UNIVERZITA KARLOVA

Právnická fakulta

Mgr. Michal Mohelský

Zajišťování digitálních stop pro účely trestního řízení

Rigorózní práce

Vedoucí práce: doc. JUDr. Bc. Tomáš Gřivna, Ph.D.

Datum vypracování práce: 15. 2. 2020

Prohlašuji, že jsem předkládanou rigorózní práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 321.135 znaků včetně mezer.

V Praze dne 15. 2. 2020 Mgr. Michal Mohelský

Rád bych tímto poděkoval vedoucímu této práce za cenné podněty, připomínky a konstruktivní konzultace během tvorby mé rigorózní práce.

OBSAH

ÚVOD

Trendem poslední doby je přesun lidské interakce do sítě Internet. Od doby, kdy byla síť Internet využívána zejména jako zdroj informací, uběhla dlouhá doba.

Ruku v ruce s nárůstem využívání služeb pro průmyslové, komerční, či volnočasové účely, dochází k tomu, že se do sítě Internet souběžně přesouvá i páchání trestné činnosti. Pro orgány činné v trestním řízení je přitom objasňování kybernetické kriminality poměrně novou a náročnou výzvou. Kriminalita, páchaná prostřednictvím výpočetní techniky, vyžaduje zcela nové vyšetřovací metody, než jaké současná kriminalistika a trestní právo po desítky let znalo a využívalo. Vyšetřování klade značné nároky na kvalifikované lidské zdroje, náročné technické vybavení, patřičné know-how a v neposlední řadě právní úpravu umožňující efektivní zajišťování elektronických stop, informací či důkazů s cílem zjištění pachatelů spáchaných skutků. Jednou z nejpodstatnějších fázi objasňování trestné činnosti, spáchané v síti Internet je zajišťování digitálních stop.

Pokud obecně při vyšetřování trestné činnosti platí, že vyšetřovatel je vždy krok za pachatelem, u kybernetické kriminality toto pravidlo platí dvojnásob. Stopy, které za sebou pachatel zanechává, jsou jen stěží uchopitelné. Nejčastěji se vyskytují ve formě binárního kódu. Jejich uchovávání a trvanlivost je jen velmi omezená a možností jejich zastření či pozměnění je mnoho.

Vzhledem k tomu, že o hmotněprávních aspektech kybernetické kriminality bylo napsáno již mnoho, se autor zaměří především na procesní stránku zajišťování digitálních stop za účelem odhalování pachatelů kybernetické kriminality. Digitální stopou se pro účely této práce rozumí jakákoliv skutečnost, informace a potenciální důkaz, významný pro trestní řízení.

Tato práce si bere za cíl podrobně nastínit možnosti a problémy získávání a zajišťování stop a důkazů, zajištěných v souvislosti s pácháním kybernetické kriminality. Jak to již u právních řádů bývá, reflexe zákonodárce aktuálně reagovat na potřebu vývoje právní úpravy nebývá zcela bezprostřední. U tak živelného vývoje, jakým bezpochyby rozmach sítě Internet je, tento stav bohužel není výjimkou. Práce si dále bere za cíl popis procesních institutů, které mohou být využity pro vyšetřování kriminality páchané skrze síť Internet. Rozvede podmínky pro jejich využití, meze, v jakých k jejich užití může dojít a v neposlední řadě nepomine úvahy *de lege ferenda*. Práce zohlední nejnovější rozhodovací praxi Ústavního soudu, jakož i vyšších soudních instancí obecných soudů. U jednotlivých institutů nabídne statistiky jejich využívání.

Dalším z cílů práce je analyzovat Úmluvu o počítačové kriminalitě, popsat některé procesní nástroje, které požaduje implementovat, a provést komparaci a zhodnocení, jakým způsobem se tyto nástroje staly součástí českého právního řádu.

Během tvorby práce dojde k využití metody deskriptivní, kdy autor práce podrobně popíše legislativní možnosti, kterými OČTŘ disponují. Dále dojde k popisu využívané praxe těchto orgánů. Dalším použitím komparativní metody dojde k ověření správnosti využívané praxe jejím porovnáním s judikaturou Ústavního soudu a soudů vyšších instancí obecných soudů.

Ačkoliv si autor uvědomuje, že by si téma zasloužilo zapracovat materii i v přeshraničních souvislostech, je bohužel zároveň názoru, že skutečně kvalitní zpracování této problematiky je (i vzhledem k náročnosti tématu) zcela mimo kvantitativní rozsah rigorózní práce. Krom některých nutných přeshraničních souvislostí se tedy práce soustředí na ryze českou právní úpravu. Primárně se autor věnuje skutečnostem, relevantním pro trestní řízení. Zajištění digitálních dat dále umožňují i další zákony. Například odposlech a záznam o uskutečnění telekomunikačního provozu je možné také provádět dle zákona č. 154/1994 Sb., o Bezpečnostní informační službě ve znění pozdějších předpisů a dále zákona č. 289/2005 Sb., o Vojenském obranném zpravodajství, ve znění pozdějších předpisů. Takto zajištěné informace však nemohou být považovány a použity jako důkaz v trestním řízení. Informace získané dle výše uvedených „zpravodajských zákonů“ mohou mít pouze operativní hodnotu, a sloužit jako vodítko pro získání informací v souladu s TŘ.[1]

[1] JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie.* [online] 2018, č. 9. [cit. 7. 9. 2019]. Dostupné z: https://journals.muni.cz/revue/about/submissions?navItem=0

1. Budapešťská úmluva o boji proti počítačové kriminalitě

Snaha o postihování mezinárodně páchané kybernetické kriminality v globálním měřítku vedla v roce 2001 k první významné mezinárodní snaze o harmonizaci právních úprav více států. Výsledkem těchto snah je Úmluva o počítačové kriminalitě. Tato úmluva si stanovuje několik cílů. Unifikuje skutkové podstaty některých TČ, které jsou páchány prostřednictvím výpočetní techniky. Dále zavádí procesní nástroje právních řádů jednotlivých signatářů, které jsou významným nástrojem v boji s kybernetickou kriminalitou. Významným cílem Úmluvy o počítačové kriminalitě je dále zavedení procesní úpravy mezinárodní spolupráce mezi členskými státy.[2]

Česká republika k Úmluvě o počítačové kriminalitě přistoupila v roce 2005. K ratifikaci však došlo až v roce 2013. Jak je dále rozvedeno v této práci, teprve v roce 2019 dochází k implementaci nejvýznamnější procesních nástrojů, které se Česká republika zavázala ve svém právním řádu zavést. Absence implementování procesních nástrojů ze strany některých signatářů však může vést ke ztížení odhalování pachatelů, neboť dožádaný stát nebude schopen žádosti o vydání informací vyhovět. Tím dochází k ohrožení cíle úmluvy – kterým je vytvoření prostoru, ve kterém je možné stíhat kybernetickou kriminalitu mimo hranice jednotlivých zemí.

1.1. Hmotněprávní úprava

Jak již bylo zmíněno, cílem Úmluvy je harmonizace skutkových podstat TČ v oblasti výpočetní techniky. Významná část naší národní úpravy požadavkům Úmluvy vyhověla bez dalšího. Za příklad můžeme uvést čl. 9 Úmluvy o počítačové kriminalitě[3] – Trestné činy související s dětskou pornografií. Stejná skutková podstata je již kriminalizována v ustanovení § 192 TZ ve spojení s ustanovením § 162 TZ.

Požadavek Úmluvy na kriminalizaci závadných jednání, týkající se výpočetní techniky či jednání prostřednictví této techniky spáchané byl obsažen především při rekodifikaci TZ v roce 2009. Jedná se o zavedení nových skutkových podstat TČ: neoprávněný přístup k počítačovému systému (§ 230 TZ), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ), poškození záznamu v počítačovém systému a na nosiči informací a zásah do

[2] CARTHY, Joe, KECHADI, Tahar, GILLEN, Paul. *Investigating Digital Crime.* 1. vydání. Chippenham, Wiltshire: Canterbury Christ Church University, 2008, s. 168.
[3] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě 104/2013 Sb. m. s.

vybavení počítače z nedbalosti (§ 232 TZ). Jedná se o transpozici ustanovení čl. 4 – 7 Úmluvy. Úmluva zároveň vznáší požadavek na účinné a odstrašující trestní sankce.

1.2. Procesněprávní úprava

Úmluva dále definuje legislativní nástroje, které její signatáři zavedou za účelem možnosti zajištění důkazů v elektronické podobě.

Jedná se o požadavek o implementaci následujících institutů: urychlené uchování digitálních dat a provozních a lokalizačních údajů (čl. 16 a 17), nařízení předložení digitálních dat (čl. 18), provedení prohlídky a možnost zajištění digitálních dat (čl. 19), shromažďování provozních dat (čl. 20) a odposlech obsahových dat (čl. 21).

Státy musí výše uvedené instituty implementovat v souladu s vnitrostátní úpravou, která poskytne přiměřenou ochranu lidských práv a svobod. Nejspíše i vzhledem na rozmanitost právních úprav (signatáři jsou i země jako Japonsko, Ázerbajdžán či Gruzie) Úmluva o počítačové kriminalitě požaduje garanci podmínek a záruk lidských práv v rozsahu, jak je zaručuje Úmluva Rady Evropy na ochranu lidských práv a základních svobod z roku 1950 a Mezinárodní pakt OSN o občanských a politických právech z roku 1966.

V následujících odstavcích jsou rozvedeny některé požadavky na implementaci procesních ustanovení tak, jak je vyžaduje Úmluva o počítačové kriminalitě. Právní posouzení řádnosti jejich implementace je uvedeno u konkrétních rozvedení ustanovení českého právního řádu.

1.2.1. Urychlené uchování počítačových dat

Článek č. 16 Úmluvy o počítačové kriminalitě vznáší požadavek na existenci institutu, umožňující urychlené uchování uložených počítačových dat. Každá ze smluvních stran je povinna zavést do svého právního řádu institut, který příslušným orgánům umožní nařídit:

1) urychlené zajištění nebo zachování specifických digitálních dat, včetně provozních dat, které byly uloženy prostřednictvím počítačového systému,
2) aby došlo k zajištění dat dle bodu 1) po dobu minimálně 90 dnů,
3) aby povinná osoba zachovala v tajnosti, že došlo k zajištění dat dle odst. 1

Článek 17 Úmluvy o počítačové kriminalitě dále stanovuje, že:

4) takové urychlené zachování provozních dat je použitelné bez ohledu na to, zda se přenosu dané komunikace účastnil jeden či více poskytovatelů služeb; a
5) držitel dat je povinen zajistit urychlené zpřístupnění dostatečného množství provozních dat k tomu, aby orgány daného státu mohly identifikovat poskytovatele služeb a cestu, jakou byla komunikace vedena.

Urychlené uchování digitálních dat se vžilo pod zkratku *„data freeze“*. Jedná se o jeden z nejvýznamnějších nástrojů, který Úmluva o počítačové kriminalitě do české právní úpravy zavádí. *Data freeze* se dle požadavku úmluvy má dít na pokyn OČTŘ, povinným je osoba, které má tyto data v držení, resp. dispozici. Typicky půjde o poskytovatele webhostingu či e-mailových služeb. Účelem nástroje je pouhé předejití smazání či pozměnění dat. K jejich samotnému získání či analýze mohou sloužit další procesní instituty. Tímto je však nástroj potencionálně velmi široce použitelný. Jeho užití (tedy pouhé zakonzervování, či jen zakonzervování kopie dat) nepředstavuje (oproti jiným institutům) významný zásah do lidských práv.

S implementací tohoto nástroje byla Česká republika po dlouhou dobu v prodlení. Jedná se však o zásadní procesní nástroj, který může být pro zajištění digitálních stop nepostradatelný. Podrobnosti v příslušné kapitole *data freeze* dle § 7b TŘ.

1.2.2. Příkaz k předložení digitálních dat

Článek 18 Úmluvy vznáší požadavek na přijetí institutu, který umožní jeho OČTŘ nařídit:

1) osobě, nacházející se na jeho území, aby předložila specifikovaná počítačová data uložená v počítačovém systému či na médiu,
2) poskytovateli služby, nabízející své služby na území země signatáře Úmluvy, aby předložil požadované informace, kterými disponuje o konkrétních uživatelích jeho služeb.

Česká právní úprava reflektuje požadavek článku 18 především v ustanoveních § 78, § 79 TŘ příkaz k vydání a odnětí věci, důležité pro trestní řízení a ustanovení § 8 TŘ dožádání. O tomto viz v příslušných pasážích.

1.2.3. Prohlídka a zajištění uložených počítačových dat

Článek 19 Úmluvy vznáší požadavek zavedení institutu, dle kterého budou orgány daného státu oprávněny k:

1) prohledání nebo podobnému přístupu k počítačovému systému, či datům k němu uloženým, a dále k médiu pro ukládání počítačových dat, které může obsahovat uložená data,
2) využití zavedeného institutu, na základě kterého, budou orgány státu oprávněny po zajištění zařízení či počítačového systému při důvodném podezření, že se data nacházejí i v jiném systému urychleně rozšířit prohlídku nebo podobným způsobem zajistit i v tomto druhém systému
3) výše uvedené body mají být orgány členského státu oprávněny provést způsobem, který umožňuje: zajistit, nebo podobně zabezpečit počítačový systém, jeho část či paměťové médium, pořídit bitovou kopii dat, uchovat neporušenost relevantních dat,
4) přikázání kterékoliv osobě, která má znalost o fungování počítačových systémů či jejich zabezpečení, aby poskytla nezbytné informace v přiměřeném rozsahu, umožňující provedení bodu 1 – 2 tohoto odstavce.

Česká právní úprava reflektuje požadavek článku 19 ustanovením § 82 a násl. TŘ domoví prohlídka, osobní prohlídka a prohlídka jiných nebytových prostor a pozemků a požadavek na možnost přístupu k datům v jiném systému je obsažen v § 158d odst. 3 TŘ sledování osob a věcí za využití technického prostředku. Zajišťování zařízení i vzdálený přístup do počítačových systému viz níže jako samostatné kapitoly.

1.2.4. Shromažďování provozních dat v reálném čase

Článek 20 Úmluvy o počítačové kriminalitě požaduje po stranách zavedení institutu, umožňující shromažďování provozních dat v reálném čase. Konkrétně žádá zavedení následujícího nástroje:

1) za pomoci technických prostředků na svém území provádět shromažďování nebo zaznamenávání provozních dat, vzniklých v rámci interakce počítačových systémů, a to i v reálném čase,
2) zavést povinnost ISP pomocí technických prostředků na svém území provádět shromažďování,
3) pokud právní řád strany úmluvy neumožňuje zavedení požadavku dle bodu 1), musí členský stát zajistit jiné opatření, aby pomocí technických prostředků na svém území zajistil shromažďování nebo záznam provozních dat v reálném čase, vzniklých v rámci interakce počítačových systémů.

Česká právní úprava požadavek reflektuje především v ustanovení § 97 odst. 3 ZEK které zavádí povinnost ISP k uchovávání provozních a lokalizačních údajů. OČTŘ mají k těmto údajům přístup zejména za podmínek definovaných ustanovením § 88a TŘ záznam o uskutečnění telekomunikačního provozu. Tento institut, jakož i rozsah uchovávání provozních a lokalizačních údajů je obsáhle rozveden níže.

1.2.5. Odposlech obsahových dat

Článek 21 Úmluvy o počítačové kriminalitě požaduje po stranách zavedení následujících nástrojů:

1) umožnit svým orgánům za pomoci technických prostředků na svém území shromažďování nebo záznam obsahových dat, které jsou přenášeny interakcí počítačových systémů a to v reálném čase,
2) přinutit ISP k tomu, aby za pomoci technických prostředků na svém území shromažďování nebo záznam obsahových dat, které jsou přenášeny interakcí počítačových systémů a to v reálném čase, nebo aby spolupracoval a napomáhal orgánům k tomuto.

Česká právní úprava reflektuje požadavek tohoto článku v ustanovení § 88 TŘ, který stanovuje podmínky, za kterých může dojít k zásahu do soukromí. ISP a Operátoři jsou povinni do své komunikační infrastruktury umožnit instalaci rozhraní, umožňující odposlech realizované komunikace v reálném čase.

2. PROVOZNÍ A LOKALIZAČNÍ ÚDAJE

Každou interakcí zařízení (nebo pojmem Úmluvy o počítačové kriminalitě interakcí počítačových systémů) v síti Internet vznikají data, která mohou posloužit ke komparaci této interakce s konkrétní osobou. Tyto data vznikají v rámci přenosu obsahových dat nazýváme provozní a lokalizační údaje (vznikají např. odesláním e-mailu, surfováním v síti, stažením či sdílením souboru, zalogováním na sociální síť atd.). Provozní a lokalizační údaje představují při vyšetřování kybernetické kriminality jednu z nejdůležitějších elektronických stop. Jak provozní, tak lokalizační údaje mají charakter digitální stopy.[4] Často plní roli startovacího důkazu, na základě kterého, dojde k ustanovení pravděpodobného pachatele. Typicky půjde o zajištění IP adresy, která má spojitost se spáchaným skutkem. Následně je možné splnit podmínky pro provedení domovní prohlídky, či odposlechu datového toku při kterém může dojít k zajištění dalších důkazů.[5]

Co jsou to provozní údaje definuje český právní řád v ustanovení § 90 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých zákonů (tento zákon ve znění pozdějších předpisů dále jen jako „ZEK“). Dle tohoto je provozním údajem jakýkoliv údaj, zpracovávaný pro potřebu přenosu zprávy sítí elektronických komunikací nebo pro její účtování.

Lokalizačním údajem se dle ustanovení § 91 ZEK rozumí jakékoliv údaje, které jsou zpracovávány zpracovatelem v síti elektronických komunikací nebo službou, která zpracovává elektronické komunikace, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.

[4] KOLOUCH, Jan. *CyberCrime.* 1. Vydání. Praha: CZ.NIC, 2016, s. 117.

[5] Nález Ústavního soudu ze dne sp. zn. Pl. ÚS 45/17 bod č. 24

2.1. Typy uchovávaných údajů

Rozsah uchovávání provozních údajů, jejichž uchovávání a způsob jejich předávání a likvidaci v současné době upravuje vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů (tato ve znění pozdějších předpisů dále jen jako „Vyhláška o uchovávání“).

Na tvorbě této vyhlášky, kterou vydalo Ministerstvo průmyslu a obchodu úzce spolupracovalo s Ministerstvem vnitra. Na její tvorbě se dále podíleli Operátoři, ISP, Úřad pro ochranu osobních údajů jakož i Český telekomunikační úřad. Vyhláška je tedy snahou o nalezení kompromisu mezi možnostmi a potřebami oprávněných a povinných subjektů, jakož i požadavků na ochranu těchto údajů.[6]

Dle ustanovení § 2 této vyhlášky se u sítí elektronických komunikací s přepojováním paketů uchovávají následující údaje.

U služby přístupu k Internetu z pevného připojení:

1. typ připojení,
2. telefonní číslo nebo označení uživatele,
3. identifikátor uživatelského účtu,
4. adresa MAC[7] zařízení uživatele služby,
5. datum a čas zahájení a ukončení připojení k internetu,
6. označení přístupového bodu u bezdrátového připojení k internetu,
7. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno.

U služby přístupu k Internetu z mobilního připojení je poskytovatel služeb povinen uchovávat údaje:

1. typ připojení,
2. telefonní číslo uživatele,
3. identifikátor mobilního zařízení,
4. datum a čas zahájení a ukončení připojení k internetu,
5. označení základnové stanice Start a základnové stanice Stop,
6. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno.

U služby přístupu ke schránce elektronické pošty

1. adresa IP a číslo portu, ze kterých bylo připojení uskutečněno,

[6] Nález Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 bod 20

[7] MAC adresou se rozumí jednoznačný identifikátor síťové karty uživatelského zařízení či jiného počítačového systému

2. identifikátor uživatelského účtu,
3. datum a čas zahájení připojení ke schránce elektronické pošty,
4. datum a čas ukončení připojení ke schránce elektronické pošty,
5. identifikátor protokolu elektronické pošty.[8]

U výše uvedeného se dále uchovává jméno, popřípadě jména a příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení.

Uchovávat či jakkoliv zkoumat samotný obsah přepravovaných zpráv (resp. obsah datového toku) však Operátor ani ISP není oprávněn.[9] Takto nesmí ISP činit především z požadavků, obsažených v čl. 10 a čl. 13 LZPS[10] a čl. 8 EÚLP[11]. Tento standard ochrany byl z ústavní do zákonné roviny zakotven v ustanovení § 89 ZEK, a v něm uvedené povinnosti zachovávat důvěrnost komunikací.[12]

Vyhovuje však výše uvedená definice provozních a lokalizačních údajů požadavkům Úmluvy o počítačové kriminalitě? Úmluva definuje provozní údaje extenzivním, a ne zcela konkrétním způsobem. Uvádí, že se jimi rozumí: *„jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému, vytvořená počítačovým systémem, jakožto součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby“.*[13]

Dle názoru autora není možná přesná komparace s českou úpravou, neboť Úmluva o počítačové kriminalitě nedefinuje konkrétní požadavky na informace, které mají být uchovávány. Nejzajímavější údaje, které Vyhlášky o uchovávání definuje jsou adresa MAC, označení přístupového bodu a IP adresa. Jak je rozvedeno níže, velmi významným údajem je i informace o tom, na jaké fyzické (resp. poštovní) adrese se nachází nemovitá věc, ve které je umístěn přístupový bod do sítě Internet.

---

[8] Ustanovení § 2 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

[9] VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, s. 313.

[10] Usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod

[11] Evropská úmluva o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8, Řím, vyhlášená pod č. 209/1992 Sb.

[12] MYŠKA, Matěj, HARAŠTA, Jakub a kolektiv. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015., s. 165.

[13] Ustanovení čl. 1, písm. d) Úmluvy o počítačové kriminalitě

Smyslem a cílem Úmluvy o počítačové kriminalitě je efektivní postihování a vyšetřování kybernetické kriminality. Autor uzavírá, že definice provozních a lokalizačních údajů tak, jak je definuje současná legislativa vyhovuje stanoveným cílům.

2.2. Povinnost uchovávat provozní a lokalizační údaje

Uchovávání provozních a lokalizačních údajů se vžilo pod pojmem *data retention*.[14] V minulosti prošla právní úprava *data retention* poměrně bouřlivým vývojem. Neurčitý právní rámec způsoboval, že dožádání údajů bylo ze strany OČTŘ nadužíváno. Byla patrná snaha za pomoci nich objasňovat i méně závažnou a také obecnou kriminalitu.

Mobilní Operátoři a ISP mají nyní všeobecně povinnost uchovávat provozní a lokalizační údaje. Tuto povinnost jim ukládá ustanovení § 97 odst. 3 ZEK. Dle tohoto ustanovení je ISP povinen uchovávat po zmíněnou dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování vzájemné komunikace. Jak již bylo zmíněno, provozní a lokalizační údaje definuje ustanovení § 90 a § 91 ZEK.

Nesplnění výše uvedené povinnosti uchovávat provozní a lokalizační údaje je správním deliktem[15] dle § 118 odst. 14 písm. c) ZEK, za který hrozí uložení pokuty až do výše 20.000.000 Kč. Za přestupek je však dále považováno i jednání právnické, či podnikající fyzické osoby, která den následující po uběhnutí 6 měsíců od rozhodného okamžiku údaje nezlikviduje předepsaným způsobem (viz dále).

Operátor i ISP je po uplynutí 6 měsíců povinen údaje zlikvidovat způsobem, který trvale znemožní jejich obnovení, a který provede dle technicko-organizačního předpisu. [16] Nesplnění této povinnosti je přestupkem, za který hrozí uložení pokuty až do výše 20.000.000 Kč.

Z toho plyne, že ISP jsou provozní a lokalizační údaje povinni uchovávat přesně po dobu 6 měsíců od okamžiku, kdy vzniknou. Protože však vznikají plynule v čase (každou vteřinou, v níž dochází k interakci v síti Internet či GSM) je nutné správu

[14] VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, s. 299.
[15] Po nabytí účinnost zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich se nyní jedná o přestupek, nikoliv o správní delikt.
[16] Dle ustanovení § 4 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

provozních a lokalizačních údajů provádět automatizovaně tak, aby se ISP nedopustil jednání, kdy buď nebude po určitý čas disponovat těmito údaji (tj. že je neuchová po předepsanou dobu od interakce), nebo že naopak bude těmito údaji disponovat po delší dobu (tj. že jimi bude disponovat, ačkoliv je již měl za určité uběhlé období od interakce již znehodnotit).

2.3. Vývoj právní úpravy týkající se uchovávaní provozních a lokalizačních údajů

Problematika *data retention* spadá do oblasti, jejíž unifikace náleží Evropské unii. EU v minulosti vydala směrnici Evropského parlamentu a Rady 2006/24/ES (dále jen „Směrnice o data retention“).[17] Předmětem této směrnice bylo zejména definice a stanovení rozsahu doby uchovávání údajů provozních a lokalizačních údajů.

Vzhledem k tomu, že Evropská unie přistoupila k normativnímu pramenu ve formě směrnice, vznikla členským státům povinnost směrnici implementovat. Tato směrnice byla později zrušena.[18] Zrušující rozhodnutí Soudního dvora Evropské unie sice derogovalo směrnici, národní úpravy však bez dalšího zůstaly nadále v platnosti a účinnosti. V zemích Evropské unie je tedy na národních zákonodárcích, či v jako našem případě negativním normotvůrci (derogace národní úpravy, která z této směrnice vycházela zásahem Ústavního soudu) aby rozhodl o ústavní konformitě takto provedené národní úpravy dle již neplatné směrnice EU.

Povinnost ISP a Operátorů uchovávat a poskytovat *data retention* byla do českého právního řádu v poměrně invazivní podobě přijata v roce 2005. Právní úprava reagovala na trend zvyšování trestné činnosti, týkající se kybernetické kriminality. Na našem územní byla dále implementována plně v podobě, jakou ukládala směrnice Směrnice o data retention.[19] Tato právní úprava implementující zmíněnou směrnici byla v minulosti derogována zrušujícím nálezem Ústavního soudu. Tento ve svém nálezu ze dne 22. 3. 2011, sp. zn. ÚS 24/10[20] zrušil odstavce 3 a 4 ustanovení tehdy platného a účinného § 97 ZEK. Tento nález se dále velmi významně dotkl i ustanovení § 88a TŘ[21]. Ve znění před zrušením těchto ustanovení byla velmi vágně a neurčitě popsána povinnost

[17] Nález Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 bod 7 a 24

[18] Rozsudek Soudního dvora Evropské unie ze dne 4. 4. 2014 ve spojených věcech sp. zn. C-293/12 a C-594/12

[19] Nález Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17

[20] Nález Ústavního soudu ze dne 22. 3. 2011 sp. zn. Pl. ÚS 24/10

[21] Ke zrušení tehdy účinného ustanovení § 88a TŘ došlo nálezem Ústavního soudu ze dne 20. 12. 2011 sp. zn. Pl. ÚS 24/11

právnických a fyzických osob uchovávat provozní a lokalizační údaje. Pro ukázku, tehdejší ustanovení zákona stanovovalo povinnost uchovávat provozní a lokalizační údaje následovně: „*Doba uchování těchto provozních a lokalizačních údajů nesmí být kratší než 6 měsíců a delší než 12 měsíců*“. Nález se dále kriticky vyjádřil k nejasnému a nepřesně vymezenému účelu, za jakým jsou provozní a lokalizační údaje oprávněným orgánům předávány. Provozní a lokalizační údaje byly ze strany ISP a Operátorů vydávány na základě tehdejšího ustanovení § 97, odst. 3 ZEK, dle kterého existovala všeobecná povinnost je: *„…na požádání je bezodkladně poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu.“* Absentovala dále jasná definice subjektů, které byly oprávněny k vyžádání údajů.[22]

V důsledku nejasně nastavených pravidel předávání bylo využívání těchto údajů výrazně nadužíváno i pro účely vyšetřování méně závažné kriminality. V neposlední řadě došlo k výtce absence stanovení postupu likvidace provozních a lokalizačních údajů.[23]

Po derogačním nálezu, který rozhodl o nepřípustnosti dané úpravy bylo nezbytné upravit situaci, kdy došlo k zajištění provozních a lokalizačních údajů pro účely trestního řízení ještě za účinnosti zrušených ustanovení. Ústavní soud se k použitelnosti vyžádaných údajů pro účely trestního řízení vyjádřil ve smyslu, že jejich použití ze strany obecných soudů musí být podmíněno zkoumáním proporcionality zásahu z hlediska zásahu do práva na soukromí v každém jednotlivém individuálním případě. Musí být dále zohledněna závažnost TČ.[24]

Následkem zrušení příslušných ustanovení zákonodárce do české právní úpravy s účinností od 1. 10. 2012 znovu zavedl plošné uchovávání *data retention,* resp. povinnost ISP a Operátorů k uchovávání a definování situací, kdy mohou data vydávat konkrétním subjektům.[25]

Nejnověji posuzoval ÚS danou právní úpravu na základě podnětu ke zrušení výše uvedených ustanovení (§ 88a TŘ a § 97 ZEK jakož i ustanovení dle ZOP)

[22] JIROVSKÝ, Lukáš. *Data retention – ukládání provozních a lokalizačních údajů.* Diplomová práce: Univerzita Karlova v Praze, Právnická fakulta. Praha, 2015, str. 35.
[23] VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, s. 313.
[24] VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, s. 313.

[25] K zavedení povinnosti uchování provozních a lokalizačních údajů došlo zejména nabytím účinnosti novelizace zákona č. 273/2012 Sb., která zavedla ustanovení § 97 odst. 3 ZEK, podle kterého jsou (i) ISP povinni uchovávat data po dobu 6 měsíců.

iniciovaného skupinou 58 poslanců. Navrhovatelé argumentovali neproporcionálním řešením zásahu plošného uchovávání provozních a lokalizačních údajů ve vztahu k ústavně zaručenému právu na soukromí. Nejpodstatnějším z argumentů pro zrušení, které zazněly, bylo tvrzení, že se jedná o plošné a nevýběrové shromažďování údajů, které jsou potencionálně automatizovaně zpracovatelné. Ústavní soud neposuzoval totožnou věc – zákonná úprava byla přijata v odlišné podobě, než v jaké byla zrušena (což by vzhledem k zásadě *ne bis in idem* bylo nepřípustné), ale obdobnou právní otázku. ÚS tedy zejména posuzoval ústavnost nové právní úpravy plošného uchovávání provozních a lokalizačních údajů, a dále podmínky, za kterých jsou tyto údaje vydávány.[26]

Ústavní soud dne 14. 5. 2019 v rozhodnutí pléna, vydaného pod sp. zn. Pl. ÚS 45/17 dospěl k závěru, že právní úprava *data retention* je souladná s Ústavou.

Ústavní soud podrobil nové znění obvyklým testem proporcionality, ve kterém zkoumal (1) vhodnost, (2) potřebnost, (3) přiměřenost dané legislativy.

O (1) vhodnosti (způsobilosti daného prostředku k dosažení cíle – v tomto případě objasnění trestné činnosti za využití *data retention*) neměl v řízení ÚS pochyby. Shromažďování provozních a lokalizačních údajů probíhá za účelem objasňování trestné činnosti, jakož i k cíli pátrání po osobách hledaných nebo nezvěstných. Konstatoval, že tyto cíle mají silný veřejný zájem (na ustanovení pachatele, na nalezení pohřešované nebo hledané soby atd.) a jako takové jsou tedy tyto cíle legitimní.

Potřebnost (2) posuzoval ÚS se záměrem zjistit, zda existují ve vztahu k ústavně chráněným zájmům jednotlivců mírnější prostředky, pomocí kterých by šlo sledovaných cílů (viz předchozí bod) dosáhnout. Potřebnost zákonné úpravy shledal ÚS především z důvodu, že dle jeho názoru k objasnění kybernetické kriminality neexistuje jiný ekvivalentní prostředek k případnému ztotožnění pachatele, dle již spáchaného skutku. Jedině *data retention* (tedy plošné uchování provozních a lokalizačních údajů) může vést k odhalení pachatele za využití zajištěných digitálních stop. Všechny ostatní nástroje, např. odposlech dle § 88, nebo sledování osob a věcí dle § 158d odst. 3 TŘ směřují svým použitím *pro futuro* od podmínek jejich splnění (typicky nařízení odposlechu, povolení sledování). I z tohoto důvodu je ÚS názoru, že princip *data*

[26] KOKEŠ, Marian. *Judikatura ÚS: Ochrana soukromí v tzv. době internetové.* Soudní rozhledy. Praha: C. H. Beck, 6/2019, str. 182.

preservation (za využití nástroje *data freeze*[27]) nemůže uchovávání *data retention* zcela nahradit.

Konečně ÚS vyjmenoval řadu důvodů, proč právní úpravu shledává (3) přiměřenou. Za zmínku stojí zejména následující úvahy. K délce plošného uchovávání *data retention* poznamenal, že se jedná o nejmírnější délku doby, po jakou (v okamžiku nabytí účinnosti ustanovení, zavádějící *data retention*) Směrnice o data retention plošné uchování umožňovala. Dále ohledně zabezpečení a garancí před zneužitím těchto údajů ÚS konstatoval, že sice plošné shromažďování *data retention* představuje zásah do soukromí osob, zůstává však otázkou, zda by při absenci principu *data retention* nedocházelo k využití jiných, invazivnějších metod k získání informací. S obavou, že by legislativní stín způsobil situaci ještě horší, neboť by k využívání provozních a lokalizačních údajů stejně docházelo ÚS pracuje jako s faktem ve více pasážích tohoto nálezu.

K podmínkám přístupu OČTŘ k informacím *data retention.* ÚS poznamenal, že za pozitivní posun označuje namísto dříve platné neurčité formulace „objasňování trestné činnosti" nyní pevně stanovené podmínky pro přístup k údajům, a to včetně vyjmenovaných TČ.[28]

Současné znění tedy bylo shledáno jako ústavně konformní. ÚS však zároveň nad plošným, neadresným a preventivním shromažďováním údajů pomyslně zdvihl prst s výstrahou, že pohled na konformitu *data retention* může být vzhledem k rychlému technologickému pokroku brzy změněn.[29]

Dle názoru autora je výše uvedený nález jedním z nejvýznamnějším rozhodnutí, dopadající na předmět této práce. Výsledek řízení před ÚS ho však nikterak nepřekvapil. Princip *data retention* je skutečně (jak již byl uvedeno, a jak je dále rozváděno napříč touto prací) stěžejním pilířem vyšetřování kybernetické kriminality. Na druhou stranu se nelze zcela ztotožnit s odůvodněním, jakým ÚS tento stav konstatoval.

Dokazováním se ÚS však dle názoru autora omezil pouze na vyslechnutí převážně méně, či více zainteresovaných osob. Jak plyne z nálezu, došlo zejména k vyslechnutí zástupců státního zastupitelství, zástupce Unie obhájců, PČR, jednoho ze zástupců

[27] *Data freeze* je institut, na základě kterého dochází k urychlenému zajištění existujících digitálních dat s cílem předejít jejich znehodnocení či pozměnění. Institutu se podrobně věnuje samostatná kapitola této práce.

[28] Dle nálezu Ústavního soudu ze dne 20. 12. 2011 sp. zn. Pl. ÚS 24/11

[29] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17

mobilního operátora či akademického pracovníka. Některé skutečnosti byly ÚS za fakt převzaty zavádějícím způsobem – např. konstatování o tom, že nedošlu k prokázání nadužívání údajů *data retention*, tedy že k jejich nadužívání nedochází.[30] Zavádějící jsou i statistiky, sdělené nejspíše zástupkyní spol. T-Mobile Czech Republic a.s.

Podstatnou výhradu má však autor práce k tomu, že nález pomíjí, že v době vydání nálezu již bylo součástí českého právního řádu ustanovení § 7b, odst. 1 TŘ, umožňující zajišťování provozních a lokalizačních údajů na principu *data preservation.* Ztotožňuji se však s názorem ÚS, že princip *data preservation* bez dalšího (tedy pouze využívání příkazu data freeze k zajištění digitálních stop) není schopen plnohodnotně zastoupit úlohu *data prevention* při vyšetřování již spáchané kriminality. Kupříkladu jednorázově spáchaný skutek (netrvajícího TČ) pouze za využitím metody *data freeze* není možné objasnit. OČTŘ teprve po tom, co se dozvědí o spáchání skutku mohou vydat příkaz *data freeze*. Komparace takto zajištěných digitálních stop, kde může být zajištěna i IP adresa však nebude být s čím komparována, neboť ISP nebude dle názoru autora uchovávat informace o tom, komu byla přidělena. ISP bude pouze schopen sdělit, komu IP adresa náleží v okamžiku dotázání. Na druhou stranu však toto šlo vzít v úvahu, či alespoň rozvinout v souvislosti s posouzením, zda je délka plošného uchovávání 6 měsíců přiměřená.

[30] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 bod 103

2.4. Provozní a lokalizační údaje jako osobní údaj

Současný trend české právní úpravy směřuje k navyšování standardu ochrany osobních údajů. Nejde pouze o trend právní úpravy České republiky. Snahy Evropské unie se přes harmonizaci právních úprav, tedy vydáváním směrnic, stanovující jednotný minimální standard ochrany osobních údajů přesunují ke sjednocování úprav vydáváním normativních právních aktů ve formě nařízení.[31] V nedávné době vstoupilo v účinnost nařízení, stanovující unijní standard ochrany osobních údajů, které je širokou veřejností vnímáno jako zásadní změna v přístupu k osobním údajům. Z tohoto důvodu považuje autor za vhodné rozebrat relevanci či oprávněnost uchovávat a zpracovávat digitální stopy, a jejich charakter jako osobního údaje, se zvláštním důrazem na uchování IP adresy. Na úvod autor zdůrazňuje, že IP adresa je nejčastěji pouhým identifikátorem přístupového místa do sítě Internet. K problematice podrobněji viz níže.

2.4.1. Národní úprava

Osobní údaje definoval národní předpis především v ustanovení § 4 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále také jako „Zákon o ochraně osobních údajů“). Dle ustanovení § 4 písm. a) se za osobní údaj považovala jakákoliv informace, týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže ho lze přímo nebo nepřímo identifikovat zejména na základě čísla, kódu, nebo jednoho či více prvků, specifikovaných pro jeho fyzickou, fyziologickou, psychickou, ekonomickou kulturní nebo sociální identitu.[32]

Dle ustanovení § 4 písm. d) se subjektem údajů rozuměla fyzická osoba, k níž se osobní údaje vztahují.

Od 24. 4. 2019 dochází k derogaci Zákona o ochraně osobních údajů a v účinnost vstupuje zákon č. 110/2019 Sb., o zpracování osobních údajů (dále také jako „Zákon o zpracování osobních údajů“). Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis (Nařízení EU 2016/679 viz níže).

---

[31] TÝČ, Václav. *Základy práva Evropské unie pro ekonomy*. 6. Vydání. Praha: Leges, 2010. S. 104.

[32] FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *§ 4 [Vymezení pojmů]. Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 47.

2.4.2. Unijní úprava

Dne 25. 5. 2018 vstupuje v účinnost Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES[33] (dále jen jako „nařízení GDPR“). Vzhledem k tomu, že Česká republika je členem Evropské unie, a dle ustanovení čl. 288 Smlouvy o fungování evropské unie[34] má normativní právní akt nařízení aplikační přednost před právem členského státu, se národní úprava (Zákon o ochraně osobních údajů) nadále nepoužije. Zákon ochraně osobních údajů zůstal až do 24. 4. 2019 v platnosti, dle všeobecných principů fungování evropského práva však aplikační přednost mělo nařízení GDPR.

Dle článku č. 4 odst. 1 nařízení GDPR se osobním údajem rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Dle článku č. 4 odst. 6 GDPR, se evidencí rozumí jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

Případné vydání osobních údajů je však v případě rozhodnutí soudu povinností subjektu, zpracovávající osobní údaje dle výše uvedených předpisů. Zpracovávání vydaných osobních údajů pro účely vyšetřování trestné činnosti zcela vyňato z režimu GDPR.[35]

2.4.3. IP adresa jako osobní údaj

Právní povahu IP adresy jako osobního údaje posuzoval Evropský soudní dvůr (dále jen jako „ESD“). Tento ve věci C-582/14, Patrick Breyer proti Bundesrepublik Deustchland v rámci řízení o předběžné otázce dle ustanovení čl. 267 SFEU posuzoval výklad unijního práva. V tomto řízení ESD vyložil unijní předpis, konkrétně článek č. 2

[33] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

[34] Smlouva o fungování Evropské unie. In: EUR-Lex. Úřad pro publikace Evropské unie.

[35] DOSTÁL, Otto. *Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl).* Trestněprávní revue. 2019, č. 3, str. 66.

směrnice 95/46 ve smyslu, že dynamickou IP adresu je třeba vnímat jako osobní údaj dle tohoto ustanovení.[36] Článek 2 této směrnice česká právní úprava implementovala doslovně do výše zmíněného ustanovení § 4 ZOOU. Lze tedy uzavřít, že IP adresa je osobním údajem. Je-li osobním údajem dynamická IP adresa, lze dovodit, že je tím spíše osobním údajem i statická IP adresa.[37]

2.4.4. Trend logování IP adresy

Vzhledem k výše uvedeným důvodům může být uchovávání IP adresy problematické. Současný trend ochrany osobních údajů stále posiluje na významu. Všeobecné rozpaky, které nástup GDPR v účinnost způsobil může vést mnoho subjektů, které nejsou povinny IP adresu uchovávat k tomu, že takto činit buď nebudou vůbec, nebo budou údaje IP adresy a MAC adresy uchovávat minimálně v pseudo anonymizované podobě.[38] Tyto údaje budou chtít správci osobních údajů uchovávat pouze na nezbytně nutnou dobu. Jedná se tedy o ohrožení uchovávání stop, jinak potencionálně vedoucích (po zajištění OČTŘ na základě dožádání dle § 8 TŘ či 7b TŘ k ustanovení pachatele TČ. Z hlediska odhalování kybernetické kriminality jde názoru autora o krok nesprávným směrem. Zákonná úprava by se z důvodu nezbytného uchování stop měla posunout k maximální snaze - a především legálnosti uchovávat digitální stopy. Snahy o zákonnou úpravu tímto směrem však musí být vyvíjeny na unijní, a nikoliv pouze národní úrovni.

Při úvaze *de lege ferenda* je na místě zavést zákonnou licenci pro uchovávání (logování) údajů, jako je IP adresa pro široký okruh poskytovatelů digitálních služeb, mezi které mohou patřit např. provozovatelé webových portálů, provozovatelé chatovacích služeb atd.

[36] Rozhodnutí Soudního dvora ze dne 19. 10. 2016, sp. zn. C-582/14.

