UNIVERZITA KARLOVA

PRÁVNICKÁ FAKULTA

Mgr. Kristina Rademacherová

POČÍTAČOVÁ KRIMINALITA:

VYBRANÉ ASPEKTY POSTIHU V MEZINÁRODNÍM PROSTŘEDÍ

RIGORÓZNÍ PRÁCE

Vedoucí rigorózní práce: prof. JUDr. Jiří Jelínek, CSc.
Katedra trestního práva
Datum vypracování práce (uzavření rukopisu): 24. února 2017

Prohlašuji, že předloženou rigorózní práci jsem vypracovala samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 24. února 2017.

Mgr. Kristina Rademacherová

PODĚKOVÁNÍ

Děkuji prof. JUDr. Jiřímu Jelínkovi, CSc. za jeho vstřícný a trpělivý přístup během vedení této práce, odborný dohled i cenné rady, které mi poskytnul.

A děkuji rovněž mým nejbližším – mému příteli Vaškovi a rodině.

Obsah

ÚVOD

Moderní informační a komunikační technologie již několik desetiletí utváří lidskou společnost a do okolního světa vnáší nové prvky, které usnadňují každodenní činnost, stírají hranice zemí, šíří poznání, ale také přetváří mezilidskou komunikaci a poskytují příležitosti pro mnohé protispolečenské jevy. Značná část aktivit se přesouvá do virtuálního světa a odehrává kdesi v kyberprostoru, smyšleném a pro řadu lidí těžko představitelném prostředí. Někteří využívají moderních technologií ku prospěchu okolí, jiní v nich objevili dříve netušený potenciál, kterého se rozhodli zneužít pro vlastní kriminální aktivity.

Pachatelé trestné činnosti hojně využívají výhod nabízených celosvětově propojenými počítačovými sítěmi. Globální virtuální prostor jim z cesty odstranil řadu překážek – hranice států v něm neexistují, cíl útoku je snadno dosažitelný, vlastní trestnou činnost lze snáze skrýt. Právní regulace je ze své podstaty spíše rigidní a často se ocitá v konfliktu se společenskými změnami, které vývoj informačních a komunikačních technologií přináší, a na něž právo nereaguje buď vůbec, anebo s příliš velkým zpožděním.

O mezinárodním přesahu počítačové kriminality mezi odborníky není pochyb,[1] virtuální prostředí umožňuje neomezený transfer digitálních dat bez ohledu na jurisdikce států. Bylo by až s podivem, kdyby lidé příležitost páchat trestnou činnost skrze propojené počítačové sítě nevyužili. Mezinárodní společenství při postihu počítačové trestné činnosti však naráží na řadu překážek, které brání úspěšnému odhalení, stíhání, dopadení i potrestání pachatelů. Počítačová kriminalita se stává vážným globálním problémem.

Roku 2013 bylo k Internetu[2] připojeno přes 2,7 bilionu obyvatel světa, tj. zhruba 40% světové populace.[3] Ačkoli procento připojení k Internetu je mnohem vyšší v

[1] Lze odkázat na práce zahraničních autorů jako Susan Brenner, Bert-Jaap Koops, Peter Grabosky, Nicolai Seitz, Ulrich Sieber, Anna Maria Osula, Henrik Kaspersen aj.

[2] „Internet“ s velkým počátečním písmenem označuje celosvětovou informační a komunikační síť. Naopak „internet“ označuje jakékoli propojené počítačové sítě. Rozlišení respektuje i tato práce. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 52.

[3] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online].

rozvinutých zemích, rozvojové země je rychle dohání.[4] Lze hovořit o vzniku globálního virtuálního společenství, jehož nejčastěji užívaným jazykem je angličtina s čínštinou.[5] K rozvoji počítačové trestné činnosti dochází zejména v oblasti elektronického obchodování a bezpečnosti informačních systémů a sítí. Podle srovnávací studie Organizace spojených národů, na které se podílelo 61 zemí světa, se ⅓ počítačové trestné činnosti vztahuje k padělání a různým formám podvodného jednání, ⅓ až ½ ke škodlivému obsahu[6] a zbývajících 10 až 33% představuje hacking, tedy trestnou činnost spojenou s neoprávněným přístupem k počítačovému systému.[7]

V předkládané rigorózní práci si kladu za cíl pojednat o komplexní problematice postihu počítačové kriminality v mezinárodním prostředí. Postih vnímám v širokém významu slova jako činnost orgánů činných v trestním řízení směřující k odhalení a stíhání pachatele konkrétní formy počítačové kriminality. Vědomě se přitom zaměřuji na proces objasňování a vyšetřování počítačových trestných činů jako na typickou činnost orgánů činných v trestním řízení, jejímž smyslem je poznat kriminalisticky relevantní událost.[8] Nesoustředím se na problematiku sankcionování, neboť tato se u počítačových trestných činů neliší od případů jiné trestné činnosti. Ukládání trestních sankcí je do značné míry též ovlivněno kriminální politikou konkrétního státu a aktivity mezinárodního společenství se soustředí spíše na regulaci trestněprocesních institutů usnadňujících vyšetřování počítačové trestné činnosti s mezinárodním přesahem, nežli na její sankcionování.

Rigorózní práce je rozdělena do pěti kapitol. Chceme-li se věnovat počítačové kriminalitě v mezinárodním prostředí, je nutné se nejprve seznámit s jejími

---

Australian National University Cybercrime Observatory, 2013, (May 16), str. 2. Dostupné z http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

[4] V letech 2009 až 2013 se zvýšilo procento připojení k Internetu o 27%. BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 2. Dostupné z http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

[5] Tamtéž.

[6] Především jde o materiál dětské pornografie, podněcování a podpora terorismu a porušování autorského práva a práv souvisejících.

[7] *Comprehensive Study on Cybercrime* [online]. United Nations Office on Drugs and Crime, 2013, str. 26. Dostupné z https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [cit. 2016-03-10]. Překlad autorka.

[8] KONRÁD, Zdeněk; PORADA, Viktor; STRAUS, Jiří; SUCHÁNEK, Jaroslav. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2015, str. 15.

specifickými vlastnostmi. První kapitola práce se zaměřuje na vývoj počítačové kriminality a její projevy, seznamuje čtenáře s užívaným pojmoslovím, definuje kriminogenní faktory a rozebírá v současnosti dostupné poznatky o jejích pachatelích i obětech. Druhá kapitola se věnuje zvláštnímu vztahu práva a kyberprostoru – osvětluje, proč vůbec vnímat právo ve virtuálním prostředí[9] jako legitimní regulační systém a zda je vynutitelné. Zaměřuje se na specifika působení trestněprávních norem v kyberprostoru, zejména z hlediska jurisdikce a závěrem na příkladech z mezinárodní praxe rozebírá některé jurisdikční konflikty. Třetí kapitola se soustředí na závažnou trestnou činnost s přeshraničním charakterem, jakou je organizovaný zločin a terorismus a zodpovídá otázku, zda existuje spojení počítačové kriminality a organizovaného zločinu, potažmo počítačové kriminality a terorismu. Kapitola rozebírá i mezinárodní instrumenty zaměřené na boj proti organizovanému zločinu a terorismu, které míří i na projevy skrze informační a komunikační technologie. Čtvrtá kapitola, v níž vycházím z vlastní diplomové práce, se věnuje vybraným procesním institutům českého trestního práva, které ovlivňují odhalování a vyšetřování počítačové kriminality v České republice. Poukazuje i na některá specifika a nedostatky právní úpravy. Jádrem rigorózní práce je kapitola pátá, pojednávající o mezinárodní justiční spolupráci v trestních věcech. Kapitola se zaměřuje na mezinárodní justiční spolupráci v užším slova smyslu, tj. mezinárodní právní pomoc, a na specifika mezinárodní spolupráce při postihu počítačové kriminality. Kapitola pojednává o pramenech právní úpravy z pohledu českého práva, práva Evropské unie i mezinárodního práva veřejného a závěrem upozorňuje na problematické aspekty mezinárodní praxe, která leckdy nevyhovující úpravu mezinárodní justiční spolupráce obchází. Nechybí ani vlastní vyjádření se k předpokládanému vývoji v oblasti, selžou-li právní mechanismy mezinárodní spolupráce.

[9] Pro účely práce jsou pojmy kyberprostor, kybernetické prostředí či virtuální prostředí užívány synonymně.

1. POČÍTAČOVÁ KRIMINALITA – VSTUP DO PROBLEMATIKY

Trestná činnost spojená s výpočetní technikou, počítači a světem moderních technologií obecně bývá pro převážnou část právnické odborné veřejnosti oblastí, které se snaží vyhnout. Nadšenců do světa technologií sice mezi právníky postupně přibývá, avšak v profesní komunitě aplikující především trestní právo hmotné a procesní převládá vůči kriminalitě spojené s počítači nedůvěřivost a vědomé přehlížení.

První kapitola rigorózní práce pojednává o rozsáhlé problematice počítačové kriminality. Vysvětluje pojmy, s nimiž se právnická odborná veřejnost v oblasti setká, a nabízí rozbor vybraného pojmosloví a souvisejících teoretických i praktických problémů. Pomocí historického vývoje představí transformaci počítačové kriminality a nové způsoby páchání trestné činnosti. Nevyhýbá se ani problematice pachatele a oběti počítačové kriminality, tedy oblasti, v níž bude zapotřebí v budoucnu zvláště doplnit nedostatečné poznatky rozsáhlým výzkumem. Kapitola dále poukazuje ve zkratce na specifika páchání trestné činnosti na Internetu a problematiku průniku trestné činnosti do kyberprostoru doplňuje v závěru poznatky o informační a kybernetické válce a kyberterorismu.

1.1. Základní pojmy

Počítačová kriminalita je oblastí, v níž se prolínají právní pojmy s technickými. Část technických pojmů v právní nauce zdomácněla a užívá se jich jako notoriet, byť jejich původní význam může být chápán různě.[10] V souvislosti s technologickým pokrokem se mění obsah a význam řady pojmů, některé neobstojí a bývají proto nahrazeny.

Propojení technologického vývoje a rigidní právní úpravy působí v každodenní právní praxi značné komplikace. Přetrvávající nejasnosti v používané české terminologii vedou k mnohému nedorozumění. Již roku 1995 napsali autoři jedné

[10] Pojmy jako software, počítač, či počítačový program se objevují v právních předpisech – výběrem v zákoně č. 40/2009 Sb., trestní zákoník, zákoně č. 121/2000 Sb., autorský zákon, zákoně č. 89/2012 Sb., občanský zákoník. Jejich jednoznačnost je sporná. Například pro pojem *software* uvádí Smejkal třináct možných definic. Viz SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Aleš Čeněk, 2015, str. 25-27.

z prvních publikací na téma počítačové kriminality u nás, že neexistuje jasná shoda v tom, co vlastně počítačovou kriminalitou je.[11]

Ani o 22 let později není situace jasnější. Statistiky vedle sebe srovnávají pojmy jako počítačová kriminalita, zneužití počítače a skimming.[12] S terminologickou entropií se setkáváme v teoretických publikacích i právních předpisech, autoři užívají totožných pojmů, avšak jejich obsah chápou různě. Posun v terminologii se vztahem k počítačové kriminalitě je patrný především v závislosti na času publikace textu. Typický je posun od pojmu počítačová kriminalita směrem ke kybernetické kriminalitě.

Hovoříme-li o spojení trestného činu a počítače, setkáváme se v literatuře často s termíny počítačová kriminalita, informační kriminalita, či nejaktuálněji kybernetická kriminalita.[13] Autoři i širší veřejnost je běžně zaměňují, používají jako synonyma anebo jejich obsah chápou a vykládají různě, což lze hodnotit jako negativní jev, neboť neutříděné pojmosloví k jednodušší orientaci v problematice nepřispívá.

S ohledem na rozsah předkládané práce definuje následující text jen část z množství pojmů, které považuji za stěžejní pro orientaci v dalším textu i problematice jako takové. Uvědomuji si existenci neohraničeného množství různých definic týchž pojmů, které nalézáme jak v odborné literatuře, tak v právních normách či normách technické povahy. Dále se proto zaměřuji na nejdůležitější z nich, a to včetně definic objevujících se v platné právní úpravě. Výběrovým kritériem se stala přehlednost, jednoduchost a pochopitelnost vybraných definic.

Pro snazší pochopení, co představuje počítačová, informační či kybernetická kriminalita, je zapotřebí vysvětlení základních pojmů. Jimi jsou především počítač, data a informace.

---

[11] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 99.

[12] Skimming je útok na bankovní účty klientů bank za použití informačních a komunikačních technologií. Pojmy uvádí srovnávací tabulka odhadu expertů na četnost aktivit organizovaného zločinu. Viz CEJP, Martin et al. *Společenské zdroje vývoje organizovaného zločinu*. 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 149.

[13] Pojem kybernalita, který používá jako zkratku pro kybernetickou kriminalitu Jirovský, se mezi širší odbornou veřejností neujal. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007.

1.1.1. Počítač

Pojem počítač lze široce chápat jako *„každý programovatelný stroj, který může provést naprogramovaný seznam instrukcí a reagovat na pokyny zadávané z vnějšku, přičemž zpracovává určitá data, zadaná prostřednictvím vstupních zařízení a výsledky prezentuje pomocí výstupních zařízení“*.[14] Pojmem počítač nestačí rozumět pouze osobní počítač či dřívější velké sálové počítače, ale též mobilní telefon nebo jiná zařízení, která mohou být součástí vybavení dopravních prostředků nebo domácích spotřebičů.[15] Vyjdeme-li z jiné, jednodušší definice, můžeme počítačem rozumět *„jakýkoliv stroj, který dokáže tři věci: přijímá strukturovaný vstup, zpracovává jej podle předepsaných pravidel a produkuje výsledky jako výstup“*.[16] Uvedená definice je stará přes 23 let a přesto stále platná. Právě díky jednoduchosti a uplatnitelnosti na širokou škálu zařízení od jednodušších až po přístroje využívající nejnovější technologie z citované definice vycházím v přístupu k počítačové kriminalitě, který klade důraz na počítačové zařízení. Jiná východiska, jak uvádím dále, akcentují virtuální prostor. Přístup zdůrazňující virtuální prostor, který převládá v posledních letech, bude pro mezinárodní praxi možná výrazněji využitelným. Státy se v přístupu k mezinárodní bezpečnosti liší, a právě USA spolu s Evropskou unií (dále též „EU“) kladou důraz na ochranu svého kyberprostoru, oproti obecné ochraně informace jako takové. [17]

Synonymem k pojmu počítač je počítačový systém, tj. funkční jednotka sestávající z jednoho či více technických zařízení s programovým vybavením.[18] Počítač a počítačový systém práce užívá jako synonyma. Úmluva Rady Evropy o počítačové

[14] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 22.
[15] Jde o koncept tzv. internetu věcí (Internet of Things – zkratka IoT). I taková zařízení, jako je např. televizor, lze považovat za počítač, který se může stát nástrojem k protiprávní činnosti. Lze uvést aféru z roku 2015, týkající se televizoru zn. Samsung, který bez vědomí uživatelů zaznamenával a zpracovával audio signály ze svého okolí. Technologie zjednodušující ovládání umožnila behaviorální analýzu dat pro marketingové účely, což vyvolalo obavy z neoprávněného zasahování do soukromí. Dostupné z http://techxplore.com/news/2015-02-samsung-smart-tvs-subject-blog.html [cit. 2016-02-18].
[16] *Slovník výpočetní techniky*. 1. vyd. Praha: Microsoft Press, Plus s.r.o., 1993, str. 81.
[17] Východisko je poplatné na poli kybernetické bezpečnosti a bezpečnosti sítí komunikačních a informačních technologií. EU vymezila svůj „kybernetický prostor“ již v Usnesení Evropského parlamentu ze dne 15. června 2010 o řízení internetu: další kroky [2009/2229(INI)]. Úřední věstník (2011/C 236 E/05). I ČR se soustředí na ochranu svého kybernetického prostoru, a to v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.
[18] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. vyd. Praha: C.H. Beck, 2004, str. 63.

kriminalitě (dále též „Úmluva o počítačové kriminalitě“)[19] obsahuje vlastní definici počítačového systému jako *„jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu“*.[20]

Nezbytnou složkou počítače je jeho vybavení, a to vybavení fyzického charakteru, neboli hardware, a vybavení programové, neboli software. Hardware jako součást informačních technologií představují technické prostředky, zejména počítače, přídavná, komunikační a rozšiřující zařízení.[21] Software či počítačový program jsou, jednoduše řečeno, instrukce, díky nimž hardware, tj. fyzický počítač, pracuje.[22]

1.1.2. Data, informace, informační systémy, informační a komunikační technologie

Pojmu data, z latinského *dare*, tj. dát, se v kontextu počítačové vědy užívá tradičně jako označení čísel, textu, zvuku i jiných smyslových vjemů reprezentovaných v podobě, která je způsobilá zpracování počítačem.[23] Data vyjadřují skutečnost, názory a myšlenky, mají potenciál být informací. Úmluva o počítačové kriminalitě definuje počítačová data jako *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem“*.[24] Provozními daty 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*

[19] Úmluva Rady Evropy č. 185 ze dne 23. listopadu 2001 o počítačové kriminalitě. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 104/2013 Sb. m. s. Anglické a francouzské znění dostupné z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. [cit. 2016-02-01]. Název v oficiální anglické verzi je „*Convention on Cybercrime,* “ nikoli „*Convention on Computer Crime*,“ podobně v oficiální francouzské verzi „*Convention sur la cybercriminalité*.“ Přiléhavějším by již v době přijetá byl překlad Úmluva o „kybernetické“ kriminalitě.
[20] Čl. 1 písm. a) Úmluvy o počítačové kriminalitě.
[21] HINDLS, Richard; HOLMAN, Robert; HRONOVÁ, Stanislava. *Ekonomický slovník*. 1. vyd. Praha: Beck, 2003. str. 135.
[22] *Slovník výpočetní techniky*. 1. vyd. Praha: Microsoft Press, Plus s.r.o., 1993, str. 346.
[23] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 31.
[24] Čl. 1 písm. b) Úmluvy o počítačové kriminalitě.

služby.“[25] Provozní data chápeme jako tzv. metadata, což jsou data poskytující informace o jiných datech.[26] Zajištění metadat považuje Úmluva o počítačové kriminalitě za menší zásah do soukromí, neboť neodkrývají příslušný obsah komunikace osob.[27]

Data jsou ukládána na nosičích dat - paměťových médiích, která uchovávají data využívajíce některého z fyzikálních principů.[28] V širším smyslu lze za nosič dat považovat i operační paměť počítače nebo síťová datová úložiště, včetně populárního způsobu užívání počítačových technologií, tzv. cloud computing. Jde o webové úložiště umožňující uživatelům ukládat a sdílet data s ostatními uživateli sítě.[29] Populární je využívání technologie ke sdílení nelegálního obsahu.

Latinský termín *informatio*, tj. představa či poučení, dal vzniknout pojmu informace. Jednoznačná definice informace neexistuje. Lze však souhlasit s vymezením informace jako způsobu a míry uspořádanosti určitého jevu, rozpoznatelné v daném okamžiku jejím příjemcem.[30] Vlivem kybernetiky[31] přestala být informace chápána pouze ve spojení s lidským myšlením a stala se synonymem pro poznání vnější reality lidmi i stroji a předpokladem lidské i strojové komunikace.[32] Podstatou informace je systematická organizace poznávaného. Norbert Wiener, zakladatel kybernetiky, staví informaci do kontrastu k entropii, veličině míry neuspořádanosti určitého systému; informaci chápe jako zápornou entropii.[33] Informace stojí kvalifikačně výše nežli data,

---

[25] Čl. 1 písm. d) Úmluvy o počítačové kriminalitě.
[26] *Česká terminologická databáze knihovnictví a informační vědy* [online]. Dostupné z http://aleph22.nkp.cz/F/?func=file&file_name=find-b&local_base=ktd [cit. 2016-02-23].
[27] *Explanatory report to the Convention on Cybercrime (ETS No. 185)* [online]. Treaty Office. Council of Europe, 2001, bod 29. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-02-23]. Překlad autorka.
[28] V minulosti rozšířené diskety či magnetické pásky představují magnetická média, na optickém principu jsou založena CD, DVD či Blue-ray disky, typickým příkladem elektronického media je USB flash paměť.
[29] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 55.
[30] Tamtéž, str. 36.
[31] Zakladatel kybernetiky Norbert Wiener odvodil její název roku 1947 z řeckého překladu slova kormidelník a definoval ji jako *„vědu o řízení a komunikaci v živých organismech a strojích.“* Viz JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 17.
[32] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 34.
[33] POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 13.

která nemusí být vždy informací. Nicméně i absence dat může být v určitém kontextu informací.[34]

Informační systém zahrnuje podle Smejkala, Sokola a Vlčka informační dokumenty (nosiče informací), informační pracovníky a informační procesy. Informačními činnostmi jsou všechny činnosti, jimiž se manipuluje s informacemi, a vztahy mezi nimi.[35] Pozitivem této definice je technologická nezávislost. Definici je možno vztáhnout na fyzické i elektronické informační systémy bez ohledu na využití technického či programového zpracování. Ochranu dle ustanovení zákona č. 40/2009 Sb., trestní zákoník (dále též „trestní zákoník" či „TZ") požívají toliko informační systémy vedené automatizovaným způsobem.[36]

Informačními technologiemi předkládaná práce rozumí využívání počítačů a elektroniky k ukládání a zprostředkování informací. S rozvojem počítačových sítí, v jejichž rámci dochází ke vzájemné komunikaci počítačových systémů, byl původní koncept doplněn o prvek komunikace. V zahraniční literatuře se setkáváme se zkratkou ICT.[37] Termín označuje informační a komunikační technologie, tedy *„hardwarové a softwarové prostředky pro sběr, přenos, ukládání, zpracování a distribuci dat."*[38] V návaznosti na vývoj terminologie obohacené o prvek komunikace užívá další text pojmu informační a komunikační technologie (dále též „ICT").

1.1.3. Kyberprostor a počítačová síť

Podstatná část počítačové kriminality se v současnosti odehrává v rámci virtuálního světa počítačových sítí, pročež jí mnozí nazývají kriminalitou kybernetickou. Díky globálním počítačovým sítím vznikají podmínky pro pozvolné přetváření trestné činnosti. Kybernetické prostředí nabízí pachatelům trestných činů příležitosti dříve netušené. Samotné páchání trestné činnosti v kyberprostoru postrádá řadu překážek přítomných ve světě fyzickém. Prostředí globálních počítačových sítí,

[34] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 38.
[35] Tamtéž, str. 198.
[36] Tamtéž, str. 43.
[37] V angličtině „*Information and Communication Technologies*".
[38] HINDLS, Richard; HOLMAN, Robert; HRONOVÁ, Stanislava. *Ekonomický slovník*. 1. vyd. Praha: Beck, 2003. str. 161.

definované pro účely práce jako kyberprostor, si z uvedeného důvodu zasluhuje větší pozornost trestního práva. Jen detailní znalost specifik kybernetického prostředí umožní vytvářet kvalitnější právní úpravu i efektivněji stíhat významnější části počítačové kriminality. Alespoň základní orientace v problematice virtuální reality, tj. kybernetického prostředí, je pro studium počítačové kriminality klíčová.

Kyberprostor představuje metaforu pro prostor vytvářený počítačovými systémy. Stejně jako v reálném světě se i v kyberprostoru nachází různé objekty - složky, e-mailové zprávy, obrázky apod. Na rozdíl od reálného prostoru však využívání kyberprostoru nevyžaduje jiného fyzického pohybu než stlačení příslušných kláves nebo pohybu myší.[39]

Předpona kyber[40] odkazuje na koncept řízení a kontroly elektronických dat, daný možností manipulace s daty. Pojem prostor evokuje virtuální místo, ve kterém dochází k interakci dvou či více lidských aktivit.[41] Kyberprostor zahrnuje Internet jako celek i veškerá globální média a komunikační kanály. Kyberprostor je širším pojmem než Internet, neboť zahrnuje veškerá myslitelná zařízení kontrolovaná počítačovým programem, která však nemusí být napojena na síť Internet.

Slovem kyberprostor popsal americký spisovatel William Gibson fiktivní svět a jazyk v románu Neuromancer z roku 1984, tedy zhruba dekádu před informační revolucí a světovým rozšířením internetu.[42] Teprve Barlow v roce 1990 užil pojmu kyberprostor jako *„v daném čase aktuální nexus mezi počítačem a telekomunikačními sítěmi“*.[43]

Počítačovou sítí rozumíme technické a programové prostředky, zajišťující spojení a výměnu informací mezi jednotlivými počítači.[44] Podle geografické vzdálenosti počítačů můžeme počítačové sítě rozdělit na lokální (v angličtině označované jako

[39] AWAN, Imran; BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012, str. 5. Překlad autorka.
[40] Předpona *kyber* je odvozena z řeckého termínu *kybernetes*, tj. v českém jazyce kormidelník, vladař, pilot. ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 34.
[41] AWAN, Imran; BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012, str. 5. Překlad autorka.
[42] ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 30.
[43] BARLOW, John Perry. *Crime and Puzzlement: in advance of the law on the electronic frontier*. Whole Earth Review, 1990. str. 44 – 57. Překlad autorka.
[44] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 45.

Local Area Network, dále jen „LAN“) i vzdálené (Wide Area Network, dále jen „WAN“). LAN je popisována jako počítačová síť zřízená u uživatele ve vymezené geografické oblasti, například v domácnosti, kavárně či podniku, ale také jako počítačová síť, jejíž uživatel je shodný s provozovatelem sítě. WAN naopak umožňuje komunikaci počítačů v geograficky oddělených a vzdálenějších oblastech. Jejím nejznámějším příkladem je právě Internet. Jednotlivé počítače se přímo k WAN nepřipojují, neboť to se děje za pomoci LAN. Jako osobní síť, tedy *Personal Area Network* (dále jen „PAN“), bývá označován stále častější jev několika osobních počítačových zařízení jediného uživatele či skupiny uživatelů (např. v domácnosti), která spolu prostřednictvím sítě komunikují. Rovněž na IoT[45] lze nahlížet jako na komunikační síť, s *ad hoc* vznikající architekturou.[46]

Trestněprávní předpisy užívají pojmu veřejně přístupná počítačová síť. Spáchání konkrétního trestného činu veřejně přístupnou počítačovou sítí dle výkladového ustanovení § 117 písm. a) TZ implikuje veřejné spáchání trestného činu, z čehož dovozujeme vyšší míru závažnosti činu. Uvedené může být znakem základní skutkové podstaty trestného činu nebo kvalifikační okolností podmiňující použití vyšší trestní sazby.[47] Veřejně přístupná počítačová síť dle zákonodárce značí *„funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy.“*[48] Zatímco výše zmíněné dělení počítačových sítí na lokální a vzdálené vychází z geografického rozmístění jednotlivých „uzlů“, tj. počítačů v síti, pro kvalifikaci veřejně přístupnou počítačovou sítí bude podstatné, zda je počítačová síť veřejnosti skutečně přístupna či nikoli.

Výkladové ustanovení § 117 TZ vymezuje taxativním způsobem, kdy je trestný čin spáchán veřejně. S ohledem na možný široký výklad kategorie „jiného obdobně účinného způsobu“ lze dopad ustanovení vnímat poměrně dalekosáhle. Šámal uvádí příkladem jiného obdobně účinného způsobu nahrávku na CD či DVD, jestliže je

[45] Srov. cit. bod 15.
[46] Podrobněji SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 45-47.
[47] Například přečin neoprávněného nakládání s osobními údaji dle § 180 odst. 1 či 2, odst. 3 písm. b) TZ, přečin pomluvy dle § 184 odst. 2 TZ, či přečin šíření pornografie dle § 191 odst. 1 či 2, odst. 3 písm. b) TZ.
[48] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1300.

zpřístupněna většímu počtu posluchačů nebo diváků.[49] Domnívám se, že s ohledem na technologický vývoj bude možné za „jiný obdobně účinný způsob" považovat jakékoli médium pro přenos informací či obdobně funkční software (např. hostingové[50] služby), jejichž obsah bude zpřístupněný většímu počtu recipientů, pokud nepůjde o veřejně přístupnou počítačovou síť. V případě sítě veřejnosti nepřístupné, přesto však dostupné širokému okruhu osob, by bylo možné říci, že půjde právě o spáchání trestného činu „jiným obdobně účinným způsobem" ve smyslu výkladového ustanovení § 117 písm. a) TZ.[51]

1.1.4. Internet

Neexistuje všeobecně přijímaná definice Internetu, a výjimkou není ani český právní řád. Absenci právní definice za nedostatek ale nepovažuji. Legislativu co nejvíce nezávislou na technologii, tj. technologicky neutrální, by právníci měli vnímat jako kladný jev. Technologický vývoj není možné dostatečně určitě předpovědět ani jej „svázat" právními definicemi. Fakt, že ne vždy se snaha o co nejpřesnější právní definici vyplatí, dokládá zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále též „ZEK"), který považuje Internet za veřejnou informační síť a tuto neobratně definuje.[52]

Definice Internetu jako informační sítě může být zavádějící. Polčák poukazuje na nesprávnost myšlenky, podle které považujeme Internet *a priori* za prostředí informační.[53] Internet není perfektně organizován, ne každý paket dat je zároveň informací. Naopak, Internet je zahlcen masou chybných a nadbytečných dat. Internet je prostředím spíše entropickým, kde se některým uživatelům informaci nalézt podaří.

---

[49] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1301.
[50] Služby informační společnosti umožňující ukládání digitálních dat.
[51] Srov. stanovisko Nejvyššího soudu ze dne 30. 1. 2013, sp. zn. Tpjn 300/2012, uveřejněné pod číslem 20/2013 Sbírky soudních rozhodnutí a stanovisek, část trestní.
[52] Dle § 2 písm. h) ZEK jde o *„síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací, a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání."*
[53] POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 14.

Z technologického hlediska představuje Internet celosvětový systém jednotlivých propojených počítačových sítí, v jehož rámci spolu komunikují počítače pomocí rodiny protokolů TCP/IP.[54] S trochou nadsázky lze říci, že každý, kdo ovládá jazyk, může se volně zapojit do komunikace. V současnosti se celkový počet uživatelů Internetu odhaduje na tři miliardy.[55]

Architektura Internetu měla v době jeho vzniku zajistit obranu vůči vnějším zásahům a cenzurním snahám.[56] Zatímco v počátcích představoval uživatelský substrát odborníky a nadšené zasvěcence více méně respektující specifická pravidla a morální normy, s celosvětovým rozmachem Internetu a nárůstem uživatelů neregulovaného prostředí se objevuje i užívání společensky těžko akceptovatelné. Brzy proto zazněly požadavky na (důslednější) kontrolu prostředí Internetu.

Internet jako takový právně neexistuje. Z pohledu práva nelze hovořit o věcné povaze, neboť ačkoli slouží potřebě lidí, nelze jej ve smyslu vlastnického práva ovládat ani si jej přivlastnit.[57] Smejkal poznamenává, že *„Internet se skládá z různých subjektů práva: lidí a organizovaných sdružení lidí (právnických osob) včetně státu a dále z majetku, tj. věcí a práv. Problémem je, že na rozdíl od automatizovaných informačních systémů netvoří technické a programové prvky a lidé s nimi pracující určitou společenskou celistvost, tj. instituci, která může být subjektem práva.“*[58] Z uvedených znaků plyne problematická kontrola Internetu jakožto prostředí, v němž je právo chráněno. I vymahatelnost deliktní odpovědnosti za chování uživatelů je značně ztížena.

[54] TCP/IP je zkratka pro anglické termíny Transmission Control Protocol/Internet Protocol, neboli primární přenosový protokol a přenosový protokol, přenášející data.
[55] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 52.
[56] Předchůdcem Internetu byla na konci 60. let síť ARPANET (the Advanced Research Projects Agency Network) sponzorovaná armádou USA. Síť spojovala výzkumná univerzitní pracoviště a komunity s vládními agenturami. Cílem bylo umožnit bezpečný a odolný prostředek vojenské komunikace. Technologie umožnila „rozbít“ komunikaci na menší části, tzv. pakety, které cestovaly různými cestami k adresátovi, kde byly složeny do původní podoby. Právě variabilita možných cest zajišťuje větší odolnost sítě. YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013, str. 7. Překlad autorka.
[57] § 489 zákona č. 89/2012 Sb., občanský zákoník.
[58] SMEJKAL, Vladimír. Internet *a §§§*. 1. vyd. Praha: Grada, 2001, str. 17 – 18.

1.1.5. Počítačová kriminalita, trestné činy v informační vědě a kybernetické trestné činy

Co se dělících kritérií pojmů kriminality počítačové, kybernetické, kyberkriminality, kriminality informační, kriminality v informační vědě a dalších obdobných podob trestné činnosti týče, nepanuje zde jasná shoda. V literatuře se setkáme v různé míře se všemi uvedenými termíny. Autorův subjektivní přístup ovlivňuje i preferovanou terminologii díla.

Termín počítačová kriminalita se objevuje na počátku 90. let, kdy počítač představoval vrchol vývoje v oblasti elektroniky. Nazývat trestnou činnost vztahující se k počítačům jinak než počítačovou kriminalitou se zdálo nemyslitelné. Část autorů, předpokládaje nezbytný prvek odborné znalosti při páchání tohoto druhu trestné činnosti, navrhovala termín trestný čin v informační vědě.[59] Například Picotti rozlišuje mezi trestnými činy v informační vědě (infractions informatiques) a kybernetickými trestnými činy (infractions cybernétiques). Zatímco objektivní stránku prvních charakterizuje fakultativní znak spočívající v určitém využití ICT zvyšující typovou závažnost daného trestného činu, kybernetické trestné činy se dle Picottiho odehrávají toliko ve virtuální realitě kybernetického prostředí.[60] S nástupem pozdějších generací trestných činů vyskytujících se v návaznosti na počítačovou vědu (k vývojovým generacím srovnej níže) v zásadě teorie přestává prvotního termínu počítačové kriminality ve větším měřítku užívat, resp. termín již nevnímá jako kategorii zahrnující veškeré představitelné formy uvedené trestné činnosti.

Počítačovou kriminalitu vymezili autoři jedné z prvních publikací věnujících se této problematice u nás, následovně: *„Pod pojmem „počítačová kriminalita“ je třeba chápat páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité, nebo jako nástroj*

[59] ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 32 - 33.
[60] PICOTTI, Lorenzo. *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l´informatique*. Ramonville Sainte Agne: Révue internationale de droit pénal, 2006, str. 529 – 533. Překlad autorka.

trestné činnosti.“[61] Definice budí dojem relativně obsáhlé množiny trestných činů, splňujících uvedený široký definiční znak - určitý vztah k počítačovému systému. Počítačový systém představuje předmět útoku nebo nástroj - tehdy se stává prostředkem umožňujícím páchání trestné činnosti. Uvedená definice počítačové kriminality staví do centra pozornosti počítač. Toliko v návaznosti na šířce vymezení termínu počítače lze citovanou definici počítačové kriminality považovat za velice univerzální, pojímající v sobě zároveň i kriminalitu kybernetickou.

Termín kybernetické kriminality do centra pozornosti počítač nestaví. Klade důraz na využívání komunikačních a informačních technologií a především na virtuální prostor, tj. kyberprostor. Právě v rámci kyberprostoru dochází ke spáchání deliktu. Vývojově pozdější termín odráží rozvoj technologií, počítačové vědy, včetně počítačových funkcí. Nesmíme ovšem zapomenout na následující: abychom mohli v kyberprostoru jakýmkoli způsobem jednat, potřebujeme počítač. Kyberprostor vzniká právě díky jednotlivým počítačům. Bez počítačů není ani kyberprostoru. Z tohoto úhlu pohledu musí v kybernetické kriminalitě určitým způsobem pokaždé figurovat i počítač a každý případ kybernetické kriminality bude možné označit taktéž kriminalitou počítačovou. Předkládaná práce z tohoto důvodu vnímá pojem počítačové kriminality v kontextu dalších termínů jako termín představující nejširší možnou množinu trestných činů. Na druhé straně rozeznává i negativa zmíněného pojetí. Přespříliš široký přístup nemusí být do budoucna udržitelným. S dalším rozvojem počítačových technologií se využívání počítačových systémů v každodenním životě stane natolik rozšířeným, že bude možné podřadit pod takto širokou definici počítačové kriminality takřka cokoli. Tímto okamžikem by však definice ztratila svůj smysl, neboť by nevyjádřila nic odlišného a tedy nic podstatného.

Významným nedostatkem definice počítačové kriminality autora Smejkala, Sokola a Vlčka je návaznost na počítač v podobě nástroje. *Ad absurdum* by bylo možné považovat za projev počítačové kriminality každý trestný čin, v jehož rámci by nějakým způsobem došlo k využití počítače jako nástroje, například k získání informací umožňujících spáchat trestný čin, k vytipování obětí, k bezhotovostnímu převodu peněžní částky apod. Následně by bylo možné podřadit pod termín počítačová kriminalita obsáhlou množinu trestných činů. Nad rámec lze citovat Završnika, podle

[61] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 99.

kterého není zvykem v právní teorii specifikovat kategorii trestných činů podle použitých prostředků.[62]

Termín počítačová kriminalita má obdobný charakter jako termíny násilná kriminalita, kriminalita mladistvých apod. Charakterizuje skupinu trestných činů se společným faktorem, jakým je např. způsob provedení.[63] Podřazení kriminality pod počítačovou by mělo poukázat na specifický znak. Ten by dle mého názoru měl být natolik relevantní, aby vyloučil hraniční případy trestné činnosti, které by již pod uvedenou definici spadat neměly. Za dostatečně relevantní praxe například nepovažuje, figuruje-li v deliktu počítač pouze jako penězi ocenitelný předmět, neboť v takovém případě je skutková podstata vesměs shodná s trestnými činy kategorie majetkové kriminality.[64] Relevantním znakem by naopak mohl být počítač figurující v trestné činnosti právě díky svým technologickým funkcím.

Podíváme-li se však na věc z pohledu kriminalistiky,[65] využitím počítače jako nástroje k trestnému činu, byť okrajově, dochází ke vzniku kriminalistických stop,[66] které jsou stěžejní při vyšetřování trestného činu, ačkoli pachatel mohl počítače využít jen jako dílčího nástroje a předmětný delikt by mezi počítačovou kriminalitu spadat jinak nemusel.[67] Z uvedených důvodů bývá stanovení bezpečné hranice toho, co lze ještě považovat za relevantní znak počítačového deliktu a co již nikoli, velice obtížným. Proto může být vhodnější vycházet při stanovení konkrétní definice z jejího konkrétního smyslu v předkládaném díle. Pro statistické účely se zdá vhodnější vycházet z definice užší, nežli pro účely vyšetřovací. Předkládaná práce vychází z širokého pojetí počítačové kriminality tak, jak je vymezeno výše.

[62] ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 32.
[63] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 99.
[64] Srov. trestný čin krádeže dle § 205 TZ, zpronevěry dle § 206 TZ aj. K problematickým aspektům počítačové kriminality ve vztahu k počítači jako věci movité SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 100 a násl.
[65] Kriminalistika je nauka zabývající se vznikem, trváním a zánikem stop a jiných kriminalisticky relevantních informací o trestných činech, jakož i jejich vyhledáváním, zkoumáním a zajišťováním.
[66] Vznikají stopy materiální, jako jsou např. otisky prstů na vnější struktuře zařízení. Typické jsou především specifické stopy digitální.
[67] Pachatel trestného činu vydírání dle § 175 TZ, spáchaného jinak bez využití počítače, shromáždí na svém počítači či paměťovém médiu sérii vysoce choulostivých fotografií vydírané osoby.

1.1.5.1. Kybernetická kriminalita

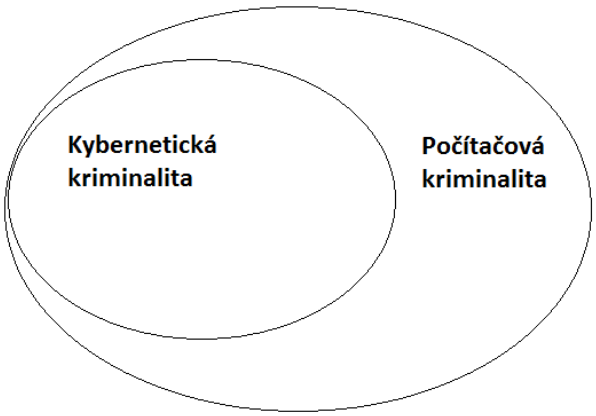
Pojem počítačová kriminalita je však podle některých autorů považován za příliš úzký.[68] I vlivem anglické verze Úmluvy o počítačové kriminalitě se v českém prostředí rozšířil termín kyberkriminalita, který se zdá přiléhavější pojmu cybercrime používanému v oficiálním anglickém znění.[69] Někteří autoři užívají paralelně k pojmu cybercrime český pojem kybernetická kriminalita, načež jej nevhodně vymezují definicí počítačová kriminalita autorů Smejkala, Sokola a Vlčka.[70] Smejkal nyní užívá termínu kybernetická kriminalita. Naznačuje tím, že těžištěm útoku již není počítač, ale kyberprostor tvořený počítačovými sítěmi a jejich jednotlivými prvky, ve kterém spolu komunikují veškerá zařízení ovládající protokol TCP/IP.[71] Picotti obdobně vyděluje trestné činy odehrávající se ve virtuální realitě kybernetického prostoru.[72] Pojmy kyberkriminalita a kybernetická kriminalita užívá předkládaná práce synonymně.

S ohledem na řídící princip trestního práva *lex certa* není vhodné pro oblast trestního práva měnit pojmosloví užívané trestním zákoníkem a Úmluvou o počítačové kriminalitě, která vymezuje pojmy počítačový systém, počítač, počítačová kriminalita. Právní jazyk by měl užívat termínů nezávislých na technologickém vývoji. V opačném případě budeme neustále nuceni vlivem vědeckého pokroku měnit nevyhovující právní normy. Naopak technologicky neutrální právní jazyk bude mít šanci obstát v rychlém technologickém vývoji po delší dobu, než právní norma navázaná na konkrétní technologický vývoj.[73]

Přestože jsem si vědoma odlišného pojetí některých autorů, termín počítačová kriminalita užívám ve své práci v širším smyslu. Vycházím z výše citované definice Smejkala, Sokola a Vlčka. Kybernetickou kriminalitu vnímám jako logické označení

[68] ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 33.
[69] Termín *cybercrime* je v zahraničí chápán velice univerzálně, což usnadňuje komplikovanou terminologickou situaci.
[70] Takto ve svém díle činí POŽÁR, Josef. Příspěvek k rozvoji informatiky v oblasti kybernetické kriminality. *Bezpečnostní teorie a praxe: periodikum Policejní akademie České republiky*. 2008, Díl I. (Zvláštní číslo), str. 8.
[71] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 15.
[72] PICOTTI, Lorenzo. *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l´informatique*. Ramonville Sainte Agne: Révue internationale de droit pénal, 2006, str. 529 – 533. Překlad autorka.
[73] Příkladem nevhodné podoby právní normy, úzce navázané na technologický stav věci, je např. definice služby elektronických komunikací v § 2 písm. n) ZEK.

počítačové kriminality, kde se těžiště trestné činnosti nachází v kyberprostoru. Zpravidla půjde o mladší generace počítačových trestných činů. Nikoli každý případ počítačové kriminality bude nutně kybernetickou kriminalitou.[74] Pro přehlednost uvádím graf prolnutí obou termínů:



Příloha č. 1: Vztah kybernetické a počítačové kriminality.

Vycházím z teze, že bez počítačů není ani kyberprostoru. Počítačová kriminalita představuje nejširší kategorii, do níž spadá i kybernetická kriminalita. Užití pojmu kybernetická kriminalita naopak zdůrazňuje vyšší technologickou vyspělost deliktu a současně fakt, že se centrem zájmu již stal kyberprostor.

1.2. Historický vývoj

1.2.1. Transformace počítačové kriminality

John Austin, detektiv inspektor z New Scotland Yard v Londýně, na svém vystoupení na semináři „Ochrana výpočetní techniky a dat, počítačová kriminalita“ organizovaném Československou společností pro kriminalistiku dne 13. prosince 1990, uvedl jako demonstrativní příklad mezinárodního charakteru počítačové kriminality dnes již úsměvný případ. Jednalo se o pachatele, který v roce 1989 rozeslal do mnoha

[74] Typicky půjde o delikty, ve kterých nebude figurovat kyberprostor, ale předmětem či nástrojem trestné činnosti bude počítač. Příkladem může být mechanické poškození počítačového systému a způsobení značné škody na cizím majetku ztrátou nezálohovaných důležitých dat v počítačovém systému.

zemí světa nemocnicím, univerzitám a obchodním společnostem zabývajícím se výzkumem viru HIV, asi 25 000 disket, o kterých tvrdil, že obsahují důvěrné informace o pacientech trpících AIDS. Místo toho však diskety obsahovaly trojského koně, vir, který poškodil paměť dotčených počítačů.[75] Případ ukazuje nejenom na rozmanitost cest, které si pachatelé počítačové kriminality vybírají, ale i význam technologického vývoje, který jim cestu značně ulehčuje. Grabosky přiléhavě charakterizuje převážnou část počítačové kriminality jako „staré víno v nových lahvích.“[76]

Rozvoj a transformace počítačové kriminality jde ruku v ruce se společenským a technologickým vývojem. Bez vzniku sítě ARPANET, Internetu, i bez rozšíření osobních počítačů mezi širokou veřejnost by dnes nebylo možné hovořit o počítačové kriminalitě.[77] Historický vývoj počítačové kriminality je spojen s klíčovými momenty technologického vývoje.

Způsobů třídění počítačových trestných činů je mnoho. Austen dělil na počátku 90. let počítačové trestné činy do dvou skupin: v první skupině představoval počítač pouze prostředek k ukládání významných informací pro páchání určitého druhu trestné činnosti (např. informace bankovního charakteru), v druhé skupině figuroval počítač již jako předmět útoku; do této kategorie spadal hacking,[78] útoky virů, časované a logické bomby a jiné neoprávněné manipulace s počítačem.[79] Smejkal dělí kriminalitu v prostředí informačních systémů a na Internetu následovně:

- sabotáže a útoky na zařízení ICT
- trestná činnost, v níž je zařízení ICT nástrojem pro její páchání
- trestná činnost spojená se získáváním a šířením informací
- trestná činnost proti ochraně duševního vlastnictví v prostředí ICT
- ryze počítačová trestná činnost

[75] AUSTEN, John. Praktické příklady vyšetřování počítačové kriminality. *Kriminalistická společnost*. Praha, 1991, (3), str. 8 - 9.
[76] GRABOSKY, Peter. Virtual criminality: Old wine in new bottles? *Social and legal studies* [online]. 2001, (10), str. 243 – 249. Dostupné z http://sls.sagepub.com/content/10/2/243.full.pdf. [cit. 2016-02-18] Překlad autorka.
[77] První osobní počítač (anglická zkratka PC, tedy personal computer) vytvořila společnost IBM na konci 80. let 20. století. Viz KOLOUCH, Jan; VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České Republiky v Praze. 2013. str. 5.
[78] Detailněji viz kapitola 1.3.1.
[79] AUSTEN, John. Praktické příklady vyšetřování počítačové kriminality. *Kriminalistická společnost*. Praha, 1991, (3), str. 9.

- ostatní trestná činnost související s počítačem.[80]

Uvedené detailní dělení je praktického charakteru, autor jej pravděpodobně zvolil s ohledem na své letité zkušenosti soudního znalce v oblasti kybernetiky, kriminalistiky i ekonomie.

Pro představení historického vývoje v oblasti považuji za srozumitelnou a přiléhavou typologii počítačové kriminality britského kriminologa Davida Walla.[81] Wall představuje svoji tezi transformace kriminálních aktivit v propojené informační globální společnosti. Trestné činy zařazuje na pomyslnou časovou osu a rozděluje je do příslušných generací podle vztahu příležitosti k páchání trestné činnosti a technologického rozvoje v oblasti ICT. Generace dokládají vývoj včetně významných milníků v transformaci počítačové kriminality a rozdělení období do několika generací je vhodným interpretačním hlediskem. Každá generace má svou typickou charakteristiku, Wall se soustředí na stěžejní témata každé generace z hlediska kriminologie i trestního práva. Přístup umožňuje orientaci v široce vymezené kategorii počítačové kriminality. Následující text podrobněji rozebírá generace počítačových trestných činů dle Wallovy kriminologické typologie.

1.2.1.1. První generace počítačových trestných činů

Počítače mezi sebou zpočátku nebyly propojené skrze sítě. Trestné činy první generace jsou klasickými trestnými činy, které lze páchat běžným způsobem,[82] pachatel se však rozhodl k jejich spáchání využít počítače - počítač pouze usnadní spáchání trestného činu. Počítače mohou být využívány i v rámci přípravy jako nástroje komunikace mezi pachateli, nástroje k získání potřebných informací k provedení činu apod. Jako příklad počítačového trestného činu první generace lze uvést pokračující trestný čin zpronevěry dle § 206 TZ, kdy pachatel využívá mezer v designu počítačového programu, umožňujících mu opakovaně převádět na vlastní peněžní účet

[80] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015.
[81] WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 44 – 48. Překlad autorka.
[82] Běžným v tom smyslu, že v jednání pachatele nemusí jinak figurovat počítač.

z velkého počtu jednotlivých bankovních transakcí přebývající částky, neboť tyto nedosahují nejnižší určující hodnoty, kterou počítačový program již rozezná (pachatel dlouhodobě převádí přebývající desetiny haléřů). Jiným příkladem může být trestný čin padělání a pozměnění veřejné listiny dle § 348 TZ, pokud by pachatel přechovával specializovaný počítačový program ke snazšímu provedení jednotlivých padělků.

Klíčové pro první generaci počítačových trestných činů je východisko, dle něhož v případě neexistence počítače může trestný čin nadále existovat. Pachatel bude toliko nucen zvolit jiný nástroj k jeho úspěšnému dokonání. Uvedené trestné činy, označované též jako tradiční,[83] jsou ovšem v rámci první generace počítačové kriminality spáchány s využitím počítače, tj. nikoli běžným způsobem.

1.2.1.2. Druhá generace počítačových trestných činů

Roku 1990 byla síť ARPANET (viz výše) zpřístupněna široké veřejnosti a výzkumníci ve švýcarském institutu CERN[84] vyvinuli první webový prohlížeč. Počátkem 90. let došlo k masovému rozšíření sítě Internet a do pěti let vstoupili na nově se utvářející trh služeb informační a komunikační společnosti první poskytovatelé internetových služeb, aby nabídli majitelům počítačů připojení k „síti všech sítí“.[85] Následující léta zaznamenala masivní rozšíření osobních počítačů do většiny domácností vyspělého západního světa. Neomezené zpřístupnění Internetu k osobnímu a komerčnímu využití představovalo významný milník v rámci světové globalizace, technologického i společenského vývoje a dříve netušené možnosti vedly k nástupu nových příležitostí trestné činnosti.

Do druhé generace počítačových trestných činů řadí Wall známé běžné trestné činy, pro které znamená rozšíření sítě Internet nové příležitosti - nově jsou páchány napříč globální počítačovou sítí. Wall označuje tyto trestné činy jako tzv. hybridní.

[83] Z anglického „traditional“ nebo „ordinary crimes“. Viz WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 45. Překlad autorka.
[84] *Conseil Européen pour la Recherche Nucléaire*, neboli Evropská organizace pro jaderný výzkum, zřízená roku 1954 v Ženevě.
[85] CASTELLS, Manuel. *The internet galaxy: reflections on the internet, business, and society*. 1. vyd.Oxford: Oxford University Press, 2003, 292 s. Překlad autorka.

Prostředí veřejně přístupné globální počítačové sítě umožnilo pachatelům dosažení vyšších zisků i rozsáhlejších škod a bez překážek v masovém měřítku rozšiřovat ilegální obsah.

Příkladem uvedené trestné činnosti je šíření nelegální pornografie.[86] Vznikají webové stránky umožňující přístup k takřka neomezenému množství materiálů nejen dětské pornografie. Internetové aukční síně vytváří nové možnosti pro podvod. Předtím obtížně dostupné údaje, jako návody na výrobu syntetických drog, výbušnin a dalších nebezpečných materiálů, jsou mnohem snadněji dostupné. Klíčovou charakteristikou druhé generace je výrazně větší měřítko trestné činnosti a její extrémní dopad, který se s dobou před expanzí Internetu nedá srovnat.

Představíme-li si druhou generaci počítačové kriminality bez nových technologií, resp. bez globálního virtuálního prostoru v podobě internetových sítí, trestná činnost nevymizí, nýbrž uvedené škály ani zdaleka nedosáhne – rozsah trestné činnosti bude mnohem nižší.

1.2.1.3. Třetí generace počítačových trestných činů

Na přelomu 21. století byl nahrazen analogový způsob připojení k Internetu širokopásmovým, umožňujícím rychlejší přenos dat[87] i vyšší míru automatizace jednotlivých aktivit trestné činnosti. Třetí generace počítačových trestných činů existuje výlučně díky virtuálnímu prostředí vytvořenému počítačovými sítěmi. Poškození však účinky trestných činů citelně vnímají v reálném světě a dopad trestné činnosti bývá mimo kybernetické prostředí značný.

Představme si rozesílání spamů. Pojem spam[88] lze v širším významu chápat jako doručování jakékoli nevyžádané hromadné e-mailové korespondence,

[86] Např. přečin šíření pornografie dle § 191 odst. 1 nebo 2, odst. 3 písm. b), odst. 4 písm. a) TZ.
[87] Dříve rozšířené připojení přes telefonní linku pomocí modemu bylo založeno na analogovém principu. Modem převedl digitální signál na analogový, který přes telefonní linku vysílal k serveru. Rychlost analogového připojení je však omezená. Širokopásmové připojení (anglicky *broadband*) souvisí s vývojem v oblasti datových služeb; označuje se jím datové připojení k internetu rychlostí vyšší než definovaná rychlost (obvykle vyšší než 600 bitů/s).
[88] Pojem „spam“ vymysleli Monty Pythons roku 1970. Viz *Merriam-Webster Dictionary*. [online]. Dostupné z http://www.merriam-webster.com/dictionary/spam [cit. 2016-04-17]. Překlad autorka.

zpravidla reklamního obsahu.[89] Spam sám o sobě nepředstavuje ilegální aktivitu. Dokáže však uživatelům znepříjemnit práci s elektronickou schránkou, a to i jejím zahlcením. Jirovský uvádí až 90% podíl nevyžádané korespondence v naší elektronické poště.[90] Předmětem zájmu trestního práva se spam stane v okamžiku, obsahuje-li v příloze soubor se škodlivým programem, tj. malware.[91] Pomineme-li oprávněné testování bezpečnostního software, úkolem malware je určitým způsobem zasáhnout do počítačového systému a způsobit škodu. Zpravidla dochází k trestnému činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ.[92] Počítač napadený malware se může stát součástí tzv. botnetu[93] a dále být bez vědomí majitele využíván k automatizované trestné činnosti. Spam proto usnadňuje automatizovanou formu trestné činnosti, mezi níž patří například DDoS útoky[94] nebo hromadné rozesílání malware. O DDoS útocích se zmiňuje čl. 5 Úmluvy o počítačové kriminalitě jako o „zasahování do systému“.[95] Na jednání dopadá skutková podstata trestného činu poškození a ohrožení provozu obecně prospěšného zařízení v úmyslné i nedbalostní formě dle § 276 a § 277 TZ. Podle výkladového ustanovení dle § 132 TZ patří mezi obecně prospěšná zařízení i zařízení a sítě elektronických komunikací, což by mohl být server využívaný širokou veřejností, jehož užívání bude DDoS útoky ohroženo.

---

[89] WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 230. Překlad autorka.

[90] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 104.

[91] Z anglického „malicious software” - „škodlivý počítačový program“. Jedná se o počítačové viry, červy, trojské koně, skenerovací programy apod. Úkolem malware je zpravidla poškozování uložených počítačových dat, jejich změna, výmaz či špionáž. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. či KOLOUCH, Jan; VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou*. 1. vyd. Praha: Policejní akademie České republiky v Praze, 2013.

[92] Např. pachatel překoná bezpečnostní opatření omezující přístup za pomoci malware - např. spuštěním přílohy spamu se aktivuje malware, dojde k zásahu software a získání dat z počítače oběti (typicky díky tzv. *spyware*). Možný postih pro přečin neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a), d) TZ.

[93] Botnet je síť počítačů infikovaných malware, které mohou být administrátorem bez vědomí majitelů ovládány skrze počítačovou síť. Botnet tvoří velké množství infikovaných IP adres. Na černém trhu jsou ceněnou komoditou. Průměrná cena za 24hodinový pronájem roku 2010 činila 67 USD. Dostupné z http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/. [online]. [cit. 2016-02-16]. Překlad autorka.

[94] Z anglického „ ‚Distributed Denial of Service‘ attacks“. Jde o řízený útok velkého množství počítačů na konkrétní místo v síti pomocí přístupových požadavků. Přetížením dojde k zablokování stránky nebo i serveru a oprávněným uživatelům služby je znemožněn přístup. DDoS útočí např. hackerské hnutí Anonymous proti webovým stránkám vybraných společností.

[95] Anglický pojem „system interference“ evokuje spíše ohrožení nebo rušení. Musí dojít k úmyslnému neoprávněnému a závažnému omezení funkčnosti počítačového systému.

Třetí generace počítačových trestných činů tvoří trestné činy *sui generis*, které jsou páchány pouze v prostředí počítačových sítí. Někteří autoři mluví o tzv. hi-tech počítačových trestných činech, popřípadě o jádru kybernetické kriminality.[96] Odmyslíme-li si kyberprostor, v němž je možné uvedené trestné činy páchat, zanikne i třetí generace počítačové trestné činnosti.

1.2.1.4. Čtvrtá generace počítačových trestných činů

Vlivem technologického vývoje se utváří nové kriminální příležitosti uvnitř virtuální reality. Jsou-li využity, bývají laickou veřejností označovány za „virtuální zločiny".[97] V reálném světě by se jednalo o trestný čin postižitelný platným trestním právem, ale virtuální čin se odehrává zcela ve virtuální realitě kyberprostoru a otázka trestnosti bývá komplikovanější, zejména s ohledem na základní trestněprávní princip *nullum crimen sine lege certa*.[98] Provést detailní rozbor trestněprávního postihu virtuálních trestných činů není cílem práce,[99] jež uvádí toliko nezbytný příklad k vystižení podstaty čtvrté generace počítačové kriminality. Označení daných případů za počítačovou kriminalitu, resp. za trestné činy, je nutno brát s ohledem na platnou a účinnou trestněprávní úpravu se značnou rezervou. Diskuze se doposud odehrávala zpravidla na akademické půdě.

Jedním z prvních „virtuálních zločinů" bylo virtuální znásilnění roku 1998 popsané Dibbellem.[100] Na zmíněném případu je patrný paradox virtuálních trestných činů typu virtuálního znásilnění. Jak uvádí Gřivna, podobné případy nelze u nás trestně

---

[96] Britský policejní vyšetřovací tým se nazývá the National Hi-Tech Crime Unit. Anglický termín „core cybercrime" a „true cybercrime" užívá Wall.

[97] GŘIVNA, Tomáš. Existují virtuální trestné činy?. *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, Wolters Kluwer, 2008, str. 28.

[98] Virtuální realita vzniká např. v rámci prostředí „Massively Multiplayer Online Game" her. Hru může hrát díky počítačové síti ve stejný okamžik velké množství hráčů v reálném čase. Prostředím hry je virtuální svět. GŘIVNA, Tomáš. Existují virtuální trestné činy?. *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, Wolters Kluwer, 2008, str. 28.

[99] Zajímavý rozbor virtuálních trestných činů v LASTOWKA, Greg; HUNTER, Dan. Virtual Crime. *New York Law School Law Review* [online]. 2004, 26. Dostupné z http://ssrn.com/abstract=564801. [cit. 2016-02-12].

