje v českém právním řádu po novele č. 287/2018 Sb., kterou se mj. novelizuje trestní řád. Účinnosti nabyl 1. 2. 2019. Dle důvodové zprávy k zákonu č. 287/2018 Sb. jde o implementaci čl. 16 Úmluvy o počítačové kriminalitě z roku 2001, vyhlášené pod č. 104/2013 Sb. m. s., kterou je ČR vázaná. Dříve

[100] IMSI (International Mobile Subscriber Identity) je unikátní číslo přidělené mobilním operátorem pro SIM kartu v mobilní síti GMS nebo UMTS.
[101] IMEI (International Mobile Equipment Identity) je unikátní číslo přidělené výrobcem mobilního telefonu.
[102] IP adresa je univerzální číslo, které je přiděleno PC, který komunikuje prostřednictvím internetového protokolu.

k tomuto účelu využívaly OČTŘ ustanovení § 8 TŘ. Dle odstavce 1 § 7b: *„Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat.“* Dle odstavce 2 § 7b: *„je-li to zapotřebí k zabránění pokračování v trestné činnosti nebo jejímu opakování, lze nařídit osobě, která drží nebo má pod svojí kontrolou data, která jsou uložena v počítačovém systému nebo na nosiči informací, aby znemožnila přístup jiných osob k takovým datům.“* Tento druhý odstavec však nevyplývá z čl. 16 výše zmiňované Úmluvy.

Pro lepší pochopení tohoto institutu je dobré si uvědomit, o jaký typ dat se jedná. Zatímco v předchozí podkapitole se probírala problematika tzv. data retention,[103] v tomto případě jde o tzv. data preservation.[104] Ustanovení § 7b se tedy týká uchování určitých dat, která jsou významná pro konkrétní trestní řízení v nezměněném stavu. Tato data již vznikla a reálně existují. Uchování proběhne na základě příkazu, který je na časově omezenou dobu a směřuje vůči osobě, jež má daná data fyzicky pod kontrolou. Tato osoba má povinnost mlčenlivosti o tom, že byl takovýto příkaz vydán, a to z důvodu možného zmaření trestního řízení. Proto OČTŘ volí výše uvedený postup jen v případě, že jde o tzv. důvěryhodného správce. Tento postup je pak šetrnější k reputaci správce a může jít o méně invazivní zásah do jeho činnosti. V případě, že správce nebude důvěryhodný, musí OČTŘ zvolit jiný postup k uchování dat, např. zajistit data na místě. Je důležité si uvědomit, že se příkaz týká všech typů dat a pokud jsou relevantní pro trestní řízení, musí být konkrétní data v příkazu dostatečně specifikována. Doba, po kterou mají být data uchována, je devadesát dní pro vnitrostátní účely a pro mezinárodní sto osmdesát dní. Osoba, vůči níž příkaz směřuje, má tak povinnost bezpečně uchovat data a tato skutečnost musí zůstat v tajnosti. Tento postup směřuje pouze k uchování dat po stanovenou dobu v nezměněné podobě, nejde o zpřístupnění jejich obsahu OČTŘ. K seznámení se s obsahem musí dojít jiným postupem sloužícím pro zajištění dat.[105] *„Účelem uvedeného předběžného uchování dat je přechodně zabránit ztrátě, pozměnění nebo zničení*

[103] Data retention znamená plošné uchovávání dat, která jsou aktuálně vytvářena, do budoucna, vztahují se k aktuálně shromažďovaným údajům. (Proces ukládání dat)
[104] Data preservation znamená uchovávání konkrétních dat, která již existují a jsou uložená, v nezměněné podobě po stanovenou dobu.
[105] *Důvodová zprava k zákonu č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony*. [online]. beck-online.cz, 31. ledna 2018 [cit. 7. 2. 2020]. Dostupné na <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge4f6mryg5pwi6q&rowIndex=0>.

údajů, které jsou důležité pro trestní řízení (pro důkazní účely), tak, aby byla zachována integrita těchto dat, a to do doby, než bude trestním řádem předvídaným postupem vydán příkaz k zpřístupnění obsahu těchto údajů orgánům činným v trestním řízení.“[106] Tento institut tak může být významným nástrojem při vyšetřování kyberkriminality páchané v prostředí internetu. Je důležité si uvědomit, že data lze jednoduše změnit a významný důkazní prostředek relevantní pro trestní řízení tak může být nenávratně ztracen, a to jak z důvodu záměrného pozměnění či zničení ze strany pachatele, tak z důvodu nedbalého nakládaní či uchovávaní takovýchto dat ze strany správce, např. automatické smazání po určité době nebo automatické přepsání.[107]