[37] Takto z důvodu, že dynamická IP adresa je přidělována proměnlivě, resp. může docházet její změně (dle technických potřeb ISP) co několik hodin. Statická IP adresa je však více spojena s přístupovým bodem do sítě Internet.

[38] Wi-Fi – provoz, odpovědnost a GDPR [online]. *Miia SE*. [cit. 17. 2. 2019] dostupné z: http://news.miia.cz/gdpr/

3. ANONYMIZAČNÍ METODY

Pachatel TČ může k zakrytí stop v síti Internet využít několika nástrojů. Spolehlivost těchto nástrojů je od velmi slabé míry anonymity, až po dosahující pomyslné dokonalé anonymity. Takto je tomu zejména v případech, kdy dojde ke kombinování více anonymizačních metod. Převážná většina metod si bere za cíl zastření TPC/IP protokolu. Sofistikovanější (a tedy účinnější) metody se však se zastřením IP adresy nespokojí, a zastírají mnohem více informací.[39] Níže je rozvedeno několik z nich.

3.1. Veřejná přípojka do sítě Internet

Jednou z nejjednodušších metod zakrytí IP adresy je připojení do sítě Internet z veřejné datové přípojky. Nejčastěji půjde o připojení skrze Wi-Fi síť.[40] Veřejné Wi-Fi sítě jsou na našem území velmi hustě rozšířeny. Připojení do sítě Internet stále častěji nabízí bezplatně v restauračních zařízení či dopravních prostředcích. Je-li síť opatřena heslem, je toto heslo sděleno na požádání bez jakékoliv nutnosti předložit informace o své identitě.

Ačkoliv jsou všichni poskytovatelé připojení do sítě Internet (ISP) všeobecně povinni k uchovávání provozních a lokalizačních údajů, v případě Wi-Fi připojení je situace nejasná. Pokud je poskytováno veřejně přístupné Wi-Fi připojení, dochází nejspíše k naplnění definice služby elektronických komunikací. Mělo by tak následovat splnění povinnosti uchovávat provozní a lokalizační údaje, ke kterému však často nedochází.[41] Provozovatelé zřídka využití své Wi-Fi sítě podmíní obligatorním souhlasem s tím, že budou síť využívat dle předložených pravidel, a že se zdrží jakéhokoliv nelegálního jednání.

V praxi nedochází k častému dožádání provozních a lokalizačních údajů od těchto subjektů, kterými mohou být například provozovatelé restauračních zařízení. Technická realita zde říká, že ISP, se kterým má dané např. restaurační zařízení smlouvu o poskytnutí připojení, přiřadí restauračnímu zařízení veřejnou IP adresu. Na provozovateli restauračního zařízení by pak mělo být, aby dle vlastního logu provozu

[39] Dochází např. k zastření souboru cookies, či zastření informací o používaném rozlišení monitoru, užívaném operačního souboru, nastavení klávesnice či hardwarových parametrech. Všechny tyto informace mohou být použitelné jako digitální stopa k identifikaci pachatele.

[40] Wi-Fi se rozumí technologie, umožňující bezdrátové připojení zařízení do sítě Internet.

[41] MYŠKA, Matěj, HARAŠTA, Jakub a kolektiv. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015., s. 166.

umožnil orgánům činným v trestním řízení další postup. ISP, který smluvně zajišťuje připojení, totiž již nemá přístup k IP adresám za NATem[42].[43]

ISP dle § 97 odst. 3 ZEK však může logovat pouze informace o zařízení (routeru) umístěném v restauračním zařízení. Aktivita dalších uživatelů je známa pouze pro zařízení provozovatele. Router, tedy zařízení, ke kterému se uživatelé připojí skrze Wi-Fi síť obsahuje informaci[44] o jednotlivých MAC adresách uživatelů. Jedná se však o NAT režim, který je osobě ISP z technických důvodů neznámý. Mnoho routerů však MAC adresy (i bez vědomí provozovatele) po různou dobu loguje. **Je tedy reálné po zajištění či vytěžení routeru analýzou jednotlivých přiřazených MAC adres a IP adres ve vnitřní síti přičíst jednání, které bylo učiněno skrze veřejnou IP adresu poskytovatele Wi-Fi připojení.** Router může být zajištěn na při výzvě k vydání či při odnětí věci, nebo při provedení domovní prohlídky (viz kapitola fyzické zajišťování důkazů). Dle názoru autora se takto často neděje, router v sobě přitom může obsahovat důležité důkazy o provozu NATu. Ty mohou přispět k vytvoření uceleného řetězu nepřímých důkazů.

Dojde-li ke spáchání útoku v síti Internet skrze tuto přípojku, OČTŘ při využití institutu § 88a odst. 1 TŘ odhalí o pachateli nejvýše toliko, že se v daný čas fyzicky nacházel poblíž tohoto přístupového bodu. Ani tento údaj však není bez dalšího jistý, pachatel mohl nacházet v blízkosti routeru, či v případě rozšíření signálu se nacházet v okruhu několika desítek metrů od tohoto restauračního zařízení.

Jedná se o pravděpodobně nejméně spolehlivou anonymizační metodu. Zpětným došetřením je možné zmapovat pohyb podezřelého, zda se v daných prostorách nacházel, či v případě restauračního zařízení komparovat platby, které byly v této provozovně realizovány.

---

[42] IP adresa prozradí často jen router, ze kterého bylo přistupováno do sítě Internet. Další provoz se děje na základě rozdělování požadavků dle MAC adres – tento provoz je bez fyzického zajištění a analýzy zajištěných zajištění OČTŘ skryt a tento „vnitřní“ provoz mezi zařízením a routerem, typicky ve Wi-Fi síti se označuje za NAT. V případě, že k připojení do sítě Internet došlo skrze mobilní zařízení s mobilním připojením se však o NAT nejedná – ISP by měl mít možnost (po omezený časový okamžik) zjistit, kterému uživateli přidělil danou IP adresu v konkrétní čas.

[43] MYŠKA, Matěj, HARAŠTA, Jakub a kolektiv. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015., s. 166.

[44] Ve vnitřní síti (např. Wi-Fi) dochází k přerozdělování informací na základě MAC adres, které jsou jednoznačné identifikátory uživatelských zařízení

3.2. VPN

Virtuální privátní síť (*Virtual Private Network*) dále jen jako „VPN“, je název služby, která kompletní, nebo částečnou komunikaci (například pouze některých portů) směruje šifrovaným tunelem skrze VPN server. Požadavek, který odchází z koncového uživatelského zařízení je veden na tento server, který ho dešifruje, a následně provede. Po obdržení odpovědi informaci VPN server zašifruje, a bezpečným šifrovaným tunelem skrze síť Internet doručí koncovému zařízení. Cílový subjekt, na který byl požadavek vznesen (například navštívená webová stránka) tak zná pouze identitu přistupujícího VPN serveru, a identita koncového zařízení mu zůstane skryta. Dojde tedy k pouze k zalogování identifikačních údajů VPN serveru.[45] Pokud se OČTŘ pokusí po VPN provozovateli dožádat údaje, ze kterých bylo např. na webovou stránku pachatelem přistupováno, dojde pouze k poskytnutí údajů IP adresy VPN serveru, nikoliv IP adresy datové přípojky,[46] ze které se připojil pachatel.

V zahraničí byly zaznamenány případy, kdy společnost, která zákazníkům poskytovala VPN služby na žádost OČTŘ vydala záznamy logů konkrétních uživatelů.[47] Tato skutečnost, tedy že reálně hrozí, že společnost předá podrobné logy OČTŘ byla zaznamenána v kriminálním prostředí, a způsobila velké narušení důvěru v tento druh anonymizační metody. Společnosti nyní své VPN služby prezentují jako s nulovou politikou logování, tedy se striktním nepořizováním záznamů o datovém provozu svých zákazníků. Přesto však všeobecně došlo ke značnému otřesu v důvěru v tuto službu.[48]

Pro pachatele TČ je dále tato metoda riziková z důvodu, že užívá svůj vlastní webový prohlížeč. Nezabezpečený webový prohlížeč sice díky VPN zastírá skutečnou IP adresu, ale není ve standardním nastavení nakonfigurován k tomu, aby skrýval identitu svého uživatele. Webové služby, jako je např. e-mail, Facebook, či Twitter při načtení titulní stránky neidentifikují jednotlivé uživatele dle přihlášených účtů dle IP adresy, ale např. dle souboru cookies. V takovéto situaci tedy pachatel zakryje svou IP

[45] ŠEPTUN, Michal. *Identita v tunelovaných a překládaných sítích.* Brno: Vysoké učení technické v Brně, Fakulta informačních technologií. Diplomová práce, 2014/2015, str. 13. Vedoucí práce POLČÁK, Libor.

[46] OČTŘ dožádají dle § 8 TŘ údaj IP adresy, obdrží však pouze číselný údaj IP adresy, který je nezbytné postupem dle § 88a odst. 1 TŘ ve spojení s § 97 odst. 3 ZEK ztotožnit s datovou přípojkou – přístupovým místem do sítě Internet.

[47] WHITWAM, Ryan. *Supposedly Non-Existent VPN Logs Help FBI Catch Internet Stalker.* ExtremeTech. [online]. 2017 [cit. 1. 2. 2019]. Dostupné z: https://www.extremetech.com/internet/257214-supposedly-non-existent-vpn-logs-help-fbi-catch-internet-stalker

[48] Viz například veřejná nabídka služeb společnosti Tefincom S.A. [online]. 2020 [cit. 30. 1. 2020]. Dostupné z: https://nordvpn.com/features/strict-no-logs-policy/

adresu, ale stále může odhalit jiná data, která potencionálně mohou umožnit jeho identifikaci zanecháním jiných digitálních stop.

3.3. TOR

Síť Tor je v době tvorby této práce jeden z nejdokonalejších anonymizačních nástrojů pro přístup a provádění aktivity v síti Internet. Svým uživatelům při využití webového prohlížeče Tor browser umožňuje anonymní, avšak plnohodnotný přístup na webové stránky v síti Internet a v síti Darknet (podrobněji v následující podkapitole). Krom samotného přístupu umožňuje uživatelům plnohodnotné využití formulářů a aplikací, jako např. využití webového rozhraní e-mailové služby či provádění online plateb. Jeho využití není zpoplatněno a stažení je volně přístupné libovolnému okruhu osob. Využití sítě nevyžaduje žádné pokročilé uživatelské znalosti, její užití je co do náročnosti srovnatelné se stažením, instalací a spuštěním prohlížeče Firefox (na jehož uživatelském rozhraní upravený webový prohlížeč ostatně funguje).

„*Síť vysoce sofistikovaný způsobem zakrývá skutečnou identitu uživatele výše uvedeného prohlížeče. Toho dosahuje tím, že když se uživatel rozhodne přistupovat skrze síť Tor do Internetu, pak nejdříve musí sestavit okruh vedoucí přes několik uzlů sítě Tor. Informace od uživatele jsou předávány postupně mezi uzly sítě Tor až k tzv. výstupnímu uzlu. Výstupní uzel vytvoří běžné spojení TCP k serveru umístěnému v Internetu. Odpovědi od serveru jsou předávány po stejné cestě zpět směrem k uživateli. Server na Internetu nevidí v požadavcích IP adresu uživatele, ale IP adresu výstupního uzlu sítě Tor. Veškerá komunikace uvnitř sítě Tor je šifrovaná a uzly sítě Tor mimo výstupního neznají skutečný cíl komunikace. Pouze vstupní uzel sítě Tor zná IP adresu uživatele.*

Cílem několikanásobného předávání zpráv v síti Tor je promíchání provozu všech uživatelů sítě Tor. Promícháním provozu dává síť Tor každému z uživatelů možnost popření autorství dat, protože není jednoduše zjistitelné, kdo která data vytvořil.“[49]

Tor Browser nejen že zakrývá IP adresu přístupu do sítě Internet, ale komunikaci v síti dále efektivně šifruje. Krom toho ve standardním nastavení blokuje soubory cookies. Obzvlášť v kombinaci s některou z výše uvedených metod, jako je využití služby VPN či připojení do sítě Tor z veřejné přípojky se jedná o prakticky dokonalé zakrytí stop, které mohou vést k jednotlivým pachatelům trestné činnosti. Využitím Tor

[49] POLČÁK, Libor. *Základní informace o síti Tor*. Brno: Vysoké učení technické v Brně, Fakulta informačních technologií. Technická zpráva č. FIT-TR-2017-01. Brno: 2017, str. 1.

dojde vzhledem k šifrování datového toku k případnému vyřazení sledování provozu datového provozu dle § 88 TŘ.

3.4. Darknet

Síť Tor umožňuje fungování vysoce sofistikované anonymizované obdoby sítě Internet. Jedná se o vytváření portálů, fungujícím na obdobném principu, jako jsou webové stránky. Ve skutečnosti se však jedná o skrytou část Internetu, označovanou jako „Darknet“. Pro Darknet je typické, že je přístupná pouze skrze prohlížeč Tor, a navštěvované stránky disponují koncovkou „.onion“. Na těchto stránkách často dochází ke kumulaci závadného obsahu, jako je například dětská pornografie, podrobné návody k výrobě výbušnin či jsou zde hostovány tržiště, které umožňují zakoupení omamných a psychotropních látek. Jednou z těchto darknetových stránek bylo i tržiště Sheep marketplace, o kterém podrobně níže.

Doménu „.onion“ můžeme označit za pseudodoménu. Není obsažena v kořenových DNS (Domain Name System) serverech, které jinak spravuje nezisková organizace ICANN se sídlem v Los Angeles. Jedná se tedy o vlastní DNS systém. Cílem Darknetové existence (či infrastruktury) je skrýt identitu uživatelů, provozovatelů a návštěvníků darnetové infrastruktury. [50]

Pohyb a vyhledávání na Darknetu usnadňuje nástroj NotEvil.[51] Tento nástroj je jakousi darknetovou obdobou vyhledávače Google v klasické síti Internet. Dle klíčových slov vyhledává relevantní portály, na které proklikem umožňuje přístup.

Krom již zmíněného tržiště Sheep Marketplace, je pro účely této práce nezbytné zmínit darnetové tržiště Silk Road. Toto tržiště je mezi českými uživateli známo jako Hedvábná stezka. Obdobně jako v případě tržiště Sheep Marketplace šlo o burzu, která sloužila pro anonymní nákup a distribuci zbraní, omamných a psychotropních látek a jiných zakázaných aktivit či zboží. V USA došlo k dopadení pachatele, provozující portál Silk Road. Údajně při vyšetřování došlo k dosazení agenta do organizace portálu. Nejednalo se tedy o prolomení zabezpečení sítě Tor, ale o klasickou detektivní práci. [52]

[50] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 497.

[51] Nástroj je dostupný na adrese https://hss3uro2hsxfogfq.onion.to Ačkoliv se jedná o vyhledávač ve speciální síti Tor, která vyžaduje při přístup na darknetové stránky zvláštní prohlížeč Tor browser, vyhledávač samotný je volně přístupný i z běžných prohlížečův síti Internet.

[52] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 71.

3.5. GeoIP

V případě, že se podaří zajistit IP adresu, v rámci prověřování policejní orgán vyhodnocuje, nakolik může být tento dílčí údaj relevantní. K těmto účelům může sloužit nástroj GeoIP.[53] Na síti Internet existuje nespočet nástrojů, které po zadání IP adresy zobrazí přibližnou geografickou polohu, na které se přístupový bod do sítě Internet nachází. Využití tohoto nástroje je nedocenitelné především z důvodu rychlé filtrace IP adres, které byly zamaskovány.

Policejní orgán může vkládat jednotlivé IP adresy do nástroje GeoIP, a velmi rychle vyhodnotit geografické polohy, ze kterých bylo do sítě Internet (resp. ke konkrétnímu cíli) přistupováno.

Tento nástroj může také v případě zajištění velkého logů IP adres sloužit k rychlé selekci okamžiků přístupu, při nichž byl využit anonymizační nástroj. Anonymizace často využívá toho, že jednotlivé relace propojuje přes servery, nacházející se v různých státech. Je-li tedy zajištěn seznam logů, kdy po porovnání IP adres policejní orgán nazná, že od ranních do večerních hodin byly jednotlivé přístupy vedeny z takových vzdáleností, při kterých není technicky možné, aby se pachatel fyzicky přepravil, jde logicky o zjištění, že pachatel využívá anonymizační nástroj. Nelze však vyloučit ani situaci, kdy je pachatelů více, a že přistupují do sítě Internet z různých států.

4. ZAJIŠŤOVACÍ ÚKONY

Zajišťovacím úkon se pro účely této práce rozumí provedení takových úkonů, které směřují zejména k zajištění digitálních stop, informací či dalších skutečností. Tyto lze definovat jako úkony, jejichž neprovedení před zahájením trestního stíhání (případně z důvodu velkého časového odstupu od skutku k trestnímu stíhání), by z oprávněných důvodů mohlo vést ke ztrátě nebo k nebezpečí zmaření či zničení důkazů.

Provádění zajišťovacích úkonů daleko před pravomocným odsouzením pachatele z principu nabízí dva protichůdné náhledy.

Za prvním z nich můžeme považovat, že zajišťovacích úkonů bude často nutné provádět bez zbytečného odkladu, neboť elektronické stopy mohou být snadno pozměnitelné či se uchovávají jen po omezenou dobu. Jejich včasné neprovedení může výrazně zkomplikovat, či zcela znemožnit vyšetření spáchaného TČ.

Druhým pohledem je však při provádění úkonů v souladu se zásadou presumpce nevinny zároveň nutno šetřit práva podezřelé osoby, proti níž úkony směřují. Níže

[53] Takovým nástrojem je například https://geoiptool.com/en/

popsané úkony se vyznačují invazivní formou. Mají charakter operativně pátracího prostředku, a jako takové by neměly sledovat jiný cíl, než získání informací důležitých pro trestní řízení.[54] Téměř všechny mají jedno společné – zásah do ústavně zaručeného práva a svobody. Demonstrativně můžeme jmenovat zásah do práva na informační sebeurčení,[55] listovní tajemství, nedotknutelnost obydlí atd. Takový zásah je možný jen v zákoně aprobovaném případě a za splněním daných podmínek. Nedodržení podmínek pro zásah do ústavně zaručených práv a svobod ze strany OČTŘ má přirozeně negativní následky. Od pouhého vzniku práva na náhradu nemajetkové újmy až po nepoužitelnost daného důkazu – či dokonce sérii dalších důkazů a skutečností, ke kterým nelegálně pořízený důkaz přispěl.

Protože cílem níže uvedených zajišťovacích úkonů je často prvotní identifikace možných podezřelých osob, jsou často návrhy na provedení úkonů ze strany soudního orgánu činěny proti (v okamžik rozhodování o přípustnosti prostředku) neznámé osobě.

Smyslem těchto níže uvedených opatření OČTŘ by mělo být předcházení, odhalování a objasňování trestné činnosti, pátrání po skrytých pachatelích či věcných důkazech.[56]

Ačkoliv jako důkaz může v trestním řízení, i vzhledem k uplatňování zásady volného hodnocení důkazů posloužit cokoliv, je nutné dodržení řádné formy zajištění skutečností, které mohou být považovány za důkaz. Práce níže rozvádí nejpodstatnější instituty, které mohou být využity k zajišťování digitálních důkazů.

4.1. Záznam o uskutečnění datového provozu dle § 88a TŘ

Pro ztotožnění zajištěných digitálních stop, které mají formu provozních a lokalizačních údajů s možným pachatelem nejčastěji poslouží nástroj záznam o uskutečnění o telekomunikačního provozu. Při vyšetřování kybernetické kriminality půjde nejčastěji po zajištění provozních a lokalizačních údajů (typicky IP adresy) dle nástroje dožádání (viz níže) o učinění dotazu v režimu tohoto nástroje na ISP. Sledovaným cílem je zjištění, ke které fyzické osobě stopy, ve formě provozních a lokalizačních údajů např. IP adresy) náleží.[57] Využitím tohoto institutu je však také

[54] Usnesení Ústavního soudu ze dne 16. 4. 2019 sp. zn. II. ÚS 1095/19 bod č. 12

[55] MATOCHA, Jakub. *Informační povinnost a oprávněné subjekty podle § 88a odst. 2 TrŘ.* Trestněprávní revue. 2019, č. 7-8, s. 152.

[56] Usnesení Ústavního soudu ze dne 16. 4. 2019 sp. zn. II. ÚS 1095/19 bod č. 9

[57] Přestože cílem je ztotožnění fyzické osoby, zejména z IP adresy dojde spíše ke zjištění přístupového bodu do sítě Internet.

možné o konkrétní fyzické osobě, vůči níž směřuje sestavit z provozních a lokalizačních údajů komunikační profil za období 6 měsíců, od vydání příkazu k vydání záznamu o uskutečnění telekomunikačního provozu.[58]

Tento institut upravuje především ustanovení § 88a TŘ ve spojení s ustanovením § 97 odst. 3 ZEK. Jedná se o identický institut, kterým dochází k získání informací o realizovaném telekomunikačním provozu mobilním zařízení (mobilní telefon) nebo dnes již téměř obsolentním pevným zařízení (pevná linka) v síti GSM.[59]

Využití institutu je možné se souhlasem nebo bez souhlasu sledované osoby. Pokud souhlas nebyl udělen, nebo je tato osoba neznámá a primárním cílem využití institut je její ustanovení, musí být k využití institutu kumulativně splněny následující podmínky:

1 řízení je vedeno pro:
   a) úmyslný TČ s horní hranicí sazby odnětí svobody nejméně 3 roky, nebo
   b) pro některý z TČ dle § 182, § 209, § 230, § 231, § 353, § 354, § 357, §365 TZ[60] (tedy takové, převážně související s kybernetickou kriminalitou),
   c) pro úmyslný TČ, k jehož vydání zavazuje vyhlášená mezinárodní smlouva,
2 sledovaného účelu nelze dosáhnout jiným způsobem, nebo by jiný postup dosažení účelu ztěžoval,
3 vydání údajů musí nařídit předseda senátu nebo samosoudce.[61]

První podmínkou je stanovení okruhu TČ, pro jejichž objasnění je využití institutu možné. Hranice trestu odnětí svobody nejméně po dobu 3 let je výrazně nižší, než pro odposlech (§88 TŘ), kdy TŘ podmiňuje využití pro objasnění TČ se spodní sazbou 5 let. Zároveň však zákonodárce umožnil pomocí § 88a TŘ objasnění těch TČ, které sice nesplňují podmínku minimální trestní sazby, avšak jsou často páchány v síti Internet (např. TČ podvodu, pomluvy atd.). Zejména druhou podmínku lze při identifikaci neznámého pachatele ze zajištěných elektronických stop (zejména IP adresy) považovat za splněnou bez dalšího. Právě zajištění IP adresy lze vnímat jako nejpravděpodobnější

[58] MATOCHA, Jakub. *Informační povinnost a oprávněné subjekty podle § 88a odst. 2 TrŘ.* Trestněprávní revue. 2019, č. 7-8, s. 152.

[59] Dle tohoto nástroje dochází i k identifikaci uživatelských stanic mobilních telefonů, které byly v daný okamžik připojeny ke konkrétní buňce operátorů. OČTŘ mají možnost zjistit, kdo se v daný okamžik pohyboval přibližně v jaké místě tím, že si vypíší seznam připojených zařízení k buňce, která se nachází na místě činu.

[60] Tímto se rozumí zákon č. 40/2009 Sb., trestní zákon, ve znění pozdějších předpisů

[61] MYŠKA, Matěj, HARAŠTA, Jakub a kolektiv. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 172.

digitální stopu. Tato stopa po využití ustanovení § 88a TŘ nabídne informaci o tom, kterému koncovému bodu (přístupovému místu do sítě Internet) byla v čase spáchání TČ přidělena. Třetí podmínka stanovuje, že o vydání provozních a lokalizačních údajů rozhoduje soudní orgán.

K přechozímu znění právní úpravy, které bylo derogováno nálezy ÚS (ÚS 24/10 a ÚS 24/11). Za jeden ze stěžejních argumentů pro zrušení stávající úpravy ÚS právě vnímal absenci stanovení konkrétních TČ, či kritérií, za kterých můžou být provozní a lokalizační data využita pro trestní řízení. Při posuzování testu proporcionality – přiměřenosti (k omezení základního práva dle čl. 10 a 13 LZPS) shledal právní úpravu za nevyhovující. Definoval tedy, že použití těchto údajů by mělo být relevantní *"...jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy a jen pro případ, že nelze sledovaného účelu dosáhnout jinak".*[62] Česká právní úprava definicí „zvlášť závažných trestných činů" nedisponuje. Zákonodárce zvolil k možnosti využití uchovávaných dat výše uvedenou podmínku, tedy úmyslné trestné činy, za které hrozí trest odnětí svobody s horní hranicí 3 roky. K tomu je obsažen taxativní výčet TČ, jejichž objasnění při spáchání v síti Internet by jinak bylo obtížné, ne-li nemožné. Soudní dvůr EU ve věci Digital Rights Ireland[63] taktéž dovodil, že využití provozních a lokalizačních údajů je možné za legitimní cíl považovat při vyšetřování závažné trestné činnosti.[64] Tuto definici EU nyní ponechává na jednotlivých členských státech.

Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a řádně odůvodněn. Jedná se o rozhodnutí *sui generis*. Vztahuje-li se žádost ke konkrétnímu uživateli, musí být v příkazu uvedena jeho totožnost, je-li známa. Dle ustanovení § 88a odst. 2 je státní zástupce, nebo policejní orgán, 1 jehož rozhodnutím byl věc pravomocně skončena povinen uvědomit o nařízením zjištění údajů o telekomunikačním sledovanou osobu, byla-li zjištěna. Součástí sdělené informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k zjištění údajů o telekomunikačním provozu. O přezkumu zákonnosti příkazu více viz níže.

[62] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 bod č .100

[63]Rozsudek Soudního dvora Evropské unie ze dne 4. 4. 2014 ve spojených věcech sp. zn. C-293/12 a C-594/12

[64]Rozsudek Soudního dvora Evropské unie ze dne 4. 4. 2014 ve spojených věcech sp. zn. C-293/12 a C-594/12

4.1.1. Příkaz dle § 88a TŘ *pro futuro*

Výše bylo zmíněno, příkaz k vydání záznamu o uskutečněném telekomunikačním provozu směřuje do období 6 měsíců před jeho vydáním (připomeňme, že ISP mají povinnost plošně uchovávat provozní a lokalizační údaje právě po tuto dobu). Nejvyšší soud aktuálně vnesl na ustálený stav, kdy se žádá až 6 měsíců zpětně zásadně odlišný názor. **V usnesení z května roku 2019 Nejvyšší soud posvětil postup soudů nižších instancí, které vydaly příkaz dle § 88a na sledované období nikoliv zpětně, ale do budoucna – tedy *pro futuro*.** [65]

Nejvyšší soud konstatoval, že příkaz k vydání *data retention* všeobecně míří do minulosti. V některých výjimečných případech je však možné v příkazu nařídit vydávat *data retention* do budoucna. Takový postup dle NS bude odůvodňovat zejména situace, kdy trestná činnost bude teprve připravována a bude se tedy jednat o ranou fázi páchání trestné činnosti. Zjišťované údaje mají směřovat zejména k ustanovení či zajištění důkazů o konkrétní osobě pachatele. Cílem získaných informací by dále mělo být ustanovení dalších osob, zjištění, kde se které osoby nacházely či informace, umožňující znemožnění dokonání TČ. Použití příkazu do budoucna by mělo být užito v případě, kdy by OČTŘ naznaly, že není na místě invazivnějšího zásahu odposlechu dle § 88 TŘ.

Dle názoru autora k zajišťování reálných telekomunikačních dat slouží pouze nástroj odposlechu dle § 88 TŘ. Jak je podrobně pojednáno níže, podmínky pro jeho naplnění a umožnění jsou přísnější. Zákonodárce si toho při jejich definování byl zjevně vědom. Není tedy přípustné, využívat méně invazivní prostředek k (způsobem jeho užití) invazivnějšímu užití. Takto extenzivně vykládaný nástroj dle § 88a TŘ by mohl vést k tomu, že za podmínek jeho naplnění může způsobit, že bude ISP o sledované osobě poskytovat údaje po dobu nejspíše až 6 měsíců po vydání příkazu. OČTŘ tedy budou mít krom plošně uchovávaných po dobu 6 měsíců zpětně možnost využít i stejného období do budoucna, tj. celkem 12 měsíců, kdy podezření na konkrétního pachatele možná existovalo pouze uprostřed této doby.

Cíle, jakých soudy nižších instancí extenzivním výkladem sledovaly (zjištění osoby a zamezení postupu vývoje rané fáze skutku v dokonaný) se nijak neliší od cíle každého trestního řízení. Dle názoru autora je tedy takto extenzivní výklad v posuzovaném případě nepřípustný. Jakákoliv data z telekomunikačního provozu v reálné době přenosu informací mohou být realizována pouze postupem a za splnění podmínek dle § 88 TŘ. Nelze se ztotožnit ani s výkladem § 2 odst. 4 TŘ dle kterého

[65] Usnesení Nejvyššího soudu ze dne 7. 5. 2019 sp. zn. 4 Tdo 1591/2018

OČTŘ tímto postupem šetří práva podezřelé osoby. Dle názoru NS je vhodnější § 88a TŘ použít *pro futuro* spíše něž § 88 TŘ, neboť 88a TŘ je méně invazivnějším nástrojem. Ostatně i poslední nález ÚS, zabývající se *data retention* konstatuje, že: *„Zatímco nařízení odposlechu lze podezřelou osobu monitorovat do budoucna, provozní a lokalizační údaje umožňují oprávněným osobám získat informace o skutku, který se již stal (...).“*.[66] Z toho sice striktně neplyne, že by ÚS vylučoval použití *data retention pro futuro*, zároveň je však jisté že ani on sám jeho použití takto nepředpokládá. Jak je zmíněno v tomto nálezu, z provozních a lokalizačních údajů je možné utvořit komplexní komunikační obraz sledované osoby, který je v některých případech i více vypovídající, než provádění odposlechu v režimu § 88 TŘ.

Lze očekávat, že proti tomuto usnesení NS bude podána ústavní stížnost. Bude tedy na ÚS, aby posoudil, zda je tento extenzivní výklad § 88a TŘ přípustný. Autor se kloní k závěru, že rozhodnutí je v rozporu se zásadou přiměřenosti, vyjádřenou v TŘ a jako takový je tento výklad nepřípustný. V případném testu proporcionality, kdy dosazované otázky nám napovídá již zmíněný nález, neb jde o věc velmi podobnou se autor domnívá, že by test nebyl úspěšný v kroku (2) potřebnosti a (3) přiměřenosti.

Z pohledu kroku (2) potřebnosti autor vnímá ve svém důsledku použití odposlechu a záznamu o tel. provozu méně invazivním, než prováděním úkonu dle § 88a TŘ takto extenzivním způsobem. Jak již bylo zmíněno, dle provozních a lokalizačních údajů je možné sestavit komunikační profil osoby, či mít podrobný přístup k její aktuální poloze (použitím buněk sítě). Z hlediska intenzity zásahu jde o srovnatelný, ne-li intenzivnější zásah než provádění odposlechu. Fakticky tedy bude po dobu až 6 měsíců po nařízení příkazu k vydávání dat docházet k zásahu, srovnatelným s odposlechem. Podmínky pro tento úkon jsou však méně přísné, než je tomu u odposlechu a záznamu tel. provozu.

Ani z pohledu kroku (3) přiměřenosti tento výklad neobstojí. Poměrně benevolentně nastavené podmínky pro vydání příkazu k vydání *data retention* (když tyto podmínky splňuje významná většina skutkových podstat TČ) neodpovídají takto intenzivnímu zásahu do soukromí osob. Znovu je nutno připomenout, že se jedná o údaje jako je geografická poloha, informace o tom, s kým a jak dlouho daná osoba komunikuje, podrobné údaje o aktivitě na návštěvách webových stránek atd.

Jediným východiskem, pokud by údaje *data retention* bylo nutné získávat do budoucna je dle názoru autora ze strany soudu vydání příkazu jak dle § 88a, tak 88 TŘ,

[66] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 bod č. 86

tedy kombinace obou zákonných nástrojů. Tím je zajištěna ochrana práv podezřelého, neboť jsou zde splněny přísnějších podmínek pro zásah do ústavně zaručených práv (zejména § 88 TŘ).

4.1.2. Předávání provozních a lokalizačních údajů

Dotazy o jednotlivých zajištěných digitálních stopách směřuje zejména PČR na ISP. Pokud není z údajů jasné, jakému ISP je přidělena, jsou žádosti o sdělení údajů o uživateli adresována všem ISP, neboť nelze spolehlivě předem určit, kterému ISP konkrétní IP adresa náleží.[67]

Právnická nebo fyzická osoba, která provozní a lokalizační údaje na základě ustanovení § 97 odst. 3 ZEK uchovává, je povinna na požádání tyto údaje poskytnout OČTŘ za podmínek, které stanoví TŘ, ZEK či ZOP.

Jsou-li informace o provozních a lokalizačních údajích vyžádány PČR, podmínky jejich předávání definuje § 66 ZOP. Zákon předpokládá, že provozní a lokalizační údaje budou předávány způsobem umožňující dálkový a nepřetržitý přístup. Povinné osoby jsou žádosti povinny vyhovět bez zbytečného odkladu a ve formě a rozsahu stanovené ve vyhlášce 357/2012 Sb., o uchovávání a předávání provozních a lokalizačních údajů. PČR je přitom povinna žádat o poskytování údajů pouze takovým způsobem, který do 5 let od požádání umožní identifikovat (1) příslušný útvar nebo konkrétního policistu, který žádal a (2) účel, za jakým k dožádání údajů došlo.[68]

V režimu trestního řádu dochází k dožádání provozních a lokalizačních údajů dle ustanovení § 88aTŘ, tedy v režimu poskytnutí záznamu o uskutečnění datového provozu. Dožádat však nelze dle § 88 TŘ, neboť toto ustanovení upravuje postup při nařízení odposlechu telekomunikačního (včetně datového) provozu. O tomto viz níže.

V souvislosti s vydáním údajů dále vzniká nárok osobám, které údaje OČTŘ poskytnou na úhradu efektivně vynaložených nákladů, které vzniknou v souvislosti s předáním údajů.[69]

---

[67] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2018.* Policejní prezidium České republiky. [online] publikováno 22. 8. 2019 [cit. dne 1. 09. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

[68] VANGELI, Benedikt. *§ 66 [Získávání informací z evidencí]*. Zákon o Policii České republiky. 2. vydání. Praha: Nakladatelství C. H. Beck, 2014, s. 276.

[69] JAMBOROVÁ, Kateřina. *Provozní a lokalizační údaje, nález Ústavního soudu a § 88a TŘ*. Trestněprávní revue. 2012, č. 3, s. 61-65.

V případě neposkytnutí údajů ve výše uvedených situací se povinná osoba dopouští přestupku dle § 118 odst. 14 písm. c) ZEK. Za toto jednání jí hrozí uložení pokuty ve výši 20.000.000 Kč.

4.1.3. Statistiky dožádání

Dle žádosti v režimu zákona o svobodném přístupu k informacím[70] byla autoru této práce sdělena statistika dožádání IP adres v letech 2013 až 2019.[71] Dle sdělených informací PČR požádala o sdělení informací k jednotlivým k datové přípojkám (přístupovým bodům do sítě Internet) adresovaných ISP (poskytovatelům internetového připojení, který s jednotlivým uživatelem uzavřel smlouvu o poskytování telekomunikačních služeb). Dle poskytnutých informací:

- za období od 1. 1. 2013 do 31. 12. 2013 bylo podáno 1065 žádostí,
- za období od 1. 1. 2014 do 31. 12. 2014 bylo podáno 1182 žádostí,
- za období od 1. 1. 2015 do 31. 12. 2015 bylo podáno 1329 žádostí,
- za období od 1. 1. 2016 do 31. 12. 2016 bylo podáno 1337 žádostí,
- za období od 1. 1. 2017 do 31. 12. 2017 bylo podáno 1395 žádostí,
- za období od 1. 1. 2018 do 31. 12. 2018 bylo podáno 1435 žádostí.[72]

Jak je z poskytnutých informací patrno, trend dožádání a ztotožňování jednotlivých IP adres s konkrétní datovou přípojkou (přístupovému místu do sítě internet) se meziročně zvyšuje. Zároveň však nelze tvrdit, že by k jeho zvyšování docházelo nikterak dramaticky.

Kupříkladu v roce 2016 však bylo v souladu s ustanovením § 88a odst. 1TŘ PČR realizováno celkem 55.211 záznamů o uskutečnění telekomunikačního provozu. Celkový počet zahrnuje výpisy o uskutečnění komunikace skrze mobilní a pevné

[70]Zákon č. 106/1999 Sb., zákon o svobodném přístupu k informacím, ve znění pozdějších předpisů.

[71] Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 25. 8. 2017 pod č. j. PPR-23209-5/ČJ-2017-990140 a dále sdělení ze dne 9.5. 2019 pod č.j. PPR-16663-4/ČJ-2019-990140.

[72] Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 25. 8. 2017 pod č. j. PPR-23209-5/ČJ-2017-990140 a dále sdělení ze dne 9. 5. 2019 pod č.j. PPR-16663-4/ČJ-2019-990140.

telefonní stanice a síť Internet.[73] Z celkového počtu dožádání jsou údaje o sdělení IP adresy tedy přibližně v poměru 2 %.

4.1.4. *Data retention* dle Zákona o Policii

Údaje je ISP povinen dále také sdělit PČR pro účely pátrání po konkrétní pohřešované nebo hledané osobě. Dále je ISP povinen údaje sdělit při zjišťování totožnosti osoby neznámé totožnosti nebo osoby zesnulé a dalších důvodů.[74] V tomto případě však PČR nežádá dle TŘ, ale dle ustanovení § 66 odst. 3, § 68 odst. 2 a dále § 71 písm. a) zákona č. 273/2008 Sb., o Policii ČR (tento zákon ve znění pozdějších předpisů dále jen jako „ZOP“).[75]

Za pozornost stojí skutečnost, že pokud policejní orgán pátrá po hledané osobě, za splnění následujících kumulativních podmínek má nárok na vydání provozních a lokalizačních údajů bez toho, aby byl tento zásah do práv člověka schválen soudem. K vyžádání údajů o hledané osobě může dojít, pokud i) je dán zákonný důvod omezení svobody (tedy např. vydán příkaz k zatčení, nebo osoba uprchla ze zabezpečovací detence), ii) není známo, kde se tato osoba zdržuje, iii) policejní orgán po osobě vyhlásil formální pátrání.

Výše uvedená ustanovení ZOP byla taktéž podrobena přezkumu Ústavního soudu.[76] Tento, mimo jiné, posuzoval, zda poskytuje dostatečnou ochranu před zneužitím tohoto nástroje k získání údajů o osobách. Ve svém nálezu došel k závěru, že zneužití je málo pravděpodobné, neboť vyžádání údajů po ISP vyžaduje formální úkon vyhlášení pátrání po zájmové osobě. K absenci povinnosti OČTŘ sdělit osobě, které se vyžádání údajů týká zaujal názor, že toto není nezbytné, neboť osoba se o využití údajů dozví již tím, že je vypátrána. Záležitost ÚS uzavřel s tím, že se v řízení nepodařilo prokázat žádné systémové zneužívání.

Jako relevantní se může jevit využívání provozních a lokalizačních údajů dle těchto ustanovení ZOP i v netrestních věcech. Jak již bylo uvedeno, jednou z podmínek

[73] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2016*. Policejní prezidium České republiky. [online] publikováno 15. 8. 2017 [cit. dne 8. 5. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

[74] VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, str. 305.

[75] Zákon č. 273/2008 Sb., o Policii ČR ve znění pozdějších předpisů.

[76] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17 bod č. 110 – 117.

je vyhlášení pátrání po konkrétní (kupříkladu pohřešované) osobě. Vyhlášení pátrání není úkon dle TŘ, ale dle interních předpisů policejního orgánu. Vyhlášení pátrání není vázáno na zahájení trestního stíhání (nebo dokonce nemusí být provedeno jako úkon neodkladný a neopakovatelný, před fází zahájení vyšetřování). Vyhlášení pátrání tak může být i důsledkem skutečnosti, která nemusí být spojena s objasňováním TČ.[77]

Je běžné, že dochází k lokalizování osoby, o níž bylo vyhlášeno pátrání na základě provozních a lokalizačních údajů sítě GSM. Bude možné obdobně využít provozní a lokalizační údaje sítě Internet? Dle názoru autora ano. Na úvod připomeňme, že stejně jako v síti GSM není relevantní při pátrání využít obsahu přepravovaných dat. Takový zásah do ústavně zaručeného práva na soukromí přepravovaných zpráv, garantovaných v čl. 13 LZPS ustanovení § 68 odst. 2 ZOP neumožňuje. Ustanovení implikuje pouze zásah do práva na informační sebeurčení, garantovaných v čl. 10 odst. 6 LZPS. ISP navíc stejně jako Operátor (v síti GSM) dle ustanovení § 89 odst. 1 ZEK není oprávněn uchovávat ani analyzovat obsah přepravovaných zpráv, informací či dat.

Pro lokalizování osoby, užívající síť Internet bude nejrelevantnější využití IP adresy.

Policejní orgán dle názoru autora může získat jednotlivé logy IP adres uživatelských účtů, služeb nebo jiných aktivit v síti Internet od poskytovatelů digitálních služeb (přihlášení do e-mailové schránky, sociální sítě atd.). Připomeňme, že dle ustanovení § 2 Vyhlášky o uchovávání je provozovatel e-mailových služeb povinen uchovávat IP adresy, ze kterých bylo do služby přistupováno. Získání těchto údajů je dle názoru autora policejní orgán oprávněn na základě dožádání dle § 8 TŘ.

Takto získané provozní a lokalizační údaje mohou být dotazovány na ISP s žádostí o sdělení identifikace fyzické (poštovní) adresy, na které je umístěn přístupový bod do sítě Internet. Povinnost ISP sdělit provozní a lokalizační údaje plyne z ustanovení § 68 odst. 2 ZOP. Připomeňme, že za provozní a lokalizační údaj se dle Vyhlášky o uchovávání[78] považuje fyzická (poštovní) adresa nemovité věci v které je umístěno telekomunikačního koncového zařízení, které disponuje danou IP adresou. Takto tedy může policejní orgán získat informaci o tom, v jakém místě se osoba, o níž bylo vyhlášeno pátrání pohybuje, či v době posledních 6 měsíců pohybovala.

[77]VANGELI, Benedikt. § 66 [Získávání informací z evidencí]. In: *Zákon o Policii České republiky*. 2. vydání. Praha: Nakladatelství C. H. Beck, 2014, s. 276.

[78] Dle § 2 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, ve znění pozdějších předpisů.