[100] Jednalo se o v reálném čase probíhající zobrazení sexuálního zmrzačení příslušníka on-line hráčské komunity, které pozorovali další hráči na obrazovkách počítačů. Zahájení trestního stíhání proti konkrétnímu hráči nebylo tehdy shledáno důvodným. LASTOWKA, Greg; HUNTER, Dan. Virtual Crime. *New York Law School Law Review* [online]. 2004, 26. Dostupné z http://ssrn.com/abstract=564801. [cit. 2016-02-12]. Překlad autorka.

stíhat jako trestný čin znásilnění, neboť nedošlo k přímému kontaktu mezi pachatelem a obětí; obdobným případem je i vražda virtuální postavy hráče. Dopředu ovšem nelze vyloučit trestní odpovědnost za psychickou újmu na zdraví, způsobenou fyzické osobě, která virtuální postavu ovládá a jejím prostřednictvím jedná.[101]

Domnívám se, že je nutné uvážit i případy, v nichž je virtuální konstrukt způsobilý samostatně právně relevantně jednat. Další otázkou je odcizení virtuálních předmětů reálně ocenitelných mimo hráčský virtuální svět, kdy se i útok uskutečněný ve virtuálním světě dostává do rámce platného trestního práva.[102] Do budoucna bude nezbytné uvědomit si i potenciální dopad virtuálních zločinů na psychiku hráčů, kteří se mohou stát oběťmi nebo pachateli trestné činnosti. Zejména děti a mladiství se snadno stávají „obětí“, aniž by v dané věci došlo k protiprávnímu činu.[103] Podle názoru některých autorů ani trestněprávní regulaci virtuální reality do budoucna nemůžeme vyloučit.[104]

1.3. Pachatelé

Z hlediska trestního práva hmotného hovoříme o pachateli trestného činu ve smyslu § 22 odst. 1 TZ jako o osobě, která svým jednáním naplnila znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná. Trestněprávní předpisy pamatují i na situace nepřímého pachatelství, spolupachatelství a účastenství. K hlubšímu právnímu rozboru pachatele trestného činu z obecného hlediska lze odkázat na dostupnou literaturu.[105] Dále se text věnuje specifikům pachatele počítačové trestné činnosti.

---

[101] GŘIVNA, Tomáš. Existují virtuální trestné činy?. *Pocta Otovi Novotnému k 80. narozeninám*. Praha: ASPI, Wolters Kluwer, 2008, str. 33.
[102] LODDER, Arno. Dutch Supreme Court 2012: Virtual Theft Ruling a One-Off or First in a Series? *Legal Governance and Challenges*. 2013, 6(3), str. 1 - 14. Překlad autorka.
[103] Roku 2012 spáchal sebevraždu skokem z okna 14letý chlapec poté, co byl svědkem smrti oblíbené animované postavy. Dostupné na adrese http://kotaku.com/5957364/report-teen-commits-suicide-after-seeing-his-favorite-naruto-character-die. [cit. 2016-02-12]. Další problematickou oblastí je výskyt šikany v kybernetickém prostředí.
[104] WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 48. Překlad autorka.
[105] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktual. a dopl. vyd. Praha: Leges, 2016.; JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 6.

Mezi pachateli počítačové trestné činnosti zpravidla dominují mladiství pachatelé a výjimkou nejsou ani děti mladší patnácti let. Hovoří-li se o pachateli - fyzické osobě, nelze proto pomíjet věkovou hranici trestněprávní odpovědnosti dle § 25 TZ, požadující dovršení patnáctého roku věku v době spáchání trestného činu. U mladistvých pachatelů bude na základě § 5 odst. 1 zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (dále též „ZSVM“) třeba zkoumat, zda v době spáchání činu dosáhli již takové rozumové a mravní vyspělosti, aby mohli rozpoznat protiprávnost činu nebo ovládat své jednání. V případě záporné odpovědi nelze dovodit trestní odpovědnost mladistvého.

V dalším textu se věnuji pojmu pachatel počítačové trestné činnosti především z pohledu kriminologického a forenzně psychologického. Zaměřuji se na psychologické zkoumání osobnosti pachatele a charakteristiku pachatelů, které označujeme jako tzv. hackery či tzv. crackery.

1.3.1. Hacking a cracking

Jedním z nejčastěji skloňovaných pojmů v souvislosti s počítačovou kriminalitou a počítačovými systémy vůbec, je hacker, potažmo jeho aktivita - hacking. Definice hackerství není s ohledem na mediálně zkreslené a spíše pejorativní pojetí jednoduchá. Podle všeobecně přijímané verze hacking představuje neoprávněný přístup a následné užívání počítačových systémů jiných osob. Schell a Dodge popisují hackery jako jedince s hlubokým zájmem o počítače a technologie, kteří užívají svých znalostí a dovedností k tomu, aby získali přístup k počítačovým systémům, ať již se souhlasem jejich vlastníků či bez něj.[106] Téma neoprávněného přístupu k počítačovému systému, a riziko úniku velkého množství citlivých údajů a hrozba jejich zneužití, rezonuje mezi

aktualizované vydání. Praha: Leges, 2016.; SOLNAŘ, Vladimír. *Systém českého trestního práva*. Praha: Novatrix, 2009.

[106] SCHELL, Bernadette; DODGE, John; MOUTSATSOS, Steve. *The hacking of America: who's doing it, why, and how*. Westport, CT: Quorum Books, 2002. Překlad autorka.

jednotlivci i korporacemi.[107] Preventivní opatření s sebou přináší značné výdaje, avšak lze se domnívat, že případný ušlý zisk či zásahy do soukromí s sebou ponesou ztráty ještě vyšší.

Anglický termín hacker a hacking vznikl v 50. letech 20. století v komunitě radioamatérů. Dle Jirovského charakterizoval šikovného a technicky nadaného jedince schopného hledat nová zapojení a metody ke zlepšení výkonu a dosahu svého vysílače.[108] Počátkem 70. let termín zdomácněl v dnešním slova smyslu, když technologičtí nadšenci využívali nedostatků telefonní sítě k nezpoplatněným dálkovým hovorům.

Spolu s technologickým rozvojem v 80. letech a příchodem počítačů se vzdáleným připojením a rozmachem informačních průniků do databází dochází k rozvoji hackingu. První hackerské skupiny se zaměřovaly na sdílení poznatků o zjištěných přístupových heslech k počítačům a o nástrojích využívaných k průnikům do nich. Narůstající objem dostupných informací způsobil změny i v komunitě hackerů, do níž přichází nováčci bez hlubšího vzdělání a technických znalostí, označovaní jako tzv. script-kiddies, snažící se získat respekt svých druhů průniky do cizích počítačových systémů pomocí svých programů.[109] Jako tzv. samurai, popřípadě tzv. white hat hackeři a guru hackeři se označují ti, kteří jednají nikoli ze zištných, nýbrž z etických motivů. Svými znalostmi a dovednostmi pomáhají jiným dosáhnout cílů souladných s hackerskou etikou.[110]

Základ etiky hackera představuje povinnost sdílet své vědomosti a dovednosti s ostatními a striktní zákaz škodit. Uvážíme-li uvedená maxima, jsou to crackeři, kdo využívá svých znalostí k páchání trestné činnosti.[111] Podle Walla jsou crackeři a black hat hackeři motivováni primárně snahou dosažení zisku.[112] Na značný posun ve vnímání pojmu hacker poukazuje i Jirovský. Hovoří o tradičním významu termínu v 70. letech

[107] HOLT, Thomas; STRUMSKY, Deborah; SMIRNOVA, Olga; KILGER, Max. Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*. 2012, 6(1), str. 891 - 903. Překlad autorka.
[108] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 47.
[109] WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 229. Překlad autorka.
[110] Tamtéž, str. 228.
[111] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 47 – 48.
[112] WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 223. Překlad autorka.

20. století, kdy se označením hacker honosila řada nadaných studentů, později známých a úspěšných osobností na poli technologického průmyslu, mezi něž patřil i Bill Gates.[113] Vzhledem k celosvětovému rozvoji Internetu a četnosti hackerské komunity však není překvapivý právě vzrůstající výskyt trestněprávně relevantních vzorců chování.

1.3.2. Psychologické zkoumání osobnosti pachatele

Problematika počítačové kriminality je jevem, který lze zkoumat pouze interdisciplinárně. V rámci jejího postihu se vedle právního vědomí uplatní i znalosti technologické, sociologické či psychologické. Psychologické zkoumání osobnosti pachatele pomáhá vytvořit vhodnou strategii vyšetřování trestné činnosti a ovlivňuje různé přístupy metodik vyšetřování počítačové kriminality.

Lidský faktor ve vztahu k páchání počítačové trestné činnosti zůstává v rámci psychologického i kriminologického výzkumu do značné míry opomíjen. Psychologické zkoumání pachatelů počítačové trestné činnosti, včetně extremismu a kyberterorismu, je stěžejní v našem porozumění vyvíjející se trestné činnosti.[114] Především policejní orgány se bez důkladnějších znalostí potenciálního psychologického profilu pachatele neobejdou.

Počítačová kriminalita bývá často řazena mezi kriminalitu tzv. bílých límečků. Pojem užil poprvé americký kriminolog Edwin Hardin Sutherland, který se teorii a výzkumu kriminality bílých límečků věnoval.[115] Dle definice Erwina Sutherlanda z roku 1939 je zločinem bílého límečku zločin spáchaný respektovanou osobou požívající značný společenský status, která zneužívá své pracovní zařazení ke spáchání trestného činu.[116] Smejkal hovoří o tzv. dematerializovaném zločinu, neboť se jedná o trestnou

[113] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 49.
[114] Obdobně též Position Paper Terrorism and Cybercrime. *Netherlands Institute for the Study of Crime and Law Enforcement* [online]. Dostupné z https://www.nscr.nl/wp-content/uploads/position-paper.pdf. [cit. 2016-11-06]. Překlad autorka.
[115] JELÍNEK, Jiří. Edwin H. Sutherland – K odkazu zakladatele moderní americké kriminologie pro studium organizované kriminality. In: JELÍNEK, Jiří, (ed.). *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014, str. 9.
[116] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 2., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009, str. 273.

činnost páchanou vlivem technologického vývoje vůči dematerializovaným předmětům, jako jsou například informace bankovního charakteru. Tato kriminalita s sebou nepřináší prvek běžného násilí, nýbrž vynalézavost, inteligenci a rafinovanost pachatelů. Dematerializovaná kriminalita je značně výnosná a motiv pachatelů bývá obvykle zištný.[117]

Pachatele počítačových trestných činů dělí Smejkal do pěti skupin:[118]

První skupina pachatelů pochází z řad zaměstnanců poškozené organizace. Tito často trpí pocity nedostatečného ocenění zaměstnavatelem či svými kolegy.

Druhá skupina pachatelů počítačových trestných činů jsou typičtí hackeři, v jejichž chování jsou patrné anarchistické rysy, čemuž odpovídá i charakter páchané trestné činnosti – zavirování počítačového systému, neoprávněný přístup do vládních počítačových systémů a sítí, útoky typu DDoS apod.

Do třetí kategorie Smejkal řadí pachatele organizovaného zločinu. Ti využívají počítač jako nástroj ke skryté komunikaci, k legalizaci výnosů z trestné činnosti, k výrobě padělků software i platebních prostředků či k výrobě a distribuci nelegální pornografie všeho druhu.

Čtvrtou skupinu představují profesionálové nabízející výjimečné technologické znalosti a dovednosti k nejrůznějším aktivitám v kyberprostoru – od neoprávněného přístupu k počítačovým systémům až k obchodní a státní špionáži.

Pátá kategorie je tvořena osobami běžně ve věku blízkém věku dětí a mladistvých, kteří nepřemýšlí blíže nad důsledky svého jednání a páchají trestnou činnost zpravidla proto, že to tak vidí i u jiných. Typicky půjde o neoprávněné užívání autorských děl, šíření nelegálního software či jiná porušení autorských práv.

Řada mladistvých pachatelů počítačové kriminality časem zaměří své aktivity do oblastí společensky akceptovatelných a nachází uplatnění jako odborníci na poli počítačové bezpečnosti. Pakliže se ale dostávají do kontaktu s hlubším kriminálním podsvětím, stávají se často pachateli organizovaného zločinu.[119] Podstatný důraz je proto vhodné klást na prevenci kriminálních vzorců chování mezi mladistvými hackery.

---

[117] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 486 - 487.
[118] Tamtéž, str. 488.
[119] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 50.

1.3.2.1. Pachatelé hospodářské a finanční kriminality

Čírtková se v rámci psychologických aspektů vybraných deliktů soustředí na psychologické profilování pachatelů hospodářské a finanční kriminality.[120] Ačkoli s ohledem na různé zaměření pachatelů počítačové kriminality vidíme, že se nejedná o homogenní skupinu, nelze pomíjet shodné rysy pachatelů hospodářské a finanční kriminality s pachateli počítačové kriminality především z první, třetí a čtvrté skupiny Smejkalovy kategorizace. Počítačový systém je častým nástrojem páchání hospodářské a finanční kriminality, jejíž pachatelé se dopouští specifických forem podvodného jednání. Z uvedeného důvodu je vhodné zde rozebrat psychologický profil pachatelů hospodářské a finanční kriminality.

Dle Čírtkové byl původní forenzně psychologický přístup ovlivněn teorií příležitostí. Pachatelé finanční a hospodářské kriminality jsou zvláště vnímaví vůči výskytu vhodných příležitostí ke spáchání trestného činu. Mezi jejich společnými znaky Čírtková uvádí relativizaci viny a její přesouvání, neskrývaný narcismus a pesimistický pohled na člověka jako takového.[121] Baloun a Cejp předpokládají v individuální charakteristice pachatelů finanční kriminality sofistikované jednání, vzdělání v oblasti podnikání a původ z podnikatelských kruhů či společenských elit a spíše mužské pohlaví. Nad rámec psychologického profilu poukazují i na vznik škody velkého rozsahu projevující se u mnoha obětí, vysokou latenci kriminálního jednání a dosavadní absenci odsouzení.[122] Přestože neexistuje jednoznačný profil pachatele finanční a hospodářské kriminality, bývá ve forenzní psychologii s uvedeným druhem kriminality často spojen pojem kriminalita bílých límečků.

Kriminalitu bílých límečků vztahujeme k okruhu pachatelů s určitými typickými znaky, mezi něž se řadí mužské pohlaví, vyšší věk, vysoký sociální status, vyšší inteligence, ukončené profesní vzdělání, dobrá sociální integrace a vysoký příjem.[123] Uvedené charakteristice pachatele bílého límečku ovšem neodpovídají pachatelé

[120] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 2., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009, str. 272.
[121] Tamtéž, str. 272 – 273.
[122] BALOUN, Vladimír. *Organizovaný zločin a jeho možné projevy ve finančním sektoru ekonomiky: dílčí závěrečná studie úkolu "Výzkum organizovaného zločinu v České republice II"*. Praha: Institut pro kriminologii a sociální prevenci, 1999, str. 84.
[123] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 2., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009, str. 274.

z druhé Smejkalovy kategorie, tj. typičtí hackeři, kteří se naopak vyznačují anti-systémovými rysy chování a mladším věkem. Předpokládá se u nich i nižší míra začlenění v okolní společnost. Otázkou je, zda uvedené vžité představy nejsou již limitující.

1.3.2.2. Hackeři

Široká veřejnost sdílí přesvědčení, že hackeři jsou osamělí podivíni trpící nedostatkem sociálních dovedností. Společenskovědní výzkum ovšem prokázal, že opak je pravdou. Hackeři vytváří ojedinělé subkultury, v jejichž rámci spolu vzájemně sdílí své poznatky. Společenství hackerů neexistují pouze ve sféře virtuální, nýbrž působí i v reálném světě. Mnozí hackeři přiznávají, že se pohybují ve společenství jiných hackerů, byť jde o společenství limitované, se kterým však udržují tzv. on-line i off-line kolegiální vztahy, což přispívá nejen k výměně potřebných poznatků a nástrojů, nýbrž i k utřídění vlastních hodnot a cílů.

Samotné činnosti, tj. hackingu, se hackeři věnují osamoceně. Důvodem je fakt, že komunita hackerů je společenství, které soudí jedince podle jeho partikulárních dovedností a úspěchů. Ačkoli hacker získává část dovedností skrze výměnu zkušeností se svými kolegy, podstatnou část si osvojuje díky vlastní zkušenosti, dosažené zpravidla metodou pokusu a omylu. Někteří autoři předpokládají silnější sklon k neoprávněnému přístupu k počítačovému systému a další počítačové trestné činnosti spíše u jednotlivců nežli skupin, s ohledem na motivaci hackerů porozumět technologii detailněji a tím i hlouběji rozvíjet svou dovednost.[124]

Komunita hackerů je poměrně uzavřená. Důraz na ochranu vlastního soukromí je patrný zejména u jedinců porušujících zákon, kteří se před odhalením chrání různými metodami, mezi něž patří užívání přezdívek i krytí vlastních IP adres. Na druhé straně se ale řada úspěšných hackerů chlubí svými dovednostmi, především nabízí-li pod

[124] HOLT, Thomas; STRUMSKY, Deborah; SMIRNOVA, Olga; KILGER, Max. Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*. 2012, 6(1), str. 892 - 893. Překlad autorka.

určitou přezdívkou své produkty k dispozici na černém trhu. V důsledku podobných reklamních snah se vystavuje řada autorů malware riziku odhalení.[125]

S vědomím určitého zevšeobecnění lze na základě několika dostupných studií sociálních sítí hackerů a tvůrců malware charakterizovat typického hackera jako mladého muže ve věku do 29 let, inteligentního, zpravidla studujícího univerzitu či bývalého vysokoškoláka, pocházejícího s nejvyšší pravděpodobností ze země bývalého Sovětského bloku, nejčastěji z Ruské federace či Ukrajiny. Dívky a ženy se v komunitě hackerů vyskytují pouze v minimální míře. Překvapivě nepatrné procento příslušníků komunity má skutečně hluboké znalosti programování a technologií, tolik potřebné pro aktivity hackerů.[126] Vzhledem ke sdílení poznatků v rámci komunity hackerů se však k nástrojům umožňujícím (jednodušší) páchání trestné činnosti snadno dostanou i jedinci bez hlubších znalostí.

1.3.2.3. Pachatelé kyberterorismu

Další odlišující se kategorií bývají pachatelé kyberterorismu, teroristé útočící na informační nebo telekomunikační systémy, popřípadě tyto systémy využívající jako nástroj útoku. Dle Smejkala[127] lze útočníky v kybernetickém prostředí členit do tří základních skupin: individuální útočníci, ideologicky motivované skupiny (bez ohledu na druh ideologie) a pachatelé státního terorismu.

Kategorii individuálních útočníků, lze považovat za nejvíce heterogenní. Mezi pachateli se objevují nejrůznější motivy, nikoli však motiv zištný. Zištný motiv je typický pro hospodářskou a finanční kriminalitu (viz výše), ne terorismus. Motivací pachatelů bude zejména extremismus, rasová nenávist, politické přesvědčení či náboženský fundamentalismus.

[125] HOLT, Thomas; STRUMSKY, Deborah; SMIRNOVA, Olga; KILGER, Max. Examining the Social Networks of Malware Writers and Hackers. *International Journal of Cyber Criminology*. 2012, 6(1), str. 893. Překlad autorka.
[126] Tamtéž, str. 896 - 901. Překlad autorka.
[127] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 90.

Ideologicky motivované skupiny útočí proti svému ideovému protivníku. Smejkal uvádí běžné útoky na webové stránky protivníků (kyber)teroristů na Blízkém Východě.

Pachatele z poslední skupiny náležící ke státnímu terorismu lze charakterizovat jako profesionální hackery či crackery. Jejich společným znakem bývá vysoká úroveň získaných znalostí a dovedností v oblastech informační bezpečnosti, kterou uplatňují ve státních službách.

1.4. Oběti

Obětí se z hlediska trestního práva rozumí především *„fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena majetková nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil.“*[128] Platná právní úprava pamatuje i na sekundární oběti v případě usmrcení oběti v důsledku trestného činu a na kategorii zvláště citlivou vůči vzniku druhotné újmy, tj. zvlášť zranitelné oběti. Kategorie definuje § 2 odst. 3, odst. 4 zákona č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů. Hlubší právní rozbor problematiky by do značné míry překročil rámec této práce a lze proto odkázat na dostupnou literaturu.[129]

Na rozdíl od poškozeného, kterým se může stát i právnická osoba, se za oběť trestného činu považuje dle platné právní úpravy pouze osoba fyzická. S poškozenou právnickou osobou, tedy nikoli s obětí trestného činu, se v rámci počítačové kriminality setkáme především u té její části, jež je orientována na dosažení zisku. Typicky půjde o různé typy podvodného jednání či softwarové pirátství.[130] Poškozené právnické osobě bývá způsobena škoda, tj. újma na majetku, popřípadě dochází trestnou činností k obohacení pachatele na úkor poškozené právnické osoby.

Naukou o obětech se zabývá viktimologie, vědní disciplína, jež se vyčlenila z kriminologie. Předmětem jejího zájmu jsou změny v chování a prožívání obětí

[128] Dle § 2 odst. 2 zákona č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů.
[129] Např. JELÍNEK, Jiří. *Zákon o obětech trestných činů: komentář s judikaturou*. 2. dopl. a rozš. vyd. Praha: Leges, 2014.; JELÍNEK, Jiří; PELC, Vladimír. Zákon o obětech trestných činů - jeho nedostatky a možnosti řešení. *Bulletin advokacie: stavovský časopis české advokacie*. 2015, str. 19-23.; JELÍNEK, Jiří; GŘIVNA, Tomáš. *Poškozený a oběť trestného činu z trestněprávního a kriminologického pohledu*. Praha: Leges, 2012.
[130] Srov. zejména kapitolu 3.2.2.

trestného činu i to, jakou roli hraje oběť v motivaci pachatele a jakým způsobem dochází k interakci mezi chováním pachatele a oběti v průběhu trestného činu.[131] Smyslem viktimologie je mimo jiné prevence trestné činnosti, metody jednání s oběťmi v průběhu jejího vyšetřování a vhodná podoba právní a psychologické pomoci obětem kriminality.

Oběti počítačové trestné činnosti jsou kategorií, k níž viktimologie i právní nauka teprve svůj zájem obrací. Zajisté jedním z důvodů, proč bylo téma doposud spíše opomíjeno, je značná míra latence počítačové trestné činnosti. Mnohé osoby nemají ponětí o skutečnosti, že se staly oběťmi počítačové trestné činnosti.

Podobně jako nelze podat ucelenou charakteristiku obecně platnou pro pachatele počítačové trestné činnosti, nelze s jednoznačným vědomím charakterizovat ani její oběti. K dispozici jsou v současné době psychologické a kriminologické studie, které se zaměřují zpravidla na konkrétní nebezpečnou činnost pro společnost, jakou bývá cyberstalking či kybernetická šikana (kyberšikana), nikoli na počítačovou kriminalitu jakožto celek. Proto následující text uvádí jen některé aspekty problematiky obětí vybrané části počítačové kriminality.

1.4.1. Vybrané poznatky: cyberstalking, kyberšikana, sextorting

Aktivity spadající pod pojem cyberstalking,[132] lze uvést v rámci přečinu nebezpečného pronásledování dle § 354 odst. 1 písm. c), písm. e) TZ. Pachatel zpravidla zneužívá prostředky elektronických komunikací a vytrvale kontaktuje a obtěžuje jinou osobu, často za současného zneužití jejích osobních údajů nalezených na Internetu. Psychologické studie uvádí, že množství času, které uživatel Internetu stráví on-line, ve spojení s mírou zveřejňování údajů o své osobě, jsou přímo úměrné míře rizika viktimizace.[133]

---

[131] ČÍRTKOVÁ, Ludmila. *Forenzní psychologie*. 2., upr. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2009, str. 98.

[132] Cyberstalking je systematické pronásledování jiného skrze elektronické prostředky. KOOPS, Bert-Jaap. *Netherlands Reports to the 18th International Congress of Comparative Law*. Antwerp: Intersentia, 2010, str. 630. Dostupné z https://ssrn.com/abstract=1633958 [cit. 2017-02-07]. Překlad autorka.

[133] WELSH, Andrew; LAVOIE, Jennifer. Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. 2012, 6(1). Dostupné z

Další z oblastí, které se staly předmětem zájmu odborných studií, je kyberšikana. Pod uvedeným pojmem rozumíme *„úmyslné a opakované působení újmy prostřednictvím počítače, mobilního telefonu a dalších elektronických zařízení“*.[134] Kyberšikana, byť ne vždy spadne do oblasti trestního práva, je vysoce společensky nebezpečným jevem, především uvážíme-li stoupající výskyt sebevražd obětí.[135] Z hlediska trestněprávní kvalifikace může pachatel naplnit znaky skutkové podstaty trestných činů nebezpečného vyhrožování dle § 353 TZ, vydírání dle § 175 TZ, pomluvy dle § 184 TZ, porušení tajemství dopravovaných zpráv dle § 182 TZ, ale i výtržnictví dle § 358 TZ.[136] Studie poukazují na podobnost kyberšikany se šikanou odehrávající se v reálném světě. Viktimizace šikanou i kyberšikanou bývá nerozlučně spjata – oběť šikany v reálném světě bývá i obětí kyberšikany ve světě virtuálním. Riziko kyberšikany souvisí s družností dítěte v reálném světě a s jeho technologickou zručností. Zásadní je rovněž angažovanost a zájem rodičů o život dítěte. Čím jsou vztahy dítěte s okolím četnější a hlubší, tím je riziko viktimizace nižší.[137]

Další oblastí, kde existují určité poznatky o obětech počítačové trestné činnosti, je kategorie trestných činů proti lidské důstojnosti v sexuální oblasti. Oběti, nezřídka mladší osmnácti let, bývají lákány či nuceny k obnažování a jinému sexuálně explicitnímu chování prostřednictvím internetových komunikačních platforem. V zahraničí se pro uvedený jev vžilo označení sextorting.[138] Trestný čin pachatele lze právně kvalifikovat jako trestný čin sexuálního nátlaku dle § 186 TZ, kuplířství dle § 189 TZ, a podle věku oběti, i jako trestný čin zneužití dítěte k výrobě pornografie dle

---

http://www.cyberpsychology.eu/view.php?cisloclanku=2012051301&article=4 [cit. 2016-11-19]. Překlad autorka.

[134] PATCHIN, Justin; HINDUJA, Sameer. Bullies Move Beyond the Schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice* [online]. 2006, 4(2), str. 152. Dostupné z http://yvj.sagepub.com/content/4/2/148 [cit. 2016-11-19]. Překlad autorka.

[135] SEILER, Steven; NAVARRO, Jordana. Bullying on the pixel playground: Investigating risk factors of cyberbullying at the intersection of children's online-offline social lives. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. 2014, 8(4) Dostupné z http://www.cyberpsychology.eu/view.php?cisloclanku=2014111001&article=1#authors [cit. 2016-11-19]. Překlad autorka.

[136] Jako provinění výtržnictví dle § 358 TZ lze např. kvalifikovat čin mladistvého pachatele, který skrze elektronické prostředky šikanuje svého učitele, veřejně během výuky, popřípadě i na jiném místě veřejnosti přístupném.

[137] SEILER, Steven; NAVARRO, Jordana. Bullying on the pixel playground: Investigating risk factors of cyberbullying at the intersection of children's online-offline social lives. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. 2014, 8(4) Dostupné z http://www.cyberpsychology.eu/view.php?cisloclanku=2014111001&article=1#authors [cit. 2016-11-19]. Překlad autorka.

[138] Výraz vznikl spojením slov sex a extortion, anglického výrazu pro vydírání.

§ 193 TZ. Studie ukazují, že děti a mladiství prodávající či nabízející sex skrze internet, mají už určité zkušenosti se sexuálním zneužíváním v reálném světě. Ty posléze vedou k pohrdání vlastním tělem a nabízením sebe sama skrze Internet. Vedle sexuální viktimizace z minulosti zvyšuje riziko i závislost oběti na Internetu a míra času stráveného on-line.[139]

1.5. Od běžné trestné činnosti přes kybernetickou válku ke kyberterorismu

1.5.1. Kriminogenní faktory sítě Internet

Rozšíření osobních počítačů a celosvětové sítě Internet v první polovině 90. let přinesly nové příležitosti pro pachatele trestné činnosti páchané do té doby bez využití počítače. Koops a Wall poukazují na charakteristické znaky Internetu vytvářející z této globální počítačové sítě prostředí kriminogenní,[140] jehož specifika významně ovlivňují rozvoj (zejména) kybernetické trestné činnosti.

Globální dosah a neexistence výsostných státních území v podobě, jak je chápe nauka mezinárodního práva veřejného, umožňuje bez potíží vyhledat nejzranitelnější a nejlukrativnější objekt útoku. Globální dosah je podstatou přeshraničního charakteru kybernetické kriminality. Pomineme-li jazykové bariéry a geoblokaci[141] webových stránek, bývá okruh adresátů prakticky neomezený. Možnost následné kontroly šíření informací skrze globální počítačovou síť je prakticky nulová.

Decentralizace a flexibilita sítě Internet brání cenzuře a jakékoli efektivní kontrole Internetu. Anonymita a vzdálená interakce usnadňuje páchání trestné činnosti a přetváří běžné vzorce mezilidské komunikace. Minimalizace verbálního projevu vytváří odlišná pravidla jednání i specifické morální normy. Pachatelé se skrývají za virtuální

[139] JONSSON, Linda; SVEDIN, Carl; HYDÉN, Margareta. "Without the Internet, I never would have sold sex": Young women selling sex online. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* [online]. 2014, 8(1) Dostupné z http://www.cyberpsychology.eu/view.php?cisloclanku=2014021703 [cit. 2016-11-19]. Překlad autorka.
[140] KOOPS, Bert-Jaap. The Internet and its Opportunities for Cybercrime: Tilburg Law School Research Paper No. 09/2011. *Transnational Criminology Manual* [online]. Nijmegen: WLP, 2010, (1). Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223. [cit. 2016-02-18]. WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 30 – 51. Překlad autorka.
[141] Zamezení přístupu na webovou stránku z počítačového zařízení se zahraniční IP adresou.

identitou a mizí strach z odhalení. Sociální kontrola, podstatný element bránící páchání trestné činnosti v reálném světě, v kybernetickém prostředí zpravidla zcela chybí.[142] Anonymní prostředí dále vytváří pole působnosti pro černý trh kybernetického zločinu[143] - specifický digitální datový trh, kde jsou komoditou citlivé informace bankovního charakteru, osobní údaje, hesla či nový druh malware, ale i IP adresy infikovaných počítačových systémů, které se staly součástí botnetu.

Snadná manipulace s daty bez zvláštních nákladů je dalším typickým znakem sítě Internet. Data lze kopírovat a přisvojit si tak hodnotu potenciální informace, aniž by byla vlastníku původních dat odňata možnost s nimi manipulovat. Data lze upravit bez zanechání viditelných stop a vydávat je za autentická.

Další faktor, možnost automatizace procesů, vytváří z kybernetické kriminality nebezpečný fenomén. Jediný počítačový virus na vhodném místě, jako jsou často navštěvované webové stránky nebo vhodná doména,[144] je způsobilý replikace a napadení mnoha dalších počítačů.[145] Klasický právní princip vyjádřený latinskou frází *de minimis non curat lex* v kybernetickém prostředí poněkud ztrácí smyslu. Značné procento kybernetické trestné činnosti nezpůsobí citelnou škodu. Pokud však sečteme jednotlivé výše škody způsobené týmiž pachateli napříč globální sítí, výsledná částka bude nesrovnatelně vyšší.

Kybernetická trestná činnost podléhá rychlému koloběhu inovace. Pachatelé počítačové trestné činnosti sdílí prostřednictvím Internetu nejnovější poznatky a nachází nové odběratele a partnery, oběti i způsoby, jak překonat stávající bezpečnostní překážky. Těmito cestami inovují dosavadní modus operandi. Jedinou zábranou se stává nedostatečná znalost jazyka, který opanovává to které diskuzní fórum či server.[146]

---

[142] Dle kriminologické teorie rutinních aktivit vyžaduje spáchání trestného činu v určitém místě a čase střet tří elementů: motivovaného potenciálního pachatele, vhodného cíle a konečně absenci způsobilého ochránce. GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014, str. 69.

[143] Účastníci černých trhů zakrývají svoji identitu využíváním sítě TOR (The Onion Router) či jinými způsoby. Detailněji viz *Tor: Hidden Service Protocol.* [online]. Dostupné z https://www.torproject.org/docs/hidden-services.html.en. [cit. 2016-02-18]. Překlad autorka.

[144] Doména označuje počítač nebo počítačovou síť připojené do sítě Internet a tvořící hierarchickou soustavu. Podrobněji k doménám např. SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. vyd. Praha: C.H. Beck, 2004.

[145] WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007, str. 43. Překlad autorka.

[146] Prostřednictvím legendární webové stránky *CarderPlanet* se sdružovali anglicky mluvící kartáři z celého světa (pachatelé zaměřující se na trestnou činnost spojenou se zneužíváním údajů z bankovních karet). *CarderPlanet* byla v provozu několik let, než roku 2004 pozatýkala americká tajná služba velkou

1.5.2. Vývoj počítačové trestné činnosti

Vývoj společnosti, včetně technologického rozvoje přinášejícího vyšší míru dostupnosti moderních technologií v každodenním životě, značně ovlivňuje podobu počítačové kriminality, která následuje technické a uživatelské možnosti počítačů.

Počítače zpočátku nebyly dostupné širší skupině uživatelů, neboť se jednalo o rozměrná zařízení v klimatizovaných sálech vyžadující profesionální obsluhu.[147] Mezi běžnými počítačovými trestnými činy v 80. letech převládaly tzv. dokladové delikty, jejichž pachatelé v rámci podvodného úmyslu manipulovali informačními vstupy určenými ke zpracování počítačem. Jednání bylo před rokem 1989 většinou kvalifikováno jako trestný čin rozkrádání majetku v socialistickém vlastnictví dle § 132 zákona č. 140/1961 Sb., trestního zákona (dále jen „bývalý trestní zákon"). S rozšířením běžné dostupnosti osobních počítačů začali pachatelé manipulovat s údaji přímo v počítačovém systému.[148]

Smejkal upozorňuje na tři nejrozšířenější kategorie počítačové trestné činnosti.[149] První zahrnuje široké spektrum jednání, které lze kvalifikovat jako trestný čin podvodu dle § 209 TZ. Druhá kategorie představuje útoky na počítačové systémy a sítě s cílem omezit jejich dostupnost a funkčnost, popřípadě získat přístup k datům a tím i k obsahu přenášených zpráv. Takové jednání je možné kvalifikovat jako trestný čin porušení tajemství dopravovaných zpráv dle § 182 TZ. V rámci třetí a zřejmě nejběžnější kategorie Smejkal uvádí porušování autorských práv, tj. trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ. Ačkoli cílem práce není rozbor práv duševního vlastnictví a jejich ochrany v kybernetickém prostředí, ve vztahu k počítačové trestné činnosti je vhodné uvést alespoň některé aspekty této ve společnosti velmi rozšířené trestné činnosti.

Výroba a distribuce tzv. pirátského software, představující ve virtuálním světě nejběžnější trestnou činnost porušující autorská práva, bývá označována jako tzv. warez, popřípadě tzv. warez scéna. Warez je organizovanou komunitou, obvykle

---

část správců a úlohu webu převzal *CardersMarket* a *DarkMarket*. GLENNY, Misha. *Temný trh: kyberzloději, kyberpolicisté a vy*. 1. vyd. v českém jazyce. Praha: Argo, 2013, str. 21 – 94.

[147] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 73.

[148] Tamtéž.

[149] Tamtéž, str. 74.

rozdělenou do soupeřících skupin, v nichž má každý z účastníků specifickou roli.[150] Vůdce skupinu řídí a jedná se správci warezových serverů, kteří je udržují v chodu a vytváří uživatelsky vstřícné prostředí. Další členové skupiny zajišťují díla k šíření. Obvykle jde o jedince působící uvnitř průmyslu, tj. o spolupracovníky prodejců software, hudebního a filmového průmyslu, či o publicisty. Technicky nejzručnější jedinci překonávají technickou ochranu proti kopírování a nelegálnímu šíření díla.

Warez scéna rozšiřuje mezi běžné uživatele Internetu ilegální kopie autorských děl,[151] tzv. release. Může se jednat o počítačovou hru, filmové, literární, hudební či vědecké dílo nebo počítačový program. Warez po celém světě zpřístupňuje nejnovější i klasická díla autorů tím, že prostřednictvím celosvětově přístupné počítačové sítě uveřejňuje jejich nelegální kopie. Nezřídka k uvedenému dochází i před oficiálním zpřístupněním díla široké veřejnosti.

Vzhledem k technologickému rozvoji je ochrana autorského práva, založená na principu teritoriality, v kyberprostoru velice problematická. Zvláštní roli v ní hraje kolektivní správa autorských děl a mezinárodní spolupráce jednotlivých států. Uvážíme-li povahu kybernetického prostředí, pochopíme, že boj proti warez scéně bude vždy komplikovaný. Řada asociací zabývajících se ochranou autorských práv i jejich kolektivní správou proti warez scéně již dlouho bojuje. Patrně nejznámější z nich je americká organizace The Motion Picture Producers of America, prosazující dodržování právních předpisů USA na ochranu práva duševního vlastnictví.[152] Zisky plynoucí z filmového a hudebního průmyslu do rozpočtu USA dosahují sumy přes 1,1 trilionu amerických dolarů ročně.[153] Není proto překvapivé, že se boj proti pirátskému software nachází v zájmu veřejnoprávních i soukromoprávních subjektů, včetně politické scény.[154]

---

[150] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 69 – 71.

[151] § 2 odst. 1 zákona č. 121/2000 Sb. (autorský zákon) definuje autorské dílo jako *„dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam“*.

[152] Zejména Copyright Act of 1976, The Piracy and Counterfeiting Amendments Act of 1982, Cable Communications Policy Act of 1984, Digital Millennium Act of 1998, Family Entertainment and Copyright Act of 2005. Dostupné z http://www.copyright.gov/legislation/ [cit. 2016-11-17].

[153] Motion Picture Association of America: Why copyright matters. *Motion Picture Association of America* [online]. Dostupné z http://www.mpaa.org/why-copyright-matters/ [cit. 2016-11-17]. Překlad autorka.

[154] Některá politická uskupení však propagují svobodný přístup k výsledkům lidského bádání a lidské tvorby. Uvedený proud je na české politické scéně zastoupen Českou pirátskou stranou.

Právní postih aktivit warez scény, vzhledem k organizovanosti členů působících po celém světě a využívajících mechanismy krytí vlastní identity, není jednoduchý. Získání důkazních prostředků a samotný výkon trestněprávní jurisdikce je globálním dosahem warez scény velmi ztížen. Činnost orgánů činných v trestním řízení je běžně zapotřebí koordinovat v rámci několika států.[155] Zmínit lze úspěch orgánů USA, které 20. července 2016 zajistily doménu nejnavštěvovanější tzv. peer-to-peer sítě[156] s názvem kickasstorrents.to obsahující databázi pirátského software. Souběžně se zajištěním domény byl v Polsku zatčen a vzat do vazby Ukrajinec Artem Vaulin, domnělý majitel sítě, na kterého byla v USA podána obžaloba pro trestnou činnost spojenou s porušením autorských práv a legalizací výnosů z trestné činnosti. USA nyní požadují jeho vydání z Polska za účelem trestního stíhání.[157]

1.5.3. Nástroje

Spolu s masivním šířením poznatků hackerů se vyskytují i sofistikovanější způsoby páchání počítačové kriminality. Specifické nástroje pachatelů počítačové kriminality výrazně přispěly k jejímu globálnímu rozvoji v mezinárodním prostředí. Mezi hlavními příčinami rapidního nárůstu množství případů kybernetické kriminality v rámci mezinárodního prostředí po roce 2000 bývá uveden rozmach sítě botnetů,[158] jejichž vznik usnadňují právě specifické nástroje pachatelů počítačové trestné činnosti. Následujícím text proto ve stručnosti pojednává o příslušných programových nástrojích, které nejsou právnické veřejnosti obvykle příliš známé.

---

[155] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 74.

[156] Peer-to-peer nebo též P-2-P sítě jsou počítačové sítě využívané jako svobodná platforma pro výměnu informací a dat, odvislá od účasti svých členů. Jako decentralizované sítě jsou vytvářeny svými vlastními uživateli. WALL, David. *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity, 2007, str. 226. Překlad autorka.

[157] Dostupné z https://torrentfreak.com/feds-seize-kickasstorrents-domains-charge-owner-160720/ [cit. 2016-11-17]. Překlad autorka.

[158] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 2. Dostupné z http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

Jirovský člení technologie umožňující jednodušší páchání trestné činnosti skrze počítač na nástroje hardwarové a softwarové a na nástroje sociálního inženýrství.[159] Nástroje sociálního inženýrství uvádí v omyl nikoli počítač, nýbrž lidskou mysl. Nejrozšířenější jsou nástroje softwarové, ačkoli bývají běžně užívány i s nástroji sociálního inženýrství. Tak je tomu u tzv. phishingových útoků, v rámci nichž se pachatel snaží uvést oběť v omyl, v důsledku kterého by vyzradila citlivé údaje obvykle bankovního charakteru, jako přístupová hesla a informace o bankovních účtech.[160]

Nástroje se postupně přizpůsobují vzrůstající složitosti počítačových systémů a stávají se automatizovanými. Přípravě nových průnikových technik se věnuje pouze malá skupina pachatelů. Zpravidla půjde o osoby s vynikající znalostí informačních technologií a s hlubšími programátorskými schopnostmi, osoby působící ve zpravodajských službách, v řadách organizovaného zločinu či terorismu. Tzv. exploity, programy využívající nově nalezené slabiny, se nejprve šíří v úzké komunitě uživatelů. Jakmile se přemění v automatizovaný nástroj a dostávají se do širší distribuce v komunitě hackerů a crackerů, zareagují dodavatelé operačních systémů a antivirových programů, kteří vyvinou odpovídající bezpečnostní opatření. Koloběh je charakteristický pro bezpečnost informačních a komunikačních technologií jako celek.[161]

Podrobné představení jednotlivých programových nástrojů by bylo nad rámec předkládané práce, lze však uvést nejdůležitější z nich.

Tzv. prolamovače hesel prolamují ochranu počítače vytvořenou kombinací nejrůznějších znaků. Čím obsáhlejší bude množina znaků, z nichž může být heslo utvořeno, tím déle trvá jeho prolomení. Tzv. backdoors, neboli „zadní vrátka“, umožňují vzdálený přístup k napadenému počítači i k jeho řízení. Skenery zjišťují programy, které na napadeném počítači běží a informují o jeho uživateli. Tzv. sniffery umožňují odposlech komunikace mezi jednotlivými počítačovými systémy ve smyslu odposlechu síťového provozu. Slouží opět k získání potřebných informací o uživatelích. Tzv. rootkity umožňují skrýt činnosti prováděné na operačním systému počítače. Bývají

[159] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 59.
[160] Nejčastějším příkladem phishingu bývá nevyžádaná e-mailová zpráva vydávající se za zprávu od banky. Příjemce je po přesměrování na falešnou webovou stránku požádán o zadání svých osobních údajů, které jsou následně použity k získání přístupu k jeho bankovnímu účtu.
[161] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 60 - 61.

uváděny mezi nástroji backdoors. Nástroje Denial of Service, neboli „odepření služby“, představují kombinaci technik vedoucích jednoduše řečeno k zahlcení počítače, a to za pomoci zahlcení přístupových cest k němu. Tzv. trojans, neboli trojské koně, umožňují útočníkovi mnohé - od monitorování aktivit uživatele počítače, přes získání zadaných údajů a jejich zasílání na předem určené místo, až po vlastní replikaci sebe samých. Tzv. debuggery umožňují ověřit správnou funkci konkrétního programu, často nového exploitu.

1.5.4. Současný stav

O skutečném stavu trestné činnosti páchané prostřednictvím informačních a komunikačních technologií mnoho nevíme. K dispozici jsou především poznatky zahraniční kriminologicky orientované literatury.[162] Pro internetové prostředí je typická vysoká míra latence trestné činnosti. Pouze minimum incidentů oznámených na policii je prošetřeno a objasněno.

Statistické ročenky kriminality Ministerstva spravedlnosti České republiky ani policejní statistiky neudávají kompletní přehled počítačové kriminality. Řada vykazovaných počítačových trestných činů bývá podřazena pod jiné kategorie či označena zavádějícími názvy. Počítačová kriminalita je běžně zaznamenána v rámci hospodářské či majetkové kriminality i jako jev spadající pod organizovaný zločin. Trestněprávní kvalifikace nemusí nijak poukazovat na využití počítače při spáchání deliktu, ačkoli tomu tak bývá u trestných činů nebezpečného pronásledování dle § 354 TZ, šíření pornografie dle § 191 TZ a další trestné činnosti běžně páchané prostřednictvím ICT. Pouze u tzv. ryze počítačových trestných činů neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ, opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231 TZ a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti dle § 232 TZ, a popřípadě trestného činu poškození a zneužití záznamu na nosiči informací dle § 257a bývalého trestního zákona,

[162] Jedná se především o anglicky psanou literaturu. Tématu z kriminologického úhlu pohledu se dlouhodobě věnují např. Susan W. Brenner a David Wall. Dále lze zmínit autory jako Bert-Jaap Koops, Orin S. Kerr, Ulrich Sieber či Nicolai Seitz.

lze s jistotou vycházet ze statistických údajů. Vždy je nutné počítat se skutečností, že obsahem statistik jsou pouze případy, které policejní orgán zaznamená.

Kybernetický útok se pachatelům vyplatí co do výše zisku, pravděpodobnosti odhalení, dopadení, odsouzení i výše uloženého trestu. Jirovský srovnává bankovní přepadení s kybernetickým útokem následovně:[163]

Parametr	**Průměrné ozbrojené přepadení**	**Průměrný kybernetický útok**
Riziko	pachatel riskuje zranění či zabití	bez rizika fyzického zranění
Zisk	průměrně 3 až 5 tis. USD	od 50 až 500 tis. USD
Pravděpodobnost dopadení	dopadeno 50 až 60% útočníků	dopadeno cca 10% útočníků
Pravděpodobnost odsouzení	odsouzeno 95% dopadených útočníků	z dopadených útočníků je pouze 15% soudně projednáno a z nich je odsouzeno jen 50%
Trest	průměrně 5 až 6 let, pokud pachatel někoho zranil	průměrně 2 až 4 roky

Příloha č. 1: Srovnání klasického a kybernetického trestného činu.

Atraktivitu kybernetické kriminality pro pachatele majetkové trestné činnosti dokládá sofistikovaný bankovní podvod, k němuž došlo roku 2009 v USA. Pachatelé jednající z území mimo USA vyvedli postupnými bankovními převody z účtů spořitelny ve státě Kentucky částku ve výši 415.989 USD. Postiženy byly účty obchodní společnosti, jejíž systém autorizace odchozích plateb spolu se zabezpečením spořitelny pachatelé obešli.

Zabezpečení bankovních transferů spořitelny spočívalo ve ztotožnění počítače klientů pomocí vytvoření jednoznačného „označení“ počítače, z něhož klient do účtu vstupoval. Jestliže informační systém spořitelny zaznamenal pokus o přihlášení se do klientského účtu z jiného počítače, odeslal klientovi e-mail s jednorázovým heslem pro

[163] Srovnávací tabulka vychází z dlouhodobých statistik amerického úřadu pro vyšetřování (FBI). Ačkoli jsou údaje již z roku 2007, nabízí srovnání výstižnou představu o výhodách přesunu kriminálních aktivit do kybernetického prostředí. Např. pravděpodobnost dopadení klesne u kybernetického útoku o 40-50%. Převzato od JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 30.

přihlášení. Pachatelé podvodu za pomoci programu Zeus (počítačový vir typu trojského koně),[164] který instalovali do klíčového počítače poškozené společnosti, získali přístup k identifikačním údajům a heslům jednotlivých účtů u spořitelny i k přístupovým údajům do emailových schránek poškozené společnosti. Přestože příkazy k bankovním převodům zasílali z cizích počítačů (z cizích IP adres), následná autentifikace pomocí vygenerovaného jednorázového hesla zaslaného na infiltrované emailové adresy byla snadná. Jednotlivé částky putovaly na bankovní účty různých osob, tzv. bílých koní, které je za nepatrnou provizi posílaly na cizozemské účty, vedené nejčastěji u ukrajinských bank, kde byly předmětné částky ztraceny. Pachatelé nebyli nikdy identifikováni. Díky programu Zeus získali obdobným způsobem neznámí pachatelé za rok 2007 celkem 6 milionů USD z bankovních institucí v USA, Velké Británii, Španělsku i Itálii.[165] Způsobenou škodu v podobných případech obvykle hradí samotné banky, což se zpravidla podepíše na zvýšení bankovních poplatků klientům.

Přesné vyčíslení škod kybernetické kriminality naráží na problém nedostatku spolehlivých údajů. Nejčastěji prezentují veřejnosti příslušná čísla obchodní společnosti prodávající bezpečnostní software.[166] Relevantní souhrnné údaje o výskytu počítačové kriminality chybí.

Počítačovou kriminalitu můžeme běžně označit za „neviditelnou“. Poškození nemusí mít o proběhlém trestném činu ani ponětí. U automatizované kybernetické trestné činnosti škoda obvykle dosahuje v konkrétním případě nepatrné výše, tudíž ji poškození buď nezaznamenají, anebo jim nestojí za podání trestního oznámení. S ohledem na nízké technické znalosti si nemusí být v řadě případů trestné činnosti vědomi. Značná část poškozených právnických osob, typicky z řad obchodních korporací, nepodává trestní oznámení z obavy před negativní publicitou a bezpečnostní incidenty řeší na soukromé bázi.[167] S ohledem na stoupající výskyt kybernetických

[164] Program Zeus po instalaci v postiženém počítači zaznamenává aktivitu uživatele na klávesnici počítače a informace o ní automaticky odesílá na předem naprogramovanou adresu.
[165] BRENNER, Susan. *Cybercrime and the law: challenges, issues, and outcomes* [online]. Boston: Northeastern University Press, c2012, str. 6 - 11. Dostupné z http://site.ebrary.com/lib/cuni/Doc?id=10620947 [cit. 2016-02-29]. Překlad autorka.
[166] Např. společnost Symantec, nabízející na trhu zabezpečení a správu dat, každoročně vydává souhrnnou zprávu o stavu kybernetické kriminality. Otázkou je spolehlivost údajů s ohledem na podnikatelské cíle společnosti.
[167] KOOPS, Bert-Jaap. The Internet and its Opportunities for Cybercrime: Tilburg Law School Research Paper No. 09/2011. *Transnational Criminology Manual* [online]. Nijmegen: WLP, 2010, (1), str. 738. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223. [cit. 2016-02-18]. Překlad autorka.

útoků na řadu společností je efektivnější a rychlejší řešit útoky v rámci vnitřního specializovaného oddělení, než pokaždé věc oznámit policii. Důvodem vysoké míry latence počítačové kriminality je i charakter digitálních stop, značně nestálých a pro počítačového laika až nedohledatelných.

1.5.5. Kybernetická válka a informační válka

Využití aspektů globálních počítačových sítí a moderních technologií se dotýká i sféry bezpečnostní politiky a mezinárodních vztahů. Pojmy kybernetická a informační válka se prvně objevují během studené války. Hlubší význam získaly s rozvojem ICT na konci 20. století. Informační válku definoval roku 1976 ve své studii Weapons Systems and Information War Thomas P. Rona jako „*boj rozhodovacích systémů*“.[168] Informační válka může být vnímána jako součást státní politiky, užívající namísto tradičních vojenských zbraní zbraně latentní. *Kybernetickou válku* popisuje Jirovský jako *„aktivity vedené nebo koordinované státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka“*. Informační válku považuje za součást války kybernetické. Pojem infoware označuje nový druh válečného arzenálu, představující bojové prostředky určené ke zničení informační infrastruktury nepřítele.[169]

Informační boj se do určité míry zdá logickým vyústěním přesunu aktivit společnosti do virtuálního prostředí počítačových sítí. Informační boj je starší než počítačové systémy, avšak vlivem technologického rozvoje získal nové možnosti. Nejde pouze o aktivity ryze soukromého charakteru, do kybernetického prostoru se přesunula řada činností veřejné správy a pro funkčnost společnosti a státu se stává bezpečnost jeho kybernetického prostoru stále zásadnější. Mezi příklady nejzranitelnějších systémů patří průmyslové řídicí systémy, telekomunikace, včetně veřejné počítačové sítě, i informační systémy zdravotních, bankovních a dalších finančních institucí.

Mezi znaky kybernetické války patří relativní personální a materiální nenáročnost spolu s asymetrickou povahou konfliktu – utajený a dobře cílený kybernetický útok může citelně zasáhnout obranyschopnost silnějšího státu. Zatímco

[168] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 151.
[169] Tamtéž, str. 152.

útočníku postačí minimální vybavení a připojení k počítačové síti kdekoli na světě, preventivní aktivity obránce je zapotřebí provádět plošně a ve značném rozsahu.[170]

U některých odborníků se lze setkat i s názory, hodnotícími reakci západního světa na riziko kybernetické války jako přehnanou.[171] Poukazují na skutečnost, že kybernetická válka je součástí politického diskurzu západního světa teprve krátce, přičemž konkuruje i samotné hrozbě terorismu. Po roce 2007, kdy vleklá politická krize v Estonsku vyústila v napadení estonských vládních serverů a státních finančních institucí (patrně) ruskými hackery,[172] začala být problematika kybernetické bezpečnosti i hrozba kybernetické války vnímána jednotlivými státy jako jednoznačná hrozba. Můžeme se domnívat, že zvolený diskurz nahrává určitým politickým snahám s cílem posílit bezpečnost a obranyschopnost státu za současného oslabení svobody virtuálního prostoru.

V roce 2010 se dostala na veřejnost aféra ohledně viru Stuxnet, specifického druhu malware zaměřeného na kontrolu a ovládání průmyslových řídicích systémů (tzv. SCADA).[173] V rámci utajené spolupráce mezi americkými a izraelskými tajnými službami, která měla za cíl překazit íránský nukleární program, byl vyvinut extrémně komplexní počítačový program, který byl později tajně instalován do komunikačních a kontrolních systémů jaderného zařízení na obohacování uranu v íránském Natanzu. Skrze vzdálenou kontrolu průmyslového řídicího systému v Natanzu došlo ke zničení několika centrifug zařízení, jehož důsledkem bylo i zpomalení íránského jaderného programu. Malware Stuxnet byl nakonec odhalen díky programátorské chybě. USA i Izrael existenci celé operace i vzájemné spolupráce popírají.[174]

Metody kybernetické války nejsou cizí ani ozbrojeným občanským konfliktům a válkám, do kterých se v rámci globálního virtuálního prostoru zapojují různá politická

---

[170] Detailněji k informační válce a obraně před informačními útoky JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 153 - 155.

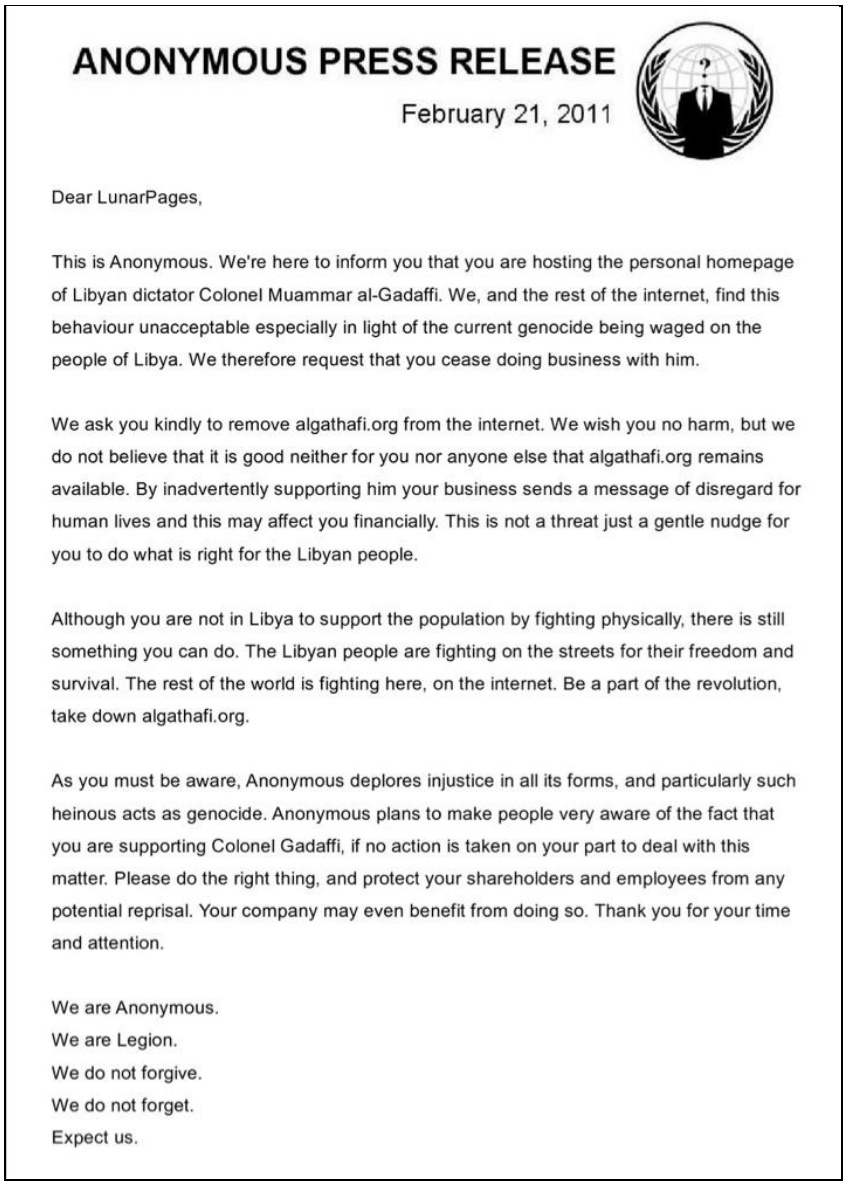
[171] KAISER, Robert. The birth of cyberwar. *Political Geography* [online]. 2015, 46(5), str. 11 - 20 Dostupné z http://www.sciencedirect.com.ezproxy.techlib.cz/science/article/pii/S0962629814000961 [cit. 2016-11-20]. Překlad autorka.

[172] Srov. kapitolu 3.3.4.2.

[173] Průmyslové systémy dispečerského řízení dat, známé pod anglickou zkratkou SCADA, tj. *Supervisory Control and Data Aquisition*.

[174] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 5. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

hnutí a organizované skupiny z celého světa. Hnutí Anonymous podporovalo rebely proti plukovníku Kaddáfímu v občanské válce v Libyi roku 2011. Ve své kampani označilo Internet za další prostředí boje proti diktatuře libyjského vůdce a vyzvalo poskytovatele připojení k Internetu k ukončení spolupráce s plukovníkem Kaddáfím. Pro ilustraci práce uvádí otevřený dopis od hnutí Anonymous:



ANONYMOUS PRESS RELEASE

February 21, 2011

Dear LunarPages,

This is Anonymous. We're here to inform you that you are hosting the personal homepage of Libyan dictator Colonel Muammar al-Gadaffi. We, and the rest of the internet, find this behaviour unacceptable especially in light of the current genocide being waged on the people of Libya. We therefore request that you cease doing business with him.

We ask you kindly to remove algathafi.org from the internet. We wish you no harm, but we do not believe that it is good neither for you nor anyone else that algathafi.org remains available. By inadvertently supporting him your business sends a message of disregard for human lives and this may affect you financially. This is not a threat just a gentle nudge for you to do what is right for the Libyan people.

Although you are not in Libya to support the population by fighting physically, there is still something you can do. The Libyan people are fighting on the streets for their freedom and survival. The rest of the world is fighting here, on the internet. Be a part of the revolution, take down algathafi.org.

As you must be aware, Anonymous deplores injustice in all its forms, and particularly such heinous acts as genocide. Anonymous plans to make people very aware of the fact that you are supporting Colonel Gadaffi, if no action is taken on your part to deal with this matter. Please do the right thing, and protect your shareholders and employees from any potential reprisal. Your company may even benefit from doing so. Thank you for your time and attention.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

Příloha č. 3: Dopis hnutí Anonymous s požadavkem ukončit hostování webové stránky libyjského diktátora plukovníka Muammara Kaddáfího.[175]

[175] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 7. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

Co se kybernetického útoku týče, lze jej v rámci počítačové kriminality i kybernetické války vnímat obdobně. Na rozdíl od počítačové kriminality bude ale kybernetická válka vždy součástí státní vojenské politiky. Z trestněprávního hlediska mohou metody informačního boje naplnit některé ze skutkových podstat trestných činů proti bezpečnosti České republiky, cizího státu a mezinárodní organizace ve druhém díle hlavy deváté trestního zákoníku. Klasickou špionáž zaměřenou na získání utajované informace, jejíž zneužití může vážným způsobem ohrozit nebo poškodit ústavní zřízení, svrchovanost, územní celistvost, obranu a bezpečnost České republiky, s cílem vyzradit ji cizí moci, uvádí skutková podstata trestného činu vyzvědačství dle § 316 TZ. Ochranu proti vyzvídání, tedy proti každé úmyslné činnosti zaměřené na získání určitých údajů, poskytuje trestní zákoník utajovaným informacím podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „ZBZ"). Jedná se o informaci označenou dle příslušného stupně utajení a zaznamenanou na jakémkoli nosiči, *„jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací."*[176] Seznam utajovaných informací vláda vydává nařízením. Cizí mocí se má na mysli jakýkoli stát mimo Českou republiku, ale i nadstátní organizace, jejímž členem Česká republika není. Cizí moc představují orgány a instituce reprezentované vládními úředníky, vojenskými funkcionáři, diplomaty apod.[177]

1.5.6. Terorismus a kybernetický prostor

Pro terorismus, obávanou globální hrozbu, vytváří kyberprostor vhodné prostředí, které jednotlivcům i organizacím umožňuje nalézt způsobilý cíl a vést útok prakticky odkudkoli. V rámci kyberprostoru může dojít buď ke spáchání teroristického útoku, anebo k využití jeho specifických vlastností k podpoře rozlišných aktivit teroristů. Europol na začátku roku 2016 poukázal na skutečnost, že nábožensky motivované teroristické skupiny využívají díky technologické zručnosti Internet i sociální média. Tato jsou teroristy běžně zneužívána k opatření nástrojů trestné činnosti

[176] § 2 písm. a) ZBZ.
[177] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 2, § 140 – 421. [Zvláštní část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 3087.