Ministerstvo vnitra České republiky vydalo 21. 8. 2019 metodiku k aplikaci tohoto ustanovení v podobě stanoviska Odboru bezpečnostní politiky k aplikaci ustanovení § 7b TŘ čj. MV-115844-2/OBP-2019. V metodice upozorňuje, že tento institut smí být užit jen na data již existující a v žádném případě jej nelze aplikovat na sběr dat do budoucna. Dále, že nesmí být užíván jako preventivní opatření. Až po provedení bude ze strany OČTŘ vyhodnocováno, že takový příkaz byl potřeba. *„Pro vydání příkazu dle § 7b tr. řádu musí orgán činný v trestním řízení pečlivě zvažovat skutkové okolnosti, zejména pak posuzovat přiměřenost svého postupu při posuzování doby, po kterou mají být data uchovávána, a jejich rozsahu.“*[108] Dále zdůrazňuje dodržení principu přiměřenosti, jenž musí být brán v potaz při určování rozsahu dat, který má být příkazem zasažen. Rovněž doporučuje zdrženlivost při určování délky doby uchovávání dat s tím, že využití maximální délky doby by nemělo být automatické, a pokud to situace dovolí, má být uložena kratší délka uchovávání, avšak v případě, kdy to bude nezbytné, se má prodloužit až na dobu devadesáti dní. Metodika se věnuje použití ustanovení § 7b TŘ v kombinaci s § 158d odst. 3 TŘ, kdy zastává názor, že bude záležet na konkrétních skutkových okolnostech každého případu. Například pokud ze skutkových okolností vyšetřovaného případu vyplyne, že se v e-mailové komunikaci nachází informace relevantní pro trestní řízení, které nelze získat jiným způsobem, popřípadě nahradit jiným důkazem, lze tuto kombinaci využít a zároveň musí být nenahraditelnost takového důkazu součástí zdůvodnění v žádosti. Ovšem užití této kombinace v případě, kdy by měl postup dle § 7b TŘ být jen jakousi mezidobou mezi žádostí a vydáním povolení soudce, je dle metodiky nepřípustné a takovýto postup se považuje

[106] *Důvodová zprava k zákonu č. 287/2018 Sb.,….*
[107] Tamtéž.
[108] Ministerstvo vnitra, Odbor bezpečnostní politiky. *Stanovisko OBP k aplikaci ustanovení § 7b trestního řádu*. [online]. mvcr.cz, 21. srpna 2019 [cit. 7. 2. 2020]. Dostupné na <https://www.mvcr.cz/clanek/poskytnuti-informace-metodika-tykajici-se-aplikace-7b-trestniho-radu.aspx>.

za obcházení zákona. Za obcházení zákona považuje i kombinaci § 7Btř a § 88a TŘ, ale zcela ji nevylučuje v naprosto výjimečných a odůvodněných případech.

Toto ustanovení ve znění, v jakém bylo přijato, vyvolalo vlnu kritiky ze strany odborné veřejnosti. Petr Toman, ve svém článku poukazuje na nedostatky této právní úpravy. Je názoru, že toto ustanovení nemá potřebné limity. K vydání příkazu není potřeba souhlasu soudu, použití není limitováno závažností trestného činu, který je vyšetřován. Chybí úprava, která by reflektovala důvěrnost komunikace mezi advokátem a jeho klientem. Nařízení směřuje vůči třetí osobě, které je tímto uložena povinnost, aby na své vlastní náklady uchovávala konkrétní data, a to až po dobu devadesáti dnů, a až poté přijde rozhodnutí soudu o jejich případném vydání či odnětí. Za výše uvedených podmínek smí policejní orgán nařídit vypnutí kterékoli webové stránky, e-mailové schránky či jakékoli jiné aplikace, kterou je obvykle komunikováno. Dle názoru autora je toto ospravedlnitelné např. v případě hrozby terorismu, ustanovení však takovéto limity neobsahuje a může být užito při vyšetřování kteréhokoli trestného činu. Následky v případě nesprávnosti tohoto postupu mohou být obrovské. Autor uvádí příklad se zablokováním e-shopu některého z velkých obchodníků, škody by mohly být v takových případech nedozírné.[109]

Tomáš Sokol se s kritikou Petra Tomana ztotožňuje a ve svém článku se věnoval dopadům tohoto ustanovení na advokáty. Upozorňuje na ne zcela jasné a přesné definice pojmů vyjádřené v ustanovení § 7b TŘ. Dále poukazuje na to, že po uchování dat následuje jejich transfer, jeho podoba však není nikterak upravena. Autor v článku poukazuje na nejasnosti úpravy ve vztahu k advokátům, které mohou činit velké obtíže ve vztahu advokát-klient z důvodu dostání povinnosti stanovené příkazem dle § 7b TŘ. Autor je názoru, že advokát by neměl být považován za tzv. důvěryhodného správce, a proto by se nemuselo ustanovení vůči advokátům užít. Autor doporučuje advokátům, aby se v případě, kdy jim bude přikázáno uchovat určitá data ve smyslu § 7b TŘ a advokát je názoru, že jde o data, na která se vztahuje advokátní mlčenlivost, obrátili na advokátní komoru a celou situaci s ní konzultovali. Podle autora má advokát z titulu svého postavení povinnost učinit opatření, aby nedošlo k vyzrazení skutečnosti, o které se dozvěděl při poskytování právní služby. Tato povinnost je dle autora silnější než povinnost podřídit se příkazu dle § 7b TŘ.[110]

[109] TOMAN, Petr. *Podstrčený paragraf 7b trestního řádu – kde se vzal a o čem je*. Advokátní deník. cak.cz, [online]. 22. července. 2019 [cit. 7. 2 2019]. Dostupné na <https://www.cak.cz/scripts/detail.php?id=20932>.
[110] SOKOL, Tomáš. Povinnost dle § 7b trestního řádu z pohledu advokáta. *Bulletin advokacie*, 2019, roč. 49, č. 9, s. 15-19.