Z výše uvedeného plyne, že k pátrání po osobách mohou být využity i provozní a lokalizační údaje, vzniklé z užívání sítě Internet. Krom netrestních případů (pátrání po nezvěstné osobě) může být tato metoda využita i za účelem pátrání po pachateli TČ, který byl již ustanoven, avšak OČTŘ neví, kde se vyskytuje. Je však nutné nejprve identifikovat účty (např. e-mailové účty, účty na sociálních sítích atd.), které osoba, po níž bylo vyhlášeno pátrání užívá. Mnoho elektronických služeb však nevyžaduje vyplnění či ověření jednoznačných identifikačních údajů. Zjištění těchto „elektronických identit", které osoba, po níž je vyhlášeno pátrání vyhlášeno a do kterých se přihlašuje tedy bude muset být prvním krokem.

Autor vyžádal statistiky, týkající se žádostí o vydání provozních a lokalizačních údajů v režimu ustanovení § 68 odst. 2 ZOP. Ze sdělení PČR v režimu zákona o svobodném přístupu k informacím plyne, že:

- v roce 2018 došlo k celkovému množství dožádání v 16.965 případech,
- v roce 2019 došlo k celkovému množství dožádání v 18.249 případech.

Tyto čísla zohledňují všechny dožádání, ať už v síti GSM nebo v síti Internet. PČR však dožádala v režimu § 68 odst. 2 ZOP i provozní a lokalizační údaje, týkající se výhradně interakce v síti Internet:

- v roce 2018 došlo k dožádání v množství 102 případů,
- v roce 2019 došlo k dožádání v množství 104 případů.

PČR dále sdělila, že všechny dotazy, které byly za účelem pátrání po konkrétní osobě dotázány v souvislosti s její aktivitou v síti Internet se týkaly výhradně IP adres.[79] Z toho lze dovodit správnost výše uvedených závěrů. **PČR tedy k pátrání po osobách využívá i zkoumání jejich aktivit v síti Internet.** Z poskytnutých statistik však zároveň plyne, že se jedná o méně frekventovaný institut.

4.1.5. Identifikace pomocí IP adresy

Lze konstatovat, že využití nástroje záznamu o uskutečnění telekomunikačního provozu je pro odhalování kriminality spáchané v kyberprostoru klíčové. Vzhledem k tomu, že ISP plošně uchovávají provozní a lokalizační údaje po dobu 6 měsíců je nezbytné všechny úkony provádět bez zbytečného odkladu. Jak bylo výše uvedeno, ISP

[79] Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 17. 1. 2020 pod č. j. PPR-1074-4/ČJ-2020-990810.

je po dobu delší uchovávat nesmí, neboť by se dopouštěl přestupku s dostatečně odstrašují sankcí.

Z výše uvedeného je dále nutno mít na paměti, že ISP sdělí pouze údaj o osobě, která uzavřela smlouvu o poskytování telekomunikačních služeb. Sdělení identity osoby, která uzavřela smlouvu nemusí znamenat shodu s osobou pachatele. Pro nejzákladnější rozdělení druhu smluv o poskytování telekomunikačních služeb poslouží rozdělení na poskytování čistě datových služeb (tedy pouze přístup k internetu) tak na telekomunikační služby převážně umožňující volání či zasílání SMS zpráv v GSM síti, navíc se službou poskytování datových služeb (služba mobilního internetu).

V případě první ze služeb, tedy čistě služeb přístupu do Internetu (pevného místa přístupu do sítě Internet), se často jedná o zřízení služby pro větší skupinu uživatelů (pracoviště, domácnost, restaurační zařízení…). Krom využívání služby v okruhu osob, žijící ve společné domácnosti není vyloučeno, že se bude jednat o Wi-Fi připojení, které bude zřízeno v kavárně či jiném veřejném místě. Mnoho domácích Wi-Fi sítí je navíc stále nedostatečně, nebo dokonce zcela nezabezpečeno. K takové nezabezpečené síti se může připojit kdokoliv v okruhu dosahu této sítě, které dosahuje v případě běžného signálu routeru.

Signál routeru je možné nepozorovaně rozšířit technickým zařízením. Může se jednat o směrovou anténu, či zařízení extender,[80] které prodlouží signál a funkčnost sítě až na násobnou vzdálenost. V případě sofistikovaného využití těchto technických zařízení se může koncové zařízení, připojené do Wi-Fi sítě nacházet i stovky metrů daleko od původního routeru. Nachází-li se tedy router v hustě obydlené oblasti, identifikace jednotlivého uživatele může být dosti obtížná.

Jaké konkrétní zařízení je k přístupovému bodu připojeno, je možné identifikovat na základě MAC adresy zařízení.[81] Jak již bylo uvedeno výše, prostor za routerem je nazýván NAT, a spolehlivý údaj o připojených zařízení ve vnitřní síti může být v routeru logován, a na základě MAC adres přiřazen jednotlivým zařízením, které je dále možné komparovat s konkrétní osobou. I údaj MAC adresy však není zcela neměnný, a technicky zdatnější uživatel je schopen ho změnit na libovolnou hodnotu.[82]

[80] Extender je zařízení, umožňující rozšíření dosahu Wi-Fi signálu.

[81] O'SHEA, Kevin. *Cyber Crime Investigation: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Rockland: Syngress publishing, 2007. S. 114.

[82] PÍŠA, Miroslav. Datová bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí. Zlín, 2008. s. 23. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce JAŠEK, Roman.

Může se však jednat i o situaci, kdy jde o přípojku, kterou užívá jediný člověk a připojení do sítě Internet přes tuto přípojku je kvalitně zabezpečeno.

Nelze tedy pouze na základě identické IP adresy protokolu, kterým byla navázána interakce (např. mezi navštívenou webovou stránkou a přistupujícím routerem) činit závěr o tom, že osoba, která uzavřela smlouvu o poskytování telekomunikačních je bez dalšího osobou pachatele.[83]

V případě služby mobilního internetu je již více pravděpodobné, že ztotožnění IP adresy s uživatelem konkrétního přístupového bodu bude totožné. Přístup do sítě Internet je totiž často spjatý s daným zařízením, ve kterém je vložena SIM karta. Půjde tedy převážně o mobilní telefon, či přenosné zařízení, disponující modemem. Zde je sdílení připojení s jiným uživatelem možné pomocí funkce hotspotu. Služba hotspotu je v případě využití v mobilním telefonu značně energeticky náročná a jeho oprávněný uživatel je o jeho aktivaci často srozuměn, neboť zařízení notifikuje informace o připojených zařízeních, a to včetně jejich názvů, a často i typu mobilního zařízení. Připojení konkrétního zařízení k zařízení oprávněného uživatele velmi často vyžaduje heslo.

Je běžné, že soudy vydávají příkazy k provedení domovní prohlídky pouze na základě skutečnosti, že existující skutečnosti nasvědčující tomu, že skutek byl spáchán z IP adresy (přístupového bodu do sítě Internet) která je přiřazena ke konkrétní nemovité věci.[84] Z výše popsaných důvodů se však může jednat o zcela nepřiměřený zásah do práva na soukromí a nedotknutelnost obydlí, garantovaných LZPS, neboť může dojít k nařízení provedení domovní prohlídky u osoby, která si pouze nedostatečně zabezpečila Wi-Fi síť, či někdy v minulosti heslo sdělila třetí osobě. Vzhledem k následnému průběhu domovní prohlídky, kdy při vyšetřování internetové kriminality nezřídka dochází k zajištění veškeré výpočetní techniky (mobilní telefony, tablety, osobní i stolní počítače, či další elektronické zařízení) dochází k mimořádnému zásahu do osobního i pracovního života osob, které žijí ve společné domácnosti osoby, která uzavřela smlouvu o poskytování telekomunikačních služeb nebo domnělého pachatele.

[83] Respektive IP adresy, která byla zalogována a je známa OČTŘ.

[84] Viz například ve věci, posuzované Ústavním soudem dne 10. 7. 2018 pod sp. zn. IV. ÚS 1313/18 nebo ve věci, posuzované Ústavním soudem dne 23. 8. 2016 pod sp. zn. IV. ÚS 3636/15.

4.1.6. Závěrem

Jak plyne z výše uvedeného, sledování informací o tom, komu byla v daný okamžik, či jakému přístupovému bodu (a ideálně i uživateli) v konkrétním čase přidělena jednotlivá IP adresa je dle názoru autora jedna z nejcennějších informací pro účely odhalení pachatele skutku spáchaného v kyberprostoru. Vzhledem k tomu, že vypovídá jen o přístupovém místě do sítě Internet jde však spíše o startovací důkaz, který je vhodné podpořit dalšími skutečnostmi – například využitím dalších institutů, neboť OČTŘ může již být známo, která osoba mohla skutek spáchat. Takové zjištění může poskytnout argumentaci pro splnění podmínek pro naplnění dalších institutů (např. domovní prohlídka, odposlech datového toku atd.). Dle dožádaných údajů se počet využití institut zvyšuje postupným trendem. V současné době je však trendem u sousedních zemí (např. Spolková republika Německo) shromažďování *data retention* z důvodu nevýběrového a plošného uchovávání spíše omezovat. Ústavní soud při posledním posouzení národní úpravy *data retention* s Ústavou, naznačil, že tentokrát o nesouladu s Ústavou nerozhodne. Nad zněním úpravy však pomyslně pozvedl prst s tím, že se jeho názor v blízké době může změnit. Je zároveň zřejmé, že uchovávání provozních a lokalizačních údajů zaslouží právní ochranu. Minimálně charakter IP adresy jako osobního údaje je dle názoru autora nepopiratelný.

Jistě bude zajímavé sledovat případný názor Ústavního soudu na extenzivní výklad § 88a TŘ kdy se *data retention* žádají *pro futuro*. Jeho použití tak, aby nedocházelo nejen k jednorázovému zpětnému vydání údajů až za 6 měsíců, ale i k (nejspíše) postupnému hlášení OČTŘ o konkrétním uživateli může nabídnout nové možnosti odhalování kybernetické kriminality. Autor je však spíše názoru, že tento výklad testem proporcionality neobstojí.

Velmi zajímavým zjištěním je využívání zkoumání aktivity jedince v síti Internet při pátrání po této osobě. Ačkoliv se jedná o méně často využívaný institut, lze předpokládat, že jeho využívání bude častější. Při této metodě je však problematické zjištění uživatelských účtů, do kterých se osoba, po níž je vyhlášeno pátrání loguje.

4.1.7. Návrh *de lege ferenda*

Při úvaze *de lege ferenda* lze dospět k možnosti zkrácení doby uchovávání údajů na dobu 2 měsíců. Zákonodárce byl při stanovení doby 6 měsíců vázán touto dobou jako nejnižší, kterou byl dle tehdejší směrnice Evropského parlamentu a Rady 2002/58/ES

povinen implementovat. Vzhledem k tomu, že došlo ke zrušení směrnice již lze délku této doby přehodnotit.

Je dále na místě zúžení okruhu uchovávaných informací, které vymezuje Vyhláška o uchovávání. Za stěžejní informace považuje autor práce především MAC identifikátor zařízení, informace o uživateli a údaje o místě připojení do sítě Internet (fyzické adrese nemovité věci, ve které je umístěn přístupový bod do sítě Internet). Další úvahou *de lege ferenda* v oblasti *data retention* je stanovení povinnosti uchovávat údaje poskytovatelům OTT služeb, jako jsou (Facebook, Instagram či Twitter). Na ty totiž povinnost tak, jako na ISP nedopadá.[85]

Za vhodné se při úvaze *de lege ferenda* jeví zavést národní databázi, která OČTŘ umožní rychlé ověření, který ISP poskytuje IP adresu uživatelům. Doposud musejí OČTŘ dotázat všechny ISP providery, až následně z jejích odpovědí zjišťují, který ISP uzavřel smlouvu na poskytování služeb k přístupovému bodu do sítě Internet. Takový úkon, ač lze předpokládat že je do jisté míry automatizován zbytečně navyšuje časovou náročnost prováděného úkonu.

4.2. Odposlech a záznam datového provozu § 88 TŘ

Po první identifikaci přístupového bodu do sítě Internet, ze které byl s nejvyšší pravděpodobností proveden TČ, jakož i po jiných indiciích, nasvědčujících o tom, že skutek spáchala konkrétní osoba je za splnění níže uvedených podmínek možné využít nástroje odposlechu a záznamu telekomunikačního provozu.[86] Odposlech slouží k objasnění skutečností, které jsou důvodné z již existujících podezření či důkazů. Odposlech a záznam telekomunikačního provozu lze považovat za jeden z nejefektivnějších nástrojů, který lze k odhalování trestné činnosti použít.

Jedná se o zákonem předvídaný a aprobovaný zásah do ústavně zaručených práv a svobod. Odposlech a záznam telekomunikačního provozu je zásah do ústavně zaručeného soukromí zpráv, předávaným telefonem nebo jiným podobným zařízením, zaručených zejména čl. 13 LZPS. Dále se jedná o potenciální kolizi s čl. 10, odst. 3

[85] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17

[86] Dle usnesení Nejvyššího soudu ze dne 15. 11. 2016, sp. zn. 4 Pzo 14/2016: „*Není totiž přípustné, aby teprve na základě a prostřednictvím povoleného odposlechu byly získávány informace o tom, zda se odposlouchávaná osoba dopustila protiprávního jednání. Takový poznatek musí vydání příkazu k odposlechu předcházet, přičemž je třeba, aby byl validní, což znamená, že musí pocházet ze spolehlivého zdroje a musí být dostatečně přesvědčivý.*“

LZPS, které zaručují ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužitím osobních údajů. Jedná se tedy o prolomení povinnosti zabezpečení ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikací, kterou je jinak ISP dle ustanovení § 88 ZEK povinen zajistit.

OČTŘ jsou legálně i technicky vybaveny k provádění komplexního odposlechu datového toku konkrétní přípojky do sítě Internet. Zákonný rámec poskytuje především ustanovení § 88 TŘ. Oproti záznamu o uskutečněném telekomunikačního provozu dle § 88aTŘ jsou ze zákona k plnohodnotnému odposlechu stanoveny výrazně přísnější podmínky, za kterých může být proveden. Odposlech může být nařízen, dojde-li ke splnění následujících podmínek:

1 řízení je vedeno pro:
   a) zločin s horní hranicí sazby odnětí svobody nejméně 8 roky, nebo
   b) pro některý z TČ dle § 226, § 248 odst. 1, § 256, § 257, § 258, § 329 TZ,
   c) pro úmyslný TČ, k jehož vydání zavazuje vyhlášená mezinárodní smlouva,
2 sledovaného účelu nelze dosáhnout jiným způsobem, nebo by jiný postup dosažení účelu ztěžoval,
3 provedení musí nařídit předseda senátu nebo samosoudce.

Po kumulativním splnění těchto podmínek je dále nezbytné posoudit, zda lze při použití tohoto prostředku důvodně předpokládat, že budou získány významné skutečnosti k objasnění trestné činnosti, a sledovaného účelu nelze dosáhnout jinak, či by jiné dosažení bylo podstatně ztížené.

Nařídit odposlech a záznam telekomunikačního provozu je oprávněn předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Příkaz k odposlechu musí být vydán písemně a musí být odůvodněn, a to pro to, jaký skutek se stal.

V příkazu k odposlechu a záznamu tel. provozu musí být stanovena uživatelská adresa či zařízení, je-li toto známo a dále osoba uživatele, je-li známa. Musí být uveden konkrétní trestný čin a konkrétní skutkové okolnosti které vydání příkazu odůvodňují. Dále je nutné uvést účel odposlechu, jakož i důvody, proč nelze sledovaného účelu dosáhnout jinak nebo proč by bylo jinak jeho dosažení podstatně ztížené.[87] Dále je nutné uvést, na jakou dobu je odposlech nařízen. Nařídit jej lze maximálně na dobu 4 měsíců. Jedná se o rozhodnutí *sui generis.*

Pořizování odposlechu a záznamu tel. provozu před zahájením trestního stíhání je možné pouze pokud se jedná o neodkladný úkon dle § 158 odst. 3 písm. i) TŘ

[87] Dle rozhodnutí Nejvyššího soudu ze dne 7. 6. 2017 sp. zn. 6 Tz 3/2017 bod č. 72

v návaznosti na § 160 odst. 4 TŘ.[88] Má-li být úkon prováděn před zahájením trestního stíhání, je nutné uvést důvody, které tomu nasvědčují včetně odůvodnění do návrhu na vydání příkazu, jakož i do jeho odůvodnění.[89]

[88] LOVÍŠKOVÁ, Zuzana. *Odposlech a záznam telekomunikačního provozu*. Praha, 2013, s. 10. Univerzita Karlova v Praze, Právnická fakulta. Vedoucí práce Jiří ŘÍHA.

[89] Dle rozhodnutí Nejvyššího soudu ze dne 7. 6. 2017 sp. zn. 6 Tz 3/2017 Absence odůvodnění, proč je nutné úkon vnímat za neodkladný a neopakovatelný v situaci, kdy je vydávám před zahájením fáze vyšetřování však nutně nemusí znamenat nepoužitelnost důkazů, získaných na základě takto vydaného příkazu. Je nutné krom striktně formálního pohledu zohlednit i materiální skutečnosti daného případu.

4.2.1. Provádění odposlechu datového toku

Odposlech a záznam telekomunikačního provozu provádí pro potřeby všech orgánů činných v trestním řízení PČR, a to konkrétně Útvar zvláštních činností služby kriminální policie a vyšetřování.[90]

Odposlech datového provozu, je stejně jako odposlech telefonické komunikace jeden z nejzásadnějších zásahů do práva na soukromí. Policejní orgán je dle ustanovení § 88 odst. 3 TŘ povinen průběžně vyhodnocovat, zda nadále trvají důvody, které vedly k vydání příkazu k odposlechu. Pokud již důvod pominul, je policejní orgán povinen odposlech ihned ukončit.

Orgán, provádějící odposlech je povinen vyhotovit písemný záznam o uskutečnění provedení odposlechu. Záznam kromě obecných náležitostí obsahuje údaj o místě, čase, způsobu a obsahu prováděného odposlechu, jakož i uvedení identifikace provádějícího orgánu.[91] Judikatura Vrchního soudu[92] k úkonu záznamu o uskutečnění provedení odposlechu (sic k odposlechu telefonního hovoru) zastává postoj, že nedostatek údajů v protokolu, zejména o místě, času, způsobu provedení a osobě, která záznam pořídila lze zpětně odstranit, stejně jako formální nedostatky protokolu v případě jakéhokoliv jiného úkonu v trestním řízení.[93] S tímto lze částečně souhlasit. Velké množství zajištěné komunikace může vytvářet situaci, kdy lpění na formálních detailech protokolu (jako např. na informaci, kde byl záznam vyhotoven) může způsobit při drobné lidské chybě nepoužitelnost záznamu. Druhým pohledem je však možná rezignace příslušného útvaru na detailnější vyplňování záznamu.

[90] VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, str. 315.

[91] LOVÍŠKOVÁ, Zuzana. *Odposlech a záznam telekomunikačního provozu*. Praha, 2013, s. 17. Univerzita Karlova v Praze, Právnická fakulta. Vedoucí práce Jiří ŘÍHA.

[92] Usnesení Vrchního soudu v Praze ze dne 18. 1. 2001 sp. zn. 4 To 3/01.

[93] MUSIL, Jan. *Trestní právo procesní.* 4. přepracované vydání. Praha: C.H.Beck, 2013. s. 328.

Ačkoliv je pořizování záznamu odposlechu mezi sledovanou osobou a advokátem zpravidla nepřípustné, autor této práce se setkal se situací, kdy došlo k záznamu odposlechu telefonické konverzace[94] mezi pachatelem TČ jako právnické osoby a obhájcem. Policejní orgán a státní zástupce dovodil, že právnická osoba dle zákona o trestní odpovědnosti právnických osob[95] a řízení proti nim ve znění pozdějších předpisů, nepožívá práva zákazu odposlechu mezi sledovanou osobou a advokátem, neboť se nejedná o fyzickou osobu. Autor je však názoru, že se v tomto případě jednalo spíše o exces.

Odposlech obsah elektronické komunikace (včetně např. e-mailů, či jiného obsahu přepravovaných zpráv a informací) v reálném čase je možné provádět výhradně při provádění odposlechu dle § 88 odst. 1 TŘ, postup zachycení obsahu zpráv podle ustanovení § 88a odst. 1 TŘ není možný.[96]

Ustanovení § 88 odst. 7 TŘ stanovuje, že zničení záznamů o provedeném odposlechu telekomunikačního provozu, kterým nebyly zjištěny skutečnosti významné pro trestní řízení je možné za splnění kumulativních podmínek 1) po souhlasu soudu (v přípravném řízení postačuje souhlas státního zástupce), 2) po uplynutí 3 let od pravomocného skončení věci. Podmínku uplynutí 3 let zavedl zákonodárce s ohledem na možnost iniciace mimořádných opravných prostředků (dovolání § 256a TŘ, stížnost pro porušení zákona § 266 TŘ, návrh na povolení obnovy řízení § 277 TŘ).[97] Zničení je nutné provést ideálně kombinací přepisem zapsaných dat a následné fyzické zničení nosičů (přehrání CD/DVD či flash disku v množství dat, rovnající se celé kapacitě média) a jejich následné fyzické zničení – rozdrcení, znehodnocení za pomoci vysoké teploty atd. O znehodnocení záznamu je nutné vyhotovit protokol. V tomto je nutné uvést i způsob znehodnocení nosiče. Následně je třeba zaslat protokol státnímu zástupci, který rozhodl o skončení věci. Pokud se nejedná o přípravné řízení, ale o fázi řízení před soudem je třeba protokol poskytnout soudci k založení do spisu.[98]

---

[94] Ačkoliv šlo o záznam telefonického rozhovoru, institut je dle názoru autora aplikovatelný i na odposlech datového provozu.

[95] Dle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů.

[96] ZEMAN, Pavel. *Stanovisko ke sjednocení výkladů zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.* Nejvyšší státní zastupitelství. Brno, 2015.

[97] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. *§ 88 [TŘ]. Trestní řád I, II, III*. 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1192.

[98] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. *§ 88 [TŘ]. Trestní řád I, II, III. 7*. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1192.

4.2.2. Rozhraní pro odposlech a záznam zpráv

Odposlech datového provozu je možné provádět zřízením speciálního zařízení, které je ISP po obdržení písemné žádosti povinen umožnit začlenit do své infrastruktury.

Tato povinnost byla širokou veřejností i samotnými ISP přijata s velkou nelibostí. Právní základ pro umožnění odposlechu přepravovaných dat upravuje krom TŘ i ustanovení § 97 ZEK. Dle tohoto ustanovení jsou právnické nebo fyzické osoby, zajišťující veřejnou komunikační síť nebo poskytující službu elektronických komunikací povinni umožnit do své infrastruktury připojení zařízení, umožňující odposlech a záznam přepravovaných zpráv. Subjekty, které jsou na své náklady oprávněny zařízení umístit, jsou Policie ČR, Bezpečnostní informační služba a Vojenské zpravodajství.

Tyto výše uvedené orgány dle ustanovení § 97 odst. 2 ZEK prokazují své oprávnění k odposlechu a záznamu zpráv předáním písemné žádosti, která obsahuje číslo jednací soudu a které je podepsáno osobou odpovědnou u výše uvedeného orgánu za vykonání odposlechu a záznamu zpráv. Tato osoba musí mít náležité bezpečností osvědčení, a to alespoň pro práci s informacemi ve stupni „vyhrazené“.

Nevyhovění žádosti o umožnění instalace zařízení je přestupkem, a dle ustanovení § 118 odst. 14 písm. b) ZEK je sankcionováno možným uložením pokuty až do výše 20.000.000 Kč.

4.2.3. Statistika odposlechů datového provozu

Dle žádosti v režimu zákona č. 106/1999 Sb., o svobodném přístupu k informacím byla autoru této práce Policií České republiky sdělena statistika, v kolika případech docházelo k odposlechu datového provozu z přípojky (přístupového bodu) do sítě Internet v režimu ustanovení § 88 TŘ. Z poskytnutých informací plyne, že mezi 1.1.2013 až 1.1.2017 policejní orgán prováděl odposlech datového provozu (sítě Internet) v režimu ustanovení § 88 TŘ v celkem 136 případech.[99] Jedná se tedy o institut, kterého je využíváno spíše zřídka. Počet realizovaných případů „klasických" telefonických odposlechů je však neporovnatelně vyšší. Za zmínku dále stojí, že statistiky PČR se vyznačují trendem snižování počtu realizovaných odposlechů (jedná se o statistiku využití § 88 TŘ, v těchto číslech jsou zohledněny jak telefonní odposlechy, tak odposlechy datového toku). V roce 2016 byl institut § 88 TŘ využit v celkem 1064 případech,[100] v roce 2017 je zaznamenáno 934 případů,[101] v roce 2018 je zaznamenáno 895 případů.[102] Snižování počtu realizovaných odposlechů lze vnímat pozitivně. Ve veřejném mínění je otázka odposlechu telekomunikace kontroverzní záležitostí. Značná část veřejnosti se může domnívat, že dochází k nadužíváním tohoto invazivního nástroje. Využívání nástroje pouze v těch případech, kdy je jeho použití nezbytné šetří i lidské zdroje. Právě odposlech datového toku lze považovat za velmi náročný úkon jak technicky, tak nárokem na vyškolené odborníky k jeho provedení.

---

[99] Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 22. 3. 2018 pod č. j. PPR-9726-3/ČJ-2018-990140.

[100] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2016*. Policejní prezidium České republiky. [online] publikováno 15. 8. 2017 [cit. dne 8. 10. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

[101] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2017*. Policejní prezidium České republiky. [online] publikováno 5. 10. 2018 [cit. dne 11. 10. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

[102] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2018*. Policejní prezidium České republiky. [online] publikováno 22. 8. 2019 [cit. dne 1. 09. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

4.2.4. Šifrování komunikace v reálném čase subjektem ISP

Nešifrovaná komunikace lze přirovnat k odeslanému korespondenčnímu lístku, s jehož obsahem se určitý okruh lidí může seznámit. Zašifrovaná komunikace lze přirovnat k zaslání informací v neprůhledné obálce. Šifrování, nebo jinou, obdobnou kompresi vedoucí k nečitelnosti průtoku dat může provádět i právnická nebo fyzická osoba, poskytující službu připojení do sítě Internet. Pokud však takto učiní, je dle ustanovení § 97 odst. 7 ZEK povinna zajistit, aby požadované informace za podmínek daných ustanovením § 97 odst. 1 ZEK a následující byly policejnímu orgánu předány v čitelné a předepsané formě.[103] Pokud se tedy ISP rozhodne při poskytování služby datového připojení přenášená data šifrovat, např. z důvodu zajištění ochrany přenášených dat před třetí osobou, je povinen zároveň umožnit OČTŘ šifrovaná data poskytnout v nešifrované podobě. Takovéto zašifrování dat by tedy pro objasňování trestné činnosti nemělo činit nepřekonatelnou překážku.

4.2.5. Šifrování datového toku pachatelem

Další možným rozsahem šifrování je ale také kryptování informačního toku mezi koncovým zařízením a sítí Internet aktivitou pachatele. Šifrováním aplikační vrstvy TPC/IP protokolu dojde k znemožnění odposlechu telekomunikačního provozu dle ustanovení § 88 TŘ. Dojde tedy k nemožnosti využít technických zařízení, připojovaných do sítě ISP providerů. K samotnému zachycení paketů technickým zařízením dojde, zjištěná data však pro OČTŘ budou bez dalšího nečitelná. **Vzhledem k tomu, že data šifruje pachatel, nemá ISP povinnost (resp. technicky nemá ani možnost) data předat v čitelné formě tak, jako když komunikaci šifruje sám.[104]**

Pachatel TČ může zašifrovat a dostatečně chránit svůj datový provoz například za využití nástroje VPN nebo Tor, které jsou schopny při správném nastavení všechnu komunikaci uživatelského zařízení do sítě Internet směřovat přes kryptovaný tunel.

[103] Předávávání údajů se řídí ustanovením § 3 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

[104] STUPKA, Václav. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015., s. 189.

4.2.6. Šifrování komunikace v reálném čase třetí osobou

Povinnost zpřístupnit šifrovaná data dopadá pouze na ISP, tedy na právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Nejčastěji půjde o Operátory, či subjekty ISP. Jiný subjekt, např. provozovatel aplikace (příkladem těchto provozovatelů jsou např. služby Viber či WhatsApp), která umožňuje provozování šifrované komunikace je v teoretické rovině povinen spolupráce s OČTŘ k objasnění trestné činnosti z důvodu uvedených v § 8 odst. 1 TŘ. Dle tohoto jsou právnické a fyzické osoby povinny, nestanoví-li zvláštní předpis jinak, bez zbytečného odkladu i bez úplaty vyhovovat OČTŘ při plnění jejích úkolů.[105]

Je otázkou, zda by na daný případ nedopadalo speciální ustanovení. Jako relevantní se jeví § 88 TŘ. OČTŘ by třetí osobě, kterou může být např. provozovatel aplikace Whatsapp nebo Viber přikázat umožnění provádění odposlechu přepravovaných zpráv. Za problematické však autor shledává, že dle jeho názoru absentuje relevantní úprava, stanovující podmínky umožnění odposlechu. Operátoři a ISP mají povinnost dle § 97 ZEK na žádost nechat do své infrastruktury na žádost instalací zařízení, umožňující odposlech konkrétních uživatelů sítě. Oprávnění k jednotlivým odposlechům OČTŘ přirozeně následně prokazují vydaným příkazem k odposlechu. Ustanovení § 97 však tuto povinnost ukládá *pouze právnické nebo fyzické osobě, zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací.* Je možné osobu, provozující uživatelskou aplikaci (např. i umožňující šifrování datového toku metodou end-to-end[106]) považovat za adresáta této povinnosti? K tomu je nutné posoudit, zda tato osoba 1) zajišťuje veřejnou komunikační síť nebo 2) poskytuje veřejně dostupnou službu elektronických komunikací.

[105] ŠÁMAL, Pavel. *§ 8 [Dožádání a ochrana utajovaných skutečností a údajů, na něž se vztahuje mlčenlivost]*. Trestní řád. 6. vydání. Praha: Nakladatelství C. H. Beck, 2008, s. 79.

[106] End-to-end nebo také koncové šifrování je označení pro kryptovací metodu, kdy přenos dat je po odeslání ze zařízení zašifrován. Klíčem k rozšifrování disponuje pouze zařízení příjemce a odesílající zařízení.

První z možností (1) tedy *zajišťování veřejné komunikační sítě* v ustanovení § 2 písm. h) ve spojení s písm. f) ZEK definuje jako zřízení sítě přenosových systému, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace, její provozování, dohled nad ní nebo její zpřístupnění. Z takto dovozené definice[107] je zřejmé, že se jedná o provozování sítě Internet, resp. o službu umožnění připojení k síti Internet.

Druhou z možností, tedy (2) *poskytování veřejně dostupné službu elektronických komunikací* v ustanovení § 2 písm. ZEK lze vnímat identicky jako (1) první možnost, pouze s rozdílem, že nyní bude zpravidla úplatná.

ZEK bohužel nenabízí další výkladová pravidla. Výše uvedené definice není jednoduché spolehlivě vyložit s ohledem na okruh adresátů, na které dopadají a kterým ukládají povinnost. Autor se kloní k názoru, že tyto definice ani extenzivním výkladem nelze ztotožnit s činností poskytováním služby komunikační platformy, byť využívající síť Internet k přenosu dat mezi koncovými uživateli této platformy. Uzavírá tedy, že povinnost dle § 97 ZEK, včlenit na písemnou žádost do své infrastruktury zařízení, umožňující odposlech provozu sítě na tyto subjekty spíše nedopadá.

Výše uvedená otázka je poměrně významná. Pokud by povinnosti dle § 97 ZEK dopadaly na provozovatele komunikační aplikace, dle odst. 6 stejného ustanovení by mu dále vznikla povinnost poskytovat data (za splnění podmínek § 88 TŘ) v dešifrované podobě. Stejně tak by dle byl provozovatel povinen uchovávat, a za podmínek § 88a TŘ vydávat provozní a lokalizační údaje, spojené s jednotlivou uživatelskou aktivitou v provozované aplikaci.

[107] Zejména z ustanovení § 2, písm. h) a f) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů

I pokud by však povinnosti dle ustanovení § 97 ZEK na provozovatele dopadaly, zpřístupňování šifry ze strany provozovatele této komunikační platformy nemusí být možné, pokud je komunikace zabezpečena např. metodou „End-to-end“ šifrování. OČTŘ se informací nemusí být schopny ani právně, ale ani technicky domoci. Poznamenejme, že pokud by se autor nesprávně domníval, že na tyto subjekty povinnosti dle § 97 nedopadají (tedy zejména umožnit instalaci zařízení, umožnit dešifraci či dekompresi přepravovaných zpráv nebo logování a vydávání provozních a lokalizačních údajů), jedná se o přestupek, za který hrozí sankce až do výše 20.000.000 Kč. Dále hrozí možnost ukládání pořádkových pokut dle § 66 TŘ.

4.2.7. Přezkum zákonnosti příkazu k odposlechu a záznamu o uskutečnění telekomunikačního provozu

„Důležitou zárukou kontroly ústavnosti odposlechů je povinnost orgánů činných v trestním řízení informovat dotčenou osobu po pravomocném skončení věci o provedeném odposlechu a záznamu telekomunikačního provozu (§ 88 odst. 8 trestního řádu). Informační povinnost orgánů činných v trestním řízení má význam nejen sama o sobě, ale je zároveň formálním předpokladem toho, aby se dotčená osoba mohla domáhat přezkumu zákonnosti (a potažmo také ústavnosti) odposlechu Nejvyšším soudem v řízení podle § 314l trestního řádu.“[108]

Notifikace osoby, do jejíchž práv bylo zasaženo příkazem k odposlechu nebo záznamu telekomunikačního provozu plyne i z ustálené judikatury ESLP. Tato judikatura navazuje na ustanovení čl. 8 EÚLP, dle kterého je nezbytné osobu, do jejíž práv bylo zasaženo odposlechem či vydáním záznamu zpětně uvědomit.[109] Tato osoba musí mít k dispozici možnost využít účinného opravného prostředku, jehož využitím se může domáhat vyslovení nezákonnosti nebo bezdůvodnosti odposlechu nebo záznamu telekomunikačním provozu.

[108] Nález Ústavního soudu ze dne 26. 4. 2016, sp. zn. III. ÚS 3457/14.

[109] GRÜNWALDOVÁ, Vladimíra. K odposlechům mobilní telefonické komunikace. *Bulletin advokacie*. 2019, č. 12. Str. 60.

Aktivně legitimovaným podat podnět k přezkumu jsou v případě odposlechu datového provozu osoby uvedené v ustanovení § 88 odst. 8 TŘ. V případě přezkumu příkazu k vydání záznamu o uskutečněním telekomunikačního provozu jsou aktivně legitimovány osoby uvedené v ustanovení § 88a odst. 2 TŘ. Předpokladem pro podání návrhu na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu podle § 314l TŘ k Nejvyššímu soudu je podle § 88 odst. 8 TŘ jednak pravomocné skončení trestní věci, v níž byl vydán takový příkaz, dále skutečnost, že předseda senátu soudu prvního stupně, popřípadě státní zástupce, následně informoval o nařízeném odposlechu a záznamu telekomunikačního provozu osobu oprávněnou k podání tohoto návrhu, která byla uživatelem odposlouchávaného zařízení (§ 88 odst. 2 TŘ).[110] OČTŘ však nejsou povinny vždy a za každé situace odposlouchávanou osobu uvědomit, zákon taxativně vyjmenovává případy, kdy tuto povinnost nemají.

Nejvyšší soud provede přezkum v senátu, složeném z předsedy a dvou soudců z povolání.[111] Shledá-li, že příkaz k odposlechu a záznamu telekomunikačnímu provozu nebo příkaz k zajištění údajů o telekomunikačním provozu byl vydán nebo jeho provedení bylo provedeno v rozporu se zákonem, vysloví usnesením porušení zákona. Proti tomuto usnesení není přípustný opravný prostředek. V případě, že shledá, že výše uvedené úkony byly provedeny v souladu s ustanovením § 88 odst. 1 nebo 88a odst. 1 TŘ vysloví usnesením, že zákon porušen nebyl. Proti usnesení není přípustný opravný prostředek.

[110] ŠÁMAL, Pavel. *§ 314l [Věcná příslušnost Nejvyššího soudu]*. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 3621.
[111] ŠÁMAL, Pavel. § 314l [Věcná příslušnost Nejvyššího soudu]. *Trestní řád I, II, III*. 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 3621.

Nejvyšší soud přezkoumává zákonnost vydání a provedení příkazu. Soud v případě usnesení o porušení zákona (§ 314m odst. 1 TŘ) není oprávněn přezkoumávat dopad takto nezákonně provedeného důkazu do celkového skutkového hodnocení případu, a tedy není oprávněn zrušit rozhodnutí o vinně či nevinně pachatele. **Usnesení soudu má toliko pouze deklaratorní charakter, neboť nemá přímý vliv na meritorní rozhodnutí o vinně pachatele.[112] Nemá dále vliv na právní moc meritorního rozhodnutí ve věci.**

Bez dalšího může usnesení o nezákonně prováděném úkonu dle § 88 a § 88a TŘ (a tedy o porušení zákona) zakládat nemajetkovou újmu navrhovatele.[113] Za splnění dalších podmínek může být úspěšným impulsem k zahájení řízení o mimořádném opravném prostředku (stížnosti pro porušení zákona dle § 266 TŘ a obnovou řízení dle § 278 TŘ).[114]

Dodejme ještě, že ačkoliv se dle dostupných informací počty realizovaných odposlechů (jak telefonních, tak datových) pohybují ve stovkách případů ročně, konkrétně:

V roce 2017 v 934 případech, v roce 2018 v 895 případech.[115] **PČR však odposlouchávané osoby o provedení úkonu dle § 88 odst. 8 TŘ informovala v roce 2017 pouze 71 případech[116] a v roce 2018 pouze v 55 případech.[117]** Je otázkou, zda u zbývajících stovek případů byly naplněny podmínky, za kterých k notifikaci podezřelé osoby dojít nemusí, či zda se ze strany policejního orgánu jedná o liknavý přístup při plnění své zákonné povinnosti.

---

[112] MUSIL, Jan. *Trestní právo procesní.* 4. přepracované vydání. Praha: C.H.Beck, 2013. Str. 888.

[113] JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie.* [online] 2018, č. 9. [cit. 7. 9. 2019]. Dostupné z: https://journals.muni.cz/revue/about/submissions?navItem=0

[114] MUSIL, Jan. *Trestní právo procesní.* 4. přepracované vydání. Praha: C.H.Beck, 2013. Str. 888.

[115] Viz výše.

[116] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2017*. Policejní prezidium České republiky. [online] publikováno 5. 10. 2018 [cit. dne 11. 10. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

[117] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2018*. Policejní prezidium České republiky. [online] publikováno 22. 8. 2019 [cit. dne 1. 09. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

4.2.8. Závěrem k využití odposlechu datového toku

Z výše uvedeného plyne, že OČTŘ jsou schopny realizovat odposlech datového toku za stejných podmínek, jako odposlech telefonního hovoru. Četnost využívání tohoto nástroje je spíše výjimečná (viz přiložená statistika). Je otázkou, proč je mezi statistikou „klasických" odposlechů v síti GSM a odposlechů datové provozu takový nepoměrný rozdíl. Lze se domnívat, že odposlech datového toku je tak logisticky, technicky a personálně náročný proces, že na jeho využívání dochází jen zřídka. Kladně lze ovšem hodnotit, že zákonná úprava takový nástroj poskytuje, a tento nástroj je způsobilý k získávání informací významných pro trestní řízení. ISP jsou povinni pro OČTŘ zpřístupňovat data v čitelné podobě i v případě, kdy umožňují transfer dat v zašifrované podobě. Velkou výzvou je však šifrování komunikace pomocí softwarového nebo hardwarového řešení end-to-end nebo při uživatelském užívání VPN šifrovaných tunelů dat. V takovém případě využití odposlechu datového toku nepřinese nic jiného, než zajištění šifrovaných dat, které ISP není povinen zpřístupnit a to z důvodu, že jejich komprese či šifrování není v jeho dispozici. OČTŘ se mohou pokusit o dešifrování zajištěných dat. Jak však plyne z níže uvedené skutečnosti, pokusy o dešifrování zabezpečených dat nejsou často úspěšné. Kolem povinností, ukládaných § 97 ZEK mohou vznikat nejasnosti, na které subjekty dopadají.

Jak je však rozvedeno dále v této práci, i komunikace prováděná výhradně v šifrované podobě může OČTŘ nabídnout informace k objasnění konkrétního skutku. Tyto informace mohou nabídnout jiné instituty, jako např. § 158d odst. 3 TŘ, využitý jako softwarový odposlech (viz níže), nebo analýza zajištěných dat (po fyzickém odnětí, např. při domovní prohlídce) forenzním softwarem. Analýza zajištěných dat nenabídne živá data (tedy informace o obsahu komunikace v reálném čase), ale může prozradit obsah uložených zpráv či jiných souborů, přenášených datových provozem (o tomto taktéž níže).

4.2.9. Návrh *de lege ferenda*

Podmínkou pro podání návrhu na přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu je (i) pravomocné skončení věci, ve které byl příkaz vydán a (ii) sdělení předsedy senátu soudu prvního stupně nebo státního zástupce o tom, že byla osoba podrobena úkonu odposlechu. Byl-li přesto takový návrh učiněn, Nejvyšší soud ho podle § 265i odst. 1 písm. a) TŘ per analogiam odmítne jako nepřípustný.[118] V případě, že není případný stěžovatel o úkonu následně notifikován, postrádá možnost iniciace přezkumu. O faktickém provedení úkonu se může dozvědět po seznámení se spisovým materiálem, nebo v následující fázi trestního řízení (tedy ještě před tím, než má předseda senátu či státní zástupce povinnost notifikovat dle § 88 odst. 8 TŘ). V případě, kdy odposlouchávaná osoba není notifikována dochází ke kolizi čl. 8 EÚLP, dle které musí mít odposlouchávaná osoba k dispozici účinný opravný prostředek, jímž může namítat nezákonnost nebo bezdůvodnost odposlechu. Druhou z podmínek (ii) (nutná notifikace odposlouchávané osoby) je tedy vhodné modifikovat (jakkoliv přímo z litery zákona neplyne).

Druhou z úvah *de lege ferenda* nelze pominout stav, kdy usnesení soudu o tom, že příkazem k odposlechu došlo k porušení zákona má pouze deklaratorní charakter bez přímého vlivu na právní moc meritorního rozhodnutí. V případě významného porušení zákona by měl senát v případě zjištění zásadního porušení disponovat možností odložit vykonatelnost meritorního rozhodnutí.