(zbraně, falešné průkazy totožnosti), elektronické služby jako Whatsapp, Viber a Skype slouží k šifrované komunikaci a sociální platformy jako Facebook a Twitter ke globálnímu sdílení poznatků uvnitř uzavřených skupin. Často využívanou službou bývají i anonymizační nástroje jako je VPN či ToR.[178]

Na problém terorismu lze nahlížet z mnoha úhlů pohledu – s akcentem na aspekty politické, psychologické, vojenské, právní či jiné. Z trestněprávního pohledu je terorismus především činem ohrožujícím ústavní zřízení a obranyschopnost státu, ale i demokratické principy, na nichž je republika založena, základní hospodářskou strukturu, život a zdraví obyvatel republiky.[179] Kyberterorismus představuje *„zneužívání výpočetní a telekomunikační techniky včetně internetu jako prostředku a prostředí pro uskutečnění teroristického útoku.*“[180] S ohledem na výrazný podíl médií na Internetu je vhodné poukázat i na zneužívání virtuálního mediálního prostoru teroristickými skupinami. Jirovský uvádí vedle kyberterorismu tzv. mediální terorismus jako další formu konvenčního neletálního terorismu a popisuje jej jako *„plánované zneužívání hromadných sdělovacích prostředků a dalších psychologických prostředků v době míru, za účelem ovlivnění názorů celé populace nebo cílených skupin obyvatelstva.“*[181]

Přes určitou vágnost definice mediálního terorismu je patrné, že aktivity teroristických skupin, které využívají virtuální prostor k podněcování teroristických činů, náboru nových jedinců a k šíření hrozby terorismu, jsou součástí plánované strategie teroristů. Virtuální prostor tedy může sloužit ke spáchání teroristického útoku nejen v rámci kybernetických útoků na počítačové systémy a sítě, ale i prostřednictvím psychologického nátlaku, jako například při zveřejnění záznamu či on-line přenosu poprav uskutečňovaných teroristickými skupinami. Hlubší rozbor problematiky terorismu v kybernetickém prostředí bude náplní třetí kapitoly předkládané práce.

---

[178] EUROPOL. Changes in modus operandi of Islamic State terrorist attacks.[online]. The Hague, 2016 Dostupné z https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks [cit. 2017-01-31]. Překlad autorka.

[179] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 2, § 140 – 421. [Zvláštní část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 3052.

[180] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 129.

[181] Tamtéž, str. 130.

2. PŮSOBENÍ TRESTNĚPRÁVNÍCH NOREM V KYBERPROSTORU

Mnozí právní vědci přirovnávají prostor celosvětové informační sítě k minovému poli.[182] Uvážíme-li charakteristické vlastnosti kyberprostoru, zejména globální počítačové sítě Internet, nelze než souhlasit s uvedenou paralelou. Působení právní normy v prostředí kyberprostoru je specifickou záležitostí. Mnohé běžně aplikované právní principy vychází z tradičního pojetí reálného světa, rozděleného hranicemi jednotlivých států na určitá teritoria. V souvislosti s působností trestního práva vyvstává řada otázek, z nichž se mnohé dotýkají vymezení pravomoci státu pomocí pravidel místní působnosti. Do jaké míry mohou orgány činné v trestním řízení zasahovat do státní suverenity ostatních států a osobovat si právo na důkazní prostředky nacházející se na území cizích států? Lze se v rámci pravidel exteritoriální pravomoci dožadovat přístupu k elektronickým materiálům nacházejícím se na úložišti mimo území vyšetřujícího státu? Jak lze lokalizovat vzdálenou prohlídku skrze počítačovou síť?[183] Hodlají jednotlivé státy interpretovat vybranou vyšetřovací techniku jako zásah do vlastní suverenity?

V rámci hledání odpovědí na položené otázky považuji v kapitole za důležité představit teoretické argumenty k problému legitimity právních norem v kyberprostoru. Formální existenci a aplikaci práva v kyberprostoru lze posléze srovnat s jeho faktickou vynutitelností. Jádro kapitoly tvoří rozbor působení trestněprávních norem v kyberprostoru, který se zaměřuje na otázku pravomoci státu ve spojení s limity místní působnosti. Kapitola pojednává o klasických principech místní působnosti a představuje ideje moderní koncepce jurisdikce. Závěrem cituje vybrané příklady ze zahraniční judikatury s rozborem problematiky jurisdikčních konfliktů.

[182] POLČÁK, Radim; ŠKOP, Martin; MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia)*. 1. vyd. Brno: Masarykova univerzita, 2005, str. 5.
[183] Díky prohlídce skrze počítačovou síť mohou orgány činné v trestním řízení státu A získat přístup k počítačovým systémům a datům uloženým na serverech na území státu B.

2.1. LEGITIMITA PRÁVA V KYBERPROSTORU

Z hlediska právní vědy je kyberprostor specifickým prostředím, v jehož rámci vznikají, mění se a zanikají právní vztahy, jejichž prostřednictvím se právo ve společnosti fakticky realizuje.[184] Původně to měl být právě kyberprostor a jeho virtuální realita, co poskytne lidské bytosti neomezenou možnost naplnění a seberealizace, neboť člověk není ve virtuální realitě omezován přírodními zákony ani právními normami reálného světa, které nezřídka vedou k jeho frustraci. Svoboda jedince v prostředí internetových sítí, osvobozených od zákonodárství jednotlivých států, představuje ústřední motiv známé Deklarace nezávislosti kyberprostoru (dále též „Deklarace“).[185] Byly to i myšlenky vyjádřené Deklarací, které přispěly k počátečním debatám o samotné oprávněnosti státních zásahů a právní regulace kyberprostoru. Přestože je spor již z části minulostí, považuji za vhodné uvést vybrané argumenty z Deklarace, které kritizují právní regulaci a státní zásahy v kyberprostoru, včetně představení možných protiargumentů, jež roli právních norem v kyberprostoru naopak obhajují.

2.1.1. Vybrané argumenty proti právní regulaci

Řada pasáží Deklarace obsahuje pro otázku působení práva v kyberprostoru klíčové momenty. Z Deklarace lze k ilustraci uvést její úvodní část: *„Vy, vlády všech průmyslových světů, Vy, unavení obři z masa a oceli. Já, přicházející z Kyberprostoru, nového sídla Mysli, Vás v zájmu budoucnosti vyzývám: Nechte nás být! Nejste mezi námi vítáni. Nemáte žádnou moc nad místy, kde přebýváme. Nemáme vládu ani po žádné netoužíme. Mluvím k Vám tedy z pozice autority ne větší, než jakou má sama Svoboda. Vyhlašuji, že globální společenství, jež budujeme, nezávisí na tyranii a zákazech, kterými jste nás svázali. Nemáte morální právo nás řídit a nemáte ani nástroje, kterých bychom se museli bát… Pojmy Vašeho práva, jako vlastnictví,*

[184] POLČÁK, Radim; ŠKOP, Martin; MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia)*. 1. vyd. Brno: Masarykova univerzita, 2005, str. 11.
[185] Deklarace představuje stěžejní dokument americké organizace Electronic Frontier Foundation, kterou roku 1990 založil v oboru známý aktivista John Perry Barlow. Organizace se zabývá podporou svobodného Internetu. Text Deklarace v plném znění anglického originálu je dostupný z https://www.eff.org/cyberspace-independence [cit. 2016-03-08].

vyjadřování, subjektivita, pohyb nebo okolnosti, se na nás nevztahují. Všechny jsou založeny na hmotné podstatě a zde žádná hmotná podstata není.“[186]

Deklarace zmínila několik stěžejních argumentů proti legitimitě práva v kyberprostoru, a to předně neexistenci společenské smlouvy v rámci internetového společenství, nepotřebnost autoritativní regulace a konečně neschopnost států právo v kyberprostoru efektivně prosadit. Deklarace předpokládala vznik a nezávislou existenci internetového společenství, odmítajícího vládu jako takovou. Autoři v Deklaraci tvrdí, že jakékoli případné konflikty lze řešit uvnitř společenství jeho vlastními samoregulačními mechanismy. Odmítají paralelu s konflikty existujícími v reálném světě. Poslední z uvedených argumentů se týká neschopnosti států právo v kyberprostoru efektivně prosazovat. Tento argument vychází z premisy, že je-li něco nevynutitelné, nemůže to být ani legitimní.

Domnívám se, že citovaný předpoklad lze těžko bez dalšího přijmout, neboť právo samo často k faktické vynutitelnosti přispívá svými vlastními mechanismy (typicky procesními normami) a nelze tak argumentovat proti právu samotnému odůvodněním jeho nevynutitelnosti. Problém vynutitelnosti práva proto uvádím vedle otázky legitimity jako samostatný.

2.1.2. Vybrané argumenty pro právní regulaci

Předně je nutné uvést, že ve vztahu k některým požadavkům, které Deklarace před více než 20 lety stanovila, došlo k určitému vývoji. Řada právních institutů již není založena toliko na hmotné podstatě. Existují právní nástroje, díky nimž lze v některých případech právo v prostředí Internetu vymoci. Příkladem budiž institut odpovědnosti poskytovatelů služeb informační společnosti, který je založen na klasické soukromoprávní, popřípadě veřejnoprávní odpovědnosti, limitované zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých

[186] Vybraná pasáž z Deklarace v překladu z publikace POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 19.

zákonů.[187] Na druhé straně problém svobody projevu jedince a vynutitelnosti práva v rámci kyberprostoru přetrval dodnes.

Vyjdeme-li z teorie společenské smlouvy, podle níž se v rámci určitého společenství (státu) jeho příslušníci implicitní dohodou vzdávají části své svobody ve prospěch ochrany svých oprávněných práv státem,[188] lze vůči argumentu neexistence společenské smlouvy namítnout, že členové internetového společenství nepřestávají být zároveň příslušníky jiného společenství, a to určitého státu, jehož státní moc včetně jednotlivých zákonů běžně respektovat musí. Přestože pojímáme kyberprostor jako prostředí *sui generis*, neznamená to automaticky negaci práva v rámci tohoto prostoru. Nabízí se do určité míry paralela s povinností občanů dbát zákonů státu i vně státní hranice.

K samoregulačnímu argumentu Polčák zdůrazňuje, že *„autoritativně vynucované právo má smysl (je legitimní) tam, kde společnost není sama o sobě dostatečně organizována, což brání jejímu dalšímu rozvoji.“*[189] Existence znaku samoregulace ve společnosti však nestačí, neboť tato může tolerovat jevy ve své podstatě natolik škodlivé, že o potřebnosti autoritativního zásahu zvenčí nebude pochyb. Příkladem může být šíření dětské pornografie, krádeže identity, rozmanitá podvodná jednání, anebo kybernetické útoky ohrožující bezpečnost stěžejních informačních systémů.[190]

2.1.3. K regulaci definiční normou

Americký konstitucionalista Lawrence Lessig se ve svém díle věnuje normativitě kyberprostoru, kterou staví na vlastní teorii kódování. V rámci regulativů lidského chování zmiňuje právo, sociální normy a kód. Kód je předpisem, na jehož

[187] Otázkou zůstává, zda je však povinnost právem vymáhána skutečně efektivně a vůči správnému subjektu.
[188] K jiné situaci by došlo, nastal-li by důvod opravňující vypovězení společenské smlouvy. Případný rozbor společenské smlouvy však dalece přesahuje rámec práce. K teorii společenské smlouvy např. HOBBES, Thomas; CHOTAŠ, Jiří; MASOPUST, Zdeněk; BARABAS, Marina (eds.). *Leviathan, aneb, Látka, forma a moc státu církevního a politického*. 1. vyd. Překlad Karel Berka. Praha: OIKOYMENH, 2009.
[189] POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim. *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008, str. 20 – 21.
[190] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 101.

základě funguje informační infrastruktura. Nejedná se pouze o počítačový program, ale i o jiné formy technických pravidel, kterými mohou být parametry prostředí, formáty dat, přenosové protokoly apod.[191] Lessig označuje definiční normu jako kód. Definiční normy jsou vytvářeny subjekty, které mohou v kyberprostoru definovat určité prostředí. Tyto subjekty Lessig nazývá definičními autoritami a definiční normy označuje jako normy *sui generis*.[192] Jedná se o velmi efektivní formu regulace lidského chování. Lessig kód přirovnává k přírodním zákonům. Na rozdíl od přírodních zákonů můžeme kódu nejenom využít, nýbrž pomocí něj i regulovat a utvářet požadované chování. Až na komunitu hackerů je velká část uživatelů kyberprostoru nucena dodržovat právní pravidla, jsou-li zajištěna i kódem.[193] Právní norma oproti kódu samozřejmě takto inherentně efektivní není.

Kyberprostor je dle Lessiga tvořen vůlí definičních autorit. A přestože jsou to definiční autority, představované zejména poskytovateli nejrůznějších služeb informační společnosti (dále též „ISP“), kdo disponuje technickými kompetencemi a faktickými možnostmi přímo i bezprostředně ovlivňovat kódem informační sítě informační život společnosti,[194] i ony podléhají určité jurisdikci. Ve své specifické kybernetické normotvorbě nejsou tedy neomezené.

2.2. Vynutitelnost právních norem v kyberprostoru

Přes specifické vlastnosti kybernetického prostředí odmítají někteří autoři důvod odlišného přístupu v právu. S odmítavým přístupem, hraničícím s principem zakazujícím *denegatio iustitiae*, se lze setkat i v postoji některých orgánů činných v trestním řízení k uplatňování práva v prostředí informačních sítí.[195] Goldsmith uvádí,

[191] Podrobněji viz POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 188.
[192] Definiční normy mohou vytvářet telekomunikační operátoři, tvůrci on-line her nebo každý, kdo si otevře blog, anebo kdo má emailovou schránku a nastaví v ní určitý filtr pro příchozí zprávy. Podrobněji POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, 2007, str. 88 a násl.
[193] Např. u diskuzních serverů dochází k využívání automatického filtru zachycujícího vulgární výrazy. Hypotézou filtru je výskyt vulgárního výrazu a dispozicí smazání dotyčného příspěvku. Viz POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 188 – 193.
[194] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 109.
[195] Např. odložení trestního stíhání Policií ČR s poukázáním na to, že k trestnému činu pomluvy dle § 184 TZ došlo v prostředí internetového diskuzního fóra, v důsledku čehož není možné prokázat jeho spáchání.

že *„mezinárodní transakce v kyberprostoru se nijak neliší od těch, které známe z „reálného“ prostředí. Zahrnují jednotlivce umístěné v určitém prostoru pod jurisdikcí nějakého státu, kteří komunikují, ať už s dobrým nebo špatným efektem, s jinými jednotlivci rovněž umístěnými v reálném prostoru pod jurisdikcemi jiných států. Nenacházíme řádné normativní argumenty, které by podporovaly imunizaci kyberprostoru od klasické teritoriální regulace. A máme všechny důvody se domnívat, že státy mohou vykonávat svou autoritu na klasické teritoriální bázi a dostatečně regulovat transakce v kyberprostoru.“*[196] Nutno ovšem říci, že podobných názorů s postupem času a narůstajícím výskytem konkrétních problematických situací plynoucích z virtuální podstaty kyberprostoru ubývá.

Problematika vynutitelnosti právních norem v kyberprostoru, respektive v rámci sítě Internet, úzce souvisí s globálním charakterem a možností vzdálených interakcí jednotlivců v rámci sítí. Polčák chápe tzv. delokalizaci společenských vztahů jako jeden ze zásadních problémů aplikace právních norem v informační společnosti.[197] Upozorňuje na fakt, že *„teoretická formální platnost hmotného práva je postavena proti fakticitě ovlivněné kromě institucionálního fenoménu poskytovatelů služeb informační společnosti též problémy souvisejícími s globalitou informační sítě a suverenitou národních jurisdikcí.“*[198] Právě suverenita národních jurisdikcí činí v případě vyšetřování počítačové kriminality jeden z největších problémů. Například prohlídkou provedenou orgány jednoho státu skrze počítačovou síť dochází lehce k zásahu do státní suverenity druhého státu. Na poli mezinárodního práva je možné problém jurisdikce do určité míry řešit smluvně, ačkoli někteří autoři se zmiňují též o možné existenci obyčeje.[199] Efektivní vynutitelnost práva omezuje i výskyt negativních jurisdikčních

---

Usnesení napadl ministr spravedlnosti stížností pro porušení zákona, které Nejvyšší soud vyhověl. Viz rozsudek Nejvyššího soudu, sp. zn. 4 Tz 265/2000, ze dne 16. 1. 2001.

[196] GOLDSMITH, J. Against Cyberanarchy. *The University of Chicago Law Review.* 1998, č. 65, str. 1199 an. Překlad úryvku Polčák in POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 72 – 73.

[197] Delokalizaci lze chápat jako naprosté oddělení virtuálních společenských vztahů od fyzické infrastruktury jejich sítí. Podrobněji viz POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 101 - 103.

[198] Tamtéž, str. 14.

[199] SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1). Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10]. Překlad autorka.

konfliktů. Vybraným mezinárodním a evropským právním instrumentům se předkládaná práce podrobněji věnuje v kapitole páté.

K efektivní vynutitelnosti právních norem v kyberprostoru je zapotřebí posílit mezinárodní spolupráci, v jejímž rámci lze řešit problematiku státní suverenity a předcházet jurisdikčním konfliktům, stejně jako zlepšit spolupráci s definičními autoritami, které podstatnou měrou fakticky regulují internetové prostředí.[200]

2.3. Trestněprávní jurisdikce v kyberprostoru

Trestní právo bylo tradičně chápáno jako oblast výsostné pravomoci jednotlivých států, představující symbol svrchované státní moci vykonávané na území konkrétního státu a odrážející jeho specifické kulturní a morální normy. Státy zpravidla vykonávají státní moc s ohledem na konkrétní území (teritoriální pravomoc) či vůči svým státním příslušníkům (personální pravomoc). Suverénní státy určují normy vhodného chování v rámci svého státního území a toto chování následně vymáhají vůči osobám, které svým jednáním normy poruší, i zpravidla vůči vlastním státním příslušníkům, porušujícím dané normy vně území státu.

Podle zásady svrchované rovnosti států vykonávají státní moc na území státu jeho orgány nezávisle na cizí státní moci. Při výkonu státní moci jsou jednotlivé státy omezeny normami mezinárodního práva veřejného, které nedovolují, aby podrobily své moci cizí státy nebo aby zasahovaly do jejich vnitřních záležitostí.

Z povahy počítačové, a zejména kybernetické kriminality vyplývá, že jde o trestnou činnost hranicemi jednotlivých států zpravidla neomezenou.[201] Od počátku vyšetřování je zapotřebí klást zvláštní důraz na mezinárodní spolupráci mezi dotčenými státy, aby prováděnými vyšetřovacími úkony nedocházelo k zásahům státní moci do státní suverenity jiných států a porušení norem mezinárodního práva veřejného.

Se zásahy do státní suverenity úzce souvisí problematika státní pravomoci a místní působnosti vnitrostátních norem. V rámci vyšetřování počítačové kriminality nebývá vždy lehké zodpovědět otázku, zda došlo k porušení suverenity jiného státu,

[200] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 107.
[201] KOOPS, Bert-Jaap; BRENNER, Susan W. et al. *Cybercrime and Jurisdiction: A Global Survey*. Den Haag: T.M.C. Asser Press, 2006, str. 1. Překlad autorka.

popřípadě byl-li zásah do cizí státní suverenity z hlediska mezinárodního práva oprávněný.[202]

2.3.1. K pojmům jurisdikce a působnosti

Jurisdikcí rozumíme pravomoc státu, tedy soubor práv a povinností, které stát a jeho orgány vykonávají v rovině normotvorby, rovině soudní a rovině mocenské. Pojem pochází z latinského výrazu *ius dicere*, tedy určovat či nalézat právo. Značí *„moc stanovit nebo nalézat právo, kterou stát svěřuje svým orgánům za tím účelem, aby ji vykonávaly jeho jménem a podle zákona.“*[203] Daný soubor práv a povinností státu je limitován normami vyjadřujícími jejich působnost. Působnost blíže definuje okruh společenských vztahů, v jejichž rámci stát pravomoc vykonává. Tyto společenské vztahy jsou vymezeny různými kritérii, podle kterých rozeznáváme působnost místní, časovou, osobní a věcnou.[204] Pravomoc uplatňovaná na určitém území, za aplikace norem místní působnosti bývá často označována jako jurisdikce v užším slova smyslu.[205] Přestože dochází užíváním pojmu jurisdikce v užším slova smyslu do určité míry k matoucímu směšování dvou pojmů, pro další text bude praktické jej zvolit, a to s ohledem na zaměření rozboru pravomoci zejména ve smyslu pravidel místní působnosti. Proto následující text užívá pojmu jurisdikce ve smyslu uplatnění pravomoci státu v rámci pravidel místní působnosti trestněprávních norem.

Otázky působnosti časové a osobní nepůsobí v rámci problematiky postihu počítačové kriminality větší komplikace; naopak zvláštní význam zaujímá otázka místní působnosti trestního práva. Hranice místní působnosti jsou v případě trestní legislativy nastaveny poměrně široce. Běžně je možné stíhat trestné činy, které se odehrály mimo

[202] Podrobněji SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1). Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10]. Překlad autorka.
[203] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 15.
[204] JELÍNEK, Jiří; DANKOVÁ, Katarína; NAVRÁTILOVÁ, Jana; PELC, Vladimír; ŘÍHA, Jiří; STEJSKAL, Vojtěch. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktualizované a doplněné vydání. Praha: Leges, 2016, str. 66.
[205] TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1), str. 33.

území státu, avšak jejichž následky se na daném státním území projevily, stejně jako v určitých případech trestné činy, které zdánlivě nemají s územím státu žádnou spojitost.[206]

Určení rozhodného práva ve vztahu k jurisdikci nečiní u trestního práva problémy jako v případě soukromoprávního sporu, neboť trestní právo je odvětvím chránícím elementární hodnoty společnosti a státu a tedy bude-li příslušný k rozhodnutí ve věci orgán činný v trestním řízení, rozhodnutí bude činit vždy podle práva svého státu.[207]

2.3.2. Jednotlivé jurisdikční principy

Jednotlivé principy následující text uvádí v pojetí trestního zákoníku, přičemž je pro ilustraci doplňuje relevantními dokumenty mezinárodního i evropského práva.

2.3.2.1. Princip teritoriality

Princip teritoriality je vůdčí zásadou místní působnosti českého trestního zákona.[208] Princip, popřípadě zásada[209] teritoriality vyplývá ze státní svrchovanosti, podmínkou je ovšem spáchání činu na území státu.[210] Jako vůdčí princip jej uznává většina mezinárodních dokumentů na poli počítačové kriminality. Princip teritoriality je stále převažujícím konceptem v mnohých trestněprávních doktrínách světa.[211]

Působnost trestních zákonů se podle principu teritoriality vyjádřeného v § 4 TZ vztahuje na celé státní území bez ohledu na osobu pachatele či oběti, stejně jako na některá místa nacházející se vně státního území. Pro uplatnění místní působnosti

[206] Typickým příkladem je uplatnění zásady univerzality. K jednotlivým principům místní působnosti viz níže.
[207] POLČÁK, Radim. K problému působnosti trestního práva na internetu. *Acta Universitatis Carolinae. Iuridica*. 2008, 2008(4), str. 98.
[208] K pojmu trestního zákona srov. § 110 TZ.
[209] Práce užívá pojmů synonymně.
[210] JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 6. aktualizované vydání. Praha: Leges, 2016, str. 21.
[211] KOOPS, Bert-Jaap; BRENNER, Susan W. et al. *Cybercrime and Jurisdiction: A Global Survey*. Den Haag: T.M.C. Asser Press, 2006, str. 10. Překlad autorka.

netřeba, aby tu byl trestný čin uskutečněn ve všech svých znacích, ale dle ustanovení § 4 odst. 2 písm. a), písm. b) TZ postačí, *„dopustil-li se tu pachatel zcela nebo zčásti jednání, i když porušení nebo ohrožení zájmu chráněného trestním zákonem nastalo nebo mělo nastat v cizině“,* stejně jako *„porušil-li nebo ohrozil-li tu pachatel zájem chráněný trestním zákonem nebo měl-li tu alespoň z části takový následek nastat, i když se jednání dopustil v cizině.“* Tedy i v případě, kdy pachatel jedná v cizině, aniž by v tuzemsku zamýšlený následek nastal, bude delikt trestný podle tuzemského práva.[212] Zmíněné případy typické pro delikty počítačové kriminality označuje trestněprávní nauka jako distanční.

Jak poznamenává Táborová, *„vzhledem k tomu, že elektronická komunikace spočívá v přenosu informace, nelze striktně určit jedno jediné místo, kde se akt přenosu odehrál.“*[213] Z uvedeného důvodu vymezují státy jurisdikci šířeji. Takto může být založena podle místa zahájení nebo naopak skončení přenosu informace, tedy podle míst odeslání a doručení informace. Budeme-li vnímat podstatu kybernetické kriminality ve smyslu přenosu informace, můžeme dospět k závěru, že se jedná o tranzitní delikty. U tranzitních deliktů se považují za místo činu všechna místa, kde se rozvíjel vztah příčinné souvislosti mezi jednáním a účinkem.[214] Uvedený přístup by však u kybernetických deliktů vedl k nechtěné, až tristní situaci, neboť zjistit faktickou dráhu informace po síti by bylo téměř nemožné, zejména uvážíme-li rozmach služeb cloud computing.

Zmíněné „tranzitní“ pojetí je možné zúžit, vyjdeme-li z následující teze: V řadě případů je počítačový systém alfou a omegou počítačových deliktů, neboť zprostředkuje účinek konkrétního protiprávního jednání lidským smyslům. Dle mého názoru lze s ohledem na konkrétní trestný čin říci, že digitální informaci „vnímá“ buď člověk a stroj, anebo pouze stroj (člověk účinek buď nezaznamená vůbec, anebo nikoli skrze počítačový systém v podobě digitální). V případě stroje jím rozumím počítačové zařízení, které informaci určitým způsobem vyhodnotí a zpracuje. Hledisko akcentující okamžik, v němž bude informace vnímatelná a seznatelná smysly, prosazuje ve své

[212] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 69.
[213] TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1), str. 36.
[214] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 70.

práci mimo jiné Kerr. Podle něj k prohlídce počítače a zabavení dat nedochází okamžikem kopírování dat z dotčeného hard disku či jiného úložiště, ani okamžikem načtení dotčených dat počítačovým programem, nýbrž k ní dojde teprve v okamžiku, kdy je informace vystavena lidským smyslům a podrobena lidskému vnímání.[215] Rozhodné místo přenosu informace je tedy možné zúžit na místo vnímání konkrétních digitálních dat.

V rámci zásady teritoriality jsou státy, které jsou stranami mezinárodní smlouvy, povinny stíhat jakýkoliv počítačový delikt vymezený smlouvou, k jehož spáchání dojde na území takového státu. Typickým příkladem je čl. 22 odst. 1 písm. a) Úmluvy o počítačové kriminalitě, dále čl. 30 odst. 1 písm. a) Arabské úmluvy Ligy arabských států o boji proti trestným činům informačních technologií[216] nebo čl. 4 odst. 1 Opčního protokolu k Úmluvě o právech dítěte.[217] Důvodová zpráva k Úmluvě o počítačové kriminalitě uvádí jako možné uplatnění zásady teritoriality i v případě, kdy se napadený počítačový systém nachází na území státu, ačkoli pachatel nikoliv.[218] Stejně tak čl. 17 odst. 1 písm. a) směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV[219] stanoví působnost k trestnímu stíhání, pokud byl trestný čin spáchán zcela nebo zčásti na území státu, přičemž čl. 17 odst. 3 citované směrnice ukládá členským státům zajistit pro vybrané trestné činy vlastní jurisdikci i v případě spáchání trestných činů prostřednictvím ICT použitých z jeho území bez ohledu na to, zda jsou tyto ICT na jeho území skutečně provozovány či nikoli. V daném případě tedy postačí

[215] KERR, Orin S. Searches and Seizures in a Digital World. *Harvard Law Review* [online]. 2005, 119(531), str. 532 – 585. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=697541 [cit. 2016-02-24]. Překlad autorka.
[216] Arabská úmluva Ligy arabských států ze dne 21. prosince 2010 o boji proti trestným činům informačních technologií dostupná v anglickém znění na adrese http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences [cit. 2016-03-10].
[217] Opční protokol ze dne 19. prosince 2011 k Úmluvě OSN o právech dítěte. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 28/2016 Sb. m. s.
[218] *Explanatory Report to the Convention on Cybercrime (ETS No. 185)* [online]. Treaty Office. Council of Europe, 2001. Bod 233. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-03-10]. Překlad autorka.
[219] Dostupná na adrese http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1461056639475&uri=CELEX:32011L0093 [cit. 2016-12-04].

pro aplikaci zásady teritoriality i existence pouhého přístupu k ICT na území daného státu, byť se pachatel i oběť může fyzicky nacházet v jiných státech.[220]

2.3.2.2. Zásada registrace

Zásada registrace byla uzákoněna v českém trestním právu na základě požadavků mezinárodních smluv, kterými je Česká republika vázána. Zaručuje místní působnost českých trestních zákonů v případě trestného činu spáchaného mimo tuzemsko na palubě lodi, letadla či jiného vzdušného dopravního prostředku, jsou-li registrovány v České republice. Zásada registrace se řídí stejným režimem jako princip teritoriality.

2.3.2.3. Princip personality

Princip personality, resp. aktivní i pasivní zásada personality, jsou vůči zásadám teritoriality a registrace v poměru subsidiarity. Jejich uplatněním dochází k určitému zohlednění vztahu mezi státem a pachatelem, popřípadě mezi státem a obětí, pakliže jsou občany České republiky nebo tu mají povolen trvalý pobyt.

Podle aktivní zásady personality vyjádřené v § 6 TZ, se podle českého trestního zákona posuzuje trestný čin spáchaný v cizině občanem České republiky či osobou bez státní příslušnosti, avšak s povoleným trvalým pobytem na našem území. Naopak pasivní zásada personality vyjádřená v § 7 odst. 2 TZ umožňuje podle českého trestního zákona stíhat trestné činy spáchané v cizině proti občanu České republiky či osobě bez státní příslušnosti mající v tuzemsku trvalý pobyt, avšak za předpokladu trestnosti činu i v místě jeho spáchání (popřípadě nepodléhá-li místo žádné trestní pravomoci). Princip personality nelze zaměňovat s osobní působností trestních zákonů, která zohledňuje výjimky z působnosti trestních zákonů, a to ve smyslu hmotněprávní i procesněprávní exempce.

[220] Jurisdikce země A by tak mohla být dovozena i v natolik složité situaci, jako v případě ovládnutí počítače pomocí viru v zemi A, pachatelem nacházejícím se v zemi B, který by prostřednictvím počítače v zemi A umisťoval materiál dětské pornografie na webový server v zemi C.

Řada mezinárodních smluv vedle principu teritoriality aplikuje běžně i princip personality. Příkladem lze uvést čl. 17 odst. 1 písm. b) směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV nebo čl. 25 odst. 1 písm. d) Úmluvy o ochraně dětí před sexuálním vykořisťováním a sexuálním zneužíváním.[221]

Některé mezinárodní smlouvy omezují zásadu pasivní personality požadavkem tzv. oboustranné trestnosti.[222] Jde o požadavek, aby pachatelovo jednání bylo trestné i na území státu, kde k němu došlo. Podmínku oboustranné trestnosti stanoví i Úmluva o počítačové kriminalitě, protože však ve svém čl. 22 odst. 1 požaduje kriminalizaci konkrétních činů, definovaných jako počítačové delikty, dochází ke sjednocení hmotněprávní úpravy smluvních států Úmluvy o počítačové kriminalitě, v důsledku čehož je zajištěna i oboustranná trestnost u počítačových deliktů uvedených v čl. 2 až čl. 11 Úmluvy o počítačové kriminalitě. Současně však dochází i k vyšší pravděpodobnosti vzniku pozitivních jurisdikčních konfliktů, aniž by Úmluva o počítačové kriminalitě obsahovala jakákoli pravidla pro jejich řešení.

Čl. 22 odst. 3 Úmluvy o počítačové kriminalitě upravuje také princip *dedere aut judicare*, požadující buď extradici obviněného, anebo jeho trestní stíhání v zemi, jež jej odmítla vydat za účelem trestního stíhání do cizího státu s odkazem na jeho státní příslušnost. Úmluva o počítačové kriminalitě se tak snaží v každém případě zajistit postih pachatele počítačových trestných činů vymezených v čl. 2 až čl. 11 Úmluvy o počítačové kriminalitě, i při uplatnění principu aktivní personality, tj. v situacích, v nichž státy běžně nevydávají vlastní státní příslušníky k trestnímu stíhání do ciziny.

Pouze několik mezinárodních dokumentů upravuje i zásadu pasivní personality. Jedná se zejména o mezinárodní instrumenty na ochranu práv dětí.[223] O zásadě pasivní personality se zmiňuje například čl. 17 odst. 2 písm. a) směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu

[221] Úmluva Rady Evropy č. 201 ze dne 25. října 2007 o ochraně dětí před sexuálním vykořisťováním a zneužíváním. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 59/2016 Sb. m. s.
[222] V zahraniční literatuře též „double criminality" principle. KLIP, André. *European criminal law: an integrative approach*. 2nd ed. Cambridge: Intersentia, 2012, str. 344. Překlad autorka.
[223] *Comprehensive Study on Cybercrime* [online]. United Nations Office on Drugs and Crime, 2013. Dostupné z https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [cit. 2016-03-10]. Překlad autorka.

zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV.

2.3.2.4. Princip ochrany a univerzality

Princip ochrany vyjadřuje pragmatický přístup států chránících své zájmy i vně státního území, neboť právo jiných států běžně dostatečnou ochranu cizím státním zájmům neposkytuje. Vůči výše zmíněným principům se princip ochrany uplatní subsidiárně. Princip ochrany vyjadřuje požadavek stíhat trestné činy útočící na zvlášť důležité zájmy, bez ohledu na místo jejich spáchání i osobu pachatele.[224] Na základě zásady ochrany obsažené v § 7 odst. 1 TZ lze považovat za trestný dle tuzemských trestněprávních předpisů kybernetický útok vedený v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, ačkoli nebude možné dovodit místní působnost českého trestního zákona podle zásady teritoriality, registrace ani personality.

Subsidiární zásada univerzality vyjádřená v § 8 TZ stanoví podmínky, kdy lze dle českých zákonů posuzovat trestnost činu spáchaného v cizině cizím státním příslušníkem či osobou bez státní příslušnosti, která nemá na našem území trvalý pobyt. Subsidiarita značí subsidiární uplatnění zásady vůči extradici a předání osoby na základě evropského zatýkacího rozkazu a uplatní se pouze tehdy, požádá-li cizí stát o vydání nebo předání osoby a Česká republika žádosti vyhoví.[225]

Princip ochrany se například v USA uplatnil v poměrně známém zákoně USA Patriot Act, který zavedl pojem „chráněný počítač“. Jím se má na mysli počítač, jenž plní tzv. funkce mezinárodního obchodu a komunikace. Není důležité, zda se zmíněný počítač nachází na území USA či nikoli, plní-li stěžejní význam pro stát.[226] Uvedená právní úprava reaguje na teroristické útoky z 11. září 2001 a umožňuje účinnější boj proti kyberterorismu. Nutno ovšem podotknout, že úprava, která přinesla orgánům USA dříve nevídané vyšetřovací pravomoci, do značné míry omezila občanské svobody.

[224] JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 6. aktualizované vydání. Praha: Leges, 2016, str. 23.
[225] Tamtéž, str. 24.
[226] TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1), str. 37.

Patriot Act je z toho důvodu podroben značné kritice. Vyvážit únosnou míru pravomocí orgánů činných v trestním řízení při současném zachování informačních svobod je zejména v kybernetickém prostředí námětem neutuchajících debat. Terčem soudobých kritiků je především skutečnost, že citovaný zákon podstatně rozšířil okolnosti, za nichž ISP informují vyšetřovací orgány o domněle podezřelém obsahu uživatele.[227]

Princip univerzality je ze všech principů exteritoriální jurisdikce pojat nejobecněji, neboť bez ohledu na pachatele, oběť i místo činu stíhá stát na základě mezinárodních smluv v zájmu mezinárodní spolupráce vybrané mimořádně závažné trestné činy. Mezi státy však nepanuje jednotný názor, jaké trestné činy by měly být předmětem zásady univerzality. Zatímco podle některých má být princip univerzality vyhrazen pouze aktům spadajícím pod mezinárodní právo trestní, jiné státy navrhují zahrnout i závažné případy počítačové kriminality, jako například dětskou pornografii.[228] Počítačové trestné činy v širším slova smyslu v mnohých státech nespadají do kategorie stíhatelných činů při uplatnění principu univerzality. Výjimku představují Belgie s Německem. Tyto země na základě principu univerzality stíhají i právě zmíněné šíření dětské pornografie.[229]

Státy však zpravidla vyžadují existenci specifičtějšího vztahu mezi trestným činem a národním právním řádem, v zahraniční literatuře označovaný jako tzv. nexus requirement. Právě požadavek přítomnosti dalšího určujícího vztahu mezi státem a trestným činem opakovaně dovozuje Nejvyšší soud USA.[230]

---

[227] PODGOR, Ellen S. Computer Crimes and the USA Patriot Act. *Criminal Justice Magazine* [online]. 2002, 17(2). Dostupné z http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_17_2_crimes.html [cit. 2016-03-10]. Překlad autorka.

[228] *Comprehensive Study on Cybercrime* [online]. United Nations Office on Drugs and Crime, 2013, str. 194. Dostupné z https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [cit. 2016-03-10]. Překlad autorka.

[229] BRENNER, Susan W.; KOOPS, Bert-Jaap. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law* [online]. 2004, 4(1), str. 28. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507 [cit. 2016-03-10]. Překlad autorka.

[230] KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 14. Překlad autorka.

2.3.3. Vybraná hlediska moderní koncepce jurisdikce

Jurisdikční principy aplikované na případy počítačové kriminality často umožňují více státům uplatnit v trestním řízení vlastní pravomoc. Moderní jurisdikční koncepce proto usilují o nalezení dalších kritérií, které by v konkrétních případech určily jurisdikci co nejvhodnější. Uplatněním doplňkových hledisek poté státy předchází zejména výskytu pozitivních jurisdikčních konfliktů.

2.3.3.1. Test přiměřenosti

Moderní koncepce jurisdikce nespoléhají toliko na tradiční principy, nýbrž je dále podrobují testu přiměřenosti. Přístup je výsledkem určité snahy o racionalizaci výkonu státní moci.[231]

Brennerová a Koops zmiňují pravidla sepsaná v dokumentu respektovaném širší odbornou veřejností, s názvem Restatement (Third) of Foreign Relations Law of the United States,[232]z nichž lze při určení jurisdikce v širším kontextu vycházet. Hledisko přiměřené a rozumné jurisdikce je založeno na existenci některých z následujících pravidel:

- vztah činnosti vůči území státu, resp. rozsah, v jakém se daná činnost uskutečňuje v rámci území státu nebo v jakém má podstatný, přímý a předvídatelný dopad na území státu nebo v rámci území státu,
- právní vztah mezi osobou a státem, jako např. občanství, místo trvalého pobytu, výkon ekonomické činnosti apod., a to bez ohledu na to, zda je osoba pachatelem či obětí,

[231] V anglicky psané literatuře se objevuje termín „reasonableness“. Viz BRENNER, Susan W.; KOOPS, Bert-Jaap. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law* [online]. 2004, 4(1), str. 9. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507 [cit. 2016-03-10]. Překlad autorka.

[232] Dokument obsahuje právní texty vydávané Americkým právním institutem, na kterých se podílí renomovaní soudci, právníci i pedagogové. Dokument je dostupný z http://www.macalester.edu/courses/intl114/docs/restatement.pdf [cit. 2016-03-11]. Překlad autorka.

- charakter činnosti, její význam pro stát, míra, v jaké vykonávají jiné státy nad činností jurisdikci a v jaké je kontrola dané činnosti obecně akceptována,
- existence ospravedlnitelných výjimek, které mohou být v rámci jurisdikce dotčeny nebo naopak chráněny,
- politický, právní či ekonomický význam v mezinárodním měřítku,
- míra konzistence s tradicemi mezinárodního systému,
- míra, v jaké má jiný stát zájem na výkonu jurisdikce v dané věci,
- pravděpodobnost konfliktu s právním řádem jiného státu.[233]

Kritéria jsou poměrně obecná a poskytují státům pouze návod, čím je možné se při uplatnění vlastní jurisdikce řídit. S ohledem na nezávazný a doplňkový charakter pravidel bude při jejich aplikaci záležet především na jejich výkladu jednotlivými orgány činnými v trestním řízení.

2.3.3.2. Místo spáchání deliktu

Určení místa spáchání počítačového deliktu, zejména odehrál-li se v kyberprostoru, není jednoduché. Jak uvádím výše, za místo činu lze leckdy považovat všechna místa, kde se rozvíjel kauzální vztah mezi jednáním a účinkem. V určitých případech se zdá vhodné upřednostnit některé lokace před jinými.

Za místo spáchání deliktu je možné považovat fyzickou lokaci, kde pachatel užil nástroj ke spáchání trestného činu, kterým je počítačový systém, včetně technického vybavení k překonání bezpečnostních opatření. Jiný úhel pohledu vnímá jako místo spáchání deliktu i území, kde se fyzicky nachází cílový počítačový systém, do něhož se pachatel snaží neoprávněně získat přístup.[234]

V případě počítačových trestných činů souvisejících s obsahem, jako například u trestných činů týkajících se dětské pornografie či rasistických a jiných nenávistných

[233] BRENNER, Susan W.; KOOPS, Bert-Jaap. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law* [online]. 2004, 4(1), str. 8 - 9. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507 [cit. 2016-03-10]. Překlad autorka.
[234] KOOPS, Bert-Jaap; BRENNER, Susan W. et al. *Cybercrime and Jurisdiction: A Global Survey*. Den Haag: T.M.C. Asser Press, 2006, str. 11. Překlad autorka.

projevů šířených prostřednictvím Internetu, budou podle Brennerové a Koopse více určujícími elementy jednání, vztahující se k šíření závadného obsahu, jeho zpřístupňování a zprostředkování, než elementy vztahující se k pachatelově fyzické přítomnosti na určitém místě.[235] Přístup představuje tzv. doktrínu efektu.[236] Též Kolouch a Volevecký uvádí, že pro zodpovězení otázky, zda stíhat či nestíhat internetový trestný čin, je zpravidla rozhodující místo, kde nastal účinek trestného činu.[237]

2.3.3.3. Významný vztah deliktu k území státu

Aplikací principu teritoriality lze dojít k širokému vymezení jurisdikce. Výše uvedený test přiměřenosti požaduje, aby byl výkon státem uplatněné pravomoci v konkrétním případě rozumný. Esencí testu přiměřenosti se tak stává míra přítomnosti dostatečného pojítka mezi státem a deliktem. Zahraniční literatura obsahuje požadavek, podle něhož musí být vztah deliktu ke konkrétnímu státu ve své povaze dostatečně významný.[238]

Význam spojení je běžně posuzován subjektivními měřítky jednotlivých států. Často je předmětem posouzení místo, kde se projevil efekt trestněprávně relevantního jednání, které se nemusí překrývat s místem odeslání ani doručení informace. Typicky půjde o případy, kde dochází k využívání služeb informační společnosti ve smyslu ukládání obsahu poskytnutého uživatelem, tedy tzv. hosting.[239] K posouzení přítomnosti

[235] KOOPS, Bert-Jaap; BRENNER, Susan W. et al. *Cybercrime and Jurisdiction: A Global Survey*. Den Haag: T.M.C. Asser Press, 2006, str. 11. Překlad autorka.
[236] Koops a Brennerová hovoří o „*jurisdiction over effect*“. Viz BRENNER, Susan W.; KOOPS, Bert-Jaap. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law* [online]. 2004, 4(1), str. 15. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507 [cit. 2016-03-10]. Překlad autorka.
[237] KOLOUCH, Jan; VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České Republiky v Praze. 2013, str. 27.
[238] Objevují se termíny „*substantial link*“, či „*sufficient connection*“, či „*genuine link*“. Viz KOOPS, Bert-Jaap; BRENNER, Susan W. et al. *Cybercrime and Jurisdiction: A Global Survey*. Den Haag: T.M.C. Asser Press, 2006, str 12.; SIEBER, Ulrich. *General report on Internet crimes: for the 18th International Congress of the International Academy of Comparative Law*. Washington D.C.: International Academy of Comparative Law, 2010, str. 59. Překlad autorka.
[239] TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1), str. 36.

dostatečně významného vztahu tak často dojde za uplatnění doktríny efektu, díky níž mohou státy lépe zhodnotit dopad konkrétního deliktu na své území.

Úmluva o počítačové kriminalitě významný vztah deliktu k území státu nijak neupravuje. V zahraniční judikatuře se lze s posouzením významného vztahu a potažmo i se samotným zhodnocením uplatněného výkonu jurisdikce již setkat. Závěry soudů však nejsou přijímány na poli mezinárodního společenství jednoznačně.

2.3.3.4. Vybrané příklady ze zahraniční judikatury

Příklady ze zahraniční judikatury prokazují značně subjektivní přístup národních soudů k otázce trestní jurisdikce. Místní působnost trestního práva je tradičně nastavena široce, a pokud tomu tak není, soudy se nebrání atrahovat ji svým výkladem pro konkrétní (zpravidla vlastní) stát.

K otázce trestní jurisdikce v případě trestného činu spáchaného v rámci Internetu se vyjádřil britský Královský soudní dvůr v trestní věci týkající se šíření rasově nenávistných materiálů umístěných na kalifornském serveru.[240] V předmětné věci byla obhajobou zpochybněna jurisdikce britských soudů, neboť k publikaci nenávistného obsahu došlo prostřednictvím serveru umístěného v USA, kde byl čin na ústavní úrovni chráněn institutem svobody projevu. Britský soud na základě předchozích případů dospěl k závěru opačnému. Argumentoval, že z podstatné části pachatel trestněprávně relevantně jednal na území Velké Británie a obžalované, kterým USA zamítla poskytnutí azylu, odsoudil k několikaletému nepodmíněnému trestu odnětí svobody.

Dalším případem, který se rovněž vztahuje k šíření nelegálního obsahu, je v zahraniční literatuře hojně diskutovaná trestní kauza, kterou se zabývalo francouzské soudnictví již v roce 2000.[241] Spor se týkal americké společnosti The Yahoo!, Inc., které francouzský soud nařídil zablokovat francouzským residentům přístup k nacistickým memorabiliím, jež společnost nabízela v rámci internetové aukce. Ve Francii se jednalo o nelegální digitální obsah, neboť francouzský trestní zákoník zakazuje zveřejňování

[240] Rozhodnutí Královského soudního dvora, sp. zn. 2009.04020 B5, ze dne 29. 1. 2010. Zkrácená verze rozhodnutí v *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1), str. 22.
[241] Rozsudek Tribunal de Grande Instance de Paris, ve věci The Yahoo!, Inc., ze dne 20. 11. 2000. Vybrané pasáže dostupné z http://www.lapres.net/yahweb.html [cit. 2015-06-03]. Překlad autorka.

nacistických symbolů. Data byla uložena na serverech umístěných na území USA, kde propagace nacistických předmětů spadá pod ochranu Prvního dodatku k Ústavě USA.[242] Francouzský soud proklamoval pravomoc rozhodnout ve věci na základě domněnky, že protiprávní jednání a s ním spojená újma z propagace nacistických symbolů měly podstatný dopad na území Francie a na francouzské občany a residenty. Rozhodnutí francouzských soudů však nenašlo oporu u soudů amerických a nebylo na půdě USA nijak vymahatelné.

Ve výše zmíněných judikátech se jednalo o materiály obrazové či písemné v místní jazykové verzi. Nabízí se proto otázka, zda lze předpokládat významný vztah deliktu k území státu i v případě, kdy by zakázaný obsah byl publikován v cizím jazyce. Kaspersen,[243] předseda legislativních komisí Rady Evropy v době vypracování návrhů Úmluvy o počítačové kriminalitě i Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů (dále též „Dodatkový protokol k Úmluvě o počítačové kriminalitě“),[244] uvádí, že pakliže bude informace konstituující trestný čin zveřejněna na Internetu, národní soudy vesměs nepředpokládají žádný efekt v případech, kdy je daná informace uvedena v cizím jazyce a jasně určena pro cizí státní příslušníky.[245]

Na základě výše uvedeného lze dovodit jurisdikci České Republiky pro případy jak obrazového, tak písemného materiálu v českém jazyce, ačkoli bude uložen na serverech lokalizovaných mimo státní území. Například v případě rasistických a xenofobních webových stránek White Media, hostovaných na kalifornském serveru v USA, avšak publikujících obrazové i písemné materiály v českém jazyce, tedy fakticky zaměřené na občany a území České republiky, je možné bez dalšího dovodit působnost českého trestního zákona a pravomoc českých orgánů činných v trestním řízení. K závěru dojdeme aplikací principů teritoriality, doktríny efektu a významného vztahu deliktu a státu.

---

[242] *The First Amendment of the Constitution of the United States* [online]. Dostupné z https://www.law.cornell.edu/constitution/first_amendment [cit. 2015-06-03]. Překlad autorka.
[243] Henrik W. K. Kaspersen je emeritním profesorem na Vrije Universiteit Amsterodam v Nizozemí, a bývalý ředitel Institutu pro informační technologie a právo tamtéž.
[244] Dodatkový protokol č. 189 ze dne 28. ledna 2003 k Úmluvě Rady Evropy o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 9/2015 Sb. m. s.
[245] KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 12. Překlad autorka.

Co se písemného materiálu v cizích jazykových verzích týče, situace se jeví nejasně. Striktní přístup zaujalo německé soudnictví, které dovodilo pravomoc německých soudů i v případě písemného obsahu v anglické jazykové verzi, uloženého na serveru mimo území státu. Německý odvolací soud nekompromisně odsoudil pachatele za trestný čin ohrožování veřejného pořádku. Frederik Toben, australský občan, na webu hostovaném na serveru v Austrálii popíral Holocaust. Německý odvolací soud dovodil pravomoc německých soudů i za okolností, kdy trestný čin je spáchán na území jiného státu cizím státním občanem, je-li způsobilý ohrozit veřejný pořádek v Německu. Ačkoli se jednalo o webové stránky v anglickém jazyce, které Toben vůči německým občanům nijak nepropagoval, umožnění přístupu německým občanům k uvedenému anglickému obsahu postačovalo německému soudu k tomu, aby Tobena po jeho příjezdu do Německa umožnil vzít do vazby a poté odsoudit podle německého trestního zákoníku za trestný čin ohrožování veřejného pořádku v Německé spolkové republice.[246] Důvodová zpráva Rady Evropy k Dodatkovému protokolu[247] bohužel neposkytuje žádnou další informaci k problematice publikace rasistických a xenofobních materiálů v cizích jazykových verzích. Nezbývá než opět vyjít z uvedených hledisek moderní koncepce jurisdikce.

2.3.4. Jurisdikční konflikty

Vzhledem k charakteru počítačové kriminality často dochází k situaci, kdy jsou k trestnímu stíhání příslušné orgány dvou či více různých států. V takovém případě hovoříme o konfliktu konkurujících pravomocí či o pozitivním konfliktu pravomocí, tj. o pozitivním konfliktu jurisdikce. Oproti tomu negativní jurisdikční konflikt, kdy není dovozena jurisdikce žádného státu, popř. kdy žádný ze států nemá zájem na výkonu

[246] Rozhodnutí Bundesgerichtshof, sp. zn. 1 StR 184/00, ze dne 12. 12. 2000. Vybrané pasáže rozhodnutí přeložené do anglického jazyka a rozbor případu viz KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 201 - 204. Překlad autorka.

[247] *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* [online]. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d37ae [cit. 2016-03-15]. Překlad autorka.

jurisdikce, může nastat také, jakkoli se ve vztahu k počítačové kriminalitě bude jednat o méně obvyklou situaci.

O negativním konfliktu jurisdikce lze hovořit za situace, kdy dopad deliktu bude ve svém souhrnu značný, avšak jednotlivými státy nebude vyhodnocen jako dostatečně závažný k tomu, aby jejich orgány činné v trestním řízení zahájily v jednotlivých případech trestní stíhání. Konkrétním příkladem by mohl být virus, který z globálního pohledu napáchá na v různých státech citelné škody, avšak žádný z příslušných orgánů trestní stíhání nezahájí, neboť každý stát zaznamená toliko nepatrnou část z celkově způsobené škody.[248]

2.3.4.1. Pozitivní konflikt

Vyznačuje-li se právní vztah, lhostejno zda soukromoprávní či veřejnoprávní, mezinárodním prvkem, lze spatřovat snahu národních soudů dostat zmíněný vztah pod vlastní jurisdikci.[249] Jedním z prvních jurisdikčních pozitivních konfliktů byl případ francouzského parníku Lotus, který havaroval v tureckých vodách při srážce s tureckým parníkem. Spor se roku 1927 dostal ke Stálému dvoru mezinárodní spravedlnosti v Haagu, který v případu uplatnil doktrínu efektu.[250] Uvedený přístup nikoli fyzické, nýbrž tzv. efektivní přítomnosti pachatele na státním území, je možné uplatnit i v případech počítačové kriminality.[251]

Pozitivní jurisdikční konflikty řeší státy na základě mezinárodní spolupráce zpravidla formou konzultací, s cílem nalézt nejvhodnější místo pro zahájení trestního stíhání.[252] Formální i neformální komunikace bývá nejvhodnější strategií řešení positivních jurisdikčních konfliktů a způsob, jak se vyvarovat souběžnému trestnímu stíhání vedenému orgány více států. V případě práva Evropského společenství byla

[248] Podrobněji KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 6. Překlad autorka.
[249] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 103.
[250] Rozhodnutí *Permanent Court of International Justice*, Ser. A, No. 10, 1927. Dostupné z http://www.worldcourts.com/search/search.cgi?zoom_query=lotus&zoom_cat[]=29 [cit. 2016-03-15].
[251] POLČÁK, Radim. K problému působnosti trestního práva na internetu. *Acta Universitatis Carolinae. Iuridica*. 2008, 2008(4), str. 99.
[252] Např. čl. 22 odst. 5 Úmluvy o počítačové kriminalitě nebo čl. 25 odst. 8 Úmluvy o ochraně dětí proti sexuálnímu vykořisťování a sexuálnímu zneužívání.

upřednostňována strategie směřování soudních řízení do jediného státu.[253] Nyní je kladen důraz na vzájemnou spolupráci a pohotovostní výměnu informací týkajících se trestných činů vymezených v příslušných pramenech evropského práva, jako je tomu v čl. 13 odst. 1 směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.[254] Jednání mezi státy může probíhat na bilaterální úrovni či prostřednictvím institucí jako Interpol, Europol a Eurojust.[255]

V rámci postihu počítačové kriminality bývá běžné, že hlavní slovo mají orgány činné v trestním řízení ve státě, kde se domnělý pachatel aktuálně zdržuje. Výjimku z tohoto zavedeného pravidla pro vymezené trestné činy stanoví čl. 22 odst. 5 Úmluvy o počítačové kriminalitě, který uvádí: *„Pokud si více než jedna strana nárokuje pravomoc vůči údajnému trestnému činu podle této Úmluvy, zúčastněné strany se, pokud to bude vhodné, vzájemně poradí, aby určily nejvhodnější pravomoc pro trestní stíhání.“* Úprava zaměřená na neformální konzultaci je velice flexibilní. Slovní spojení „pokud to bude vhodné“ může poukazovat na situace, kdy jedna ze zúčastněných stran Úmluvy o počítačové kriminalitě již ohlásila svůj záměr dále ve věci nečinit další kroky. V takovém případě mohou být konzultace odloženy.[256] Naopak tomu může být v situaci, kdy se jedna ze zúčastněných stran obává, že by trestní stíhání v jiné zemi ohrozilo vyšetřování vedené na domácí půdě.

2.3.4.2. Negativní konflikt

Případy, kde pravomoc může uplatnit vícero států, avšak ani jeden tak nečiní, představují pro pachatele počítačové kriminality ideální koncept, neboť trestný čin

[253] Viz dřívější úprava v čl. 11 odst. 5 Rámcového rozhodnutí Rady 2005/222/SVV, které již nahradila nová směrnice EP a Rady 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.
[254] Dostupná z http://eur-lex.europa.eu/search.html?DTN=0040&DTA=2013&qid=1480877459921&DB_TYPE_OF_ACT=directive&CASE_LAW_SUMMARY=false&DTS_DOM=ALL&excConsLeg=true&typeOfActStatus=DIRECTIVE&type=advanced&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL [cit. 2016-12-04].
[255] *Comprehensive Study on Cybercrime* [online]. United Nations Office on Drugs and Crime, 2013, str. 195. Dostupné z https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [cit. 2016-03-10]. Překlad autorka.
[256] KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 18. Překlad autorka.

zůstane nepotrestán. Důvodem tohoto negativního jevu mohou být nedostatky procesního práva jednotlivých států, spoléhání se na aktivní konání orgánů jiného státu či pochybení příslušných orgánů.[257] Polčák uvádí příklad, ve kterém Policie České republiky odložila případ trestného činu pomluvy dle § 184 TZ z důvodu jeho spáchání v prostředí internetového fóra s odkazem na nemožnost prokázat spáchání činu. Poznatek, že k deliktu došlo v prostředí globální počítačové sítě, postačil vyšetřovateli k tomu, aby se činem dále nezabýval.[258]

Pozitivní i negativní jurisdikční konflikty od počátku ovlivňují postih počítačové kriminality. S ohledem na suverenitu jednotlivých států obvykle nelze hledat řešení mimo formy mezinárodní spolupráce, umožňující definovat nejvhodnější jurisdikci nebo požádat cizí stát o právní pomoc. Větší výzvou se v řadě případů stává nikoli určení jurisdikce, nýbrž samotné vyšetřování počítačové kriminality, které se bez mezinárodní spolupráce neobejde. Seitz uvádí, že až 80% všech případů v Německu, v nichž je Internet prostředím deliktu nebo nástrojem k jeho spáchání, vyžaduje přístup k digitálním důkazním prostředkům uložených na serverech v zahraničí.[259] Právnímu rámci vyšetřování počítačové kriminality podle českého trestního práva procesního se věnuje kapitola čtvrtá. Pátá kapitola předkládané práce poté pojednává o mezinárodní spolupráci při postihu počítačové kriminality.

[257] TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1), str. 35.
[258] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 105. Rozsudek Nejvyššího soudu, sp. zn. 4 Tz 265/2000, ze dne 16. 1. 2001.
[259] SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1). Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10]. Překlad autorka.

3. POČÍTAČOVÁ KRIMINALITA JAKO FORMA ORGANIZOVANÉHO ZLOČINU A TERORISMU

Počítačová kriminalita jako specifická kategorie trestné činnosti disponující vlastnostmi, mezi něž patří přeshraniční charakter, globální dosah, anonymita, snadná manipulovatelnost daty i rychlý koloběh inovace, patří mezi nebezpečné jevy ohrožující mezinárodní společenství. Závažná trestná činnost, jakou je organizovaný zločin a terorismus, představuje nebezpečí pro demokratický právní stát, neboť oslabuje jeho společenské struktury, bezpečnostní i justiční složky, sféru politickou i administrativní. Vlivem organizovaného zločinu i terorismu dochází k pokřivení společenských hodnot i morálky, k radikalizaci společnosti a narušení spravedlivého společenského uspořádání.