Ustanovení rovněž podrobily kritice i autorky článku "*Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?"* V něm upozorňují na to, že subjekt, jenž je povinný, nepatří mezi OČTŘ, avšak realizuje zásah do práv jedince, kterých se uchovávaná data týkají. Ustanovení TŘ neřeší otázku nákladů týkajících se takového jednání, jelikož může jít o proces, jenž je pro povinného finančně nákladný. Autorky mají za to, že způsob, jakým došlo k implementaci závazku z Úmluvy o počítačové kriminalitě, není zcela nejvhodnější a neodpovídá ani cílům a podmínkám úmluvy. Hlavním účelem Úmluvy je boj proti počítačové kriminalitě a usnadnění jejího vyšetřování a postihování. Autorky upozorňují, že tento institut nemá sloužit k potírání jakékoli kriminality, ale požadavek implementace této úpravy se vztahuje na kyberkriminalitu, jak stanoví čl. 14 a čl. 16 Úmluvy. Dle názoru autorek přijatá právní úprava nenaplňuje předpoklady pro zákonný zásah do práva na soukromí, jelikož nesplňuje základní podmínky (legalita, legitimita a proporcionalita). Autorky hodnotí za zcela nevhodný postup užití tohoto institutu v praxi, kdy po užití § 7b TŘ k vydání dat použijí OČTŘ § 158d odst. 1 a odst. 3 TŘ. Výše uvedený postup je nevhodný z důvodu, že ustanovení § 158d odst. 1 a odst. 3 TŘ primárně slouží ke sledování dat do budoucna, zatímco ustanovení § 7b TŘ se užívá na data, která již vznikla a byla uchována v minulosti. Dále upozorňují, že dle TŘ lze zpětně a na základě příkazu soudu požadovat jen provozní a lokalizační údaje a nikoli obsah komunikace. Proto daný postup shledávají za obcházení zákona, zejména v kombinaci s ustanovením týkajícím se odposlechů. Autorky zastávají názor, že použití ustanovení § 158d TŘ je úkonem, který jsou oprávněny vykonat jen OČTŘ a třetím osobám tuto povinnost nelze uložit, a to ani na základě žádosti o poskytnutí součinnosti. Pojmem součinnost tak autorky rozumí poskytnutí pomoci ze strany osob nezúčastněných na trestním řízení, nikoli nahrazování činnosti OČTŘ, kterou by zasahovaly do práv a svobod jednotlivců způsobem vyhrazeným výlučně veřejné moci.[111]

Okamžité zajištění dat je dle mého názoru institut, který může být užitečný a významným způsobem napomoci při vyšetřování kyberkriminality. Bohužel se jeho implementace do našeho právního řádu prostřednictvím ustanovení § 7b TŘ jeví jako nedostatečná a vágní. Vytváří mnoho nejasností a nedostatečně chrání práva a svobody jedince, nemluvě o nereflektování vztahu advokáta a klienta. Dále ustanovení bohužel nerespektuje požadavky na implementaci stanovené samotnou Úmluvou o počítačové kriminalitě, která požaduje v čl. 14 aplikaci procesních institutů v ní obsažených jen na trestné činy stanovené

[111] NAVRÁTILOVÁ, TLAPÁK, Jana, GALOVCOVÁ, Ingrid. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?. *Bulletin advokacie*, 2019, roč. 49, č. 11, s. 36-39.

podle článků 2 až 11 této Úmluvy, na jiné trestné činy spáchané prostřednictvím počítačového systému a na zajištění důkazů o trestném činu, které jsou v elektronické formě, není-li stanoveno v Úmluvě jinak. A. Završnik zastává názor, že okamžité zmrazení dat lze vyžadovat pro každý elektronický důkaz ve spojení s jakýmkoli trestným činem, tento institut není omezen jen na závažnou kriminalitu či na kyberkriminalitu.[112] To však nemění fakt, že česká implementace je vadná, jelikož český právní řád nezná pojem elektronický důkaz, nenalezneme zde jeho definici. Avšak kdyby český právní řád obsahoval definici elektronického důkazu pro trestní řízení, už by se dalo teoreticky výkladem dovodit, že se ustanovení § 7b TŘ užije na takové případy. V současné době tomu tak ale není. Nicméně i kdyby český právní řád obsahoval definici elektronického důkazu, neměnilo by to nic na faktu, že implementace § 7b TŘ není v pořádku, jelikož neobsahuje podmínky a záruky požadované čl. 15 výše zmiňované Úmluvy. Stále ji lze tak označit za nedostatečnou. Můžeme tedy jen doufat, že zákonodárce vyslyší kritiku odborníků a pokusí se současný stav napravit. Osobně s výše uvedenou kritikou souhlasím. Nedostatky právní úpravy byly vytýkány relativně brzy po jejím přijetí. Zákonodárce však na tuto výzvu ze strany odborné veřejnosti prozatím nereagoval. Je tedy možné, že z důvodů jeho nečinnosti odborníci přesvědčí osoby oprávněné podat návrh ÚS k podání návrhu na zrušení tohoto ustanovení. Ovšem otázkou je, jak by se k takové situaci ÚS postavil.

[112] ZÁVRŠÍK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. s. 60.

Závěr

Informační a komunikační technologie se staly neoddělitelnou součástí každodenního života člověka, jsou snadno dostupné a výrazně změnily tvář společnosti. Nelze jim upřít jejich obrovský přínos ve vědě, umění, vzdělávání, komunikaci, medicíně a mnoha dalších oblastech. Tím, jak významně zasahují do života jedince, však s sebou přinášejí i velká rizika, která jsou úrodnou půdou pro páchání trestné činnosti.[113] Kyberkriminalita je, jak již bylo několikrát řečeno, dynamicky se rozvíjející oblast a lze předpokládat, že pachatelé tohoto druhu trestných činů budou vždy o krok před zákonem. Proto je důležité, aby zákonodárce vytvořil efektivní právní úpravu, která bude schopna alespoň částečně vykrývat slepá místa v právním řádu. Je potřebné reagovat na nové způsoby páchání trestné činnosti a na příliv nových technologií, které budou pachateli zneužity k páchání trestné činnosti. Takový přístup zcela jistě usnadní OČTŘ vyšetřování trestných činů spojených s kyberkriminalitou.