Dále se nelze než plně ztotožnit s názorem prof. Jelínka: *„aby oprávněná osoba, jejíž práva byla nezákonným odposlechem a záznamem o telekomunikačním provozu porušena, mohla v případě takového výroku Nejvyššího soudu podat kvalifikovaný podnět ministru spravedlnosti. Ten by byl za takové situace povinen podat stížnost pro porušení zákona, na základě které, by předchozí pravomocné rozhodnutí ve věci samé mohlo být Nejvyšším soudem zrušeno.“*[119]

[118] Rozhodnutí Nejvyššího soudu ze dne 13. 12. 2016 sp. zn. 4 Pzo 16/2016.

[119] JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie.* [online] 2018, č. 9. [cit. 7. 9. 2019]. Dostupné z: https://journals.muni.cz/revue/about/submissions?navItem=0

Je vhodné zavést povinnost policejního orgánu k pečlivému vyplňování záznamu o uskutečnění odposlechu datového toku. Zatímco telefonní hovory mohou být v případě nejasností jednoduše v soudním řízení během provádění dokazování přehrány, provést jednoduché ověření toho, co policejní orgán během provádění odposlechu skutečně zachytil, u zjištění obsahu toku dat sítě Internet již toto tak jednoduché není. Rezignace na formální náležitosti záznamu o uskutečnění úkonu dle § 88 je situaci rozdílnou, a ze zákona by měla plynout nepoužitelnost takového záznamu, se všemi důsledky absence takového záznamu.

4.3. Sledování za využití technických prostředků § 158d TŘ

Zvláštní postavení mezi instituty, relevantními k vyšetřování kybernetické kriminality má sledování věci dle § 158d TŘ. Ustanovení má blízko k institutu odposlechu dle § 88 TŘ a zajištění věci dle § 78, § 79, § 82 TŘ.

Institut sledování věci umožňuje následující:

1) **prosté sledování** (§ 158d odst. 1 TŘ);
2) **sledování, při kterém jsou pořizovány zvukové, obrazové nebo jiné záznamy** (§ 158d odst. 2 TŘ);
3) **sledování, při kterém je zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků** (§ 158d odst. 3 TŘ).[120]

Během objasňování TČ spáchaného za pomoci výpočetní techniky přichází v úvahu využití ustanovení o sledování osob a věcí dle § 158 odst. 3 TŘ, který upravuje zjišťování obsahu jiných písemností a záznamů, uchovávaných v soukromí za pomoci technických prostředků.

Definici „sledování“ TŘ neobsahuje. Toto neurčité ustanovení je typickou ukázkou situace, kdy zákonodárce není schopen reflektovat potřeby OČTŘ a praxe vyžaduje tento nedostatek překlenout. Využití nástroje (§ 158d odst. 3 TŘ) je na místě především v případě:

1) při získávání digitálních dat utajeným operativně pátracím technickým prostředkem;

[120] Gřivna, Tomáš. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Praha: Leges, 2018. s 314 a násl.

2) kdy je nezbytné zajistit volně nepřístupná elektronická data ze vzdálených úložišť nebo služeb, která nejsou uložena v již fyzicky zajištěném zařízení a která nejsou provozními a lokalizačními údaji, nebo je nelze analyzovat v reálném čase za využití institutu odposlechu a záznamu o uskutečnění telekomunikačního provozu.[121]

Podmínky pro vydání povolení jsou pro obě kategorie identické. Dle odstavce § 158d odst. 4 TŘ lze povolení k takovémuto úkonu vydat pouze na základě předchozí písemné žádosti. Žádost musí být podrobně odůvodněna. V odůvodnění musí být uvedeno, pro podezření, z jaké konkrétní trestné činnost se úkon činí a jsou-li známy, též údaje o osobách a věcech které mají být sledovány. Dále musí být obligatorně uvedena doba, po kterou bude sledování prováděno.[122]

V případě, že prováděním úkonu dochází k zásahu do nedotknutelnosti obydlí, uchovávání listin v soukromí nebo zjišťování jiných písemností, uchovávání v soukromí o přípustnosti žádosti rozhoduje soudce.[123] Ačkoliv to zákon přímo nevyžaduje, v praxi zpravidla povolení soudce vydává na návrh státního zástupce.[124] Pokud nedojde k naplnění předepsaných podmínek, může dojít k využití institutu pouze za podmínky souhlasu osoby, do jejíž práv a svobod je zasahováno. Takový vydaný souhlas lze později i odvolat.

V povolení ke sledování musí být stanovena doba, po kterou může být sledování prováděno. Povolená doba sledování nesmí být vyšší než 6 měsíců.[125]

Úmluva o počítačové kriminalitě v článku 19, odst. 2 na členské státy vznáší požadavek následující požadavek. V případě, že (1) zajišťují počítačový systém, data na něm uložená nebo k médiu pro ukládání počítačových dat a je zřejmé, že hledaná data jsou uložena na (2) jiném počítačovém systému, nacházející na území stejného státu, mají mít OČTŘ prohlídku či zajišťování z (1) původního systému rozšířit i na (2) další systém, na kterém se nacházení zájmová data.[126]

---

[121] PŮRY, František. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 58 - 61.

[122] Rozhodnutí Nejvyššího soudu ze dne 7. 6. 2017 sp. zn. 6 Tz 3/2017 bod č. 74

[123] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 158d [Sledování osob a věcí]. *Trestní řád I, II, III.* 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2001. Bod č. 13

[124] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 158d [Sledování osob a věcí]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2001.

[125] Usnesení Ústavního soudu ze dne 16. 4. 2019 sp. zn. II. ÚS 1095/19 bod 12

[126] Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě. Senát Parlamentu České republiky. [online] Publikováno 2013 [cit dne 8. 9. 2019] dostupné z: https://www.senat.cz/xqw/webdav/pssenat/original/66810/56264

Logická spojka mezi (1) prvním počítačovým systémem a (2) druhým počítačovým systémem měla býti nejspíše „i“. Dle názoru autora postrádá smysl, aby měl členský stát povinnost zavést takovou právní úpravu, při které OČTŘ mají možnost rozšířit prohlídky pouze v případě, že se zájmová data nenachází na (1) prvním systému, ale pouze na (2) druhém systému. Teologickým výkladem se nejspíše dopátráme smyslu požadavku na rozšíření prohlídky i v případě, že se zájmová data nachází na (1) prvním počítačovém systému, a minimálně část nich i na (2) druhém systému.

Dle názoru autora česká právní úprava tento požadavek Úmluvy splňuje. Pokud by došlo k zajištění věci (1) např. při domovní prohlídce, ale došlo ke zjištění, že data či informace významné pro trestní řízení se nacházejí např. na cloudovém systému, který lze považovat za další systém (2), mají OČTŘ možnost požádat o vydání příkazu (dle § 158d TŘ) o zajištění dat na tomto sytému uložených.

4.3.1. Získávání digitálních dat utajeným operativně pátracím technickým prostředkem

Technickým prostředkem dle § 158d odst. 3 TŘ se rozumí různá technická zařízení, umožňující zjišťování obsahu korespondence a jiných písemností, a záznamů uchovávaných v soukromí.[127]

V nedávné době byla diskutována skutečnost, že PČR využívá softwarové trojské koně, které umožňují vzdálený přístup do uživatelských zařízení. Způsob využívání zařízení je předmětem kontroverze.[128]

Existenci využívání skrytého přístupu do uživatelských zařízení nepřímo potvrzuje tisková zpráva „Použití sledovacího softwaru" ve které PČR přiznává, že Útvar zvláštních činností SKPV určitým sledovacím programovým disponuje. Jeho pořízení a fungování však podléhá utajení.[129] Využívání utajené operativně pátrací techniky, pomocí které lze skrytě zajistit obsah zařízení po interpelaci na půdě poslanecké sněmovny přiznal i ministr vnitra ČR.[130] Autor této práce v režimu zákona o svobodném přístupu k informacím dožádal PČR ke sdělení skutečnosti, jaký software k takovémuto jednání využívá, jakou metodou k infikaci zařízení dochází, a jaké jsou podrobné statistiky využité tohoto zařízení. PČR žádost odmítla z důvodu, že se jedná o utajované informace.

Výše uvedené potvrzuje i nález ÚS, dle jeho názoru: *„V rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky. Pořízení otisku elektronických dat lze povolit postupem dle § 158d odst. 3 tr. řádu, pokud jde o data na sledovaných počítačích již uložená, … ".*[131]

---

[127] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 158d [Sledování osob a věcí]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2001.

[128] Útvar PČR - ÚZČ minimálně v roce 2015 využíval softwarové nástroje kontroverzní skupiny Hacking Team. Nákup zařízení PČR provedla skrze prostředníka, spol. Bull s.r.o. Skupina Hacking Team se stala předmětem kybernetického útoku, a ztratila přibližně 400 GB citlivých dat. Z uniklých dat je zřejmé, že software vždy nepracoval, jak měl. Z uniklé konverzace vyšlo najevo, že zástupce ÚZČ si stěžoval na skutečnost, že se řídící SMS zprávy zobrazují na displeji infikovaného zařízení dle institutu § 158d odst. 3 TŘ. – zdroj: Dopis ministra vnitra ČR Milana Chovance poslankyni Janě Černochové č.j. PPR-20893 – 1/ ČJ-2015-990300 ze dne 17. 8. 2015 a dále: KRČMÁŘ, Petr. *Hacking Team hacked: prodával spyware mnoha státům včetně Česka. Root.cz.* [online] publikováno 7. 7. 2015. [cit. 1. 11. 2019]. Dostupné z: *https://www.root.cz/clanky/hacking-team-hacked-prodaval-spyware-mnoha-statum-vcetne-ceska/*

[129] Použití sledovacího softwaru. *Policie České republiky.* [online] publikováno 7. 7. 2015 [cit. 18. 12. 2019] dostupné z: http://www.policie.cz/clanek/pouziti-sledovaciho-softwaru.aspxF

[130] Dopis ministra vnitra Milana Chovance poslankyni Mgr. Janě Černochové ze dne 17. 8. 2015 č. j. PPR-20893–1/ČJ-2015-990300

[131] Viz usnesení Ústavního soudu ze dne 3. 10. 2013 sp. zn. III. ÚS 3812/2012

Nabízí se tedy otázka, zda pro tak zásadní zásah, jakým je instalace sledovacího softwaru do uživatelského zařízení bude ze strany OČTŘ postačovat splnit stejné podmínky, jako pro sledování, prováděné technickým prostředkem, tedy např. „prostorový“ odposlech v obydlí či kanceláři podezřelé osoby.

V pojetí zákona se totiž jedná o identické instituty, které vyžadují splnit stejné zákonné podmínky pro rozhodnutí o jejich umožnění ze strany soudu, resp. o vyslovení souhlasu s jejich užitím. Výše uvedenou zákonnou definici: *„sledováním osob a věcí (...) se rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky“* je nutné vnímat jako obecnou. Pod ní lze podřadit jak prostorový odposlech, tak právě instalaci sledovacího softwaru do zařízení. Protože při sledování bude typicky zacházet do zásahu do nedotknutelnosti obydlí nebo zjišťován obsah písemností či jiných záznamů, uchovávaných v soukromí, je nutné získat souhlas soudce.

Jedním z nejvýznamnějších případů poslední doby je využití nástroje § 158d TŘ ve formě prostorových odposlechů v kauze Rekonstrukce zámku Buštěhrad.[132] V této kauze sehrály prostorové odposlechy stěžejní úlohu. Pro umístění prostorového odposlechu do kanceláře bývalého vrcholového politika, Davida Ratha státní zástupce žádal z důvodu, že se domníval, že se v prostorách jeho kanceláře (budovy Krajského úřadu) schází pachatelé za účelem upřesnění dalšího postupu při ovlivnění průběhu zadávacího řízení veřejné zakázky.

Uvedení těchto skutečností, spolu s postoupením spisového materiálu, ze kterého nejspíše plynou skutečnosti o tomto svědčící postačovalo okresnímu soudu k vydání povolení ke sledování, resp. k umístění sledovacího zařízení.

Žádost byla odůvodněna především tím, že obsah domluvy podezřelých, kdy se schůzka koná v kanceláři jednoho z podezřelých lze zjistit pouze za použití operativně technických prostředků. Dále bylo argumentováno, že při vzájemné osobní znalosti podezřelých nelze použít pouze instituty trestního řádu nezasahující do práv podezřelých, ale že k zadokumentování jejich trestné činnosti je nutné využívat především operativně pátrací prostředky, jejichž použití bude před podezřelými utajováno. Dále došlo k uvedení dalších formálních i materiálních podmínek, např. odůvodnění, proč se jedná o neodkladný úkon.

Obvodní soud žádost přezkoumal, a vydal povolení (které je rozhodnutím *sui generis*), ve kterém doslovně převzal výše uvedenou žádost státního zástupce,

[132] Jedním z pachatelů je bývalý vrcholový politik MUDr. David Rath.

doplněnou o odstavce ve kterých je konstatováno, že soudkyně žádost přezkoumala, a že má za to, že došlo ke splnění podmínek dle § 158d odst. 3 TŘ. Konstatovala dále, že je zřejmé, že při vzájemné osobní znalosti podezřelých a konspirativnosti jejich jednání nelze použít pouze běžné instituty trestního řádu nezasahující do práv podezřelých, ale že k zadokumentování jejich trestné činnosti je nutné využívat především operativně pátrací prostředky, jejichž použití bude před podezřelými utajováno. Uvedla, že souhlasí s tím, že se jedná o neodkladný úkon, který nesnese odkladu do fáze zahájení vyšetřování. **Konstatovala tedy, že shledává podmínky pro povolení sledování uvedené kanceláře podezřelého.**

Na výše uvedeném jsou zajímavé další skutečnosti. Předně to, že fakticky došlo k překopírování obsahu žádosti státního zástupce při vydávání souhlasu o povolení sledování věci. K překopírovanému obsahu žádosti soudkyně obvodního soude pouze doplnila odstavec pojednávající o tom, že se s tímto ztotožňuje, a že má za to, že došlo ke splnění podmínek. **Nejvyšší soud k tomuto uvedl, že takto uvedenému postupu okresního soudu nejde z formálního, natož z materiálního hlediska cokoliv vytknout.**[133]

Autor práce si položil otázku, zda je nutné rozlišovat, zda po vydání povolení soudu, lze dle preferencí policejního orgánu využít fyzický prostorový odposlech či instalaci sledovacího softwaru. Jak plyne z výše uvedeného, ale i z nespočtu dalších rozhodnutí, v povolení provádění sledování věci dochází k základní identifikaci prostorů, v nichž do zásahu na soukromí dochází. Připomeňme, že dle ustálené praxe ÚS[134] se ve smyslu zásahu do těchto prostor za obydlí považují i místa, užívaná k pracovní či podnikatelské činnosti nebo k uspokojování vlastních potřeb či zájmových aktivit.

K samotnému prostorovému odposlechu může dojít fyzickou instalací zařízení, přenášející audiovizuální záznam. Byla by však ve výše uvedeném případě, kdy došlo k povolení odposlechů kanceláře (vyslovený souhlas soudu hovoří o povolení odposlechu kanceláře) možné provádět odposlech instalací softwaru, který umožňuje využití audiovizuálních vstupů zařízení (integrovaného mikrofonu či webkamery)? Nabízí se dvě možné varianty. Instalace software, který přenáší pouze audiovizuální informace zařízení, které je lokalizováno pouze ve sledovaném prostoru bude zřejmě možná. Zásah do zařízení, který by využil např. extrakci ukládaných souborů či

[133] Rozhodnutí Nejvyššího soudu ze dne 7. 6. 2017 sp. zn. 6 Tz 3/2017

[134] Nález Ústavního soudu ze dne 8. 6. 2010 sp. zn. Pl. ÚS 3/09

informací by již byl značně extenzivním výkladem vydaného povolení, který by byl v rozporu s v TŘ vyjádřenou zásadou přiměřenosti. Není vyloučeno, že by došlo k neoprávněného zásahu do integrity zařízení (a tedy naplnění skutkové podstaty trestného činu § 230 TZ). Takto získané informace jsou nejen nepoužitelné, ale OČTŘ se mohou dopustit spácháním TČ neoprávněného přístupu k počítačovému systému.

4.3.2. Instalace sledovacího softwaru do zařízení třetích osob

Jak to bude s uživatelskými zařízeními, které jsou buď vlastněny právnickou (či podnikající fyzickou osobou), či jsou ve vlastnictví podezřelé osoby, ale tato je používá k plnění pracovních úkolů?[135] Obsah těchto zařízení je dle názoru autora nutné považovat za písemnosti, či jiné záznamy, uchovávané v soukromí. Takto je tomu z důvodu, že zaprvé, je velmi pravděpodobné, že je podezřelá osoba může používat stejně, jako zařízení soukromé a dále s ohledem na zásah do práv právnické (nebo podnikající fyzické) osoby. Opačný výklad by znamenal, že by nebylo chráněno právo na informační sebeurčení podezřelé osoby (při užití pracovního zařízení podezřelou osobou) či zásah do práv právnické osoby. Pokud by však při provádění úkonu došlo ke zjištění, že se právnická osoba dopouští páchání TČ, kterou s vyšetřovanou či prověřovanou věcí nesouvisí, je možné tyto informace použít pouze za předpokladu, že s tím osoby souhlasí (jak podezřelý v původní věci, tak právnická osoba v nové věci) souhlasí, nebo že se právnická osoba dopouští úmyslného TČ.

Shrňme tedy, že o instalaci sledovacího softwaru do pracovních zařízení platí podmínky identicky, jako při povolování nástroje pro čistě uživatelské zařízení. Pokud nejde jinak, software může být nainstalován i do pracovních zařízení.

4.3.3. Způsob instalace sledovacího softwaru

Je otázkou, jakým způsobem může dojít k „infikaci“ uživatelských zařízení, za účelem provádění operativního úkonu. Dle názoru autora se nabízejí dvě možnosti.

První z možností, je fyzický přístup k zařízení, a nainstalování sledovacího softwaru do věci, jíž bude prováděn odposlech. Instalace softwaru bude přirozeně probíhat bez vědomí podezřelé osoby. Může být provedena například v zaměstnání podezřelého, jeho osobním vozidle ale dokonce i v obydlí podezřelého. To, že může být instalace softwaru do zařízení provedena v obydlí podezřelého, nepřímo plyne z čl. 12

[135] tedy půjde např. o osobu v pracovněprávním vztahu v postavení zaměstnance, užívající pracovní počítačový systém.

odst. 3 dle kterého jiné zásahy do nedotknutelnosti obydlí, než domovní prohlídka mohou být zákonem dovoleny, jen je-li toho v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku, kterým je i páchání úmyslných trestných činů. Soudce před tím, než povolí (resp. rozhodne o souhlasu) infikaci zařízení, o kterém se lze domnívat, že bude provádět shromažďování informací o podezřelém musí uvážit, zda je spáchaný, nebo páchaný úmyslný TČ dostatečným dostatečně závažným ohrožením veřejné bezpečnosti a pořádku. Možnost infikovat zařízení v obydlí podezřelého plyne i z ustanovení § 158d odst. 3 TŘ, dle kterého platí, že: *„při vstupu do obydlí pak nesmějí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků.“*. Instalací zařízení dle názoru autora může dojít i k prolomení zabezpečení zařízení, je-li toho provádějící subjekt schopen, neboť instalace softwaru bude považována za umístění technického prostředku. Zároveň však ze zařízení, do nejž bude instalován software není možné extrahovat žádná data. Úkonem instalování technického prostředku nelze nahrazovat zásahy do práv a svobod, ohledně nichž je stanoven zvláštní režim TŘ (jedná se zejména o § 78, 79, 82, 83, 83a, 85c, § 86 až 87a, § 88 a 88a TŘ).[136] Uvážíme-li, že za technický prostředek se dle citovaného ustanovení považuje software, pak dojdeme nutně k tomu, že ze zařízení, jehož infikace je prováděna nemohou být při procesu instalování zajišťována či vytěžována žádná data. Ty mohou být vytěžována až po instalaci softwaru. Datový tok při tomto úkonu (samotné instalace) je tedy veden pouze do uživatelského zařízení, v žádném případě směrem z něj. To, zda je zařízení zabezpečeno, např. uživatelským heslem či nikoliv na tom nic nemění. Instalace zařízení by tedy měla být prováděna za využití hardwarového blokátoru,[137] který umožní pouze jednosměrný provoz zásahu, tj. pouze zápis na úložiště infikovaného zařízení.

Druhou z možností je instalace sledovacího softwaru distančně. Typicky půjde o odeslání škodlivého kódu elektronickou poštou. K infikaci zařízení sledovacím algoritmem může dojít i vložením paměťového média či propojením s jiným zařízením. Je však otázkou, zda bude sledovací software schopen autoinstalace na široké platformě možných zařízení, které mohou užívat různé operační systémy s různým stavem

[136] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 158d [Sledování osob a věcí]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2001 - 2011.

[137] Hardwarový blokátor umožňuje pouze jednostranný tok digitálních dat. Může se jednat jak o povolení pouze zápisu, tak pouze kopírování nebo čtení analyzovaných dat. Jak je dále rozvedeno níže, PČR těmito blokátory disponuje.

instalovaných zabezpečení a pravidelně vydávaných bezpečnostních záplat a aktualizací. Legálně je však tato metoda možná. Bude na policejním orgánu, aby na trhu poptal a pořídil dostatečně vyspělý software.

Jaké informace mohou být z infikovaných zařízení vytěžovány? Dle názoru autora jakékoliv, jejichž pořízení nebo poskytnutí je dané zařízení schopno. Relevantní je tedy užití informací, významných pro trestní řízení, které jsou uloženy na úložišti zařízení či pořizování zvukového, ale i obrazového záznamu skrze mikrofon, fotoaparát či kameru zařízení. Zákon jasně pojednává o odposlechu, prováděným technickým prostředkem. A protože se za technický prostředek po instalaci sledovacího softwaru stává celé uživatelské zařízení, jeví se jako relevantní užití i veškerých jeho senzorů.

Sledování za pomoci technického prostředku může být důležitý nástroj z důvodu, že analýza datového toku může být šifrována, a tedy nebude možné jí dle ustanovení § 88 odst. 1 TŘ technicky provést. Datový tok je však nejčastěji šifrován pouze po dobu přenosu dat. V uživatelském zařízení je již zpřístupněn v nešifrované podobě – minimálně k okamžiku, kdy se uživatel seznamuje s obsahem přepravované informace. Pokud bude skrze výše uvedený „sledovací“ software ze zařízení možné extrahovat informace a písemnosti, bude tak možné alespoň jednorázově zajistit (již nešifrovaný) soubor informací, které jsou uloženy v e-mailové schránce, či jiné, obdobné službě, neboť výše uvedené stanovisko NSZ je dle názoru autora aplikovatelné i na služby typu WhatsApp, Viber a jiné, které datový tok šifrují metodou end-to-end. **Dle názoru autora nic nevylučuje, aby při současném splnění podmínek § 158d odst. 3 a zároveň § 88 odst. 1 TŘ docházelo k extrakci doručených zpráv, zobrazovaných písemností či ukládaných písemností jakož i jiných informací, zobrazovaných či ukládaných do uživatelského zařízení.**

4.3.4. Přístup k obsahu e-mailové schránky a cloud computingu

Poskytovatel služby e-mailového účtu dle ustanovení § 89 ZEK není oprávněn obsah zpráv uchovávat v pro něj čitelné podobě. Dle stanoviska NSZ lze však připustit možnost výše uvedeným institutem zjištění aktuálního stavu e-mailové schránky.[138] Takto se však lze seznámit jednorázově s obsahem v tomto úložišti uložených zpráv.

Stejná situace dle názoru autora nastává v případě, kdy dojde k zajištění počítače, mobilního telefonu nebo obdobného zařízení, které pro příjem e-mailových zpráv využívá aplikaci na principu aplikace MS Outlook. Analyzovat doručené (a automaticky stažené zprávy) je možné jen do okamžiku zajištění zařízení.[139] Soudní praxe musí vyřešit otázku, zda pro analýzu dalších doručených zpráv po zajištění zařízení je nutné krom § 158d odst. 3 TŘ splnit i podmínky dle § 88 TŘ. Autor je názoru, že analýza doručování nových zpráv (či ukládání souborů do cloudu) je již faktické realizování odposlechu přepravovaných zpráv, a § 158d odst. 3 TŘ přitom nemusí definovat dostatečně přísné podmínky pro zásah do ústavně zaručeného práv a svobody, neboť zákonodárce úkon odposlechu (§ 88) podmiňuje, mimo jiné, vyšetřováním TČ – zločinu, za který hrozí trest odnětí svobody v trvání 8 let. Stejný názor zastává výkladové stanovisko státního zastupitelství.[140] Pokud tedy vyžadují OČTŘ dlouhodobější možnost zkoumat budoucí odchozí a příchozí zprávy, či jiné data nebo informace je nutné tento úkon realizovat pouze na základě soudního příkazu dle § 88 odst. 1 TŘ.

Pokud mají být data, získaná výše uvedeným postupem použita jako důkaz v trestním řízení, je nezbytné o jejich zajištění sepsat řádný a podrobný protokol.[141]

Současný výrazný rozmach využívání cloudových služeb vede k legitimní potřebě zkoumání jejich obsahu. Zajištění uživatelského zařízení (§ 78, § 79, § 82 TŘ), které část digitálních dat dislokuje na cloudové služby však neznamená, že i tato dislokovaná data jsou bez dalšího použitelná pro účely trestního řízení.[142]

---

[138] ZEMAN, Pavel. *Stanovisko ke sjednocení výkladů zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.* Nejvyšší státní zastupitelství. Brno, 2015.

[139] V této věci platí obdobný princip, jako v případě doručování SMS zpráv. Autor je názoru, že judikatura, týkající se SMS zpráv v síti GSM je aplikovatelná na e-mailové zprávy obdobně. Viz např. usnesení Nejvyššího soudu ze dne 15. 12. 2000 sp. zn. 7 Tz 9/2000.

[140] ZEMAN, Pavel. *Stanovisko ke sjednocení výkladů zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.* Nejvyšší státní zastupitelství. Brno, 2015.

[141] PŮRY, František. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 58 – 61.

Typický příklad využití tohoto institut při vyšetřování kybernetické kriminality je přístup na cloudové služby skrze zařízení, zajištěné při domovní nebo osobní prohlídce. Takovým zařízením může být server, osobní počítač, mobilní telefon, či jiné, obdobné zařízení. Pokud má takovéto zařízení v sobě uložené přístupové údaje ke cloudové službě, která je jinak zabezpečena potřebnou znalostí přístupového údaje (loginu) a hesla, není možné do této služby prostřednictvím způsobilého zařízení vstoupit.

Vstoupit do cloudové služby (bez splnění podmínek § 158d odst. 3 TŘ) není možné ani v případě, kdy je k tomu zajištěné zařízení bez dalšího schopné, tedy když má tyto přihlašovací údaje uloženy v prohlížeči, nebo když cookies nastavení umožní přístup do služby bez znalosti hesla.

V případě, že by OČTŘ přistoupily prostřednictvím zajištěného zařízení bez splnění podmínek (§ 158d odst. 3 TŘ), není vyloučeno, že se dopustí TČ neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ.[143]

Principem ukládání dat do cloudových úložišť je jejich průběžná dislokace z uživatelských zařízení na vzdálené servery. V případě, že je poskytovatel cloudových služeb právnickou osobou se sídlem na území ČR, a server s daty se fyzicky nachází na území ČR postačuje nejspíše kombinace příkazu *data freeze* dle § 7b TŘ a § 158d odst. 3 TŘ k zajištění a zjištění obsahu uživatelských dat.[144]

Všechna uživatelská data, či jejich část mohou být nahraná na cloudové úložiště, fyzicky dislokované na několika místech po světě. Zajištění dat ze serverů, umístěných v zahraničí tak již často bude vyžadovat mezinárodní součinnost.

Za data, vyžadující splnění podmínek institutu § 158d odst. 3 TŘ se však nebudou považovat data, která jsou uložena na pevném disku, i na cloudové službě – tj. např. v případě synchronizované složce. Pokud dojde při pořizování bitové kopie paměťového zařízení k těmto datům při provádění §§ 78, 79, 82 TŘ, není třeba dalšího svolení soudu.[145]

---

[142] HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. *Revue pro právo a technologie*. [Online]. 2016, č. 14, s. 11. [cit. 2019-10-23]. Dostupné z: https://journals.muni.cz/revue/article/view/6120

[143] PEJČOCHOVÁ, Alena a ELBERT, Tomáš. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 214.

[144] Problematika vyžádávání dat, zajištěných dle § 7b TŘ je rozsáhle rozvedena níže.

[145] HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. Revue pro právo a technologie. [Online]. 2016, č. 14, s. 10. [cit. 2019-10-23]. Dostupné z: https://journals.muni.cz/revue/article/view/6120

4.3.5. Zpětná kontrola využití institutu § 158d odst. 3 TŘ

Autor považuje za nezbytné upozornit na skutečnost, že ačkoliv přístup do cloudové služby, e-mailové schránky či dokonce softwarové provádění odposlechu může být z hlediska proporcionality zásahu minimálně srovnatelný s odposlechem telekomunikace, institut sledování za využití technického prostředku dle § 158d odst. 3 TŘ neukládá OČTŘ zpětnou notifikaci „odposlouchávané" osobě o skutečnosti, že vůči ní došlo k využití tohoto institutu. Dále neexistuje možnost srovnatelná s přezkumem příkazu k odposlechu dle § 314l TŘ. Jak upozorňuje kolegyně Lovíšková,[146] Nejvyšší soud shledal, že z ustanovení § 314 TŘ je jasné, že Nejvyšší soud může přezkoumat pouze příkaz k odposlechu a záznamu telekomunikačního provozu podle § 88 nebo 88a TŘ, nikoliv však povolení ke sledování osoby obviněného podle ustanovení § 158d TŘ.[147] To je poměrně alarmující skutečnost, pokud uvážíme, že policejní orgán má (sic po nutném vydání souhlasu soudu) možnost bez vědomí podezřelého instalovat do zařízení software, který je schopen velmi invazivním způsobem vytěžovat jakákoliv zájmová data, informace či důkazy ze sledovaného zařízení. Pokud OČTŘ takto vytěžená data nepoužijí v trestním řízení, podezřelý ani nemá jakoukoliv šanci se o provedeném úkonu dozvědět.

Statistiky hovoří o velmi vysokém čísle využívání tohoto nástroje. Jen v roce 2018 došlo ukončení celkem 5.580 úkonů, spojených s využitím sledování osob a věcí (sic i dle ostatních ustanovení, tedy dle § 158d odst. 2, 3 a 6 TŘ). O použití úkonu sledování osob a věcí došlo v roce 2018 v celkem 1.058 unikátních spisech.[148]

---

[146] LOVÍŠKOVÁ, Zuzana. *Odposlech a záznam telekomunikačního provozu*. Praha, 2013, Univerzita Karlova v Praze, Právnická fakulta. Vedoucí práce Jiří ŘÍHA. s. 10.

[147] Usnesení Nejvyššího soudu ze dne 19.9.2012 sp. zn. 4 Pzo 3/2012

[148] *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2018*. Policejní prezidium České republiky. [online] publikováno 22. 8. 2019 [cit. dne 1. 09. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

Za zmínku stojí, že ÚZČ SKPV PČR Poslanecké sněmovně v ročním intervalu předkládá zprávu, jejímž předmětem je analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací PČR. **V aktuální verzi, předložené zákonodárcům bohužel zcela absentuje informace o tom, zda dochází k využíváním nástroje jako možnosti pro zjištění obsahu e-mailové schránky, cloud computingu nebo jako vzdálený přístup do uživatelského zařízení (instalace sledovacího softwaru).** Absentuje nejen statistika takových použití, která se velmi nepřehledně vyskytuje pouze pro celkový počet úkonů dle § 158d odst. 2, 3 a 6 TŘ či rozlišena způsobem, který ničeho spolehlivě nevypovídá, ale absentuje i popis, že k takovému využití nástroje dochází.

4.3.6. Závěrem ke sledování, za využití technických prostředků

Z výše uvedeného lze shrnout, že institut § 158d odst. 3 TŘ je zcela stěžejní pro realizaci softwarového odposlechu, přistupování do e-mailových, cloudových služeb jakož i obdobných služeb. Institut však vykazuje výrazné nedostatky. Předně dle názoru autora původně mířil ke zcela rozdílnému účelu, a to ke sledování osob a věcí a k prostorovému odposlechu. Institut vzhledem k intenzitě zásahu postrádá nastavení jasných a dostatečně přísných podmínek pro jeho užití.

Instalace „odposlouchávacího" softwaru, např. do mobilního telefonu je nesmírně cenný nástroj k boji s kybernetickou kriminalitou. Zároveň jde o takřka sci-fi nástroj, zasahující do ústavně zaručených práv podezřelé osoby snad tím nejinvazivnějším možným způsobem. Toho by si měl být soudce při jeho povolování (resp. vyslovení souhlasu s úkonem) vědom, a tento nástroj by měl být při vyšetřování skutečně nástrojem *ultima ratio.* Jakkoliv nepředstavitelně jeho běžné využívání zní, z doložených skutečností plyne, že policejní orgán podobný software zakoupil a dle všeho i do uživatelských zařízení nasazoval. Jeho skutečná technologická funkčnost je však otázkou. Jisté však je, že může být jeden z mála nástrojů, kterým alespoň v teoretické rovině může dojít k překonání efektivního šifrování přepravovaných zpráv, dat či informací.

Zjištění, že ustanovení neobsahuje povinnost OČTŘ vyrozumět o jeho užití subjekt „odposlechu" a následnou možnost přezkumu jeho užití považuje autor práce za kritické. V případě, že by ÚS rozhodl o jeho nesouladu s ústavně zaručeným právem a svobodou (zejména pro absenci povinnosti notifikace a pro nedostatečně přísně nastavené podmínky pro jeho nařízení) a přitom nevyužije možnost odložení vykonatelnosti rozhodnutí hrozí, že OČTŘ nebudou schopny přistupovat na cloud, zajišťovat obsah e-mailového účtu či nadále užívat prostorový odposlech. Lze očekávat, že zavádění obdobného institutu do TŘ bude mezi zákonodárci za kritického sledování veřejnosti konfliktní.

4.3.7. Návrh *de lege ferenda*

Plynoucím návrhem *de lege ferenda* k využívání § 158d odst. 3 TŘ je z výše uvedených okolností především:

1) jednoznačná úprava textace zákonné úpravy, ideálně s uvedením, že ustanovení může být využíváno i vyšetřování kybernetické kriminality, tj. jako vzdálený přístup do zařízení (ať už na vzdálené serverové služby či do

fyzických uživatelských zařízení). Institut, zavedený do TŘ novelou v roce 2002 je totiž ohýbán jako původní nástroj, umožňující „prostorový odposlech“[149] pomocí technického zařízení;

2) stanovení přísnějších podmínek pro využívání institutu. Je zřejmé, že v případě, kdy dojde k infikaci zařízení, umožňující stažení obsahu zařízení jde intenzitou zásahu do základních práv a svobod o minimálně stejný zásah, jako dle § 88 odst. 1 TŘ;
3) zavedení povinnosti notifikovat podezřelou osobu po provedení úkonu po vzoru § 88 odst. 8 a dále zavést možnost podezřelé osoby iniciovat řízení o vylovení nezákonnosti provedeného úkonu dle § 314l až § 314n TŘ;
4) jeví se také jako vhodné doplnit zákonné znění o ustanovení, striktně zakazující jakoukoliv změnu integritu uživatelských dat, vyjma instalace samotného „odposlouchávacího“ softwaru;
5) povinnost soudu, vyslovit při souhlasu s použitím úkonu identifikaci účtů (e-mailových či cloudových) nebo zařízení, do nichž má být zasahováno.

Minimálně absenci povinnosti notifikovat podezřelou osobu o tom, že vůči ní došlo k využití § 158d odst. 3 TŘ považuje autor za velmi vážné porušení čl. 8 EÚLP a zásah do základních práv a svobod.

Kromě hrozby napadaní takového postupu ústavní stížností a s tím potencionálně hrozící naplnění doktríny ovoce z otráveného stromu, tedy nepoužitelnost takto získaných důkazů se dle názoru autora ČR dostává do rozporu s Úmluvou o počítačové kriminalitě.[150] Ta v článku 15 odst. 1 a 2 stanovuje povinnost signatářů implementovat procesní nástroje úmluvy způsobem, který je v souladu s vnitrostátními předpisy jakož i s Úmluvou Rady Evropy na ochranu lidských práv a základních svobod z roku 1950, Mezinárodního paktu OSN o občanských a politických právech z roku 1966, a dalších příslušných mezinárodních dokumentů o lidských právech, a které budou obsahovat princip přiměřenosti.

[149] Jak podotýká prof. Jelínek, trestně-právní zákonná úprava ostatně nedefinuje ani termín prostorový odposlech. JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie.* [online] 2018, č. 9. [cit. 1. 9. 2019]. Dostupné z: https://journals.muni.cz/revue/about/submissions?navItem=0

[150] Relevance možnosti dovolání se doktríny z otráveného stromu částečně plyne z nálezu Ústavního soudu ze dne 14. 5. 1999 sp. zn. IV. ÚS 135/99, dále nálezu Ústavního soudu ze dne 26. 9. 2000 sp. zn. I. ÚS 129/2000, nebo nálezu Ústavního soudu ze dne 27. 3. 2003 sp. zn. IV. ÚS 757/2000. Přesto však autor není názoru, že doktrína byla přijata bez dalšího.

Připomeňme, že notifikace osoby, do jejíchž práv bylo zasaženo odposlechem plyne z ustálené judikatury ESLP. Tato judikatura navazuje na ustanovení čl. 8 EÚLP, dle kterého je nezbytné osobu, do jejíž práv bylo zasaženo odposlechem či vydáním záznamu zpětně uvědomit. Vzhledem k tomu, že jde o zásah svojí intenzitou minimálně shodný není důvodem se domnívat, že by tomu u tohoto institutu mělo být jinak.

4.4. Ohledání

Digitální stopy, které jsou volně přístupné v síti Internet, například ve formě veřejně přístupné webové stránky, volně stažitelného souboru či veřejné části sociální sítě (Facebook, Twitter, Instagram atd.) je možné zajistit bez dalšího. Zákon nestanovuje žádné restrikce či podmínky pro jejich zajištění.[151] Zajištění těchto stop se řídí ustanovením § 113 TŘ.

Ohledání obsahu elektronických stop (skutečností významných pro trestní řízení) bude realizováno formou přímého pozorování, resp. pozorování digitálních dat, zprostředkovaných prostřednictví zobrazovacích zařízení výpočetní techniky.

O průběhu, jakož i o výsledku ohledání je všeobecně nutné vyhotovit písemný protokol. Zákon zdůrazňuje, že protokol o ohledání musí obsahovat úplný a věrný obraz předmětu ohledání. Z tohoto důvodu je tedy vhodné k němu připojit fotografie, náčrty a jiné pomůcky.[152]

Není důvod se domnívat, že výše uvedený postup by se měl zásadně odlišovat od ohledání elektronických stop. Technik, nebo příslušník PČR (nebo jiná osoba, zpravidla znalec) o pozorování elektronického obsahu, zobrazeného prostřednictvím zobrazovací techniky (monitor či reproduktory počítače) pořídí protokol. Do toho podrobně uvede sledované skutečnosti. Protokol doplní o snímky obrazovky sledovaného obsahu. Je však vhodné, aby došlo k pořízení zobrazených souborů. Pokud bude závadný obsah text, je vhodné provést stažení zdrojového kódu sledovaného obsahu (typicky webové stránky). Pokud je vnímaným obsahem fotografie, videozáznam, či datový soubor, je vhodné daný soubor zajistit. Je tedy vhodné pořídit kopii zobrazovaných dat. Tyto data mohou být přiložena jako příloha protokolu o ohledání.

---

[151] PŮRY, František. *Elektronické důkazy v trestnímřízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 78.

[152] ŠÁMAL, Pavel. § 113 [Účel ohledání a protokol o něm]. *Trestní řád I, II, III.* 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1628. bod 7

4.5. Dožádání dle § 8 TŘ

Situaci, kdy bylo ze strany OČTVŘ nutné zajistit obsah digitálních dat TŘ do nedávné doby výslovně neuváděl. Nejrelevantnější bylo využití ustanovení § 8, odst. 1 TŘ, dle kterého jsou všeobecně všechny osoby (či státní orgány) povinny i bez úplaty vyhovovat dožádání OČTVŘ při plnění jejich úkolů, a to bez zbytečného odkladu. Dle odstavce 7 tohoto ustanovení jsou zároveň všechny osoby povinny zachovávat mlčenlivost o všech skutečnostech, které se v souvislostech s dožádáním informace dozvědí. Ačkoliv meze tohoto ustanovení dle autora nejsou pevně vymezeny, je jeho užití relevantní jen v těch případech, kdy v dané situaci nelze využít jiného institutu.[153] Pokud tedy OČTŘ potřeboval získat informaci či digitální data, měl možnost zaslat žádost právnické či fyzické osobě, které má k datům přístup (tedy je držela jak fyzicky na serverech či k nim měla možnost přístup), využil právě tohoto institutu. Tento institut však nepřikazuje formu dožádání – postačuje tedy běžný přípis či ústní výzva. Povinná osoba žádosti musí vyhovět bez zbytečného odkladu a nestanoví-li zákon jinak, i bez úplaty.

Neuposlechnutí výzvy k součinnosti je dle ustanovení § 66 TŘ sankcionovatelné uložením pořádkové pokuty. Její výše může dosáhnout až částky 50.000 Kč. Pokud by však byla identická osoba dožádána ve více věcech, byť se týkající konkrétního skutku, lze uložit více jednotlivých sankcí. Uložit pokutu však v žádném případě nelze uložit osobě, proti níž se trestní řízení vede. Takový postup by byl v rozporu s principem *nemo tenetur se ipsum accusare*, vyjádřeným čl. 37 odst. 1 a čl. 40 odst. 4 Listiny.

Dle komentářové literatury lze tuto pokutu uložit ve lhůtě jednoho roku ode dne, kdy došlo k jednání, které je důvodem k jejímu uložení. Po více než roce již uložení pokuty není možné.[154] Zůstává otázkou, kdy započne lhůta k poskytnutí odpovědi na dožádání běžet, neboť povinné osoby odpovídají bez zbytečného odkladu. Lze se domnívat, že časový okamžik, po kterém se povinná osoba ocitne v prodlení může být závislý na charakteru a rozsahu dožádané informace.

[153] Typicky dle institutu dožádání (§ 8 odst. 1 TŘ) nebude možné požádat ISP o sdělení provozních a lokalizačních údajů, zde OČTŘ musí postupovat dle § 88a TŘ.