V rámci mezinárodního společenství, zejména na půdě EU, Organizace spojených národů i Rady Evropy, zaznamenáváme snahy organizovaný zločin a terorismus tvrdě stíhat. Kapitola se snaží nalézt odpověď na otázku, zda existuje spojení počítačové kriminality a organizovaného zločinu, jakož i počítačové kriminality a aktivit terorismu. Zaměření se na propojení uvedené závažné trestné činnosti s počítačovou kriminalitou může přinést nové poznatky pro další studium těchto společensky nebezpečných jevů s mezinárodním přesahem.

Obsahem kapitoly je rozbor a obecná charakteristika organizovaného zločinu v pojetí dokumentů mezinárodního práva i dle českého právního řádu. Kapitola se soustředí posléze na oblast kriminálních aktivit, kde se organizovaný zločin propojuje s počítačovou kriminalitou. Kapitola se rovněž věnuje specifickým kriminogenním faktorům a rozebírá vybrané formy specializované počítačové trestné činnosti, které se objevují mezi aktivitami organizovaného zločinu. Pojednává dále o terorismu, popisuje jeho promítnutí do kybernetického prostředí a rozebírá relevantní úpravu na úrovni mezinárodní i vnitrostátní. Okrajově se kapitola dotýká i velice aktuálního fenoménu, kterým je kybernetická bezpečnost.

3.1. Organizovaný zločin

3.1.1. Historický vývoj

Organizovaný zločin nebo organizovaná kriminalita[260] představuje jev, jehož vnímání a vymezení vždy do značné míry vedle právní nauky ovlivňovala i sféra mediální a politická. Termín organizovaný zločin se poprvé objevil před více než sto lety v USA. Snahy o jeho vymezení od roku 1920 v zásadě kolísají mezi pojetím, které klade důraz na organizaci, a přístupem naopak zdůrazňujícím aktivity, jimiž se organizovaný zločin zabývá. Prvý přístup definuje organizovaný zločin jako určitou stabilní ilegální organizaci, jejíž členové se pravidelně zapojují do páchání trestné činnosti. Druhý přístup jej vnímá spíše jako uskupení závažných kriminálních aktivit, zaměřujících se především na zabezpečování ilegálního zboží a služeb, přičemž tyto aktivity jsou vykonávány s cílem dosažení co největšího zisku.[261]

Veřejnost, média a politická sféra nejčastěji pod spojením organizovaný zločin označují mafiánská uskupení, představovaná sicilsko-americkou Cosa Nostra, japonskou Yakuzou či drogovými kartely Latinské Ameriky a dalšími kriminálními organizacemi po celém světě s trvalou hierarchickou strukturou. Na půdě EU se konkrétně hovoří jak o organizovaných kriminálních uskupeních, tak o konkrétních oblastech závažné trestné činnosti, v nichž organizované skupiny působí.[262] Koncept kriminální organizace či sítě se mnohdy používá pro nejrůznější organizační modely, ať již půjde o kriminální organizaci primárně s rodinnou základnou, anebo na sebe volně navazující kriminální aktivity organizované pouze okrajově.[263]

Rozsáhlé strukturované organizace typu drogových kartelů nebo sicilské mafie, jejichž struktury zasahují do státní politiky a ekonomiky, jsou spíše vzácné. Vznikají v kontextu slabé vlády, neschopné zabezpečit život a majetek místního obyvatelstva a další jeho základní potřeby. Kořeny organizovaných mafiánských skupin jako sicilská Cosa Nostra a ´Ndrangheta sahají do 18. století a do značné míry nahrazovaly

[260] Pojmy jsou mnohými autory užívány synonymně, taktéž je tomu v této práci. Nelze ovšem směšovat pojmy organizované zločinecké skupiny tak, jak ji chápe výkladové ustanovení § 129 TZ, a organizované skupiny, která je znakem řady kvalifikovaných skutkových podstat trestných činů.
[261] PAOLI, Letizia (ed.). *The Oxford handbook of organized crime*. [1st ed.]. Oxford: Oxford University Press, 2014, str. 14. Překlad autorka.
[262] Tamtéž, str. 2 - 3.
[263] GOUNEV, Philip; RUGGIERO, Vincenzo (eds.). *Corruption and Organized Crime in Europe: Illegal partnerships*. New York: Routledge, 2012, str. 8 – 9. Překlad autorka.

nedostatečnou roli státu v některých oblastech státní politiky. Jiné organizace, představované zejména kolumbijskými a mexickými drogovými kartely, vznikají teprve později za účelem poptávky západní společnosti po ilegálních drogách. I tyto těží ze slabé role zkorumpovaných místních vládních struktur.[264] Vedle široce působících a hierarchicky organizovaných uskupení existují po celém světě kriminální organizace, které se zaměřují primárně na vytváření ekonomického profitu. Jejich aktivity, zprvu představované vydíráním a výběrem výpalného, byly spjaty s konkrétním územím a zaměřeny na specifické společenství. Později došlo k rozšíření pole ilegálních aktivit, z nichž kriminální organizace profitují, přičemž bylo zároveň možné zaznamenat rozvoj činnosti organizovaných skupin i za hranice jejich původních teritorií.

Především od 90. let hovoříme o výskytu nadnárodního organizovaného zločinu. Od té doby značná část zemí západního světa, podporována činností mezinárodních organizací, přijala řadu domácích, regionálních i univerzálních právních instrumentů zaměřených na boj proti organizovanému zločinu. Následkem uvedených politik došlo v mnoha zemích k značnému rozšíření pravomocí orgánů činných v trestním řízení.[265] Dochází-li k vážnému ohrožení fungování společnosti, je však přiměřený zásah do ústavně garantovaných práv a svobod akceptovatelný. I některé procesní instituty používané v boji s organizovaným zločinem jsou proto utajované, což vede k absenci běžných prostředků kontroly v trestním řízení.[266] Na poli EU představuje organizovaná trestná činnost s přeshraničním charakterem, stejně jako trestná činnost v oblasti výpočetní techniky, harmonizovanou oblast, v níž Evropský parlament a Rada stanoví cestou směrnic členským státům minimální pravidla týkající se vymezení trestných činů a sankcí.[267]

Území České republiky využívají nadnárodní zločinecké skupiny jako tranzitní či zdrojové, popřípadě je zneužívají k legalizaci výnosů z trestné činnosti. Nadnárodní organizovaný zločin představuje pro Českou republiku ohrožení vnitřní i vnější

[264] PAOLI, Letizia (ed.). *The Oxford handbook of organized crime*. [1st ed.]. Oxford: Oxford University Press, 2014, str. 3. Překlad autorka.
[265] Tamtéž, str. 15. Překlad autorka.
[266] STUPKOVÁ, Lucie. Institut spolupracujícího obviněného a korunního svědka ve světle základních zásad trestního práva procesního. In: JELÍNEK, Jiří (eds). *Základní zásady trestního řízení – vůdčí ideje českého trestního procesu.* Praha: Leges, 2016, 2010.
[267] Viz čl. 83 odst. 1 Smlouvy o fungování Evropské unie. Dostupné z http://eur-lex.europa.eu [cit. 2016-12-11].

bezpečnosti, přičemž v globalizovaném světě bude vychýlení vnitřní bezpečnosti jedné země negativním faktorem i pro bezpečnost zemí jiných.[268]

3.1.2. Charakteristika organizovaného zločinu

Organizovaný zločin lze z kriminologického úhlu pohledu charakterizovat jako *„opakující se (soustavné) páchání cílevědomě koordinované závažné trestné činnosti (a aktivit tuto činnost podporujících), jehož subjektem jsou zločinecké skupiny nebo organizace (většinou s vícestupňovou vertikální organizační strukturou) a jehož hlavním cílem je dosahování maximálních nelegálních zisků při minimalizaci rizika.“*[269] Cejp akcentuje ve svém pojetí kriminální aktivity, nikoli organizaci. Organizovaný zločin chápe především jako zabezpečování aktivit, jež jsou zakázané, regulované nebo obtížně dostupné, avšak společností žádané, přičemž jejich primárním cílem je vždy ekonomický profit. Tyto aktivity pokrývají oblasti, mezi něž patří obchod s lidmi (včetně prostituce a nelegální migrace), obchod s návykovými látkami či nelegální obchod se zbraněmi, a dále zasahují do oblastí finanční, počítačové a násilné kriminality.[270]

Chceme-li charakterizovat organizovaný zločin, musíme si především uvědomit, že se jedná o aktivity a skupiny organizované, které se primárně zaměřují na dlouhodobé dosahování zisku. Mezi hlavní charakteristiky organizovaného zločinu patří *„absence ideologií, organizovaná hierarchie či struktura organizace, kontinuita aktivit, užití násilí, síly nebo hrozby násilím, omezené členství, ilegální podnikání, pronikání do legální ekonomiky a schopnost korupce.“*[271] Jednotlivé organizované zločinecké skupiny charakterizujeme dle konkrétních vlastností jako velikost organizované zločinecké skupiny, počet a „pestrost“ realizovaných kriminálních aktivit, podíl

[268] CEJP, Martin; BLATNÍKOVÁ, Šárka; HÁKOVÁ, Lucie; HOLAS, Jakub; TRÁVNÍČKOVÁ, Ivana; VLACH, Jiří. *Společenské zdroje vývoje organizovaného zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 9.
[269] CEJP, Martin. *Vývoj organizovaného zločinu na území České republiky*. Praha: Institut pro kriminologii a sociální prevenci, 2010, str. 10.
[270] CEJP, Martin; BLATNÍKOVÁ, Šárka; HÁKOVÁ, Lucie; HOLAS, Jakub; TRÁVNÍČKOVÁ, Ivana; VLACH, Jiří. *Společenské zdroje vývoje organizovaného zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 15.
[271] Tamtéž, str. 18.

přeshraničních operací, míra využití násilí a korupce pro dosažení cílů skupiny, pronikání do legálních ekonomických aktivit, nebo i zda se členové skupiny vůči ostatním vymezují určitou sociální či etnickou identitou.[272]

3.1.2.1. Kriminogenní faktory

Organizovaný zločin ve svůj prospěch využívá specifické faktory společenského uspořádání, které jeho činnost usnadňují, popřípadě mohou být i jeho příčinou. Pakliže tyto faktory souvisí s kriminalitou ve společnosti, hovoříme o kriminogenních faktorech. V jejich rámci lze rozlišit jak kriminogenní faktory subjektivní, tj. spjaté s psychickými a fyzickými vlastnosti jedince, tak faktory objektivní, působící v rámci celého společenského systému.[273]

Jako hlavní objektivní kriminogenní faktor organizovaného zločinu v České republice zdůrazňuje Cejp globalizaci současného světa. V důsledku globalizace dochází ke vzájemnému celosvětovému propojení obchodních, právních a finančních systémů a z toho plynoucí vzájemné závislosti jednotlivých zemí, které ztrácí hospodářskou i fyzickou autonomii. Globalizaci doprovází anonymita komunikačních sítí a globální dosah internetu. Prohlubují se rozdíly mezi politickými systémy a v určitých regionech dochází k destabilizaci politické situace. Organizovaný zločin bývá běžně zapojen do válečných a politických konfliktů, které využívá ve svůj prospěch, ať již k získání ekonomického profitu či politické výhody pro své budoucí působení. Válečné konflikty tak může organizovaný zločin využít k obchodu se zbraněmi, s lidmi či k organizování nelegální migrace.[274]

Uvedené aspekty globalizace přispívají k anonymitě jedinců jednajících v rámci propojeného společenství i k obtížné regulaci a kontrole globálních systémů včetně sítě internet. Organizovaný zločin získává široké pole působnosti pro zvolené kriminální aktivity. Vzhledem k specifickým vlastnostem sítě internet, popsaným v práci výše,

[272] Detailněji k typologii organizovaných zločineckých skupin viz CEJP, Martin; BLATNÍKOVÁ, Šárka; HÁKOVÁ, Lucie; HOLAS, Jakub; TRÁVNÍČKOVÁ, Ivana; VLACH, Jiří. *Společenské zdroje vývoje organizovaného zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 19 - 20.
[273] CEJP, Martin. Organizovaný zločin v České republice v mezinárodním kontextu. *Trestněprávní revue*. 2016, 15(4), str. 88.
[274] Tamtéž, str. 89 - 90.

získává organizovaný zločin v globálních systémech jednoduchý způsob dosažení velkých zisků skrze co nejnižší náklady. Nábor nových členů skupiny je snazší, stejně jako vyhledávání nejdostupnějších a nejzranitelnějších objektů útoku. Získání nástrojů ke spáchání trestné činnosti je rovněž jednodušší. Prostředky získané trestnou činností jsou posléze snadno legalizovány v globálních platebních systémech. Způsoby páchání trestné činnosti jsou neustále inovovány a vzájemná spolupráce jednotlivých členů zrychlována a zjednodušována. Mark Galeotti poukazuje na skutečnost, že *„mezinárodní zločin se přelévá ze země do země podle toho, kde vidí dobré příležitosti.“*[275] V případě kybernetického prostředí uvedené pro organizovaný zločin neplatí, neboť tu existuje území jediné - globální virtuální prostor.

Co se subjektivních kriminogenních faktorů týče, jedná se o individuální faktory spjaté se strukturou osobnosti pachatele organizovaného zločinu, projevující se v jeho vlastnostech a chování. Zkoumání osobnosti organizovaného zločince je téma sporadické, u nás se mu věnoval například Netík a Markusová.[276] Dle výsledků psychologického zkoumání odsouzených pachatelů organizované kriminality a jejich porovnání s osobami odsouzenými za spáchání trestné činnosti neorganizované je možné shrnout, že osobnost pachatele organizovaného zločinu se zvláště vyznačuje egocentričností a demoralizací, tj. *„bezohledností vůči druhým a normám, zvýšeným zájmem o sebe, o své zájmy a problémy a negativním emočním vyladěním, jakousi „centrální“ nespokojeností.“*[277] U pachatele organizovaného zločinu je patrný kriminální životní styl. Na rozdíl od ostatních odsouzených se srovnává se situací dlouhodobějšího uvěznění snáze, je rovněž sociabilnější.[278] Zvýšená sociabilita oproti ostatním pachatelům trestné činnosti usnadňuje pachatelům organizovaného zločinu vzájemnou interakci a působení v organizovaných skupinách.

[275] CEJP, Martin. Organizovaný zločin v České republice v mezinárodním kontextu. *Trestněprávní revue*. 2016, 15(4), str. 89.
[276] SCHEINOST, Miroslav; NETÍK, Karel. *Český organizovaný zločin v mezinárodním kontextu*. Praha: Institut pro kriminologii a sociální prevenci, 2010. MARKUSOVÁ, Renata; NETÍK, Karel. *Výzkum pachatelů trestné činnosti spáchané v organizované skupině: dílčí studie v rámci výzkumu struktury, forem a možností postihu organizovaného zločinu v ČR*. Praha: Institut pro kriminologii a sociální prevenci, 1997.
[277] SCHEINOST, Miroslav; NETÍK, Karel. *Český organizovaný zločin v mezinárodním kontextu*. Praha: Institut pro kriminologii a sociální prevenci, 2010, str. 56.
[278] Tamtéž, str. 56.

3.1.2.2. Organizovaný zločin v mezinárodněprávním pojetí

Organizovaný zločin není ohraničen teritoriem jednoho státu, nýbrž běžně hranice států překračuje a nabývá rozměrů mezinárodních. Nezřídka se proto setkáváme i s pojmy nadnárodní nebo transnacionální organizovaný zločin.[279]

Pojem organizovaný zločin nebyl na mezinárodní úrovni dlouhá léta uspokojivě vymezen. Teprve s příchodem globalizované společnosti a s rozvojem nadnárodních aktivit organizovaného zločinu na začátku 90. let vyvstala potřeba univerzální úpravy a sjednocení terminologie. Po dlouhých debatách mezinárodní společenství vymezilo pojem organizovaného zločinu v rámci Úmluvy OSN proti nadnárodnímu organizovanému zločinu,[280] která v čl. 2 písm. a) definuje organizovanou zločineckou skupinu jako *„strukturovanou skupinu tří nebo více osob, existující po určité časové období a jednající ve vzájemné shodě s cílem spáchat jeden či více závažných trestných činů nebo trestných činů stanovených v souladu s touto Úmluvou, aby získala, přímo či nepřímo, finanční nebo jiný hmotný prospěch.“*

Roku 1998 EU sjednotila v členských státech definici zločinného spolčení, kterým se napříště mělo na mysli *„strukturované sdružení více než dvou osob, existující po delší dobu, které jedná ve shodě s cílem páchat protiprávní jednání, za která lze uložit trest odnětí svobody nebo opatření omezující svobodu s horní hranicí sazby nejméně čtyři roky nebo závažnější trest, ať tyto trestné činy představují cíl sám o sobě, nebo jsou prostředkem pro získání majetkových výhod a případně pro nedovolené ovlivnění fungování orgánů veřejné moci.“*[281]

Sjednocení právní úpravy a aplikace práva v rámci mezinárodního společenství v praxi představuje značný problém. Státní zástupci, soudci i experti specializovaných policejních a celních útvarů u organizovaného zločinu zdůrazňují, že i přes veškeré harmonizační a unifikační snahy EU neexistuje v jejích členských zemích jednotná

[279] COUFALOVÁ, Bronislava. Organizovaný zločin – vymezení pojmu. In: JELÍNEK, Jiří, ed. *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014, str. 28.

[280] Úmluva OSN ze dne 15. listopadu 2000 proti nadnárodnímu organizovanému zločinu. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 75/2013 Sb. m. s.

[281] Čl. 1 Společné akce 98/733/JHA ze dne 21. prosince 1998 přijaté Radou na základě článku K. 3 Smlouvy o Evropské unii, kterou se stanoví, že účast na zločinném spolčení je v členských státech Evropské unie trestným činem. Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31998F0733&from=EN [cit. 2016-12-22].

legislativa. Právní úprava bývá vykládána různorodě. Nejednotnost postihu stejného jednání v různých zemích značně komplikuje samotný postih organizátorů skupin organizovaného zločinu.[282] Tito posléze mohou skrze globální systémy koordinovat jednotlivé aktivity skupiny z regionů, které jim skýtají relativní bezpečnost. Organizovaný zločin může působit v rámci širokého území různých států. Státní zástupci a soudci kritizují především odlišné podmínky určující pro zařazení organizované skupiny anebo aktivity pod kategorii organizovaného zločinu. Rozdílné podmínky panují i přesto, že jsou mnohé státy smluvní stranou unifikačních mezinárodních úmluv. Rovněž řada klíčových zájmů státu, například fiskální zájmy, které bývají výsostnou doménou státu, nemusí být na mezinárodní úrovni dostatečně efektivně chráněny. Ohrožení či porušení fiskálních zájmů v mezinárodním prostředí je přitom poměrně snadné.[283]

3.1.2.3. Organizovaný zločin dle právního řádu České republiky

Platné české trestní právo organizovaný zločin výslovně nedefinuje. Trestní zákoník vymezuje organizovanou zločineckou skupinu, jež nahradila zločinné spolčení užívané dříve trestním zákonem.[284] Podle důvodové zprávy pojem organizovaná zločinecká skupina lépe koresponduje s pojetím organizovaného zločinu v mezinárodních dokumentech, zejména v Úmluvě OSN proti nadnárodnímu organizovanému zločinu.[285]

Legální definice zločinného spolčení existovala v českém trestním právu od roku 1995. Tehdy zákonodárce požadoval, aby bylo zločinné spolčení zaměřeno na dosahování zisku soustavným páchání úmyslné trestné činnosti, čímž limitoval postih

[282] CEJP, Martin. Organizovaný zločin v České republice v mezinárodním kontextu. *Trestněprávní revue*. 2016, 15(4), str. 91.
[283] Tamtéž.
[284] Citovaná změna však zasáhla toliko terminologii.
[285] COUFALOVÁ, Bronislava. Organizovaný zločin – vymezení pojmu. In: JELÍNEK, Jiří, ed. *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014, str. 28.

určitých skupin organizovaného zločinu zaměřených primárně na jiné cíle. Jako nadbytečný byl odstraněn novelou z roku 2001.[286]

Hovoříme-li v kontextu platného českého trestního práva o organizované zločinecké skupině, respektujeme znění výkladového ustanovení § 129 TZ, dle něhož je organizovaná zločinecká skupina *„společenstvím více osob s vnitřní organizační strukturou, s rozdělením funkcí a dělbou činností, která je zaměřena na soustavné páchání úmyslné trestné činnosti.“* Problematickým aspektem této definice bývá při její aplikaci orgány činnými v trestním řízení ona vnitřní organizační struktura, jejíž prokazování u konkrétního společenství činí potíže. Prokázání dělby činností a rozdělení funkcí bývá rovněž obtížným. Nepodaří-li se zákonné znaky prokázat, dojde ke změně právní kvalifikace a členové skupiny jsou stíhání toliko jako členové organizované skupiny, v důsledku čehož není vystihnuta pravá podstaty společensky nebezpečné součinnosti v trestné činnosti.[287]

Organizovanou skupinu lze poté vymezit jako sdružení více osob, tj. nejméně tří trestně odpovědných fyzických či právnických osob, v jehož rámci dochází k určité dělbě úkolů mezi jednotlivými členy sdružení a činnost sdružení se vyznačuje plánovitostí a koordinovaností. Existence organizované skupiny zvyšuje šance na úspěšné provedení trestného činu, v důsledku čehož stoupá i závažnost, resp. společenská škodlivost trestné činnosti v rámci organizované skupiny.[288] Typickým znakem trestného činu spáchaného organizovanou skupinou bývá, že *„při plánovitém a promyšleném rozdělení úkolů mezi její členy dochází ze strany některých členů jen k dílčím jednáním, která se sama o sobě jeví jako méně závažná, a to jak z hlediska své povahy, tak z hlediska příčinného významu pro způsobení následku. Rozdělení úkolů mezi více spolupachatelů je předpokladem toho, aby po spojení všech dílčích činností jednotlivých spolupachatelů bylo zamýšleného cíle dosaženo snáze a spolehlivěji.“*[289] Spáchání trestného činu členem organizované skupiny bývá kvalifikační okolností mnohých kvalifikovaných skutkových podstat. Není-li již znakem kvalifikované

[286] COUFALOVÁ, Bronislava. Organizovaný zločin – vymezení pojmu. In: JELÍNEK, Jiří, ed. *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014, str. 28.
[287] Tamtéž, str. 29.
[288] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1377.
[289] Usnesení Nejvyššího soudu, sp. zn. 8 Tdo 1584/2010, ze dne 26. 1. 2011.

skutkové podstaty konkrétního trestného činu, lze uvedenou skutečnost v rámci sankcionování pachatele hodnotit jako obecně přitěžující okolnosti dle § 42 písm. o) TZ. Vhodné je poukázat i na pravidlo obsažené v § 107 odst. 2 TZ, tj. „*skutečnost, že pachatel se trestného činu dopustil jako člen organizované skupiny nebo ve spojení s organizovanou skupinou, nebrání tomu, aby za splnění podmínek stanovených tímto zákonem byl současně postižen jako pachatel trestného činu spáchaného ve prospěch organizované zločinecké skupiny.*“

Kvalifikační okolností, která hodnotí mezinárodní prvek při páchání vybrané trestné činnosti, bývá okolnost spáchání trestného činu ve spojení s organizovanou skupinou působící ve více státech (například u zločinu legalizace výnosů z trestné činnosti dle § 216 odst. 1, odst. 4 písm. a) TZ). K naplnění zákonného znaku „ve více státech“ postačí působení skupiny alespoň ve dvou státech, tedy i jen v České a Slovenské republice.[290] Co se týče pojmu „ve spojení“, zde postačí forma spolupráce, jež nemusí představovat vždy činnost vysoce koordinovanou, nýbrž takovou, která je dostatečně významná pro podporu aktivit organizované skupiny.[291]

Na rozdíl od organizované skupiny se vyznačuje organizovaná zločinecká skupina vnitřní organizační strukturou s rozdělením jednotlivých funkcí. Hovořit lze až o stabilním hierarchickém uspořádání organizace. Účast na organizované zločinecké skupině představuje vyšší formu trestné součinnosti, skupina se zaměřuje na soustavné, tj. trvalejší páchání úmyslné trestné činnosti. Dochází k naplnění znaků charakteristických pro organizovaný zločin uvedených výše v citaci výkladového ustanovení § 129 TZ. Dopustí-li se pachatel trestné činnosti ve prospěch organizované zločinecké skupiny, tj. ve smyslu § 107 odst. 1 TZ spáchá úmyslný trestný čin jakožto její člen, vědomě s jejím členem anebo v úmyslu organizované zločinecké skupině napomáhat, je možné uvedenou okolnost zhodnotit dle ustanovení § 108 TZ při ukládání trestu odnětí svobody, kdy § 108 odst. 1 TZ umožňuje zpřísnit zákonnou výměru trestní sazby zvýšením horní hranice o jednu třetinu a uložit pachateli konkrétní trest odnětí svobody v horní polovině takto zvýšené trestní sazby.

Samotnou účast na organizované zločinecké skupině je možné stíhat i dle samostatné skutkové podstaty trestného činu účasti na organizované zločinecké skupině dle § 361 TZ, kdy se pravidla vyjádřená v § 107 a § 108 TZ při sankcionování pachatele

[290] Usnesení Nejvyššího soudu, sp. zn. 5 Tdo 794/2004, ze dne 15. 7. 2004.
[291] Usnesení Nejvyššího soudu, sp. zn. 8 Tdo 1584/2010, ze dne 26. 1. 2011.

nepoužijí. Účasti na organizované zločinecké skupině dle § 361 TZ se může dopustit jak fyzická tak i právnická osoba, přičemž samotná organizovaná zločinecká skupina může mít formu právnické osoby.[292] Vždy je zapotřebí důsledně prokázat naplnění všech zákonných znaků organizované zločinecké skupiny. Kriminalizováno je jak její založení (bez ohledu na to, zda skupina stačila vyvinout protiprávní činnost), tak účast na činnosti organizované zločinecké skupiny, ač nedošlo k aktivnějšímu chování člena v rámci skupiny. Kriminalizována je i podpora organizované zločinecké skupiny nečlenem, tj. jakákoli pomoc (byť jen morální) poskytnutá skupině jako celku anebo členu v zájmu skupiny. Z hlediska subjektivní stránky se vyžaduje úmyslné zavinění, kdy pachatel musí být alespoň srozuměn s tím, že spolčení může být organizovanou zločineckou skupinou. V případě zakladatele organizované zločinecké skupiny musí jeho úmysl zahrnovat i cíl skupiny - soustavné páchání úmyslné trestné činnosti.[293]

Kvalifikačními okolnostmi je spáchání činu ve vztahu k organizované zločinecké skupině zaměřené či určené k páchání vlastizrady, teroristického útoku či teroru.[294] K aktivitám spojeným s terorismem, včetně kyberterorismu, viz níže. Samostatnou skutkovou podstatou je ustanovení § 361 odst. 3 TZ, dopadající na vedoucí činitele a představitele takto specificky zaměřené organizované zločinecké skupiny. Pachatel zde nemusí být přímo hlavou spolčení, avšak v rámci skupiny se vyznačuje dostatečně významnou pravomocí rozhodovat.[295]

3.2. Propojení organizovaného zločinu a počítačové kriminality

Informační a výpočetní technologie, jež daly vzniknout globálnímu virtuálnímu prostředí, umožňují organizovanému zločinu především perfektně komunikovat a spolupracovat na rozlehlém území. K propojení světa organizovaného zločinu může docházet různými způsoby. Tradiční hierarchické organizace mafiánského typu mohou najímat profesionální odborníky ve sféře ICT. Rovněž mohou vznikat flexibilnější a

[292] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 1, § 1 – 139. [Obecná část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1377.
[293] Podrobněji viz ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 2, § 140 – 421. [Zvláštní část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 3343 - 3344.
[294] Srov. § 361 odst. 1, odst. 2 TZ.
[295] S ohledem na současnou podobu § 7 zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, postihuje uvedené ustanovení i pachatele, kterým bude právnická osoba.

organizačně volnější uskupení kratšího charakteru, kdy se skupina zaměří na páchání jednoho druhu počítačové trestné činnosti a útočí na vybraný snadno dostupný cíl. Online vznikají i komunity operující toliko ve virtuálním prostředí - nejčastěji jde o trestnou činnost zaměřenou proti autorským právům či distribuce nelegální pornografie. Lze se setkat i s jedinci, kteří páchají trestnou činnost sice individuálně, avšak ve spojení s širší kriminální sítí, vyskytující se například v prostředí sítě Darknet.[296] U posledních dvou uvedených případů součinnosti je vzájemná koordinace a organizace společenství nejslabší a také nejobtížněji prokazatelná.

Ačkoli se stále častěji lze setkat s názory, že se počítačová trestná činnost stává pomalu, ale jistě doménou organizovaného zločinu, o počítačové kriminalitě páchané v rámci organizovaného zločinu a vzájemných vztazích uvnitř skupiny mnoho nevíme. V následující podkapitole se proto snažím porovnat dostupné znalosti o počítačové kriminalitě a světě organizovaného zločinu, což by mohlo pro budoucí studium obou fenoménů přinést určité výchozí poznatky.

3.2.1. Kriminogenní faktory počítačové kriminality v rámci organizovaného zločinu

U objektivních kriminogenních faktorů lze poukázat na fakt, že počítačová kriminalita páchaná v rámci organizovaného zločinu je orientována na zisk. Využívá příležitostí, jež jí poskytují špatně zabezpečené služby ICT, ale i jurisdikce s benevolentním či neexistujícím trestním zákonodárstvím, efektivně regulujícím počítačovou kriminalitu.[297] Za dostatečně lukrativní lze považovat online obchod a nedostatečně zabezpečené online platební systémy. V širším slova smyslu je možné u objektivních kriminogenních faktorů opět odkázat na společenské změny, přinášející rozvoj ICT a globální celosvětové sítě Internet, popsané výše.

Domnívám se, že počítačovou trestnou činnost páchanou skrze organizovaný zločin, zpravidla nebude možné osvětlit jen poukázáním na individuální faktor

[296] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 3. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.
[297] Tamtéž, str. 10.

charakteristický pro organizovaný zločin - motivaci pachatele dosáhnout co nejvyššího zisku. U počítačové kriminality hrají roli specifické socio-kulturní vzorce chování skupiny popsané výše. V některých případech nalézáme i určité obsesivně – kompulzivní chování pachatelů i pocit nezranitelnosti díky anonymním strukturám globálních počítačových sítí. Motivace orientovaná na dosažení zisku bude jednou z mnohých osobnostních rysů pachatelů, vedle rebelie, snahy o nonkonformitu, vůle překonávat technologické překážky a snahy o zviditelnění se ve světě podobně smýšlejících jedinců.[298]

Někteří autoři člení pachatele počítačové kriminality do dvou skupin. Příčinou je odlišný přístup k vyšetřování kybernetické kriminality a k vyšetřování softwarového pirátství.[299] V důsledku odlišného přístupu rozlišují tito autoři i subjektivní kriminogenní faktory obou forem počítačové trestné činnosti. Porada poukazuje na výzkumy z let 1995 – 98 podporující názor o existenci významných rozdílů v rámci komponent při tvorbě jejich kriminalistických charakteristik.[300] Výzkumy v kriminalistické praxi vedly i k odlišnému přístupu při vytváření samostatných metodik odhalování, vyšetřování a prevence uvedené trestné činnosti.

Ačkoli lze poukázat na značnou variaci různých forem počítačové kriminality, nalézáme její specifické individuální kriminogenní faktory, tj. typické osobnostní rysy jejích pachatelů. Tyto lze dále srovnávat s typickými osobnostními rysy pachatelů organizovaného zločinu, jakož i s osobnostními rysy pachatelů hospodářské a finanční kriminality, pod níž bývá značná část organizovaného zločinu podřazena.[301]

---

[298] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 10. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2017-1-04]. Překlad autorka.

[299] Oba druhy trestné činnosti jsou do určité míry specificky kriminalisticky charakterizované. Srov. PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, kapitola 18 - 19.

[300] Tamtéž, str. 803.

[301] Srov. BALOUN, Vladimír. *Organizovaný zločin a jeho možné projevy ve finančním sektoru ekonomiky: dílčí závěrečná studie úkolu "Výzkum organizovaného zločinu v České republice II"*. Praha: Institut pro kriminologii a sociální prevenci, 1999.

3.2.1.1. Porovnání individuálních kriminogenních faktorů organizovaného zločinu, hospodářské a finanční kriminality a počítačové kriminality

Mezi osobnostními rysy pachatelů počítačové kriminality Porada uvádí vysoké IQ, hamižnost, touhu po moci, vytrvalost a bezohlednost. Dále poukazuje na neuroticismus, neobratnost v sociálním kontaktu a častou přítomnost sexuálních problémů. Pachatelé počítačové kriminality nemají obvykle na jimi páchanou trestnou činnost náhled – pocity viny absentují, ve svém jednání nevidí nic špatného.[302] Určitým specifikem je postavení v zaměstnání, které pachateli nezřídka skýtá výchozí postavení pro páchání uvedené trestné činnosti vůči svému zaměstnavateli. Pachateli jsou nejčastěji právě o zaměstnanci různých útvarů výpočetní a komunikační techniky v poškozené organizaci. Například USA uvádí až 24% pachatelů mezi zaměstnanci výpočetního střediska poškozené instituce a 70% pachatelů mezi koncovými uživateli výpočetní techniky v poškozené organizaci; toliko 6% pachatelů pochází z jiné než poškozené organizace.[303]

U pachatelů softwarového pirátství (typické vlastnosti a motivy jednání rozebírá Porada samostatně), zdůrazňuje značnou různorodost osobnostních charakteristik, především co do věkové skladby a technických schopností pachatelů, typickým motivem věkové skupiny mladší 15 let ovšem bývá získání nelegálního software pro vlastní potřebu hraní počítačových her.[304] Uvedená různorodost a obtížnost definování charakteristických rysů pachatelů softwarového pirátství je vcelku logická vzhledem k rozmanitosti forem této trestné činnosti. Pachatelem se může stát každý uživatel ICT, který v rozporu s licenční smlouvou užívá či šíří určitý počítačový program, tedy jednání pro řadového českého občana snadno představitelné. V české společnosti je obecný postoj k softwarovému pirátství tradičně benevolentní, v důsledku čehož jej převážná část populace nepovažuje za čin natolik závažný, aby byl způsobilý přivodit osobě trestní stíhání. Co se některých méně závažných forem softwarového pirátství týče, by *ad absurdum* bylo možné poznamenat, že typické osobnostní rysy pachatele se shodují s osobnostními rysy běžného občana.

[302] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, str. 791.
[303] Tamtéž.
[304] Tamtéž, str. 806.

Mezi závažnější formy softwarového pirátství lze například zařadit pašování, výrobu, prodej a šíření nelegálního software.[305] Pachatelé tohoto typu softwarového pirátství se trestné činnosti často dopouští skrze organizovanou skupinu. Ty tvoří specializovaní a technicky schopní jedinci, z nichž značná část má v rámci IT managementu určité postavení či funkci, které páchání trestné činnosti umožňují či usnadňují.[306]

Porovnáme-li individuální kriminogenní faktory pachatelů organizovaného zločinu, hospodářské a finanční kriminality a počítačové kriminality (včetně softwarového pirátství), nalezneme některé společné znaky. U pachatelů organizovaného zločinu i hospodářské a finanční kriminality je patrný zvýšený stupeň egocentričnosti a orientace na dosažení co nejvyššího zisku. Bývají i dobře sociálně integrováni. Naopak pachatelé počítačové kriminality, především ti, kteří nabízí k dispozici znalosti programování a technologií, tj. typičtí hackeři či crackeři, jsou o poznání méně sociabilní, resp. jsou sociálně integrováni toliko ve vlastní komunitě. Jednání ve smyslu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ se zpravidla dopouští spíše jednotlivci nežli organizované skupiny, což na druhou stranu neplatí pro závažnější formy softwarového pirátství. Společnou individuální charakteristikou pachatelů finanční a počítačové kriminality je sofistikované jednání, vysoká latence, spíše mužské nežli ženské pohlaví pachatele. Škoda rovněž vzniká většímu okruhu obětí.

Závěrem lze poznamenat, že individuální kriminogenní faktory hrající roli u pachatelů organizovaného zločinu jsou směrodatné i pro pachatele finanční a hospodářské kriminality. Průnik nalézáme i v zištné motivaci členů organizovaných skupin zaměřujících se na distribuci nelegálního software. S ohledem na širokou škálu trestné činnosti spadající pod pojem počítačová kriminalita nelze ovšem jednoznačně stanovit individuální faktory společné pro všechny formy počítačové kriminality páchané skrze organizovaný zločin.

[305] K dalším typickým formám softwarového pirátství srovnej Tamtéž, str. 804 – 806.
[306] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, str. 806.

3.2.2. Specializace v trestné činnosti a vybrané nové formy organizovaného zločinu v mezinárodním prostředí

Organizovaný zločin doplňuje legální trh v oblastech, kde sám nestačí uspokojit potřeby obyvatelstva. S ohledem na pravidlo nabídky a poptávky uspokojuje poptávku na trhu a ve svých aktivitách se přizpůsobuje společenskému vývoji. Cejp uvádí posun kriminálních aktivit organizovaného zločinu následovně:[307]

Původní aktivity organizovaného zločinu	Novodobé / současné podoby aktivit organizovaného zločinu
• **místní sázky, loterie a hazard (gambling), herny**	➢ **gambling na mezinárodních internetových stránkách (www)**
• **obchod s heroinem a kokainem**	➢ **syntetické drogy (odpadají problémy se zásobováním, dovozem materiálu k výrobě)**
• **pouliční prostituce**	➢ **prostituce a obchod s lidmi s využitím Internetu**
• **vymáhání peněz od místních obchodníků za jejich ochranu**	➢ **vydírání společností, korporací, únosy**
• **lichva**	➢ **praní špinavých peněz, obchod s drahými kameny, surovinami**
• **překupníci kradeného zboží**	➢ **krádeže duševního majetku**

Příloha č. 4: Odhad expertů pro pořadí aktivit organizovaného zločinu pro rok 2020

Informační systémy jsou zneužívány s ohledem na množství uchovávaných digitálních dat. Nejčastěji jsou útoky cíleny na informace bankovního charakteru, obchodního tajemství či státem utajované informace klasifikované vnitrostátním právním řádem.[308] Moderní ICT jsou místem sdílení a ukládání dat, provádění finančních transakcí a distribuce informací širokému okruhu uživatelů. Využívány jsou i pachateli organizované trestné činnosti, kteří díky nim dokáží snáze legalizovat výnosy

[307] CEJP, Martin; BLATNÍKOVÁ, Šárka; HÁKOVÁ, Lucie; HOLAS, Jakub; TRÁVNÍČKOVÁ, Ivana; VLACH, Jiří. *Společenské zdroje vývoje organizovaného zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 16.
[308] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 3. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

z trestné činnosti, dojednat konkrétní kriminální aktivity či distribuovat návody k výrobě drog.

3.2.2.1. Zneužití informací platebního a bankovního charakteru, skimming

Příkladem aktivit organizovaných skupin působících na území několika států a zaměřujících se na páchání specifické počítačové trestné činnosti je zneužívání údajů týkajících se nepřenosných platebních karet, v rámci globálních elektronických platebních systémů a internetového bankovnictví. Prostřednictvím trestné činnosti známé jako skimming dochází v rámci organizované skupiny k dělbě funkcí a činnosti členů tak, že po obstarání nástroje kopírování platebních karet,[309] buď domácí výrobou nebo zajištěním výroby u výrobce či online na černém trhu, zajistí skupina instalaci nástroje na příhodných místech. Volí nedostatečně zabezpečené bankomaty nacházející se v zahraničí v turisticky atraktivních lokalitách, které bývají užívány velkým množstvím osob s účty v bankách západního světa. Člen skupiny po několika dnech zařízení z bankomatu odinstaluje a se získanými bankovními údaji cestuje zpravidla do země, z níž skupina činnost řídí. Odtud za pomoci dovedností technicky zručnějších členů skupiny jsou bankovní údaje zneužity prováděním plateb skrze globální počítačové systémy, k padělání platebních karet nebo k dalšímu obchodování se získanými informacemi na virtuálních černých trzích. Dosah skupiny je díky síti Internet globální. Poškozeným nezbývá než si své účty se zneužitými přístupovými údaji co nejdříve zablokovat, neboť trestní postih členů organizované (zločinecké) skupiny v zahraničí, existuje-li podezření ze spáchání trestného činu vůči konkrétním osobám, nebude příliš efektivní.

V českém prostředí lze hovořit o postihu činu jako zvlášť závažného zločinu neoprávněného opatření, padělání a pozměnění platebního prostředku dle § 234 odst. 3 alinea první, odst. 5 písm. a) TZ, pakliže dojde k padělání nepřenosné platební karty. V případě uskutečnění platebních operací a způsobení škody se právní kvalifikace odvíjí

[309] Přístroje čtou a zaznamenávají údaje z magnetické pásky na zadní straně platební karty, některé lze připevnit k bankomatu. Po vložení platební karty ji přístroj přečte spolu s bankomatem. Jiné se podobají platebním terminálům. Spolu s přístrojem bývá instalována i miniaturní kamera umožňující sledovat zadávání PIN kódu. GLENNY, Misha. *Temný trh: kyberzloději, kyberpolicisté a vy*. Praha: Argo, 2013, str. 45.

od výše škody. Možným je jednočinný souběh se zločinem krádeže dle § 205 odst. 1 písm. a), odst. 4 písm. a) TZ (v přesné právní kvalifikaci se promítne výše způsobené škody).

Informace bankovního charakteru mohou být zneužity ze strany zaměstnanců finančních institucí, kteří jsou pro organizovaný zločin cenným zdrojem informací. K regulaci trestněprávní ochrany před neoprávněným nakládáním s osobními údaji došlo prvně zákonem č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.[310] Ochranu před zneužitím osobních údajů získaných v souvislosti s výkonem povolání, zaměstnání nebo funkce, nikoli v souvislosti s výkonem veřejné moci, poskytuje samostatná skutková podstata trestného činu neoprávněného nakládání s osobními údaji dle § 180 odst. 2 TZ, kterého se dopustí, *„kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.“* Pachatelem se může stát osoba vázaná státem uloženou nebo uznanou povinností mlčenlivosti, ale i kterákoli fyzická osoba, která se s osobními údaji o jiném seznámila náhodně a rozhodla se jich využít, anebo je získala záměrně, např. pomocí hackingu. Osobním údajem je jakákoli informace týkající se určeného nebo určitelného subjektu údajů, tj. fyzické osoby.[311] Osobními údaji tak mohou být i údaje vztahující se k bankovnímu účtu. Státem uloženou a uznanou povinnost mlčenlivosti pro účely trestního zákona definuje výkladové ustanovení § 124 TZ jako *„mlčenlivost, která je uložena nebo uznána jiným právním předpisem.“* Nejedená se o mlčenlivost, jejíž rozsah vyplývá z právního jednání, byť učiněného na základě právního předpisu. Zda jde o jednání neoprávněné, zjistíme z jiného právního předpisu. Rozsah způsobené újmy na právech nebo právem chráněných zájmech posoudíme se zřetelem na okolnosti konkrétního případu, zejména *„k tomu, o jaké právo či právem chráněný zájem šlo, jaká byla intenzita újmy na tomto právu či právem chráněném zájmu a jaké následky to mělo pro poškozeného.“*[312]

[310] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 2, § 140 – 421. [Zvláštní část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1795.
[311] K určitelnosti subjektu údaji srovnej § 4 písm. a), d) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
[312] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 2, § 140 – 421. [Zvláštní část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 1796.

Výše uvedené jednání zaměstnanců bank a jiných finančních institucí bude možné stíhat právě ve smyslu trestného činu neoprávněného nakládání s osobními údaji dle § 180 odst. 2 TZ. Případy spáchání činu členem organizované skupiny i způsob spáchání činu veřejně přístupnou počítačovou sítí, jsou okolnostmi zvlášť přitěžujícími, podmiňujícími použití vyšší trestní sazby. V případě naplnění všech zákonných znaků organizované zločinecké skupiny bude možné čin postihnout tak, jak je uvedeno výše.

Příkladem zneužití digitálních dat klientských bankovních účtů je odsouzení zaměstnance banky, jež neoprávněně získal přístup k souboru dat týkajících se sporožirových účtů, který si v zašifrované podobě odnesl domů na paměťovém nosiči a data týkající se klientů banky posléze opakovaně nabízel na prodej. Později požadoval po generálním řediteli banky výměnou za data částku 25 milionů Kč. Odsouzen byl pro trestné činy neoprávněného nakládání s osobními údaji dle § 178 bývalého trestního zákona a poškození a zneužití záznamu na nosiči informací dle § 257a bývalého trestního zákona k trestu odnětí svobody v trvání tří let.[313] Ačkoli nešlo o projev organizovaného zločinu, případ ilustruje možnosti obchodování s údaji bankovního charakteru skrze globální počítačové sítě. Nové příležitosti lákají k zapojení se do aktivit organizovaného zločinu v rámci specializace pachatelů na „dodavatele“ žádaných digitálních dat.

Neoprávněné nakládání s údaji bankovního charakteru je jedním z nejčastěji se vyskytujících případů počítačové trestné činnosti orientované na zisk. Smejkal uvádí, že za účinnosti bývalého trestního zákona měla převážná většina zjištěných trestných činů spáchaných pomocí počítače charakter neoprávněné manipulace s bankovními záznamy, zejména s účty, hlavní knihou, soubory převodních příkazů apod. Případy byly obvykle právně kvalifikovány jako trestný čin podvodu dle § 250 bývalého trestního zákona.[314]

3.2.2.2. Podvod, scareware a ransomware

Tzv. scareware je škodlivý počítačový program, který je prezentován jako antivirus, tj. program schopný vyhledat a zneškodnit počítačové viry a jiné škodlivé

[313] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 148.
[314] S výjimkou výše popsaného případu zneužití informací o klientských sporožirových účtech. Tamtéž, str. 135.

programy (malware). Malware, proti němuž má falešný antivirový program (scareware) zakročit, ve skutečnosti v počítači neexistuje. Hrozbou pro počítač se naopak stává scareware. Ten bývá běžně distribuován pomocí reklamních oken a náhle se objevivších zpráv (tzv. pop-up messages), informujících o napadení počítače malware, jemuž se lze bránit pouze zakoupením nabízeného antiviru, kterým je scareware.

Základním cílem podvodného jednání je zmást uživatele natolik, aby zaplatil za dodání falešného antivirového programu. V případě způsobení škody nikoli nepatrné, tj. škody dosahující ve smyslu výkladového ustanovení § 138 odst. 1 TZ částky nejméně 5000 Kč, půjde o přečin podvodu dle § 209 odst. 1 TZ, neboť pachatel sebe nebo jiného obohatí tím, že uvede někoho v omyl, a způsobí tak na cizím majetku škodu nikoli nepatrnou. Spáchání činu jako člen organizované skupiny či vyšší škoda jsou okolnostmi zvlášť přitěžujícími. Některý scareware je pro počítač nebezpečnější, neboť spolu s ním dochází i k instalaci konkrétního zvláště nebezpečného malware. V takovém případě by byl možný jednočinný souběh s přečinem neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 2 písm. a), b), d) TZ, a to podle konkrétních škodlivých účinků daného typu malware. Spáchání činu členem organizované skupiny či vyšší škoda jsou okolnostmi zvlášť přitěžujícími. K postihu pachatele organizované zločinecké skupiny platí výše uvedené.

Roku 2011 mezinárodní vyšetřovací tým pod názvem Operation Trident Tribunal, v rámci něhož byla koordinována spolupráce orgánů činných v trestním řízení dvanácti států,[315] překazil aktivity dvou organizovaných skupin zaměřujících se na prodej scareware.[316] Pachatelé poškodili přes jeden milion počítačových uživatelů a výše celkové škody v souhrnu přesáhla 74 milionů amerických dolarů. Jedna ze skupin operující z ukrajinského Kyjeva užívala při podvodném jednání různorodou taktiku; uživatele například přesměrovala na webovou stránku s falešnými výsledky antivirové kontroly jeho počítače, v důsledku čehož došlo poté k instalaci malware. Uživatelé byli též vyzýváni k zadání čísla kreditní karty a úhradě za uvedení jejich počítače do původního stavu.

[315] Ukrajiny, Litvy, Lotyšska, Německa, Nizozemí, Kypru, Francia, Rumunska, Kanady, Švédska, Velké Británie a USA.
[316] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 4. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

Instalace malware a aktivity spojené s vydíráním napadené osoby jsou známé ve spojení s tzv. ransomware, tj. s malware spojeným s požadavkem úhrady vysokých finančních částek za uvedení počítače do původního stavu, eventuálně za nenaplnění výhrůžky formulované kybernetickými útočníky. V mezinárodním prostředí bývají cílem útoku obchodní korporace, u nichž se předpokládá dobrá ekonomická situace a vysoký obrat za rok, i snaha vyhnout se negativní publicitě způsobilé poškodit společnost v konkurenčním obchodním prostředí.[317] Útočníci bývají orientováni na dosažení co nejvyššího zisku. Vedle výše uvedených právních kvalifikací lze jednání pachatelů hodnotit i ve smyslu trestného činu vydírání dle § 175 TZ. Žádanou měnou ransomware, v níž má dojít k úhradě útočníky požadované částky, bývá měna virtuální, nejčastěji bitcoin.

Bitcoin (též „BTC“ nebo „XTC“) je decentralizovanou virtuální měnou spočívající v silném šifrování, která umožňuje oboustranný tok mezi virtuální a reálnou ekonomikou. V BTC probíhá 80% celosvětových transakcí ve virtuální měně. BTC je nejpopulárnější a neomezeně přístupnou kryptoměnou, s níž lze platit prostřednictvím decentralizované peer-to-peer sítě. Unikátem BTC je právě jeho decentralizace – design měny neumožňuje její regulaci ze strany jednotlivce, skupiny či vlády - nikdo jej nemůže zvenčí autoritativně ovlivňovat, ničit, padělat, zapříčinit inflaci, kontrolovat peněžní toky či zabavovat konkrétní účty. Celkové množství peněz je konečné, předem známé a definované matematickými zákony.[318]

Virtuální měny v současné době nejsou dle vyjádření České národní banky peněžním prostředkem ve smyslu zákona č. 284/2009 Sb., o platebním styku, v žádném státě nemají charakter zákonného platidla a nejsou plnohodnotnou národní měnou. Právní ochrana při transakcích virtuálních měn prakticky neexistuje.[319] Přesto jsou BTC užívány jako zvláštní prostředek směny. Dostanou-li kybernetičtí útočníci zaplaceni v BTC, šance na dopadení za pomoci vysledování toku finančních prostředků je snížena na minimum.

---

[317] Příkladem mohou být online sázkové kanceláře, online kasina apod.
[318] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 555 - 556. Dále též http://blog.bitcoin.cz/ [cit. 2017-01-09].
[319] SINGER, Miroslav. Bezpečnost internetových plateb a virtuální „měny“ z pohledu ČNB. Fórum Zlaté koruny, ČNB, 2015. Dostupné na http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/verejnost/pro_media/konference_projevy/vystoupeni_projevy/download/singer_20150421_zlata_koruna.pdf [cit. 2017-01-09].

3.2.2.3. Legalizace výnosů z trestné činnosti a virtuální měna

Legalizace výnosů z trestné činnosti, neboli „praní špinavých peněz“,[320] je provázejícím jevem organizovaného zločinu. Umožňuje zastřít skutečný původ finančních prostředků a navrátit je do oběhu legální ekonomiky státu. Legalizace výnosů z trestné činnosti upevňuje pozici organizovaného zločinu a jeho vliv na oficiální instituce legální státní ekonomiky a spojuje stát i společnost s korupčními aktivitami.[321] Virtuální globální prostředí a technologický pokrok přináší legalizaci výnosů z trestné činnosti dříve netušených možností.

Na pojem špinavých peněz lze nahlížet v užším i širším slova smyslu, tj. buď jako na finanční prostředky pocházející toliko z trestné činnosti, anebo jako na veškeré výnosy a výhody trestnou činností získané. Někteří chápou špinavé peníze jako veškerý majetek získaný nelegální činností.[322] Z širokého pojetí vychází i směrnice Evropského parlamentu a Rady 2014/42/EU ze dne 3. dubna 2014 o zajišťování a konfiskaci nástrojů a výnosů z trestné činnosti v Evropské unii, o níž pojednávám níže.[323]

Skutková podstata trestného činu legalizace výnosů z trestné činnosti dle § 216 TZ postihuje jednání, kterým se pachatel snaží vzbudit zdání, že výnos z trestné činnosti je ve skutečnosti legálně nabytým příjmem.[324] Na rozdíl od trestného činu podílnictví dle § 214 TZ není jeho podstatou pouze převod výtěžku z trestné činnosti, nýbrž zahrnuje i další jednání na spáchání trestné činnosti navazující, kterými se pachatel snaží odstranit stopy výnosů trestné činnosti a zajistit zdání jejich legálnosti.[325] Trestný čin legalizace výnosů z trestné činnosti dle § 216 odst. 1 TZ obsahuje dvě základní skutkové podstaty. Objektivní stránku první naplní, *„kdo zastírá původ nebo jinak*

[320] Výrazy užívám synonymně. Populární výraz se objevil poprvé v USA ve 20. letech minulého století, kde jím policie popisovala zneužívání vlastnictví samoobslužných prádelen mafiánskými skupinami k legalizaci peněz pocházejících z trestné činnosti. Nejčastěji byly legalizovány výnosy ze „špinavého“ obchodu z drogami. Viz JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 151 - 152.
[321] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 151.
[322] Tamtéž, str. 152.
[323] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014L0042&qid=1483385077105&from=EN [cit. 2017-01-02].
[324] Ustanovení provádí závazky plynoucí z Evropské úmluvy o praní, vyhledávání, zadržování a konfiskaci výnosů ze zločinu, publikované pod č. 33/1997 Sb.
[325] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. Sv. 2, § 140 – 421. [Zvláštní část]. 2. vyd. V Praze: C.H. Beck, 2012, str. 2155 - 2156.

usiluje, aby bylo podstatně ztíženo nebo znemožněno zjištění původu a) věci, která byla získána trestným činem spáchaným na území České republiky nebo v cizině, nebo jako odměna za něj, nebo b) věci, která byla opatřena za věc uvedenou v písmenu a)“, druhá postihuje zvláštní formu účastenství, konkrétně toho, *„kdo jinému spáchání takového činu umožní.“* Z hlediska subjektivní stránky se vyžaduje úmysl. Nedbalostní jednání, kterým pachatel jinému umožní zastřít původ nebo zjištění původu věci získané trestným činem nebo jako odměna za něj, je stíháno v rámci skutkové podstaty trestného činu legalizace výnosů z trestné činnosti z nedbalosti dle § 217 TZ, která ovšem dopadá pouze na věci větší hodnoty, dosahující ve smyslu ustanovení § 138 odst. 1 TZ alespoň hodnoty 50.000 Kč.

Legalizace výnosů z trestné činnosti organizovaného zločinu představuje značné riziko pro stabilitu globálních finančních systémů, neboť při ní dochází k zneužívání legálních postupů k zakrytí původu výnosů z trestné činnosti. Napomáhá, aby zůstal beze změny stav vytvořený hlavní trestnou činností, na níž navazuje. Bylo by chybou soustředit se pouze na cesty praní špinavých peněz skrze bankovní sektor, když vhodné možnosti nabízí i sázkové kanceláře, kasina, směnárny, realitní kanceláře a především sektor kapitálového trhu a pojišťovnictví.[326] Moderní způsoby bezhotovostních převodů na různé platební účty kdekoli na světě umožňují snadno skrýt původ výnosů z trestné činnosti. Usnadňují i obchod s ilegálními komoditami na virtuálním černém trhu a v neposlední řadě i finanční podporu terorismu. Ačkoli pachatelům nebrání téměř nic převádět finanční prostředky prakticky kamkoliv na světě, orgány činné v trestním řízení jsou při zjišťování trasy špinavých peněz omezeny jurisdikcí států.

Virtuální měny představují bezpečnostní rizika, neboť lákají ke zneužití k trestné činnosti a k financování terorismu. Dle metodického pokynu Finančně analytického útvaru Ministerstva financí České republiky je v souvislosti s nákupem či prodejem jakékoli virtuální měny považována za velmi rizikovou k posouzení a k rozhodnutí o dalších opatřeních podle okolností každá platba s hodnotou nad 1000 EUR.[327]

---

[326] BALOUN, Vladimír. *Organizovaný zločin a jeho možné projevy ve finančním sektoru ekonomiky: dílčí závěrečná studie úkolu "Výzkum organizovaného zločinu v České republice II"*. Praha: Institut pro kriminologii a sociální prevenci, 1999, str. 65.

[327] SINGER, Miroslav. Bezpečnost internetových plateb a virtuální „měny“ z pohledu ČNB. Fórum Zlaté koruny, ČNB, 2015. Dostupné na http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/verejnost/pro_media/konference_projevy/vystoupeni_projevy/download/singer_20150421_zlata_koruna.pdf [cit. 2017-01-09].

V případě směny výnosů z trestné činnosti na virtuální měnu získávají pachatelé unikátní možnost neomezených a státem neregulovaných transakcí v rámci sítě Internet. Ačkoli např. u BTC musí být každá transakce transparentní v tom smyslu, že lze v rámci sítě BTC ověřit její platnost a pravost (transakce obsahuje odkaz na předchozí transakci, což zamezuje užití stejných BTC dvakrát) a transakce i bilance jednotlivých účtů jsou volně dostupné na Internetu,[328] k vytvoření účtu či peněženky není třeba ztotožnit jejího majitele. Při snaze dohledat původce transakce se sice lze dostat k IP adrese, z níž byla konkrétní transakce uskutečněna, avšak tato se může nacházet v jiné jurisdikci.

Nejproblematičtějšími jurisdikcemi v souvislosti s praním špinavých peněz i financováním terorismu jsou KLDR a Írán. Strategické nedostatky v oblasti právní regulace praní špinavých peněz mají i Bosna a Hercegovina, Afgánistán, Irák, Sýrie, Laos, Uganda, Vanatu a Jemen.[329] Uvážíme-li možnosti krytí IP adres i zneužívání cizích IP adres k páchání trestné činnosti, nemusí ani zjištění konkrétní IP adresy, z níž byla transakce provedena, určit skutečného majitele BTC „peněženky“. Navíc při zjištění IP adresy z některé z výše vyjmenovaných problematických jurisdikcí bude spolupráce více než problematická.

3.2.2.4. Softwarové pirátství

Porušování autorských práv doznalo s příchodem osobních počítačů a rozšířením sítě Internet rovněž nový rozměr. Ochrana poskytovaná duševnímu vlastnictví v rámci virtuálního prostředí nebyla vždy samozřejmostí a trvalo určitou dobu, než se do práva obchodního, daňového či trestního promítla. Duševní vlastnictví je přitom běžným objektem trestné činnosti, především v oblasti neoprávněného užívání a šíření počítačových programů, databází a zvukových i zvukově-obrazových děl.[330]

[328] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 556.
[329] FATF. Veřejné prohlášení ze dne 21. října 2016 – rizikové jurisdikce. Dostupné z http://www.mfcr.cz/cs/archiv/agenda-financniho-analytickeho-utvaru/novinky-fau/2016/verejne-prohlaseni-fatf-z-21-rijna-2016-26767 [cit. 2017-01-09].
[330] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, str. 803.

Softwarové pirátství je *„neoprávněné nakládání se software, jejich dokumentací a dalšími součástmi právně chráněných softwarových produktů.“*[331] Trestněprávní úprava chrání duševní vlastnictví především ve smyslu vědecké, literární, hudební, audiovizuální a jiné umělecké tvůrčí činnosti i z ní plynoucích požitků, jakož i práv výrobků zvukového a zvukově-obrazového záznamu a práv pořizovatele databáze. Trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi, představuje normu s blanketní dispozicí, odkazující na zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (dále jen „autorský zákon“). Odkazem na mimotrestní úpravu je zajištěn soulad s případnými novelizacemi uvedené normy upravující autorská práva a práva související. Počítačový program je dle § 2 odst. 2 autorského zákona považován za autorské dílo, pakliže je autorovým vlastním duševním výtvorem.