V současné době lze podle mého názoru u některých institutů TŘ spatřovat významné nedostatky, které jsou schopny negativně ovlivnit vyšetřovaní a bohužel i zasáhnout do práv a svobod jedince nežádoucím způsobem. Na základě výsledků své diplomové práce jsem dospěla k závěru, že zákonodárce v případě institutu uchovávání provozních a lokalizačních údajů zapomněl reagovat vhodnou právní úpravou na aktuální stav společnosti a způsoby využívání komunikačních technologií. Rovněž jsem dospěla k závěru, že ustanovení § 7b TŘ bylo do českého právního řádu implementováno vadně, právní úprava se jeví jako vágní a vytváří mnoho nejasností, což považuji za nežádoucí efekt s ohledem na potencionální možnost využití tohoto institut v praxi při objasňování kyberkriminality. Myslím si, že zavedení definice elektronického důkazu do TŘ by usnadnilo využívání procesních institutů stanovených v Úmluvě o počítačové kriminalitě ze dne 23. 11. 2001 a současně by mohlo i usnadnit práci zákonodárce.

Zákonodárce však není jediným, kdo je povinen vytvářet vhodné nástroje pro účinný boj s kyberkriminalitou. OČTŘ a především PČR jsou rovněž povinny reagovat na vývoj v této kriminální oblasti a přizpůsobit svůj postup při vyšetřování vynalézavosti pachatelů novým trendům, které jsou užity ke spáchání trestné činnosti. Tyto postupy a poznatky se pak promítají do metodiky vyšetřování kyberkriminality.

Cílem mé diplomové práce bylo získat poznatky o kriminalistickém postupu při odhalování této trestné činnosti, přiblížit některé procesní postupy při zajišťování důkazních

[113] *Nebezpečí elektronické komunikace - strašák nebo vážný problém?*. [online]. e-bezpeci.cz, 22. května 2009 [cit. 19. 3. 2020]. Dostupné na < https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/140-160>.

prostředků a upozornit na nedostatky konkrétní právní úpravy. Záměrem bylo zhodnotit, jestli je jednotný názor odborné veřejnosti na pojmenování této oblasti, na vymezení pojmu a na dělení tohoto druhu kriminality. Dále bylo záměrem zjistit, jaké jsou v současné době metodiky vyšetřování kyberkriminality a zda se v čase mění, přiblížit čtenáři některé zvláštnosti metodiky vyšetřování, vysvětlit pojem digitální stopa a zabývat se tím, zdali má význam definovat v české právní úpravě pojem elektronický důkaz. Dále jakým způsobem lze zajišťovat důkazní prostředky související s touto trestnou činností. V práci jsem se zaměřila na oblast domovní prohlídky, prohlídky jiných prostor a pozemků, zajištění věci pro důkazní účely, kde jsem se blíže zabývala užitím tohoto institut v kontrastu se zásadou zákazu sebeobviňování, dále údaji o telekomunikačním provozu a okamžitým zajištěním dat a ustanovením § 7b TŘ.

Podle mého názoru se mi povedlo naplnit cíle této práce stanovené v úvodu. Její přínos spatřuji zejména v tom, že čtenáři v rámci možností dostupných a uveřejnitelných informací přiblíží postup OČTŘ při vyšetřování tohoto druhu trestné činnosti, a to především postup PČR. Dále spatřuji přínos v tom, že poukazuji u vybraných procesních institutů na jejich nedostatky. Myslím si, že tato práce může být dílčím přínosem do odborné diskuze zabývající se konkrétními problémy právní úpravy TŘ.

Zdroje

Monografie

CASEY, Eoghan. *Digital evidence and Computer crime*. Third Edition. London: Elsevier Books, 2011. 840 s.

FRYŠTÁK, Marek. *Dokazování v přípravném řízení*. 2. vyd. Brno: Masarykova univerzita, 2015. 392 s.

GÁBRIŠ, Tomáš. *Cyber Law textbook*. 1. vydání. Bratislava: Univerzita Komenského v Bratislavě, Právnická fakulta, 2014. 249 s.

GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana. Kriminologie. 4. aktualizované vydání. Praha: Wolters Kluwer, 2014. 536 s.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. 284 s.

KALVODOVÁ, Věra, HRUŠÁKOVÁ, Milana a kol. *Dokazování v trestním řízení právní – právní, kriminologické a kriminalistické aspekty.* 1. vydání. Brno: Masarykova univerzita, Právnická fakulta, 2015. 503 s.

KOLOUCH, Jan. *CyberCrime.* 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016. 522 s.

KOLOUCH, Jan, VOLOCECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013. 117 s.

KONRÁD, Zdeněk, PORADA, Viktor, STRAUS, Jiří, SUCHÁNEK, Jaroslav. *Kriminalistika: Kriminalistická taktika a metodiky vyšetřování.* Plzeň: Aleš Čeněk, 2015. 414 s.