[154] ŠÁMAL, Pavel a GŘIVNA, Tomáš. § 66 [Pořádková pokuta]. In: *Trestní řád I, II, III.* 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 714.

Pokud však jiné ustanovení stanovuje podmínky, za kterých je možné přistoupit k zásahu do zákonem zaručené mlčenlivosti (např. čl. 13 LZPS – uchovávání listin v soukromí) je nutné užít tohoto speciálního ustanovení. Přiléhavé bude tedy např. požadovat data, uchovávané v soukromí dle ustanovení vydání věci nebo domovní podmínky.

4.6. Urychlené zajištění digitálních dat v síti Internet dle § 7b TŘ

Český právní řád do nedávné doby nenabízel nástroj, který by bylo možné použít k urychlenému zajištění digitálních dat. Problematické na existenci digitálních dat (tedy například i stopám vedoucím k dopadení pachatele či závadném obsahu, potencionálně použitelném jako důkazu o spáchání TČ) je to, že jsou velmi snadno vymazatelné či pozměnitelné. Pachatel je schopen taková digitální data nenávratně odstranit v horizontu několika vteřin. Autor je názoru, že toto ustanovení je vůči ustanovení § 8 TŘ v postavení *lex specialis*. OČTŘ tedy při zajišťování digitálních důkazů nemají možnost volby mezi instituty[155], ale pokud dojde k naplnění okolností (viz níže), předpokládaných § 7b TŘ, je nutné využít právě jej.

Příkladem může být smazání obsahu e-mailové schránky, účtu na sociální síti nebo obsahu webové stránky. Disponent online účtu je tak například po spáchání TČ podvodu, kdy z oběti vyláká finanční prostředky jednoduše schopen obsah stránky odstranit. Obdobný osud může potkat existenci či obsah zpráv profilu na sociálních sítích.

4.6.1. Data freeze dle § 7b TŘ

[155] Resp. nemají možnost volby mezi § 8 odst. 1 TŘ a § 7b odst. 1 TŘ.

S účinností od 1. 2. 2019 vstoupil v účinnost zákon č. 287/2018 Sb., který doplnil TŘ o institut, který je pro boj s kybernetickou kriminalitou dle názoru autora klíčový. Účelem nového, převážně procesního ustanovení je legální možnost OČTŘ urychleně nařídit zajištění digitálních dat tím, že vydají osobě, které jimi disponuje (např. na serveru) příkaz k jejich zajištění pro účely trestního řízení. Doplnění právního řádu o tento institut předpokládá článek č. 16 Úmluvy, který vyžaduje zákonný nástroj, dle kterého smluvní strany: (i) mohou svým orgánům přikázat anebo obdobně zajistit urychlené uchování specifických počítačových dat a (ii) zajistit jejich uchování povinnou osobou tak, aby mohly orgány požádat o jejich zpřístupnění a (iii) povinná osoba bude mít povinnost držte informaci o tomto postupu v tajnosti. Tento institut se vžil pod pojmem *data freeze*.

Tento institut je možné využít v případě, že je zapotřebí zabránit ztrátě, zničení nebo pozměněním dat, která se nacházejí v síti Internet, v počítačovém systému nebo na paměťovém médiu. Příkaz k zadržení dat, které znemožní jejich změnu je možné vydat osobě, které tato data drží až na dobu 90 dnů.

Novým procesním nástrojem je taktéž možné nařídit osobě, které má data v dispozici (o tom, zda jde nutně jen o výše uvedená data viz dále) jejich znepřístupnění. Typicky se bude jednat o blokaci obsahu webové stránky.

S implementací tohoto nástroje byla Česká republika po dlouhou dobu v prodlení. Jedná se však o zásadní procesní nástroj, který může být pro zajištění digitálních stop nepostradatelný.

4.6.2. Data freeze dle § 7b odst. 1 TŘ

Jaká data mohou být zajištěna? Dle znění § 7b, odst. 1 TŘ viz: „*Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění* ***dat*** *důležitých pro trestní řízení,* ***která jsou uložena v počítačovém systému nebo na nosiči informací****, (...)"* mohou být zajištěna jakákoliv data, který jsou uložena v počítačovém systému nebo na nosiči informací.

Vyložit pojem data nejspíše nebude problém. Bude se jednat o jakékoliv informace, skutečnosti s libovolnou vypovídající hodnotou. Z důvodu, že jde o data, která musí být uložena v počítačovém systému či na paměťovém médiu plyne, že se jedná o data digitální.

Interpretační obtíže však mohou nastat s pojmem počítačový systém. Důvodová zpráva[156] k novelizaci TŘ, která institut zavádí přejímá definici počítačového systému dle Šámala.[157] Dle této se počítačovým systémem rozumí *„jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. (...)"*. Z této definice dle názoru autora neplyne, zda se za součást počítačového systému bude považovat propojené cloudové úložiště.

[156] Vláda: Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz
[157] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C. H. Beck, 2012. Str. 2300.

Za nosič informací důvodová zpráva,[158] znovu inspirována komentářovou literaturou, demonstrativně vyjmenovává: *„pevný disk (tzv. „HDD“ nebo „hard disk“), operační paměť (tzv. RAM), disketa, CD-R, CD-RW, DVD-R, DVD+R, DVD-RW, DVD+RW, Blu-Ray, USB key, mobilní telefon.“*. Zde je výklad dle názoru autora jasný. Není pochyb o tom, že díky technickému rozvoji budou přibývat další paměťové nosiče. Bohužel, důvodová zpráva pomíjí, že nyní velmi běžným trendem je průběžné ukládání dat na cloudové servery. Je otázkou, zda cloudové úložiště posoudit jako počítačový systém dle předchozího odstavce, nebo nosič informací.

Jak plyne z předchozích odstavců, okruh dat, které mohou být zajištěny příkazem na principu *data preservation* je nesmírně široký, a dokáže pokrýt jakýkoliv typ elektronického důkazu, se kterým se lze v souvislosti s vyšetřováním kybernetické kriminality setkat. Obava, že praxe bude vyžadovat zajištění digitálních dat, které z legálních důvodů nebude možné urychleně zajistit nehrozí. Ruku v ruce se širokým záběrem zajistitelných digitálních dat se nabízí i velmi široký okruh subjektů, které mohou být povinni k provedení příkazu. Výše došlo k předestření typických povinných osob. Dle názoru autora však povinnou osobou může být prakticky libovolná právnická či fyzická osoba. Nabízí se otázka, jak bude subjekt, který není technicky zdatný schopen příkazu fakticky vyhovět. Technicky nezdatný uživatel možná bude chtít využít pomoci technicky odborné osoby. Je to však možné? Ustanovení § 7b, odst. 1 TŘ vyžaduje: … (povinná osoba je povinna) *učinit potřebná opatření, aby nedošlo ke* ***zpřístupnění informace o tom,*** … (že došlo k zajištění dat). Z litery zákona neplyne standard ochrany zajištěných dat. Autor není názoru, že by povinný měl zachovat absolutní utajení o tom, že došlo k příkazu k zajištění dat. Pokud tedy dojde k využití služeb odborné osoby, např. soudního znalce, který je vázán zákonnou mlčenlivostí,[159] k porušení podmínky nezpřístupnění informací o tom, že došlo k zajištění nejspíše nedojde.

[158] Vláda: Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz

[159] Mlčenlivost je nejen věcí dobrých mravů či etiky ale i zákonnou povinností – viz zákon o soudních znalcích

Dostáváme se k požadavku zákona uchovat data v ***nezměněné podobě***. Ideálním postupem povinné osoby bude nejspíše zajistit bitovou kopii označených dat. Kopii dat bude vhodné provést za využití hardwarového blokátoru (viz níže). Nejspíše nebude proti ničemu, pokud OČTŘ v příkazu nařídí povinnému o zajištění dat nařídí vyhotovit protokol, do kterého bude uveden kontrolní součet bitových dat. Jedině takový způsob uchování dat zajistí jejich integritu a hodnověrnost.

Požadavek na existenci legislativního, nebo jiného opatření, které umožní příslušným orgánům přikázat nebo obdobně urychleně zajistit konkrétní digitální data pokud existuje důvod, že jsou tyto data ohrožena ztrátou vznáší Úmluva o počítačové kriminalitě v článku 16. Se splněním povinnosti implementace článku 16 Úmluvy byla Česká republika v prodlení déle než 6 let.[160] Takto dlouhé prodlení se zavedením stěžejního ustanovení a legitimní požadavek pro signatáře Úmluvy disponovat možností efektivně zajistit digitální důkazy. Jedním z cílů Úmluvy je bezpochyby vytvoření prostoru, v němž je možné efektivní odhalování kybernetické kriminality. V takovém případě absence implementace klíčového ustanovení na území, byť i jediné smluvní strany způsobuje nejistotu a nežádoucí situaci, kdy část závadného jednání zejména s přeshraničním prvkem nebude možné odhalit z důvodu, že jiná smluvní strana nebude mít možnost efektivně požádat přeshraniční spolupráci jiný stát, tvořící nejslabší článek řetězu.

K využití institutu *data freeze* (dle § 7bodst. 1 TŘ), resp. k nařízení příkazu, musí být tedy splněny následující podmínky:

1) existence potřeby zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací,
2) označení dat, na která se příkaz vztahuje, důvod, pro který mají být data uchována nebo k nim má být znemožněn přístup, a doba, po kterou mají být tato data uchována nebo k nim má být znemožněn přístup.

Příkaz k zajištění digitálních dat je oprávněn vydat předseda senátu. V přípravném řízení příkaz vydává státní zástupce. Pokud však věc nesnese odkladu, a předchozího

[160] Ratifikační listina České republiky byla uložena u generálního tajemníka Rady Evropy, depozitáře Úmluvy, dne 22. srpna 2013. Úmluva vstoupila v platnost na základě svého článku 36 dne 1. července 2004. Pro Českou republiku vstoupila v platnost podle odstavce 4 téhož článku dne 1. prosince 2013. Viz sbírka mezinárodních smluv č. 104/2013.

souhlasu státního zástupce v přípravném řízení nelze dosáhnout, může být příkaz k uchování digitálních dat vydán pouze policejním orgánem. **Příkaz k uchování digitálních dat tedy může být vydán policejním orgánem nejen bez posouzení nezávislým subjektem (po fázi přípravného řízení konkrétně předsedou senátu), ale dokonce i bez souhlasu státního zástupce.**

Nařízení osobě, která má data k dispozici se děje formou příkazu, který se neprodleně doručuje subjektu *data-holder* (nejčastěji ISP, provozovatel webhostingu, freemailových služeb…), který je povinný data zajistit či znepřístupnit.

Lze bezpochyby kladně hodnotit skutečnost, že na rozdíl od institutu § 88a TŘ, ukládající povinnost shromažďovat *data retention* plošně tento institut cílí pouze na osoby, u kterých existují indicie o tom, že se dopouštějí páchání TČ. Institut, dle kterého dojde k zajištění dat konkrétní osoby při důvodné pochybnosti je v době významného rozmachu páchání trestné činnosti v síti Internet bezpochyby nezbytný. Připomeňme, že princip uchovávání *data retention* je totiž obecný, a plošně dopadá na prakticky všechny uživatele výpočetní techniky.

Jak zdůrazňuje důvodová zpráva,[161] příkaz *data freeze* se vztahuje pouze na již shromážděná a uchovaná data – princip *data preservation*. V žádném případě se příkaz k uchování dat nevztahuje a nemůže vztahovat na data, vznikající *pro futuro*. Dle názoru autora je žádoucí, že zákonodárce poskytl tento výklad zákona. Bez tohoto výkladového vodítka by bylo pravděpodobné, že by mohlo docházet ke snahám OČTŘ k přikazováním subjektům *data-holders* k zajišťováním dat *pro futuro.* Takto se již ostatně událo extenzivním výkladem § 88a TŘ rozhodnutím Nejvyššího soudu.[162] Taková iniciativa je dle názoru autora nepřípustná. Jediný institutem pro zajišťování digitálních stop, informací či důkazů, který slouží k zajišťování dat *pro futuro* je odposlech a záznam telekomunikačního provozu dle § 88 TŘ. Jediný tento institut vyvažuje invazivní zásah do zaručených práv nutností splnění přísných podmínek pro jeho nařízení, jakož i dalších podmínek (nutnost posuzování nutnosti jeho trvání, možnost přezkumu atd.). To ostatně plyne i z jazykového výkladu zákona, neboť dle § 7b, odst. 4 TŘ: *„V příkazu podle odstavce 1 nebo 2* ***musí být označena data, na která se příkaz vztahuje****…“*. Není zřejmé, jak by šlo označit data, která mají teprve v budoucnu vzniknout.

[161] Vláda: Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz
[162] Usnesení Nejvyššího soudu ze dne 7. 5. 2019 sp. zn. 4 Tdo 1591/2018

4.6.3. Vydání zajištěných dat dle příkazu data freeze

Je však povinná osoba po zajištění dat dle vydaného příkazu bez dalšího povinna data vydat OČTŘ? Vydáním zajištěných dat se povinná osoba může dostat do střetu s povinností uchovávání písemností a jiných informací v soukromí, zaručených v čl. 13 LZPS. Jazykovým výkladem části § 7b odst. 1 TŘ (viz: „*... 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.****"*) dojdeme k závěru, že data bez dalšího povinna vydat není. Z litery zákona plyne, že má dojít k (i) uchování dat a (ii) učinění opatření k tomu, aby podezřelý nebyl notifikován či jinak seznámen s informací, že došlo k zajištění digitálních dat. Omezit ústavně zaručená práva a svobody je však možné jen v případech, stanovených zákonem. Dalším z argumentů pro neexistenci k vydání dat zajištěných příkazem nasvědčují poměrně benevolentní podmínky pro nařízení příkazu – ze všech zajišťovacích legálních nástrojů, jsou snad dle všeobecného nástroje dožádání nejméně přísné. Implementovat nástroj způsobem, aby bylo možné bez dalšího požadovat předání zajištěných dat neplyne ani z Úmluvy o počítačové kriminalitě.

Současné znění § 7b TŘ tedy dle názoru autora nejen neukládá jejich vydání, ale vydání dat či jejich osud po uplynutí stanovené lhůty k uchování ani nikterak neřeší. Povinný dle příkazu však zpravidla zpracovává digitální data třetí osoby. Při absenci povinnosti k vydání je dle názoru autora nelze vydat ani dobrovolně. Povinný oprávněn data vydat není, neboť by tím zasáhl do ústavně zaručených práv podezřelého. Podezřelý zase není srozuměn o tom, že byla data zajištěna.

Vzhledem k tomu, že ustanovení vstupuje v účinnost jen necelý rok před odevzdáním této práce, doposud není sjednocen názor odborné veřejnosti na postup, jakým by zajištěná data měla být získávána pro účely trestního řízení jako procesně použitelný důkaz. Dle jakých institutů je v teoretické rovině zajištěná data relevantní požadovat? Nejspíše půjde o dožádání (§ 8 TŘ), vydání a odnětí věcí (§ 78 – 79 TŘ), domovní prohlídky a prohlídka nebytových prostor (§ 82 a násl. TŘ), odposlech a záznam telekomunikačního provozu (§ 88 TŘ), sledování osob a věcí (§ 158d TŘ).

Sokol[163] uvádí, že OČTŘ (konkrétně policejní orgán) v současné době požadují vydání dat v režimu § 158d TŘ (o tomto ustanovení, podmínkách pro jeho použitelnost atd. viz níže). Připomeňme, že toto ustanovení primárně míří na sledování osob a věcí. Požadavek praxe, vzhledem k absenci vhodnějšího institutu z něj učinila primární nástroj, pomocí kterého lze (i) přistupovat do e-mailové schránky jakož i do cloudových služeb a (ii) provádět softwarový odposlech zařízení. **Sokol poukazuje na to, že dle § 158d TŘ soudce vyslovuje povolení, nikoliv příkaz.** Poukazuje na jazyková paradox, neboť nástroj primárně míří k souhlasu s instalací zařízení k odposlechu. Dle jeho názoru ho tedy není možné jej použít k požadavku na vydání zajištěných dat.

Dle Púryho,[164] data veřejně nedostupná, nebo zabezpečená je nutné považovat za písemnosti a záznamy uchovávané v soukromí. K takovým datům je možné přistoupit po (i) předchozím souhlasu soudce za splnění podmínek § 158d odst. 3 nebo (ii) dobrovolným vydáním podezřelým.

Dle názoru Gřivny nemůže být o data žádána ani v režimu institutu § 8 odst. 1 TŘ (dožádání), neboť je třeba využít zvláštního institutu. Pokud by nástroj dožádání bez dalšího složil k překonání ústavně zaručeného práva na tajemství informací, uchovávaných v soukromí, nebylo by v TŘ třeba již jiného zajišťovacího institutu. V úvahu připadá vydání věci, provedení osobní či domovní prohlídky a prohlídky nebytových prostor.

Toman[165] je dokonce názoru, že žádný z výše uvedených institutů se bez dalšího k vydání zajištěných dat na bázi *data preversation* bez dalšího nehodí.

Argumentace, že dle § 158d odst. 3 TŘ soudce vydává souhlas a nikoliv příkaz je dle názoru autora relevantní. Zákonodárce předvídal strpění jednání (jakkoliv o tom podezřelý v době provádění úkonu vědět nemusel, a jak je uvedeno níže, vzhledem k absenci povinnosti notifikovat se ani nikdy dozvědět nemusí) a nikoliv aktivní jednání povinné osoby. Na druhou stranu, zcela identickým postupem soudce povoluje přístup k datům, uloženým v e-mailové schránce, či v cloudovém úložišti. Poskytovatel e-mailových či cloudových služeb je taktéž povinen data vydat jen na základě souhlasu soudu. Jako dočasné tedy takovéto řešení nejspíš bude fungovat, je však vhodné ze strany zákonodárce zavést zcela nový institut. Níže komentář k dalším nástrojům.

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

[164] STUPKA, Václav. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015. Str. 104.

[165] TOMAN, Petr. Podstračený paragraf 7b Trestního řádu - kde se vzal a o čem je. *advokatnidenik.cz* [online]. 22. 7. 2019 [cit. 3. 11. 2019]. Dostupné z: https://www.cak.cz/scripts/detail.php?id=20932

Dožádáním dle § 8 TŘ není možné překonat ústavně zaručené právo. Stejný problém nastává u vydání věci dle § 78 TŘ. Při existenci speciálního ustanovení, definující zásah do mlčenlivosti nebo do soukromí je nutné takového institutu. Institut dožádání se tedy užije jen v případě, že neexistuje jiné zákonné ustanovení.[166]

Odposlech a záznam telekomunikačního provozu splňuje dostatečně přísné podmínky pro jeho nařízení na to, aby mohl zasáhnout do ústavně zaručených práv a svobod. Z principu se však jedná o nástroj, kterým se důkazy získávají *pro futuro.* I přes tento problém se spolu s § 158d TŘ jedná o jeden z vhodnějších nástrojů.

Zcela scestná není ani úvaha nad zajištěním dat nástrojem domovní či nebytové prohlídky. Tento úkon v sobě obsahuje zákonné zmocnění k zajištění dat. Proti použití tohoto nástroje však stojí nespočet odborných názorů, zastávajících k přístupu k datům, uloženým na cloudovém úložišti či na e-mailových serverech nezbytnost využití nástroje § 158d TŘ. Zbývá k zamyšlení, zda by však například příkaz k provedení domovní prohlídky, či sledování prováděné technickým prostředkem směřovalo proti povinnému (tedy tomu, který má povinnost zajistit data) nebo podezřelému. Provedení domovní prohlídky či sledování povinné osoby zřejmě vyloučíme, a zbyde nám možnost zajistit příkaz k provedení domovní prohlídky (či odnětí věci, prohlídky nebytových prostor atd.) vůči podezřelému.

I přes výše uvedený, a poměrně významný problém s tím, jak budou zajištěná data v souladu se zákon předávána OČTŘ tak, aby se jednalo o použitelný důkaz je však autor názoru, že došlo k implementaci ustanovení § 7b TŘ v souladu s požadavkem čl. 16 Úmluvy o počítačové kriminalitě. Příslušné ustanovení Úmluvy o počítačové kriminalitě krom povinností tak, jak je zavádí § 7b odst. 1 TŘ neuvádí ničeho dalšího.

4.6.4. Znemožnění přístupu k digitálním datům (dle § 7b odst. 2 TŘ)

Způsob implementace článku č. 16 Úmluvy o počítačové kriminalitě je extenzivnější, než jak jej ukládá tento dokument. V současném znění ustanovení § 7b odst. 2 TŘ zákonodárce poskytl OČTŘ nástroj, dle kterého mají možnost, je-li to zapotřebí, nařídit osobě, která drží digitální data či je má k dispozici, aby zajistila jejich znepřístupnění po dobu až 90 dnů.

[166] ŠÁMAL, Pavel. § 8 [Dožádání a ochrana utajovaných skutečností a údajů, na něž se vztahuje mlčenlivost]. In: *Trestní řád I, II, III.* 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 120.

K využití institutu *znemožnění přístupu k digitálním datům* (§ 7b odst. 2 TŘ) musí být kumulativně splněny následující podmínky:

1) existence potřeby zabránění pokračování v trestné činnosti nebo jejímu opakování,
2) označení dat, na která se příkaz vztahuje, důvod, pro který mají být data uchována nebo k nim má být znemožněn přístup, a doba, po kterou mají být tato data uchována nebo k nim má být znemožněn přístup.

Subjekt, oprávněný příkaz vydat je určen stejně jako k příkazu *data freeze*. Příkaz je oprávněn vydat předseda senátu. V přípravném řízení příkaz vydává státní zástupce. Pokud však věc nesnese odkladu, a předchozího souhlasu státního zástupce v přípravném řízení nelze dosáhnout, může být příkaz k znepřístupnění digitálních dat vydán pouze policejním orgánem. **Příkaz k znepřístupnění digitálních dat tedy může být vydán policejním orgánem nejen bez posouzení nezávislým subjektem (po fázi přípravného řízení konkrétně předsedou senátu), ale dokonce i bez souhlasu státního zástupce.**

Skutečnost, že příkaz může vydat policejní orgán vyvolává kontroverze. Jen stěží si lze představit situaci, kdy by žádost o znepřístupnění dat snesla odkladu. Typicky se bude jednat o data na volně přístupných webových stránkách. Výskyt potenciálně závadného obsahu (podvodného e-shopu, phisingové stránky či dětské pornografie) z principu vždy vyžaduje rychlý zásah, směřující k nápravě nežádoucího stavu.

Není přitom zřejmé, zda se za znepřístupnitelná mohou označit pouze data, která jsou zároveň předmětem příkazu dle § 7b odst. 1 TŘ, či jakákoliv jiná, volně dostupná digitální data.[167] Z jazykového výkladu plyne, že se nejspíše jedná o jakákoliv data. Autor je však názoru, že úmyslem zákonodárce bylo nejspíše pouze rozšíření pravomocí dle § 7b odst. 1 TŘ, tedy aby data mohla být nejen uchována v nezměněné podobě, ale v závažných případech též znepřístupněna. Proti tomu by však šlo argumentovat, že povinná osoba dle § 7b odst. 1 TŘ je povinna o nařízení uchování dat zachovat mlčenlivost. O znepřístupnění obsahu by se pachatel bezpochyby dozvěděl. **Ať už byl úmysl zákonodárce jakýkoliv, dle jazykového výkladu lze za splnění výše**

[167] SOKOL, Tomáš. Povinnost dle § 7b trestního řádu z pohledu advokáta. *Bulletin advokacie*. 2019, č. 9, s. 15-19. ISSN 1210-6348.

uvedených podmínek nařídit znepřístupnění jakýchkoliv volně přístupných digitálních dat.

Situace, kdy policejní orgán dle své vlastní úvahy rozhoduje o znepřístupnění digitální obsahu a disponuje nástrojem, dle kterého může vydat příkaz k zablokování webových stránek, profilů sociálních služeb či celých internetových aplikací lze jen obtížně považovat za ústavně konformní pro možný rozpor se svobodou projevu, zaručenou v čl. 17 odst. 4, právem na výkon výdělečné činnosti zaručeným v čl. 26 odst. 2 a ochranou vlastnického práva ve smyslu čl. 11 odst. 3 Listiny.

Ostatně sama Úmluva o počítačové kriminalitě ukládá členským státům článek 16 (respektive všechny procesní ustanovení čl. 16 – 21) povinnost implementovat a jeho orgánům následně využívat článku v souladu s podmínkami a zárukami stanovenými dle vnitrostátních předpisů, které poskytnou přiměřenou ochranu lidských práv a svobod. Zároveň musí být tato ustanovení implementována a využívána zejména v souladu se zaručenou ochranou lidských práv, kterou poskytuje Úmluva rady Evropy na ochranu lidských práv a základních svobod z roku 1950 a Mezinárodní pakt OSN o občanských a politických právech z roku 1966. Dle článku 15 odst. 2 Úmluvy o počítačové kriminalitě je třeba, dle názoru autora, za takovou podmínku zahrnovat mimo jiné soudní či jiný nezávislý dohled, spočívající v nezávislém posouzení o nutnosti blokaci předmětných dat.

4.6.5. Blokace nelegálního hazardu v kyberprostoru

Blokování digitálních dat bez rozhodnutí soudu není v české právní úpravě úplnou novinkou. Dne 1. 1. 2017 nabyl účinnosti zákon č. 186/2016 Sb., o hazardních hrách (tento zákon ve znění pozdějších přepisů dále jen jako „ZOHH"). Ustanovení § 82 – 84ZOHH vymezuje institut, dle kterého jsou ISP po rozhodnutí správního orgánu povinni zamezit přístupu k internetovým stránkám, poskytující nelegálních herní aktivity. Ustanovení konkrétně vymezují povinnost ISP blokovat pro uživatele ty webové stránky, které jsou uvedeny či dojde k zápisu na seznam nepovolených webových hazardních her, provozovaných v síti Internet. Zápis do seznamu provádí *ex offo* Ministerstvo financí. Řízení o zápisu do seznamu je správním řízením. ISP mají povinnost sledovat seznam, a nejpozději po 15 dnech od doplnění seznamu splnit povinnost zamezení přístupu. Nesplnění této povinnosti je dle ustanovení § 123 odst. 5 ZOHH sankcionováno pokutou až do výše 1.000.000 Kč. Stejnou povinnost mají krom ISP i provozovatelé platebních služeb ve prospěch či v neprospěch bankovních účtů.

K povinnosti vydalo Ministerstvo financí, odbor 73 – Procesní agendy a regulace hazardu dne 16. 1. 2017, tedy 16 dnů po nabytí účinnosti zákona, metodický pokyn[168] povinným osobám.

Výše uvedené ustanovení se v době schvalování v legislativním procesu setkalo s odporem široké veřejnosti. Veřejnost kritizovala zákon především z důvodu, že seznam nepovolených hazardních her vyhotovuje Ministerstvo financí – tedy složka moci výkonné. Nejčetnější argument zaznával, že rozhodnutí o zařazení konkrétní webové adresy do seznamu rozhodne úředník bez zvláštní kvalifikace. [169]

O zrušení výše uvedených ustanovení na návrh skupiny senátorů rozhodoval Ústavní soud. V plenárním nálezu ze dne 14. 2. 2017, sp. zn. Pl. ÚS 28/16[170] posuzoval soud soulad ustanovení, ukládající povinnost blokovat webové stránky, uvedené na seznamu nepovolených hazardních her s články čl. 11 odst. 3, čl. 17 odst. 4, čl. 26 odst. 2 Listiny. Ústavní soud shledal ustanovení ústavně konformní.

K existenci seznamu nelegálních her, který je ve správě Ministerstva financí (blacklist) a do nějž zavedené webové stránky musí být subjekty ISP blokovány ÚS

[168] Ministerstvo Financí. *Metodický pokyn k plnění povinností (ve věci seznamu nepovolených internetových her)*. [online]. 16. 1. 2017. [cit. 10. 11. 2019]. Dostupné z: https://www.mfcr.cz/cs/legislativa/metodiky/2017/metodicky-pokyn-k-plneni-povinnosti-ve-v-27269

[169] Poslanci schválili zákon o hazardu, počítá i s blokováním webových stránek In: *E15.CZ* [online]. 13. 4. 2016. [cit. 12. 11. 2019]. Dostupné z: https://www.e15.cz/byznys/obchod-a-sluzby/poslanci-schvalili-zakon-o-hazardu-pocita-i-s-blokovanim-webovych-stranek-1287700

[170] Nález Ústavního soudu ze dne 14. 2. 2017 sp. zn. Pl. ÚS 28/16

uvedl, že jej neshledává ústavně nekonformní. O cenzuru dle jeho názoru nejde, neboť ji nelze přirovnávat k cenzuře Internetu, jako systémové kontrole či omezování sdělování informací. Dle jeho vysloveného názoru se jedná technické opatření, jehož účelem je zamezit ilegálním aktivitám.

Požadavek na blokaci přístupu webových stránek ze strany ISP a nikoliv poskytovatelů nelegálních her shledal legitimní, neb dovodil, že žádat o blokaci poskytovatele her by nebylo účelné. Nelegální online hazardní hry jsou dle jeho názoru provozovány často ze zahraničí, a efektivní postih státní orgánů není možný. Dle ÚS jsou ISP dále schopni zajistit efektivní blokaci obsahu, a navíc jsou dostupní za účelem komunikace s orgány státu. Aplikace zákona tak je, na rozdíl od zahraničních subjektů vymahatelná. U ISP navíc existují předpoklady pro průběžné (automatizované) sledování změn a aktualizací v seznamu nepovolených hazardních her. Dále je ISP, na rozdíl od zahraničních subjektů za neplnění povinností sankcionovatelný. K situaci, kdy o uvedení na seznam zakázaných stránek rozhoduje Ministerstvo financí ve správním řízení uvedl, že se nejedná o zásah do ústavně zaručených práv, neb existuje možnost přezkumu u nezávislého soudu ve formě žalobě proti rozhodnutí ve správním soudnictví[171] a tuto možnost považuje za dostatečnou pojistku zákonnosti postupu správních orgánů.

4.6.6. Ustanovení § 7b, odst. 2 TŘ ve světle nálezu o blokaci nelegálních hazardních her

Skutečnost, že o zablokování digitálního obsahu dle ustanovení § 7b odst. 2 TŘ za splnění dalších podmínek může rozhodnout policejní orgán a přikázat jejich znepřístupnění, byla s první touto žádostí o znepřístupnění dat medializována, a vžila se pod názvem „WEDOS gate“.[172] Takto vešla pod název z důvodu, že se proti tomuto ustanovení ostře ohradila společnost WEDOS Internet, a.s., která je významným tuzemským poskytovatelem webhostingu.[173] Skutečnost, že o blokaci rozhodne policejní

[171] dle § 65 a násl. zákona č. 150/2012 Sb., soudního řádu správního, ve znění pozdějších předpisů.

[172] WEDOS Internet, a.s. *První web vymazán z internetu na základě nového paragrafu §7b trestního řádu*. In: Blog WEDOS. [online]. 13. 3. 2019. [cit. Dne 16. 10. 2019]. Dostupné z: https://blog.wedos.cz/prvni-web-vymazan-z-internetu-na-zaklade-noveho-paragrafu-§7b-trestniho-radu

[173] Webhostingem se rozumí pronájem kapacity serverů za účelem umístění veřejně přístupných webových stránek. Zpravidla se jedná o komerčně nabízenou službu, resp. předmět činnosti podnikající osoby.

orgán společnost vnímala jako zásadní zásah do svobodného Internetu, jakož i do jejího práva na svobodné podnikání.

Pokud by ÚS posuzoval, že dle ustanovení § 7b odst. 2 TŘ o zablokování stránek rozhoduje policejní orgán, nejspíše lze očekávat část výše uvedené argumentace. I v případě výskytu závadného obsahu v síti Internet převládá potřeba co nejrychleji daný obsah webové stránky znepřístupnit. Zároveň je stejně jako v posuzované věci dán předpoklad toho, že jakékoliv výzvy k odstranění závadného obsahu nebudou splněny. Jeví se, že by jako jeden z argumentů zazněl, že jde pouze o časově omezený okamžik, po který mohou být data znepřístupněna.

4.6.7. Přezkum příkazu dle § 7b odst. 1 a 2 TŘ

Vydaný příkaz dle § 7b postrádá zvláštní ustanovení, umožňující se dotčenému subjektu (podezřelému) domáhat vyslovení nezákonně provedeného úkonu. Vzhledem k tomu, že se jedná o rozhodnutí formou příkazu – a možnost jeho vydání má i policejní orgán (viz § 7b odst. 2 TŘ) není dle komentářové literatury[174] relevantní ani užití opravného prostředku stížnosti dle § 141 TŘ. Tento opravný prostředek (resp. dle názoru autora spíše přezkumný, neboť jde jen o úkon zajišťující informace k meritornímu rozhodnutí ve věci) je možné směřovat jen proti procesní formě usnesení. Komentářová literatura[175] výslovně uvádí, že stížnost není přípustná proti jiným formám rozhodování a postupů OČTŘ, jako je např. příkaz.

Připomeňme, že příkazem může policejní orgán rozhodnout o blokaci digitálních dat bez dalšího, a to pouze za poměrně snadno splnitelných podmínek (i) existence potřeby zabránění pokračování v trestné činnosti nebo jejímu opakování a (ii) označení dat, která mají být znepřístupněna.

Ve světle výše uvedeného nálezu ÚS, týkajícím se blokace nelegálních hazardních her v kyberprostoru,[176] tedy skutkově velmi obdobné věci, by takto formulovaný § 7b odst. 2 TŘ mohl být dle názoru autora posouzen jako ústavně nekonformní. Ve zmiňovaném nálezu ÚS jako jeden z nejvýznamnějších argumentů pro zachování ustanovení, umožňující moci výkonné bez rozhodnutí soudu rozhodnout o blokaci webových stránek shledal existenci dostatečné pojistky zákonnosti postupu výkonných

[174] GŘIVNA, Tomáš. § 141 [Přípustnost a účinek]. *Trestní řád I, II, III*. 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1754.
[175] GŘIVNA, Tomáš. § 141 [Přípustnost a účinek]. *Trestní řád I, II, III*. 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1754.
[176] Nález Ústavního soudu ze dne 14. 2. 2017, sp. zn. Pl. ÚS 28/16

orgánů možností iniciace žaloby proti rozhodnutí správního orgánu dle zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů. Jakýkoliv opravný prostředek však v posuzovaném ustanovení (§ 7b TŘ) absentuje. Zbývá pouze faktická libovůle policejního orgánu rozhodnout o blokaci webových stránek, bez jakékoliv nutnosti zpětně tento svůj postup posvětit nezávislým soudním orgánem. Posouzení či výklad podmínek pro splnění vydání blokace digitálních dat je taktéž v kompetenci tohoto orgánu. Shrňme tedy, že tento stav je stěží akceptovatelný.

4.6.8. Závěrem k urychlenému zajišťování digitálních dat

Závěrem lze k institutu *data freeze* uzavřít, že jeho část byla v souladu s potřebou mezinárodního závazku i praxe uvedena do českého právního řádu. Řádné využívání institutu má ambice zjednodušit a zvýšit objasněnost kybernetické kriminality. Akutně nutné je však vyřešit situaci, kdy ustanovení je způsobilé pouze k zajištění dat. Otázka předávaní dat pro účely trestního řízení zůstává otevřena. Jako dočasné řešení se jeví o data žádat, obdobně jako v případě žádání dat uložená na cloudu, v režimu § 158d odst. 3 TŘ. Tak, jak je institut nyní implementován není plně použitelný. Paradoxně je však implementován (vyjma výše uvedené výhrady k § 7 odst. 2 TŘ) v souladu s čl. 16 Úmluvy o počítačové kriminalitě – která vydávání dle názoru autora rovněž neřeší. Jde navíc o prostředek, jehož využívání na principu *data preservation* může přispět k šetření práva občanů, využívající síť Internet. Je však otázkou, zda jeho současné znění, kdy policejní orgán rozhoduje o blokaci digitálního obsahu obstojí do budoucna.

Současné znění ustanovení § 7b odst. 2 TŘ, umožňující blokaci obsahu webových stránek z rozhodnutí policejního orgánu lze považovat za minimálně rozporné s Listinou základních práv a svobod. Je pravděpodobné, že bude v brzké době podrobeno přezkumem ÚS. Pokud bude ÚS konzistentní v argumentaci, kterou uváděl v souvislosti s nálezem, týkajícím se blokace nelegálních hazardních her, je velmi pravděpodobné, že minimálně druhý odstavec ustanovení shledá jako v rozporu s ústavním pořádkem a že rozhodne z pozice negativního zákonodárce o jeho zrušení.

Institut *data freeze* v mnoha zemích zastupuje pro jeho menší intenzitu institut *data retention.*[177] Dle názoru autora lze tedy v případě budoucího derogačního nálezu k *data retention* Ústavním soudem (jako se již v minulosti opakovaně dělo) využít dočasně k potírání kybernetické kriminality právě tento institut. Bezpochyby by jeho existence mohla být i uvážena zákonodárcem ke zkrácení doby plošného uchovávání *data retention.*

4.6.9. Návrh *de lege ferenda*

Za vysoce aktuální téma ke změně právní úpravy autor spatřuje absenci zmocnění, dle kterého mohou OČTŘ požadovat vydání zajištěných dat. Jako možnost se jeví zavedení zcela nového legislativního nástroje, dle kterého by k vydání dat mohlo dojít.

[177] Např. Spolková republika Německo Viz: DE ZAN, Tomasso. AUTOLITANO, Simona. EUnited Against Crime: Improving Criminal Justicein European Union Cyberspace. Instituto Affari Ainternazionali. [online]. 16. 10. 2016 [cit. Dne 19. 8. 2019]. Dostupné z: http://www.iai.it/sites/default/files/iai1617.pdf

Vzhledem k velmi širokému pojetí dat, které mohou být zajištěna (ať již od pouhého obsahu webové prezentace, ale i obsah např. chatových zpráv) je nutné, aby podmínky pro vydání zajištěných dat byly nastaveny stejně přísně, jako pro odposlech datového provozu. Je také vhodné zavést zrychlený mechanismus, a to z důvodu, že data mohou být v držení maximálně po dobu 90 dnů.

Dalším z návrhů *de lege ferenda* je změnit situaci, že o blokaci webového obsahu bez dalšího může rozhodnout policejní orgán (7b odst. 2 TŘ). Tuto legislativně nešťastnou situaci lze zhojit tím, že příkaz k znepřístupnění dat, který vydal policejní orgán bez souhlasu bude muset do 3 dnů potvrdit soud. Je logické, že natolik zásadní zásah ze strany policejního orgánu musí být podroben rozhodnutím nezávislého orgánu. Je-li jednou příkaz vydán, pouhá skutečnost, že po určitý okamžik věc nesnesla odkladu neznamená, že rozhodnutí policejního orgánu nepodléhá nezávislému posouzení o oprávněnosti takového úkonu, jakým je znepřístupnění libovolných dat. Ostatně i rozhodnutí státního zástupce o příkazu k znepřístupnění dat nelze považovat za rozhodnutí nezávislého orgánu. O takto zásadní věci, jako je blokace obsahu webové stránky by měl rozhodovat bez zbytečného odkladu ideálně nezávislý soudní orgán. Je dále vysoce žádoucí doplnit zákonné ustanovení o možnost přezkumu vydání příkazu.

4.7. Fyzické zajišťování důkazů

Zajištění výpočetní techniky může být důležitým milníkem pro další zajištění digitálních důkazů. Za nejběžnější stopu v kyberprostoru uvažme jeden z provozních a lokalizačních údajů – IP adresu. Pokud budou mít OČTŘ štěstí, nevyužil pachatel žádných anonymizačních metod, a skutek nebyl spáchán skrze veřejný přístupový bod do sítě Internet (Wi-Fi síť v kavárně, MHD…). Postupem dle § 88a TŘ dojde ke zjištění osoby, která provozuje přístupový bod do sítě Internet. ISP je dle Vyhlášky o uchovávání[178] povinen uchovávat jméno a příjmení osoby, uvedené ve smlouvě o poskytování telekomunikačních služeb. **Dále je ISP povinen uchovávat adresu umístění telekomunikačního koncového zařízení.** Koncovým zařízením nejspíše zákonodárce neměl na mysli skutečné koncové fyzické zařízení, jako je počítač, tablet či mobilní telefon ale (nejčastěji Wi-Fi) síťový prvek, pomocí kterého dochází k přístupu do sítě Internet. OČTŘ se však jako nejrelevantnější informaci dozví jména a příjmení osoby, uvedené ve smlouvě a adresu, na níž je umístěn síťový prvek. K síťovému prvku může být připojeno několik koncových zařízení, využívané libovolným počtem osob. Odhalení skutku, spáchaným některou z těchto osob je komplikováno tím, že informace vedoucí k této osobě jsou skryty za NATem. Zde může být připojeno několik koncových zařízení, které využívá více osob (sdílející domácnost, pracoviště…). Fyzické zajištění a analýza uživatelských, ale i síťových zařízení, nacházejících se na místě přístupového bodu nabídne další informace o tom, která osoba spáchala skutek.

Všechny výše uvedené instituty navíc pracují pouze s elektronickými daty, které jsou zajištěny v síti Internet. Tyto stopy se mohou vyznačovat různou mírou vypovídající hodnoty o spáchání skutku konkrétním pachatelem– kupříkladu od odposlechu datového toku, kdy můžeme předpokládat, že se jedná o poměrně spolehlivou informaci s relevantnější vypovídající hodnotou po zajištěnou IP adresu, jejíž vypovídající hodnota o spáchání skutku konkrétní osobou může být velmi nízká.[179]

---

[178] Dle ustanovení § 2 odst. 5 vyhlášky č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, ve znění pozdějších předpisů se dále uchovává jméno, popřípadě jména a příjmení a adresa účastníka nebo registrovaného uživatele uvedená ve smlouvě nebo adresa umístění telekomunikačního koncového zařízení.

[179] Zajištění IP adresy jako jediného důkazu nemusí o pachateli vypovídat ničeho. Uvažme situaci, kdy pachatel spáchá TČ z domácí Wi-Fi sítě osoby na kterou je přístupový bod do sítě Internet zřízen. Tato osoba nemusí mít o jednání pachatele ani ponětí. OČTŘ však postupem dle § 88a TŘ budou důvodně podezírat ze spáchání TČ osobu, z jejíž Wi-Fi sítě byl skutek spáchán. Naproti tomu soustavný odposlech a záznam telekomunikačního provozu datového toku z přístupového bodu do sítě Internet z mobilního telefonu dle § 88 TŘ má již relevantnější hodnotu – je nepravděpodobné, že by pachatel po dobu 4 měsíců využíval za přístupový bod do sítě Internet mobilní telefon nic netušící osoby.