Objektivní stránku základní skutkové podstaty trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 odst. 1 TZ naplní, *„kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.“* Neoprávněným zásahem je třeba rozumět především jakékoliv zveřejnění díla bez souhlasu autora, zhotovení rozmnoženiny nebo napodobeniny díla a dále i výrobu, nabízení k prodeji, k pronájmu a půjčení, k dovozu a šíření pomůcek zamýšlených k odstranění, vyřazení z provozu nebo omezení funkčnosti technických elektronických zabezpečení, postupů, zařízení nebo jiných prostředků použitých oprávněnou osobou k ochraně práv.[332] Pro trestněprávní kvalifikaci musí být uvedený zásah vždy vyšší než nepatrný. Zapotřebí je proto zvažovat okolnosti konkrétního případu, intenzitu zásahu, způsob provedení činu a jeho následky, opakování zásahů či délku doby narušování chráněného práva. V případě nesplnění podmínky je možné pachatele postihnout za správní delikt dle § 105a až § 105c autorského zákona. Po subjektivní stránce se vyžaduje úmysl, zahrnující i vědomí pachatele, že jde o dílo, jež je výsledkem tvůrčí duševní činnosti

[331]PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, str. 804.
[332] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 2751.

autora. Pachatelem může být kterákoli fyzická či právnická osoba.[333] Ve vztahu k počítačové kriminalitě páchané formou organizovaného zločinu může činnost připomínat obchodní aktivity. Proto lze uvažovat o kvalifikační okolnosti dle § 270 odst. 1, odst. 2 písm. a) TZ.[334]

Mezi typické způsoby softwarového pirátství patří nelegální zásahy do software, výroba počítačových programů, šíření software a užívání počítačových programů i zužitkování databáze.[335] Formou organizované trestné činnosti dochází k domácí výrobě software bez licence, tj. k vytváření a distribuci kopií software. Organizované skupiny se věnovaly i pašování a prodeji nelegálního zahraničního software, který na domácím trhu prodávaly za nižší cenu.[336] S rozvojem peer-to-peer sítí a webů zaměřených na šíření zejména audiovizuálních autorských děl již tato forma trestné činnosti nepřináší požadovaný zisk, neboť není jedinou cestou, jak se co nejrychleji a levně dostat k novému autorskému dílu. Nejrozšířenějším je proto nelegální šíření software skrze tzv. hostingové servery umožňující ukládání digitálních dat, které často zneužívají absenci výslovné povinnosti monitorovat obsah dat ukládaných na žádost uživatele služby informační společnosti.[337]

3.2.3. Předpokládaný vývoj počítačové trestné činnosti v rámci organizovaného zločinu

V rámci změn uvnitř struktur organizovaného zločinu je patrný posun od uzavřené hierarchie k volnějším sítím organizovaného zločinu. Globalizovaný mezinárodní trh přetváří aktivity velkých hierarchizovaných kriminálních organizací,

[333] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 2752 - 2753.
[334] V takovém případě by byl i možný jednočinný souběh s trestným činem neoprávněného podnikání dle § 251 TZ. Srov. ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 2756.
[335] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, str. 805.
[336] Tamtéž, str. 805.
[337] Podle směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu). Dostupná z http://eur-lex.europa.eu/search.html?DTN=0031&DTA=2000&qid=1483724651178&CASE_LAW_SUMMARY=false&DTS_DOM=ALL&excConsLeg=true&type=advanced&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL. [cit. 2017-01-06].

které ve svém rigidním uspořádání nejsou v rámci organizovaného zločinu na globálním trhu tolik efektivní. Organizovaný zločin se vlivem ekonomických změn přesouvá od tradičních forem trestné činnosti k novým a rigidní hierarchizované organizace jsou na ústupu.[338]

Menší specializovaná kriminální společenství umožňují efektivnější dělbu činností a rozdělení funkcí, snadněji se přizpůsobí globálnímu trhu, komplexním finančním transakcím. Novodobý organizovaný zločin závisí na malém jádru trvalých členů, kteří získávají ostatní členy v závislosti na konkrétních úkolech a potřebách skupiny. Hierarchické uzavřené organizace jsou podle názoru odborníků věcí minulosti.[339] Právě skrze onu specializaci hledanou pro konkrétní a aktuální potřeby aktivit organizovaného zločinu lze dle mého dojmu nalézt spojení mezi organizovaným zločinem a počítačovou trestnou činností.

Počítačová kriminalita páchaná v rámci organizovaného zločinu bude patrně orientována v prvé řadě na zisk. Proto lze za pole působnosti do budoucna označit především lukrativní oblast elektronického obchodu. Pevnější a trvalejší struktury organizovaného zločinu se mohou zaměřit i na vydírání konkrétních obětí s přístupem k citlivým informacím platebního či bezpečnostního charakteru a na další obdobné aktivity typické pro běžný organizovaný zločin. Naopak dynamické a flexibilní struktury organizovaného zločinu budou působit především ve smyslu systematicky páchané počítačové kriminality spočívající v různých formách podvodného jednání v rámci Internetu.[340]

Setkáváme se i s odvážným názorem, podle něhož by případy počítačové kriminality páchané skrze tzv. botnet, tj. soubor velkého množství skrze malware vzdáleně kontrolovaných a ovládaných počítačových systémů, měly být považovány za formu organizovaného zločinu.[341] Východiskem úvahy je fakt, že botnet představuje koordinovanou, organizovanou, efektivní a nebezpečnou formu páchání počítačové trestné činnosti v prostředí globálních počítačových sítí. Jde o počítačový systém svého druhu, který je zpravidla ovládán jediným administrátorem, nikoli organizovanou

[338] SOULEIMANOV, Emil. *Organizovaný zločin*. Praha: Auditorium, 2012, str. 23.
[339] Tamtéž, str. 24.
[340] VON LAMPE, Klaus. Explaining the Emergence of the Cigarette Black Market in Germany. In: VAN DUYNE, Petrus; VON LAMPE, Klaus; VAN DIJCK, Maarten; NEWELL, James (eds.). *The Organised Crime Economy*. Wolfe Legal, 2005, str. 209 – 229. Překlad autorka.
[341] LYC, Chan. *Cybercrime in the Greater China Region: Regulatory Response and Crime Prevention across the Taiwan Strait* [online]. Edward Elgar, 2012. [cit. 2016-12-29]. Překlad autorka.

skupinou více osob. Definice organizovaného zločinu tak, jak jej pojímá mj. mezinárodní úmluva OSN proti nadnárodnímu organizovanému zločinu, dle současného pojetí termínu na vysoce sofistikované případy počítačové trestné činnosti páchané pomocí botnetu nedopadá.[342] Do budoucna nemůžeme vyloučit posun v chápání pojmu organizovaného zločinu a organizované skupiny osob směrem k výtvorům umělé inteligence, která za určitých okolností bude schopna jednat sama bez ingerence člověka.

3.3. Terorismus

Vlivem globalizace dochází k nestabilitě a politickým konfliktům v řadě zemí světa, které jsou doprovázeny prohlubujícími se rozdíly mezi ekonomicky vyspělými zeměmi a chudými regiony světa. Sílící náboženské napětí a nestabilita v chudých regionech zmítaných válečnými konflikty se obrací vůči bohatému západnímu světu, využívajíce záminek náboženského boje. Spolu s množícími se teroristickými útoky na starém kontinentu v posledních letech mnozí varují před islamizací Evropy a bezpečnostním rizikem radikálního islámu. Podle Cejpa se ovšem podstata bezpečnostního rizika pojí spíše ke zločinu samotnému, nežli k náboženství.[343] K problému (kyber)terorismu přistupuje předkládaná práce jako k jevu kriminálnímu, vymezenému trestněprávními předpisy, nikoli jako k jevu politickému. Jelínek poznamenává: *„Mezinárodní terorismus je jedním z příkladů nadnárodního zločinu v našem tisíciletí … Představuje rovněž jeden z nejzávažnějších útoků na demokracii a právní stát, tedy na zásady, které jsou společné členským státům Evropské unie. Mezinárodní terorismus nabývá stále nebezpečnějšího rozsahu a je nutné, aby státy učinily příslušná opatření k jeho potírání.“*[344]

[342] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 9. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.
[343] CEJP, Martin. Organizovaný zločin v České republice v mezinárodním kontextu. *Trestněprávní revue*. 2016, 15(4), str. 90.
[344] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 200.

3.3.1. Základní charakteristika terorismu a jeho vývoj

V 70. letech 20. století došlo k vymezení terorismu jako nové formy války s odlišným složením hlavních aktérů. V případě teroristických útoků, na rozdíl od válečného konfliktu, je stát postaven do role napadeného a vydíraného objektu spolu se svým obyvatelstvem, s jehož veřejným míněním teroristé manipulují a vyvolávají v něm reakce nahrávající vlastním zájmům. V okamžiku útoku se pak teroristé stávají jedinými aktivními aktéry, vytvářejícími atmosféru strachu. Ve snaze změnit vnitřní či vnější směřování státu jej destabilizují a za objekt své strategie vydávají zájmy jedné skupiny obyvatelstva. Přípravy na teroristický útok probíhají velmi skrytě v přísně utajené a nepočetné komunitě. Útokem se teroristé nesnaží působit na nejsilnější prvky obrany státu, čelnímu boji se naopak vyhýbají a stát s jeho obyvatelstvem napadají nepřímo.[345]

Teroristické útoky se vždy vyznačují silnou motivací. Pojem terorismu vznikl odvozením z latinského výrazu *terror*, znamenající extrémní strach či úzkost z těžko předvídatelného nebezpečí.[346] Mezi hlavní cíle patří vytvoření atmosféry strachu, přilákání pozornosti a vynucení si změn ve státní politice. Definice teroristických trestných činů vždy v subjektivní stránce obsahují zvlášť orientovaný úmysl spáchat trestný čin, tzv. *dolus coloratus* a specifický motiv či záměr teroristy.[347] Cíl závažným způsobem zastrašit obyvatelstvo se objevuje i v detailním vymezení teroristického činu podle Rámcového rozhodnutí Rady EU 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu.[348] Neznámější motivací teroristů bývá politická a náboženská. Jirovský uvádí i terorismus kriminální, zahrnující skupiny organizovaného zločinu cílící na zisk prostředků pro své akce, a (individuální) terorismus psychotický, vyvěrající z motivu duševně nemocného člověka.[349]

Na přelomu 60. a 70. let se setkáváme s nástupem mezinárodního terorismu útočícího na cíle za hranicemi vlastního státu. Počátkem 90. let 20. století se ještě

[345] EICHLER, Jan. *Terorismus a války v době globalizace*. 2., dopl. vyd. Praha: Karolinum, 2010, str. 142 - 146.
[346] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 201.
[347] Tamtéž, str. 201.
[348] Srov. čl. 1 odst. 1 Rámcového rozhodnutí Rady EU 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu. Dostupné z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002F0475&qid=1485883126088&from=EN [cit. 2017-01-31].
[349] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 128 – 129.

hovořilo o terorismu spíše jako o riziku, nežli o reálné hrozbě. Jakmile první teroristické útoky napáchaly obrovské materiální škody a vyžádaly si mnohé oběti, veřejné mínění se přetvářelo. S rozmachem letecké dopravy se objevil nový působivý nástroj vedení teroristických útoků. Zásadním mezníkem se staly útoky z 11. září 2001 v USA. Od té doby se stal terorismus předmětem odborných diskuzí a politických debat o jeho předcházení a následné obraně.[350] Často přitom dochází k směšování terorismu s asymetrickou čili partyzánskou válkou i s národněosvobozeneckým bojem. S rozdílnými názory se dosud setkáváme například při pohledu na boj za nezávislost Kosova. Definice terorismu proto často zůstává do určité míry subjektivně ovlivněna osobním výkladem konkrétní politické situace.

Aktivity teroristů by nemohly existovat bez finanční a ideové podpory. Tato se zvláště silně projevuje z islámských zemí, jako je například Saudská Arábie a Pákistán. Pasivní podporu terorismu často poskytují i politické strany a bohatí jednotlivci. Například od 70. let 20. století zasílala Saudská Arábie značné finance do celého muslimského světa k podpoře islamistických center a dohledat, jak velkého podílu se zmocnily teroristické organizace, je téměř nemožné.[351]

3.3.2. Promítnutí terorismu do kybernetického prostředí

O teroristickém činu můžeme hovořit s ohledem na tři klíčové oblasti, kterými jsou oblast útoku, způsob provedení útoku a prostředky útoku.[352] Kybernetický prostor může hrát roli v každé z těchto oblastí. Oblast útoku koreluje s konkrétní motivací teroristického činu, může jít o hrozbu namířenou proti menšinovému obyvatelstvu nebo vůči určitému státnímu majetku. Útok může být proveden zneužitím ICT, včetně počítačových sítí, které se stávají prostředkem vedení teroristického útoku.

Na základě formy lze dělit terorismus na letální a neletální. Obě formy se dále člení dle metod vedení útoku na konvenční a nekonvenční. Zatímco letální formu terorismu vedenou konvenčními prostředky představují útoky běžně dostupných

[350] EICHLER, Jan. *Terorismus a války v době globalizace*. 2., dopl. vyd. Praha: Karolinum, 2010, str. 142.
[351] Tamtéž, str. 159.
[352] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 128.

bojových zbraní, mezi nekonvenční prostředky spadají například zbraně hromadného ničení. Kybernetické prostředí spíše inklinuje k neletální formě terorismu a kyberterorismus tak bývá uváděn mezi formami konvenčního neletálního terorismu.[353]

Termín kyberterorismus užil poprvé v roce 1996 Barry Collin, pracovník kalifornského Institute for Security and Inteligence, který popsal několik možných scénářů kyberteroristického útoku. Nejčastěji zmiňovaným je scénář o ovládnutí systému leteckého dopravního provozu skládajícího se ze sítě počítačů teroristou. Definovat kyberterorismus ovšem můžeme jednoduše jako *„nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu nebo obyvatele k podporování sociálních nebo politických cílů.“*[354] Objektem teroristického útoku jsou v daném případě počítače, počítačové sítě a informace (respektive data) v nich se nacházející. Podle Smejkala hovoříme o kyberterorismu, pakliže je cílem nebo nástrojem teroristického útoku informační nebo telekomunikační systém.[355]

Nespornou výhodou kyberteroristického útoku pro útočníky představuje možnost napáchat obrovské škody s nízkými náklady. Mnohé aktivity soukromých i veřejných organizací vyžadují nepřetržitý provoz, jehož narušení, byť odehrávající se v řádu několika hodin či dní, způsobí značné ztráty a ohrozí další činnosti na ně navazující. Příkladem lze uvézt průmyslové řídicí systémy ovládající technické procesy v rámci distribučních sítí elektřiny, vody, dopravy, či tepelné a jaderné energie.

Brennerová však poukazuje na obtíže v jasném rozlišení mezi kybernetickou kriminalitou, kyberterorismem a kybernetickou válkou. Obdobně jako Jirovský a Smejkal považuje za charakteristický znak kyberterorismu právě motivaci pachatelů, kteří snažíce se dosáhnout náboženských či politických cílů demoralizují a destabilizují většinovou společnost.[356] I Kenney upozorňuje na leckdy příliš rozsáhlou tendenci

[353] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, str. 129.
[354] Tamtéž, str. 130.
[355] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 84.
[356] BRENNER, Susan. *Cyberthreats and the decline of the nation-state* [online]. Oxfordshire, England: Routledge, 2014, str. 16. ISBN 9780203709207. Dostupné z: http://site.ebrary.com/lib/cuni/Doc?id=10848006 [cit. 2017-01-31]. Překlad autorka.

podřazovat pod pojem kyberterorismu tzv. hacktivismus[357] a zneužívání ICT s cílem usnadnit spáchání útoků konvenčního terorismu.[358] Důležité je mít vždy na paměti, že kyberterorismus je pouze podmnožinou terorismu a jako konvenční formy terorismu musí naplnit zákonné znaky příslušných skutkových podstat teroristických trestných činů. Hovoříme-li o kyberterorismu, půjde vždy o teroristický trestný čin.

3.3.3. (Kyber)terorismus a mezinárodní prostředí

Po útocích 11. září 2001 je terorismus vnímán především jako hrozba pro mezinárodní společenství. V reakci na politickou situaci došlo k přijetí mezinárodních úmluv a rezolucí, které se snaží státy přivést k spolupráci v rámci globálního boje proti terorismu. Dalším impulzem pro navázání hlubší mezinárodní spolupráce, zejména v evropském kontextu, se staly pařížské útoky na redakci týdeníku Charlie Hebdo v lednu 2015.[359] Zejména EU vydala velké množství doporučení, akčních plánů, rámcových rozhodnutí a dalších dokumentů zaměřujících se na boj proti terorismu.

Na půdě Rady Evropy došlo k přijetí první mezinárodní úmluvy adresující hrozby terorismu v roce 1977. Evropskou úmluvu o potlačování terorismu[360] podepsaly až na Andorru všechny členské státy Rady Evropy, pro Českou a Slovenskou federativní republiku vstoupila v platnost 15. července 1992. Význam má především pro extradici pachatelů teroristických činů.[361]

Většího významu pro kyberterorismus nabyla Úmluva Rady Evropy o prevenci terorismu,[362] která ukládá smluvním stranám kriminalizovat podněcování teroristického činu, nábor a výcvik. Především podněcování a náboru je snadno možné dopouštět se

[357] Termín popisuje využívání etického hackingu a prostředků ICT k vyjádření politického protestu. WALL, David. *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity, 2007, str. 223. Překlad autorka.
[358] KENNEY, Michael. Cyber-Terrorism in a Post-Stuxnet World. *Orbis*. 2015, 59(1), s. 111 - 128. Překlad autorka.
[359] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 200 an.
[360] Úmluva Rady Evropy č. 90 ze dne 27. ledna 1977 o potlačování terorismu. Sdělení federálního ministerstva zahraničních věcí ČSFR č. 552/1992 Sb.
[361] Dodatkový protokol pozměňující Evropskou úmluvu o potlačování terorismu nebyl široce ratifikován s ohledem na rozsah trestných činů, které nemohou být označeny za politické činy.
[362] Úmluva Rady Evropy č. 196 ze dne 16. května 2005 o prevenci terorismu. Dostupná z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196/signatures?p_auth=GS4aFhEO [cit. 2017-01-31]. Česká republika ji dosud neratifikovala.

skrze ICT. Smejkal hovoří o typické informační trestné činnosti.[363] Čl. 5 Úmluvy Rady Evropy o prevenci terorismu definuje veřejné podněcování teroristického činu jako *„zpřístupnění nebo jiné poskytnutí zprávy veřejnosti, v úmyslu podnítit spáchání teroristického činu, ať již půjde o přímou či nepřímou podporu teroristických činů, která povede ke vzniku hrozby spáchání jednoho či více teroristických činů.“*[364] České trestní právo kriminalizuje veřejné podněcování teroristického činu ve skutkové podstatě zvlášť závažného zločinu teroristického útoku dle § 311 odst. 2 alinea druhá TZ, nábor a výcvik je možné posoudit jako přípravu k trestnému činu. Úmluva Rady Evropy o prevenci terorismu si klade za cíl zlepšit mezinárodní spolupráci v rámci prevence terorismu, a to cestou přijímání národních preventivních politik a doplněním mezinárodních úmluv týkajících se extradice i mezinárodní spolupráce obecně.[365] Dodatkový protokol k Úmluvě Rady Evropy o prevenci terorismu[366] požaduje po smluvních státech vytvoření nepřetržité sítě kontaktních míst umožňujících okamžitou výměnu informací. Problematiky kyberterorismu se dotýká i Úmluva o počítačové kriminalitě a její Dodatkový protokol k Úmluvě o počítačové kriminalitě, o kterých pojednává práce výše.

EU boj proti terorismu vnímá jako jeden z klíčových cílů. Vedle mezinárodní spolupráce se soustředí i na unifikaci definic teroristických trestných činů v členských státech. Z množiny předpisů, věnujících se obecně terorismu, lze uvést Společný postoj Rady 2001/931/SZBP ze dne 27. prosince 2001 o uplatnění zvláštních opatření k boji proti terorismu,[367] vytvářející seznam teroristických uskupení[368] a cílící na zmrazení jejich finančních prostředků. Stanoví i množinu teroristických trestných činů, které jsou jako trestné činy definované vnitrostátním právním řádem a mohou svou podstatou či kontextem vážně ohrozit chod státu nebo mezinárodní organizace.[369] Seznam těchto

[363] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 84.
[364] Překlad autorka.
[365] Srov. čl. 3 a čl. 4 Úmluva Rady Evropy o prevenci terorismu.
[366] Úmluva Rady Evropy č. 217 ze dne 22. října 2015, dodatkový protokol k Úmluvě Rady Evropy o prevenci terorismu. Dostupný z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217 [cit. 2017-01-31].
[367] Dostupný z http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=URISERV:l33208&qid=1486138127835&from=EN&isLegissum=true [cit. 2017-02-03].
[368] Mezi nimi např. Pokračující Irská republikánská armáda, baskická E.T.A., teroristické křídlo hnutí Hamás či Palestinský islámský džihád.
[369] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 210.

teroristických činů uvádí i rozsáhlé poškození veřejných nebo soukromých zařízení, včetně informačního systému a narušení nebo přerušení dodávek vody, elektrické energie nebo jiného základního přírodního zdroje. Uvedené činy lze snadno spáchat prostředky ICT, v takovém případě lze hovořit o kyberteroristickém útoku.

Na výše uvedený společný postoj EU navazuje rámcové rozhodnutí 2002/475/SVV o boji proti terorismu a rámcové rozhodnutí Rady EU 2008/919/SVV ze dne 28. listopadu 2008, kterým se mění rámcové rozhodnutí 2002/475/SVV o boji proti terorismu,[370] které pokračuje v harmonizaci definic teroristických trestných činů. V podrobnostech lze odkázat na příslušnou literaturu,[371] pro téma kyberterorismu ovšem není bez významu široce pojatá definice veřejného podněcování ke spáchání teroristického trestného činu.[372] Zjišťujeme, že obdobně jako v Úmluvě Rady Evropy o prevenci terorismu, se lze skrze ICT dopustit veřejného podněcování terorismu velice snadno. Je to ústavní pořádek členských států umožňující svobodu projevu, který brání přijmout příliš restriktivní opatření na základě uvedeného pramene práva EU.[373] Právní nejistota obklopující definici podněcování terorismu v EU je o to palčivější v prostředí Internetu vytvářejícím otevřené fórum pro spáchání trestného činu podněcování k terorismu. Příliš vágní definice EU byla v řadě členských států zúžena soudním výkladem, přesto by bylo vhodné na půdě EU vymezit jasnější hranici mezi trestnou činností a svobodou projevu.[374] Ke vztahu protiteroristických opatření EU a ochraně základních lidských práv a svobod se vyjádřil i Soudní dvůr EU ve věci Yassin Abdullah Kadi v. Evropská komise z 30. září 2010, kdy mimo jiné upřesnil pravidla vyvažování ochrany mezinárodní bezpečnosti a míru vůči právu na spravedlivý proces v EU.[375]

---

[370] Dostupné z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32008F0919&qid=1486139931248&from=EN [cit. 2017-02-03].
[371] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 211 an.
[372] Srov. čl. 3 odst. 1 písm. a) rámcového rozhodnutí 2002/475/SVV o boji proti terorismu. (Ve znění uvedené novelizace.)
[373] Srov. též čl. 2 rámcového rozhodnutí Rady EU 2008/919/SVV ze dne 28. listopadu 2008, kterým se mění rámcové rozhodnutí 2002/475/SVV o boji proti terorismu, který nutně vede k rozdílům v jednotlivých členských státech.
[374] REDIKER, Ezekiel. The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union. *Michigan Journal of International Law*. 2015, 36(2). Překlad autorka.
[375] Spojené věci C-584/10 P, C-593/10 P a C-595/10 P, Komise, Rada, Spojené království v. Yassin Abdullah Kadi. Podrobněji SVOBODA, Pavel. Kadi 2013: tečka za jednou kapitolou protiteroristické judikatury SDEU? *Právní rozhledy*. 2013, (23 - 24), s. 825 an.

Evropská komise předložila koncem roku 2015 Evropskému parlamentu návrh směrnice Evropského parlamentu a Rady o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí 2002/475/SVV o boji proti terorismu (dále též „návrh směrnice o boji proti terorismu“).[376] Návrh směrnice o boji proti terorismu posiluje právní prostředky prevence terorismu v EU především tím, že kriminalizuje jednání, která jsou materiálně přípravou, jako například organizování a napomáhání uskutečňování cest za účelem teroristických útoků či absolvování teroristického výcviku. Jednání jako úmyslné vycestování do konfliktní oblasti za účelem spáchání teroristických trestných činů, účast na činnostech teroristické skupiny či poskytnutí nebo absolvování výcviku teroristů, má být ve všech členských státech považováno za trestný čin.[377] Kriminalizace se má dočkat i úmyslné poskytování či shromažďování finančních prostředků, a to jakýmkoliv způsobem, přímo nebo nepřímo, se záměrem nebo s vědomím, že budou, byť částečně, použity ke spáchání teroristického trestného činu.[378] Trestným se má stát i jakékoli zpřístupňování informací veřejnosti s úmyslem podnítit spáchání některého z vyjmenovaných teroristických trestných činů, pokud tímto jednáním přímo či nepřímo obhajujícím teroristické trestné činy vznikne nebezpečí, že může dojít ke spáchání takového trestného činu.[379] Nová právní úprava posiluje i práva obětí terorismu. V současnosti projednává uvedený legislativní návrh Evropský parlament, který přijal některé pozměňovací návrhy, vesměs rozšiřující působnost směrnice. Ve vztahu ke kyberterorismu například Evropský parlament navrhl změnu v čl. 3 odst. 2 písm. h) návrhu směrnice o boji proti terorismu, postihující narušení nebo přerušení dodávek vody, elektrické energie nebo jiného základního přírodního zdroje, a to výslovným uvedením skrze kybernetický útok či jakýkoli jiný útok, jehož důsledkem bude ohrožení lidských životů. Evropský parlament tedy jednoznačně předpokládá možnost vedení

[376] Dostupný z http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52015PC0625&qid=1487935488579 [cit. 2017-02-24].
[377] Srov. čl. 9 návrhu směrnice o boji proti terorismu.
[378] Srov. čl. 11 návrhu směrnice o boji proti terorismu.
[379] Srov. čl. 5 návrhu směrnice o boji proti terorismu.

kybernetického útoku na průmyslové řídicí systémy.[380] Konečné schválení návrhu směrnice o boji proti terorismu se předpokládá v nejbližších měsících.[381]

V oblasti mezinárodní spolupráce zaměřené zejména na výměnu informací, je stěžejním předpisem rozhodnutí Rady 2005/671/SVV ze dne 20. září 2005 o výměně informací a spolupráci v oblasti teroristických trestných činů (dále též „ rozhodnutí o výměně informací“),[382] které upravuje postupy sdílení informací o trestním řízení a odsouzení za teroristické trestné činy, pakliže mohou mít dopad na dvě a více členských zemí EU. Informace jsou sdíleny skrze Europol a Eurojust,[383] které je získávají od specializovaných útvarů členských zemí. Sdíleny jsou přinejmenším informace vymezené čl. 2 odst. 4 rozhodnutí o výměně informací, tedy vedle konkrétního stíhaného trestného činu a jeho vazeb na související případy například i využívání komunikačních technologií.

Z aktuálních mezinárodních dokumentů dotýkajících se kyberterorismu lze zmínit i Memorandum z 12. ledna 2015 o porozumění mezi Národním bezpečnostním úřadem České republiky a Národním úřadem pro kybernetickou bezpečnost státu Izrael. Jedná se sice o tzv. soft law dokument, který ovšem poukazuje na nadstandardní stupeň mezinárodní spolupráce mezi zeměmi a představuje výchozí půdu pro případnou bilaterální mezinárodní smlouvu. Na základě memoranda dochází především ke sdílení poznatků o kybernetických bezpečnostních hrozbách.[384] Rovněž na půdě NATO se uskutečňuje výměna informací týkajících se kybernetických útoků. Nelze vyloučit, že v budoucnu budou některé z nich považovány za součást útoků kyberteroristických.

---

[380] Zpráva Evropského parlamentu dostupná z http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2016-0228&language=EN [cit. 2017-02-24].

[381] Tisková zpráva Rady EU č. 716/16 ze dne 5. prosince 2016. Dostupná z http://www.consilium.europa.eu/cs/press/press-releases/2016/12/05-combatting-terrorism/ [cit. 2017-02-24].

[382] Dostupné z http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=uriserv:l33252 [cit. 2017-02-03].

[383] K působení Eurojustu a Europolu v boji proti terorismu podrobněji JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 224 – 238.

[384] Dostupné z https://www.govcert.cz/cs/legislativa/smlouvy-a-memoranda/ a https://www.vlada.cz/cz/media-centrum/aktualne/premier-sobotka-jednal-v-jeruzaleme-na-cesko-izraelskych-mezivladnich-konzultacich-o-rozvoji-obchodni-spoluprace--vyzkumu-i-kyberneticke-bezpecnosti-144332/ [cit. 2017-03-02].

3.3.4. (Kyber)terorismus v právním řádu České republiky

Právní regulace boje s terorismem sestává z právních norem různé síly a oborového zařazení. Pouze jednu z oblastí dostupných nástrojů představují prostředky trestního práva, sestávající z norem hmotněprávních i procesních. Vedle rozboru teroristických trestných činů v trestním zákoníku se následující text dotýká i právní úpravy kybernetické bezpečnosti.

3.3.4.1. Trestné činy teroru a teroristického útoku

Ochranou zvláště důležitých zájmů chráněných trestním zákonem, tj. základních zájmů demokratického státu včetně základních práv a svobod občanů, se zabývá hlava devátá zvláštní části trestního zákoníku. Předmětem ochrany je ústavní zřízení, bezpečnost a obranyschopnost České republiky, a v některých případech i cizího státu a mezinárodní organizace. V případě trestných činů teroristického útoku dle § 311 TZ a teroru dle § 312 TZ je dle § 313 TZ ochrana poskytnuta i cizím státům. Ustanovení hlavy deváté trestního zákoníku se systematicky dělí do tří dílů na trestné činy proti základům republiky, cizího státu a mezinárodní organizace, trestné činy proti bezpečnosti České republiky, cizího státu a mezinárodní organizace a trestné činy proti obraně státu. Trestné činy teroristického útoku dle § 311 TZ a teroru dle § 312 TZ spadají do dílu prvého, jehož těžištěm je ochrana ústavního zřízení republiky, tedy ve smyslu čl. 5 Ústavy ČR demokratického právního státu garantujícího politický systém založený na svobodném a dobrovolném vzniku a soutěži politických stran respektujících základní demokratické principy.[385] Trestnost trestných činů teroristického útoku dle § 311 TZ ani teroru dle § 312 TZ nezaniká uplynutím promlčecí doby, jsou-li splněny okolnosti uvedené v § 35 odst. 2 písm. b) TZ.[386]

Trestný čin teroristického útoku dle § 311 TZ byl zakotven v trestním zákonodárství teprve roku 2004, mimo jiné i na základě mezinárodněprávních závazků

[385] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktual. a dopl. vyd. Praha: Leges, 2016, str. 803 – 804.
[386] JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 6. aktualizované vydání. Praha: Leges, 2016, str. 444.

České republiky, především Evropské úmluvy o potlačování terorismu a právního řádu EU.[387]

Objektem trestného činu teroristického útoku dle § 311 TZ je ústavní zřízení, obranyschopnost a základní politická, hospodářská a sociální struktura republiky, život, zdraví, osobní svoboda jednotlivců a majetek. Objektivní stránka sestává ze dvou základních skutkových podstat. První a rozsáhlejší z nich taxativně vymezuje jednotlivá násilná jednání vedoucí k závažným následkům ve sféře života a zdraví jednotlivců, škody na majetku či životním prostředí. Ochrana je poskytnuta i telekomunikačnímu systému, včetně informačního systému a energetickému, vodárenskému, zdravotnickému nebo jinému důležitému zařízení, dojde-li k jeho zničení nebo poškození ve větší míře.[388] Druhá základní skutková podstata postihuje výhružné jednání směřující k jednání v prvé skutkové podstatě. Postiženo je i veřejné podněcování nebo jakákoli materiální a imateriální podpora jednání v prvé skutkové podstatě, anebo podpora teroristy či člena teroristické skupiny. Druhou skutkovou podstatou je podpora, tj. obdoba pomoci ve smyslu účastenství, povýšena na samostatný trestný čin a ustanovení § 24 odst. 1 písm. c) TZ se neuplatní.[389]

Pachatelem se může stát kterákoli fyzická a právnická osoba, ať již domácí nebo zahraniční. Z hlediska subjektivní stránky se vyžaduje onen specifický motiv teroristy, tzv. *dolus coloratus*, o kterém bylo pojednáno výše.

Jak bylo naznačeno, v případě kyberterorismu pachatelé nepotřebují zbraně či výbušniny, aby například poškodili obranyschopnost státu či narušili jeho hospodářskou nebo sociální strukturu. Přesto se až do současnosti s kyberteroristickými útoky příliš nesetkáváme a někteří odborníci dokonce rozporují, že v popsaných případech se skutečně jednalo o kyberteroristické útoky. Například v říjnu 2012 poukazovalo ministerstvo obrany USA na sérii kybernetických útoků na finanční instituce v USA, přičemž hovořilo o „kybernetickém Pearl Harboru“ a útočníky označilo za kyberteroristy.[390] Dále lze poukázat na případ z roku 2000, kdy se Vitek Boden, bývalý zaměstnanec společnosti dodávající australskému státu Queensland řízené kanalizační

[387] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktual. a dopl. vyd. Praha: Leges, 2016, str. 810.
[388] Srov. § 311 odst. 1 písm. c) TZ.
[389] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktual. a dopl. vyd. Praha: Leges, 2016, str. 812.
[390] KENNEY, Michael. Cyber-Terrorism in a Post-Stuxnet World. *Orbis*. 2015, 59(1), str. 112. Překlad autorka.

systémy, ucházel o zaměstnání v samosprávě státu Queensland. Poté co byl odmítnut, zneužil svého přístupu k informačnímu systému řídícímu kanalizační systém a vypustil 800.000 litrů surové odpadní vody do okolních vod a půdy, v důsledku čehož došlo k úmrtí mnoha druhů mořských i sladkovodních živočichů, znečištění prostředí lidských obydlí a k dalším rozsáhlým škodám na životním prostředí i majetku. Ačkoli mnozí uvažovali o klasifikaci Bodenových útoků spáchaných skrze ICT jako o kyberterorismu, motiv narušit politickou, hospodářskou či sociální strukturu státu Queensland vyvozen nebyl.[391] Z hlediska naplnění objektivní stránky skutkové podstaty trestného činu by v Bodenově případě připadal v úvahu zvlášť závažný zločin teroristického útoku dle § 311 odst. 1 písm. c), písm. g) TZ. S ohledem na absenci specifické pohnutky pachatele ovšem nemohlo dojít k naplnění subjektivní stránky. V případě kyberteroristických útoků je proto zvláště zapotřebí pečlivě dovodit naplnění všech zákonných znaků skutkové podstaty trestného činu teroristického útoku dle § 311 TZ před tím, než vyslovíme závěr o dalším z případů kyberterorismu.

Dalším z teroristických trestných činů je teror dle § 312 TZ. Jeho objektem je rovněž zájem na ochraně ústavního zřízení republiky i lidského života. Objektivní stránku trestného činu teroru dle § 312 TZ naplní, kdo jiného úmyslně usmrtí. Jde o zvláštní případ vraždy, od níž se liší specifickým teroristickým úmyslem – poškodit ústavní zřízení republiky. Pachatelem se nově může stát každá fyzická i právnická osoba. U kyberterorismu se patrně s uvedenou právní kvalifikací příliš nesetkáme.[392]

3.3.4.2. Kybernetická bezpečnost

Česká republika přijala relativně nedávno nový zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále též „ZKB“), který nabyl účinnosti dne 1. ledna 2015. Stala se tak jedním z prvních států, které přijaly komplexní

[391] BRENNER, Susan. *Cyberthreats and the decline of the nation-state* [online]. Oxfordshire, England: Routledge, 2014, str. 15 - 17. [cit. 2017-02-04]. Překlad autorka.
[392] V případě úmrtí v důsledku kyberteroristického útoku, např. při rozsáhlém poškození řídicího systému elektrárny, v důsledku čehož by došlo k jejímu výbuchu, bychom spíše uvažovali o kvalifikaci zvlášť závažným zločinem teroristického útoku dle § 311 odst. 1 písm. c), písm. g), odst. 3 písm. b) TZ.

právní úpravu národní kybernetické bezpečnosti.[393] Cílem ZKB je stanovit podmínky spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity řešení kybernetických bezpečnostních incidentů. ZKB dále stanoví oprávnění a povinnosti vybraným soukromým osobám s cílem zvýšení bezpečnosti kybernetického prostoru. Příslušným orgánem státní správy je Národní bezpečnostní úřad a jeho vnitřní organizační útvar, Národní centrum kybernetické bezpečnosti (dále též „NCKB“).[394]

Úlohou NCKB je koordinovat spolupráci na národní i mezinárodní úrovni s cílem předcházení kybernetickým útokům. Součástí NCKB je tzv. vládní CERT,[395] pracoviště řešící bezpečnostní incidenty a spolupracující se zahraničními subjekty, především co do výměny informací o potenciálních hrozbách kybernetických útoků. V rámci mezinárodní spolupráce dochází i ke společným vzdělávacím akcím s cílem zvýšení odbornosti a navázání neformálních vztahů pro pozdější snazší spolupráci na bilaterální úrovni.

S rozšířením diskuze o kybernetické a informační válce, i v důsledku množících se kybernetických útoků, přistupují státy k posilování vlastní a společné kybernetické obrany. Milníkem v přístupu ke kybernetické bezpečnosti v evropské geografické oblasti se staly kybernetické útoky na estonskou státní infrastrukturu. V roce 2007 čelily estonské webové vládní stránky i webové stránky vybraných politických stran, médií a finančních institucí, několikatýdenním kybernetickým útokům, které je zcela vyřadily z provozu. Estonsko obvinilo z útoků Rusko a za příčinu označilo odebrání ruského válečného pomníku z Tallinnu. Incident rozhýbal mezinárodní debatu o informační válce a vedl Estonsko k posílení obrany vlastních významných informačních struktur. Nyní sídlí v Tallinnu centrum NATO pro kybernetickou bezpečnost a Estonsko se stalo vůdčí zemí v úrovni kybernetické obrany států.[396]

---

[393] POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2015, 6(11), str. 95.

[394] Nyní se hovoří o budoucím osamostatnění Národního centra kybernetické bezpečnosti v samostatný úřad.

[395] CERT je zkratkou pro Computer Emergency Responsability Team. V rámci ZKB byla definována dvě pracoviště, vládní CERT (což je NCKB) a národní CERT, jehož roli plní tým CSIRT.CZ (Computer Security Incident Response Team) provozovaný sdružením CZ.NIC.

[396] PAVLIKOVÁ, Miroslava. Estonsko-ruský incident v kontextu kyberterorismu. *Global Politics: Časopis pro politiku a mezinárodní vztahy* [online]. 2014. Dostupné z http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu [cit. 2017-02-04].

Závěrem kapitoly lze poukázat na fakt, že kybernetická bezpečnost je oblastí technicky a společensky složitou, pro právní normativní vědce značně vzdálenou. Na rozdíl od informační, resp. počítačové bezpečnosti, klade důraz na ochranu funkčnosti síťového prostředí, tvořeného informačními systémy a službami a sítěmi elektronických komunikací, umožňujícího manipulaci s informacemi.[397] Do budoucna bude zajímavé sledovat vývoj vnitrostátní i mezinárodní právní úpravy v této oblasti. Očekávat lze tendenci států v posilování kontroly nad kybernetickým prostorem a omezování některých v něm se projevujících základních lidských práv a svobod. V současné době projednává Poslanecká sněmovna Parlamentu České republiky vládní návrh novely ZKB, který transponuje do českého právního řádu požadavky směrnice Evropského parlamentu a Rady 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Rozšířením působnosti ZKB má dojít právě k posílení bezpečnosti sítí a informačních systémů.[398]

[397] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 93.
[398] Kybernetická bezpečnost: Rozšíření působnosti zákona má posílit bezpečnost sítí a informačních systémů. *Právní zpravodaj Ministerstva spravedlnosti ČR* ze dne 12. 1. 2017.

4. ODHALOVÁNÍ A VYŠETŘOVÁNÍ POČÍTAČOVÉ KRIMINALITY V PRÁVNÍM ŘÁDU ČESKÉ REPUBLIKY

Postih počítačové kriminality v mezinárodním prostředí bude vždy závislý na jejím prvotním odhalení a vyšetřování v jednotlivých státech. Předkládaná práce nahlíží na pojem vyšetřování ve smyslu kriminalistickém, jako na proces získávání a využívání relevantních informací, tj. především vytěžení informací získaných z digitálních dat uložených v počítačovém systému. V jiném smyslu slova je možno vyšetřování vnímat i jako jednu z forem přípravného řízení dle zákona č. 141/1961 Sb., o trestním řízení soudním (dále též „trestní řád" či „TŘ"). Odhalování a vyšetřování počítačové kriminality[399] klade vysoké požadavky na odbornost i přípravu všech orgánů činných v trestním řízení, neboť tyto během vyšetřování naráží na specifika vyplývající z charakteristik počítačové kriminality. Klíčovou podmínkou efektivního postihu počítačové trestné činnosti je tudíž specializace všech osob podílejících se na jejím odhalování a vyšetřování. Nelze než odkázat na názor, dle něhož „*bez skutečně špičkové průpravy v oblasti výpočetní techniky nemá policista šanci pachatele složitějších případů počítačové kriminality vůbec zjistit.*"[400]

Kapitola je zaměřena na rozbor relevantní trestněprocesní úpravy, včetně některých jejích nedostatků. Výchozím textem se pro mne stala vlastní diplomová práce, v níž jsem se zaměřila na právní rámec vyšetřování počítačové kriminality. Kapitola se věnuje vybraným institutům českého trestního práva procesního i relevantním ustanovením práva informačních a komunikačních technologií. Před samotným rozborem právních nástrojů, k jejichž využívání při vyšetřování počítačové kriminality dochází nejčastěji, kapitola pojednává o předsoudní fázi trestního řízení, neboť ta je rámcem, v němž orgány činné v trestním řízení vybrané procesní úkony uplatňují především. Vlivem specifik virtuálního prostředí se často trestní právo dostává do situace platnou trestněprocesní úpravou nepředpokládané. I jednotlivé procesní úkony byly vybrány s ohledem na specifický dopad počítačové kriminality na ně. Text kapitoly pojednává především o zajišťovacích úkonech hlavy čtvrté trestního řádu.

[399] S ohledem na vyšetřování a na možný výskyt stop trestného činu bude vhodnější vnímat pojem počítačové kriminality co nejobecněji – srov. kapitolu 1.1.5.
[400] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 136.

Rozsáhlejší pojednání, které by obsáhlo i další procesní úkony, například výslech obviněného a svědků nebo některé zvláštní způsoby dokazování, jako vyšetřovací pokus či rekonstrukce, však není cílem kapitoly, neboť odlišnosti těchto úkonů během vyšetřování počítačové trestné činnosti oproti ostatní trestné činnosti jsou spíše nepatrné.

4.1. Problematika trestního řízení

Trestní řízení je vymezeno v § 12 odst. 10 TŘ jako *„řízení podle tohoto zákona a zákona o mezinárodní justiční spolupráci ve věcech trestních“*. Trestní řád působí jako *lex generalis* vůči zákonům speciálním, které upravují určité zvláštnosti především s ohledem na vybrané skupiny obviněných.[401] Aby došlo k naplnění účelu trestního řízení, tj. k náležitému zjištění trestných činů a k zákonnému spravedlivému potrestání jejich pachatelů,[402] musí se celý trestní proces odehrávat v předem daném chronologickém rámci, za působení orgánů činných v trestním řízení a některých dalších subjektů trestního řízení. Časové úseky, ve kterých uplatňují subjekty trestního řízení vlastní pravomoc, představují samostatná procesní stádia trestního řízení. V současnosti rozlišujeme pět navzájem navazujících stádií trestního řízení, a to přípravné řízení, předběžné projednání obžaloby, hlavní líčení, řízení o odvolání a vykonávací řízení. Možné je uvést i stádium případného zahlazení odsouzení.[403]

Termín fáze trestního řízení je širší, neboť trestní řízení můžeme členit na předsoudní a soudní fázi. Předsoudní fáze zahrnuje neprocesní postup před samotným zahájením úkonů trestního řízení i přípravné řízení, jež má charakter postupu před zahájením trestního stíhání (prověřování) a povahu trestního stíhání (vyšetřování v procesním smyslu). V předsoudní fázi lze zmínit i řízení po zrušení rozhodnutí v přípravném řízení nálezem Ústavního soudu. Soudní fáze posléze zahrnuje předběžné projednání obžaloby (nejde-li o řízení před samosoudcem s ohledem na § 314c odst. 1

[401] Srov. zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů a zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.
[402] § 1 odst. 1 TŘ.
[403] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 451 – 452.

TŘ), hlavní líčení, řízení o schválení dohody o vině a trestu, řádné i mimořádné opravné řízení, vykonávací řízení, řízení o zahlazení odsouzení, řízení po zrušení rozhodnutí v soudní fázi nálezem Ústavního soudu, řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu k zjištění údajů o telekomunikačním provozu, a konečně i právní styk s cizinou.[404]

V následujícím rozboru odhalování a vyšetřování počítačové kriminality je kladen důraz na procesní úkony, jež se uplatňují zejména v předsoudní fázi trestního řízení, jejíž podstatou je připravit kvalifikovaně konkrétní trestní věc způsobem, který bude postačující pro její následné projednání před soudem. Průběh vybraných procesních úkonů tedy významně ovlivní i soudní fázi trestního řízení. Text se dotýká i soudních fází, konkrétně řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu ke zjištění údajů o telekomunikačním provozu. Následující kapitola posléze pojednává o právním styku s cizinou.

4.1.1. Postup před zahájením úkonů trestního řízení

Podle § 158 odst. 1 TŘ je policejní orgán[405] povinen *„učinit všechna potřebná šetření a opatření k odhalení skutečností nasvědčujících tomu, že byl spáchán trestný čin, a směřující ke zjištění jeho pachatele.“* Za tím účelem přijímá policejní orgán podněty a analyzuje vlastní operativně pátrací činnost. Na rozdíl od přípravného řízení a jeho postupu před zahájením trestního stíhání hovoříme o neprocesní fázi činnosti policejního orgánu. Pakliže jsou získány informace odůvodňující zahájení úkonů trestního řízení dle § 158 odst. 3 TŘ, sepíše o tom policejní orgán neprodleně záznam, čímž dochází k zahájení přípravného řízení.

V případě počítačové trestné činnosti jsou nejčastějším podnětem zahájení úkonů trestního řízení výsledky vlastní operativně pátrací činnosti služby kriminální policie a vyšetřování. Zákon č. 273/2008 Sb., o Policii České republiky (dále též „ZPČR“) obsahuje podmínky užití operativní techniky a definuje pravomoc specializovaných policejních útvarů pro předcházení a odhalování trestné činnosti,

[404] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 454.
[405] K výkladu pojmu srov. § 12 odst. 2 TŘ.

jakými jsou například orgány kriminální policie pověřené odhalováním hospodářské a finanční kriminality. Využívána bývá i síť informátorů, jejich činnost ovšem naráží na povinnost mlčenlivosti uloženou zákonem.

Útvary kriminální policie přináší pro postih počítačové kriminality podněty s největší informační hodnotou.[406] Počítačová trestná činnost bývá oznamována dále poškozenými společnostmi, výrobci či autory software a hardware i nespokojenými zaměstnanci, kteří jsou svědky trestné činnosti svých kolegů či zaměstnavatele, z níž však sami nemají dlouhodobě velkého prospěchu.[407] Oznámení pocházející od kontrolních, inspekčních, revizních a jiných správních úřadů bývají v praxi výjimkou,[408] ačkoli běžně půjde o státní orgány, na něž dopadá dle § 8 odst. 1 TŘ povinnost *„neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin.“* Výjimkou z uvedeného jsou finanční úřady, které bývají častým oznamovatelem daňově orientované trestné činnosti.

Specifikem ovlivňujícím postih počítačové trestné činnosti je skutečnost, že značná část dotčených digitálních dat požívá státem uznané ochrany - typicky půjde o bankovní či obchodní tajemství. Lze se setkat i s utajovanými informacemi, na něž dopadá povinnost mlčenlivosti či zvláštní režim stanovený zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále též „ZBZ“) Zajišťování uvedených dat si posléze vyžádá souhlasu způsobilých orgánů. Režim stanovený ZBZ může ovlivnit i výslech svědků a další nakládání s předmětnými informacemi. Vyšetřování si v takovém případě vyžádá zajištění režimu ochrany utajovaných informací.[409] Pakliže jsou během trestního řízení diskutovány utajované informace, bude zapotřebí všechny osoby, jež se předmětného řízení účastní, předem na základě § 58 odst. 5 ZBZ ve spojení s § 51b TŘ poučit. Povinnost nedopadne toliko na osoby s platným osvědčením pro požadovaný stupeň utajení. Na základě § 99 odst. 1 TŘ pak svědek nesmí být vyslechnut o okolnostech týkajících se utajovaných informací chráněných zvláštním zákonem, ledaže jej povinnosti zachovávat dané informace

[406] PORADA, Viktor; STRAUS, Jiří. *Kriminalistika: (výzkum, pokroky, perspektivy)*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, str. 528 - 529.
[407] MENDEL, Aleš. Vyšetřování počítačové kriminality. In: GŘIVNA, Tomáš; POLČÁK, Radim. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 87.
[408] PORADA, Viktor; STRAUS, Jiří. *Kriminalistika: (výzkum, pokroky, perspektivy)*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013, str. 529.
[409] Tamtéž, str. 531.

v tajnosti zprostí příslušný orgán. Za podmínek uvedených v § 99 odst. 2, odst. 3 TŘ rovněž brání výslechu svědka státem uznaná nebo uložená povinnost mlčenlivosti.

4.1.2. Postup před zahájením trestního stíhání

Postup před zahájením trestního stíhání spadá pod přípravné řízení. Pokud existuje podezření ze spáchání konkrétního trestného činu, policejní orgán dle § 158 odst. 3 TŘ opatřuje k objasnění a prověření skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin, potřebné podklady a nezbytná vysvětlení a dále zajišťuje stopy trestného činu. Smyslem tohoto stádia trestního řízení je rychlé vyhledání potenciálních důkazů, jež by byly později provedeny před soudem. *„Prověřování nenahrazuje vyšetřování a ani řízení před soudem a má pouze vytvořit co nejrychleji předpoklady pro rozhodnutí o eventuálním zahájení trestního stíhání.“*[410]

Ustanovení § 158 odst. 3, písm. a) až i) TŘ demonstrativně uvádí činnost policejního orgánu, který má k dispozici i operativně pátrací prostředky dle § 158b až 158f TŘ. Podle hlavy čtvrté trestního řádu, jež stanoví mimo jiné pravidla zajištění osob a věcí, smí policejní orgán provádět též neodkladné a neopakovatelné úkony.[411] Proč byl konkrétní procesní úkon zhodnocen jako neodkladný či neopakovatelný, je nutné v protokolu o jeho provedení vždy zdůvodnit. Ústavní soud se vyjádřil pro individuální odůvodnění potřebnosti takového postupu v každé z trestních věcí, neboť „*je třeba povahu úkonu jako úkonu neodkladného nepochybně posuzovat vždy podle okolností konkrétního případu.“*[412]

V rámci postihu počítačové kriminality zpravidla dovodíme hrozící nebezpečí zmaření nebo zničení důkazního prostředku běžně tvořeného lehce manipulovatelnými digitálními daty. Na druhé straně specifika digitálních důkazních prostředků nesmí vést k situaci, v níž by byly vyšetřovací úkony v rámci postihu počítačové kriminality výlučně prováděny jakožto neodkladné či neopakovatelné. Stěžejním principem

[410] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 500.
[411] Dle § 160 odst. 4 TŘ jsou neodkladnými ty úkony, jež vzhledem k nebezpečí zmaření, zničení nebo ztráty důkazu nesnesou odkladu na dobu po zahájení trestního stíhání a neopakovatelnými ty úkony, které nebude možné provést před soudem.
[412] Nález Ústavního soudu, sp. zn. I. ÚS 290/98, ze dne 7. 12. 1999.

trestního procesu je provedení jednotlivých procesních úkonů teprve po sdělení obvinění, kdy dochází k zahájení trestního stíhání, umožňujícího obviněnému spolu s případným obhájcem dosáhnout alespoň do určité míry rovnocennějšího postavení proti policejnímu orgánu i státnímu zástupci. Dle § 2 odst. 1 TŘ je možné stíhat osobu pouze ze zákonných důvodů a způsobem, který stanoví zákon. Zásada stíhání jen ze zákonných důvodů je základem trestního procesu a jeho nejdůležitější zásadou. Je rovněž procesním vyjádřením zásady *nullum crimen sice lege*. Proto úsilí o zjištění pravdy i za cenu nedodržení základních zásad trestního procesu je nepřípustné a stane se porušením zákonnosti a svévolí orgánu činného v trestním řízení.[413] Důkaz získaný porušením zákonného procesu bude nepřípustný. Neodkladné a neopakovatelné úkony by proto i v případě křehkých digitálních důkazních prostředků měly být nadále považovány za procesní výjimku.

Během prověřování konkrétního podezření dochází v rámci počítačové kriminality poměrně často k využití odposlechu a záznamu telekomunikačního provozu dle § 88 TŘ, popřípadě k vydání příkazu k zjištění údajů o telekomunikačním provozu dle § 88a TŘ, jakož i ke sledování osob a věcí dle § 158d TŘ, kdy bývají pořizovány zvukové, obrazové a jiné záznamy.

Při prověřování trestné činnosti související s ICT, se policejní orgán neobejde bez odborných vyjádření a znaleckých posudků, z nichž získává expertní znalosti v trestním řízení potřebné.[414] Podle § 157 odst. 3 TŘ může v závažných a skutkově složitých věcech policejní orgán i státní zástupce využít odborné pomoci konzultanta ze speciálního oboru. Za závažné se zpravidla považují trestní věci, jejichž projednání přísluší v prvním stupni krajskému soudu, anebo zvlášť závažné zločiny.[415] Konzultant smí za souhlasu policejního orgánu či státního zástupce v nezbytném rozsahu nahlížet do trestního spisu a účastnit se procesních úkonů. I na něj se vztahuje povinnost mlčenlivosti. Na zákonný průběh předsoudní fáze trestního řízení přitom stále musí dohlížet státní zástupce, jenž odpovídá za zákonnost přípravného řízení.

[413] JELÍNEK, Jiří; ŘÍHA, Jiří; SOVÁK, Zdeněk. *Rozhodnutí ve věcech trestních: se vzory rozhodnutí soudů a podání advokátů*. 3., aktualiz. a přeprac. vyd. Praha: Leges, 2015, str. 18.
[414] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 505.
[415] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1921.

Konzultant napomáhá orgánům činným v trestním řízení pojmout ty z aspektů vyšetřované věci, jež vyžadují speciálních odborných znalostí. Smyslem je vedení dokazování co nejvhodnějším směrem. Konzultant ovšem nemá postavení znalce. Bylo by nepřípustné, pokud by ve své činnosti směřoval k objasnění skutečností důležitých pro trestní řízení z hlediska odborných znalostí zprostředkovaných znalcem dle § 105 TŘ. Smyslem působení konzultanta je výlučně usměrnit odborný postup vyšetřujícího orgánu. Objeví-li se potřeba znaleckého odborného vyjádření, je povinen orgán činný v trestním řízení postupovat podle § 105 TŘ a vyžádat si buď odborné vyjádření, postačí-li, nebo pro složitost posuzovaných otázek přibrat znalce.[416] Na nepřípustné excesy v činnosti konzultanta, jenž nesmí provádět vyšetřovací úkony a získávat podklady pro znalecké posuzování a v tom smyslu i ovlivňovat následný průběh dokazování, poukázal i Vrchní soud v Olomouci.[417]

Jako konzultanta nelze přibrat osobu s určitým vztahem vůči poškozenému, například zaměstnance poškozené obchodní korporace. Veškeré výsledky uvedené spolupráce by v pozdější fázi trestního řízení bylo možné napadnout pro nedostatek objektivity u konzultanta i v postupu orgánů činných v trestním řízení.[418]

4.1.3. Vyšetřování

Policejní orgán podle § 160 odst. 1 TŘ rozhodne neprodleně o zahájení trestního stíhání osoby jako obviněného, jestliže prověřováním zjištěné a odůvodněné skutečnosti nasvědčují, že došlo ke spáchání trestného činu a závěr o tom, že jej spáchala daná osoba, je již dostatečně odůvodněn. Usnesením o zahájení trestního stíhání se zahajuje fáze vyšetřování. Fáze prověřování, tj. postup před zahájením trestního stíhání, není obligatorní fází přípravného řízení, neboť to lze zahájit i přímo vydáním usnesení o zahájení trestního stíhání.

Dle § 161 odst. 1 TŘ se vyšetřováním chápe *„úsek trestního stíhání před podáním obžaloby, návrhu na schválení dohody o vině a trestu, postoupením věci*

[416] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1921.
[417] Usnesení Vrchního soudu v Olomouci, sp. zn. 5 To 202/2002, ze dne 22. 7. 2003.
[418] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1923.

jinému orgánu nebo zastavením trestního stíhání, včetně schválení narovnání a podmíněného zastavení trestního stíhání před podáním obžaloby, návrhu na schválení dohody o vině a trestu.“

Od okamžiku zahájení trestního stíhání náleží obhájci na základě § 165 odst. 2 TŘ právo účasti při vyšetřovacích úkonech, jejichž výsledek lze později provézt jako důkaz před soudem, ledaže by obhájce nebylo možné vyrozumět a úkon odložit. Obhájce smí kdykoli během procesních úkonů vznášet námitky proti způsobu jejich provádění.

Trestní řád umožňuje podle § 158 TŘ vyhledávat a shromažďovat důkazy i před zahájením trestního stíhání proti konkrétnímu obviněnému. Osobě, proti které se trestní řízení vede, proto vzniká určité riziko z pozdního seznámení se s takto nashromážděnými důkazy. Ačkoli takové důkazy mají sloužit toliko k úvaze, jakým směrem dále směřovat dokazování, orgány činné v trestním řízení, včetně soudu, se s nimi v rámci spisového materiálu seznámí a v řadě případů jimi ve skutečnosti budou ovlivněni.[419] Důkazy získané před zahájením trestního stíhání lze rovněž za podmínek § 211 odst. 6 TŘ provézt v hlavním líčení jakožto listinné důkazy. Jako důkaz však nelze užít úředního záznamu sepsaného před sdělením obvinění, neboť tomu brání § 158 odst. 3, odst. 4 TŘ. Nebezpečí pro obhajobu tedy spočívá v nemožnosti zasáhnout do způsobu provádění jednotlivých úkonů, popřípadě v obtížnější možnosti zadat ke zpracování vlastní znalecký posudek.[420] Především u neodkladných či neopakovatelných úkonů, jež bývají prováděny i před zahájením trestního stíhání, je rovnost stran v trestním řízení značně vychýlena. Neodkladným úkonem bude například pořízení zvukového a obrazového záznamu osoby, ohledání věci a místa činu či použití operativně pátracího prostředku.[421] Úkony provedené před zahájením trestního stíhání policejní orgán nemusí opakovat, pakliže jsou prováděny podle trestního řádu.

[419] Typicky při rozporném obsahu výpovědi osoby v rámci podaného vysvětlení oproti protokolu o výslechu svědka, popřípadě výpovědi osoby v procesním postavení obviněného.
[420] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 507.
[421] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 505.

4.1.4. Dokazování

Dokazování je zvláštní formou poznání určité části objektivní reality a zároveň procesem, v němž se odráží základní zásady trestního řízení.[422] Dokazováním trestní právo rozumí zákonem upravený *„postup orgánů činných v trestním řízení, jehož smyslem je poznání skutkových okolností důležitých pro další postup orgánů činných v trestním řízení a v konečné fázi i pro rozhodnutí.“*[423] Dokazování je procesní činností orgánů činných v trestním řízení, v rámci níž dochází díky rekonstrukci předmětu trestního řízení, tj. skutku, k jeho zpětnému poznání. Ačkoli se těžiště procesu nachází ve stádiu hlavního líčení, dokazování neprobíhá pouze v rámci hlavního líčení, nýbrž představuje činnost všech orgánů činných v trestním řízení, směřují-li k opatření a provedení důkazu kdykoli v průběhu trestního řízení. Dokazování tak slouží ke zjištění skutkového stavu pro rozhodnutí povahy mezitímní i pro rozhodnutí meritorní.

Během dokazování dochází ke střetu mezi protichůdnými požadavky – mezi zájmem společnosti na stíhání a potrestání pachatele a zájmem na ochraně společenských hodnot přesahujících účel trestního stíhání. V rámci dokazování je proto zapotřebí zabývat se nejen vnitrostátní úpravou, ale i mezinárodními standardy, představovanými zejména Úmluvou Rady Evropy o ochraně základních lidských práv a svobod.[424] Účelem trestního řízení je totiž nejen spravedlivé potrestání pachatele trestného činu, ale především „fair“ proces.[425]

Dokazování ve smyslu procesní činnosti souvisí úzce s kriminalistikou, jejíž metodika přímo ovlivňuje vyhledávání, zajišťování i využití důkazních prostředků. Trestní řád přitom definuje relevantní procesní postup, bez kterého není možné získané důkazy provést. Kogentní ustanovení trestního řádu určující procesní postupy jsou závazné i pro metodiku vyšetřování počítačové trestné činnosti.