MUSIL, Jan, KONRÁD, Zdeněk, SUCHÁNEK, Jaroslav. *Kriminalistika*. 2 přepracované a doplněné vydání. Praha: C. H. Beck, 2004. 606 s.

POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub, a kol. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, Právnická fakulta 2015. 253 s.

POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium, 2012. 388 s.

POLČÁK, Radim. *Právo na internetu spam a odpovědnost ISP*. Brno: Computer Press, a. s., 2007. 150 s.

PORADA, Viktor a kol. *Kriminalistická metodika vyšetřování.* Plzeň: Aleš Čeněk, 2007. 231 s.

PORADA, Viktor a kol. *Kriminalistika Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016. 1018 s.

PORADA, Viktor, KONRÁD, Zdeněk. *Metodika vyšetřování počítačové kriminality.* Praha: Policejní akademie České republiky, 1998. 54 s.

PORADA, Viktor, STRAUS, Jiří. *Kriminalistické stopy teorie, metodologie, praxe.* Plzeň: Aleš Čeněk, 2012. 506 s.

RAK, Roman, PORADA, Viktor a kol. *Kybernetická kriminalita 1. díl.* Praha: Vysoká škola Karlovy Vary, 2013. 231 s.

REPÍK, Bohumil. *Evropská úmluva o lidských právech a trestní právo*. Praha: Orac, 2002. 263 s.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2 vydání. Plzeň: Aleš Čeněk, 2018. 934 s.

SMEJKAL, Vladimír. *Internet a §§§*. 2. aktualiz. a rozš. vyd. Praha: Grada, 2001. 284 s.

SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. vyd. Praha: C. H. Beck, 2004. 770 s.

SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C. H. Beck, 1995. 264 s.

SVOBODA, Ivo a kol. *Kriminalistika.* Ostrava: Key Publishing s.r.o., 2016. 374 s.

ŠIMOVČEK, Ivan a kol. *Kriminalistika*. Plzeň: Aleš Čeněk, 2011. 405 s.

ZAORALOVÁ, Petra. *Procesní použitelnost důkazů v trestním řízení a její meze*. Praha: Leges, 2018. 320 s.

ZÁVRŠÍK, Aleš. *Kyberkriminalita.* Praha: Wolters Kluwer, 2017. 148s.

Komentářová literatura

DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád I. díl, komentář*. Praha: Wolters Kluwer, 2017. 1383 s.

DRAŠTÍK, Antonín, FENYK, Jaroslav a kol. *Trestní řád II. díl, komentář*. Praha: Wolters Kluwer, 2017. 1117 s.

JELÍNEK, Jiří a kol. *Trestní zákoník a trestní řád s poznámkami a judikaturou.* 6. aktualizované vydání podle stavu k 1. 2. 2016. Praha: Leges, 2016. 1280 s.

ŠÁMAL, Pavel a kol. *Trestní řád I., komentář.* 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. 1898 s.

ŠÁMAL, Pavel a kol. *Trestní řád II., komentář.* 7. doplněné a přepracované vydání. Praha: C. H. Beck, 2013. 1899-3730 s.

ŠÁMAL, Pavel a kol. *Trestní řád III., komentář.* 7 doplněné a přepracované vydání. Praha: C. H. Beck, 2013. 3731-4654 s.

ŠÁMAL, Pavel a kol. *Trestní zákoník I., komentář.* 2. vydání. Praha: C. H. Beck, 2012. 1450 s.

VANGELI, Benedikt. *Zákon o Policii České republiky, komentář*. 2. vydání. Praha: C. H. Beck, 2014. 488 s.

VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích, komentář*. 1. vydání. Praha: C. H. Beck, 2017, 530 s.

Judikatura

nález Ústavního soudu ze dne 22. 5. 1997, sp. zn. III ÚS 287/96.

nález Ústavního soudu ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000.

nález Ústavního soudu ze dne 13. 2. 2001, sp. zn. IV. ÚS 536/2000.

nález Ústavního soudu ze dne 20. 2. 2001, sp. zn. Pl. ÚS 29/2000.

nález Ústavního soudu ze dne 27. 8. 2001, sp. zn. IV. ÚS 78/2001.

nález Ústavního soudu ze dne 22. 2. 2006, sp. zn. I ÚS 671/05.

nález Ústavního soudu ze dne 23. 3. 2006, sp. zn. III. ÚS 451/04.

nález Ústavního soudu ze dne 30. 4. 2007, sp. zn. III ÚS 299/06.

nález Ústavního soudu ze dne 9. 10. 2007, sp. zn. I. ÚS 677/03.

nález Ústavního soudu ze dne 8. 6. 2010 sp. zn. Pl. ÚS 3/09.

nález Ústavního soudu ze dne 9. 12. 2010, sp. zn. II ÚS 2369/08.

nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

nález Ústavního soudu ze dne 20. 12. 2011, sp. zn. Pl. ÚS 24/11.

nález Ústavního soudu ze dne 14. 11. 2012, sp. zn. IV. ÚS 2227/12.

nález Ústavního soudu ze dne 24. 7. 2013, sp. zn. I. ÚS 4457/12.

nález Ústavního soudu ze dne 28. 11. 2013, sp. zn. I. ÚS 2787/13.

nález Ústavního soudu ze dne 15. 12. 2015, sp. zn. I. ÚS 2024/15.

nález Ústavního soudu ze dne 7. 6. 2016, sp. zn. III. ÚS 905/13.

nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17.

stanovisko Ústavního soudu ze dne 30. 11. 2010, sp. zn. Pl. ÚS-st. 30/10.

usnesení Ústavního soudu ze dne 13. 10. 2005, sp. zn. III. US 255/05.

usnesení Ústavního soudu ze dne 13. 12. 2007, sp. zn. III. ÚS 1033/07.

usnesení Ústavního soudu ze dne 28. 2. 2008, sp. zn. III. ÚS 1578/07.

usnesení Ústavního soudu ze dne 11. 8. 2015, sp. zn. I. ÚS 1466/15.