Pro dostatečné zajištění všech informací a důkazů vedoucí ve výsledku k prokázání viny nadevší pochybnost je vhodné zajistit a vytěžit výpočetní techniku. Řádné zajištění a vytěžení výpočetní techniky za účelem získání důkazních prostředků v případě odhalování kybernetické kriminality může být nezbytné k naplnění zásady zjištění materiální pravdy, vyjádřené v ustanovení § 2 odst. 5 TŘ. Vzhledem k tomu, že zajištění přímého důkazu bude u vyšetřování tohoto typu kriminality značně nepravděpodobné, ne-li zcela nemožné, budou vyšetřovací orgány předkládat soudu k rozhodnutí o vinně řadu nepřímých důkazů. Bude spíše nepravděpodobné, že pouze zajištěné stopy v kyberprostoru poskytnou vnitřně nerozporný a jednotný řetězec nepřímých důkazů. Fyzickým zajištěním zařízení může dojít ke splnění požadavku, aby byl rozsudek soudu v trestní věci založen na faktech, která jsou přesně a úplně zjištěna, hodnověrná, a nevzbuzují žádné pochybnosti o své pravdivosti.[180]

Ideálním stavem, vedoucím k rozhodnutím o vinně konkrétní osoby je kombinace výše zmíněných nástrojů, tedy zajištění digitálních stop, jejich ztotožnění s možným pachatelem, následné provádění odposlechu a provedením domovní prohlídky. Ztotožnění zajištěných digitálních stop ve formě provozních a lokalizačních údajů, jak je rozvedeno níže, může postačovat k nařízení domovní prohlídky či prohlídky nebytových prostor.

V praxi dochází nejčastěji k odnětí věci důležité pro trestní řízení (počítače, mobilní telefony, paměťová média atd.) při domovní nebo osobní prohlídce. Pro zajištění a vytěžení takto zajištěných zařízení a médií není třeba zvláštního příkazu, neboť výzva k vydání takové věci a příkaz k jejímu odnětí jsou již zahrnuty v příkazu k domovní, resp. osobní prohlídce, jehož důvodem je právě i vydání, resp. odnětí, věci důležité pro trestní řízení.[181]

Pokud nedojde k naplnění podmínek pro příkaz k provedení domovní podmínky, nebo to není účelné (např. pro vysokou personální, taktickou a logistickou náročnost), je možné zajistit a vytěžit zařízení (či jiné věci, důležité pro trestní řízení) zejména za využití institutů předložení a vydání věci dle § 78 nebo odnětí věci dle § 79 TŘ. V

V režimu těchto institutů je možné požadovat jak vydání fyzické věci (obsahující i digitální data), tak i samotných digitálních dat.[182]

[180] CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008, s. 85.
[181] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 79 [Odnětí věci]. *Trestní řád I, II, III.* 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1020.
[182] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. Díl). *Trestněprávní revue*. 2019, č. 3, str. 66.

Věc, která je důležitá pro trestní řízení je dle § 78 TŘ povinna vydat osoba, která s ní disponuje. Vyzvat k předložení nebo vydání věci je oprávněn předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán. Nelze však nikoho nutit k vydání věci, která by mohla sloužit jako důkaz proti ní, nebo osobě jí blízké. Neuposlechnutí je sankcinovatelné (i) uložením pořádkové pokuty a (ii) odnětím věci dle § 79 TŘ. Věc za předpokladu předchozí výzvy a poučení o možnosti neuposlechnutí (s následkem uložení pokuty a odnětím věci) může být na příkaz předsedy senátu a v přípravném řízení na příkaz státního zástupce nebo policejního orgánu odňata.[183]

Jak však upozorňuje Dostál,[184] vydání elektronických dat dle těchto nástrojů nelze zaměňovat s institutem dožádání dle § 8 TŘ. Dožádání obsahuje možnost něco vyžadovat, nikoliv však oprávnění v případě nevyhovění výzvě přistoupit k fyzickému odebrání. V případě nevyhovění § 8 TŘ připadá v úvahu pouze uložení pořádkové pokuty do maximální výše 50.000 Kč. Připomeňme, že pokud ve vztahu k ustanovení § 8 odst. 1 existuje jiné, zvláštní ustanovení, je využít právě jej.

Vydaná výzva k vydání věci dle § 78 TŘ, i příkaz k odnětí věci dle § 79 TŘ postrádá zvláštní ustanovení, umožňující dovolat se přezkumu takového požadavku. Dle komentářové literatury[185] není relevantní ani užití přezkumného prostředku stížnosti dle § 141 TŘ. Tento přezkumný prostředek je možné směřovat jen proti procesní formě usnesení. Komentářová literatura výslovně uvádí, že stížnost není přípustná proti jiným formám rozhodování a postupů OČTŘ, jako je i např. příkaz.

[183] Dle ustanovení § 79 odst. 1 zákona č. 141/1963 Sb., trestní řád, ve znění pozdějších předpisů.

[184] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. Díl). *Trestněprávní revue*. 2019, č. 3, str. 66.

[185] GŘIVNA, Tomáš. § 141 [Přípustnost a účinek]. *Trestní řád I, II, III*. 7. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1754.

4.7.1. Domovní prohlídka

V případě důvodného podezření, že v bytě nebo v jiném prostředí sloužícím k bydlení je věc, nebo osoba důležitá pro trestní řízení lze za splnění dalších podmínek vykonat úkon domovní prohlídky.[186]

Na nařízení a provedení domovní prohlídky jsou kladeny přísné procesní podmínky. Nedotknutelnost obydlí je zaručena v čl. 12 LZPS. Domovní prohlídka dle tohoto článku je možná pouze pro účely trestního řízení a to na písemný odůvodněný příkaz soudu.

Dle ustanovení § 83 TŘ je oprávněn nařídit domovní prohlídku předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Návrh na provedení domovní prohlídky by měl obsahovat údaje o nemovité věci, dle kterých ji lze jednoznačně a nezaměnitelně identifikovat. K návrhu je vhodné doložit skutečnosti z katastru nemovitostí. Návrh obligatorně dále obsahuje údaje o účelu, který státní zástupce navržením domovní prohlídky sleduje. Obsahuje dále informaci o popisu skutku, pro který je návrh podáván a stručná právní kvalifikace.

Jak již bylo v této práci zmíněno, ISP je k IP adresám povinen uchovávat údaje o adresách (sloužící k identifikaci nemovitých věcí), ve kterých se nachází přístupový bod do sítě Internet. Postačuje však k vydání příkazu k provedení domovní prohlídky pouze stopa provozních a lokalizačních údajů – např. IP adresy, nasvědčující, že pachatelem mohla být osoba, u které SZ či PČR žádá o příkaz k provedení domovní prohlídky? Stěží si lze totiž představit invazivnější zásah do soukromí nevinné osoby, než provedení domovní prohlídky. O provádění domovní prohlídky se často dozví okolí podezřelé osoby. Ač je trestní řízení ovládáno zásadou presumpce neviny, právní laik si pohled na policejní orgán, provádějící prohlídku pravděpodobně spojí s vinou podezřelé osoby. Takto invazivní zásah (u možná i nevinné osoby) představuje reputační problém, snižující kvalitu života podezřelé osoby minimálně do doby meritorního rozhodnutí ve věci. Jak je rozvedeno níže, provádění domovní prohlídky za účelem zajišťování digitálních dat postihne pravděpodobně všechny členy společné domácnosti.

[186] FRYŠTÁK, Marek a kol. *Trestní právo procesní.* Ostrava: Nakladatelství KEY Publishing, 2008 s. 54.

Z následného písemného odůvodnění příkazu k domovní prohlídce musí být patrno, z jakých skutečností plyne podezření, že se v obydlí nachází věc nebo osoba důležitá pro účely trestního řízení. Posouzení toho, zda z pouhých provozních a lokalizačních údajů dokáže soudce zpracovat dostatečné odůvodnění příkazu k domovní prohlídce bude nejspíše posuzováno a vyhodnocováno *ad hoc*. Soudce v mezích svého uvážení posoudí, zda předkládané skutečnosti nasvědčují tomu, že existuje důvodné podezření, opravňující zásah do nedotknutelnosti obydlí. Úvahy, které ho k nezbytnosti úkonu vedly musí uvést do odůvodnění příkazu. Přirozeně bude vhodnější do návrhu na vydání příkazu, který předpokládá státní zástupce uvést co nejvíce rozhodných skutečností. Těmito může být větší množství zajištěných logů – tedy stopy, zajišťované po delší časové období. Informace o tom, že jednotlivé přístupy zanechávající stopy byly po dobu několika měsíců vedeny z IP adresy přístupového bodu, umístěné v identické nemovité věci budou relevantnější, než zaznamenání jediného přístupu z IP adresy, situované v nemovité věci, o jejíchž prohlídku státní zástupce žádá. Žádoucí bude i uvedení kombinace více stop – např. kombinace IP adresy a dalšího provozního a lokalizačního údaje, např. telefonního čísla v síti GSM, které je dnes ve stále více uživatelských účtech, aplikacích či webových stránkách při registraci vyžadováno. Z rozhodovací praxe plyne, že k nařízení příkazu k provedení domovní prohlídky může postačovat i jediná stopa ve formě zajištěné IP adresa.[187]

Nabízí se dále otázka, vůči komu bude příkaz k provedení domovní prohlídky směřovat? Zákon stanovuje, že domovní prohlídka bude provedena v bytě či nemovité věci. Pasivně legitimovanou osobu dle názoru autora zákon striktně neurčuje. Je tedy možné, že bude nařízena i proti osobě, které není primárním podezřelým ze spáchání TČ, a tato osoba bude povinna ji strpět. Ostatně tomuto svědčí i fakt, že bude-li ve společné domácnosti či obydlí žít více osob, bude nutné provést domovní prohlídku, a teprve zajištěním všech uživatelských zařízení a jejich analýzou mohou OČTŘ dojít ustanovení skutečného pachatele. Nevinné osoby budou povinny úkon strpět.

[187] Usnesení Ústavního soudu ze dne 10. 7. 2018 sp. zn. IV. ÚS 1313/18 nebo usnesení Ústavního soudu ze dne 23. 8. 2018 sp. zn. sp. zn. IV. ÚS 3636/15.

Příkaz k domovní prohlídce soud obligatorně vydává písemně a musí být řádně odůvodněný. Řádné neodůvodnění příkazů může mít za následkem jeho nepoužitelnost.[188] V neodkladných případech může na místo příslušného předsedy senátu nebo soudce učinit předseda senátu nebo soudce, v jehož obvodu má být domovní prohlídka vykonána. Osobě, u níž se domovní prohlídka koná se příkaz doručuje zpravidla při začátku domovní prohlídky. V případech, kdy není možné této osobě příkaz doručit osobně při domovní prohlídce z důvodu existující překážky, se doručuje nejpozději do 24 hodin od opadnutí této překážky, která bránila doručení.[189]

Zákonodárce zmírňuje tvrdost institutu provedení domovní prohlídky nebo prohlídky jiných prostor až po obligatorním provedení předchozího výslechu toho, u koho se má tento úkon konat. Z tohoto pravidla existuje výjimka, a to sice v případě, kdy věc nesnese odkladu a výslech nelze provést okamžitě.

Za podmínek uvedených v ustanovení § 160 odst. 4 TŘ, může být domovní prohlídka provedena i před zahájením trestního stíhání dle ustanovení § 158 odst. 3 písm. i) ve spojení s ustanovením § 160 TŘ.[190] Pokud je domovní prohlídka prováděna před zahájením trestního stíhání, má podezřelý první možnost využít práva na přítomnosti advokáta při předchozím výslechu.[191]

[188] Nález Ústavního soudu ze dne 1. 11. 2006 sp. zn. II. ÚS 362/06.

[189] FRYŠTÁK, Marek a kol. *Trestní právo procesní.* Ostrava: Nakladatelství KEY Publishing, 2008 s. 54.

[190] ŠÁMAL, Pavel. § 82 [Důvody domovní prohlídky a osobní prohlídky a prohlídky jiných prostor a pozemků]. *Trestní řád*. 6. vydání. Praha: Nakladatelství C. H. Beck, 2008, s. 674.

[191] Usnesení Nejvyššího soudu ze dne 26. 6. 2013 sp. zn. 15 Tdo 510/2013

Zde judikatura dovodila pro oblast nařízení domovní prohlídky, týkající se počítačové kriminality odklon od jinak běžné praxe, neboť: *„Neodkladnost a neopakovatelnost úkonu, pokud nebyly podrobně odůvodněny v příkazu k domovní prohlídce podle § 83 TŘ, musí alespoň vyplývat z povahy trestní věci. Přitom v případech tzv. počítačové kriminality nemůže formální nedostatek odůvodnění neodkladnosti a neopakovatelnosti označeného úkonu bez dalšího znamenat nezákonnost domovní prohlídky a nepoužitelnost důkazů při ní opatřených. Zásah do softwarového či hardwarového vybavení počítače nebo úprava na něm uložených dat předtím, než by byl odborně zjištěn a zadokumentován jeho skutečný stav, by znamenal zmaření objasňování skutečností závažných pro trestní stíhání. Uvedené riziko pak dostatečně odůvodňuje kvalifikaci zmiňovaného úkonu jako neodkladného a neopakovatelného.*

Ani určitý časový odstup od vydání příkazu k domovní prohlídce do okamžiku jejího provedení nemůže zpochybnit závěr o neodkladnosti a neopakovatelnosti předmětného úkonu. Zde totiž vždy závisí na uplatněné taktice vedení přípravného řízení, jež je plně v kompetenci orgánů činných v přípravném řízení.“[192]

Ústavní soud tedy dovodil, že v případě týkající se kriminality páchané pomocí výpočetní techniky chybějící odůvodnění neodkladného nebo neopakovatelného úkonu v příkazu k domovní prohlídce a časový odstup k provedení tohoto úkonu nemá vliv na zákonnost prováděného úkonu, což je pro odhalování počítačové kriminality bezpochyby vítaným stavem. Dle názoru ÚS[193] je časová prodleva od nařízení domovní prohlídky a jejím faktickém provedení po dobu 2 měsíců v pořádku, a OČTŘ mají možnost úkon po tuto dobu odložit z taktických důvodů. I po 2 měsících od nařízení domovní prohlídky může být pro provádění zachován znak neodkladnosti a neopakovatelnosti takovéhoto úkonu.

4.7.2. Proporcionalita nástroje domovní prohlídky

Při zvažování využití institutu domovní prohlídky jsou orgány činné v trestním řízení povinny postupovat tak, aby do práva na soukromí osob nezasahovaly víc, než je nezbytně nutné. Proporcionalitu zásahu je třeba hodnotit s ohledem na okolnosti každého případu, přičemž hodnotící kritéria zahrnují např. povahu a závažnost trestného

[192] Viz rozhodnutí Nejvyššího soudu ze dne 15. 12. 2010 sp. zn. 5 Tdo 1312/2010, shodně i usnesení Ústavního soudu ze dne 9. 2. 2016 vedené pod sp. zn. I. ÚS 2816/15.
[193] Usnesení Ústavního soudu ze dne 9. 2. 2016 sp. zn. I. ÚS 2816/15 bod. č. 16

činu, v souvislosti s jehož objasňováním byla provedena prohlídka prostor a zajištěny věci, okolnosti, za nichž byl příkaz k prohlídce vydán, existenci důvodného podezření, že čin byl spáchán, dostupnost jiných důkazů či rozsah možných dopadů na pověst osoby dotčené příkazem k prohlídce.[194]

Dle ustanovení § 85 TŘ je nutné umožnit osobě, u níž se úkon domovní prohlídky koná její přítomnost při prohlídce. V úvodu domovní prohlídky je osoba poučena o svých právech. Dále je jí předán příkaz k provedení domovní prohlídky. Osobě je dále umožněno kontaktovat advokáta (resp. v návaznosti na konkrétní fázi trestního řízení obhájce). Osoba je vyzvána k vydání věcí, k jejichž zajištění domovní prohlídka směřuje.

Následně může dojít k systematickému prohledání nemovité věci, kdy je prohlídka prováděna místnost po místnosti. V každé místnosti, ve která je aktuálně vykonávána prohlídka je nezbytné zajistit účast nezúčastněné osoby. Tato osoba se na vyhledávání důkazů nepodílí. Její přítomnost má zajišťovat zákonnost domovní prohlídky, a to jako dohled nestranné osoby.

4.7.3. Protokol o provedení domovní prohlídky

O průběhu úkonu domovní prohlídky je obligatorně nezbytné vyhotovit protokol. Policejní orgán je často vybaven potřebnou technikou k sepsání a vytištění protokolu v místě konání domovní prohlídky.

Obligatorní údaj v protokolu o provedení domovní prohlídky je skutečnost o tom, zda byla dodržena ustanovení o předběžném výslechu a pokud se tak nestalo, uvedení důvodů, proč se předběžný výslech nekonal.[195] Do protokolu je nezbytné zaznamenat průběh úkonu, specifikovat místo konání úkonu a dostatečně identifikovat všechny přítomné osoby. Všechny přítomné osoby následně stvrzují správnost a pravdivost protokolu svým podpisem.

Dovozená soudní praxe formální nedostatky vyhotoveného protokolu nutně nespojuje jeho nedostatky s nepoužitelností takto získaných důkazních informací v trestním řízení, viz Nejvyšší soud: „*Trpí-li protokol o provedení domovní prohlídky některými formálními nedostatky, např. není-li zde dostatečně konkretizován důvod, proč nedošlo k předchozímu výslechu (§ 84, § 85 odst. 3 TŘ), neznamená to samo o*

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

[195] FRYŠTÁK, Marek a kol. *Trestní právo procesní.* Ostrava: Nakladatelství KEY Publishing, 2008. Str. 56.

sobě nezákonnost domovní prohlídky a nepoužitelnost důkazů při ní opatřených, jestliže je z jiných důkazů patrné, že domovní prohlídka proběhla v souladu se zákonem.“[196]

4.7.4. Prohlídka jiných prostor

Provedení prohlídky jiných prostor nebo pozemků je možné za podmínky důvodného podezření, že se v nich nachází věc nebo osoba důležitá pro trestí řízení. Prostorem nesloužícím k bydlení rozumíme zejména nebytové prostory, tedy takové prostory, které neslouží k bydlení. Těmito mohou být kanceláře, sídlo společností, či místnosti, v nichž jsou umístěny servery.

Příkaz k provedení prohlídky těchto prostor vydává předseda senátu a v přípravném řízení státní zástupce se souhlasem policejního orgánu. Bez příkazu k provedení prohlídky je může policejní orgán prohlídku vykonat pouze v případě, jestliže příkazu nebo souhlasu nelze předem dosáhnout a věc nesnese odkladu. Takový příkaz má charakter *sui generis*, a není proti němu přípustná stížnost. O provedení prohlídky musí být podobně jako u domovní prohlídky zajištěna účast dospělé osoby, a dále sepsán protokol.[197]

4.7.5. Prohlídka jiných prostor, ve kterých je vykonávána advokacie

Při provádění domovní prohlídky, či prohlídky jiných prostor, ve kterých je vykonávána advokacie a v jichž se nacházejí listiny, nebo data chráněné advokátním tajemstvím je nutné si vyžádat součinnost České advokátní komory.Za místo výkonu advokacie však nemusí být považována pouze oficiální kancelář, ale jakýkoli prostor, který souvisí s výkonem advokacie a v němž se proto vyskytují informace o klientech ať již v písemné, elektronické či jiné podobě.[198] Za místo podnikání advokáta ale nemůže být považován prostor, sloužící pouze k úschově datových serverů, na nichž jsou data chráněna advokátním tajemstvím uložena.[199]

S obsahem zajištěných listin se policejní orgán může seznámit pouze za přítomnosti a se souhlasem zástupce ČAK.[200] Odmítne-li zástupce souhlas udělit, musí

[196] Viz rozsudek Nejvyššího soudu ze dne 29. 3. 2000, sp. zn. 5 Tz 32/2000 In: Beck-online [právní informační systém] C.H. Beck [cit. 10.5.2018]

[197] FRYŠTÁK, Marek a kol. *Trestní právo procesní.* Ostrava: Nakladatelství KEY Publishing, 2008. Str. 57.

[198] K otázce výkladu pojmu „jiné prostory, v nichž advokát vykonává advokacii“ (§ 85b odst. 1 TŘ) a k otázce, zda o návrhu ve smyslu § 85b odst. 3 tr. ř. Bulletin advokacie. [online] publikováno 6. 10. 2015 [cit 1. 6. 2020] dostupné z: http://www.bulletin-advokacie.cz/k-otazce-vykladu-pojmu-jine

[199] SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015. 601 s.

[200] Viz ustanovení § 85b odst. 1 zákona č. 141/1963 Sb., trestní řád, ve znění pozdějších předpisů.

být listiny za účasti orgánů provádějící úkon zabezpečeny způsobem vylučující seznámení se s obsahem dokumentů. Zajištěné písemnosti či paměťové nosiče jsou PČR ukládány zejména do plastových pytlů a jsou opatřeny pečetí PČR s identifikačním číslem a podepsány zástupcem ČAK.[201] Všechny takto zajištěné listiny či jiné nosiče informací jsou následně předány do držení ČAK. Nevyslovení souhlasu ČAK lze nahradit rozhodnutím soudce či předsedy nejblíže soudu vyšší instance soudce, který vydal povolení k domovní prohlídce.[202] Návrh k nahrazení souhlasu zástupce ČAK vyplývá z ustanovení § 60 odst. 1 TŘ. Ve spojení s § 85b odst. 6 TŘ lze dovodit, že se jedná o propadnou lhůtu, ve které musí být podán bezvadný návrh.[203] Judikatura ÚS přinesla poměrně významnou změnu podmínek, za kterých se soud může s obsahem listin a digitálních dat seznámit.[204]

Doposud bylo běžnou praxí, že se soud s obsahem listin (poté co je obdržel od ČAK, která je měla zapečetěné v držení) seznamoval mimo veřejné jednání. Smyslem posouzení soudu je zjistit, zda se na dané listiny nebo digitální data vztahuje mlčenlivost advokáta. Stěžovatel se spolu s ČAK v řízení před ÚS domáhal změny postupu Krajského soudu v Praze, který faktické zkoumání listin prováděl mimo veřejné jednání. Za účelem seznámení se s listinami krajský soud dokonce i odročil jednání.

ÚS rozhodl o nepřípustnosti takovéhoto jednání. **Dle nálezu ze dne 22. 10. 2019 je nutné veškeré seznamování se zajištěnými důkazy provádět pouze při veřejném zasedání. Takto zajištěné údaje musí vždy mimo veřejné jednání zůstat zapečetěné.**[205] Zmiňme však, že se nejedná o veřejné jednání v pravém slova smyslu. Jednání jsou účastni i zástupci ČAK, a dále advokát,[206] kterému byla data zajištěna. Při jednání se však zpravidla s informacemi seznamuje jen soudce či znalec. Postrádalo by smysl, kdyby byla data, chráněná advokátním tajemstvím nahlas přečtena či poskytnuta policejnímu orgánu a státnímu zástupci, a následně by po vyhodnocení jejich obsahu dospěl k tomu, že se jedná o informace chráněné mlčenlivostí, a na seznámení s nimi OČTŘ nemají právo.

[201] Nález Ústavního soudu ze dne 22. 10. 2019 sp. zn. III. ÚS 702/17 bod č. 18

[202] SOKOL, Tomáš. Domovní prohlídka u advokátů. [online] *Právní rádce*, publikováno 15.1.2016. [cit. dne 4.4.2018] dostupné z: https://www.cak.cz/scripts/detail.php?id=15462

[203] viz nález Ústavního soudu ze dne 28.08.2009, sp. zn. II. ÚS 2894/08 In: Beck-online [právní informační systém] C.H. Beck [cit. 11.5.2018]

[204] Listinou se dle ustanovení § 85d odst. 12 TŘ Rozumí i jiný nosič informací. Není důvod se domnívat, že by tímto nosičem nemohl být pevný disk či jiné paměťové médium (CD nosič, flash disk, externí pevný disk atd.).

[205] Nález Ústavního soudu ze dne 22. 10. 2019 sp. zn. III. ÚS 702/17.

[206] Nález Ústavního soudu ze dne 11. 6. 2019 sp. zn. II. ÚS 3533/18.

Digitální data bývají zpravidla zpřístupňována osobou znalce. Soud vymezí klíčová slova, která znalec v zajištěném objemu dat vyhledává. Takto získané informace soud následně posoudí a rozhodne o jejich osudu. Tímto postupem dochází k selekci pouze některých listin (obsahující zájmová data pro které OČTŘ vedou řízení), a ostatní listiny chráněné advokátním tajemstvím (hledaná slova neobsahující), které se spáchaným TČ nesouvisejí zůstanou nedotčeny.[207] Tímto by mělo dojít k minimalizaci zásahu do státem zaručeného advokátního tajemství, ale zároveň k efektivnímu nalezení nutných listin v případě, že je tato situace nezbytná a oprávněná. Tento úkon je zpravidla provádět soudním znalcem.[208] **I tento postup znalce však ve světle uvedeného nálezu musí být prováděn při veřejném jednání.**

Lze předpokládat, že pravidla pro nakládání se zajištěnými informacemi se uplatní obdobně i v jiných případech zákonem uznané mlčenlivosti (např. ve věcech daňových, lékařských, zpovědních atd.).

4.7.6. Vytěžování důkazů z výpočetní techniky

Zajištění výpočetní techniky je vhodné provádět vyškoleným odborníkem, policejním technikem nebo soudním znalcem. Odborné zajištění je nezbytné z důvodu předcházení neodbornému zajištění dat, které často vede k znesnadnění dobytnosti hledaných dat ve výpočetní technice. Přítomná osoba s patřičnou odborností může vyhodnotit, zda je úložná kapacita zařízení šifrována. Při každém zajišťování elektronických zařízení hrozí, že vypnutí zařízení odstraní nechráněná (nešifrovaná) data v operační paměti. Při dalším zapnutí již zařízení bez znalosti potřebného klíče nebude možné vytěžit.[209]

Zajišťování výpočetní techniky má oproti zajišťování jiných důkazů značná specifika. Výpočetní technika může být nastavena způsobem, kdy jediný stisk klávesy způsobí kompletní likvidaci uložených dat. V případě propojených počítačových systémů nastává problém, protože osoby mohou manipulovat s daty i z vnějšího prostoru. Zajišťování takovýchto důkazů vyžaduje zvláštní přípravu. Je tedy nutné, aby orgán provádějící prohlídku zajistil všechny přítomné osoby a zabránil jim takto

[207] SOKOL, Tomáš. Domovní prohlídka u advokátů. [online] *Právní rádce*, publikováno 15.1.2016. [cit. dne 4.4.2018] dostupné z: https://www.cak.cz/scripts/detail.php?id=15462.

[208] Nález Ústavního soudu ze dne 20. 10. 2015 sp. zn. II. ÚS 3907/14 připouští možnost soudu využít znalce z oboru kybernetika a elektronika k analýze digitálních dat pomocí vyhledávání klíčových slov.

[209] KOTHÁNEK, Jakub. *Vytěžování důkazů z výpočetní techniky.* Brno, 2013/2014 Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA. Strana??

v přístupu k výpočetní technice.[210] Při zajišťování zařízení je nutné zohlednit, že do zajištěného zařízení lze zasahovat i po fyzickém odebrání zařízení. Moderní mobilní telefony či jiná uživatelská zařízení disponují funkcí, umožňující vzdáleným přístupem kompletní smazání dat v nich uložených. Protože příkaz ke smazání dat musí být doručen nejčastěji skrze internetové, nebo GSM připojení, je vhodné zařízení držet a uchovávat mimo bezdrátové připojení k síti Internet a zároveň mimo dosah GSM signálu.

V místě zajišťování výpočetní techniky lze provést tvorbu bitové kopie dat, obsažených na pevném disku, či jiném paměťovém úložišti zajišťovaného zařízení. Tento úkon může provést soudní znalec, či lze provést vyškoleným technikem PČR. PČR disponuje hardwarovým a softwarovým vybavením které jsou krom pořízení bitové kopie pevného disku a paměti RAM osobního počítače schopná pořídit kopii dat v tabletu či mobilním telefonu.[211] Pořizování kopií je vhodné provádět za použití hardwarového blokátoru,[212] který umožní pouze čtení dat a znemožní jakýkoliv zápis a tedy porušení integrity zkoumaného paměťového média.[213]

PČR disponuje analytickým zařízením FRED DX v technicky, výkonnostně a softwarově nejvyspělejší specifikaci, které je nyní dostupná na trhu. Toto zařízení v součinnosti s dodatečným softwarem (např. Virtual Forensic Suite) umožňuje obejít uživatelské heslo k přihlášení do systému Windows, analyzovat zjištěná data z pevného disku či RAM, provést analýzu cloudových účtu a úložišť, dále je zařízení například schopno automatizovaně identifikovat a označit konverzace lákání dítěte, sexuální konverzace nebo obrazové soubory obsahující drogy, zbraně nebo nahotu. Zařízení umožňuje dešifrování šifrovaných souborů (a to i celých disků – BitLocker či jednotlivých souborů – TrueCrypt).[214]

---

[210] KOTHÁNEK, Jakub. *Vytěžování důkazů z výpočetní techniky.* Brno, 2013/2014 Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA. Strana 33.

[211] Smlouva mezi Ministerstvem vnitra – Krajským ředitelstvím policie Libereckého kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 12. 9. 2019 č. j. KRPL-44479/2019. Registr smluv. [online] publikováno 12. 9. 2019 [cit. 6. 2. 2020] dostupné online z: https://smlouvy.gov.cz/smlouva/10135722

[212] Smlouva mezi Ministerstvem vnitra – Krajským ředitelstvím policie Jihomoravského kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 15. 4. 2019 č. j. KRPB-65709-3/ČJ-2019-0600VZ dostupné online z: https://smlouvy.gov.cz/smlouva/8814079

[213] VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů.* Zlín, 2013. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce David MANALÍK.
KOTHÁNEK, Jakub. *Vytěžování důkazů z výpočetní techniky.* Brno, 2013/2014 Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA. Strana

[214] Kupní smlouva mezi Českou republikou – Krajské ředitelství policie Libereckého kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 12. 9. 2019, č. j. KRPL-44479/2019. https://smlouvy.gov.cz/smlouva/10135722

Je vhodné, aby proceduře zajišťování paměťových médií či vytváření bitové kopie byla přítomna osoba, které zařízení náleží. Po dobu úkonu by se v místnosti, ve které k pořizování dat dochází měla nacházet nezúčastněná osoba. Po dokončení úkonu osoby podepisují protokol, obsahující kontrolní sumy zabezpečující integritu a neměnnost dat.[215]

Pokud pořízení bitových kopií zařízení není možné provést na místě, dojde k zajištění techniky a odeslání znalci k expertíze. V takovém případě je však nezbytné zajištěná zařízení řádně specifikovat do protokolu a uložit do zapečetěného obalu, který znemožňuje manipulaci s důkazem bez porušení pečetí.

Přístupu do cloudového systému je výše uvedené zařízení dle technické specifikace sice schopno, ale bez splnění podmínek § 158d, odst. 3 TŘ OČTŘ k přístupu do cloudových systémů nejsou oprávněny. Je tedy nutné posečkat na vydání souhlasu s provedením úkonu ze strany nezávislého soudu.

4.7.7. Analýza zajištěných dat

Vytěžování zajištěné techniky probíhá za pomoci forenzního softwaru. Tento software je schopen v zařízení vyhledat zájmové soubory. Je schopen vyhledat specifické soubory, obsahující vyhledávanou část textu, obnovit běžně uživatelsky smazané soubory či například vyhledat všechny soubory, obsahující audiovizuální soubory. Tím policejnímu orgánu odpadá nutnost procházet jednotlivé soubory po složkách adresářového systému. Data je nutné nejprve (i) vyextrahovat – z mobilního zařízení, pevného disku, flash disku a následně (ii) identifikovat. Následuje fáze interpretace (iii) získaných informací. Interpretaci získaných informací (např. o nelegálnosti obsahu) již nebude provádět policejní orgán, ale nezávislý soudní orgán.

4.7.8. Šifrování

Vytěžování zajištěné výpočetní techniky komplikuje, pokud uživatel zajištěného zařízení využil možnosti šifrování dat. Šifrování je způsob uchování dat, kdy jsou původně volně čitelná data převedena do podoby volně nečitelné a to tak, aby tento způsob znepřístupnění byl později návratný. Moderní šifrovací metody dělíme na symetrické a asymetrické.

[215] KOTHÁNEK, Jakub. *Vytěžování důkazů z výpočetní techniky.* Brno, 2013/2014 Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA. Strana??

Šifrovací metodu, která využívá pro kryptování a dekryptování stejný (symetrický) klíč nazýváme symetrickou šifrovací metodou. Mezi tyto šifry řadíme AES-256, Twofish či DES. Tato metoda tedy funguje způsobem, kdy pro přečtení znečitelněných (zašifrování) souborů je nutné znát jedinečnou kombinaci znaků (heslo), bez které rozšifrování není možné.[216] Asymetrickou šifrou nazýváme metodu, která k zašifrování dat využívá tzv. klíčový pár. Tento se skládá ze dvou klíčů: veřejného, a dále soukromého. Příkladem asymetrické šifrovací metody je RSA.[217]

Komprimace dat je možná po jednotlivých souborech, celých oddílech disku, včetně operačního systému či datového toku (interakce) mezi koncovým uživatelem a adresátem na druhé straně.

Šifrování individuálních souborů může být prováděno za pomocí programů TrueCrypt či WinRar. Jedná se z pohledu pachatele o poměrně rizikovou metodu, neboť na pevném disku daného zařízení mohou neplánovaně zůstat zbytky dat, či celé nezabezpečené kopie souborů. Tyto data mohou zůstat například v mezipaměti webového prohlížeče, v uživatelských aplikacích, zálohách (a to i na cloudových systémech nebo na paměťových nosičích) či jen jako zapomenutá kopie v jiné složce.

Pro osobní počítače se systémem Windows je ve verzi Windows Vista Ultimate a novějších verzích umožněno uživatelům využít aktivace nástroje BitLocker, který kompletně šifruje všechna data na pevném disku. BitLocker je nástroj pro šifrování disků, který je součástí operačního systému Windows.[218] Tento nástroj používá symetrický šifrovací algoritmus AES s délkou klíče 128 nebo 256 bitů. [219]

Nově distribuované zařízení společnosti Apple mají již v základním nastavení aktivovaný nástroj FileVault. Tento nástroj, obdobně jako nástroj BitLocker zajišťuje kompletní šifrování pevného disku, včetně operačního systému. K tomu využívá symetrické šifrování XTS-AES-128 s 256 bitovým klíčem.[220]

Ačkoliv mohou být data na pevných discích primárně šifrována, je vhodné provádět zajištění a provádět analýzu všech paměťových médií, nacházejících v místě

---

[216] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací.* Praha: Nakladatelství GRADA Publishing, 2017. S. 241.

[217] NEZMAR, Luděk. *GDPR: Praktický průvodce implementací.* Praha: Nakladatelství GRADA Publishing, 2017. S. 242.

[218] O'SHEA, Kevin. *Cyber Crime Investigation: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Rockland: Syngress publishing, 2007. S. 151.

[219] BitLocker [online] Microsoft., Publikováno 16. 10. 2017 [cit. 20. 6. 2018] dostupné z: https://docs.microsoft.com/cs-cz/windows/security/information-protection/bitlocker/bitlocker-overview

[220] Šifrování startovacího disku pomocí FileVaultu [online] Apple Inc., 3.1.2018 [cit. 20.6.2018], dostupné z: https://support.apple.com/cs-cz/ht204837

konání domovní prohlídky. Jak je uvedeno níže, policejní orgán disponuje softwarem, umožňujícím automatizované vyhledávání, a i dokonce detekování závadného obsahu. Je pravděpodobné, že se na paměťových médiích (CD a DVD nosiče, flash disky, externí pevné disky atd.) mohou nacházet nešifrované identické zálohy souborů, které jsou na pevném disku zašifrovány. Možnost zajištění těchto médií je přitom implikována v příkazu k provedení domovní prohlídky. Velmi významným zdrojem elektronických důkazů mohou být i mobilní telefony. Z těchto je možné vyextrahovat používaná hesla, soubory či přístupy ke cloudovým systémům (k přístupu na ně je již třeba požádat o souhlas soudu dle § 158d, odst. 3 TŘ). Významným zdrojem elektronických důkazů může být i již nepoužívá výpočetní technika, včetně nepoužívaných mobilních telefonů či v nich používaných paměťových karet.

4.7.9. Dopad šifrování na odhalování kybernetické kriminality

Šifrování tak představuje pro orgány činné v trestním řízení často poměrně zásadní překážku při využívání elektronických důkazů. Zajištěná data, která jsou zašifrovaná silným algoritmem, jsou při nedostupnosti dešifrovacího klíče prakticky nepoužitelná. Je-li algoritmus dešifrovatelný, mohou se orgány činné v trestním řízení pokusit o jejich dekrypci. V takovém případě jsou zpravidla využíványsložby znalce nebo je realizována kriminalistická expertiza. Pokud dekrypce bez klíče možná není, je nutné získat šifrovací klíč. Klíče však často lze získat i jinak, například mohou být uchovány v zajištěných zařízeních nebo na datových nosičích.[221]

Velmi často se dále stává, že k zajištění hesel dojde z důvodu, že si je pachatel uložil k automatickému vyplňování.[222] Tyto hesla jsou často nešifrována, a dají se vhodným forenzním nástrojem ze systému extrahovat. Takto však přirozeně za předpokladu, že není zašifrovaný celý pevný disk, který se nepodařilo zajistit v nezabezpečené fázi (tedy např. zapnutý, s aktivním systémem na RAM paměti, kde data nejsou chráněna). Je pravděpodobné, že pachatel používá identické heslo k více účelům. Extrahované heslo, uložené k předvyplnění pro přihlášení do e-mailové schránky například v mobilním telefonu může posloužit i k odemčení zašifrovaného pevného disku. V případě zajištění uživatelských hesel je jejich použití možné v případě, že dojde ke splnění podmínek nástrojů, které analýzu dat umožňují. Bude se

[221] STUPKA, Václav. *Elektronické důkazy v trestním řízení*. 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 100-101.

[222] Takto se stalo například ve věci, posuzované Krajským soudem v Plzni dne 30. 3. 2017 v rozsudku sp. zn. 34 T 13/2016.

jednat především o splnění podmínek § 83 TŘ (zejména analýza obsahu paměťových nosičů a obsahu zařízení, zajištěných zejména při domovní prohlídce) dále § 158d odst. 3 TŘ (zejména přístup ke službám e-mail a cloud) a § 88 odst. 1 TŘ (služby, umožňující sledování komunikace v reálném čase). **Dle názoru autora jsou tedy zjištěná hesla podezřelé osoby použitelná v případě, že jsou ze strany nezávislého soudu splněny podmínky pro zásah do ústavně zaručených práv (např. §§ 83, 158d odst. 3 a 88 odst. 1 TŘ). Zjištěné heslo podezřelé osoby může být vyzkoušeno, resp. zadáno, pokud existuje povolení k zásahu, které dané heslo chrání. Tyto hesla jsou využitelná taktéž k dešifrování zašifrovaných dat.**

PČR má k dispozici hardwarové a softwarové zařízení, kterým se může pokusit prolomit šifrování digitálních dat. Disponuje minimálně kombinací 2 výkonných zařízení Tableau Password Recovery, které umožňují prolamovat zabezpečení šifrování běžně užívaných typů šifrovaných souborů.[223]

Autor práce dotázal PČR, zda za využití zařízení Tableau Password Recovery došlo úspěšnému rozšifrování dat, uložených na zajištěných pevných discích či na paměťových nosičích. **PČR v režimu zákona o svobodném přístupu k informacím sdělila, že se pokusila rozšifrovat zajištěná data v celkem 130 případech. Žádný z pokusů o rozšifrování zajištěných digitálních dat doposud nebyl úspěšný.**[224]

Kladně lze hodnotit aktivitu PČR směřující k udržení se na technologické špičce co do dispozice s nejvyspělejší technikou pro prolamování šifrovacích algoritmů a analýzu zajištěných digitálních důkazů. Je však otázkou, proč ani při dispozici nejvyspělejších zařízení doposud nedošlo k úspěšnému rozšifrování zajištěných dat. Úspěšnost prolomení šifry bude záležet zejména na typu zvoleného šifrovacího algoritmu a na složitosti zvoleného hesla. V případě užití bezpečného hesla, které může definovat vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, je prolomení šifry za využití pouhých dvou dešifrovacích zařízení dané kapacity do doby, než dojde k promlčení TČ velmi nepravděpodobné. **V případě bezpečně zvoleného hesla a jeho neposkytnutí pachatelem či jeho jiného nezjištění je tedy rozšifrování dat, jinak sloužící jako důkaz pro účely trestního řízení spíše nepravděpodobné.**

[223] Smlouva mezi Česká republika – Ministerstvo vnitra a společností Risk Analysis Consultants, s.r.o. ze dne 3. 11. 2017, č. smlouvy objednatele PPR-14605-86/ČJ-2017-990656, jejímž předmětem je nákup uvedeného HW a SW, dostupné online z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjG_c_8wrvnAhXOPFAKHbreCIcQFjAAegQIAxAB&url=https%3A%2F%2Fsmlouvy.gov.cz%2Fsmlouva%2Fsoubor%2F5103736%2FForenznihwaswcastH.pdf&usg=AOvVaw0YR1b_Q-yxFUsSmv7aq88j

[224] Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 6. 11. 2019 pod č. j. PPR-33938-8/ČJ-2019-990810

4.7.10. Povinnost dešifrovat digitální data

Vzhledem k faktické technické nemožnosti rozšifrování dat se nabízí otázka, jakým způsobem mohou OČTŘ získat součinnost podezřelé osoby k dešifrování zařízení.

V úvahu nepřichází ustanovení § 66 TŘ, jinak sloužící k součinnosti s OČTŘ formou ukládání pořádkových pokut. Jak poukazují shodně Smejkal[225] a Dostál,[226] vymáhat aktivní spolupráci podezřelé osoby k vydání hesla či dešifrovacího klíče formou ukládání pořádkových pokut nepřichází v úvahu. Takový postup by byl v rozporu se zákazem donucování k poskytnutí důkazů proti sobě samému. Tento zákaz plyne především z čl. 37 odst. 1 a čl. 40 odst. 4 LZPS.

Pořádkovou pokutu po podezřelém je dle názoru Dostála možné ukládat pouze v případě fyzického nevydání věci dle § 79 TŘ. Odebrání věci je dle jeho názoru ze strany podezřelého pouze snášen. S tímto však autor práce nesouhlasí, a poukazuje na ustálenou judikaturu ÚS,[227] ze které dle názoru autora plyne, že vydání věci je považováno za aktivní jednání a jako takové je nepřípustné.