Trestní řád neupravuje veškeré vyšetřovací metody a postupy. Podle pravidla základního předmětu dokazování v § 89 odst. 2 TŘ může sloužit za důkazní prostředek vše, co přispěje k objasnění věci. Procesní přípustnost zákonem neupravených

[422] JELÍNEK, Jiří. *Trestní právo procesní*. 4. aktualiz. a dopl. vyd. Praha: Leges, 2016, str. 358.
[423] Tamtéž, str. 346.
[424] Úmluva Rady Evropy ze dne 4. listopadu 1950 o ochraně lidských práv a základních svobod. Federálním ministerstvem zahraničních věcí ČSFR vyhlášena pod č. 209/1992 Sb.
[425] Nález Ústavního soudu sp. zn. II. ÚS 268/03, ze dne 3. 11. 2004.

vyšetřovacích metod však musí vždy odpovídat rámcovým procesním ustanovením a předně základním zásadám trestního řízení. Zákonnou bude taková vyšetřovací metoda, jež směřuje k objektivnímu skutkovému zjištění, je vědecky ověřena, nezakazují ji kogentní ustanovení trestního řádu a je v souladu se základními zásadami trestního řízení i rámcovými procesními ustanoveními.[426]

V rámci dokazování počítačové kriminality existují vedle obecných ustanovení předmětu dokazování dle § 89 odst. 1 TŘ určité zvláštnosti. V závislosti na konkrétních formách počítačové trestné činnosti a skutkové podstatě trestného činu dovodíme konkrétní podobu metodiky vyšetřování. Jak je uvedeno výše, specifická metodika vyšetřování se vztahuje například na softwarové pirátství. Bez ohledu na konkrétní specifika však bývá u všech forem počítačové trestné činnosti dokazováno:

- zda jde o jeden nebo více skutků,
- ztotožnění počítače zneužitého ke spáchání trestného činu,
- způsob a postup provedené operace na počítači,
- zda šlo o trestnou součinnost,
- rozsah pachatelova oprávnění s počítačem nakládat,
- hloubka pachatelových znalostí v oblasti ICT,
- zda a s jakým časovým odstupem došlo po události k zajištění techniky,
- zda je zajištěný obsah počítače původní,
- rozsah vzniklé škody a další.[427]

Při dokazování se zásadním způsobem uplatní zásada materiální pravdy, obsažená v § 2 odst. 5 TŘ. Orgány činné v trestním řízení zjišťují skutkový stav věci, o kterém nejsou důvodné pochybnosti, a to v rozsahu nezbytném pro každé z jejich rozhodnutí. Do jaké míry se během dokazování podaří předmětný skutek věrně rekonstruovat, bude stěžejní pro zásadu materiální pravdy i pro správnost rozhodnutí.[428] Zásada materiální pravdy ovšem není bezbřehá. Limituje ji zákonný rámec, ve kterém orgány činné v trestním řízení uplatňují svou pravomoc. Konkrétní zákonný rámec vyplývá ze specifické zákonné úpravy jednotlivých procesních úkonů.

[426] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 348.
[427] CHMELÍK, Jan; PORADA, Viktor. Vybrané problémy vyšetřování a dokazování počítačové kriminality II. In: *Identifikace potřeb právní praxe jako teoretický základ pro rozvoj kriminalistických a právních specializací*. 1. vyd. Karlovy Vary: Vysoká škola Karlovy Vary, o. p. s., 2011, str. 356.
[428] JELÍNEK, Jiří. *Trestní právo procesní*. 4. aktualiz. a dopl. vyd. Praha: Leges, 2016, str. 358.

4.2. Vybrané procesní úkony

4.2.1. K pojmu procesního úkonu

„Procesními úkony jsou všechny úkony vykonávané orgány činnými v trestním řízení podle trestního řádu a na jeho základě.“[429] Jde tedy o úkony trestního řízení, přičemž *„nezáleží na stádiu trestního řízení, v kterém jsou prováděny.“*[430] Procesními úkony jsou i úkony prováděné na základě § 158 TŘ před zahájením trestního stíhání, včetně neodkladných a neopakovatelných úkonů. Hovoříme rovněž o úkonech subjektů trestního řízení, s nimiž trestní řád spojuje vznik, změnu nebo zánik trestně procesních vztahů.[431]

Dle povahy procesního úkonu popsaného v trestním řádu lze zpravidla dovodit i jeho obsah. Forma procesních úkonů zaručí zákonnost trestního řízení i splnění jeho účelu. Značná část procesních úkonů v rámci trestního řízení se provádí ústně, pročež je zapotřebí průběh každého úkonu protokolovat.[432] Ustanovení § 55 odst. 1 TŘ určuje zásadní pravidlo protokolování každého procesního úkonu, není-li stanoveno zákonem jinak. Sepsaný protokol svědčí o dodržení stanovené zákonné formy, neboť porušení předepsané formy procesního úkonu je i důvodem zrušení rozhodnutí v opravném řízení.[433] Zákonnost procesních úkonů se posuzuje z hlediska znění trestního řádu a relevantních procesních předpisů účinných v době jejich aplikace, na rozdíl od hmotněprávních ustanovení časové působnosti trestního práva.[434]

V průběhu procesních úkonů jsou orgány činné v trestním řízení povinny šetřit osobnost a ústavním pořádkem zaručená práva osob na úkonu zúčastněných. Zásadním při provádění procesních úkonů se stává princip proporcionality uvedený v čl. 4 odst. 4 Listiny základních práv a svobod (dále též „Listina“),[435] i základní zásady trestního řízení, především zásada oficiality dle § 2 odst. 4 TŘ, podle níž orgány činné v trestním

[429] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 247.
[430] ŠÁMAL, Pavel. *Trestní řád: komentář. I. svazek, § 1 – § 156.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 607.
[431] JELÍNEK, Jiří. *Trestní právo procesní*. 4. aktualiz. a dopl. vyd. Praha: Leges, 2016, str. 286.
[432] Tamtéž, str. 289.
[433] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 248.
[434] Usnesení Nejvyššího soudu České republiky, sp. zn. 2 Tzn 63/95, ze dne 14. 12. 1995.
[435] Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.

řízení při provádění úkonů trestního řízení do práv a svobod chráněných na ústavní úrovni zasahují jen v odůvodněných případech a v míře nezbytné pro zajištění účelu trestního řízení. Postup orgánů činných v trestním řízení musí být nejen v souladu se zákonem, ale *„v rámci možností do těchto ústavně zaručených základních práv a svobod zasahovat co nejméně, což je výrazem humanizace trestního řízení a úcty k lidským právům a svobodám.“*[436]

Vyšetřovací a operativně pátrací úkony představují obsáhlou množinu procesních úkonů, prováděných zejména v předsoudní fázi trestního řízení. S ohledem na klíčový význam přípravného řízení pro naplnění účelu trestního řízení je nezbytným vždy dbát na přesné dodržení procesní stránky úkonů.[437]

4.2.2. Operativně pátrací prostředky

Operativně pátrací prostředky lze definovat jako *„souhrn opatření policejních orgánů prováděný v souladu s trestním řádem a dalšími právními předpisy za účelem předcházení, odhalování a objasňování trestné činnosti, pátrání po skrývajících se pachatelích, hledaných nezvěstných osobách a věcných důkazech.“*[438] Trestní řád umožňuje zvukové, obrazové a jiné záznamy získané použitím operativně pátracích prostředků způsobem podle trestního řádu využít jako důkaz.[439]

Operativně pátrací prostředky uvedené v § 158b až 158f TŘ se řadí pod operativně pátrací činnost. Operativně pátrací činností je systém činností prováděný utajeně specializovanými orgány, pomocí kterých dochází k průzkumu informací a signálů o případné trestné činnosti ve společnosti. Vedle operativně pátracích prostředků uvedených v trestním řádu jsou operativně pátrací činností i podpůrné operativně pátrací prostředky na základě § 72 a násl. ZPČR. ZPČR uvádí jejich

[436] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 250.
[437] MENDEL, Aleš. Vyšetřování počítačové kriminality. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 89.
[438] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 507.
[439] § 158b odst. 3 TŘ.

taxativní výčet: jde o využití informátora, krycích prostředků, zabezpečovací techniky a zvláštních finančních prostředků.[440]

Cílem operativně pátracích prostředků upravených ZPČR je vyhledávání a dokumentování informací důležitých pro plnění úkolů Policie ČR. *„Podpůrné operativně pátrací prostředky jsou instituty policejního práva, které spíše nasazení operativně pátracích prostředků trestního řádu umožňují a podporují, než aby jejich bezprostředním účelem bylo opatření důkazu pro trestní řízení.“*[441]

V rámci postihu počítačové kriminality lze využít například podpůrný operativně pátrací prostředek zabezpečovací techniky (viz § 76 ZPČR) k pořízení záznamů dle § 158d odst. 2 TŘ. Při zachování podmínek trestního řádu je možné takto získané stopy využít jako důkazní prostředek. Při postihu zejména organizované počítačové kriminality bývají využíváni informátoři, kteří mohou uvést cenné informace pro policejní databáze crackerů, obsahující jejich přezdívky, předpokládaná místa pobytu i komunikační sítě.[442] Tyto informace však bez dalšího nemohou sloužit jako důkazní prostředek.[443]

Operativně pátracími prostředky dle trestního řádu je předstíraný převod, sledování osob a věcí a použití agenta. Ustanovení § 158b TŘ určuje společné podmínky jejich použití. Trestní řízení musí být vedeno o úmyslném trestném činu a použití operativně pátracích prostředků nesmí sledovat jiný zájem než získání skutečností důležitých pro dané trestní řízení. Vždy je nutné dbát dodržení principu subsidiarity, tj. podmínky, dle níž nebude možné sledovaného účelu dosáhnout jinak než využitím konkrétního operativně pátracího prostředku, anebo toliko s podstatnými obtížemi. Práva a svobody dotčených osob je možné omezit jen v nezbytně nutné míře, kterou vykládáme nejen z hlediska intenzity zásahu, nýbrž i délky jeho trvání.[444] Operativně pátrací prostředky je zásadně oprávněn použít jen k tomu pověřený policejní orgán.[445]

---

[440] § 72 ZPČR.
[441] VANGELI, Benedikt. *Zákon o Policii České republiky: komentář*. 2. vyd. V Praze: C.H. Beck, 2014, str. 307.
[442] GLENNY, Misha. *Temný trh: kyberzloději, kyberpolicisté a vy*. 1. vyd. v českém jazyce. Praha: Argo, 2013, str. 15.
[443] Osobu je možné vyslechnout jako svědka.
[444] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 508.
[445] § 158b odst. 1 TŘ.

Specifické podmínky operativně pátracích prostředků upravují ustanovení § 158c až § 158e TŘ. Sledováním osob a věcí na základě § 158d TŘ dochází k utajenému získávání poznatků o osobách a věcech. V rámci vyšetřování počítačové kriminality se běžně využívá sledování osob a věcí technickými prostředky[446] - i spolu s odposlechem a záznamem telekomunikačního provozu dle § 88 TŘ a § 88a TŘ.[447] Podle § 158d odst. 3 TŘ lze zajistit aktuální stav e-mailové schránky.[448] Pořízení jakéhokoli záznamu během sledování vyžaduje písemný souhlas státního zástupce. Pokud by však mělo sledování zasáhnout do nedotknutelnosti obydlí, listovního tajemství, či vést ke zjišťování obsahu písemností a záznamů uchovávaných v soukromí, trestní řád vyžaduje předchozího souhlasu soudce, který přiměřenost daného zásahu vždy zváží ve vztahu ke konkrétní vyšetřované (prověřované) trestné činnosti. Pořízený záznam by bylo možné využít jako důkaz v jiné trestní věci, pakliže by v ní bylo také vedeno řízení o úmyslném trestném činu, anebo za souhlasu osoby, do jejíchž práv a svobod bylo sledováním zasahováno.[449] Vždy je však ze sledování naprosto vyloučena komunikace obviněného s obhájcem. Zvukový, obrazový nebo jiný záznam musí být v takovém případě zničen. Striktní podmínka je však vázána na okamžik zahájení trestního stíhání, kdy se policejní orgán zpravidla konečně dozví, kdo je vlastně obhájcem obviněného. Ohledně komunikace obviněného s obhájcem nelze jako svědka vyslýchat ani policistu, jenž byl sledováním pověřen.[450]

Operativně pátrací prostředky bývají využívány v průběhu předsoudní fáze trestního řízení. I v trestním řádu jsou uvedeny v rámci hlavy deváté, upravující postup před zahájením trestního stíhání. Jak ovšem plyne z § 158f TŘ, není vyloučeno ani jejich pozdější uplatnění, například až po podání obžaloby.

V souvislosti s využitím operativně pátracích prostředků se lze též setkat s tematikou policejní provokace, a to v případě, kdy je právu na spravedlivý proces

---

[446] Zabezpečovací technikou se dle § 76 ZPČR rozumí *„technické prostředky, zařízení a jejich soubory používané za účelem předcházení nebo odstranění ohrožení veřejného pořádku a bezpečnosti.“*

[447] Státní orgány v České republice ročně provedou značný počet zmíněných úkonů. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 220.

[448] ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2015, 6(11), str. 32.

[449] Srov. § 158d odst. 10 TŘ.

[450] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 2005.

nadřazena účelnost vyšetřovacích metod.[451] V souvislosti s vyšetřováním počítačové kriminality se celosvětové známosti dočkal projekt namířený proti konzumentům dětské on-line pornografie. Digitální konstrukt s věrnou podobou desetileté dívky láká na Internetu potenciální pachatele k provozování sexuálních aktivit přes webovou kameru. Digitální dívku ovládají z Amsterodamu vyšetřovatelé díky speciálnímu software, který zároveň zaznamenává průběžně její komunikaci s druhou stranou. V závislosti na přímosti požadavku komunikující osoby jsou získané poznatky dány k dispozici orgánům činným v trestním řízení v konkrétním státě, jež mohou na základě získaných informací zahájit trestní stíhání. První odsuzující rozsudek padl na podzim roku 2014 před Okresním soudem v Brisbane v Austrálii.[452]

Ústavní soud k policejní provokaci uvedl, že natolik významný zásah do soukromí občanů musí vždy podléhat přísné kontrole jiných nezávislých orgánů. K míře přípustnosti provokace ze strany orgánů státu dodal: *„Je nepřípustným porušením čl. 39 Listiny a čl. 7 odst. 1 Úmluvy, pakliže jednání státu (v dané věci Policie) se stává součástí skutkového děje, celé posloupnosti úkonů, z nichž se trestní jednání skládá. Jinými slovy nepřípustný je takový zásah státu do skutkového děje, jenž ve své komplexnosti, tvoří trestný čin, resp. takový podíl státu na jednání osoby, jehož důsledkem je trestní kvalifikace tohoto jednání.“*[453] Policejní orgán se nesmí aktivně podílet na vytváření skutkového děje. Na aktivní jednání pachatele smí reagovat pouze v mezích zákonných ustanovení.

4.2.2.1. Použití sledovacího software

V rámci operativně pátrací činnosti policejní orgán využívá různé druhy sledovacího software. V praxi se může jednat o využití GSM interceptoru, tzv. systému Agáta, zařízení simulujícího základnovou stanici, k níž se hlásí mobilní telefon při

[451] SOTOLÁŘ, Alexander; PÚRY, František; WORATSCHOVÁ, Vladana. Posuzování policejní provokace. *Trestněprávní revue*. 2002, 1(11), str. 313.
[452] Podrobněji STARR, Michelle. First man convicted in child predator sting with virtual girl Sweetie [online]. Dostupné z http://www.cnet.com/news/first-man-convicted-in-child-predator-sting-with-virtual-girl-sweetie/ [cit. 2016-03-26]. Překlad autorka.
[453] Nález Ústavního soudu, sp. zn. III. ÚS 597/99, ze dne 22. 6. 2000.

zahájení volání.[454] Lze využít i spyware, tj. software skrytě sledující aktivitu uživatele počítače s cílem zachytit a zaznamenat osobní údaje a další informace, které se mohou i nemusí týkat obsahové komunikace. Sledovat lze i datovou komunikaci, poté hovoříme o metodě sniffing.[455]

Nasazení sledovacího software se vždy musí dít toliko na základě zákona a zákonem předepsaným způsobem. Software jako počítačový program zpracovává vstupní informace dle zadaných příkazů, proto z reálného světa zaznamenává poznatky a převádí je do virtuální podoby, ve které jsou způsobilé zpracování. Striktně vzato tedy při použití sledovacího software dochází vždy k pořizování záznamu, v důsledku čehož nutně dospějeme k absolutnímu vyloučení použití sledovacího software v rámci § 158d odst. 1 TŘ, kde jeho použití podléhá toliko úvaze pověřeného policejního orgánu. Sledování, v rámci něhož vznikají obrazové, zvukové či jiné záznamy, musí písemně povolit státní zástupce, přičemž doba sledování nesmí překročit šest měsíců.[456]

Poznatky získané operativně pátrací činností dle trestního řádu jsou procesně využitelné pouze jako operativní informace, na jejichž základě může soudce například nařídit odposlech a záznam telekomunikačního provozu dle § 88 TŘ.[457] Použití sledovacího software ve smyslu operativně pátracího prostředku dle § 158d TŘ s cílem získání důkazů pro trestní řízení je nepřípustné tam, kde by jeho aplikací docházelo k obcházení speciálních ustanovení trestního řádu, resp. zvláštních zajišťovacích institutů. Zásahem do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťování obsahu jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků sledování osob a věcí nelze nahrazovat zásahy již specificky upravené v jiných ustanoveních hlavy čtvrté trestního řádu.[458] Příkladem lze uvést zajištění paměťového nosiče s usvědčujícími informacemi – věc důležitou pro trestní řízení.

[454] Agáta přinutí mobil zaregistrovat se k ní a následně získá z komunikace klíč k rozšifrování hovoru. Donutí cílový telefon používat namísto obvyklé méně zabezpečenou šifru, kterou software umí rozluštit. Jde o falešnou základnovou stanici, která donutí odposlouchávaný telefon se k ní připojit, tj. o útok typu „man-in-the-middle. Podrobněji SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 226.

[455] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 226.

[456] Srov. § 158d odst. 2, odst. 4 TŘ.

[457] Sledovací software lze využít i v rámci odposlechu a záznamu telekomunikačního provozu dle § 88 TŘ.

[458] Úprava § 158d odst. 3 TŘ je z hlediska sledování osob a věcí doplňující. Podrobněji ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 2007.

Uvedeného lze docílit skrze domovní prohlídku, anebo monitorováním aktivity sledovaného zařízení pomocí sledovacího software typu spyware. Nad rámec lze dodat, že instalací spyware se policejní orgán dopustí jednání popsaného ve skutkové podstatě trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 TZ.

Sledovací software bývá využíván i jinými orgány, jako je Bezpečnostní informační služba (dále též „BIS“) a Vojenské zpravodajství, které jej využívají jako zpravodajský prostředek. I zde je nutné trvat na nasazení sledovacího software striktně na základě zákona a v jeho mezích. Podmínky specifických prostředků získávání informací upravuje v případě BIS zákon č. 154/1994 Sb., o Bezpečnostní informační službě, a v případě další zpravodajské služby zákon č. 289/2005 Sb., o Vojenském zpravodajství.[459] Využití takto získaných poznatků jako důkazu v trestním řízení je striktně zakázáno, neboť by došlo k popření principů demokratického právního státu a k faktickému obcházení trestního řádu skrze předpisy zpravodajské. Zmíněný postup popírá rámec zákonného trestního procesu jako takového, jehož smyslem je náležitě zjistit trestné činy vždy toliko zákonným způsobem. Generální klauzuli o použitelnosti důkazů v § 89 odst. 2 TŘ zde nelze použít.[460]

4.2.3. Zajištění věcí

Zajišťovací úkony upravené v hlavě čtvrté trestního řádu hrají významnou roli při získání důkazních prostředků. Zajištění věcí je upraveno v § 78 až 81b TŘ, jež definují podmínky přípustnosti zásahu do vlastnických práv. Porušení procesních předpisů může vést až k neúčinnosti důkazu z důvodu nezákonnosti jeho získání či

[459] Nyní projednává v 1. čtení Poslanecká sněmovna PČR návrh na novelizaci zákona č. 289/2005 Sb., s cílem založit Vojenskému zpravodajství novou oblast působnosti při zabezpečování kybernetické obrany České republiky. Použití technických prostředků kybernetické obrany by mělo být pod kontrolou Vrchního soudu v Praze. Existují však oprávněné obavy z přílišného rozšíření pravomoci Vojenského zpravodajství. Sněmovní tisk 931 Novela z. o Vojenském zpravodajství, včetně vládního návrhu dostupné z http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=931&CT1=0[cit. 2017-02-11].
[460] Nález Ústavního soudu ČR, sp. zn. I ÚS 3038/07-1, ze dne 29. 2. 2008.

nezákonnosti získání jeho zdrojů.[461] Důkaz, ke kterému se orgán činný v trestním řízení dostal nezákonnou cestou, není v trestním řízení přípustný.[462]

Současná právní úprava s ohledem na povahu předmětné věci rozlišuje zajištění věci hmotné a zajištění věci nehmotné. Specificky upravuje zajištění peněžních prostředků na účtu u banky, zajištění zaknihovaných cenných papírů a zajištění nemovitosti. Rozdílu mezi zajištěním nehmotné věci a zajištěním digitálních dat úprava nečiní, ačkoli pro digitální data není nejvhodnější a s ohledem na jejich zvláštnosti bude do budoucna vhodné procesně specifika oblasti upravit.[463] Orgány činné v trestním řízení se k důkazům nyní dostávají skrze vytěžení informací ze zajištěných datových nosičů, a to až s pomocí odborné forenzní expertízy (ať již znaleckého posudku či odborného vyjádření). Expertíza představuje leckdy příliš zdlouhavou činnost, jejíž náročnost se s ohledem na narůstající objem zpracovávaných dat bude do budoucna zvyšovat.

Povinnost na vyzvání předložit či vydat hmotnou věc důležitou pro trestní řízení, tj. ediční povinnost, upravuje § 78 TŘ. Není-li nutné hmotnou věc zajistit pro účely trestního řízení, postačí její předložení, v ostatních případech se věc zajistí. Povinnou osobou je držitel předmětné věci. Nevyhoví-li výzvě orgánu činného v trestním řízení, může být osobě hmotná věc odňata, popřípadě i uložena pořádková pokuta dle § 66 TŘ. Ke splnění ediční povinnosti nelze jakkoli nutit podezřelého, neboť by došlo k porušení zásady *nemo tenetur se ipsum accusare*, podle které není nikdo povinen jakýmkoli způsobem přispět k usvědčení sebe samého.[464]

Není-li splněna ediční povinnost, lze hmotnou věc odejmout na základě § 79 TŘ. Odnětí věci v sobě nese prvek sankce za nesplnění předchozí výzvy, avšak toliko v případě předchozího upozornění na možnost odnětí věci. K odnětí hmotné věci je třeba příkazu předsedy senátu, v přípravném řízení příkazu státního zástupce či policejního orgánu s předchozím souhlasem státního zástupce. Bez něj smí policejní

[461] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 301.
[462] Mimo jiné jde o americkou právní doktrínu „Plody z otráveného stromu“. Detailněji HERCZEG, Jiří. Zásada „nemo tenetur“ a práva obviněného v trestním řízení. *Bulletin advokacie*. 2010, (1 - 2).
[463] ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2015, 6(11), str. 32.
[464] Blíže viz HERCZEG, Jiří. Zásada „nemo tenetur“ a práva obviněného v trestním řízení. *Bulletin advokacie*. 2010, (1 - 2), str. 38 – 39.

orgán vydat příkaz sám, nelze-li předchozího souhlasu státního zástupce dosáhnout a věc odkladu nesnese. Vůči příkazu k odnětí věci není stížnost přípustná.

Na určitý okruh osob a věcí se ediční povinnost nevztahuje. Předně jí nepodléhají osoby požívající výsad a imunit dle § 10 odst. 1 TŘ. Dále jsou z ediční povinnosti vyňaty listiny obsahující poznatky, o kterých platí zákaz výslechu, ledaže dojde ke zproštění povinnosti mlčenlivosti či zachovávání věci v tajnosti. Pojem listiny vykládá trestní právo široce, úprava proto dopadne i na paměťové nosiče s obrazovým, zvukovým nebo obdobným záznamem.[465]

Novelou trestního řádu účinnou od 1. 6. 2015[466] došlo k jeho přizpůsobení občanskému právu a k rozšíření podmínek zajištění nehmotných věcí.[467] Novelizovaný § 79e TŘ upravuje zajištění nehmotné věci. Použije se především při zajištění pohledávek z nejrůznějších právních titulů, jako je tomu u práva k podílu v obchodní korporaci.[468] Nedomnívám se, že zaručí efektivnější zajištění digitálních dat.[469] Bude-li cílem zajištění věci získání důkazního prostředku, pak v případě existence paměťových nosičů s digitálními důkazy bude vhodnější zajistit úplnou bitovou kopii obsahu nosiče. Pokud zajištění věci bude mířit i na znemožnění dispozice s digitálními daty, nebude patrně ustanovení § 79e odst. 2 TŘ umožňující zákaz výkonu práv související se zajištěnou nehmotnou věcí, efektivní. Například v případě porušení autorského práva dispozicí se souborem filmových děl může dojít k zajištění paměťového nosiče, tedy hmotné věci. Osoba může mít však dále přístup k legálně instalovanému software, díky kterému nelegálně získává a šíří filmová díla, a to z kteréhokoli počítače. Abychom v takovém případě dosáhli účelu zajišťovacího institutu, museli bychom dotyčnému zakázat, resp. znemožnit přístup k jakémukoli počítači, což je absurdní.

Institut zajištění věci vychází z pravomocí orgánu činného v trestním řízení v tradičním off-line světě. S ohledem na povahu digitálních dat obvykle není zajištění hmotné věci dostačující, neboť v rámci počítačové kriminality cílí orgán především na

[465] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1018.
[466] Zákon č. 86/2015 Sb., kterým se mění zákon č. 279/2003 Sb., o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony.
[467] Dřívější pojem „jiná majetková hodnota" byl podřazen kategorii „věc", resp. „věc nehmotná".
[468] Podrobněji Sněmovní tisk 305/0 (7. volební období, od 2013), vládní návrh zákona, kterým se mění zákon č. 279/2003 Sb., o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, str. 99. Dostupné z http://www.psp.cz/sqw/tisky.sqw [cit. 2016-03-27].
[469] K povaze digitálních stop srov. PORADA, Viktor; ŠEDIVÝ, Petr. Kriminalistické a forenzní aspekty počítačové (kybernetické) kriminality. *Karlovarská právní revue*. 2011, 7(2), str. 44.

data, ne hmotné nosiče. Doba, kdy postačilo zajistit paměťové médium, popřípadě veškerý hardware a poté jej podrobit expertnímu zkoumání v laboratorních podmínkách, odeznívá, alespoň u důmyslnějších případů kybernetické trestné činnosti, kdy pachatelé neschraňují data na svém počítači, ale využívají služeb cloud computing a přístup k datům chrání hesly. V takovém případě vyvstává nutnost spolupráce s poskytovatelem služby cloud computing. Vždy se však vyplatí konzultovat s odborníky, která zařízení výpočetní techniky je vhodné zajistit.[470]

4.2.3.1. Problematika šifrování

Během vyšetřování počítačové trestné činnosti se objevují případy, kdy zajištění věci nepovede ke kýženému cíli, tj. k obstarání důkazu. Ačkoli bude paměťový nosič zajištěn, anebo vyšetřující orgán získá přístup k uloženým digitálním datům osoby jinak, zajištěná data budou chráněna šifrou, k níž daná osoba odmítne poskytnout přístupový klíč.

Šifrování je technikou určenou k ochraně soukromí a důvěrnosti komunikace uživatelů veřejných počítačových sítí. Výhody šifrování si uvědomují mnozí. Pachatelé počítačové kriminality, zejména producenti dětské pornografie, organizovaný zločin a teroristé, šifrování stále častěji využívají ke krytí vlastních aktivit. Čím jsou pachatelé vzdělanější v oblasti ICT, tím častěji svá data šifrují.[471] Je-li použita správně, nelze šifrovací techniku bez znalosti jejího klíče žádným způsobem prolomit. Podstata šifrování spočívá v přeskupení dat dle specifického vzorce, podle určitého klíče. Klíč je digitální textový řetězec, bez jehož znalosti není možné data dešifrovat, tj. uvést je do původní podoby.

Šifrovací klíč lze někdy zjistit tzv. hrubou silou, čímž se má na mysli zadat počítači projít všechny možné kombinace jednotlivých podob klíče, tj. veškeré možné variace pořadí čísel 1 a 0. Čím delší textový řetězec, tím více kombinací. Od určitého

[470] MENDEL, Aleš. Vyšetřování počítačové kriminality. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 92.
[471] Roku 1998 tým FBI analyzující hrozby počítačové kriminality (Computer Analysis Response Team) uvedl, že zhruba v 6% případů vyšetřované počítačové trestné činnosti narazil na šifrovaná data. YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013, str. 165. Překlad autorka.

počtu bitů textového klíče proto bude nemožné jej tímto způsobem zjistit.[472] Poté zbude orgánům činným v trestním řízení jen věřit ve výslech osoby, proti níž se vede trestní řízení, a svědků.

Úmluva o počítačové kriminalitě požaduje, aby smluvní strany přijaly úpravu umožňující *„přikázat kterékoli osobě, která má znalosti o fungování počítačového systému nebo o opatřeních použitých na ochranu počítačových dat v tomto systému, aby poskytla nezbytné informace“*[473] k přístupu k uloženým počítačovým datům. Jde vlastně o příkaz k vydání šifrovacího klíče.[474] Obecné ustanovení § 8 odst. 1 TŘ požaduje po právnických a fyzických osobách součinnost s orgány činnými v trestním řízení. „Dešifrovací příkaz“ však trestní předpisy neupravují. Ve vztahu k osobě podezřelé by ani nebyl možný, neboť předmětnou informaci nelze získat bez aktivního konání osoby, proti níž se vede trestní řízení - vyvstal by konflikt se zásadou *nemo tenetur se ipsum accusare*.[475] Kvalitní šifrovací klíč, jehož podobu zná toliko pachatel spolupráci nepřístupný, neumožňují zákonné prostředky získat.

4.2.4. Domovní prohlídka a prohlídka jiných prostor a pozemků

4.2.4.1. Domovní prohlídka

Domovní prohlídka slouží k zajištění osob nebo věcí důležitých pro trestní řízení. Jejím předpokladem je důvodné podezření, že v bytě nebo v jiných prostorách, které jsou součástí obydlí, se taková věc či osoba nachází.[476]

Obydlí člověka, které vykládá ustanovení § 133 TZ, požívá zvláštní ochrany, neboť jde o místo nerozlučně spjaté s ochranou základních lidských práv, jako práva na soukromí a ochranu rodinného života i nedotknutelnosti obydlí, které jsou pod ústavní ochranou.[477] Termín obydlí je vykládán extenzivně, za obydlí je nutno považovat

[472] YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013, str. 166. Překlad autorka.
[473] Čl. 19 odst. 4 Úmluvy o počítačové kriminalitě.
[474] V zahraniční literatuře se užívá pojmu „decryption order“.
[475] K rozboru této zásady jako součásti práva na spravedlivý proces viz Rozsudek Evropského soudu pro lidská práva ve věci Saunders v. The United Kingdom ze dne 17. 12. 1996, § 69.
[476] § 82 odst. 1 TŘ.
[477] Především čl. 7 odst. 1, čl. 10 odst. 2, čl. 12 a čl. 13 Listiny nebo čl. 8 EÚLP.

například i vysokoškolskou kolej, která je výchozím místem aktivit určité části pachatelů zejména softwarového pirátství.

Příkaz k domovní prohlídce vydává předseda senátu, resp. soudce na návrh státního zástupce, jde-li o přípravné řízení. Příkaz k domovní prohlídce musí být vždy písemný a odůvodněný. V neodkladných případech není zapotřebí dodržet obecná ustanovení o příslušnosti soudu – příkaz může vydat i soudce či předseda senátu, v jehož obvodu bude domovní prohlídka provedena. Příkaz k domovní prohlídce je nutno osobě, u které má být bude domovní prohlídka vykonána, při prohlídce doručit. Existuje-li překážka doručení, je nutno jej doručit nejpozději do 24 hodin po odpadnutí překážky.

4.2.4.2. Prohlídka jiných prostor a pozemků

V případě provedení prohlídky jiných prostor a pozemků, tj. míst, která nelze považovat za součást obydlí, platí pravidla obdobná jako u domovní prohlídky. Jiné prostory jsou prostory nesloužící k bydlení, avšak pakliže nejsou veřejně přístupné. Jedná se především o kanceláře, skladiště či akademickou půdu vysoké školy.[478]

Ústavní soud v rámci prohlídky jiných prostor a pozemků dovozuje obdobný význam ochrany soukromé sféry jednotlivce jako u prohlídek domovních. Nepovažuje za ústavně konformní, aby *„trestní řád, jako zákonný předpis upravující v trestních věcech stanovený postup (§ 82 a násl.), určoval podmínky, za nichž je přípustné narušit právo každého jednotlivce na soukromí výkonem domovní prohlídky (§ 83), odlišně (přísněji) než v případě výkonu prohlídky jiných prostor a pozemků (§ 83a), ačkoliv prohlídka jiných prostor nepochybně rovněž představuje zásah do práva každého jednotlivce na soukromí, a to v obdobném rozsahu jako v případě domovní prohlídky.“*[479]

Termín jiné prostory a pozemky je široký a určité odlišnosti se v jeho rámci uplatní, jinak by stačilo jediné ustanovení o obecné prohlídce prostor. Odlišnosti se týkají možnosti provedení prohlídky jiných prostor a pozemků se souhlasem uživatele

[478] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1114.
[479] Nález Ústavního soudu, sp. zn. Pl. ÚS 3/09, ze dne 8. 6. 2010, bod 3. Nález zrušil tehdejší znění části § 83a odst. 1 TŘ pro rozpor s ústavním pořádkem.

prostor a u neodkladného provedení této prohlídky bez soudního příkazu, kterého nelze dosáhnout předem. Policejní orgán je ovšem povinen si příslušný souhlas bezodkladně vyžádat. Jestliže jej nedostane, výsledek prohlídky nebude možné v trestním řízení jako důkaz použít.[480]

4.2.4.3. Společná úprava

Jde-li o neodkladný zásah, smí policejní orgán vstoupit do obydlí, jiných prostor a na pozemek i bez příkazu k příslušné prohlídce. Podmínky uvádí § 83c TŘ. Předpokladem není získání důkazních prostředků, nýbrž ochrana života a zdraví osob nebo jiných práv a svobod, či odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. S ohledem na uvedené nesmí policejní orgán po vstupu do uvedených míst provádět jiných úkonů než nezbytně nutných k odstranění nebezpečí, popřípadě k předvedení osoby. Důkazní prostředky získané v rozporu s tímto zákazem nelze v trestním řízení použít.

Osoby, u kterých se provádí domovní prohlídka či prohlídka jiných prostor a pozemků, jsou povinny strpět příslušné procesní úkony. Před jejich samotným započetím však musí být vyslechnuty. Do § 84 TŘ se promíjí princip proporcionality, zdůraznění dosažení cíle procesních úkonů cestou mírnější, tj. typicky dobrovolným vydáním potřebné věci. Předchozího výslechu není zapotřebí, nesnese-li věc odkladu a výslech nelze okamžitě provést. U právnických osob je doporučena přítomnost statutárního zástupce či jiné osoby s řídící funkcí.[481] V případě kladeného odporu jej smí policejní orgán dle § 85a TŘ po marné výzvě překonat.

V případě domovní prohlídky a prohlídky jiných prostor a pozemků, v nichž se očekává výskyt výpočetní techniky, je nutné se předem důkladně připravit, zejména s ohledem na riziko dálkové manipulace s daty nacházejícími se v místě prohlídky skrze počítačové sítě. Pokud je to možné, počítačové sítě v místě prováděné prohlídky se předem zablokují.[482]

---

[480] § 83a odst. 2 TŘ.
[481] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995, str. 139.
[482] MENDEL, Aleš. Vyšetřování počítačové kriminality. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 92.

Vyšetřování počítačové kriminality, jak je výše uvedeno, naráží na problém dat chráněných státem uloženou nebo uznanou povinností mlčenlivosti. Během domovních prohlídek a prohlídek jiných prostor a pozemků dochází při zajištění výpočetní techniky k citelnému narušení soukromí uživatele. Zajištění dopadne i na značný objem legálních dat, právě jako i na data podléhající povinnosti mlčenlivosti. Ústavní soud zmiňuje, že lze jako věci důležité pro trestní řízení zajistit i výpočetní techniku, včetně záznamových médií a jejich kopií, *„i když existuje možnost, že zajištěné nosiče informací obsahují vedle záznamů o skutečnostech důležitých pro trestní řízení i informace o skutečnostech, které se netýkají probíhajícího trestního řízení a ke kterým se váže státem uložená nebo uznaná povinnost mlčenlivosti.“*[483] Tvrzení osoby, u které se prohlídka provádí nebo osoby, jež je prohlídce přítomna, že zajišťované nosiče obsahují i informace, vůči nimž je osoba vázána povinností mlčenlivosti, nemůže jejich zajištění bránit a k porušení povinnosti mlčenlivosti nedochází. Během probíhající prohlídky obvykle nelze dost dobře oddělit tu část výpočetní techniky, v níž se nachází pouze informace, které se trestního řízení netýkají, a je proto zajišťována plošně.[484]

Ne vždy je k provedení příslušné prohlídky při vyšetřování počítačové kriminality policejní orgán připraven. Jak ilustruje následující případ, není vždy zajištěna přítomnost odborníka na výpočetní techniku, což může vést k nevhodným závěrům. Ústavní soud v dané kauze posuzoval opodstatněnost domovní prohlídky s ohledem na zásadu přiměřenosti v § 2 odst. 4 TŘ a § 84 TŘ. Ve své ústavní stížnosti namítal stěžovatel nepřiměřenost domovní prohlídky v brzkých ranních hodinách i s ohledem na předcházející chybné vyhodnocení dotčených IP adres vztahujících se k trestné činnosti.[485] Nedostatek policejní orgán nemohl na místě napravit a rozhodnout o ukončení nařízené domovní prohlídky, mimo jiné dle vlastních slov proto, že není počítačovým expertem. Ústavní soud neshledal stížnost důvodnou, neboť policejní orgán opravdu nemohl stěžovatelovo tvrzení bezprostředně ověřit a zbavit jej tak podezření. Stěžovatelova ústavní práva nebyla porušena, neboť přes podstatný zásah do jeho práv byl procesní úkon proveden v souladu s právními předpisy a sledoval veřejný

[483] Usnesení Ústavního soudu, sp. zn. IV. ÚS 2/02, ze dne 28. 3. 2002.
[484] Poznatky důležité pro trestní řízení mohou být skryty mezi nesouvisejícím obsahem a pojmenovány matoucími názvy. Jednodušší software zaměřený na klíčová hesla by je tak nemusel objevit.
[485] Stěžovatel byl policejním orgánem označen jako koncový uživatel IP adresy, ačkoli jejím prostřednictvím poskytoval připojení k síti zhruba dalšímu tisíci uživatelů.

zájem (prováděné šetření a postih trestné činnosti související se šířením dětské pornografie).[486]

Příklad z judikatury dokládá vyvažování legitimního cíle domovních a jiných prohlídek během postihu závažné počítačové trestné činnosti a ochrany soukromé sféry jednotlivce. Ačkoli ve většině případů zájem na postihu závažné trestné činnosti pravděpodobně převáží, podklady pro výkon pravomoci orgánů činných v trestním řízení musí být v podobných případech připraveny důkladněji. Konzultace s odborníky v oblasti ICT bude vždy na místě.

4.2.4.4. Domovní prohlídka nebo prohlídka jiných prostor, v nichž je vykonávána advokacie

Od roku 2006[487] obsahuje trestní řád podrobnou úpravu domovních prohlídek nebo prohlídek jiných prostor, v nichž advokát vykonává advokacii. Novela byla vedena snahou vyvážit přípustnou míru součinnosti České advokátní komory (dále též „ČAK“) při potírání trestné činnosti, ve vztahu k základním zárukám vůči klientům, neboť advokát je povinen v rámci řádného výkonu advokacie zachovávat podmínku mlčenlivosti.

Zvláštní ustanovení § 85b TŘ se uplatní při provedení domovní prohlídky nebo prohlídky jiných prostor, v nichž advokát vykonává advokacii, mohou-li se zároveň v těchto prostorách nacházet listiny (tj. i paměťové nosiče informací) obsahující skutečnosti, na které se vztahuje povinnost mlčenlivosti advokáta.

Zvláštní úprava chrání povinnost mlčenlivosti, která je nerozlučně spjata s výkonem profesní činnosti advokáta, nikoli jen s místem sídla advokáta. Přetrvávající diskuze a rozdílná soudní praxe vedly Nejvyšší soud k přijetí stanoviska vykládajícího pojem „jiné prostory, v nichž advokát vykonává advokacii“ (§ 85b TŘ).[488] Podle uvedeného stanoviska je zapotřebí vykládat pojem jako jakýkoli prostor, který souvisí s výkonem advokacie a kde se vyskytují informace o klientech, ať již v písemné,

[486] Usnesení Ústavního soudu, sp. zn. IV. ÚS 3225/09, ze dne 14. 12. 2011.
[487] Novela trestního řádu provedená zákonem č. 79/2006 Sb., kterým se mění zákon č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů, a další související zákony.
[488] Stanovisko Nejvyššího soudu, sp. zn. Tpjn 306/2014, ze dne 25. 6. 2015, uveřejněné pod číslem 35/2015 Sbírky soudních rozhodnutí a stanovisek.

elektronické či jiné podobě. Půjde nejenom o pobočku advokátní kanceláře nebo kancelář advokáta v sídle obchodní společnosti, ale i o místa určená k archivaci a ukládání advokátních spisů. Stanovisko uvádí jako jiný prostor i prostor kybernetický, a to výslovně ve smyslu elektronických úložišť dat, ať již v podobě advokátních webových stránek, datových úložišť advokáta nacházejících se mimo běžná místa výkonu jeho praxe, anebo úložišť spravovaných jinou osobou, avšak umožňujících dálkový přístup skrze Internet. Nejvyšší soud tedy výslovně označil cloud computing, externí servery a hostingové servery, v rámci advokacie využívané, za jiné prostory spadající pod ochranu § 85b TŘ.

Postoj Nejvyššího soudu lze jistě hodnotit kladně. Pakliže je listinou datový nosič, bylo by podivné, kdybychom vůči on-line variantám datového nosiče nechovali postoj totožný. Kybernetický prostor by vzhledem k nárůstu aktivit, které se v něm odehrávají, neměl být vyňat ze zvláštní úpravy chránící povinnost mlčenlivosti advokáta. Nesmíme však ignorovat zvláštnosti kybernetického prostředí, jež ovlivní především možnost „konzervace“ listin v případě odmítnutí součinnosti zástupce Komory na základě § 85b odst. 2 TŘ. Jak lze poté efektivně zabezpečit digitální data uložená kdesi v zahraničí na serverech služby cloud computing, aby se s jejich obsahem nemohl nikdo seznámit, manipulovat s nimi nebo je zničit? Potenciálně riziková se ukazuje situace, v níž by došlo k „překvapivému“ kybernetickému útoku vedoucímu ke ztrátě dotyčných digitálních dat ještě před tím, než příslušný soudce stačí ve věci rozhodnout.

Existence obsahu chráněného povinností mlčenlivosti advokáta by měla být alespoň z části opřena o důvodné skutečnosti. Toliko potenciální možnost výskytu listin s chráněným obsahem by neměla být považována za dostačující.[489]

Orgán činný v trestním řízení provádějící procesní úkon se smí s obsahem jmenovaných listin seznámit pouze za přítomnosti a se souhlasem zástupce Komory. Zástupce se účastní procesního úkonu po celou dobu a do jeho průběhu smí aktivně zasahovat.[490] Jestliže předsedou Komory ustanovený zástupce souhlas k seznámení se s obsahem listin odmítne udělit, zabezpečí se předmětné listiny, aby nedošlo k jejich

[489] Ostatně s ohledem na předmět výkonu advokacie by mohla být presumována u všech činných advokátů. Dále viz ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 317.

[490] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1155.

zpřístupnění jakékoli osobě, jakož i k jejich poškození či zničení. Zabezpečení listin je přítomen orgán činný v trestním řízení, zástupce Komory i advokát. Orgán činný v trestním řízení může následně požádat soudce o zpřístupnění listin, čímž by byla nahrazena absentující součinnost Komory.

Návrh na zpřístupnění listin je nutné podat do 15 dnů ode dne odmítnutí udělení souhlasu zástupcem Komory, jenž uvádí do protokolu své stanovisko. O nahrazení souhlasu rozhoduje ve veřejném zasedání soudce nejblíže nadřízeného soudu, u kterého působí předseda soudu nebo soudce, který byl oprávněn nařídit domovní prohlídku nebo prohlídku jiných prostor.[491] Jestliže soudce po zhodnocení obsahu listin shledá, že se na ně povinnost mlčenlivosti advokáta nevztahuje, návrhu vyhoví, popřípadě vyhoví jen v omezené části. Jinak návrh zamítne.

4.2.5. Odposlech a záznam telekomunikačního provozu a zjišťování údajů o telekomunikačním provozu

Odposlech a záznam telekomunikačního provozu upravuje trestní řád od roku 1990.[492] Při vyšetřování závažnější úmyslné trestné činnosti, která v případě počítačové kriminality není výjimkou, využívají orgány činné v trestním řízení běžně institut odposlechu a záznamu telekomunikačního provozu dle§ 88 TŘ i zjišťování údajů o uskutečněném telekomunikačním provozu dle § 88a TŘ.

Trestní řád zasazuje oba instituty mezi zajišťovací úkony hlavy čtvrté, ačkoli mají bližší vztah, co do podmínek užití, spíše k operativně pátracím prostředkům ve smyslu sledování osob a věcí nebo použití agenta.[493] Na rozdíl od sledování osob a věcí dle § 158d TŘ jsou však odposlech a záznam telekomunikačního provozu a zjišťování údajů o něm vázány na zákonem stanovené okruhy trestných činů.

Počáteční stručná úprava dle § 88 TŘ byla s rozvojem ICT značně novelizována. Roku 2001 bylo upraveno zjištění údajů o uskutečněném telekomunikačním provozu v § 88a TŘ. Reakcí na judikaturu Evropského soudu pro lidská práva byla významná

[491] § 85b odst. 3 TŘ.
[492] CEJP, Martin. *Vývoj organizovaného zločinu na území České republiky*. 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2010, str. 14.
[493] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 324.

novela č. 177/2008 Sb., která celkově úpravu zpřísnila zavedením povinnosti informovat po pravomocném skončení věci uživatele odposlouchávané stanice. Na druhé straně ovšem dochází konstantnímu rozšiřování okruhu trestných činů, u kterých dovoluje zákon zmíněné zajišťovací úkony využívat (např. novela č. 459/2011 Sb.).[494]

Smyslem úpravy je zajištění informace pro účely trestního řízení. Odposlech a záznam telekomunikačního provozu se týká obsahových dat – jedná se o klasický odposlech obsahu komunikace osob. Zjišťování údajů dle § 88a TŘ se týká metadat - údajů o telekomunikačním provozu, které *stricto sensu* o obsahu komunikace nic nevyzrazují, avšak informují nás o telekomunikačním provozu uskutečněném v minulosti. Oba zajišťovací instituty jsou zákonem dovoleným zásahem do ústavně zaručeného tajemství zpráv podávaných telefonem nebo jiným podobným zařízením dle čl. 13 Listiny, i do práva na ochranu soukromí a ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě dle čl. 10 odst. 2, odst. 3 Listiny.

Vedle trestního řádu se problematiky podstatnou měrou dotýká již zmiňovaný zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále též „ZEK“), který definuje některé v oblasti užívané pojmy a v rámci podmínek podnikání i součinnosti s orgány státu ukládá fyzickým a právnickým osobám mnohé povinností.

Telekomunikační provoz představuje komunikaci s využitím telefonu, mobilního telefonu či jiného telekomunikačního zařízení, včetně elektronické pošty.[495] Předmět telekomunikačního tajemství definuje § 88 a násl. ZEK tím, že osobám provozujícím veřejně dostupnou službu elektronických komunikací stanoví povinnosti k zabezpečení osobních, provozních a lokalizačních údajů[496] a důvěrnosti komunikace. Pro účely trestního řízení je klíčovým požadavek, aby osoby zajišťující veřejnou komunikační síť či poskytující veřejně dostupnou službu elektronických komunikací uchovávaly po dobu šesti měsíců provozní a lokalizační údaje týkající se zajišťování komunikačních sítí či

[494] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 324.
[495] Tamtéž, str. 325.
[496] Provozní a lokalizační údaje jsou podle § 97 odst. 4 ZEK *„zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.“* Součástí jsou i údaje o připojení k internetu a elektronické poště.

jimi poskytovaných služeb. Tato povinnost se ovšem nevztahuje na obsah zpráv.[497] Uchovávané provozní a lokalizační údaje musí být bezodkladně poskytnuty nejen orgánům činným v trestním řízení (při splnění podmínek trestního řádu), nýbrž například i pro účely řízení občanskoprávního za předpokladu, že s poskytnutím informací souhlasí oprávněný držitel uživatelské stanice.[498]

V důsledku zneužívání šifrovacích technologií se střetáváme se snahou důkladného sledování a kontroly on-line aktivit, což může vést i k neoprávněným zásahům do základních lidských práv a svobod sledovaných osob. Například § 75 odst. 1 ZEK ukládá osobě poskytující veřejně dostupnou telefonní službu prostřednictvím veřejné mobilní telefonní sítě povinnost znemožnit na stanovenou dobu, nejdéle však na dobu povoleného odposlechu, provozování šifrovacího zařízení na mobilním telefonu. Písemnou žádost podává se souhlasem soudce Policie České republiky.[499] Vyřazení šifrování z provozu se týká nejen majitelů šifrovacích telefonů, ale i tzv. chytrých telefonů, jež jsou vybaveny operačním systémem s možností instalace aplikací chránících obsah komunikace.[500] Efektivita obdobných státních opatření je pochybná. Lze se domnívat, že se pachatelé, nejčastěji z řad organizovaných skupin, uchýlí k technologiím nepodléhajícím státní kontrole tím, že použijí neoficiální, i na zakázku vyrobený šifrovací software. Kontrolní mechanismy rozšiřující pravomoc státních orgánů poté dopadnou především na běžné občany.

4.2.5.1. Odposlech a záznam telekomunikačního provozu

Odposlechem je *„záměrné a utajené a současné vnímání obsahu komunikace zprostředkované telekomunikačními zařízeními nebo sítěmi prostřednictvím k tomu určených zařízení.“*[501] Záznam zachytí poté obsah komunikace na paměťový nosič, umožňující jeho uchování a pozdější reprodukci. Integrální součástí odposlouchávané komunikace jsou i údaje vztahující se k účastnickým stanicím a údaje o času a délce

[497] § 97 odst. 3 ZEK.
[498] Usnesení Krajského soudu v Hradci Králové, sp. zn. 23Co 500/2007, ze dne 27. 10. 2007.
[499] § 75 odst. 2 ZEK.
[500] Nejčastěji WhatsApp, Viber, Skype apod. Více viz SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 220 a násl.
[501] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 325.

spojení.[502] Odposlech může posloužit vedle důkazního prostředku i jako preventivní prostředek, ale jen při zachování jeho zákonných předpokladů.[503] Podmínky odposlechu a záznamu telekomunikačního provozu (dále jen „odposlech a záznam“) uvádí § 88 TŘ. V příloze č. 4 předkládané práce je uvedeno přehledné schéma postupu policejního orgánu.

Odposlech a záznam lze nařídit pouze v zákonem stanovených případech. Předně jde o trestního řízení vedené o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let a dále je-li trestní řízení vedeno pro některý z taxativně stanovených trestných činů v § 88 odst. 1 TŘ, popřípadě pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Příkladem takové smlouvy může být právě Úmluva o počítačové kriminalitě vyžadující postih vyjmenovaných počítačových trestných činů.

Odposlech a záznam je rovněž omezen podmínkou subsidiarity. Není jej proto možné nařídit, jestliže lze účelu odposlechu a záznamu dosáhnout jinak, resp. bez značných obtíží. Podmínka subsidiarity představuje v trestní praxi provádění odposlechů a záznamů značné obtíže. V řadě případů se s ní orgány činné v trestním řízení nikoli vždy uspokojivě vypořádají.[504] Podle statistiky bývají uskutečněné počty odposlechů a záznamů v České republice velmi vysoké a čísla dále stoupají.[505] Další podmínkou nařízení odposlechu a záznamu je důvodný předpoklad, že jeho nařízením budou získány skutečnosti významné pro trestní řízení, tj. především skutečnosti potřebné pro účely dokazování dle § 89 odst. 1 TŘ.

Absolutní zákaz platí pro odposlech a záznam komunikace obviněného s obhájcem. Dle § 88 odst. 1 TŘ nesmí být zjištěné informace nijak použity. Doslovným výkladem nelze takto získané poznatky využít nejenom s ohledem na konkrétní trestní řízení, nýbrž jakkoli. Odposlech stanice obhájce s cílem odposlouchávání komunikace mezi ním a obviněným je nepřípustný a takový návrh musí soudce vždy zamítnout.

[502] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 326.
[503] MENDEL, Aleš. Vyšetřování počítačové kriminality. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 95.
[504] K problematice odposlechů též KUČERA, Pavel. Kdo není odposloucháván, jakoby nebyl. *Trestní právo*. 2014, 18(3), str. 3 - 4.
[505] Roku 2012 celkem 6 241 odposlechnutých linek, roku 2013 již 6 540, roku 2014 již 7 528. Podrobněji SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 220. Dále též Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2014 [online]. Dostupné z www.mvcr.cz [cit. 2016-04-09].

Odposlech a záznam stanice obviněného nařídit lze, avšak zjistí-li Police ČR, která odposlech a záznam provádí, že je zaznamenávána komunikace s obhájcem obviněného, je povinna záznam okamžitě zničit a sepsat o tom do trestního spisu protokol.[506]

Písemný a odůvodněný příkaz k odposlechu a záznamu nařizuje předseda senátu, v přípravném řízení soudce na návrh státního zástupce. Příkaz určuje odposlouchávanou stanici s telefonním číslem a osobou uživatele a dále trestný čin ve smyslu § 88 odst. 1 TŘ a konečně i dobu nepřekračující čtyř měsíců, během které bude odposlech a záznam prováděn. V odůvodnění příkazu se soudce nutně vyjádří ke konkrétním skutkovým okolnostem, jež vydání příkazu a dobu jeho trvání odůvodňují, včetně důvodů, proč nelze příkazem sledovaného účelu dosáhnout jinak, resp. proč by použití jiného způsobu bylo výrazně těžší.

Odposlech a záznam lze uskutečnit jako neodkladný či neopakovatelný úkon při splnění podmínek dle § 160 odst. 4 TŘ, nikdy však nesmí sloužit k operativně pátrací činnosti před samotným trestním řízením. Ústavní soud v tomto smyslu klade důraz na řádné odůvodnění příkazu: *„Pouhé trestní oznámení samo o sobě, není-li doloženo alespoň indiciemi, z nichž lze důvodné podezření dovozovat, nepostačuje k nařízení odposlechů, neboť totiž nepostačuje ani k zahájení řízení k objasnění a prověřování skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin podle § 158 trestního řádu. Může tedy být vydán jen v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost a musí být podložen relevantními indiciemi, z nichž lze dovodit důvodné podezření ze spáchání takového trestného činu.“*[507]

Trestní řád dovoluje odposlech a záznam nařídit na maximální dobu čtyř měsíců, což ovšem nezbavuje policejní orgán povinnosti dle § 88 odst. 3 TŘ průběžně po celou dobu trvání odposlechu a záznamu hodnotit, zda stále přetrvávají důvody jeho nařízení. Jestliže tyto důvody pominou, je policejní orgán povinen odposlech a záznam bezodkladně ukončit, a to bez ohledu na to, zda již uplynula doba, na kterou byl nařízen. Na druhé straně je s ohledem na § 88 odst. 4 TŘ možné dobu trvání příkazu opakovaně prodlužovat, vždy však nejdéle o čtyři měsíce. Po vyhodnocení dosavadního průběhu odposlechu a záznamu jej smí prodloužit soudce soudu vyššího stupně, v přípravném řízení soudce krajského soudu na návrh státního zástupce.

[506] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1206.
[507] Nález Ústavního soudu, sp. zn. II. ÚS 615/06, ze dne 23. 5. 2007, bod 16.

Možnost odposlechu a záznamu bez vydání příkazu je upravena v § 88 odst. 5 TŘ pro taxativně vymezené trestné činy. Podmíněna je souhlasem uživatele odposlouchávané stanice. V daném případě dochází k zásahu do ústavně chráněného tajemství zpráv a práva na ochranu soukromí u osob, které se s uživatelem odposlouchávané stanice spojí, pouze na základě předchozího souhlasu konkrétního uživatele s odposlechem jeho samotného. Jedná se o přístup, který s ohledem na intenzitu zásahu do soukromí neskýtá dostatečné záruky ochrany práv a svobod osob, jichž se procesní úkon dotýká.

Dle § 88 odst. 6 TŘ lze záznam telekomunikačního provozu získaný podle zákona v konkrétní trestní věci, v rámci které byl odposlech a záznam nařízen, užít jako důkaz. V jiné trestní věci je to možné, je-li v ní vedeno trestní stíhání pro trestný čin, pro který je možné podle § 88 odst. 1 TŘ nařídit odposlech a záznam, anebo jestliže uživatel odposlouchávané stanice souhlasí. Souhlas takového uživatele je vzhledem k restriktivním podmínkám § 88 odst. 5 TŘ i v tomto případě limitován uvedenými trestnými činy.[508] Požadavek, aby soudce vždy *ad hoc* posuzoval odůvodněnost nařízení odposlechu a záznamu vzhledem ke konkrétní věci, se tímto vytrácí, což nelze hodnotit jako pozitivní. Judikatura u využití odposlechu jako důkazu v jiné trestní věci považuje za nerozhodné, zda jde o odposlech a záznam telekomunikačního provozu v trestním řízení konaném v České republice nebo v cizině. Uvedený postoj dopadne především na případy mezinárodní justiční spolupráce při postihu organizovaného zločinu. *„V případě právního styku s cizinou v trestní věci, ve které by jinak byly splněny formální vnitrostátní předpoklady pro nařízení odposlechu a záznamu telekomunikačního provozu, není vyloučeno použít v České republice jako důkazní prostředek uvedený v § 88 trestního řádu záznam telekomunikačního provozu opatřený v cizině v jiné trestní věci.“*[509]

Orgány činné v trestním řízení, u nichž byla věc pravomocně skončena, jsou povinny dle § 88 odst. 8 TŘ informovat uživatele odposlouchávané stanice o odposlechu a záznamu, a poučit jej o právu podat ve lhůtě šesti měsíců od doručení informace návrh Nejvyššímu soudu na přezkum zákonnosti konkrétního příkazu. Pokud by poskytnutím informace mohl být zmařen účel trestního řízení, uživatel

[508] ŠÁMAL, Pavel. *Trestní řád: komentář. II. svazek, § 157 - § 314s.* 7., dopl. a přeprac. vyd. V Praze: C.H. Beck, 2013, str. 1213.
[509] Usnesení Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.

odposlouchávané stanice za podmínek § 88 odst. 9 TŘ informován není, což se týká zejména organizovaného zločinu.

Nejsou-li odposlechem a záznamem zjištěny skutečnosti významné pro trestní řízení, jsou na základě § 88 odst. 7 TŘ veškeré záznamy bezodkladně zničeny po třech letech od pravomocného skončení věci. Přestože není řešen vztah k možnosti uplatnění důkazů v jiné trestní věci podle § 88 odst. 6 TŘ, lze se domnívat, že záznamy by měly být zničeny bez ohledu na takovou možnost, neboť jedinou zmíněnou výjimkou je podání mimořádného opravného prostředku ve lhůtě tří let, kdy by zničení záznamů o odposlechu odporovalo právu na spravedlivý proces, neboť by obhajoba neměla možnost využít uskutečněné odposlechy ve svůj prospěch.[510]

4.2.5.2. Zjišťování údajů o uskutečněném telekomunikačním provozu

Provozní a lokalizační údaje, tedy metadata, bývají prvními údaji, které mají orgány činné v trestním řízení během vyšetřování k dispozici. Metadata jsou využívána hojně i při vyšetřování počítačové kriminality. Pomocí provozních a lokalizačních údajů například lze lokalizovat počítačový systém, kterým se pachatel připojí k síti. Existuje ovšem řada způsobů, jak IP adresu zařízení skrýt a učinit tak zjištěné údaje bezcennými.[511] Orgány činné v trestním řízení jak v České republice, tak i v jiných členských státech EU, využívají přístupu k údajům o uskutečněném telekomunikačním provozu vskutku hojně,[512] což vzbuzuje určité pochyby o uplatňování principu subsidiarity, i obavy z excesivního výkonu pravomoci státních orgánů.