Rozsudek Nejvyššího soudu ze dne 29. 3. 2000, sp. zn. 5 Tz 32/2000.

usnesení Vrchního soudu v Olomouci ze dne 2. 1. 2014, sp. zn. 6 To 94/2013.

Rozsudek Evropského soudu pro lidská práva ze dne 5. 11. 2002, *Allan versus Spojené království*, stížnost č. 48539/99.

Rozsudek Evropského soudu pro lidská práva ze dne 13. 9. 2018, *Big Brother Watch a další proti Spojenému království*, stížnost č. 58170/13.

Rozsudek Soudního dvora Evropské unie ze dne 8. 4. 2014, *Digital Rights Ireland Ltd*, C-293/12 a C-594/12.

Rozsudek Soudního dvora Evropské unie ze dne 13. 5. 2014, *Google Spain*, C-131/12.

Rozsudek Soudního dvora Evropské unie ze dne 6. 10. 2014, *Schrems v. Facebook*, C-362/14.

Rozsudek Soudního dvora Evropské unie ze dne 21. 12. 2017, *Tele2 Sverige AB v. Post-och telestyrelsen a Secretary of State for the Home Department v. Tom Watson a spol.*, C-203/15; C-698/15.

Právní předpisy

Sdělení Ministerstva zahraničí č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě.

Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 14. června 2006, kterou se mění směrnice Rady 78/660/EHS o ročních účetních závěrkách některých forem společností, 83/349/EHS o konsolidovaných účetních závěrkách, 86/635/EHS o ročních účetních závěrkách a konsolidovaných účetních závěrkách bank a ostatních finančních institucí a 91/674/EHS o ročních účetních závěrkách a konsolidovaných účetních závěrkách pojišťoven.

Usnesení č. 2/1993 Sb., předsednictva ČNR o vyhlášení Listiny základních práv a svobod, jako součásti ústavního pořádku České republiky, ve znění pozdějších předpisů.

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

Zákon č. 265/2001 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

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

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

Zákon č. 459/2011 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ve znění pozdějších předpisů.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.

Zákon č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony.

Úmluva Rady Evropy o počítačové kriminalitě ze dne 23. 11. 2001 účinná od 1. 12. 2013.

Vyhláška Ministerstva vnitra č. 336/2005 Sb., o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv.

Vyhláška Ministerstva průmyslu a obchodu č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Odborné články a příspěvky ve sborníku

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl). *Trestněprávní revue*, 2019, roč. 18, č. 3, s. 66-71.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*, 2019, roč. 18, č. 4, s. 77-83.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – sledování, důkazy od oznamovatelů (3. díl). *Trestněprávní revue*, 2019, roč. 18, č. 5, s. 104-109.

DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – úložiště, e-maily, telefony, sociální sítě a logy (4. díl). *Trestněprávní revue*, 2019, roč. 18, č. 6, s. 123-127.

FRYŠTÁK, Marek. Znalecký posudek, jeho význam a hodnocení v trestním řízení. *Trestněprávní revue*, 2019, roč. 18, č. 9, s. 186-189.

KOKEŠ, Marian. Judikatura ÚS: ochrana soukromí v tzv. době internetové. *Soudní rozhledy*, 2019, roč. 25, č. 6, s. 182-188.

KUCHTA, Josef. Aktuální problémy počítačové kriminality včetně její prevence. *Časopis pro právní vědu a praxi*, 2016, roč. 24, č. 1, s. 5-19.

MATES, Pavel, PÚRY, František. Zákaz nucení k sebeobviňování. *Bulletin advokacie*, 2019, roč. 49, č. 3, s. 7-13.

MATOCHA, Jakub. Informační povinnost a oprávněné subjekty podle § 88a odst. 2 TrŘ. *Trestněprávní revue*, 2019, roč. 18, č. 7, s. 152-155.

MYŠKA, Matěj, SCHAFFERER Michael, TSCHOHL Christof, VOBOŘIL Jan. *Data retention reoladed: zkušenosti, problémy a aplikační praxe*. Sborník z workshopu ze dne 23. 4. 2013 v Brně. Brno: Masarykova univerzita, Právnická fakulta, 2013. 231 s.

NAVRÁTILOVÁ, TLAPÁK, Jana, GALOVCOVÁ, Ingrid. Uchovávání dat uložených v počítačovém systému – poskytování součinnosti, nebo nahrazování činnosti orgánů činných v trestním řízení?. *Bulletin advokacie*, 2019, roč. 49, č. 11, s. 36-39.

SMEJKAL, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. *Trestněprávní revue*, 2003, roč. 2, č. 6, s. 161-167.

SOKOL, Tomáš. Povinnost dle § 7b trestního řádu z pohledu advokáta. *Bulletin advokacie*, 2019, roč. 49, č. 9, s. 15-19.

Vláda: ÚOOÚ: Vyjádření k nálezu Ústavního soudu ve věci data retention. *Právní rozhledy*, 2019, roč. 27, č. 12, s. III.