ÚS vnímá donucování podezřelého prostřednictvím ukládání pořádkové pokuty k opatřování, resp. svou součinností k umožňování opatření důkazů proti jemu samotnému za nepřípustné.[228] V současné době tedy panuje situace, kdy dle výše uvedených nálezů[229] je nepřípustné přinucení podezřelé osoby k součinnosti uložením pořádkové pokuty.

Jaká však bude situace, když nebude třeba donutit podezřelého k omisivní, ale komisivní spolupráci? Bude se jednat o nepřijatelné vyžadování součinnost ve světle výše uvedeného nálezu ÚS? Jak se domnívá Musil,[230] aktivní jednání podezřelé osoby spočívá zejména ve vyžadování výpovědi podezřelého, ale též lze za aktivní jednání považovat např. napsání vzorku textu ke znaleckému zkoumání, chůze a jiné motorické zkoušky atd.

---

[225] SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015, s. 599.

[226] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl*). Trestněprávní revue*. 2019, č. 3, s. 66.

[227] Např. nález Ústavního soudu ze dne 28. 1. 2003, vedený pod sp. zn. II. ÚS 118/01, nebo nález Ústavního soudu ze dne 12. 1. 2006 vedený pod sp. zn. II. ÚS 552/05, dále nález Ústavního soudu ze dne 10. 3. 2005, vydaný pod sp. zn. III.ÚS 561/04, nebo Nález Ústavního soudu, ze dne 23. 6. 2005 vydaný pod sp. zn. II. ÚS 255/05.

[228] Rozhodnutí Ústavního soudu ze dne 22. 6. 2006 sp. zn. I. ÚS 671/05

[229] MUSIL, Jan. Zákaz donucování k sebeobviňování (nemotenetur se ipsumaccusare). *In: Ministerstvo vnitra.* [online]. Publikováno 2009. [cit. 12. 11. 2019] dostupné z: https://www.mvcr.cz/clanek/4-2009-zakaz-donucovani-k-sebeobvinovani-nemo-tenetur-se-ipsum-accusare.aspx

[230] Nález Ústavního soudu ze dne 23. 5. 2007, sp. zn. III. ÚS 655/06

Prolomení zabezpečením šifrováním některých zařízení však bude možné i na základě nikoliv nutně aktivního jednání podezřelé osoby (vydání hesla), ale např. i přiložením otisku prstu k biometrickému senzoru zařízení.

4.7.11. Využití biometrických údajů podezřelé osoby k dešifrování zařízení

Mnoho zařízení je možné zpřístupnit za využití biometrických údajů, zejména otisku prstu či jedinečných rysů obličeje.[231] Dle názoru autora by povinnost odemknout zařízení přiložením prstu či nasnímáním jedinečných rysů obličeje z níže uvedených důvodů nebyla povahy aktivního, ale pasivního jednání podezřelé osoby.

Možnost překonání odporu pro komisivní složku jednání podezřelého plyne přímo ze zákona (tedy pouze složky jednání neaktivního, jako je např. strpění odběru krevních vzorků, biologického materiálu, odnětí věci nebo dle názoru autora právě snímek otisku prstů nebo snímek obličeje). Tímto se úkon přiložení otisku prstu rovná podobnému úkonu, jako když OČTŘ najdou spolu s trezorem i klíč. Jejich oprávnění k odemčení trezoru, a analýze v něm drženém obsahu zákon implikuje – onen trezor představuje úložiště zařízení. Mechanismus zámku představuje šifrovací mechanismus a za klíč považujme uživatelské heslo (nebo dnes stále častěji biometrické údaje[232]). Autor je názoru, že právní řád tedy v současné době nedisponuje ustanovením, které by podezřelou osobu nutilo k omisivní součinnosti pro sdělení kombinace či hodnoty přístupového hesla. Ačkoliv absentuje relevantní zákonná úprava či přiléhavá soudní praxe, která by odpověděla na otázku, zda je relevantní donucovat podezřelého k poskytnutím otisku prstu či k nasnímání obličeje, může být aplikovatelná legislativa a soudní praxe ve věcech poskytnutí pachové stopy nebo poskytnutí vzorku DNA.

[231] Paměť uživatelského zařízení může být šifrována. Na místo vložení dešifrovacího hesla je však možné přiložit otisk prstu. Zařízení se následně automaticky dešifruje. Referenčně se bude jednat technické řešení TouchID či FaceID společnosti Apple Inc.

[232] Jedná se o jedinečný otisk prstu, snímek obličeje ale může se jednat i o hlasovou identifikaci atd.

Trestní řád v ustanovení § 114 stanovuje, že odběr biologického materiálu, který není spojen se zásahem do tělesné integrity, jíž se úkon týká může provést lékař, nebo s jeho souhlasem OČTŘ. Nelze-li úkon odběru provést, je OČTŘ oprávněn po předchozí marné výzvě odpor překonat a odběr provést. Je-li za biologický vzorek považována DNA, můžeme za něj považovat bezpochyby i jedinečný otisk prstů. Jeho snímání na uživatelském zařízení podezřelého k zásahu do integrity osoby nedojde. Tím spíše nedojde do integrity podezřelého tím, že se nasnímá jeho obličej. Snímání obličeje za účelem odemčení uživatelského zařízení je srovnatelné s pořízením fotografie obličeje podezřelého. Ostatně jedná se o obdobnou situaci, jakou se na podezřelém vynucuje otisk prstu ke komparaci se stopou na místě činu.

Výše uvedené autora vedou k závěru, že OČTŘ jsou po předchozí marné výzvě oprávněny donutit podezřelého k přiložení otisku prstu k odemčení uživatelského zařízení, či jeho zařízení použít pro nasnímání obličeje, a to i v případě, kdy podezřelý klade odpor.

Nabízí se i úvaha nad tím, zda by OČTŘ mohly využít biometrické údaje, které jiný státní orgán o podezřelém již uchovává – například otisky prstů z cestovního pasu, obsahujícího biometrické údaje.

Zákon č. 329/1999 Sb., o cestovních dokladech (tento zákon o ve znění pozdějších předpisů dále jen jako „ZOCD“) ostatně obsahuje zmocnění OČTŘ za účelem předcházení, vyšetřování a objasňování trestné činnosti k přístupu k údajům, evidovaným dle tohoto zákona a to dokonce ve formě přímého přístupu.[233] Zákon však výslovně uvádí, že biometrické údaje se tímto způsobem nezpřístupňují.[234] Takto je tomu nejspíše z důvodu, že dle ustanovení § 29 odst. 4 a § 29a odst. 4 ZOCD stanovuje, že biometrické údaje se uchovávají maximálně do doby 60 dnů od vydání cestovního dokladu. Autor dovozuje, že údaje jsou následně vedeny pouze na paměťovém nosiči cestovního dokladu.

Z toho tedy plyne, že pokud chtějí OČTŘ získat biometrické údaje, například za účelem odemčení uživatelského zařízení, krom jejich získání od samotné podezřelé osoby je jejich načtení možné z cestovního dokladu, se strojově čitelnými údaji.

[233] Dle ustanovení § 30b odst. 1, písm. d) zákona č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů.
[234] Dle ustanovení § 30 odst. 10 zákona č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů.

Pokud by technicky bylo možné otisky prstů z paměťového nosiče, obsaženého v cestovním dokladu převést do podoby, umožňující odemknout zařízení, není důvod se domnívat, že by toto nešlo provést. TŘ ostatně nabízí možnost překonat odpor, využít méně invazivní metody – využití již získaných biometrických údajů (nebo je považujme za biologické) je dle názoru autora možné. Případné zpochybnění jejich autenticity či nehodnověrnost takového úkonu není na místě, neboť sledovaným cílem je odemčení uživatelského zařízení.

Využití biometrických údajů v evidenci jiných orgánu k prolomení zabezpečení zařízení je tedy dle názoru autora legálně možné, avšak hůře technicky proveditelné. I pokud dojde ke zjištění otisku prstů podezřelé osoby, k odemčení zařízení bude třeba tento vzorek otisků předat snímacímu zařízení (čtečka otisků prstů).

4.7.12. Závěrem k zajišťování zařízení a vytěžování dat

Stávající právní úprava je OČTŘ nápomocna v tom, že umožňuje na základě zajištěných stop, povahy provozních a lokalizačních údajů umožnit posun ve vyšetřování spáchaného skutku. Zajištění digitálních stop umožní za splnění dalších podmínek (zejména domovní prohlídka, prohlídka nebytových prostor či vydání věci) provedení fyzického zajištění zařízení a extrakci dat, v nich obsažených. Fyzicky budou uživatelská zařízení zajišťována nejčastěji při domovní prohlídce. Na její nařízení a provedení klade právní řád, jakož i soudní praxe náročné podmínky. Pokud mají OČTŘ možnost, je vhodnější provést spíše prohlídku jiných nebytových prostor. Zásah do nebytových prostor nepředstavuje potenciální porušení práva na nedotknutelnost obydlí, vyjádřenou v čl. 8 EÚLP a dále čl. 12 LZPS.

Při provádění domovní prohlídky je důležité si uvědomit, že zajištěné uživatelských zařízení[235] všech členů domácnosti, či osob žijící ve společném obydlí (pokud nejde jinak, zejména proto, že OČTŘ zkrátka neví, kdo je podezřelou osobou) může životy nevinných osob zásadně ovlivnit. Autor byl svědkem událostí, kdy byla zajištěna výpočetní techniky nezbytná pro výkon povolání osob, které se později vyhodnotily jako osoby nevinné. Zjištění jak výpočetní techniky, tak záloh profesních dat tyto osoby značně profesně poznamenalo. Při zajišťování důkazů je tedy vhodné preferovat zajišťování bitových kopií dat, na místo zajišťování celých zařízení. Z důvodu šetření práv osob, do jejichž práv OČTŘ odebráním techniky zasahují je

[235] Jakož i jiných paměťových nosičů, serverů atd.

bezpochyby přijatelnější, pokud dojde pouze k pořízení bitové kopie, a daná zařízení zůstanou fyzicky nadále v dispozici uživatele.

Policejní orgán na místě nemůže vyhodnotit, která osoba skrze domácí síť spáchala TČ. Při postupu dle § 88a odst. 1 TŘ dojde k zajištění IP adresy přístupového bodu do sítě Internet. Jak již bylo uvedeno výše, pokud se jedná o pevné připojení, které využívá více osob, vzhledem k principu skrytí jednotlivých uživatelů za NATem lze jen velice těžce bez odebrání a analýzy obsahu pevných disků dovodit, které osoba se jednání dopustila. Je však vhodní zajišťovat i síťové prvky, neboť mohou nabídnout cenné informace o provozu za NATem.

Soudní praxe dále zaznamenala případ, kdy účelově podaným trestním oznámením, kterým se oznamovatel vydával za osobu podobnou kolektivnímu správci došlo k z důvodu údajného ilegálního šíření autorských děl neoprávněným sdílením k provedení domovní prohlídky u osoby, která s daným jednáním neměla nic společného. V trestním oznámení došlo ke zfalšování technických informací nasvědčující tomu, že daný čin spáchala konkrétní osoba. Po následném „rozuzlení" celého případu došlo ke zjištění závěru, že skutečný oznamovatel se za osobu kolektivní správce pouze vydával, a e-mail s trestním oznámením zaslal takovým způsobem, aby byl způsobilý OČTŘ uvést v omyl vydáváním se za konkrétní osobou kolektivního správce. Ve skutečnosti se osobu falešného trestního oznámení nepodařilo ustanovit, neboť toto jednání učinila prostřednictvím anonymizačního nástroje Tor. ÚS po podané ústavní stížnosti vydané příkazy k provedení domovních prohlídek zrušil a konstatoval, mimo jiné že ze strany OČTŘ došlo k porušení práva na nedotknutelnost obydlí, vyjádřenou v čl. 12 LZPS.[236] ÚS upozorňuje, že z takové situace plyne, že je nutné věnovat patřičnou pozornost povinnosti *„učinit veškerá potřebná šetření a opatření k odhalení skutečností nasvědčujících tomu, že byl spáchán trestný čin, a směřujících ke zjištění jeho pachatele"* kterou ukládá ustanovení § 158d TŘ. **Poměrně snadnou možnost podvrhnutí či pozměnění elektronických důkazů je tedy nutné mít vždy na zřeteli. Toto je nutné brát v úvahu nejen během meritorního rozhodování o daném skutku a jeho pachateli, ale i při rozhodování o povolování, resp. nařizování invazivních úkonů, vedoucích k zajištění dalších skutečností či důkazů.**

Pro efektivní odhalování kybernetické kriminality se jako zásadní hrozba jeví šifrování dat uložených v zařízení. V případě, že je zařízení šifrováno, a pachatel odmítá sdělit přístupové heslo, a OČTŘ se nepodaří heslo získat, se mohou pokusit o prolomení

[236] Viz Nález Ústavního soudu ze dne 7. 6. 2016, sp. zn. III. ÚS 905/13

ochrany šifrování. Policejní orgán přitom disponuje výkonným hardwarovým a softwarovým zařízením. Jak plyne z poskytnuté statistiky, **při překonávání překážky snahou PČR o rozšifrování zabezpečených dat bohužel nedošlo k jedinému úspěšnému průlomu šifrovaných zajištěných dat.**[237]

Masivní využívání (z důvodu tovární aktivace) šifrovacího nástroje FileVault v moderních produktech společnosti Apple je při objasňování kriminality skutečným problémem. Nástroj BitLocker v zařízeních využívající operační systém Windows naštěstí není ani v nejnovějších zařízeních v současné době ve standardním zařízení (v továrním nastavení) aktivován. Pokud tedy uživatel sám nástroj neaktivoval, je vytěžení zařízení i bez znalosti hesla stále pravděpodobné.

Jednou z mála možností, jak zabezpečení překonat je buď extrakce hesla ze zajištěných dat, kdy existuje šance, že podezřelý používá identické heslo, nebo fyzické přinucení podezřelého k odemčení zařízení přiložením otisku prstu nebo nasnímáním obličeje. **Obě tyto metody jsou dle názoru (po splnění dalších podmínek) autora pro prolomení šifrování možné.**

Problematický je i nástup šifrování mobilních telefonů. Mobilní telefony vyšší třídy již taktéž umožňují vysoce kvalitní standard šifrovací ochrany. Jak však ukazuje případ odhalení provozování drogového tržiště Sheep Marketplace,[238] vytěžení dat i

[237] Autor však dotazoval pouze poslední nabyté zařízení – Tableau Password Recovery. Není vyloučeno, že v minulosti došlo k úspěšným pokusům o prolomení ochrany šifrováním. Dle sdělení PČR toto zařízení není jediným používaným. Viz. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 6. 1. 2020 pod č. j. Č. j. UZC-476-1/ČJ-2020-2800KR.

[238] Krajský soud v Brně v rozhodnutí 50 T 4/2017 pravomocně odsoudil pachatele podle § 283 odst. 3 TZ za použití § 43 odst. 1 TZ k úhrnnému trestu odnětí svobody v trvání 9 let ve věznici se zvýšenou ostrahou, když spáchal zvlášť závažný zločin nedovolené výroby a jiného nakládání s omamnými a psychotropními látkami a jedy dle § 283 odst. 1, odst. 3 písm. b) TZ, dále zvlášť závažný zločin krádeže dle § 205 odst. 1, odst. 5 písm. a) TZ a přečin nedovoleného ozbrojování dle § 279 odst. 1 TZ. Pachatel vytvořil a provozoval v anonymní síti Tor webový portálSheep Marketplace, který umožňoval nelegální transakce prodeje a nákupu psychotropních a omamných látek. Tržiště fungovalo na principu webového portálu typu Aukro, tedy umožnilo jednotlivým prodejcům inzerci a distribuci zboží. Uživatelům bylo umožněno, mimojiné, anonymní zakoupení a prodej omamných látek. Platba probíhala v měně Bitcoin a byla mezi prodejcem a kupujícím realizována skrze uživatelský portál. Kupující následně obdržel zakoupené zboží nejčastěji poštou. Pachatel TČ kořistil z tohoto jednání ziskem ve formě provize z každé realizované transakce. OČVTŘ k identifikaci pachatele navedlo několik podnětů. Jedním z nich byla výpověď svědka K. B., který na základě vlastního pátrání v rámci diskuzních fór dospěl laicky k závěru, že s tržištěm souvisí právě podezřelý, neboť tento řešil pod přezdívkou v diskuzních fórech řadu technických problémů, které nasvědčují tomu, žeprávě on provozuje v síti Darknet výše uvedený závadný portál. Z diskuzí vyplývalo, že pachatel řešil problémy se serverem, který nestačil kapacitně, a tak hledal nový server. K ustanovení dále přispělo trestní oznámení, podané Finančně analytickým útvarem Ministerstva financí, které oznámilo a následně řešilo podezřelé přesuny a finanční transakce na účtech manželky pachatele. Krom výše uvedeného tržiště v anonymní síti TOR pachatel paralelně provozoval druhou (neanonymizovanou) webovou stránku v neskryté části sítě Internet. Tato webová stránka byla propagační stránkou, a obsahovala odkaz na výše uvedené tržiště. Dožádáním dle § 8 TrŘ byla u hostingové společnosti zajištěna IP adresa osoby, která registrovala a spravovala doménu v neskryté části síti Internet. Ztotožněním dle § 88a došlo k identifikaci přístupového bodu do sítě Internet v domácnosti

z těchto mobilních zařízení může vzhledem k jejich dnešnímu všestrannému a každodennímu využití přinést nesmírně cenné informace či důkazy pro trestní řízení.

Je tedy otázkou, zda pro účely vyšetřování nejzávaznější kriminality nezavést institut, ukládající výrobci zařízení zpřístupnění dat. V současné době však vše nasvědčuje tomu, že ani samotný výrobce není schopen svá zařízení při využití šifrování odemknout, neboť toho technicky vzhledem k použitým šifrám není schopen.

pachatele. Při domovní prohlídce byla zajištěna výpočetní technika serverů. Dále byl zajištěn, mimo jiné, mobilní telefon HTC. Soud zadal vypracování znaleckého posudku v oboru kybernetika a výpočetní technika. Analytický software v zajištěných datech zajistil globální nastavení a část zdrojového kódu darknetového tržiště v síti Tor. Znalec potvrdil, že paměť mobilního telefonu obsahuje soubor dat, které tvoří živou zálohu výše uvedeného tržiště. Znalec dále potvrdil indicie podatelem trestního oznámení, neboť potvrdil, že některé popisované skutečnosti pisatelem příspěvků odrážejí zjištěnou realitu zejména v hardwarovém vybavení, na kterém provozoval server v síti Tor, ale i jiné skutečnosti, které byly v diskusi zmíněny. Velmi důležitou roli v dokazování dále sehrálo trasování a identifikace plateb za transakce v Darknetovém tržišti. Tržiště se před ustanovením pachatele stalo obětí celkem dvou krádeží měny Bitcoin. První krádeží bylo třetí osobou odcizeno celkem 5.310 Bitcoinů. Následně bylo pachatelem vyvedeno zbývajících 840,7 bitcoinů. Z toho 454 bitcoinů bylo převedeno přes tzv. transportní adresu do směnárny Bitstamp, a následně na účet manželky obžalovaného. K dosledování transakcí byl využit nástroj walletexplorer.com. Jeden ze soudních znalců osvětlil, z jakých důvodů v tomto konkrétním případě nemohlo dojít k chybě (vyloučil záměrné míchaní adres s jinými adresami) a osvětlil, jakým způsobem dospěl k závěru, že konkrétní bitcoinová transakce byla připsána ve svémdůsledku do konkrétní bitcoinové peněženky. Zajištěná data tržiště na mobilním telefonu spolu s dosledováním finančního toku z výše uvedeného tržiště na účet manželky pachatele vedlo soud k uznání pachatele vinným. - Rozhodnutí Krajského soudu v Brně ze dne 5. 10. 2017 sp. zn. 50 T 4/2017 bylo poskytnuto na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Krajský soud v Brně rozsudek poskytl v anonymizované podobě dne 8. 3. 2018 pod č.j. Si 136/2018.

4.7.13. Návrh *de lege ferenda*

Pro zajištění integrity zajištěných dat, znemožňující manipulaci s nimi je vhodné zavést zákonnou povinnost užívat při zajišťování či digitálních dat, při jejich vytěžování z fyzicky zajištěných zařízení hardwarový blokátor změny dat. Při zajišťování dat je vhodné zavést povinnost provádět kontrolní součet dat. Tento údaj by měl být *ex lege* uváděn do protokolů o zajištění zařízení či bitových kopií dat.

Ustanovení § 114 TŘ je vhodné doplnit o výslovné ustanovení nového odstavce: *„Orgány činné v trestním řízení jsou oprávněny za účelem zákonně zajištěné výpočetní techniky použít biometrické údaje obviněné osoby. Po marném upozornění s poučením následků neuposlechnutí jsou oprávněny překonat odpor. Překonání odporu obviněné osoby nesmí být nepřiměřené povaze kladení odporu.“* Bude vhodné tento úkon omezit na osobu v procesním postavení obviněné osoby, tj. na fázi řízení po sdělení obvinění. Tato alespoň bude moci využít práva na obhajobu a mít možnost zajistit si přítomnost obhájce. Podmínka zákonného zajištění výpočetní techniky poskytne ochranu před extenzivním výkladem ustanovení, kdy by docházelo k pokusům o prolomení zabezpečení a extrakci dat ze zařízení, kdy zákon neumožňuje jejich vytěžení.

Spíše k podnětem k zamyšlení je výše uvedená úvaha nad zavedením povinnosti výrobců zařízení k poskytování součinnosti při dešifrování zařízení.

5. TRESTNÍ ŘÍZENÍ

K identifikaci pachatele trestného činu na základě zajištěných stop a důkazů dochází zpravidla v přípravné fázi trestního řízení. Takto tomu není jinak ani u kybernetické kriminality.[239] Trestní řízení (jakož i fáze, která je před samotným zahájením trestního stíhání) je proces, jehož pravidla jsou striktně upravena zákonem.

Trestní řízení je komplexem stanovených postupů OČTŘ a dalších subjektů podílejících se na tomto postupu, jehož cílem a výsledkem je zjištění trestného činu a jeho pachatele, vynesení spravedlivého rozhodnutí trestu či jinému opatření, a to včetně případného nároku poškozeného na náhradu škody či jiné nemajetkové újmy.

V této kapitole dojde zejména ke stručnému vymezení podstatných fází trestního řízení do okamžiku, kdy dojde k zajištění dostatečného množství informací, dat či důkazů, které poskytnou dostatečné informace o spáchání skutku konkrétní fyzickou osobou[240] – pachatele. Tento okamžik můžeme považovat za skončení fáze vyšetřování, po které následuje podání obžaloby.

[239] Pojmem identifikace pachatele rozumějme ustanovení osoby, u které se má za to, že je z přesvědčivých důvodů skutečným pachatelem TČ.
[240] Uvažme jen odpovědnost fyzické, a nikoliv právnické osoby.

5.1. Trestní oznámení

OČTŘ se o protiprávním jednání dozvědí nejčastěji na podnět ve formě trestního oznámení. Podnět k zahájení trestního řízení může být jednak aktem jednotlivce, který se ve formě oznámení o okolnostech nasvědčující tomu, že byl spáchán trestný čin (trestní oznámení) domáhá prověření věci. Orgány činné v trestním řízení však také z úřední povinnosti prověřují skutečnosti, o nichž mohou mít za to, že by mohly být trestným činem.[241]

Trestní oznámení je možno učinit jak osobně, tedy ústně do protokolu, tak písemně. Oznámeno může být u libovolného policejního orgánu nebo státního zastupitelství. Na tento úkon nejsou zákonem kladeny žádné předepsané náležitosti. Je však vhodné uvést údaj o tom, kdo podání činí, komu je adresováno a čeho se týká. Je dále vhodné vylíčit skutkové okolnosti, a uvést, jaký trestný čin oznamovatel v popsaném jednání spatřuje.

Dle ustanovení § 158 odst. 1 TŘ je policejní orgán povinen na základě vlastních poznatků, trestních oznámení i podnětů jiných osob a orgánů, na jejichž podkladě lze učinit závěr o podezření ze spáchání trestného činu, učinit všechna potřebná šetření a opatření k odhalení skutečností nasvědčujících tomu, že byl spáchán trestný čin, a směřující ke zjištění jeho pachatele. Dále je povinen činit též nezbytná opatření k předcházení trestné činnosti.

Přitom je povinen oznamovatele poučit o odpovědnosti za vědomě nepravdivé údaje, a pokud o to oznamovatel požádá, do jednoho měsíce od oznámení jej vyrozumět o učiněných opatřeních.

5.2. Hlášení kybernetické kriminality

PČR od roku 2012 provozovala na svých webových stránkách online formulář pro hlášení závadného obsahu či chování na internetu, které má charakter kybernetické kriminality. Tento formulář byl označován jako „policejní internetový HOTLINE“. Provozováním formuláře PČR usilovala o snadné o jednoduché hlášení kybernetické kriminality. Po vyplnění a odeslání formuláře byl podnět předán odboru Informační kriminality Služby kriminální policie a vyšetřování Policejního prezidenta ČR, který podaný podnět bez zbytečného začal prověřovat.[242]

[241] CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008, s. 419.

[242] *Hlášení kyberkriminality* [online]. Policie České republiky. publikováno 1. 8. 2012 [cit. dne 15.5.2018] dostupné z: http://www.policie.cz/clanek/hlaseni-kyberkriminality.aspx

Vyhodnocení efektivity tohoto nástroje experty z Ministerstva vnitra a PČR vedlo k rozhodnutí provoz nástroje ukončit. Provoz formuláře byl ukončen k 24. 5. 2018. Formulář má být nahrazen sofistikovanějším nástrojem. Vyvíjená náhrada má být schopna přijmout oznámení ve formě elektronického trestního oznámení. Nástroj má být funkčně propojen s provozem Portálu občana,[243] který je online platformou pro kontakt s úřady.

Uzavření výše uvedeného nástroje k hlášení kybernetické kriminality je dle názoru autora bezpochyby výrazným krokem zpět. Nutnost podání trestního oznámení klasickou cestou může mít za následek zbytečný prostoj, během kterého mohlo dojít k zajištění digitálních stop vedoucích k ustanovení pachatele.

[243] Ukončení provozu Hotline. *Policie České republiky* [online]. Publikováno 24. 5. 2018 [cit. dne 20.6.2018] dostupné z: http://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx

5.3. Přípravné řízení

Přípravné řízení je prvotním stádiem trestního řízení. Jeho cílem je prověřit zjištěné skutečnosti, nasvědčující tomu, zda se skutečně stal trestný čin. Dále si bere za cíl opatření dostatku podkladů k podání obžaloby, či k jinému rozhodnutí státního zástupce v této věci. Jeho charakter je neveřejný a převážně písemný. Jeho cílem je dále zajištění některých úkonů tak, aby došlo k usnadnění hlavního líčení. Přípravné řízení však také slouží jako první síto k tomu, aby nedošlo k nedůvodnému postavení obviněného před soud.[244]

Jedná se o proces, ve kterém dochází k zajišťování stop a důkazů, a jejich prvotnímu hodnocení. Zároveň však účelem této procesní fáze není nahrazení činnosti soudu. Mělo by dojít pouze k provedení takových důkazů, které je potřeba zajistit pro účely přípravného řízení, dále nutných k podání obžaloby. Je dále nutné zajistit takové důkazy, jejichž provedení by v pozdějším mohlo vést k jejich znehodnocení nebo nemožnosti pozdějšího provedení.

Prvotní šetření a opatření k odhalení skutečností nasvědčujících tomu, že byl spáchán trestný čin, však provádí policejní orgán nikoli podle TŘ, ale v naprosto převažující míře podle Zákona o PČR, ve znění pozdějších předpisů, neboť úprava postupu před zahájením trestního stíhání (prověřování skutečností nasvědčujících spáchání trestného činu) vychází z toho, že momentem oddělujícím od sebe šetření podle zákona o Policii ČR (popř. podle ustanovení jiných zákonů) a podle TŘ je sepsání záznamu o zahájení úkonů trestního řízení.[245]

Policejní orgán je povinen neprodleně sepsat záznam o tom, že zahájil úkony k objasnění a prověření skutečností důvodně nasvědčující tomu, že byl spáchán trestný čin. V tomto záznamu uvede skutkové okolnosti, pro které řízení zahajuje a způsob, jakým se o nich dozvěděl. Opis tohoto záznamu zašle do 48 hodin státnímu zástupci. Následně policejní orgán k objasnění a prověření skutečností, důvodně nasvědčujících tomu, že byl spáchán trestný čin opatřuje potřebné podklady a nezbytná vysvětlení včetně zajištění stop trestného činu.

---

[244] CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008. Str. 416.

[245] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 158 [Přijímání a prověřování oznámení a jiných podnětů]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1932.

Dle ustanovení § 12 odst. 10 TŘ okamžik sepsání záznamu o zahájení úkonů v trestním řízení (dále jen ZÚTR) označujeme za zahájení přípravného řízení. Okamžikem zahájení přípravného řízení je taktéž provedení neodkladných nebo neopakovatelných úkonů, které tomuto záznamu předcházejí. Ve smyslu této práce půjde zejména o provedení odposlechu datového provozu, provedení domovní prohlídky nebo úkonů dle § 158d odst. 3. TŘ. Pokud dochází k těmto úkonům před zahájením fáze vyšetřování, musí být odůvodněno, proč se takto děje a proč je nutné je provést jako úkony neodkladné a neopakovatelné.[246]

Přípravné řízení můžeme rozdělit na prověřování, které se řídí ustanovení § 158 odst. 3 TŘ, a vyšetřování, které se řídí ustanovením § 160 a násl. TŘ.

5.4. Prověřování

Během prověřování policejní orgán objasňuje a prověřuje skutečnosti nasvědčující tomu, že byl spáchán trestný čin, a podniká kroky ke ztotožnění osoby pachatele. Účelem prověřování je vytvořit předpoklady pro procesní institut vyšetřování konkrétní osoby. Během prověřování dochází vyhledání potencionálních důkazů.

Státní zástupce je oprávněn uložit policejnímu orgánu v této fázi trestního řízení provedení takových úkonů, které je oprávněn provést a které povedou ke zjištění pachatele.[247]Takto prováděné úkony mohou mít charakter úkonu neodkladného a neopakovatelného. Z litery zákona plyne, že neodkladný je takový úkon, který vzhledem k nebezpečí jeho zmaření, zničení nebo ztráty důkazu nesnese z hlediska účelu trestního řízení odkladu na dobu, než bude zahájeno trestní stíhání. Neopakovatelný je takový úkon, který nebude možno před soudem provést. [248]Při vydání, resp. nařizování musí být v rozhodnutí dostatečně objasněno, proč se jedná o úkon neodkladný a neopakovatelný ve smyslu § 160 odst. 4 TŘ. Musí být také uvedeny skutečnosti, ze kterých plynulo, že byl úkon považován za neodkladný a neopakovatelný. Jako neodkladný či neopakovatelný úkon může být v této fázi trestního řízení proveden úkon domovní prohlídky.[249] Jak již bylo uvedeno výše, v případech tzv. počítačové kriminality nemůže formální nedostatek odůvodnění

[246] TOMEŠ, Jan. *Zahájení trestního stíhání a úkony prováděné před zahájením trestního stíhání*. Praha, 2016. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Jiří JELÍNEK.
[247] FRYŠTÁK, Marek a kol. *Trestní právo procesní.* Ostrava: Nakladatelství KEY Publishing, 2008 Str. 103.
[248] Viz ustanovení § 160 odst. 4 zákona č. 141/1963 Sb., trestní řád, ve znění pozdějších předpisů.
[249] Obdobně nález Ústavního soudu ze dne 15. 12. 2015 sp. zn. I.ÚS 2024/15.

neodkladnosti a neopakovatelnosti označeného úkonu bez dalšího znamenat nezákonnost domovní prohlídky a nepoužitelnost důkazů při ní opatřených.[250]

Autor je názoru, že za splnění podmínek neodkladného úkonu a dalších nezbytných podmínek, může být v této fázi trestního řízení realizován i úkon záznam o uskutečnění telekomunikačního provozu dle § 88a TŘ, dále odposlech a záznam telekomunikačního provozu dle § 88 TŘ.

Policejní orgán dále využívá institut podání vysvětlení, který je upraven v ustanovení § 158 odst. 3 písm. a) TŘ. Protokol o podání vysvětlení však zpravidla nemůže obstát před soudem jako důkaz. Aby došlo k získání procesně použitelného důkazu, je nezbytné vytěžení osoby v režimu provádění neodkladných a neopakovatelných úkonů, nejčastěji za užití institutu výslech svědka. K procesně použitelnému výstupu je nezbytné splnění poměrně přísných podmínek. Policejní orgán v takovém případě žádá státního zástupce o to, aby navrhl soudci provedení výslechu svědka. Soudce dále odpovídá za zákonnost provedení tohoto úkonu. Soudce není oprávněn realizovat průběh výslechu svědka tak, jak by jej prováděl před soudem (tedy aby byl plně v jeho dispozici) ale pouze dohlíží na zákonnost, kdy případné výhrady může zaznamenat formou námitek či připomínek. [251]

Během podání vysvětlení má dle ustanovení § 158 odst. 5 TŘ každý nárok na právní pomoc advokáta. V režimu podání vysvětlení jde však o právo obviněného, zajistit si na vlastní náklady právní pomoc advokáta (nikoliv ještě obhájce ve smyslu ustanovení § 35 TŘ). Policejní orgán je tedy povinen poskytnou osobě, podávající vysvětlení umožnit možnost kontaktovat advokáta – tedy např. umožněním telekomunikačního spojením s ním.[252]

5.5. Časový horizont prováděných úkonů

Ustanovení § 159 TŘ upravuje lhůty, v jakých musí OČTŘ tuto část přípravného řízení realizovat. Trestní řád diferencuje délku doby, po kterou může policejní orgán prověřování provádět dle příslušnosti soudu (resp. senátu či samosoudce). Předpokládá tímto, že prověřování věci patřící do příslušnosti samosoudce bude časově méně

[250] Viz rozhodnutí Nejvyššího soudu ze dne 15. 12. 2010 sp. zn. 5 Tdo 1312/2010 nebo Nález Ústavního soudu ze dne 9. 2. 2016 I. ÚS 2816/15.
[251] CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní*. 5. vydání. Praha: ASPI, 2008. Str. 422.
[252] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 158 [Přijímání a prověřování oznámení a jiných podnětů]. *Trestní řád I, II, III*. 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1932.

náročné než prověřování věci, patřící v prvním stupni do příslušnosti krajského soudu. Policejní orgán je povinen prověřit skutečnosti:

- do dvou měsíců od jejich přijetí, jde-li o věc patřící do příslušnosti samosoudce, v níž se nekoná zkrácené přípravné řízení,
- do tří měsíců, jde-li o jinou věc patřící do příslušnosti okresního soudu, a,
- do šesti měsíců, jde-li o věc patřící v prvním stupni do příslušnosti krajského soudu.

Výše uvedené lhůty běží od přijetí trestního oznámení, nebo jiného podnětu kterémukoliv z OČTŘ. Dojde-li k prověření na základě vlastního poznatku OČTŘ, započne běžet lhůta k vyřízení od prvního sepsání ZÚTR.[253]

Státní zástupce je oprávněn vydat pokyn, kterým ve formě opatření změní počet úkonů, které musí ještě policejní orgán provést. Státní zástupce tímto úkonem dále může stanovit odlišně lhůtu, po kterou může prověřování trvat. Z povahy věci vyplývá, že dojde k obligatornímu vydání v písemné podobě, neboť se toto opatření zakládá do spisu. [254]

Státní zástupce může žádosti policejního orgánu o prodloužení po ztotožněním se s obsahem žádosti vyhovět prostým písemným souhlasem, který sdělí policejnímu orgánu. V případě, že policejní orgán nestihne skončit prověřování v této poskytnuté lhůtě dle ustanovení § 159 odst. 2 TŘ, je nezbytné k dalšímu prodloužení lhůty k prověřování věci předložit spis státnímu zástupci s odůvodněným návrhem na prodloužení lhůty prověřování.[255] Z dikce ustanovení § 159 odst. 2 TŘ plyne, že se jedná o lhůtu pořádkovou.

Pokud OČTŘ nazná, že ve věci nejde o podezření z trestného činu, usnesením věc odevzdá jinému orgánu k projednání přestupku, či jiného kázeňského či kárného projednání. Policejní orgán věc obligatorně odloží z důvodů uvedených v ustanovení § 11 TŘ. Státní zástupce může před zahájením trestního stíhání věc usnesením odložit, např. je-li jeho výsledek neúčelný vzhledem k jinému očekávanému trestu, který pachatele postihne. Státní zástupce může o odložení věci taktéž rozhodnout, pokud vzhledem k chráněnému zájmu, způsobu provedení činu, jeho následkům a následnému chování pachatele po spáchání činu, jako je např. snaha o nahrazení škody či odstranění

[253]ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 159 [Lhůty ke skončení prověřování]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2030.
[254]ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 159 [Lhůty ke skončení prověřování]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2030.
[255]ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 159 [Lhůty ke skončení prověřování]. *Trestní řád I, II, III.* 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2030.

následků je zřejmé, že účelu trestního řízení bylo dosaženo rozhodnout. Neshledají-li však OČTŘ výše uvedené důvody, a nasvědčuje-li stávající prověřování k tomu, že byl spáchán trestný čin, a je dostatečně odůvodněn závěr, že jej spáchala určitá osoba, rozhodne policejní orgán neprodleně o zahájení trestního stíhání této osoby jako osobě obviněné.

5.6. Vyšetřování

Tato procesní část je výrazně formalizovanější než fáze prověřování. Ve fázi vyšetřování dochází k plnému respektování práva na obhajobu.

Úkon, jakým se vyšetřování zahajuje je vydání usnesení o zahájení trestního stíhání dle § 160 odst. 1 TŘ. Smyslem a účelem tohoto institutu je procesní podmínka přípustnosti dalších úkonů. Smyslem je dále srozumění obviněného o tom, že se proti němu vede pro konkrétní skutek a jeho právní kvalifikaci vyšetřování. Toto je nezbytné jednak z důvodu umožnění práva na obhajobu, ale dále také k jasnému ohraničení mezi jednotlivými útoky pokračujícího trestného činu.[256]

Usnesení o zahájení trestního stíhání vydá policejní orgán v případě, kdy jsou kumulativně naplněny následující podmínky. Zjištěné a odůvodněné skutečnosti nasvědčují tomu, že byl spáchán trestný čin a je dostatečně odůvodněn závěr, že jej spáchala určitá osoba. Náležitosti usnesení o zahájení trestního stíhání jsou upraveny v ustanovení § 134 odst. 1 a 2 TŘ. Výrok usnesení o zahájení trestního stíhání musí obsahovat popis skutku, ze kterého je tato osoba obviněna, aby nemohl být zaměněn s jiným, zákonné označení trestného činu, který je v tomto skutku spatřován. Usnesení musí být odůvodněno. V odůvodnění usnesení je třeba přesně označit skutečnosti, které odůvodňují závěr o důvodnosti trestního stíhání.[257]

Dozorující státní zástupce na základě podané stížnosti obviněného, nebo jiné oprávněné osoby rozhodne urychleně, a to s přihlédnutím k rozsahu spisového materiálu, které je třeba přezkoumat.[258] Podání stížnosti nemá odkladný účinek. Vyřizování stížnosti a řízení o ní se řídí ustanovením § 141 a násl. TŘ.

Opis usnesení o zahájení trestního stíhání je nutné nejpozději do okamžiku prvního výslechu doručit obviněnému. Právní účinky usnesení o zahájení vůči

[256] CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008. Str. 428.
[257] Viz. § 160 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) ve znění pozdějších předpisů.
[258] ŠÁMAL, Pavel, RŮŽIČKA, Miroslav. § 160 [Postup při zahájení]. *Trestní řád I, II, III*. 7.vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 2054.

obviněnému nastávají až okamžikem doručení, nikoliv jeho vyhotovení, jak je tomu u záznamu u záznamu o zahájení úkonů trestního řízení.

Trestní řád stanovuje i podmínky, které způsobují překážku zahájení trestního stíhání.

5.7. Skončení vyšetřování

Pokud má dozorují státní zástupce za to, že daný skutek není trestným činem ale přestupkem, postoupí věc příslušnému orgánu.[259] Dozorující státní zástupce obligatorně dále zastaví trestní stíhání v následujících případech:

- je-li nepochybné, že se daný skutek nestal,
- skutek, který se stal není trestným činem,
- nedošlo k prokázání, že daný skutek spáchala obviněná osoba,
- je-li trestní stíhání nepřípustné,
- nebyla-li obviněná osoba v době spáchání skutku nepříčetná z důvodu nepříčetnosti,
- zanikla-li trestnost činu. [260]

Krom toho je v dispozici dozorujícího státního zástupce rozhodnout o zastavení trestního stíhání v případě, že:

- je-li trest, k jehož uložení může trestní řízení vést bez významu vedle trestu, který již byl uložen, nebo který bude pachateli očekávaně uložen,
- bylo-li o skutku obviněné osoby již rozhodnuto jiným orgánem,
- jestliže vzhledem k významu a míře porušení chráněného zákona a následku a okolnostem a celkovému chování obviněné soby, zejména její snaze nahradit škodu nebo odstranit škodlivé následku skutku je zřejmé, že daného účelu trestního řízení bylo již dosaženo. [261]

Usnesení o zastavení trestního stíhání nebo o postoupení věci se doručí po nabytí právní moci Nejvyššímu státnímu zastupitelství. [262]

---

[259] § 171 odst. 1 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
[260] § 172 odst. 2 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
[261] § 173 odst. 1 zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů
[262] § 173a zákona č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů

Nazná-li policejní orgán, že je fáze vyšetřování skončena, a došlo ke shromáždění dostatečných podkladů k podání obžaloby, umožní dle § 166 odst. 1 TŘ obhájci obviněného nebo obviněnému prostudovat spis a učinit návrhy na doplnění vyšetřování. Po skončení vyšetřování předloží policejní orgán spis státnímu zástupci s návrhem na podání obžaloby, spolu se seznamem navrhovaných důkazů. [263]

[263] CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 5. vydání. Praha: ASPI, 2008. Str. 432.

ZÁVĚR

Jak plyne z obsahu této práce, implementace Úmluvy o počítačové kriminalitě proběhla relativně úspěšně. Právní řád České republiky v současné době - až na níže uvedené výhrady - úspěšně implementoval procesní nástroje, umožňující vyšetřování kybernetické kriminality tak, jak je v Úmluvě požadováno. Jistou výhradu lze mít k rozšíření práv OČTŘ u procesních nástrojů § 158d odst. 3 TŘ – sledování osob a věcí a § 7b odst. 2 TŘ – *data freeze*, resp. blokace digitálních dat v síti Internet. Absence povinnosti notifikace o provádění sledování a možnost policejního orgánu rozhodnout o blokaci obsahu webového obsahu lze považovat nejen za rozporné s čl. 19 Úmluvy o počítačové kriminalitě, stanovující standard ochrany práv občanů členských států, ale i za rozporné s LZPS.