Trestní řád řeší postup pro zjišťování údajů o uskutečněném telekomunikačním provozu v § 88a TŘ. Právní úpravu zavedla novela č. 265/2001 Sb. v reakci na judikaturu Ústavního soudu vztahující se k řadě ústavních stížností domáhajících se ochrany soukromí zpráv podávaných telefonem.[513] Telekomunikační společnosti zprostředkovávaly policejním orgánům údaje o telekomunikačním provozu jen na

[510] Usnesení Nejvyššího soudu ze dne 13. 4. 2007, sp. zn. 11 Tz 129/2006.
[511] Srov. šifrování, peer-to-peer sítě, proxy servery aj.
[512] POŠÍKOVÁ, Lenka. Získání telekomunikačních dat jako nástroj v boji s internetovou kriminalitou. *Acta Universitatis Carolinae. Iuridica*. 2013, 2012(4), str. 42- 49.
[513] Nález Ústavního soudu, sp. zn. II. ÚS 502/2000, ze dne 22. 1. 2001.

základě obecného dožádání a bez souhlasu uživatele, čímž docházelo k zásahům do ústavně zaručených základních práv a svobod.[514]

Ústavní soud později ovlivnil i podmínky uchovávání provozních a lokalizačních údajů. Argumentujíc rozhodovací praxí Evropského soudu pro lidská práva, odmítl rozsah a dobu uchovávaných provozních a lokalizačních údajů jakožto protiústavní a ke dni 30. září 2012 zrušil nálezem pléna § 97 odst. 3 a 4 ZEK.[515] V té souvislosti zrušil Ústavní soud téhož dne i tehdejší verzi § 88a TŘ, který ve srovnání se zákonnými podmínkami odposlechu a záznamu přistupoval k provozním a lokalizačním údajům příliš benevolentně a neskýtal tak dostatečnou ochranu základním lidským právům a svobodám.[516]

Následná úprava zpřísnila podmínky přístupu k provozním a lokalizačním údajům. Toliko potřeba objasnit skutečnosti důležité pro trestní řízení již k vydání příkazu dle § 88a TŘ nepostačuje. Zjišťování údajů o uskutečněném telekomunikačním provozu je omezeno vztahem k určeným skupinám trestných činů, obdobně jako je tomu u odposlechu a záznamu. Přesto je okruh daných trestných činů stále poměrně široký, což vzbuzuje pochybnosti o skutečném záměru zákonodárce využívání procesního úkonu omezit a upravit podmínky v souladu s názorem Ústavního soudu. Dle Ústavního soudu musí zásah do základního práva obstát v testu proporcionality. Omezení práva na informační sebeurčení musí *„sledovat ústavně aprobovaný účel, jímž je ochrana jiného základního práva nebo veřejného statku, přičemž posouzení vzájemné kolize těchto hodnot musí dbát imperativu minimalizace zásahů do základních práv a svobod, berouc přitom zřetel na jejich podstatu a smysl.“*[517]

Důsledkem novelizace § 97 odst. 3 ZEK nemusí již poskytovatelé služeb veřejné komunikační sítě a veřejně dostupné služby elektronických komunikací uchovávat výše zmíněné údaje, s výjimkou uchování provozních a lokalizačních údajů po dobu šesti měsíců. ZEK nicméně obsahuje vlastní definici služeb elektronických komunikací v § 2 písm. n), podle níž se část poskytovatelů služeb za poskytovatele služeb elektronických komunikací ve smyslu ZEK nepovažuje. Na ně se proto povinnost uchovávat data podle

[514] Blížeji POŠÍKOVÁ, Lenka. Získání telekomunikačních dat jako nástroj v boji s internetovou kriminalitou. *Acta Universitatis Carolinae. Iuridica*. 2013, 2012(4), str. 40.
[515] Obsahem ustanovení byla povinnost uchovávat po dobu 6 až 12 měsíců provozní a lokalizační údaje o veškeré telefonní, faxové, e-mailové a SMS komunikaci, o návštěvách webu a využívání vybraných internetových služeb. Nález Ústavního soudu, sp. zn. Pl. ÚS 24/10, ze dne 22. 3. 2011.
[516] Nález Ústavního soudu, sp. zn. Pl. ÚS 24/11, ze dne 20. 12. 2011.
[517] Nález Ústavního soudu, sp. zn. Pl. ÚS 24/11, ze dne 20. 12. 2011, bod 19.

§ 97 odst. 3 ZEK nevztahuje. Jde o poskytovatele služeb, kteří *„nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací,“* stejně jako poskytují-li *„služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.“*

Poněkud chaotická koncepce je důsledkem oddělení právní úpravy přenosu služeb poskytovaných prostřednictvím sítí elektronických komunikací od jejich obsahu. Právě vyloučení některých ISP z povinnosti uchovávat provozní a lokalizační údaje negativně ovlivňuje i postih počítačové kriminality. Na druhou stranu nelze říci, že by existence povinnosti všech ISP uchovávat provozní a lokalizační údaje byla spásná. Pravděpodobně by opět podstatnou měrou dopadla na běžné uživatele internetových služeb, nikoli na pachatele počítačové kriminality, kteří zpravidla využívají možností skrýt svou IP adresu nebo k přístupu do sítě zneužívají cizí počítač.

Předpokladem zjištění údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství nebo na které se vztahuje ochrana osobních a zprostředkovacích dat, je vedení trestního řízení pro úmyslný trestný čin uvedený v § 88a TŘ. Půjde o trestné činy, na něž zákon stanoví trest odnětí svobody s horní hranicí trestní sazby minimálně tří let, o skupinu taxativně vyjmenovaných trestných činů, a o trestné činy, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva. Výčet trestných činů je vlivem první kategorie vskutku široký, čímž se zákonné omezení aplikace institutu nezdá nijak limitující. Stejně jako u odposlechu a záznamu se zde uplatní princip subsidiarity, který by měl do určité míry korigovat široký okruh trestných činů. V jaké podobě bude princip subsidiarity uplatněn, však záleží na úvaze soudce rozhodujícího o konkrétním příkazu.

Příkaz k poskytnutí údajů o telekomunikačním provozu vydá předseda senátu, v přípravném řízení soudce na návrh státního zástupce, a označí v něm orgán činný v trestním řízení, jemuž mají být údaje vydána. S ohledem na § 88a odst. 4 TŘ lze údaje poskytnout i bez příkazu, avšak se souhlasem uživatele telekomunikačního zařízení, k němuž se údaje vztahují. V případě více uživatelů je třeba souhlasu každého z nich,

kterého se poskytnutí údajů týká.[518] Pro informační povinnost po pravomocném skončení věci platí stejné podmínky jako v případě odposlechu a záznamu.

Problematiku zjišťování údajů o uskutečněném telekomunikačním provozu dle § 88a TŘ ovlivnilo i rozhodnutí Soudního dvora EU,[519] které zrušilo směrnici Evropského parlamentu a Rady č. 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (dále též „směrnice o data retention"). Soudní dvůr EU považuje provozní a lokalizační údaje za údaje způsobilé předat detailní informace o životních návycích a aktivitách uživatelů, o místech jejich pohybu, o zdravotním stavu a sociálních kontaktech. Směrnice o data retention požadovala po členských státech EU plošné uchovávání provozních a lokalizačních údajů minimálně po šest měsíců, ačkoli jednotliví uživatelé ani nemuseli figurovat v žádné trestní věci. Soudní dvůr EU dospěl k závěru, že provozní a lokalizační údaje mohou mít v řadě případů na ochranu soukromí jednotlivců význam obdobný jako údaje týkající se obsahu komunikace. Jejich plošné uchovávání po dobu požadovanou směrnicí o data retention proto není v souladu s čl. 8 Listiny základních práv a svobod EU.[520] Zásah do základních práv a svobod je nutno omezit na nezbytné minimum.[521]

Současná podoba § 97 odst. 3 ZEK ukládá osobám zajišťujícím veřejnou komunikační síť nebo poskytujícím veřejně dostupnou službu elektronických komunikací povinnost uchovávat provozní a lokalizační údaje po dobu šesti měsíců. Správné vyvažování požadavku objasnit a stíhat pachatele trestné činnosti, tj. v daném případě mít reálnou možnost dostat se k údajům o uskutečněném telekomunikačním provozu i zpětně, vůči principu proporcionality, který trvá na minimálním zásahu do ústavou chráněných práv osob, bude problematickým i nadále. Nad rámec lze uvést, že doba šesti měsíců mnohdy ani nestačí k tomu, aby byl konkrétní trestný čin odhalen, došlo k zahájení úkonů trestního řízení a k vydání příkazu dle § 88a TŘ. Ochranou soukromí uživatelů telekomunikačních služeb se pak nestane ono omezení doby

[518] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 331.
[519] Rozhodnutí Soudního dvora EU ve spojených věcech C-293/12 a C-594/12, ze dne 8. 4. 2014.
[520] Listina základních práv a svobod Evropské unie ze dne 26. října 2012. Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:12012P/TXT [cit. 2016-04-19].
[521] Rozhodnutí Soudního dvora EU ve spojených věcech C-293/12 a C-594/12, ze dne 8. 4. 2014, bod 56.

uchování provozních a lokalizačních údajů, nýbrž doba reakce ze strany orgánů činných v trestním řízení na trestnou činnost.

Regulaci zjišťování údajů o uskutečněném telekomunikačním provozu ovlivňují protichůdné společenské postoje – na jedné straně stojí zájem na efektivním postihu kriminality a zajištění bezpečnosti, na straně druhé ochrana práv a svobod jednotlivce. Se současnou změnou politického klimatu můžeme očekávat spíše příklon k zajištění bezpečnosti.[522]

4.2.5.3. Řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu k zjištění údajů o telekomunikačním provozu

Zajišťovací instituty odposlechu a záznamu telekomunikačního provozu i zjištění údajů o něm jsou citelným zákonným zásahem státu do ústavně zaručených práv a svobod jednotlivců. Z toho důvodu je vhodné, aby nařizované příkazy podléhaly přezkumu z hlediska zákonnosti vydání i provedení. Řízení o přezkumu obou zajišťovacích institutů (dále jen „řízení o přezkumu“) zavedla do trestního řádu výše uvedená novela č. 177/2008 Sb., kterou došlo i k uzákonění informační povinnosti orgánu činného v trestním řízení po pravomocném skončení věci.[523]

Řízení o přezkumu nelze zahájit z úřední povinnosti, ale jen na návrh oprávněné osoby, kterou je dle § 314l odst. 1 TŘ v souvislosti s § 88 odst. 8 TŘ uživatel odposlouchávaného telekomunikačního zařízení v případě přezkumu odposlechu a záznamu, který byl informován o nařízeném odposlechu a záznamu a poučen o možnosti podat ve lhůtě šesti měsíců ode dne doručení informace příslušný návrh Nejvyššímu soudu. V případě přezkumu příkazu k zjištění údajů o uskutečněném telekomunikačním provozu je oprávněnou osobou dle § 314l odst. 2 TŘ v souvislosti s § 88a odst. 2 TŘ rovněž uživatel telekomunikačního zařízení ve vztahu k zjišťovaným údajům, informovaný o nařízeném příkazu i o možnosti podat příslušný návrh na přezkum.

[522] Srov. i výše zmíněný vládní návrh novelizace zákona č. 289/2005 Sb., o Vojenském zpravodajství.
[523] Informační povinnost o příkazu ke zjištění údajů o telekomunikačním provozu dle § 88a TŘ byla uzákoněna až vlivem výše uvedeného nálezu Ústavního soudu sp. zn. Pl. ÚS 24/11.

S ohledem na informační povinnost orgánů činných v trestním řízení, která se uplatní po pravomocném skončení věci, lze i řízení o přezkumu vést toliko v pravomocně skončené věci, v níž byl konkrétní uživatel telekomunikačního zařízení i náležitě informován. Návrhy na přezkum zákonnosti podané před pravomocným skončením věci Nejvyšší soud odmítá podle § 265i odst. 1 písm. a) TŘ *per analogiam* jako nepřípustné.[524]

Zákonnost napadnutého příkazu projedná Nejvyšší soud v neveřejném zasedání. Předmětem přezkumu je toliko zákonnost vydání nebo provedení příslušného příkazu, nikoli dokazování v trestní věci. Shledá-li Nejvyšší soud, že vydání nebo provedení zmíněného příkazu bylo v rozporu se zákonem, vysloví v usnesení, že byl porušen zákon. V opačné situaci vysloví, že zákon porušen nebyl. Podobně jako u stížnosti pro porušení zákona vysloví tedy akademický výrok. Usnesení má deklaratorní charakter a podle své povahy může sloužit jako podklad mimořádného opravného prostředku.[525] Opravný prostředek proti rozhodnutí Nejvyššího soudu není přípustný.

Určitou formu kontroly odposlechu a záznamu dle § 88TŘ a § 88a TŘ, jakož i sledování osob a věcí prováděné v rámci operativně pátrací činnosti dle § 158d TŘ, provádí Poslanecká sněmovna Parlamentu České republiky, která za tím účelem zřizuje kontrolní orgán. Policejní prezídium České republiky předává kontrolnímu orgánu pololetně zprávu, jež podléhá ochraně podle ZBZ. Nad dodržováním ochrany informací z odposlechu a záznamu smí rovněž provádět kontrolu i Úřad na ochranu osobních údajů, jakožto orgán státní správy provádějící správní dozor nepodřízených subjektů nad dodržováním jejich zákonných povinností.

4.2.6. K problematice znaleckých posudků

Trestní řád upravuje problematiku podávání odborných vyjádření i znaleckých posudků v ustanovení § 105 TŘ. Postih počítačové trestné činnosti, jak je uvedeno výše, se vyznačuje řadou specifik. V průběhu celého trestního řízení vyvstává potřeba řešit právně i technicky složité a odborně náročné otázky. Vedení trestního řízení bez

[524] Usnesení Nejvyššího soudu, sp. zn. 4 Pzo 1/2010, ze dne 10. 14. 2010.
[525] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013, str. 888.

odborné pomoci expertů na ICT se neukazuje příliš efektivní. Soudní znalci i znalecké ústavy proto hrají při postihu počítačové kriminality významnou roli.

Postavení znalců upravuje zákon č. 36/1967 Sb., o znalcích a tlumočnících (dále též „ZZT“) a vyhláška ministerstva spravedlnosti č. 37/1967 Sb., k provedení zákona o znalcích a tlumočnících. Znaleckou činnost mohou vykonávat jen znalci zapsaní v seznamu znalců či znalecké ústavy. V nouzových situacích, resp. za podmínek předpokládaných v § 24 ZZT, může orgán veřejné moci ustanovit znalcem i osobu v seznamu nezapsanou, pokud má potřebné předpoklady pro podání znaleckého posudku.

V souvislosti s vyšetřováním počítačové kriminality přichází v úvahu přibrání znalce z oboru kybernetiky, odvětví výpočetní techniky, a s ohledem na zajištění širšího úhlu pohledu rovněž z oboru kriminalistiky, elektroniky, popřípadě i ekonomiky. Protože členění znaleckých odborností do uvedených kategorií je přes 40 let staré, bude vhodné orientovat se i podle dalších popsaných specializací a zaměření znalce, kterými může být užší odbornost v rámci problematiky software, ochrany dat, informačních systémů atd.[526]

V souvislosti se zadáváním znaleckých posudků při vyšetřování počítačové kriminality je pro orgán činný v trestním řízení často obtížné znalci správně formulovat otázky. Oblast chybně položených otázek z hlediska práva, zejména otázek kapciózních a sugestivních, pomíjím, neboť tyto se objevují i při zadávání znaleckých posudků mimo oblast počítačové kriminality. Mezi problematické aspekty zadávání znaleckých posudků patří fakt, že po znalcích je často požadováno zodpovězení otázek nezodpověditelných. Takové dotazy míří na autorství e-mailu či na ztotožnění osoby, která uskutečňuje určité elektronické transakce prostřednictvím konkrétního počítačového systému. Nelze objasnit ani konkrétní stav dotčeného počítače před delší dobou.[527]

Při zadávání otázek představuje obvykle problém právě nedostatečná znalost ICT ze strany orgánů činných v trestním řízení. Tu lze vnímat jako určitý (pochopitelný) deficit provázející postih počítačové kriminality od počátku až do konce. Bude proto vhodné se před vyhotovení opatření o přibrání znalce, kde jsou již konkrétní

[526] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 511.
[527] Smejkal uvádí pravděpodobně příklady z vlastní dlouholeté znalecké praxe. SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 515.

otázky položeny, informovat, zda je vzhledem k nauce ICT vůbec dotaz smysluplný. Uvedeným postupem si orgán činný v trestním řízení zachová možnost určit konečnou verzi otázky sám, přičemž se sníží i pravděpodobnost vzniku následné potřeby doplnění znaleckého posudku a tím i prodloužení trestního řízení.

5. MEZINÁRODNÍ SPOLUPRÁCE PŘI POSTIHU POČÍTAČOVÉ KRIMINALITY

Globální virtuální prostředí a počítačová trestná činnost s mezinárodním prvkem jsou spjaty. Nové způsoby automatizované trestné činnosti celosvětového dosahu, černý trh sítě Darknet,[528]existence botnetů i hrozba teroristických útoků jsou některé z nežádoucích jevů, které nutně přivádějí suverénní státy ke vzájemné diskuzi.

Mezinárodní společenství uznává globální charakter kybernetické kriminality. Organizace spojených národů varuje před jejím transnacionálním charakterem, umocněným globální dostupností služeb. Vyspělé státy se obávají šíření kyberteroristických útoků ze států méně rozvinutých, které se díky nedostatečné legislativě mohou stát podhoubím organizovaného zločinu a terorismu.

Zásadní charakter mezinárodní spolupráce vystihuje i Polčák, který uvádí, že *„mezinárodní spolupráci v zajištění faktické realizace právních pravidel nutno chápat nejen jako pomůcku, ale přímo jako podmínku zachování působnosti práva na internetu. Klíčem k úspěchu mezinárodní spolupráce v nastolení efektivní působnosti práva na internetu není ve svém důsledku nic menšího než potlačení státní suverenity a přijetí a spolehlivá ochrana cizí jurisdikce.“*[529]

Kapitola si klade za cíl pojednat o mezinárodní justiční spolupráci s důrazem na mezinárodní právní pomoc, tedy mezinárodní justiční spolupráci v užším slova smyslu, při vyšetřování počítačové kriminality. Po úvodu do problematiky mezinárodní spolupráce v oblasti trestního práva následuje pojednání o vybraných dokumentech mezinárodního a evropského práva, kde se text dotýká i klíčových organizací a institucí, jež svojí činností ovlivňují současný stav právní úpravy. Zvláštní pozornost je určena Radě Evropy a Úmluvě o počítačové kriminalitě a vybraným pramenům sekundární normotvorby práva Evropské unie. Při výběru jednotlivých dokumentů byl důraz kladen na prameny procesních institutů ovlivňujících právní rámec vyšetřování počítačové kriminality. Kapitola se věnuje rovněž české zákonné úpravě v oblasti mezinárodní

[528] Darknet je běžným uživatelům skrytá část internetových sítí, která využívá techniku „peer to peer“ spojení. V rámci skryté vrstvy sítě je možné obstarat si materiály dětské a jiné ilegální pornografie, drogy, běžně nepřístupná léčiva, zjednat si nájemnou vraždu, ale též dostat se k vědeckým a jiným autorským dílům bez ohledu na práva k nehmotným statkům. Podrobně viz http://cemolid.blogspot.cz/2015/04/darknet-internetove-podsveti.html. [cit. 2016-03-17].

[529] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 113.

justiční spolupráce v trestních věcech. Závěr pojednává o vybraných problematických situacích, kde se střetávají pravidla mezinárodního práva veřejného i základní principy trestního práva s požadavky praxe při postihu počítačové kriminality v mezinárodním prostředí. Řešení mohou nabídnout i metody mezinárodní spolupráce.

5.1. Mezinárodní justiční spolupráce v trestních věcech

5.1.1. Suverenita, trestní právo mezinárodní a vývoj mezinárodní spolupráce v trestních věcech

Vlivem globalizovaného světa a rozvoje mezinárodních vztahů vyvstává v rámci trestního stíhání potřeba spolupráce s orgány činnými v trestním řízení za hranicemi státu. Nauka o státní suverenitě, jejíž kořeny sahají do období středověku,[530] dala vzniknout teorii o suverénním státu, tj. státu s uvnitř i navenek samostatnou, od nikoho neodvislou panovací mocí, projevující se v neomezené způsobilosti k činům podle mezinárodního práva. Suverénní stát je plnoprávným subjektem práva mezinárodního, jehož státní moc značí jednak výsost nad územím státu, jednak výsost nad osobami, ale také autonomii v zákonodárství, soudnictví a veřejné správě. Ani při výkonu autonomní státní moci však státy nesmí zapomenout, že jsou členy obce větší, tj. mezinárodního společenství rovnoprávných subjektů – jednotlivých autonomních států. Státy se snaží vyhýbat kolizím s autonomií jiných států, ať již v rámci mezinárodního práva soukromého či veřejného. Autonomie států může být nejčastěji omezena smluvně uloženými závazky mezinárodního práva veřejného.[531]

Suverenitu lze dělit na vnitřní a vnější. Vnitřní suverenita představuje výlučnou nejvyšší moc státu na jeho území, jež vede k negaci jakýchkoli aktů či úkonů cizí státní moci bez souhlasu daného státu. Vnější suverenita spočívá v plné způsobilosti státu

[530] Pojem suverenita vznikl jako součást politické vědy. Jean Bodin dal pojmu v 16. století význam nový, ve smyslu absolutní a trvalé moci uvnitř státu, nejvyšší státní moci omezené toliko božími příkazy a přirozeným právem. Podrobněji KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 13.
[531] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 14.

zavazovat se vlastním právním jednáním ve sféře mezinárodního práva.[532] V souvislosti s rozvojem globalizovaného světa někteří autoři podotýkají, že v oblasti mezinárodních vztahů ztrácí pojem suverenita původní význam, neboť prohlubující se mezinárodní vztahy pomáhají řešit různé konflikty, ať již válečné nebo v oblasti boje s kriminalitou.[533] Některé dříve problematické aspekty postihu přeshraniční trestné činnosti lze řešit na bázi formální i neformální spolupráce. K uvedenému lze podotknout, že neformální spolupráce orgánů činných v trestním řízení může vzbuzovat otázky ohledně zákonnosti daného procesu a míry faktické ochrany základních lidských práv a svobod při výkonu pravomoci orgánů státu.

Vnitřní suverenita je úzce spjata s právem státu potrestat pachatele trestného činu. Trestání vychází dle Hobbese z veřejné moci, kdy moc trestat byla svěřena vladaři se souhlasem všech poddaných státu za účelem jejich ochrany.[534] Jurisdikce[535] jako součást státní moci je však omezena teritoriem státu. Proto jednotlivé státy postupně nalézaly cesty, jak se domoci ochrany vlastních zájmů i na cizím státním území, a současně dopustily v ještě přípustné míře legitimní aktivity orgánů cizího státu ve vlastním teritoriu nebo vůči svým občanům.

Trestní právo hmotné i procesní se zajímá o vztahy s mezinárodním prvkem. Mezinárodní prvek může spočívat buď jen v hmotněprávním vztahu (pachatelem je cizí státní občan, ke spáchání trestného činu došlo v cizině, objektem trestného činu je zájem cizího státu), nebo jen v procesněprávním vztahu (potřeba výslechu svědka v zahraničí), anebo v hmotněprávním i procesněprávním vztahu. Mezinárodní prvek může být i toliko normativní povahy, tj. původ vnitrostátní normy a její aplikace je plněním mezinárodněprávního závazku státu. Taková norma mezinárodního práva je určena k řešení vztahu obsahujícího mezinárodní prvek a bývá v souladu se zájmy mezinárodního společenství.[536] Normy trestního práva upravující vztahy s mezinárodním prvkem jsou předmětem oboru trestního práva mezinárodního.

---

[532] MADAR, Zdeněk. *Slovník českého práva*. 3. rozš. a podstatně přeprac. vyd. Praha: Linde, 2002, str. 1124-1126.
[533] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 15.
[534] Podrobněji viz HOBBES, Thomas; CHOTAŠ, Jiří; MASOPUST, Zdeněk; BARABAS, Marina, ed. *Leviathan, aneb, Látka, forma a moc státu církevního a politického*. Překlad Karel Berka. Praha: OIKOYMENH, 2009.
[535] K výkladu pojmu jurisdikce srovnej kapitolu 2.3.1.
[536] KAMLACH, Milan; REPÍK, Bohumil. *Mezinárodní spolupráce v trestním a občanskoprávním řízení*. Praha: Panorama, 1990, str. 9.

Oproti tomu mezinárodní trestní právo, relativně nový obor mezinárodního práva veřejného, definuje zločiny mezinárodního práva, ukládá povinnosti přímo jednotlivcům a jejich porušení stíhá skrze mezinárodněprávní mechanismy. Na rozdíl od mezinárodního trestního práva,[537] jehož jádrem jsou statuty a rozsudky mezinárodních soudních tribunálů v Norimberku, Tokiu či *ad hoc* ustanovených trestních tribunálů pro bývalou Jugoslávii a pro Rwandu, i úprava v Římském statutu Mezinárodního trestního soudu v Haagu,[538] předmětem trestního práva mezinárodního jsou především otázky mezinárodní spolupráce při postihu trestných činů dle vnitrostátního trestního práva.

Historicky nejstarší formou právní pomoci je extradice, kterou znal již starověk. Vedle ní se postupně vyvinula a během 19. století oddělila právní pomoc v užším slova smyslu. V druhé polovině 20. století se objevuje převzetí trestního stíhání a dále přiznání účinku i výkon cizozemských trestních rozhodnutí, jako samostatné kooperační formy právní pomoci.[539]

Jedinými formami právní pomoci v trestních věcech byly prakticky až do období po skončení druhé světové války pouze extradice a právní pomoc v užším slova smyslu, tedy pomoc prováděním jednotlivých procesních úkonů pro potřeby trestního řízení vedeného v cizím státě. Orgány činné v trestním řízení státu, který poskytoval pomoc, tak činily svým jménem, avšak vlastní trestní jurisdikci nevykonávaly. Pomoc symbolizuje přispění při uskutečnění cizí úlohy, nikoli spolupráci při plnění společného úkolu. Uvedené formy právní pomoci lze proto nazvat jako sekundární či akcesorní, na rozdíl od rozvinutějších forem spolupráce, kterými je převzetí trestního stíhání a výkon cizozemských rozhodnutí, tedy kooperační právní pomoc, kdy je cizímu státu svěřena část trestního řízení.[540]

Kooperační formy spolupráce států v trestních věcech souvisí se změnami kriminálně politických koncepcí. Kooperující státy mění postoj k výkonu vlastní trestní jurisdikce a k problematice státní suverenity. Bezpodmínečně již netrvají na uskutečnění *ius puniendi* od zahájení trestního řízení až po samotné potrestání pachatele trestného činu. Smyslem spolupráce se postupně stává nalezení co nejvhodnější jurisdikce, která

[537] JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 5. vyd. Praha: Leges, 2016, str. 43.
[538] Římský statut Mezinárodního trestního soudu ze dne 17. července 1998. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 84/2009 Sb. m. s.
[539] KAMLACH, Milan; REPÍK, Bohumil. *Mezinárodní spolupráce v trestním a občanskoprávním řízení*. Praha: Panorama, 1990, str. 49.
[540] Tamtéž, str. 46 – 47.

by mohla nejlépe vést k naplnění cíle trestního práva.[541] Uvedené změny v trestněprávní politice mnohých států jsou logickým vyústěním postupné globalizace světa, jež přináší propojení kriminálních aktivit na území vícero států a vede k vzestupnému výskytu mezinárodního prvku v trestních věcech.

5.1.2. Podstata mezinárodní justiční spolupráce v trestních věcech

Smysl a podstatu mezinárodní justiční spolupráce v trestním řízení lze vystihnout neschopností státu prosadit v určitých případech jím určené právo, tj. státem stanovenou trestněprávní normu, dojde-li k naplnění všech znaků skutkové podstaty trestného činu. Donucovací státní moc, bez níž není možné realizovat trestní jurisdikci, je omezena suverenitou ostatních států. Hmotné trestní právo vnitrostátní, které obvykle upravuje vlastní místní působnost velmi široce, vytváří jen možnost trestního postihu pachatele. Realizaci tohoto postihu v případech s mezinárodním prvkem umožňují procesní normy trestního práva mezinárodního, jejichž předmětem je mezinárodní justiční spolupráce.

Mezinárodní justiční spolupráce je upravena především mnohostrannými mezinárodními smlouvami, vůči kterým je vnitrostátní právo v subsidiárním postavení.[542] Mezinárodní justiční spolupráce v oblasti trestního práva spočívá v právní regulaci vzájemného styku justičních orgánů různých států. Upravuje pravidla komunikace mezi orgány činnými v trestním řízení, ke které dojde v důsledku žádosti o justiční pomoc dožadujícího státu (orgánu činného v trestním řízení dožadujícího státu) vůči státu dožádanému. Vzájemnou komunikaci mezi dožádaným a dožadujícím se státem zpravidla zajišťuje v rámci každého státu k tomu určený orgán.

Základní podobou mezinárodního styku v rámci justiční spolupráce je diplomatický styk, k němuž dochází skrze diplomatické zastoupení dožadujícího se státu na ministerstvu zahraničních věcí státu dožádaného, anebo vzájemným stykem ministerstev zahraničních věcí obou států. Je-li vzájemná komunikace zprostředkována

[541] KAMLACH, Milan; REPÍK, Bohumil. *Mezinárodní spolupráce v trestním a občanskoprávním řízení*. Praha: Panorama, 1990, str. 47.
[542] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 44.

konzulem dožadujícího se státu, jedná se o styk konzulární, který však v trestním řízení není příliš běžný. Dochází-li ke spolupráci justičních orgánů obou států prostřednictvím jejich ministerstev spravedlnosti, jde o meziministerský styk. O přímý styk půjde při bezprostředním styku justičních orgánů obou států.[543]

Ministerstvo zahraničních věcí dnes v České republice zprostředkovává mezinárodní justiční spolupráci v trestních věcech vůči státům, s nimiž není na dostatečné úrovni spolupráce regulována. V České republice obvykle dochází k mezinárodní justiční spolupráci v trestním řízení v jeho přípravné fázi, a to skrze mezinárodní odbor Nejvyššího státního zastupitelství. V soudní fázi trestního řízení je využíváno Ministerstvo spravedlnosti České republiky, a to nejen jako orgán zajišťující styk v rámci mezinárodní justiční spolupráce, nýbrž i jako orgán konzultační a poradní i tam, kde lze při mezinárodní spolupráci využít přímý styk mezi soudy.

V řadě případů však přímý styk mezi soudy dožadujícího se a dožádaného státu v rámci trestního řízení v jeho soudní fázi není příliš efektivní, neboť dožadující se soud nemá na rozdíl od ministerstva spravedlnosti k dispozici prostředky, jimiž např. zjistí kontaktní orgán, bude apelovat, aby dožádání bylo vůbec vyhověno, popřípadě aby byl požadovaný úkon právní pomoci proveden v rozumném časovém rámci. Příčinou neefektivní spolupráce skrze přímý styk soudů může být skutečnost, že některé soudy vnímají požadavek dožadujícího se zahraničního soudu jako okrajovou část vlastní pracovní náplně, na níž specializovány nejsou, okolnosti požadovaného úkonu neznají a mezinárodní justiční spolupráci tak vnímají jako zdržení od vlastní pracovní náplně. Procesní normy upravující činnost soudnictví jednotlivých států nemusí též pamatovat na stanovení maximální lhůty, byť pořádkové, k vyřízení požadovaného úkonu v rámci mezinárodní justiční spolupráce, v důsledku čehož bývá žádostem vyhověno až po opakovaných apelech. Soudy proto od dožádání justičních orgánů některých zemí raději upustí, neboť by výsledek mezinárodní justiční spolupráce neodůvodnil přílišné prodloužení délky trestního stíhání.

Existují i případy, kdy dojde na základě přímého styku mezi orgány činnými v trestním řízení k poskytnutí mezinárodní justiční pomoci na základě mezinárodní smlouvy *extra legem*, neboť právní pomoc nebude poskytnuta právě smlouvou předpokládaným způsobem. V takovém případě je nutno zvážit, zda bude provedený

[543] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 44-45.

úkon procesně použitelný v trestním řízení vedeném v dožadujícím se státě. K platnosti úkonů provedených v cizině a postupu *extra legem* se vyjádřil Nejvyšší soud, který uznal možnost kompetentního orgánu cizího státu umožnit na svém území českému orgánu činnému v trestním řízení provedení úkonu podle českého trestního řádu, neboť se tak stalo s odvoláním na příslušné mezinárodní smlouvy upravující právní pomoc ve věcech trestních a práva obviněného nebyla nikterak zkrácena.[544]

5.1.3. Mezinárodní justiční spolupráce v užším slova smyslu

V užším slova smyslu hovoříme o mezinárodní justiční spolupráci v trestních věcech, jsou-li prováděny procesní úkony pro potřeby trestního řízení v cizím státě. Jde o mezinárodní právní pomoc, jež je poskytována zpravidla na základě mezinárodní smlouvy, a pokud takové smlouvy není, pak na základě principu vzájemnosti (reciprocity), který bývá upraven ve vnitrostátním právu.[545] V českém trestním právu mezinárodním upravuje princip vzájemnosti při absenci mezinárodní smlouvy § 4 zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních (dále též „ZMJS“). K provedení dožádaného úkonu, který nesmí být v rozporu s chráněnými zájmy České republiky, musí být justiční orgán oprávněn. Chráněnými zájmy se ve smyslu § 5 ZMJS rozumí ústavní pořádek, zásady našeho právního řádu, na nichž je zapotřebí bezvýhradně trvat a (do určité míry zbytková kategorie) jiné významné státní zájmy.

Zatímco vnitrostátní úprava mezinárodní právní pomoci je úpravou unilaterální, nezakládající práva a povinnosti mezi státy, smluvní úprava je vnitrostátní nadřazena, zavazuje smluvní strany vůči sobě navzájem a umožňuje upravit určitá pravidla od vnitrostátní právní úpravy odchylně. Mezi stěžejní mnohostranné mezinárodní smlouvy o mezinárodní justiční pomoci v trestních věcech patří Evropská úmluva o vzájemné pomoci ve věcech trestních, přijatá v Štrasburku dne 20. dubna 1959.[546] Úpravu doplnil

[544] Rozsudek Nejvyššího soudu, sp. zn. 4 Tz 106/2002, ze dne 26. 3. 2003.
[545] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 81.
[546] Úmluva Rady Evropy č. 30 ze dne 20. dubna 1959, Evropská úmluva o vzájemné pomoci ve věcech trestních. Federálním ministerstvem zahraničních věcí ČSFR vyhlášena pod č. 550/1992 Sb.

Dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních,[547] který znemožnil odmítnout právní pomoci toliko z důvodu, že se žádost vztahuje na trestný čin, který dožádaná strana považuje za trestný čin fiskální. Druhý dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních[548] reagoval na společenské změny v důsledku technologického rozvoje a umožnil flexibilnější právní pomoc v trestním stíhání přeshraniční trestné činnosti. Jde zejména o možnost zasílání žádostí o právní pomoc skrze elektronické a jiné telekomunikační prostředky, ovšem za podmínky, že dožadující strana bude připravena předložit na žádost písemný záznam o odeslání žádosti spolu s originálem žádosti.[549]

Zmínit je vhodné i Úmluvu o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie[550] a Protokol k Úmluvě o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie.[551] Jejich účelem je doplnit úpravu z výše uvedených mezinárodních smluv Rady Evropy týkajících se mezinárodní právní pomoci a usnadnit jejich uplatňování mezi členskými státy EU. Harmonizaci a unifikaci trestněprávních předpisů týkajících se mezinárodní právní pomoci mezi členskými státy EU rozebírá kapitola níže.

Justiční pomoc bývá nejčastěji poskytována v přípravném stádiu trestního řízení, ačkoli výjimkou není ani její užití v pozdější fázi před soudem. Určité problémy působí v různých státech rozdílné vymezení pravomocí orgánů činných v trestním řízení pro jednotlivé fáze trestního řízení - například země užívající tzv. common law systém[552] neznají tradiční úpravu přípravného řízení typickou pro kontinentální právní model.

[547] Úmluva Rady Evropy č. 99 ze dne 17. března 1978, Dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 31/1997 Sb.
[548] Úmluva Rady Evropy č. 182 ze dne 8. listopadu 2001, Druhý dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 48/2006 Sb. m. s.
[549] Česká republika dle čl. 15 odst. 9 ve znění čl. 4 odst. 9 Druhého dodatkového protokolu k Evropské úmluvě o vzájemné pomoci ve věcech trestních, požaduje vždy následně doručit originál žádosti v listinné podobě.
[550] Úmluva ze dne 29. května 2000 o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 55/2006 Sb. m. s.
[551] Protokol ze dne 16. října 2001 k Úmluvě o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 56/2006 Sb. m. s.
[552] Systém anglosaského práva spočívá oproti právním kodexům typickým pro kontinentální systém především v precedentních soudních rozhodnutí, jež vytváří s právními předpisy komplexní právní systém. Mezi zeměmi systému common law lze uvést např. Velkou Británii (s výjimkou Skotska), USA, Kanadu či Austrálii.

5.2. Východiska mezinárodní spolupráce v oblasti trestního práva

Mezinárodní spolupráce je pro vyšetřování počítačové kriminality klíčovou, neboť v důsledku výše rozvedeného všeobecně uznávaného principu suverenity států nemohou orgány státu vést na území jiného státu vyšetřování bez souhlasu místních autorit. Včasná a efektivní spolupráce mezi státy je stěžejní především při vyšetřování kybernetické kriminality, neomezené hranicemi jednotlivých států, kde bývají důkazy usvědčující pachatele v krátkém časovém rámci automaticky ničeny.[553]

Klasické formalizované procedury mezinárodní spolupráce na ministerské úrovni bývají pro efektivní postih počítačové kriminality příliš časově náročné. Jejich zdlouhavý průběh prakticky znemožňuje dosáhnout účelu trestního řízení, tedy náležitě zjistit trestný čin a potrestat jeho pachatele. Vhodnějšími se jeví užší a méně formalizované formy spolupráce, které upravují některé mezinárodněprávní instrumenty. Zda dojde k jejich přijetí, ovlivní řada faktorů. Nejdůležitější z nich rozebírá následující text.

5.2.1. Princip oboustranné trestnosti a princip speciality

Princip oboustranné trestnosti lze vysvětlit jako požadavek, aby předmětný čin byl kriminalizován jak ve státě dožadujícím se určité formy mezinárodní spolupráce, tak ve státě dožádaném. Uplatnění nachází zejména v mezinárodních smlouvách zaměřených na extradici, kdy při vydávání státních residentů k trestnímu stíhání v jiném státě extradice zpravidla možná nebude bez splnění podmínky oboustranné trestnosti činu.[554] Ačkoli oboustranná trestnost není pro poskytnutí justiční pomoci bezpodmínečně nutná, objevují se i názory, podle kterých se oboustranná trestnost

[553] Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice: Salvador, Brazil, 12 - 19 April 2010* [online]. Dostupné z https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf [cit. 2016-03-17]. Překlad autorka.

[554] BRENNER, Susan W. a Bert-Jaap KOOPS. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law* [online]. 2004, 4(1), str. 7. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507 [cit. 2016-03-10]. Překlad autorka.

vyžaduje i když není výslovně ve smlouvě či vnitrostátní normě stanovena, protože úkon justiční pomoci nesmí odporovat veřejnému pořádku dožádaného státu.[555]

Také mezinárodní smlouvy, které obvykle podmínku oboustranné trestnosti vyžadují, se stávají základem postihu počítačové trestné činnosti s mezinárodním prvkem. Princip oboustranné trestnosti však naráží na odlišné kulturní vzorce a tradice jednotlivých států, projevující se v kriminalizaci do určité míry odlišného chování. Citelné rozdíly lze spatřit v některých aspektech pojetí lidských práv a svobod, například svobody projevu. Rozdílný přístup ovlivňuje zejména postih projevů nesnášenlivosti a jiné rasisticky a xenofobně motivované trestné činnosti spáchané prostřednictvím globální počítačové sítě. Takové trestněprávně relevantní projevy lze na Internetu publikovat anonymně skrze zahraniční servery a vyhnout se postihu ve vlastním státě. Všeobecně známým faktem je například odmítavý postoj USA k žádostem o právní pomoc v oblasti potírání rasistických a jiných nenávistných veřejně přístupných webových stránek v českém jazyce, které bývají z toho důvodu často umisťovány na servery ISP situované právě v USA, neboť jsou chráněny tamní široce pojatou doktrínou svobody projevu.[556] Odmítavý postoj vůči žádostem o právní pomoc z důvodu absence oboustranné trestnosti se naopak nevyskytuje tam, kde státy sdílí postoj vůči kriminalizaci určitého druhu trestné činnosti. Společný postoj takto zaujímají státy k postihu dětské pornografie či šíření terorismu, včetně náboru členů a šíření potenciálně nebezpečných návodů.[557] Cestou jednotlivých smluvních výhrad se některé státy však opět vyjadřují odlišně třeba k definici dítěte či k požadavku kriminalizace virtuální dětské pornografie.[558]

Výchozím principem pro poskytnutí mezinárodní justiční pomoci se stal rovněž princip speciality, na základě něhož lze poskytnutou pomoc využít toliko k účelu, k němuž byla vyžádána. Princip speciality se vztahuje k činu, pro který se vede řízení. Na základě principu speciality nelze informace či důkazy získané v rámci mezinárodní justiční pomoci využít bez souhlasu cizozemského orgánu k jiným účelům, než pro

[555] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 83.
[556] HERCZEG, Jiří. *Trestné činy z nenávisti: právní monografie*. 1. vyd. Praha: ASPI, 2008, str. 90 – 91.
[557] Mezinárodní spolupráce v boji proti informační kriminalitě. *Ministerstvo vnitra České republiky: Výsledky projektů v rámci bezpečnostního výzkumu* [online]. Praha, 2009, str. 2. Dostupné z http://www.mvcr.cz/clanek/vysledky-projektu.aspx [cit. 2016-03-17].
[558] GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. *Acta Universitatis Carolinae. Iuridica*. 2008, 2008(4), str. 22.

které byly získány. Zásadu speciality v českém trestním právu mezinárodním vyjadřuje § 7 ZMJS, který ji však omezuje na situace, kdy je požadována mezinárodní smlouvou, popřípadě byly-li důkazy a informace získány za podmínky dodržení zásady speciality. V současnosti spíše převládá názor, že zásadu speciality není zapotřebí u mezinárodní justiční spolupráce respektovat.[559]

Zásada speciality však zůstává stěžejním principem v úpravě extradičního řízení. Pakliže má být například obviněný, který byl vydán nebo předán do České republiky dožádaným státem, stíhán pro jiný skutek, než pro který byl vydán (předán) a který spáchal před svým vydáním (předáním), je v takovém případě s ohledem na zásadu speciality k jeho trestnímu stíhání zapotřebí souhlasu příslušného orgánu cizího (dožádaného) státu.[560]

5.2.2. Teritoriální ochrana některých práv

S podmínkou oboustranné trestnosti souvisí i konflikty vyplývající z rozporu mezi teritoriální ochranou vybraných práv a globální fakticitou internetových sítí. Mezinárodněprávní ochrana některých práv může být poskytována pouze na vybraném území. Teritorium států, které přikládají daným právům požadovaný význam a poskytují jim trestněprávní ochranu, se stane stěžejním pro faktickou vymahatelnost trestněprávní ochrany i ve virtuálním prostoru.

Typickým příkladem je ochrana autorského práva a práv souvisejících s právem autorským. Část ilegálního obsahu je šířena z oblastí, proti nimž neexistují účinné mechanismy zásahu k ochraně autorských práv. Důvodem jsou především chybějící mezinárodní instrumenty či nízká úroveň právní kultury daného státu. Efektivní ochrana zájmu dotčených subjektů, obvykle usazených ve státech s rozvinutější (trestněprávní) ochranou autorského práva, je v globálním měřítku obtížná. Žádosti o právní pomoc mohou ztroskotat na neexistenci mezinárodní smlouvy upravující mezinárodní justiční spolupráci a nesplnění podmínek oboustranné trestnosti.

[559] KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005, str. 84.
[560] Usnesení Nejvyššího soudu, sp. zn. 11 Tcu 29/2006, ze dne 24. 5. 2006.

Na druhou stranu lze zmínit, že jsou to právě pachatelé pocházející z vyspělejších států s rozvinutou právní ochranou autorských práv, jejichž trestné činy proti průmyslovým právům a autorskému právu působí citelnější škody. Aktivity pachatelů pocházejících z chudých a méně rozvinutých zemí s nimi zpravidla srovnatelné nejsou. Softwarové pirátství dosahuje vyšší hladiny ve vyspělých zemích světa nežli v chudých oblastech. Jelikož oblast průmyslových a autorských práv více profituje ze zisků pocházejících z bohatších států, jsou to právě bohatší státy, které pro uvedený průmysl díky softwarovému pirátství přinášejí nepoměrně vyšší ztráty. Při potírání softwarové kriminality by se z uvedeného důvodu vyplatilo více zaměřit na pachatele z bohatších států s rozvinutou právní ochranou autorského práva, nežli na pachatele ze států chudších.[561] Vzhledem ke globálnímu charakteru počítačových sítí je však zapotřebí mít na zřeteli podporu rozvoje trestněprávní ochrany v celosvětovém měřítku. V případě ochrany autorských práv v globálním virtuálním světě platí, že bude tak důsledná, jako v jurisdikci s nejslabší ochranou autorských práv.

5.2.3. Prioritní oblasti spolupráce při postihu počítačové kriminality

Rozvoj mezinárodní spolupráce v oblasti trestního práva je ovlivněn vůlí jednotlivých aktérů mezinárodního společenství podrobit určité oblasti právní regulaci, zatímco jiné z ní vynechat. Existují specifické oblasti, v nichž mezi státy panuje shoda co do prevence i následného postihu trestné činnosti. Shodná vůle aktérů mezinárodního společenství se posléze stává východiskem pro přijetí mezinárodněprávních instrumentů regulujících vybrané „prioritní“ oblasti ochrany.

Mezi aktuální priority mezinárodní spolupráce v rámci postihu počítačové kriminality, alespoň co se severoatlantické geografické oblasti týče, můžeme zařadit následující okruhy:

- postih nelegálního obsahu na Internetu,

[561] Podrobněji KIGERL, Alex C. Infringing Nations: Predicting Software Piracy Rates, BitTorrent Tracker Hosting, and P2P File Sharing Client. *International Journal of Cyber Criminology* [online]. 2013, 7(1), str. 62. Dostupné z http://www.cybercrimejournal.com/Alex2013janijcc.pdf [cit. 2016-03-17]. Překlad autorka.

- ochrana kritické infrastruktury a technologická spolupráce v rámci prevence a postihu kybernetických incidentů a útoků,
- prevence hospodářských dopadů počítačové kriminality,
- potírání nevyžádaného obsahu, především spamu, na Internetu.[562]

Výběr aktivit, na něž se mezinárodní společenství zaměřuje je obdobný i v případě práva EU, kde stupeň spolupráce v rámci jednotlivých orgánů a institucí EU a členských států dosahuje hlubší úrovně. EU dále klade velký důraz na vysokou úroveň ochrany soukromí a osobních údajů svých občanů, a to i v rámci virtuálního prostředí. Legislativní úprava je rovněž doplněna četnými akčními plány a projekty. Reálný dopad akčních plánů a projektů je však obtížné objektivně zhodnotit.

V poslední době se mezi oblast prioritní spolupráce řadí především kybernetické útoky na státní infrastrukturu a problematika kyberterorismu. Oba jevy vnímá mezinárodní společenství jako imanentní hrozby. Kybernetický útok na vybrané subjekty může mít fatální dopad na funkčnost státního aparátu i životy a zdraví obyvatel státu.[563] Hrozby kybernetických útoků nám nejsou zcela neznámé. Z nedávné doby lze jmenovat například kybernetické bezpečnostní incidenty týkající se útoku na informační infrastruktury Estonska, Gruzie či Nizozemí.[564] Z právního hlediska představuje zajištění kybernetické bezpečnosti komplexní problém. Zásadní výzvou se stává i pojetí státní suverenity v globálním virtuálním prostředí či princip vázanosti státní moci zákonem. Problematickým je i fakt, že efektivní bezpečnostní opatření se vždy dostává do kolize se základními lidskými právy a svobodami jedince.[565]

V případě postihu počítačové kriminality se poměrně často vyskytují důkazní prostředky vně jurisdikce vyšetřujících orgánů, které pak volí některou z následujících možností:

---

[562] Mezinárodní spolupráce v boji proti informační kriminalitě. *Ministerstvo vnitra České republiky: Výsledky projektů v rámci bezpečnostního výzkumu* [online]. Praha, 2009, str. 2. Dostupné z http://www.mvcr.cz/clanek/vysledky-projektu.aspx [cit. 2016-03-17].
[563] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 15.
[564] Útoky v Estonsku práce zmiňuje v kapitole 3.3.4.2. Kybernetické útoky v případě Gruzie byly součástí ozbrojeného konfliktu s Ruskem. Podrobný rozbor kybernetického útoku na nizozemskou certifikační autoritu DigiNotar ze září 2011 dostupný v ARNBAK, Axel; VAN EIJK, Nico. Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain. *TRPC* [online]. 2012, (August 15), 1 - 31 s. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409 [cit. 2016-04-13].
[565] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, 347.

- zahájení formální procedury na základě mezinárodních právních instrumentů upravujících vzájemnou právní pomoc,
- oslovení zahraničního orgánu činného v trestním řízení s žádostí o neformální spolupráci,
- přímá žádost vůči zahraničnímu ISP o jeho dobrovolnou spolupráci,
- přímé získání cílených dat.[566]

Tradiční formální procedura představuje pro orgány vyšetřující počítačovou trestnou činnost často příliš zdlouhavou cestu s nejistým výsledkem. Především Úmluva o počítačové kriminalitě a sekundární právo EU obsahují však specifická pravidla s cílem spolupráci dotčených států zrychlit a učinit ji flexibilnější.

Možnosti neformální spolupráce záleží na vztazích s dotčeným státem, popřípadě na osobních vztazích s pracovníky orgánu činného v trestním řízení v cizím státě a bývají proto omezené. Poslední dvě možnosti, kterými se obchází tradiční procedury mezinárodní justiční pomoci, nejsou přijímány mezinárodním společenstvím jednoznačně. Přílišné spoléhání se na způsoby neformální spolupráce vzbuzuje otázky přičitatelnosti jednání státního orgánu, překročení jeho pravomocí a porušení mezinárodněprávního principu suverenity.

5.3. Mezinárodní spolupráce dle zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních

Česká republika přistoupila k řadě úmluv, které se dotýkají mezinárodní justiční spolupráce v trestních věcech. Vstup do EU rovněž započal významné procesy harmonizace i unifikace českého právního řádu, trestní právo hmotné a procesní nevyjímaje. Mezinárodní justiční spolupráce představuje i díky evropské sekundární normotvorbě jednou z nejdynamičtěji se rozvíjejících oblastí právní regulace.

Myšlenka vytvořit samostatný právní předpis, který by se uceleně zabýval problematikou mezinárodní justiční spolupráce, vznikla okolo roku 2005. Z pohledu

[566] WALDEN, Ian. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Queen Mary School of Law Legal Studies Research Paper No. 74/2011* [online]. 2011, str. 11. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067 [cit. 2016-03-21]. Překlad autorka.

zachování požadavku kompaktnosti trestního práva ve dvou trestních kodexech a několika vedlejších trestních zákonech nebylo vyčlenění části trestních norem do samostatného zákona přijímáno kladně.[567] Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních (dále též „ZMJS“) byl nakonec 20. března 2013 schválen, účinnosti nabyl dne 1. ledna 2014.

5.3.1. Předmět úpravy

ZMJS rozlišuje mezi justiční spoluprací s cizími státy, které nejsou členem EU, a členskými státy EU. V důsledku zapracování příslušných předpisů evropského práva dochází k prohloubení spolupráce s ostatními členskými státy EU i k uplatnění určitých zvláštních postupů, jež ZMJS obsahuje v části páté. V rámci kooperačních metod spolupráce uvnitř EU tak ZMJS upravuje společný vyšetřovací tým, předání osoby, příkaz k zajištění hodnoty nebo důkazního prostředku a uznání a výkon vybraných soudních rozhodnutí.

Styk mezi orgány činnými v trestním řízení členských států EU je v ZMJS upraven především jako přímý styk, s ohledem na zásadu rychlosti a hospodárnosti řízení. Formou přímého styku je upravena mezinárodní justiční spolupráce ve věcech dožádání, převzetí a předání trestní věci a předávání trestního řízení dle evropského zatýkacího rozkazu. Ministerský právní styk mezi členskými státy EU upravuje ZMJS ve výjimečných případech.[568]

Mimo rozšířené metody spolupráce s členskými státy EU stanoví ZMJS i obecná pravidla pro jednotlivé formy mezinárodní justiční spolupráce. Část třetí ZMJS tak upravuje podmínky právní pomoci (ve smyslu žádosti o provedení konkrétního procesního úkonu pro účely trestního řízení vedeného cizím státem), vydání osoby, předání a převzetí trestního řízení, uznání a výkonu rozhodnutí ve vztahu k cizímu státu a průvoz osob. Zvlášť v části čtvrté řeší ZMJS spolupráci s mezinárodními trestními soudy a tribunály.

[567] KUBÍČEK, Miroslav. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014, str. XXIX.
[568] TEREZA, Coufalová. *Justiční a policejní spolupráce v Evropské unii*. V Praze: Univerzita Karlova, 2015, str. 134.

Vytknuty před výše uvedené formy a případy mezinárodní justiční spolupráce jsou obecná ustanovení v části první ZMJS a ochrana informací - zejména předávaných osobních údajů (s určitými výjimkami v rámci Eurojustu a Schengenského informačního systému) v části druhé ZMJS. Část druhá ZMJS se dále věnuje zastoupení České republiky v Eurojustu - instituci usnadňující spolupráci členských států EU na úrovni státního zastupitelství, dále Schengenskému informačnímu systému a ve stručnosti i Evropské justiční síti a styčným soudcům a státním zástupcům. Ti mají být vysíláni do ostatních členských států EU (hostitelské státy) a usnadnit díky osobním kontaktům mezinárodní justiční spolupráce uvnitř EU.[569]

5.3.2. Základní zásady

ZMJS vychází z několika základních zásad, které zajišťují zachování zákonnosti trestního řízení s mezinárodním prvkem.[570] Mezinárodní právní pomoc nelze cizozemskému orgánu poskytnout, došlo-li by jí k rozporu s ústavním pořádkem České republiky nebo se zásadou, na níž je zapotřebí bezvýhradně trvat, anebo k poškození jiného významného chráněného zájmu České republiky. Pokud by nebyla spolupráce mezi Českou republikou a cizím státem upravena mezinárodní smlouvou, je možné cizozemskému orgánu vyhovět jen při poskytnutí ujištění o vzájemnosti.[571] Úkon právní pomoci lze provést toliko po zahájení úkonů trestního řízení a pro účely daného trestního řízení. Důkazy získané mezinárodní justiční spoluprací musí být v zásadě použity právě pro účely trestního řízení, v souvislosti s nímž byly získány. Uplatnění uvedené zásady speciality je však omezeno na případy, kdy ji vyžaduje mezinárodní smlouva nebo jí cizozemský orgán podmiňuje poskytnutí požadovaného důkazu.[572] Nutno je respektovat zásadu presumpce neviny a dbát práva na ochranu osobnosti účastníků řízení. Dle § 9 odst. 6 ZMJS ovšem není k předání osobních údajů do ciziny zapotřebí souhlasu Úřadu pro ochranu osobních údajů. Respektovat je zapotřebí i

[569] KUBÍČEK, Miroslav. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014, str. 95.
[570] TEREZA, Coufalová. *Justiční a policejní spolupráce v Evropské unii*. V Praze: Univerzita Karlova, 2015, str. 135.
[571] Viz výše kapitola 5.1.3.
[572] § 7 odst. 1 ve spojení s § 2 písm. d) ZMJS.

ustanovení nutné obhajoby - řízení související s vydáváním a předáváním osob do ciziny a s vybranými případy řízení o uznání a výkonu rozhodnutí cizozemského orgánu jsou totiž důvodem nutné obhajoby nad rámec úpravy trestního řádu.[573]

Při řešení určité otázky je potřebné postupovat od konkrétního k obecnému, tj. v pořadí úpravy stanovené mezinárodní smlouvou, posléze dle ZMJS a následně dle trestního řádu. Na základě § 3 odst. 1 ZMJS je ZMJS vůči trestnímu řádu zákonem speciálním. Ve smyslu § 3 odst. 2 ZMJS zaujímá primární význam pro řešení dané otázky mezinárodní smlouva. Nestanoví-li mezinárodní smlouva jinak, použije se ZMJS. Pokud ZMJS danou otázku neřeší, užije se trestního řádu.

5.3.3. Základy aplikační praxe

V úvodních ustanoveních ZMJS lze vedle základních zásad mezinárodní justiční spolupráce nalézt i praktická ustanovení týkající se styku s cizozemskými orgány. Vzájemný styk se zpravidla uskutečňuje písemně v listinné podobě, avšak vyloučeny nejsou ani žádosti o mezinárodní justiční spolupráci podávané telefonicky, elektronicky, osobně nebo jiným způsobem. Takto lze navázat mezinárodní justiční styk v naléhavých případech, kdy se však zásadně předpokládá následné doručení originálu žádosti v listinné podobě. § 8 odst. 5 ZMJS umožňuje zahájit provádění úkonu mezinárodní justiční spolupráce na základě takové žádosti, nesnese-li věc zjevně odkladu a nejsou-li pochybnosti o hodnověrnosti žádosti. Důkazy, které justiční orgán na základě provedeného úkonu získal, však smí dožadujícímu se cizozemskému orgánu zaslat teprve po obdržení originálu jeho žádosti.[574] Případy, jež vyžadují okamžité předávání důkazů, bývají v praxi výjimečné a pro urychlení získávání operativních informací je praktičtější využít mezinárodní policejní spolupráce, jejíž výsledky mohou být v rámci trestního řízení použity před soudem jako důkaz na základě souhlasu příslušného orgánu státu, jde-li o členský stát EU, anebo cestou právní pomoci.[575] V případě vyšetřování

[573] Srov. § 14 ZMJS.
[574] Srov. § 9 odst. 2 ZMJS.
[575] KUBÍČEK, Miroslav. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014, str. 29.

počítačové kriminality s mezinárodním prvkem bude policejní spolupráce vzhledem k neodkladnosti řady zajišťovacích úkonů na místě.

Do ciziny je zapotřebí vždy zasílat buď originály (stejnopisy) anebo ověřené kopie, nikoli neověřené fotokopie. K tomu poslouží doložka justičního orgánu potvrzující shodu kopie s originálem založeným ve spisu.[576] Znění ověřovací doložky určené pro členský stát EU stanovilo Ministerstvo spravedlnosti České republiky ve své instrukci (viz níže). Uvedené doložky však nejsou soudní praxi vždy známy, resp. bývají často nahrazovány kulatým úředním razítkem soudu doplněným o podpis příslušného soudce.

Překlad žádosti o mezinárodní justiční spolupráci včetně jejích příloh do cizího jazyka zajišťuje orgán činný v trestním řízení, který vede trestní řízení. Je-li k vyžádání mezinárodní justiční spolupráce příslušný ústřední orgán, zajistí i překlad žádosti. Mezinárodní smlouva může umožnit zasílání žádosti bez překladu, vždy však bude v zájmu urychlení spolupráce vhodnější opatřit překlad do příslušného jazyka. Vyřízení žádosti cizího státu českým justičním orgánem je zásadně podmíněno obdržením žádosti spolu s jejím překladem do češtiny. Výjimečně, stanoví-li tak ZMJS nebo mezinárodní smlouva, není překladu zapotřebí, resp. žádost může být přeložena do jiného jazyka než jazyka dožádaného státu. Použití angličtiny a francouzštiny, tj. úředních jazyků Rady Evropy, umožňují např. mnohostranné smlouvy sjednané v rámci Rady Evropy, včetně Evropské úmluvy o vzájemné pomoci ve věcech trestních. Podání určené orgánu EU český soud do cizího jazyka nepřekládá, neboť čeština je jedním z úředních jazyků EU.