Internetové zdroje

Bezpečnostní unie: Komise usnadňuje přístup k elektronickým důkazům. [online].ec.europa.eu, 17. duben 2018 [cit. 28. 3. 2020]. Dostupné na < https://ec.europa.eu/commission/presscorner/detail/cs/IP_18_3343>.

Co je IP adresa?. [online]. alza.cz, 27. prosince 2017 [cit. 25. 3. 2020]. Dostupné na <https://www.alza.cz/co-je-ip-adresa#definice>.

CRAIG, Christina. *Poland Surveillance Law.* [online]. nordvpn.com, 12. února 2016 [cit. 26. 2. 2020]. Dostupné na <https://nordvpn.com/blog/poland-surveillance-law/>.

ČTK, EPA. *Bradáčová: Provozní a lokalizační údaje by policie postrádala* [online]. Ceska-justice.cz, 27. března 2019 [cit. 6. 1. 2020]. Dostupné na <https://www.ceskajustice.cz/2019/03/bradacova-provozni-a-lokalizacni-udaje-by-policie-postradala/?fbclid=IwAR3YvMz7Sm2QZIY7HWEr0Xc13HwlNVLSUudwkaoNffPjJ6UIzzowMp-HxFA>.

Digitální stopa. [online]. internetembezpecne.cz, [cit. 27. 11. 2019]. Dostupné na < https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/>.

IRE. *Tichá změna v trestním řádu umožňuje podle provozovatele vypnutí webu.* iDnes.cz, 12. března 2019 [cit. 7. 2. 2020]. Dostupné na <https://www.idnes.cz/zpravy/domaci/zakontrestni-rad-odstaveni-webu-data-webos-pravnik-policie.A190304_124144_domaci_lre>.

JAMES, Rebecca. *Germany Mandatory Data Retention Directives*. [online]. privacysniffs.com, 18. července 2019 [cit. 16. 2. 2020]. Dostupné na <https://privacysniffs.com/data-retention-law/germany/>.

Jednotlivé druhy kyberkriminality. [online]. policie.cz, [cit. 24. 10. 2019]. Dostupné na <https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx?q=cHJuPTE%3d>.

Kyberkriminalita na vzestupu, oběťmi jsou stále častě. ji děti. Udělejte si test. [online]. eurozpravy.cz, 10 února 2020 [cit. 9. 3. 2020] Dostupné na <https://eurozpravy.cz/domaci/zivot/kyberkriminalita-na-vzestupu-obetmi-jsou-stale-casteji-deti-udelejte-si-test.d47c0d49/ >.

MojeNokia.cz. *Víte, co znamená IMEI a k čemu slouží?.* [online]. idnes.cz, 8. srpna 2009 [cit. 26. 3. 2020]. Dostupné na < https://www.idnes.cz/mobil/tech-trendy/vite-co-znamena-imei-a-k-cemu-slouzi.A050804_153429_mob_prakticky_brz >

NAHODIL, Tomáš. *Ústavní soud rozhoduje, zda omezí shromažďování a využívání údajů o telekomunikačním provozu*. [online]. ceska-justice.cz, 27. března 2019 [cit. 6. 1. 2020]. Dostupné na <https://www.ceska-justice.cz/2019/03/ustavni-soud-rozhoduje-zda-omezi-shromazdovani-vyuzivani-udaju-telekomunikacnim-provozu/>.

Nebezpečí elektronické komunikace - strašák nebo vážný problém?. [online]. e-bezpeci.cz, 22. května 2009 [cit. 19. 3. 2020]. Dostupné na < https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/140-160>.

NOVÁK, Adam. *Zločinci se radují, FBI umí prolomit jen zlomek smartphonů* [online]. iDnes.cz, 25. května 2018 [cit. 9. 1. 2020]. Dostupné na < https://www.idnes.cz/mobil/tech-trendy/fbi-prolomeni-zabezpeceni-smartphonu.A180523_230608_mob_tech_ada?>.

OMA. *Odmítl odemknout svůj iPhone, poslali ho na půl roku za mříže* [online]. iDnes.cz, 16. července 2018 [cit. 8. 1. 2020]. Dostupné na < https://www.idnes.cz/mobil/tech-trendy/iphone-heslo-policie-vazba.A180716_134953_mob_tech_oma?>.

PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. lupa.cz, 28. dubna. 2014 [cit. 19. 2. 2020]. Dostupné na

<https://www.lupa.cz/clanky/eu-uz-nenarizuje-uchovavat-provozni-a-lokalizacni-udaje-my-v-tom-ale-pokracujeme/>

SEDLÁČKOVÁ, Miroslava. *Současná právní úprava data retention je ústavně konformní.* [online]. usoud.cz, 22. května 2019 [cit. 19. 2. 2020]. Dostupné na <https://www.usoud.cz/aktualne/soucasna-pravni-uprava-data-retention-je-ustavne-konformni/>.

ŠOULA, Martin. *Zákaz donucování k sebeobviňování, neboli nemo tenetur se ipsum accusare*. [online]. epravo.cz, 31. července 2017 [cit. 9. 1. 2020]. Dostupné na <https://www.epravo.cz/top/clanky/zakaz-donucovani-k-sebeobvinovani-neboli-nemo-tenetur-se-ipsum-accusare-106194.html>.