Analýzou problematiky *data retention* došlo ke zjištění, které provozní a lokalizační údaje jsou uchovávány, přičemž v práci byl definován rozsah jejich uchovávání. Dle názoru autora rozsah uchovávaných údajů umožňuje efektivní vyšetřování skutků spáchaných v síti Internet. Provozní a lokalizační údaje je dle posledního nálezu ÚS subjekt ISP povinen plošně uchovávat po dobu 6 měsíců.[264] Významným zjištěním pro možnost plošného uchovávání je povaha IP adresy jako osobního údaje. Její povaha osobního údaje plyne jak z národní úpravy, tak z úpravy unijní. Ke správnému zavedení povinnosti jejího logování (nad rámec povinnosti *data retention*) je tedy nutná existence zákonného zmocnění. Na to je třeba brát zřetel při další možné změně zákonné úpravy, která se v minulosti po derogujících nálezech ÚS udála.

Dle názoru autora je stávající podoba *data retention* přijata v poměrně invazivní podobě. Plošné uchovávání provozních a lokalizačních údajů však po provedení testu proporcionality ÚS obstálo. Dle názoru autora by však po vzoru německého vzoru při využívání kombinace *data freeze* (zajištění informace o tom, z jaké IP adresy je přistupováno) a následného dotazu na ISP, kdo měl v danou dobu přidělenou konkrétní IP adresu, mohlo docházet k obdobným výsledkům při vyšetřování trestné činnosti, spáchané v kyberprostoru. ÚS existenci možnosti využít *data freeze* z nepochopitelného důvodu zcela pominul.

Jak však práce předestírá, jeden z nejvýznamnějších údajů uchovávaných při *data retention* je IP adresa. Tu lze považovat za jednu z nejvýznamnějších stop pro účely objasňování kybernetické kriminality. Nejde však o zcela jednoznačný identifikátor.

[264] Dle nálezu Ústavního soudu ze dne 14. 5. 2019 sp. zn. Pl. ÚS 45/17.

Vždy se jedná pouze o identifikátor přístupového bodu, z jakého bylo do sítě přistupováno. Existence množství anonymizačních metod nebo zakrytí možné osoby pachatele za NATem[265] má za následek, že IP adresu je třeba vnímat spíše jako „prvotní“ stopu, která však bezpochyby může vyšetřovatele nasměrovat blíže k osobě pachatele a zároveň posloužit jako skutečnost naplňující zákonné podmínky pro nařízení dalších zajišťovacích institutů (odposlech datového toku, provedení domovní prohlídky, analýza uživatelských dat v zařízeních…).

Nyní k řádné komparaci zajištěné IP adresy a fyzické osoby – pachatele. Pro provedení komparace s výsledkem použitelným v trestním řízení je nutné komparaci provést za využití institutu § 88a TŘ – záznam o uskutečnění telekomunikačního provozu. Přirozeně je nutné splnit všechny stanovené podmínky. Za účelem ustanovení pachatele je cenným provozním a lokalizačním údajem i fyzická adresa (nemovité věci), na které se přístupový bod do sítě Internet nachází. Toto může významně usnadnit přípravu na provedení domovní prohlídky a fyzické zajištění zařízení, jakož i následné vytěžení těchto zařízení. Velmi důležité informace pro zjištění konkrétní fyzické osoby může nabídnout zajištění aktivního síťového prvku zprostředkovávajícího připojení do sítě Internet. Tento prvek může obsahovat cenné informace o tom, který z uživatelů domácí nebo firemní sítě je možným pachatelem za situace, kdy navenek s identickou IP adresou disponuje více osob.

Po prvotním nasměrování OČTŘ je možné shromáždit dostatek informací k tomu, aby mohly být nařízeny další úkony vedoucí k zajištění digitálních dat či stop.

Dalším z institutů vedoucím k zajištění digitálních stop je provádění odposlechu datového toku. K jeho nařízení je zapotřebí splnit poměrně náročné podmínky. Poměrně překvapivým zjištěním byla jeho velmi nízká četnost využívání – řádově v nižších desítkách případů ročně. Tuto lze zřejmě dovodit z vysoké technické a personální náročnosti provádění odposlechu. Výzvou pro OČTŘ je bezpochyby analýza uživatelsky (end-to-end) šifrované komunikace, zprostředkovávané zpravidla za využití dalších aplikací či služeb dalších osob rozdílných od subjektů ISP. Takto šifrovaná data, dle názoru autora, ISP nemají povinnost ani možnost zpřístupňovat.

[265] IP adresa prozradí často jen router, ze kterého bylo přistupováno do sítě Internet. Další provoz se děje na základě rozdělování požadavků dle MAC adres – tento provoz je bez fyzického zajištění a analýzy zajištěných zajištění OČTŘ skryt a tento „vnitřní“ provoz mezi zařízením a routerem, typicky ve WiFi síti se označuje za NAT. V případě, že k připojení do sítě Internet došlo skrze mobilní zařízení s mobilním připojením se však o NAT nejedná – ISP by měl mít možnost (po omezený časový okamžik) zjistit, kterému uživateli přidělil danou IP adresu v konkrétní čas.

Potenciálně nesmírně cenným nástrojem, který však zároveň vyvolává spoustu praktických otázek jeho využití, je nástroj § 158d odst. 3 TŘ. Nejasnosti vyvolávají jeho dvě nejvýznamnější využití – jako sledovací software, a jako přístup do e-mailových, cloudových, či obdobných úložišť. Problémem je jeho nejasná jazyková textace, otázka jeho praktického využití, resp. nasazení. Autor upozornil na nevyvážený poměr obecných až vágních podmínek, které je nutné k jeho použití splnit vzhledem k tomu, jak intenzivní zásah do práv podezřelé osoby či dalších osob je využití způsobilé vyvolat. Neexistence povinnosti notifikovat, natož nemožnost se domoci práva na přezkum takového úkonu, je téměř alarmující. Krajně nevhodný je i zavádějící a zlehčující způsob, jakým PČR referuje o jeho užití Poslanecké sněmovně.

Neméně významné pro boj s kybernetickou kriminalitou by mohlo být efektivní zavedení institutu *data freeze.* Jak však plyne z popsaných problémů, institut je přijat jen polovičatě. V současném znění není implikována povinnost (ale ani možnost) *data holderů* „zmrazená“ data vydat OČTŘ. Jak již bylo naznačeno, část tohoto ustanovení je dle názoru autora přijata v rozporu s LZPS. **Blokace webových stránek za daných podmínek, ke které dojde rozhodnutí pouze policejního orgánu, bez možnosti přezkumu takovéhoto rozhodnutí v právním státě může obstát jen stěží.**

Fyzické zajištění stop, informací či důkazů o trestné činnosti, spáchané v síti Internet se děje nejčastěji při domovní prohlídce. Ke splnění podmínek k jejímu nařízení ustálená praxe dovodila, že postačuje zajištěná IP adresa, která nasvědčuje zjištění, že se v místě plánované prohlídky nemovité věci nachází skutečnosti či věci významné pro trestní řízení. To je na jednu stranu příznivý stav umožňující zajištění dalších skutečností (např. zajištěním a vytěžením uživatelských zařízení). Na druhou stranu, jak dokládá autor na příkladu z praxe, vydání příkazu k provedení domovní prohlídky a provedení invazivního zásahu na základě účelového trestního oznámení, spolu s uvedením pozměněné IP adresy, vedlo k porušení základních práv a svobod (provedením úkonu) u osoby, která se spáchaným skutkem neměla nic společného.

Následné vytěžování uživatelských zařízení je technicky náročný proces. Při jeho provádění je třeba přísně dodržovat předepsané postupy. Vzhledem ke snadné možnosti pozměnění dat je, dle názoru autora práce, legitimní požadavek *de lege ferenda* zavést povinnost při jakékoliv vytěžování dat používat hardwarový blokátor zaručující integritu a vylučující jakékoliv pozměnění vytěžovaných dat. Jak plyne z obsahu příslušné kapitoly, PČR již příslušnými blokátory disponuje.

Skutečnou výzvou pro objasňování této formy kriminality je využívání uživatelského šifrování digitálních dat. Jak však plyne z obsahu práce, analyzovaných smluv a ze sdělení PČR, OČTŘ mají legislativní, softwarové a hardwarové možnosti k pokusu o prolomení této formy zabezpečení. Lze však předpokládat, že PČR nebude s pokusy o rozšifrování dat příliš úspěšná. S možným zavedením zákonné povinnosti výrobců zpřístupňovat uživatelsky šifrovaná data lze očekávat negativní reakci společnosti. Snad jedinou možností, na kterou autor práce poukazuje, je skutečnost, že zákon, jakož i ustálená soudní praxe k odemykání zařízení nevylučuje použít biometrické údaje podezřelé osoby, a to i přes její odpor. Za splnění dalších podmínek je možné k pokusu o rozšifrování dat dosadit heslo, které podezřelá osoba již v minulosti použila a např. uložila ve webovém prohlížeči k automatickému vyplňování.

Všechny stopy, informace a důkazy zajištěné při vyšetřování trestné činnosti spáchané prostřednictvím výpočetní techniky je nutné dle názoru autora zpravidla považovat za důkazy nepřímé. **Vzhledem k jejich velmi snadnému zastření (viz kapitola anonymizační metody) či dokonce pozměnění (podvrh MAC adresy, podvržení odesílatele e-mailu atd.) musí být cílem OČTŘ ze zajištěných digitálních stop či důkazů vytvoření uceleného a logicky provázaného řetězce nepřímých důkazů.**

Při prokazování nade vší pochybnost je nutné zohlednit dva rozdílné pohledy. První z nich by měl reflektovat velmi náročnou činnost OČTŘ, která skládá jednotlivé informace do uceleného celku nepřímých důkazů. Tyto elektronické důkazy se vyznačují nestálostí a poměrně snadnou znehodnotitelností. Výše uvedené procesní nástroje, kterých je pro jejich zajištění nutné využít, jsou často náročné na splnění podmínek pro jejich využití jakož i na faktické provedení (např. provedení domovní prohlídky a vytěžení uživatelských zařízení). Dále často trpí jejich nevhodností pro dosažení sledovaného cíle (např. problematika vydání „zmrazených“ dat dle § 7b TŘ, nebo softwarové sledování dle § 158d odst. 3 TŘ). Při spáchaní každého TČ v kyberprostoru totiž OČTŘ stojí před nelehkým úkolem zpětného prokazování, že za klávesnicí, myší či obrazovkou zařízení seděla konkrétní fyzická osoba a že to byla právě ona, která je za daný skutek odpovědná. Pachatel přitom disponuje nespočtem možností, jak zastřít stopy o tom, že daný skutek spáchal právě on. Možnost využívání anonymizačních metod v kombinaci s možností šifrování stop či důkazů má za následek, že možnost spáchat pomyslný dokonalý zločin snad nikdy nebylo snadnější.

Druhým pohledem při prokazování viny konkrétnímu pachateli je však nutné zohlednit skutečnost, že možnost pozměnění digitálních stop a důkazů je velmi snadná – od možného podstrčení prvotních stop jako je IP adresa či pozmění MAC adresy, až po podstrčení digitálních důkazů do uživatelského zařízení. Velmi reálně se tedy může stát, že bude soud rozhodovat o vině osoby, která se spáchaným skutkem nemá nic společného.

Za stěžejní pro odhalování TČ tak autor především vnímá akutní potřebu kvalitního právního řádu, který tento nelehký úkol OČTŘ může usnadnit. Velmi důležité je klást náročné požadavky na profesní kvality osob, které se podílejí na vyšetřování, ale i na rozhodování o tom, zda se skutek stal, zda je trestný a kdo je za něj odpovědný. Na neposledním místě zůstává nutnost OČTŘ, typicky policejního orgánu, disponovat dostatečně kvalitním technickým vybavením. Jak plyne z poznatků prezentovaných touto prací, tak minimálně toto se PČR daří, a disponuje nejkvalitnějším možným vybavením.

SEZNAM ZKRATEK

Digitální stopa	digitální stopou se pro účely této práce rozumí jakákoliv skutečnost, informace, důkaz či jiný, obdobný prostředek významný pro objasnění pachatele TČ během trestního řízení;
Internet	sítí Internet se rozumí celosvětový systém, který se skládá ze sítě vzájemně propojených jednotek počítačových sítí, ve kterých mezi sebou tyto jednotky komunikují pomocí rodiny TCP/IP protokolů. Technicky je síť Internet dále tvořena soustavou sítí, serverů a různých dalších forem datových komunikačních prvků, tvořený propojovacími body, poskytovateli ISP a koncovými uživateli;[266]
IP adresa	se rozumí *„IP adresa je série číslic, sloužící k jedinečné identifikaci zařízení připojeného k síti Internet. Skládá se ze dvou částí, identifikace sítě, která určuje geografickou lokalizaci sítě, a „Host ID“ přesně určující konkrétní zařízení nebo část sítě. Na základě toho, zda je jedna IP adresa trvale přiřazena konkrétním uzařízení, nebo zda se IP adresa zařízení mění v průběhu času, rozlišujeme ještě statické a dynamické IP adresy.“*[267]
TPC/IP protokol	je unifikovaná sada protokolů, sloužící ke komunikaci v počítačové síti a propojení dvou počítačů. Základ tohoto modelu tvoří protokoly TCP (Transmision Control Protocol) a IP (Internet Protocol) ;[268]
ISP	se rozumí podnikající fyzická či právnická osoba, poskytující služby spočívající ve zprostředkování přístupu do sítě Internet dle zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů (ZEK). Zpravidla se bude jednat o osobu, která

[266] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 256.

[267] MÍŠEK, Jakub; HARAŠTA, Jakub. *IP adresy v kybernetické bezpečnosti* [online]. Brno: Masarykova univerzita, 2015 [cit. 17.5.2018]. Dostupné z: https://journals.muni.cz/revue/article/viewFile/4091/pdf

[268] TPC/IP. *ITslovník.cz* [online]. 2019 [cit. 6. 11. 2019]. Dostupné z: https://it-slovnik.cz/pojem/tcp-ip/?utm_source=cp&utm_medium=link&utm_campaign=cp

	skrze zřízení přístupového bodu umožňuje uživatelům (fyzickým osobám) přístup do sítě internet dle § 2, písm. m) ZEK
OČTŘ	se rozumí orgány činné v trestním řízení;
PČR	se rozumí Policie České republiky;
TČ	se rozumí trestný čin, tak, jak je definován v TZ;
TŘ	se rozumí zákon č. 141/1961 Sb., trestní řád, ve znění pozdějších předpisů;
TZ	se rozumí zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů;
Úmluva o počítačové kriminalitě	se rozumí Úmluva o počítačové kriminalitě Rady Evropy, které vnikla v roce 2001 a Česká republika k ní přistoupila v roce 2005;[269]
ÚS	se rozumí Ústavní soud ČR
ZEK	se rozumí zákon č. 127/2015 Sb., o elektronických komunikacích, ve znění pozdějších předpisů;
ZOHH	se rozumí zákon č. 186/2016 Sb., o hazardních hrách ve znění pozdějších předpisů;
ZOP	se rozumí zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů;
ZOCD	se rozumí zákon č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů;
Vyhláška o uchovávání	se rozumí vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, ve znění pozdějších předpisů;
ČAK	se rozumí Česká advokátní komora;
Operátor	se rozumí podnikatel, který zajišťuje nebo je oprávněn zajišťovat veřejnou komunikační síť nebo přiřazené prostředky.

[269] Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb.m.s.

SEZNAM POUŽITÉ LITERATURY A ZDROJŮ

Monografie:

1. BARTŮNĚK, Jan. Kybernetická kriminalita. Univerzita Karlova. Právnická fakulta, Katedra trestního práva. Vedoucí práce Tomáš GŘIVNA.
2. BRYANT, Robin. *Investigating Digital Crime.* 1. vydání. Chippenham, Wiltshire: Canterbury Christ Church University, 2008, 249 s. ISBN 978-0-470-51600-3.
3. CÍSAŘOVÁ, Dagmar; FENYK, Jaroslav; GŘIVNA, Tomáš a kol. *Trestní právo procesní.* 5. vyd. Praha: ASPI, 2008, 822 s. ISBN 978-80-7357-348-5.
4. DE ZAN, Tomasso. AUTOLITANO, Simona. EUnited Against Crime: Improving Criminal Justicein European Union Cyberspace. Instituto Affari Ainternazionali. [online]. 16. 10. 2016 [cit. Dne 19. 8. 2019]. Dostupné z: http://www.iai.it/sites/default/files/iai1617.pdf
5. FRYŠTÁK, Marek a kol. *Trestní právo procesní.* Ostrava: Nakladatelství KEY Publishing, 2008. 249 s. ISBN 978-80-87071-72-4.
6. JELÍNEK, Jiří a kol. *Dokazování v trestním řízení v kontextu práva na spravedlivý proces*. Vydání první. Praha: Leges, 2018. 536 s. ISBN: 978-80-7502-287-5.
7. KOLOUCH, Jan. *CyberCrime.* 1. Vydání. Praha: CZ.NIC, 2016, 511 s. ISBN 978-80-88168-18-8
8. KOTHÁNEK, Jakub. *Vytěžování důkazů z výpočetní techniky.* Brno, 2013/2014 Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Václav STUPKA.
9. KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, 536 s. ISBN 978-80-7179-226-0.
10. LOVÍŠKOVÁ, Zuzana. *Odposlech a záznam telekomunikačního provozu.* Praha, 2013, s. 10. Univerzita Karlova, Právnická fakulta. Vedoucí práce Jiří ŘÍHA.
11. MOHELSKÝ, Michal. Identifikace pachatelů trestné činnosti v kyberprostoru. Brno, 2018. Diplomová práce. Masarykova univerzita, právnická fakulta. Vedoucí práce Milana HRUŠÁKOVÁ.
12. MUSIL, Jan. *Trestní právo procesní.* 4. přepracované vydání. Praha: C.H.Beck, 2013. s. 328.
13. NEZMAR, Luděk. *GDPR: Praktický průvodce implementací.* Praha: Nakladatelství

GRADA Publishing, 2017. 301 s. ISBN: 978-80-271-0668-4.

14. PÍŠA, Miroslav. *Datová bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí.* Zlín, 2008. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce JAŠEK, Roman.
15. PÍŠA, Miroslav. Datová bezpečnost bezdrátové komunikace v rámci vnitřních podnikových sítí. Zlín, 2008. s. 23. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce JAŠEK, Roman.
16. POLČÁK, Radim, PÚRY, František, HARAŠTA, Jakub a kolektiv. *Elektronické důkazy v trestním řízení.* 1. vyd. Brno: Masarykova univerzita, Právnická fakulta, 2015. 254 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7.
17. REYES, Anthony, O'SHEA, Kevin, STEELE, Jim, HANSEN, John, JEAN, Banjamin, RALPH, Thomas. *Cyber Crime Investigation: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Rockland: Syngress publishing, 2007. 411 s. ISBN: 978-1-59749-133-4.
18. SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015. 636 s. ISBN 978-80-7380-501-2.
19. ŠÁMAL, Pavel, BAXA, Josef, GŘIVNA, Tomáš, KRÁL, Vladimír, NOVOTNÁ, Jaroslava, PÚRY, František, RŮŽIČKA, Miroslav, ŠKVAIN, Petr. *Trestní řád. 6. vydání.* Praha: Nakladatelství C. H. Beck, 2008, 3014 s. ISBN 978-80-7400-043-0.
20. ŠÁMAL, Pavel, GŘIVNA, Tomáš, NOVOTNÁ, Jaroslava, PÚRY, František, RŮŽIČKA, Miroslav, ŘÍHA, Jiří, ŠÁMALOVÁ, Milada, ŠKVAIN, Petr. *Trestní řád I, II, III. 7.vydání*. Praha: Nakladatelství C. H. Beck, 2013, 4720 s. ISBN 978-80-7400-465-0.
21. ŠEPTUN, Michal. *Identita v tunelovaných a překládaných sítích.* Brno: Vysoké učení technické v Brně, Fakulta informačních technologií. Diplomová práce, 2014/2015, str. 13. Vedoucí práce POLČÁK, Libor.
22. TOMEŠ, Jan. *Zahájení trestního stíhání a úkony prováděné před zahájením trestního stíhání*. Praha, 2016. Diplomová práce. Univerzita Karlova, Právnická fakulta. Vedoucí práce Jiří JELÍNEK.
23. TÝČ, Václav. *Základy práva Evropské unie pro ekonomy*. 6. Vydání. Praha: Leges, 2010. 301 s. ISBN 978-80-87212-60-8.
24. VANGELI, Benedikt. *Zákon o Policii České republiky.* 2. vydání. Praha: Nakladatelství C. H. Beck, 2014, 488 s. ISBN 978-80-7400-543-5.

25. VLACHOVÁ, Barbora. *Zákon o elektronických komunikacích.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, 536 s. ISBN 978-80-7400-632-6.

Internetové články:

26. BitLocker. *Microsoft Inc.* [online] publikováno 16. 10. 2017 [cit. 20. 6. 2018] dostupné z: https://docs.microsoft.com/cs-cz/windows/security/information-protection/bitlocker/bitlocker-overview
27. Hlášení kyberkriminality. *Policie České republiky*. [online] publikováno 1. 8. 2012 [cit. dne 15.5.2018] dostupné z: http://www.policie.cz/clanek/hlaseni-kyberkriminality.aspx
28. KRČMÁŘ, Petr. Hacking Team hacked: prodával spyware mnoha státům včetně Česka. *Root.cz.* [online] publikováno 7. 7. 2015. [cit. 1. 11. 2019]. Dostupné z: *https://www.root.cz/clanky/hacking-team-hacked-prodaval-spyware-mnoha-statum-vcetne-ceska/*
29. Poslanci schválili zákon o hazardu, počítá i s blokováním webových stránek. *E15.CZ.* [online] publikováno 13. 4. 2016. [cit. 12. 11. 2019]. Dostupné z: https://www.e15.cz/byznys/obchod-a-sluzby/poslanci-schvalili-zakon-o-hazardu-pocita-i-s-blokovanim-webovych-stranek-1287700
30. Použití sledovacího softwaru. *Policie České republiky.* [online] publikováno 7. 7. 2015 [cit. 18. 12. 2019] dostupné z: http://www.policie.cz/clanek/pouziti-sledovaciho-softwaru.aspx
31. SOKOL, Tomáš. *Domovní prohlídka u advokátů.* Právní rádce, 2016. [online] dostupné z: https://www.cak.cz/scripts/detail.php?id=15462
32. Šifrování startovacího disku pomocí FileVaultu. *Apple Inc.* [online] publikováno 3. 1. 2018 [cit. 20.6.2018], dostupné z: https://support.apple.com/cs-cz/ht204837
33. Uchovávání provozních a lokalizačních údajů. *Policie České republiky.* [online] publikováno 2. 6. 2015 [cit. 22. 6. 2018] dostupné z: http://www.policie.cz/clanek/uchovavani-provoznich-a-lokalizacnich-udaju.aspx
34. Ukončení provozu Hotline. *Policie České republiky*. [online] publikováno 24. 5. 2018 [cit. dne 20.6.2018] dostupné z: http://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx
35. Veřejná nabídka služeb společnosti Tefincom S.A. [online]. 2020 [cit. 30. 1. 2020]. Dostupné z: https://nordvpn.com/features/strict-no-logs-policy/

36. VYMAZAL, Tomáš; LÍŇOVÁ, Hana. Přípustnost a podmínky použití lokalizačních údajů v trestním řízení. *EPRAVO.CZ*. [online] publikováno 16.1.2017 [cit. 22. 6. 2018] dostupné z: https://www.epravo.cz/top/clanky/pripustnost-a-podminky-pouziti-lokalizacnich-udaju-v-trestnim-rizeni-104734.html
37. WEDOS Internet, a.s. První web vymazán z internetu na základě nového paragrafu §7b trestního řádu. *Blog WEDOS*. [online] publikováno 13. 3. 2019. [cit. Dne 16. 10. 2019]. Dostupné z: https://blog.wedos.cz/prvni-web-vymazan-z-internetu-na-zaklade-noveho-paragrafu-§7b-trestniho-radu
38. WHITWAM, Ryan. Supposedly Non-Existent VPN Logs Help FBI Catch Internet Stalker. *ExtremeTech*. [online] Publikováno 2017 [cit. 1. 2. 2019]. Dostupné z: https://www.extremetech.com/internet/257214-supposedly-non-existent-vpn-logs-help-fbi-catch-internet-stalker
39. Wi-Fi – provoz, odpovědnost a GDPR. *Miia SE*. [online] [cit. 17. 2. 2019] dostupné z: http://news.miia.cz/gdpr/

Judikatura:

40. Nález Ústavního soudu ze dne 23. 6. 2005 sp. zn. II. ÚS 255/05.
41. Nález Ústavního soudu ze dne 1. 11. 2006 sp. zn. II. ÚS 362/06.
42. Nález Ústavního soudu ze dne 10. 3. 2005 sp. zn. III.ÚS 561/04.
43. Nález Ústavního soudu ze dne 11. 6. 2019 sp. zn. II. ÚS 3533/18.
44. Nález Ústavního soudu ze dne 12. 1. 2006 sp. zn. II. ÚS 552/05.
45. Nález Ústavního soudu ze dne 14. 11. 2012 sp. zn. IV. ÚS 2227/12.
46. Nález Ústavního soudu ze dne 14. 2. 2017 sp. zn. Pl. ÚS 28/16.
47. Nález Ústavního soudu ze dne 15. 12. 2015 sp. zn. I.ÚS 2024/15.
48. Nález Ústavního soudu ze dne 15. 12. 2015 sp. zn. I.ÚS 2024/15.
49. Nález Ústavního soudu ze dne 20. 10. 2015 sp. zn. II. ÚS 3907/14.
50. Nález Ústavního soudu ze dne 22. 10. 2019 sp. zn. III. ÚS 702/17.
51. Nález Ústavního soudu ze dne 23. 5. 2007 sp. zn. III. ÚS 655/06.
52. Nález Ústavního soudu ze dne 26. 4. 2016 sp. zn. III. ÚS 3457/14-2.
53. Nález Ústavního soudu ze dne 26. 4. 2016 sp. zn. III. ÚS 3457/14.
54. Nález Ústavního soudu ze dne 28.08.2009 sp. zn. II. ÚS 2894/08.

55. Nález Ústavního soudu ze dne 7. 6. 2016 sp. zn. III. ÚS 905/13.
56. Nález Ústavního soudu ze dne 8. 6. 2010 sp. zn. Pl. ÚS 3/09.
57. Nález Ústavního soudu ze dne 9. 2. 2016 sp. zn. I. ÚS 2816/15.
58. Rozhodnutí Krajského soudu v Plzni dne 30. 3. 2017 sp. zn. 34 T 13/2016.
59. Rozhodnutí Nejvyššího soudu ze dne 13. 12. 2016 sp. zn. 4 Pzo 16/2016.
60. Rozhodnutí Nejvyššího soudu ze dne 15. 12. 2010 sp. zn. 5 Tdo 1312/2010.
61. Rozhodnutí Nejvyššího soudu ze dne 15. 12. 2010 sp. zn. 5 Tdo 1312/2010.
62. Rozhodnutí Nejvyššího soudu ze dne 29. 3. 2000, sp. zn. 5 Tz 32/2000.
63. Rozhodnutí Nejvyššího soudu ze dne 7. 6. 2017 sp. zn. 6 Tz 3/2017
64. Rozhodnutí Soudního dvora ze dne 19. 10. 2016, sp. zn. C-582/14.
65. Rozhodnutí Ústavního soudu ze dne 22. 6. 2006 sp. zn. I. ÚS 671/05.
66. Rozsudek Soudního dvora Evropské unie ze dne 4. 4. 2014 ve spojených věcech sp. zn. C-293/12 a C-594/12
67. Usnesení Nejvyššího soudu ze dne 15. 11. 2016, sp. zn. 4 Pzo 14/201.
68. Usnesení Nejvyššího soudu ze dne 15. 11. 2016, sp. zn. 4 Pzo 14/2016
69. Usnesení Nejvyššího soudu ze dne 15. 12. 2000 sp. zn. 7 Tz 9/2000.
70. Usnesení Nejvyššího soudu ze dne 19.9.2012 sp. zn. 4 Pzo 3/2012.
71. Usnesení Nejvyššího soudu ze dne 26. 6. 2013 sp. zn. 15 Tdo 510/2013.
72. Usnesení Nejvyššího soudu ze dne 7. 5. 2019 sp. zn. 4 Tdo 1591/2018
73. Usnesení ÚS ze dne 9. 2. 2016 vedené pod sp. zn. I. ÚS 2816/15.
74. Usnesení Ústavního soudu ze dne 10. 7. 2018 sp. zn. IV. ÚS 1313/18.
75. Usnesení Ústavního soudu ze dne 14.12.2011 sp. zn. IV. ÚS 3225/09.
76. Usnesení Ústavního soudu ze dne 16. 4. 2019 sp. zn. II. ÚS 1095/19 bod č. 12
77. Usnesení Ústavního soudu ze dne 23. 8. 2018 sp. zn. sp. zn. IV. ÚS 3636/15.
78. Usnesení Ústavního soudu ze dne 9. 2. 2016 sp. zn. I. ÚS 2816/15.
79. Usnesení Vrchního soudu v Praze ze dne 18. 1. 2001 sp. zn. 4 To 3/01.
80. Ústavního soudu ze dne 28. 1. 2003 sp. zn. II. ÚS 118/01.

Ostatní:

81. *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2016*. Policejní prezidium České republiky. [online] publikováno 15. 8. 2017 [cit. dne 8. 5. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-

telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx

82. *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2017*. Policejní prezidium České republiky. [online] publikováno 5. 10. 2018 [cit. dne 11. 10. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx
83. *Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací za rok 2018*. Policejní prezidium České republiky. [online] publikováno 22. 8. 2019 [cit. dne 1. 09. 2019] dostupné z: https://www.mvcr.cz/clanek/analyzy-odposlechu-a-zaznamu-telekomunikacniho-provozu-a-sledovani-osob-a-veci-dle-trestniho-radu-a-ruseni-provozu-elektronickych-komunikaci-policii-cr-archiv.aspx
84. Dopis ministra vnitra ČR Milana Chovance poslankyni Janě Černochové č.j. PPR-20893–1/ČJ-2015-990300 ze dne 17. 8. 2015
85. DOSTÁL, Otto. *Zajišťování důkazů u počítačové kriminality – dožádání, vydání věci a prohlídky (1. díl)*. Trestněprávní revue. 2019, č. 3, str. 66. ISSN 1213-5313.
86. GRÜNWALDOVÁ, Vladimíra. K odposlechům mobilní telefonické komunikace. *Bulletin advokacie*. 2019, č. 12. Str. 60. ISSN 1210-6348.
87. HLAVÁČOVÁ, Kateřina a Oliver CHORVÁT. Přístup orgánů činných v trestním řízení k datům uloženým v cloudu. *Revue pro právo a technologie*. [Online]. 2016, č. 14, s. 11. [cit. 22. 11. 2019]. Dostupné z: https://journals.muni.cz/revue/article/view/6120
88. JAMBOROVÁ, Kateřina. *Provozní a lokalizační údaje, nález Ústavního soudu a § 88a TŘ*. Trestněprávní revue. 2012, č. 3, s. 61-65. ISSN 1213-5313.
89. JELÍNEK, Jiří. K chybějící právní úpravě tzv. prostorového odposlechu v trestním řádu. *Bulletin advokacie.* [online] 2018, č. 9. [cit. 7. 9. 2019]. Dostupné z: https://journals.muni.cz/revue/about/submissions?navItem=0
90. K otázce výkladu pojmu „jiné prostory, v nichž advokát vykonává advokacii“ (§ 85b odst. 1 TŘ) a k otázce, zda o návrhu ve smyslu § 85b odst. 3 tr. ř. *Bulletin advokacie.* [online] publikováno 6. 10. 2015 [cit 1. 6. 2020] dostupné z: http://www.bulletin-advokacie.cz/k-otazce-vykladu-pojmu-jine
91. KOKEŠ, Marian. *Judikatura ÚS: Ochrana soukromí v tzv. době internetové.* Soudní

rozhledy. Praha: C. H. Beck, 6/2019, str. 182. ISSN 1211- 4405.

92. Kupní smlouva mezi Českou republikou – Krajské ředitelství policie Libereckého kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 12. 9. 2019, č. j. KRPL-44479/2019. Registr smluv. [online] publikováno 12. 9. 2019 [cit. 12.1.2020] Dostupné z: https://smlouvy.gov.cz/smlouva/10135722
93. MATOCHA, Jakub. *Informační povinnost a oprávněné subjekty podle § 88a odst. 2 TrŘ.* Trestněprávní revue. 2019, č. 7-8, s. 152. ISSN 1213-5313.
94. Ministerstvo Financí. *Metodický pokyn k plnění povinností (ve věci seznamu nepovolených internetových her)*. [online]. 16. 1. 2017. [cit. 10. 11. 2019]. Dostupné z: https://www.mfcr.cz/cs/legislativa/metodiky/2017/metodicky-pokyn-k-plneni-povinnosti-ve-v-27269
95. MÍŠEK, Jakub a Jakub HARAŠTA. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*. [Online]. 2015, č. 12, s. 21-42. [cit. 7. 2. 2020]. Dostupné z: https://journals.muni.cz/revue/article/view/4091
96. POLČÁK, Libor. *Základní informace o síti Tor.* 2017, Brno: FIT VUT. Technická zpráva č. FIT-TR-2017-01. [online] [cit. 15. 5. 2018] dostupné z: http://www.fit.vutbr.cz/research/pubs/index.php?file=%2Fpub %2F11513%2Ftr.pdf&id=115
97. Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě 104/2013 Sb. m. s.
98. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 25. 8. 2017 pod č. j. PPR-23209-5/ČJ-2017-990140
99. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 22. 3. 2018 pod č. j. PPR-9726-3/ČJ-2018-990140
100. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 25. 8. 2017 pod č. j. PPR-23209-5/ČJ-2017-990140 a dále sdělení ze dne 9. 5. 2019 pod č.j. PPR-16663-4/ČJ-2019-990140.
101. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 6. 1. 2020 pod č. j. Č. j. UZC-476-1/ČJ-2020-2800KR.
102. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 17. 1. 2020 pod č. j. PPR-1074-4/ČJ-2020-990810.

103. Sdělení Policie České republiky na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím ze dne 6. 11. 2019 pod č. j. PPR-33938-8/ČJ-2019-990810

104. Smlouva mezi Českou republikou – Ministerstvo vnitra a společností Risk Analysis Consultants, s.r.o. ze dne 3. 11. 2017, č. j. PPR-14605-86/ČJ-2017-990656 Registr smluv. [online] publikováno 3. 11. 2019 [cit. 11. 1. 2020] dostupné online z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjG_c_8wrvnAhXOPFAKHbreCIcQFjAAegQIAxAB&url=https%3A%2F%2Fsmlouvy.gov.cz%2Fsmlouva%2Fsoubor%2F5103736%2FForenznihwaswcastH.pdf&usg=AOvVaw0YR1b_Q-yxFUsSmv7aq88j)

105. Smlouva mezi Ministerstvem vnitra – Krajským ředitelstvím policie Libereckého kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 12. 9. 2019 č. j. KRPL-44479/2019. Registr smluv. [online] publikováno 12. 9. 2019 [cit. 6. 2. 2020] dostupné online z: https://smlouvy.gov.cz/smlouva/10135722

106. Smlouva mezi Ministerstvem vnitra – Krajským ředitelstvím policie Jihomoravského kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 15. 4. 2019 č. j. KRPB-65709-3/ČJ-2019-0600VZ. Registr smluv. [online] publikováno 15. 4. 2019 [cit. 2. 1. 2020] dostupné online z: https://smlouvy.gov.cz/smlouva/8814079 online z: https://smlouvy.gov.cz/smlouva/8814079

107. Smlouva mezi Ministerstvem vnitra – Krajským ředitelstvím policie Jihomoravského kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 15. 4. 2019 č. j. KRPB-65709-3/ČJ-2019-0600VZ. Registr smluv. [online] publikováno 15. 4. 2019 [cit. 2. 1. 2020] dostupné online z: https://smlouvy.gov.cz/smlouva/8814079

108. Smlouva mezi Ministerstvem vnitra – Krajským ředitelstvím policie Jihomoravského kraje a společností Risk AnalysisConsultants, s.r.o. ze dne 15. 4. 2019 č. j. KRPB-65709-3/ČJ-2019-0600VZ. Registr smluv. [online] publikováno 15. 4. 2019 [cit. 2. 1. 2020] dostupné online z: https://smlouvy.gov.cz/smlouva/8814079

109. SOKOL, Tomáš. Povinnost dle § 7b trestního řádu z pohledu advokáta. *Bulletin advokacie*. 2019, č. 9, s. 15-19. ISSN 1210-6348.

110. TOMAN, Petr. Podstračený paragraf 7b Trestního řádu - kde se vzal a o čem je.

advokatnidenik.cz [online]. 22. 7. 2019 [cit. 3. 11. 2019]. Dostupné z: https://www.cak.cz/scripts/detail.php?id=20932

111. TPC/IP. *ITslovník.cz* [online]. 2019 [cit. 6. 11. 2019]. Dostupné z: https://it-slovnik.cz/pojem/tcp-ip/?utm_source=cp&utm_medium=link&utm_campaign=cp

112. Vláda: Důvodová zpráva k zákonu č. 287/2018 Sb. kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, č. 287/2018 Dz

113. Vládní návrh, kterým se předkládá Parlamentu České republiky k vyslovení souhlasu s ratifikací Úmluva o počítačové kriminalitě. Senát Parlamentu České republiky. [online] Publikováno 2013 [cit dne 8. 9. 2019] dostupné z: https://www.senat.cz/xqw/webdav/pssenat/original/66810/56264

114. ZEMAN, Pavel. *Stanovisko ke sjednocení výkladů zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek.* Nejvyšší státní zastupitelství [online]. Brno, 2015 [cit. 17. 5. 2018] dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

Právní předpisy:

115. Evropská úmluva o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8, Řím, vyhlášená pod č. 209/1992 Sb.

116. Evropská úmluva o ochraně lidských práv a základních svobod ve znění protokolů č. 3, 5 a 8, Řím, vyhlášená pod č. 209/1992 Sb.

117. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

118. Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb.m.s.

119. Smlouva o fungování Evropské unie

120. Usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod

121. Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů ve znění pozdějších předpisů

122. Zákon č. 127/2005 Sb., o elektronických komunikacích ve znění pozdějších předpisů

123. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
124. Zákon č. 141/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.
125. Zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů.
126. Zákon č. 273/2008 Sb., o Policii ČR ve znění pozdějších předpisů.
127. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
128. Zákona č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů.

129.

ABSTRAKT, KLÍČOVÁ SLOVA

Zajišťování digitálních stop pro účely trestního řízení

Tato rigorózní práce analyzuje procesně právní instituty, které slouží k zajišťování digitálních stop v síti Internet za účelem vyšetřování trestné činnosti, spáchané v kyberprostoru.

Práce pojednává o vybraných procesních ustanovení Úmluvy o počítačové kriminalitě, které slouží k zajišťování digitálních stop. Dále je provedeno posouzení, zda česká právní úprava těmto požadavkům vyhovuje.

Analýza právní úpravy *data retention* poskytla informace o tom, co jsou to provozní a lokalizační údaje a popsala rozsah jejich uchovávání. Pominuta není ani aktuální judikatura. Došlo k rozvedení problematiky identifikace pachatelů na základě zajištěných IP adres a vysvětlení anonymizačních metod.

Nejpodstatnějším cílem práce je rozsáhlé rozvedení zajišťovacích institutů dle zákona č. 141/1961 Sb., trestního řádu, prostřednictvím kterých dochází k zajišťování digitálních stop, vedoucích ke zjištění pachatele a využití těchto údajů pro účely trestního řízení. Práce rozvádí záznam o uskuteční telekomunikačního provozu, odposlech datového toku, sledování prováděné technickým prostředkem, *data freeze* a fyzické zajišťování důkazů.

Jednotlivé instituty tato práce komparuje s požadavky Úmluvy o počítačové kriminalitě. Tato práce dále detailně popisuje podmínky, za kterých může k jejich využití dojít. Práce nabízí ukázku praktického užití nástrojů a poskytuje statistiky využití těchto institutů. Jednotlivé instituty doplňuje o úvahy *de lege ferenda*. Práce nepostrádá rozvedení problematiky šifrování, jakož i možnosti OČTŘ k prolomení šifrování či jiné skutečnosti, spojené s vytěžováním digitálních dat či důkazů.

Jako poslední kapitolu práce ve stručnosti uvádí jednotlivé fáze trestního řízení před fází sdělením obžaloby. Do těchto fází zasazuje možnost užití jednotlivých zajišťovací úkony.

V závěru práce hodnotí vhodnost české právní úpravy k efektivnímu zajišťování digitálních stop, jakož i k postihování trestné činnosti, páchané v síti Internet.

Klíčová slova:

Kybernetická kriminalita, provozní a lokalizační údaje, digitální stopy

ABSTRACT, KEY WORDS

Seizing digital tracks for the purpose of a criminal proceeding

This thesis analyzes procedural institutes of law that serve to seize digital traces on the Internet to investigate cybercrime.

This document also deals with a selected procedural institute of the Convention on Cybercrime, which serves to secure digital traces. Furthermore, an assessment is made as to whether the Czech legislation meets these requirements.

Data retention analysis provided information on what traffic and location data are and describes the extent of their retention. The issue of identification of offenders based on seized IP addresses was explained and anonymization methods were explained.

The main goal of the thesis is an extensive elaboration of some relevant procedural institutes of the Code of criminal procedure no. 141/1961 Sb., through which digital traces are seized. This data may lead to the identification of the offender, and also for conviction of guilt during criminal proceedings. The thesis elaborates institutes: a record of telecommunication traffic, monitoring digital communication, data freeze, and physical provision of devices.

This work compares individual institutes with the requirements of the Convention on CyberCrime. The author of this thesis describes in detail the conditions defined by Czech legislation, under which they can be used. This thesis offers a demonstration of the practical use of legal instruments and provides statistics on the use of these instruments. The individual legal institutes are supplemented by a proposal of de lege ferenda. This document also describes problems of encryption, as well as the possibilities of law enforcement authorities to break encryption or other facts associated with the extraction of digital data or evidence.

The last chapter of the work briefly lists the various stages of criminal proceedings. In these phases it puts the possibility of using individual institutes.

At the end of the thesis, it evaluates the suitability of the Czech legislation for the effective provision of digital traces, as well as for penalizing crimes committed on the Internet.

Keywords

Cybercrime, operational and location data, digital traces