ŠRÁMEK, Dušan. *Odborníkům se nelíbí, že policie žádá o vydání internetových dat bez souhlasu soudu.* [online]. ekonomickydenik.cz, 28. srpna 2019 [cit. 7. 2. 2020]. Dostupné na<https://ekonomickydenik.cz/odbornikum-se-nelibi-ze-policie-zada-o-vydani-internetovych-dat-bez-souhlasu-soudu/>.

TOMAN, Petr. *Podstrčený paragraf 7b trestního řádu – kde se vzal a o čem je.* Advokátní deník. cak.cz, [online]. 22. července. 2019 [cit. 7. 2 2019]. Dostupné na <https://www.cak.cz/scripts/detail.php?id=20932>.

VARENINOVÁ, Sandra. *Princip nemo tenetur se ipsum accusare ve světle judikatury Evropského soudu pro lidská práva.* [online] epravo.cz ,16. září 2013 [cit. 9. 1. 2020]. Dostupné na <https://www.epravo.cz/top/clanky/princip-nemo-tenetur-se-ipsum-accusare-ve-svetle-judikatury-evropskeho-soudu-pro-lidska-prava-92244.html>.

VOLYŇSKÝ, Tomáš. *SIM karta: známe ji všichni, jak ale funguje a co vlastně umí?*. [online]. idnes.cz, 13. května 2008, [cit. 26. 3. 2020]. Dostupné na https://www.idnes.cz/mobil/tech-trendy/sim-karta-zname-ji-vsichni-jak-ale-funguje-a-co-vlastne-umi.A080512_233832_mob_tech_hro>.

Jiné zdroje

Důvodová zprava k zákonu č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony. [online]. beck-online.cz, 31 ledna 2018 [cit. 7. 2. 2020]. Dostupné na <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=oz5f6mrqge4f6mryg5pwi6q&rowIndex=0>.

Informovaný zdroj z prostředí PČR , působící na Krajském ředitelství policie Olomouckého kraje, Odboru analytiky a kybernetické kriminality, oddělení kybernetické kriminality.

Ministerstvo vnitra, Odbor bezpečnostní politiky. *Stanovisko OBP k aplikaci ustanovení § 7b trestního řádu.* [online]. mvcr.cz, 21. srpna 2019 [cit. 7. 2. 2020]. Dostupné na <https://www.mvcr.cz/clanek/poskytnuti-informace-metodika-tykajici-se-aplikace-7b-trestniho-radu.aspx>.

Návrh Nařízení Evropského Parlamentu a Rady o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech. [online]. eur-lex.europa.eu, ze dne 17. dubna 2018, [cit. 30. 3. 2020]. Dostupné na <https://eur-lex.europa.eu/legalcontent/CS/TXT/HTML/?uri=CELEX:52018PC0225&from=CS>.

Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě č. 104/2013 Sb. m. s..[online]. beck-online.cz, 22. srpna 2013, [cit. 7. 2. 2020]. Dostupné na <https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrg2427giydcm27geydiljq&rowIndex=0>.

Abstrakt

Tato diplomová práce pojednává o kyberkriminalitě a jejím odhalování a vyšetřování. Vyšetřování je zde míněno v širším slova smyslu a ne jen jako specifická část definovaná trestním řádem. Záměrem práce je zkoumat kriminalistický postup při odhalování této trestné činnosti a přiblížit některé postupy při zajišťování důkazních prostředků, popřípadě upozornit na jejich možné nedostatky. Tato diplomová práce převážně pracuje s právní úpravou České republiky a zabývá se postupy OČTŘ působícími v ČR. Cílem práce je poukázat nejen na kriminalistické aspekty a procesně právní aspekty, ale zároveň se pokusit spojit informace získané odborníky z praxe a poznatky kriminalistické vědy s vybranými procesními instituty TŘ. Práce je členěna do čtyř kapitol. První kapitola je věnována vymezení pojmu kyberkriminality a jejímu možnému dělení. Ve druhé kapitole je popsán možný postup OČTŘ při odhalování a vyšetřování kybekriminality, kriminalisticko-taktický postup a metodika vyšetřování. Třetí kapitola se zaměřuje na pojem digitální stopa a elektronický důkaz. Čtvrtá kapitola se zabývá vybranými způsoby zajištění důkazních prostředků a vyjadřuje se i k možným nedostatkům právní úpravy těchto vybraných institutů.

Abstract

This diploma thesis addresses the issue of cybercrime and detection and investigation thereof. The term "investigation" should be understood in its broader sense and not only as a specific part of the Code of Criminal Procedure. The aim of the thesis is to describe the criminalistic method used for detecting this type of criminality, to elaborate on selected methods of evidence collection and to identify possible weak points. For the most part, the thesis works with legal regulations valid in the Czech Republic and focuses on the activities of the Czech law enforcement authorities. The goal of the thesis is not only to pinpoint certain criminalistic and procedural or legal aspects but also to integrate information obtained by experts and insights of the forensic science with selected procedural institutes of the Code of Criminal Procedure. The thesis is divided into four chapters. In the first chapter, the definition of "cybercrime" and its possible classification are presented. The second chapter describes possible methodology of the law enforcement authorities for detection and investigation of the cybercrime, criminalistic strategy and investigation methodology. The third chapter introduces the notion of "digital footprint" and "electronic evidence". Finally, the fourth chapter analyzes selected methods of evidence collection and comments on possible weak points in the respective legal regulations.

Klíčová slova

Kybernetická kriminalita, kyberkriminalita, počítačová kriminalita, digitání stopa, orgán činný v trestním řízení.

Key words

Cybercrime, computer crime, digital evidence, law enforcement authorities.