Úkony mezinárodní spolupráce by měl justiční orgán vždy provádět bez zbytečného odkladu, zejména může-li jeho rozhodování ovlivnit délku vazby. Zjistí-li nutnost vyžádat si dodatečné podklady, neprodleně o ně cizozemský orgán požádá.

V případě mezinárodní právní pomoci v užším slova smyslu se postupuje podle části třetí ZMJS. V přípravném řízení je oprávněným orgánem k vyžádání právní pomoci státní zástupce, po podání obžaloby soud. Právní styk s cizinou se nejčastěji děje v přípravném řízení skrze Nejvyšší státní zastupitelství. Co se přijetí žádosti o právní pomoc týče, oprávněným bude rovněž Nejvyšší státní zastupitelství, vede-li se v cizím státě přípravné řízení. Ve zbylých případech přijímá žádosti Ministerstvo

[576] KUBÍČEK, Miroslav. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014, str. 26.

spravedlnosti České republiky. Problematickou pro vymezení kompetence se proto může stát absence fází trestního řízení a nerozlišení řízení přípravného a řízení před soudem, s níž se setkáváme ve státech systému common law. V řízení před soudem má značnou pravomoc Ministerstvo spravedlnosti České republiky. Oprávněno je vypracované žádosti o právní pomoc kontrolovat a po dožadujícím se soudu žádat nezbytné opravy a doplnění. Jeho stanovisko k podobě žádosti o právní pomoc je dle § 40 odst. 2 ZMJS pro soud závazné.

Na závěr lze uvést i interní předpis Ministerstva spravedlnosti České republiky, které k postupu soudů při styku s členskými státy EU vydalo instrukci, jež má soudům sloužit jako metodická pomůcka při aplikaci jednotlivých ustanovení ZMJS i příslušných mezinárodních smluv. Jedná se o Instrukci Ministerstva spravedlnosti ze dne 30. dubna 2014, č. j. 42/2013-MOT-J/60, o postupu soudů ve styku se členskými státy Evropské unie ve věcech trestních (dále jen „Instrukce“). Instrukce obsahuje mimo jiné informace kde zjišťovat konkrétní mezinárodní smlouvy platné ve vztazích mezi Českou republikou a členskými státy nebo informace o výhradách a prohlášeních k nim se vztahujících, detailní postup při vytváření písemností určených členskému státu EU[577] či kde nalézt adresu orgánu členského státu, kterému má být doručena písemnost.

Obsah a forma právní pomoci musí odpovídat příslušným ustanovením ZMJS. Ministerstvo spravedlnosti České republiky pro zjednodušení vypracování žádostí vytvořilo vzory, které jsou soudům dostupné na jeho Extranetu. V případě naléhavé nutnosti právní pomoci členského státu EU je však možné vznést žádost i skrze mezinárodní organizaci kriminální policie – Interpol. V takovém případě justiční orgán kontaktuje odbor mezinárodní policejní spolupráce Policejního prezidia České republiky.

5.4. Mezinárodní spolupráce na úrovni univerzální i regionální

Mnohé z aktivit mezinárodních organizací a institucí působí jako styčný prostor k navázání hlubších vztahů. Do značné míry proto spolupráci v oblasti počítačové

[577] Každá písemnost musí být opatřena razítkem soudu, datem a vlastnoručním podpisem soudce spolu s jeho jménem a funkcí. V písemnostech nesmí být uvedena žádná pohrůžka sankcí za nedostavení se k úkonu, včetně předvedení.

kriminality usnadňují - například pořádáním mezinárodních setkání a zprostředkováním mezinárodní diskuze zahrnující státní i soukromý sektor. V oblasti zprostředkování uvedeného dialogu na mezinárodní úrovni lze zmínit zejména činnost Organizace pro hospodářskou spolupráci a rozvoj.

V rámci mezinárodního společenství působí řada mezinárodních organizací, které se v rámci své činnosti postihu přeshraniční počítačové kriminality dotýkají. O počítačové kriminalitě se začíná na půdě jednotlivých organizací hovořit až zhruba od přelomu 80. a 90. let 20. století. Vedle mnohých rezolucí a dokumentů povahy soft law jsou přijímány i mezinárodní smlouvy obsahující ustanovení týkající se specificky postihu počítačové kriminality či jevů s ní spojených. Uvedené mezinárodní smlouvy se stávají pramenem mezinárodního práva veřejného a skrze sebe samé sjednocují právní úpravu smluvních stran.

Jediným pramenem mezinárodního práva veřejného, který byl zaměřen výlučně na postih počítačové kriminality, doposud zůstává již zmiňovaná Úmluva o počítačové kriminalitě, která byla na půdě Rady Evropy přijata roku 2001. S ohledem na množství dokumentů mezinárodních organizací, které se tématu počítačové kriminality dotýkají, se následující text soustředí pouze na některé, u nichž lze předpokládat větší význam pro mezinárodní spolupráci při postihu různých forem počítačové kriminality.

5.4.1. Organizace spojených národů

V rámci Organizace spojených národů (dále též „OSN“) doposud nedošlo k přijetí samostatné mezinárodní smlouvy týkající se kyberprostoru. Kyberprostoru se ale dotýkají jiné specificky zaměřené dokumenty, mezi které lze řadit Rezoluci Rady bezpečnosti OSN č. 1624 ze dne 14. září 2005, zavazující členy OSN k zákazu podněcování aktů terorismu. Rezoluce nabádá členské státy k výměně informací a zkušeností i k zabránění vzniku bezpečných útočišť pro potenciální pachatele.[578]

Dalším dokumentem OSN, který se dotýká postihu počítačové kriminality, je Rezoluce o boji se zneužíváním informačních technologií ze dne 22. ledna 2001.

[578] Mezinárodní spolupráce v boji proti informační kriminalitě. *Ministerstvo vnitra České republiky: Výsledky projektů v rámci bezpečnostního výzkumu* [online]. Praha, 2009, str. 2 - 3. Dostupné z http://www.mvcr.cz/clanek/vysledky-projektu.aspx [cit. 2016-03-17].

Zdůrazňuje význam posílené spolupráce při postihu trestné činnosti páchané prostřednictvím informačních technologií, a to jak mezi státy navzájem, tak i mezi státy a soukromými subjekty. Požaduje, aby trestní stíhání s mezinárodním prvkem bylo koordinováno ve všech dotčených státech, a doporučuje výměnu poznatků s cílem nalézt řešení konkrétních problémů při potírání této trestné činnosti.[579]

Tématu organizovaného zločinu, který souvisí s postihem počítačové kriminality, se věnuje Úmluva OSN proti nadnárodnímu organizovanému zločinu z roku 2000 (dále též „Palermská úmluva“).[580] Palermská úmluva představovala zásadní krok vpřed zejména s ohledem na rozšíření kriminalizace legalizace výnosů z trestné činnosti z aktivit vztahujících se toliko na obchod s drogami, na veškeré formy legalizace výnosů pocházejících ze závažnější trestné činnosti.[581]

Palermská úmluva dopadá na předcházení, vyšetřování a stíhání vyjmenovaných trestných činů a všech závažných trestných činů, jsou-li nadnárodní povahy[582] a zahrnují organizovanou zločineckou skupinu. Závažnou trestnou činností se přitom rozumí dle čl. 2 písm. b) Palermské úmluvy trestná činnost, za kterou je stanoven trest odnětí svobody s horní hranicí trestní sazby v trvání nejméně čtyř roků. Kriminalizaci legalizace výnosů z trestné činnosti ukládá smluvním stranám čl. 6 Palermské úmluvy. Opatření k boji proti praní špinavých peněz poté shrnuje čl. 7 Palermské úmluvy, který opakuje stávající prevenční postupy (evidence hlášení podezřelých transakcí apod.) a nově ukládá smluvním stranám vytvořit „finanční zpravodajské jednotky“, specializující se na shromažďování a následnou analýzu informací.[583]

---

[579] Texty rezolucí OSN jsou dostupné v anglickém jazyce z http://research.un.org/en/docs/ga/quick/regular/70 [cit. 2016-03-17]. Překlad autorka.

[580] Úmluva OSN ze dne 15. listopadu 2000 proti nadnárodnímu organizovanému zločinu. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 75/2013 Sb. m. s.

[581] *Odhad nezákonných finančních toků plynoucích z obchodu s drogami a jiného nadnárodního organizovaného zločinu: výzkumná zpráva Úřadu Spojených národů pro drogy a kriminalitu (UNODC)*. Praha: Institut pro kriminologii a sociální prevenci, 2013, str. 169.

[582] Dle čl. 3 odst. 2 Palermské úmluvy, tj. je-li spáchán ve více než jednom státě; je spáchán v jednom státě, avšak podstatná část příprav na něj, jeho plánování, řízení či kontroly se odehrává v jiném státě; je spáchán v jednom státě, avšak zahrnuje účast organizované zločinecké skupiny, která se zabývá trestnou činností ve více než jednom státě; nebo je spáchán v jednom státě, avšak jeho podstatné dopady se projevují v jiném státě.

[583] *Odhad nezákonných finančních toků plynoucích z obchodu s drogami a jiného nadnárodního organizovaného zločinu: výzkumná zpráva Úřadu Spojených národů pro drogy a kriminalitu (UNODC).* Praha: Institut pro kriminologii a sociální prevenci, 2013, str. 169.

5.4.2. Severoatlantická obranná aliance (NATO)

Obranná strategie Severoatlantické obranné aliance (dále též „NATO“) reagovala na změny v Severoatlantickém bezpečnostním prostředí. V rámci boje proti počítačové kriminalitě se NATO soustřeďuje především na kybernetickou obranu a kyberterorismus. Kybernetické útoky NATO považuje za součást hybridní války a kybernetickou obranu již vnímá jako základ zajišťované kolektivní obrany.[584]

NATO tradičně působilo ve třech bojových doménách – ve vzduchu, na zemi a na moři. V červnu roku 2016 na svém Summitu ve Varšavě NATO připojilo i čtvrtou doménu, kterou je kybernetické prostředí. Rozšíření své působnosti na čtvrtou doménu NATO odůvodnilo čím dál významnější rolí, kterou kybernetické prostředí hraje v moderních bezpečnostních konfliktech.[585] Kyberprostor již dlouho není považován za prostředí, kde právo vliv nemá. Většina jurisdikcí světa uznává právní regulaci virtuálního prostředí a není tedy důvodu, proč by mezinárodní právo veřejné mělo být výjimkou. Summit NATO ve Varšavě jen potvrdil působnost mezinárodního práva veřejného v kyberprostoru.

Posílení kybernetické bezpečnosti informačních a komunikačních sítí spojenců zařadilo NATO mezi své základní úkoly po útocích na estonskou infrastrukturu v roce 2007. V případě žádosti členského státu NATO přistoupí k posílení obrany kyberprostoru. Postup umožní společný koordinovaný přístup k obraně kyberprostoru, včetně odezvy na případný kybernetický útok. Někteří však upozorňují na zbytečnou duplikaci obranných postupů na půdě EU a NATO.[586]

Jednotlivé členské země jsou zodpovědné za bezpečnost národních sítí samy, avšak jsou povinny zaručit kompatibilitu i mezi sebou a především s infrastrukturou NATO. Mezi stěžejní požadavky NATO patří posílení výměny informací i vzájemné pomoci jak v rámci prevence, tak při odražení a nápravě dopadů kybernetických útoků na spojenecké země. Při zajišťování kybernetické bezpečnosti NATO začíná

[584] Podrobněji http://www.nato.int/cps/en/natohq/topics_78170.htm [cit. 2017-01-29]. Překlad autorka.
[585] NATO Summit Guide, Warsaw 2016, str. 128. Dostupné z http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf [cit. 2016-03-18]. Překlad autorka.
[586] AWAN, Imran; BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012, str. 166. Překlad autorka.

intenzivněji spolupracovat také s EU. Skrze tzv. CERT[587] pracoviště na úrovni NATO i EU, která řeší bezpečnostní incidenty, má probíhat oboustranná výměna informací a sdílení osvědčených postupů.[588]

Ačkoli smyslem NATO je působit v oblasti obrany, jeho aktivity ovlivňují obecný politický postoj jednotlivých států k problematice kybernetické bezpečnosti. Značný význam má NATO pro posílení mezinárodní spolupráce spojeneckých zemí a rychlou výměnu cenných poznatků týkajících se kybernetických útoků.

5.4.3. Rada Evropy

Rada Evropy je významnou mezinárodní organizací přispívající nejen k mezinárodní spolupráci v trestních věcech obecně, nýbrž i k mezinárodní spolupráci při postihu počítačové kriminality. Základním pramenem mezinárodní spolupráce v trestních věcech je Evropská úmluva o vzájemné pomoci ve věcech trestních, přijatá v Štrasburku dne 20. dubna 1959, kterou doplňují i dva dodatkové protokoly.[589] Pro oblast počítačové kriminality je zásadním pramenem práva zmiňovaná Úmluva o počítačové kriminalitě, která představuje vůbec první projev globální snahy po právní regulaci počítačové kriminality.

Úmluva o počítačové kriminalitě je dosud jediným pramenem mezinárodního práva veřejného, který se komplexně zabývá počítačovou kriminalitou. Vedle ní má určitý význam pro postih počítačové kriminality v mezinárodním prostředí i Úmluva o ochraně dětí před sexuálním vykořisťováním a sexuálním zneužíváním.[590] Větší význam pro mezinárodní spolupráci při postihu počítačové kriminality má bezesporu Úmluva o počítačové kriminalitě a proto se jí následující text věnuje detailněji.

[587] Computer Emergency Responsibility Team.
[588] Podrobněji http://www.nato.int/cps/en/natohq/topics_78170.htm a http://www.nato.int/cps/en/natohq/news_127836.htm [cit. 2016-03-18]. Překlad autorka.
[589] Viz kapitola 5.1.3.
[590] Úmluva Rady Evropy č. 201 ze dne 25. října 2007 o ochraně dětí před sexuálním vykořisťováním a zneužíváním. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 59/2016 Sb. m. s.

5.4.3.1. Úmluva o počítačové kriminalitě

Úmluva o počítačové kriminalitě je první mezinárodní smlouvou upravující výlučně problematiku trestných činů spáchaných v internetovém prostředí. Za jejím přijetím stál požadavek definovat společné východisko pro trestní politiku, které by vedlo k ochraně společnosti před počítačovými delikty v globálnějším měřítku. Význam Úmluvy o počítačové kriminalitě lze proto spatřit především ve sjednocení kriminalizovaného jednání a posílení mezinárodní spolupráce.[591]

Úmluva o počítačové kriminalitě se dotýká hmotněprávních i procesněprávních aspektů postihu počítačové trestné činnosti a úpravy mechanismů usnadňujících mezinárodní justiční spolupráci při postihu počítačové kriminality s mezinárodním prvkem. Úmluva o počítačové kriminalitě byla otevřena k podpisu 23. listopadu 2001 v Budapešti a 28. ledna 2003 ji doplnil Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.[592] Úmluvu o počítačové kriminalitě ratifikovalo celkem 42 členských států Rady Evropy, otevřena k ratifikaci je i nečlenským státům, z nichž k ní dosud přistoupilo států deset - včetně USA, Kanady, Izraele či Japonska.[593]

Nelze ovšem přehlédnout, že tempo ratifikací Úmluvy o počítačové kriminalitě ze strany států je více než laxní. Ani téměř po 16 letech od svého přijetí nebyla ratifikována všemi členskými státy Rady Evropy (chybí ratifikace Irska, Monaka, Švédska či Ruska). Česká republika, která Úmluvu o počítačové kriminalitě ratifikovala 22. srpna 2013, si též s podpisem nepospíšila.[594] Lze se domnívat, že jedním z důvodů, proč státy váhají připojit k Úmluvě o počítačové kriminalitě svůj podpis, je množství zemí, které se ji rozhodly neratifikovat a ani tak v nejbližší době neplánují učinit. V kyberprostoru ovšem postačí jediné bezpečné útočiště ilegálních aktivit pro jejich následné rozšíření do zbylého světa.

---

[591] YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013, str. 160. Překlad autorka.
[592] Viz opak. cit. 243.
[593] Kompletní seznam viz Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime. *Council of Europe* [online]. Dostupné z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=gf19uMUq [cit. 2017-01-29]. Překlad autorka.
[594] V platnost pro Českou republiku vstoupila dne 1. prosince 2013.

Na motivaci ratifikovat Úmluvu o počítačové kriminalitě jistě nepřidá i fakt, že jedním z váhajících států je Rusko. Úmluvu o počítačové kriminalitě nepodepsalo, ačkoli je samo členským státem Rady Evropy. Rusko (spolu s Čínou) je řadou expertů podezříváno z podporování kybernetických útoků.[595] S ohledem na vysoké nároky na mezinárodní spolupráci při vyšetřování a stíhání počítačových trestných činů, které Úmluva o počítačové kriminalitě vyžaduje, nelze v dohledné době předpokládat přílišnou vůli Ruska ani Číny se k Úmluvě o počítačové kriminalitě připojit.[596] Na druhé straně ratifikace nemusí zaručit kýžený úspěch. Řada chudých rozvojových zemí, které přistoupily k Úmluvě o počítačové kriminalitě a transponovaly její ustanovení do národních právních řádů, nedisponuje dostatečnými prostředky ani nástroji k vynucení nové právní úpravy.[597]

Vedle požadavků kriminalizace činů, které definuje jako počítačové trestné činy[598] a podmínek přijetí příslušných procesních ustanovení k jejich vynucení, obsahuje Úmluva o počítačové kriminalitě i ustanovení týkající se mezinárodní spolupráce, včetně tradiční trestní praxe týkající se vydávání osob.[599] Jestliže se smluvní stát rozhodne nevydat svého občana na žádost jiného státu vázaného Úmluvou, musí podle principu *dedere aut judicare*[600] sám uskutečnit trestní stíhání. Protože Úmluva o počítačové kriminalitě vyžaduje kriminalizaci počítačových deliktů definovaných v čl. 2 až čl. 11 Úmluvy o počítačové kriminalitě vždy (dochází ke sjednocení hmotněprávní úpravy smluvních států), měl by stát odmítající extradici zahájit v uvedené situaci trestní stíhání v každém případě.[601]

---

[595] AWAN, Imran; BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012, str. 160. Překlad autorka.

[596] Smysl Úmluvy o počítačové kriminalitě bez její ratifikace Ruskem a Čínou vedl jednoho britského novináře k jednoduchému konstatování: „No Russia + No China = No point“. Srov. UK finally ratifies Cybercrime Convention during Obama visit: No Russia + No China = No point. *The Register* [online]. 2011. Dostupné z http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ [cit. 2016-03-18]. Překlad autorka.

[597] YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013, str. 17. Překlad autorka.

[598] Tyto se dělí na: 1) trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů, 2) trestné činy související s počítači, 3) trestné činy související s obsahem a 4) trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

[599] Čl. 22 odst. 3 Úmluvy o počítačové kriminalitě.

[600] Jednodušeji „vydej, anebo stíhej“.

[601] Podrobněji KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006, str. 17. Překlad autorka.

5.4.3.2. Procesní ustanovení Úmluvy o počítačové kriminalitě ovlivňující postih počítačové kriminality

Procesní ustanovení Úmluvy o počítačové kriminalitě nejsou limitována počítačovými trestnými činy vyjmenovanými v čl. 2 až 11 Úmluvy o počítačové kriminalitě, ale uplatní se jak ve vztahu k jiným trestným činům spáchaným díky využití počítače, tak i při zajištění důkazů trestných činů obecně v elektronické formě. Pouze u shromažďování provozních dat a obsahových dat v reálném čase dle čl. 20 a čl. 21 Úmluvy o počítačové kriminalitě je ponechána státům možnost učinit vůči okruhu přípustných trestných činů výhradu.[602]

Čl. 15 Úmluvy o počítačové kriminalitě zdůrazňuje podmínky a záruky ve vztahu ke všem procesním postupům a pravomoci orgánů činných v trestním řízení – těmi má být princip přiměřenosti a zajištění standardu ochrany lidských práv a svobod v souladu s mezinárodními lidskoprávními závazky.

Ve vztahu k uvedené množině trestných činů požaduje Úmluva o počítačové kriminalitě po jednotlivých státech následující procesní opatření:[603]

- urychlené uchování uložených počítačových dat,
- urychlené zachování a urychlené částečné zpřístupnění provozních dat,
- příkaz k předložení,
- prohlídka a zajištění uložených počítačových dat,
- shromažďování provozních dat v reálném čase,
- odposlech obsahových dat.

Urychlené uchování uložených počítačových dat a urychlené zachování a částečné zpřístupnění provozních dat dle čl. 16 a čl. 17 Úmluvy o počítačové kriminalitě dopadá na veškerá data (tj. obsahová data i metadata) uložená v počítači. Cílem je předejít ztrátě či modifikaci dat důležitých pro objasnění a postih trestné činnosti předtím, než budou zkoumána v rámci digitální forenzní expertízy. Vyšetřující orgány

[602] Čl. 14 odst. 2, odst. 3 ve spojení s čl. 42 Úmluvy o počítačové kriminalitě.
[603] Autorka v názvech ustanovení respektuje český překlad Úmluvy o počítačové kriminalitě, byť lze mít vůči němu výhrady.

by měly mít možnost přikázat urychlené uchování dat po nezbytně nutnou dobu, než si opatří v rámci mezinárodní justiční spolupráce přístup k datům uloženým v počítači.

Požadavky Úmluvy o počítačové kriminalitě vůči provozním datům provádí § 97 odst. 3 ZEK, který požaduje uchování provozních a lokalizačních údajů po šest měsíců. Nad rámec české právní úpravy by mělo být možné na základě čl. 16 odst. 2 Úmluvy o počítačové kriminalitě i další uchování po nezbytně nutnou dobu, nejvýše po 90 dní. Uvedený požadavek nebyl do českého právního řádu proveden. Orgány činné v trestním řízení tak musí přímo požádat o zajištění provozních a lokalizačních dat dle § 88a TŘ, bez možnosti přikázat urychlené uchování dat. Povinnost uchovávat jiné než provozní a lokalizační údaje český právní řád neukládá, v důsledku čehož nelze ani žádat urychlené uchování jiných než uložených provozních dat.

Co se příkazu k předložení počítačových dat nebo informací o odběrateli služby (dále jen „příkaz k předložení“) v čl. 18 Úmluvy o počítačové kriminalitě týče, vztahuje se na uložená počítačová data, s nimiž povinná osoba disponuje. Ačkoli je působnost příkazu k předložení omezena na území smluvních stran, povšimněme si dalekosáhlých důsledků čl. 18 odst. 1, písm. b) Úmluvy o počítačové kriminalitě, kdy poskytovatelé služeb nabízející své služby na území smluvní strany, mají předložit příslušným orgánům informace o odběrateli vztahující se k službě poskytované na území smluvní strany. Budou-li přitom požadované informace v držení poskytovatele služby, je irelevantní, jsou-li uchovávány na dálku.[604] Doslovným výkladem lze dospět k názoru, že zahraniční poskytovatel služby nabízející své služby na území České republiky, řekněme společnost Google, je povinen předložit informace o odběrateli služby, které jsou v jeho držení nebo pod jeho kontrolou (zpravidla na serverech v USA), což se však v praxi neděje. Jde ve svém důsledku o exteritoriální rozšíření pravomocí smluvní strany. Povinnost je ale prakticky nevymahatelná.

Při příkazu k předložení jsou využívány zajišťovací instituty vydání a odnětí hmotné věci (například paměťového nosiče) dle § 78 a § 79 TŘ i zajištění nehmotné věci dle § 79e TŘ, popřípadě ke zjištění provozních a lokalizačních údajů zjišťování údajů o telekomunikačním provozu dle § 88a TŘ. Ne všechny uvedené instituty však plně vyhovují charakteru digitálních dat.

[604] Explanatory report to the Convention on Cybercrime (ETS No. 185) [online]. Bod 173. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-02-23]. Překlad autorka.

Prohlídka a zajištění uložených počítačových dat v čl. 19 Úmluvy o počítačové kriminalitě cílí na zachycení digitálních důkazních prostředků a konfiskaci dat.[605] Týká se opět jen uložených dat. Smyslem je umožnit smluvním stranám získat přístup k počítači a jeho části a tím pádem i k datům zde uloženým, anebo k paměťovému médiu, kde by se data mohla nacházet.[606] Kvůli volatilitě počítačových dat a potřebě jejich urychleného zajištění požaduje Úmluva o počítačové kriminalitě uzákonění urychleného rozšíření prohlídky i na jiné počítačové systémy na území smluvní strany, existuje-li domněnka, že v nich jsou hledaná data ve skutečnosti uložena, a z počítače, k němuž příslušné orgány získali díky prohlídce přístup, je možné se k hledaným datům legálně dostat.[607] Česká právní úprava umožňuje prohlídku a zajištění uložených počítačových dat díky zajištění nehmotné věci dle § 79e TŘ a domovní prohlídce a prohlídce jiných prostor a pozemků dle § 82 až § 85c TŘ. Urychlené rozšíření prohlídky do dalších počítačových systémů nebylo provedeno. Trestní řád v případě přístupu k dalšímu počítači skrze počítač již prohledávaný s existencí „nového" prostoru, pro který by bylo zapotřebí nového povolení prohlídky, vůbec nepočítá.

Shromažďování provozních dat v reálném čase a odposlech obsahových dat v čl. 20 a čl. 21 Úmluvy o počítačové kriminalitě se váží k datům přenášeným v rámci komunikace, nikoli k uloženým datům. Čl. 20 Úmluvy o počítačové kriminalitě se týká provozních dat a čl. 21 Úmluvy o počítačové kriminalitě obsahových dat. Působnost procesních opatření lze omezit vymezením příslušné kategorie trestných činů. Odposlech obsahových dat považuje Úmluva o počítačové kriminalitě za výraznější zásah do základních lidských práv a svobod. Proto požaduje, aby nebylo

[605] GŘIVNA, Tomáš. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008, str. 127.

[606] U neotevřeného e-mailu záleží na vnitrostátním právu, zda jej považuje za již uložená počítačová data nebo za data ještě přenášená, na které se uplatní odposlech komunikace. Podrobněji Explanatory report to the Convention on Cybercrime (ETS No. 185) [online]. Bod 190. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-02-23]. Překlad autorka.

[607] Úmluva hovoří o legálním přístupu. Přístup k počítačovému systému, který je neoprávněný, nemohou orgány činné v trestním řízení využít, byť by tak mohly prohlídku rozšířit i na vzdálený počítač. Podrobný rozbor problematiky přeshraniční prohlídky skrze počítačovou síť podává SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1). Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10]. Překlad autorka.

shromažďování provozních dat v reálném čase omezeno výrazněji než odposlech obsahových dat.

Odposlech a záznam obsahových dat v reálném čase již upravuje § 88 TŘ. Provozních dat uskutečněného telekomunikačního provozu se týká § 88a TŘ. Záznam provozních dat v reálném čase se však děje dle § 88 TŘ, tj. díky probíhajícímu odposlechu a záznamu obsahových dat (vedle obsahových dat jsou logicky zaznamenávána i provozní data). Požadavek plošného uchovávání obsahových i provozních dat rozebírá práce výše.[608]

5.4.3.3. Ustanovení Úmluvy o počítačové kriminalitě dotýkající se mezinárodní spolupráce

V kapitole třetí upravuje Úmluva o počítačové kriminalitě tradiční mechanismy mezinárodní právní pomoci. Ustanovení se uplatní jak při neexistenci smluvní úpravy mezi státy, tak za situace, kdy právní základ mezinárodní spolupráce mezi státy již existuje.[609] Při neexistenci mezinárodních dohod se východiskem spolupráce stávají postupy v čl. 27 a čl. 28 Úmluvy o počítačové kriminalitě. Při existenci smluvního základu spolupráce budou ustanovení Úmluvy o počítačové kriminalitě doplňující. Jak vyplývá z čl. 39 Úmluvy o počítačové kriminalitě, cílem nebylo stávající zásady spolupráce mezi státy nahradit. Z tohoto pohledu se jeví jako výjimečný požadavek na vytvoření právního základu k mechanismům spolupráce podle čl. 29 až čl. 35 Úmluvy o počítačové kriminalitě.[610]

Obecnou zásadou je pravidlo spolupracovat v co nejširší možné míře a minimalizovat překážky. Je vhodné zdůraznit, že úprava mezinárodní spolupráce se netýká výlučně kategorie počítačových trestných činů dle čl. 2 až čl. 11 Úmluvy o počítačové kriminalitě, nýbrž dopadá na trestní řízení týkající se všech trestných činů se vztahem k počítačovým systémům a datům. Uplatní se i pro účely shromažďování

[608] Je patrné, že současná česká právní úprava plně neodráží všechny procesní závazky stanovené Úmluvou o počítačové kriminalitě.
[609] Typicky Úmluva Rady Evropy č. 30 ze dne 29. 4. 1959 o vzájemné pomoci v trestních věcech, včetně jejích dvou dodatkových protokolů.
[610] GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. *Acta Universitatis Carolinae. Iuridica*. 2008, 2008(4), str. 26.

důkazů v elektronické formě ve vztahu k trestným činům obecně.[611] Extradici umožňuje Úmluva o počítačové kriminalitě v zásadě vždy pro již uvedené případy počítačových trestných činů dle čl. 2 až čl. 11 Úmluvy o počítačové kriminalitě, jestliže v dotčených státech podléhají trestu odnětí svobody s horní hranicí trestní sazby alespoň jednoho roku. Při neexistenci extradičních úmluv mohou státy vycházet z Úmluvy o počítačové kriminalitě.

Smyslem úpravy mezinárodní právní pomoci je především zajištění rychlosti a flexibility s ohledem na volatilitu digitálních důkazních prostředků. Každá ze stran tak může v naléhavých případech žádat o právní pomoc nebo sdělení cestou rychlých komunikačních prostředků, např. elektronickou poštou, za předpokladu dostatečné úrovně zabezpečení. Následné formální potvrzení žádosti o právní pomoc je fakultativní - záleží na vůli dožádané strany. Pro případ odmítnutí vzájemné pomoci pro nesplnění podmínky oboustranné trestnosti se má za to, že podmínka oboustranné trestnosti bude splněna, jestliže předmětné jednání bude považováno za trestný čin bez ohledu na jeho pojmenování nebo zařazení pod jinou kategorii trestných činů podle práva dožádané strany. Lze se domnívat, že podmínka oboustranné trestnosti splněna nebude, bude-li dožádaný stát považovat čin za správní delikt, neboť výkladová zpráva k Úmluvě o počítačové kriminalitě užívá spojení *„criminal offence in requested Party´s laws“*, nikoli tzv. delict či tzv. administrative offence.[612]

Reakce na pomalé tradiční procedury mezinárodní pomoci nacházíme v čl. 29 a čl. 30 Úmluvy o počítačové kriminalitě. Představují prozatímní opatření, na jejichž základě mohou státy žádat o urychlené uchování uložených počítačových dat i sdělení provozních dat. V situaci nasvědčující výskytu digitálního důkazního prostředku v počítači nacházejícím se mimo jurisdikci státu lze s ohledem na akutní hrozbu ztráty či modifikace uložených počítačových dat žádat o jejich urychlené zajištění. Součástí žádosti dožadující se strany musí být i její záměr předložit žádost o vzájemnou pomoc týkající se prohlídky či obdobného získání přístupu k datům. Úmluva o počítačové

[611] *Explanatory report to the Convention on Cybercrime (ETS No. 185)* [online]. Treaty Office. Council of Europe, 2001, bod 243. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-02-23]. Překlad autorka.
[612] *Explanatory report to the Convention on Cybercrime (ETS No. 185)* [online]. Treaty Office. Council of Europe, 2001, bod 259. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-02-23]. Překlad autorka.

kriminalitě výslovně zakazuje podmiňovat vyřízení žádosti k prozatímnímu opatření podmínkou oboustranné trestnosti.[613] Stanoví však benevolentnější podmínky pro smluvní stranu požadující splnění oboustranné trestnosti jako podmínku vyřízení pozdější žádosti týkající se prohlídky či přístupu k datům. Česká republika si v souladu s čl. 42 Úmluvy o počítačové kriminalitě vyhradila právo odmítnout žádost o uchování dat, pokud lze předpokládat, že nebude možné ve vztahu k jiným než trestným činům dle čl. 2 až čl. 11 Úmluvy o počítačové kriminalitě podmínku oboustranné trestnosti splnit. Žádost o uchování dat smí strana odmítnout z důvodů ochrany svrchovanosti, bezpečnosti, veřejného pořádku nebo jiných základních zájmů, anebo považuje-li trestný čin za politický.

Počítačová data musí dožádaná strana uchovat nejméně po dobu 60 dní, s ohledem na poskytnutí přiměřené lhůty k podání následné žádosti o právní pomoc dožadující se stranou. V souvislosti s výše uvedenou žádostí lze urychleně sdělit provozní data.

S ohledem na zásadu svrchovanosti musí mít každá ze smluvních stran prostor požadovat provedení potřebných procesních úkonů orgány činnými v trestním řízení na dotčeném území. Na žádost druhé strany proto smluvní stát provede prohlídku a zajištění uložených počítačových dat v počítačovém systému umístěném na jeho území. Zvláště urychleně tak učiní v případě dat obzvláště ohrožených ztrátou nebo pozměněním.

Dále jsou smluvní strany Úmluvy o počítačové kriminalitě zavázány poskytnout si vzájemnou pomoc při shromažďování provozních dat v reálném čase. S ohledem na povahu provozních dat, kterým poskytují právní řády států obvykle nižší standard ochrany než obsahovým datům, nepředstavuje vyhovění takové žádosti o právní pomoc problém. Přesto některé země mohou volit odlišný přístup a právě z toho důvodu požaduje Úmluva o počítačové kriminalitě, aby bylo žádostem o shromažďování provozních dat vždy vyhověno minimálně ve vztahu k trestným činům, kde to dovoluje vnitrostátní právo dožádaného státu.

Efektivní spolupráce mezi stranami Úmluvy o počítačové kriminalitě vyžaduje rychlou a nepřetržitou komunikaci. Proto Úmluva o počítačové kriminalitě požaduje zřízení sítě kontaktních míst provozovaných 24 hodin denně po 7 dní v týdnu, za

[613] Čl. 29 odst. 3 Úmluvy o počítačové kriminalitě.

účelem poskytování okamžité pomoci během probíhajícího vyšetřování či shromažďování elektronických důkazů. Kontaktní místo, s ohledem na podmínky stanovené vnitrostátním právním řádem, přímo nařizuje uchování dat dle čl. 29 a čl. 30 Úmluvy o počítačové kriminalitě. Kontaktním místem České republiky byl určen Odbor informační kriminality Úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky.[614]

5.4.3.4. Úmluva o ochraně dětí před sexuálním vykořisťováním a sexuálním zneužíváním

Hovoříme-li o mezinárodní spolupráci při postihu počítačové kriminality zaměřené na šíření škodlivého obsahu, zejména dětské pornografie, stojí za zmínku i další významná úmluva Rady Evropy, kterou je Úmluva o ochraně dětí před sexuálním vykořisťováním a sexuálním zneužíváním (dále též „Lanzarotská úmluva“).[615] Lanzarotská úmluva je prvním mezinárodním pramenem práva sjednocujícím kriminalizaci různých forem sexuálního zneužívání dětí, včetně jednání spáchaného skrze prostředky ICT. V tomto směru lze uvést cyber-grooming, tedy snahu přimět dítě k sexuálně explicitnímu chování díky komunikaci skrze ICT (typicky využitím chatu či aplikací Skype, Viber), kdy se pachatel vydává za jinou osobu. V rámci české trestněprávní úpravy bude možné uvažovat o kvalifikaci přečinem navazování nedovolených kontaktů s dítětem dle § 193b TZ. Ustanovení Lanzarotské úmluvy ovlivnily podobu hmotněprávních i procesněprávních trestních norem České republiky. Lanzarotská úmluva vstoupila v platnost 1. července 2010, Česká republika ji ratifikovala 2. května 2016 a v platnost pro ni vstoupila 1. září 2016.

Lanzarotská úmluva mimo jiné ukládá státům kriminalizovat výrobu, nabízení, distribuci, opatření, držení a vědomé získání přístupu k dětské pornografii prostřednictvím ICT.[616] Vůči kriminalizaci vědomého získání přístupu k dětské pornografii skrze ICT mohou státy učinit výhradu. V případě České republiky již

[614] Sdělení Ministerstva zahraničních věcí ČR o sjednání Úmluvy o počítačové kriminalitě, vyhlášené pod číslem 104/2013 Sb. m. s.
[615] Viz opak. cit. 583.
[616] Čl. 20 Lanzarotské úmluvy.

k novelizaci příslušného ustanovení § 192 odst. 2 TZ došlo, s ohledem na požadavky sekundární normotvorby EU, a případná výhrada tak pozbyla pro náš stát významu.

Lanzarotská úmluva požaduje po smluvních státech co nejširší možnou spolupráci, při níž se dle čl. 38 odst. 1 Lanzarotské úmluvy vychází z existujících mezinárodních smluv, kterými jsou státy vázány, i z jejich vnitrostátních právních úprav. Pokud mezi státem dožadujícím se právní pomoci a státem dožádaným není uzavřena mezinárodní smlouva, lze díky čl. 38 odst. 3 Lanzarotské úmluvy tuto považovat za právní základ vzájemné pomoci ve věcech trestních.

Pro vzájemnou výměnu informací a důkazů není bez významu ani ustanovení týkající se záznamu a uchování údajů v čl. 37 Lanzarotské úmluvy. Ten požaduje provádět systematický sběr a uchování osobních údajů o totožnosti a genetickém profilu osob odsouzených za stanovené sexuální trestné činy. Systém zajišťuje v České republice v současnosti Národní databáze DNA,[617] ve které jsou údaje pachatelů zmíněných trestných činů uchovávány. Lanzarotská úmluva v případě potřeby ukládá zajistit přenos dat shromažďovaných za účelem prevence a postihu sexuálních trestných činů směrem k ostatním smluvním stranám. Ustanovení v mezinárodním kontextu zcela jistě usnadní a urychlí proces vyšetřování sexuálně zaměřených počítačových trestných činů v případě sexuálních recidivistů, na druhé straně ale vzbuzuje otázky přiměřenosti natolik intruzivního monitorovacího mechanismu. Česká republika tak do budoucna ztratí možnost kontroly nad souborem zvláště citlivých osobních údajů odsouzených.

5.5. Spolupráce členských států Evropské unie

Vliv práva EU na trestněprávní postih počítačové kriminality v České republice je nesporný. Zejména sekundární normotvorba EU postupně proměňuje českou právní úpravu v oblasti trestního práva hmotného i procesního. V rámci EU vzniká i rozsáhlé množství dokumentů a právních předpisů regulujících problematiku informačních a komunikačních technologií.

Sdělení Komise Evropskému parlamentu, Radě a Výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. května 2007 dokládá patrnou

[617] Databáze byla zřízena na základě závazného pokynu policejního prezidenta č. 88/2002.

snahu EU bojovat proti počítačové kriminalitě.[618] Česká republika je zavázána k postihu ryze počítačových trestných činů díky Rámcovému rozhodnutí Rady EU 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům,[619] které požaduje kriminalizaci protiprávního přístupu k informačním systémům i zásahu do systému a dat.[620] Uvedené rámcové rozhodnutí bylo nahrazeno směrnicí Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV,[621] která představuje stěžejní předpis bezpečnosti informačních systémů i postihu počítačové kriminality v prostředí EU. Zásadním právním předpisem pro vyšetřování a postih trestných činů v prostředí členských států EU je i směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech.[622]

Na půdě EU došlo taktéž k přijetí obecných instrumentů usnadňujících spolupráci ve věcech trestních. Jedná se o Úmluvu o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie, doplněnou o jeden protokol, o kterých práce již pojednává výše.[623] Z množství právních předpisů a dokumentů veskrze politické povahy uvádí následující text prameny sekundární evropské normotvorby dotýkající se specifických oblastí počítačové kriminality, včetně legalizace výnosů z trestné činnosti díky zneužití ICT (v rámci boje proti organizovanému zločinu) a šíření škodlivého obsahu skrze ICT (zejména dětské pornografie).

5.5.1. Evropský vyšetřovací příkaz

Zjednodušení a zrychlení přeshraničního vyšetřování trestných činů je cílem směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o

[618] Podrobněji GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. *Acta Universitatis Carolinae. Iuridica*. 2008, 2008(4), str. 31 – 32.
[619] Dostupné z http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32005F0222&qid=1485613101828 [cit. 2017-01-28].
[620] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 287.
[621] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1485613101828&uri=CELEX:32013L0040 [cit. 2017-01-28].
[622] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1485613871878&uri=CELEX:32014L0041 [cit. 2017-01-28].
[623] Viz kapitola 5.1.3.

evropském vyšetřovacím příkazu v trestních věcech (dále též „evropský vyšetřovací příkaz“).[624] Základem je zásada vzájemného uznávání, podle níž je členský stát povinen uznat a vyhovět žádosti jiného členského státu o provedení jednoho či několika konkrétních vyšetřovacích úkonů, s cílem shromáždit důkazy v probíhajícím trestním řízení. U počítačové kriminality se znaky organizovaného zločinu působícího ve více členských státech,[625] lze snad očekávat, že evropský vyšetřovací příkaz přispěje k urychlení vyšetřování.

Výhodou evropského vyšetřovacího příkazu je působnost na veškeré vyšetřovací úkony zaměřené na shromáždění důkazů.[626] Evropský vyšetřovací příkaz představuje rozhodnutí justičního orgánu členského státu a má podobu standardizovaného formuláře. Požádat o jeho vydání smí i podezřelý, obviněný a obhájce.[627] Vydání příkazu není omezeno na zahájení trestního stíhání, ale lze jej vydat i ve správním řízení, existuje-li možnost pozdějšího řízení trestního.

Úprava se snaží nastavit rychlý a flexibilní rámec, což lze s ohledem na charakter počítačové kriminality hodnotit kladně. Veškerý úřední styk je uskutečňován přímo mezi vydávajícím a vykonávajícím orgánem. Nebude-li mít dožádaný orgán příslušnou pravomoc úkon provést, postoupí z moci úřední evropský vyšetřovací příkaz příslušnému orgánu. Vyšetřovací úkon musí vykonávající orgán provést se stejnou rychlostí a prioritou, jako by šlo o vnitrostátní případ. Vydávající stát smí uvést s ohledem na okolnosti případu nezbytnou časovou lhůtu, kterou by vykonávající orgán měl zohlednit, nicméně ten bude vázán až časovými lhůtami v čl. 12 evropského vyšetřovacího příkazu.[628] Uvedené lhůty jsou však s ohledem na snadnou a rychlou manipulaci digitálními daty pro postih počítačové kriminality s mezinárodním prvkem bez většího významu. V případě odposlechu je však možné využít přímo přeshraniční možnost provedení úkonu (srov. níže).

Členské státy smí odmítnout vykonat evropský vyšetřovací příkaz jen z vymezených důvodů, například s ohledem na imunitu či výsadu dle vnitrostátního

[624] Opak. cit. 615.
[625] Např. skimming je často páchán na území více států. Bankomaty pro umístění zařízení na skimming jsou vybírány v „lukrativnějších“ lokalitách, kopie bezhotovostních platebních prostředků jsou posléze zhotovovány v jiné zemi a opět v jiné lokalitě (či přes internet) je s nimi placeno jako s pravými.
[626] Na rozdíl od procedur založených dnes již zrušeným rámcovým rozhodnutím Rady 2008/978/SVV o evropském důkazním příkazu, které se vztahovalo pouze na existující důkazní prostředky.
[627] Čl. 1 odst. 3 evropského vyšetřovacího příkazu.
[628] Lhůta 30 dní, respektive 90 dní a ve výjimečných případech ještě delší. Viz čl. 12 odst. 6 evropského vyšetřovacího příkazu.

práva, znemožňující provést vyšetřovací úkon, na nepřípustnost vyšetřovacího úkonu ve vymezených řízeních v obdobném vnitrostátním případě, na ochranu národní bezpečnosti, či pro rozpor se zásadou *ne bis in idem*.[629] Odložit uznání či výkon je možné pouze na přiměřeně nutnou dobu, jestliže by bylo narušeno probíhající trestní stíhání, anebo jsou-li důkazní prostředky užívány již v jiném řízení.[630]

Evropský vyšetřovací příkaz zvláště upravuje kontrolu bankovních a jiných finančních účtů osob, proti nimž se vede trestní řízení, nepřetržité shromažďování důkazů v reálném čase a skryté formy vyšetřování, u kterých stanoví širší rámec důvodů pro odmítnutí vyšetřovacího úkonu.[631]

Zvlášť upravuje evropský vyšetřovací příkaz přeshraniční odposlech telekomunikačního provozu, ke kterému může docházet s pomocí i bez pomoci jiného členského státu. Nelze-li odposlech provézt bez technické pomoci jiného členského státu, pak platí, že dožádaný stát smí vedle obecných důvodů pro odmítnutí podmínit odposlech podmínkami svého vnitrostátního práva.[632] Členské státy vzájemně konzultují volbu buď bezprostředního přenosu anebo záznamu odposlechu a následného přenosu jeho výsledku do vydávajícího státu. Možné je požádat též o dekódování či dešifrování záznamu.[633]

K evropskému vyšetřovacímu příkazu se nepřipojilo Dánsko a Irsko.[634] Bude zajímavé sledovat, zda se tento fakt promítne v přeshraničním vyšetřování počítačové kriminality, například tím, že se země stanou „bezpečnějšími přístavy“. Ostatní členské státy jsou povinny transponovat směrnici do 22. května 2017.

5.5.2. Směrnice o útocích na informační systémy

EU považuje bezpečnostní útoky na kriticky významné informační systémy členských států za hrozbu pro oblast svobody, bezpečnosti a práva, na kterou reaguje zintenzivněním spolupráce. Význam směrnice Evropského parlamentu a Rady

[629] K dalším důvodům odmítnutí uznání či výkonu příkazu srov. čl. 11 evropského vyšetřovacího příkazu.
[630] Čl. 15 odst. 1 evropského vyšetřovacího příkazu.
[631] Čl. 28 a čl. 29 evropského vyšetřovacího příkazu.
[632] Čl. 30 odst. 5 evropského vyšetřovacího příkazu.
[633] Čl. 30 odst. 7 evropského vyšetřovacího příkazu.
[634] Pro tyto země ovšem zůstává v platnosti Úmluva o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie (2000/C 197/01).

2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (dále též „směrnice o útocích na informační systémy“) spočívá v harmonizaci skutkových podstat vybraných trestných činů a jejich sankcí. Směrnice usiluje mimo jiné o zavedení trestních sankcí za vytváření botnetů. Cílem je rovněž zlepšit spolupráci mezi orgány členských států i cestou sjednocení hmotněprávní úpravy, společnými pojmovými definicemi a zajištěním kontaktní sítě pro předcházení kybernetickým útokům.

Směrnice o útocích na informační systémy navazuje na úpravu v Úmluvě o počítačové kriminalitě a apeluje na členské státy EU, aby co nejdříve dokončily proces její ratifikace. Směrnice o útocích na informační systémy využívá v některých členských státech EU již existující sítě kontaktních míst a po zbylých požaduje zřízení národního kontaktního místa. Národní kontaktní místa zřízená za účelem výměny informací o stanovených trestných činech,[635] by měla naléhavé žádosti členských států EU urychleně zpracovat. Minimálně do osmi hodin od obdržení žádosti by kontaktní místo mělo dožadující se členský stát EU informovat o konkrétní reakci.[636] Vyjádřením časového rámce lze usuzovat na snahu EU upřednostnit reakci na žádosti jiných členských států před žádostmi ostatních smluvních států Úmluvy o počítačové kriminalitě, pakliže by v rámci sítě kontaktních míst nastala kolize.

Směrnice o útocích na informační systémy zdůrazňuje i význam spolupráce mezi veřejným a soukromým sektorem a apeluje na členské státy EU, aby zapojily ISP do komunikační sítě za účelem výměny informací týkajících se vymezených trestných činů. S ohledem na nedostatek relevantních poznatků využitelných pro mezinárodní srovnání a prevenci, doporučuje předávat informace o způsobu, kterým pachatelé páchají trestnou činnost, Evropskému centru pro boj proti kyberkriminalitě v rámci Europolu i agentuře ENISA.[637]

---

[635] Trestné činy v čl. 3 až čl. 8 směrnice o útocích na informační systémy, tedy neoprávněný přístup k informačním systémům, neoprávněné zasahování do informačních systémů, neoprávněné zasahování do údajů a neoprávněné sledování údajů, včetně trestního postihu všech forem účastenství, pokusu a některých forem jednání, která jsou materiálně přípravou k uvedeným trestným činům.

[636] Čl. 13 odst. 1 směrnice o útocích na informační systémy.

[637] Evropské centrum pro boj proti kyberkriminalitě (European Cybercrime Center) sídlící v Haagu, bylo zřízeno v rámci Europolu v lednu roku 2013. Agentura ENISA (European Union Agency for Network and Information Security) řeší témata kybernetické a informační bezpečnosti a je centrem pro mezistátní výměnu informací, osvědčených postupů a poznatků v oblasti.

5.5.3. Směrnice proti pohlavnímu zneužívání a vykořisťování dětí

Boj proti pohlavnímu zneužívání dětí skrze Internet patří mezi klíčové iniciativy EU. Směrnice Evropského parlamentu a Rady 2011/93/EU[638] ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje Rámcové rozhodnutí Rady 2004/68/SVV (dále též „směrnice proti pohlavnímu zneužívání a vykořisťování dětí“)[639] harmonizuje skutkové podstaty a sankce trestných činů souvisejících s formami pohlavního zneužívání dětí a postihuje šíření dětské pornografie na Internetu i sexuální turistiku.

Směrnice proti pohlavnímu zneužívání a vykořisťování dětí se okrajově dotýká spolupráce mezi členskými státy při potírání dětské pornografie na Internetu. Členské státy jsou povinny přijmout opatření umožňující neprodleně odstranit internetové stránky podílející se na šíření dětské pornografie, jsou-li spravovány na jejich území.[640] O jejich odstranění musí však stát usilovat i jsou-li stránky spravovány mimo jeho území. Členské státy jsou povinny vzájemně se informovat o existenci stránek obsahujících a šířících dětskou pornografii, a informovaný stát, na jehož území jsou stránky spravovány, je musí neprodleně odstranit.

5.5.4. Boj proti organizovanému zločinu - postih legalizace výnosů z trestné činnosti a prevence zneužívání finančního systému a financování terorismu

Jedním z klíčových nástrojů boje proti organizovanému zločinu práva EU je zajištění a konfiskace výnosů z trestné činnosti. Cílem právní úpravy je překazit vstup výnosů z trestné činnosti do legální ekonomiky a předejít vzniku možných způsobů legalizace výnosů z trestné činnosti. Ta se stejně jako financování terorismu běžně

[638] Směrnice byla vyhlášena v obsahu a titulku s chybným číselným označením „2011/92/EU“. K opravě číslování na správné „2011/93/EU“ došlo v Úředním věstníku EU dne 17. 12. 2011. Přesto se pod chybným označením stále objevuje v mnohých publikacích.
[639] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1485615180792&uri=CELEX:32011L0093 [cit. 2017-01-28].
[640] Čl. 25 odst. 1 směrnice proti pohlavnímu zneužívání a vykořisťování dětí.

odehrává v mezinárodním prostředí a vnitrostátní regulace tak nebude nikdy plně dostačující.

V rámci práva EU lze nalézt dokumenty zamezující praní špinavých peněz[641] v aktech přijatých v rámci bývalého prvního a třetího pilíře komunitárního práva. Po přijetí Lisabonské smlouvy se postih praní špinavých peněz objevuje v rámci boje proti závažné trestné činnosti s přeshraničním rozměrem.[642] Praní špinavých peněz je spolu s trestnou činností v oblasti výpočetní techniky a organizovanou trestnou činností dle čl. 83 Smlouvy o fungování EU jednou z oblastí harmonizace pravidel definujících trestné činy a sankce v oblasti mimořádně závažné trestné činnosti s přeshraničním rozměrem.

Jedním z prvních dokumentů věnujících se legalizaci výnosů z trestné činnosti byla Společná akce 98/699/SVV ze dne 3. prosince 1998 přijatá Radou na základě článku K. 3 Smlouvy o Evropské unii o praní peněz, identifikaci, vysledování, zmrazení, zajištění a propadnutí nástrojů trestné činnosti a výnosů z ní,[643] jejímž smyslem bylo zefektivnit boj proti organizovanému zločinu na území EU. Následovala řada rámcových rozhodnutí,[644] právní instrumenty však nebyly podle Evropské komise členskými státy uspokojivě implementovány a jejich praktické využití i skutečná harmonizace právních úprav zůstává otázkou. Nedostatečná mezinárodní spolupráce mezi členskými státy EU činí boj proti organizovanému zločinu méně efektivní a vede k nízkým hodnotám reálně konfiskovaných zisků organizovaného zločinu oproti výnosům pocházejícím z jiné trestné činnosti.[645]

Preventivním právním nástrojem pro zneužívání finančního systému pro účely praní špinavých peněz a financování terorismu se stala směrnice Evropského

---

[641] K vysvětlení pojmu viz kapitola 3.2.2.3.
[642] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 153.
[643] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31998F0699&qid=1483382623972&from=EN [cit. 2017-01-02].
[644] Např. rámcové rozhodnutí Rady 2001/500/SVV z 26. června 2001 o praní špinavých peněz, identifikaci, vyhledávání, zmrazení, zajištění a konfiskaci prostředků a příjmů z trestné činnosti; rámcové rozhodnutí Rady 2006/783/SVV z 6. října 2006 o uplatňování zásady vzájemného uznávání příkazů ke konfiskaci; rámcové rozhodnutí Rady 2007/845/SVV z 6. prosince 2007 o spolupráci mezi úřady pro vyhledávání majetku z trestné činnosti v členských státech v oblasti vysledování a identifikace výnosů z trestné činnosti nebo jiného majetku v souvislosti s trestnou činností.
[645] SZABOVÁ, Eva. Boj s organizovanou kriminalitou na úrovni Európskej únie – aktuálny vývoj. In: JELÍNEK, Jiří, ed. *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014, str. 78 - 79.

parlamentu a Rady 2005/60/ES ze dne 26. října 2005 o předcházení zneužití finančního systému k praní peněz a financování terorismu.[646] Její přijetí urychlili teroristické útoky v USA i v Evropě, odhalující předchozí nedostatečnou úpravu.[647] Nově se objevuje myšlenka, že oslabení stability finančního sektoru masivními toky špinavých peněz lze čelit nejen trestněprávními prostředky, nýbrž i posílením prevence uvnitř finančního systému. Cílem je proto posílit integritu a stabilitu úvěrových a finančních institucí i výkon vybraných profesních činností, mezi něž patří audit, daňové poradenství, notářství či advokacie. Úprava dopadá na činnosti těchto osob a institucí vykonávané i skrze Internet. Podrobnými pravidly je zajištěno prověření skutečné identity klientů finančního sektoru (tzv. hloubková kontrola klienta), jakož i hlášení podezřelých transakcí a zavedení preventivních ochranných vnitřních postupů v rámci finančního sektoru.

K 26. červnu 2017 bude dosavadní úprava nahrazena novou směrnicí,[648] zavádějící centrální registr vlastnických struktur právnických osob a zajišťující kompatibilitu právní úpravy s aktuálními doporučeními mezinárodní Finanční akční skupiny (FATF). Centrální registr vlastnických struktur lze hodnotit pozitivně, neboť přinese informace o skutečném vlastnictví společností a jiných právnických osob zapsaných ve veřejných rejstřících. Nedostupnost údajů a neznalost cizozemské rejstříkové úpravy může hrát při vyšetřování organizovaného zločinu značnou roli.

Prostředkem dosažení vyšší míry harmonizace právních úprav by měla být i směrnice Evropského parlamentu a Rady 2014/42/EU ze dne 3. dubna 2014 o zajišťování a konfiskaci nástrojů a výnosů z trestné činnosti v Evropské unii (dále též „směrnice o zajištění výnosů“).[649] Směrnice o zajištění výnosů stanoví minimální pravidla pro zajištění výnosů z trestné činnosti i prostředků sloužících k získání finančního prospěchu. Konfiskace se týká vedle výnosů i nástrojů, kterým je dle čl. 2

[646] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32005L0060&qid=1483464370977&from=EN [cit. 2017-01-03].
[647] JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. Praha: Leges, 2015, str. 162.
[648] Směrnice Evropského parlamentu a Rady 2015/849/EU ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady 648/2012/EU a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES. Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32015L0849&qid=1483467008854&from=EN [cit. 2017-01-03].
[649] Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32014L0042&qid=1483385077105&from=EN [cit. 2017-01-02].

bodu 3. směrnice o zajištění výnosů *„jakýkoli majetek zcela nebo částečně použitý nebo určený k použití libovolným způsobem pro spáchání jednoho nebo více trestných činů.“* Oblast věcné působnosti určují trestné činy v čl. 3 směrnice o zajištění výnosů. Mezi nimi jsou mimo jiné trestné činy podle rámcového rozhodnutí Rady 2001/413/SVV ze dne 28. května 2001 o potírání podvodů a padělání bezhotovostních platebních prostředků, trestné činy podle rámcového rozhodnutí Rady 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu, trestné činy podle směrnice proti pohlavnímu zneužívání a vykořisťování dětí i trestné činy podle směrnice o útocích na informační systémy. Na základě výše uvedeného je jasné, že nová pravidla harmonizace boje proti praní špinavých peněz dopadnou i na značnou část výnosů a nástrojů navázaných na počítačovou kriminalitu.

Směrnice o zajištění výnosů do značné míry ovlivňuje trestní postih vybraných forem počítačové kriminality. Výnosy i nástroje počítačové kriminality je možné v trestním řízení na území EU zajistit i konfiskovat. Výjimkou zůstává území Velké Británie a Dánska. Čl. 5 směrnice o zajištění výnosů rozšiřuje pravomoc soudu ve vztahu k částečné nebo úplné konfiskaci majetku odsouzeného (tzv. rozšířená konfiskace), pakliže lze na základě okolností případu předpokládat, že konkrétní majetek pochází z trestné činnosti. Rozšířenou konfiskací majetku může dojít i k zabrání majetku odsouzeného, který přesáhne přímé výnosy z trestné činnosti. Oproti dřívější úpravě postačí k rozhodnutí o rozšířené konfiskaci pouhé přesvědčení soudu o danosti uvedeného stavu. Směrnice o zajištění výnosů se takto snaží překlenout nedostatečné využívání konfiskace v praxi.[650] K „flexibilní“ formě rozšířené konfiskace však soud nemůže přistoupit u všech trestných činů, nýbrž jen u výslovně uvedených v čl. 5 odst. 2 směrnice o zajištění výnosů. Přísná úprava rozšířené konfiskace se dotkne zejména korupčních trestných činů, trestných činů týkajících se zločinného spolčení vedoucího k hospodářskému prospěchu, trestných činů spojených s výrobou dětské pornografie i případů rozsáhlého hackingu. Zda budou členské státy poměrně progresivní úpravu v rámci prevence i boje proti uvedeným závažným formám počítačové trestné činnosti využívat, ukáže teprve čas.

[650] SZABOVÁ, Eva. Boj s organizovanou kriminalitou na úrovni Európskej únie – aktuálny vývoj. In: JELÍNEK, Jiří, ed. *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014, str. 83.

5.6. Vybrané problémy mezinárodní spolupráce při postihu počítačové kriminality

Praxe mezinárodní spolupráce při vyšetřování počítačové kriminality se často potýká s problémy v přístupu k počítačovým datům nacházejícím se v zahraničí. Situaci komplikuje i nástup služeb cloud computing v posledních letech.

5.6.1. Přeshraniční prohlídka skrze počítačovou síť

Ani rozvinutá mezinárodní spolupráce pokaždé efektivní výsledky nezaručí. Mohou nastat případy, kdy druhý stát nebude disponovat dostatkem materiálních prostředků, potřebných znalostí nebo adekvátní právní úpravou. Může chybět i vůle příslušného orgánu cizího státu podílet se na vyšetřování a poskytnout potřebnou součinnost při obstarávání digitálních důkazních prostředků. Reakce dostavující se v horizontu jednoho roku není u žádosti o mezinárodní právní pomoc výjimkou.[651] V takových případech ostatní státy zvažují obstarání důkazního prostředku vlastními prostředky, jako je provedení přeshraniční prohlídky skrze počítačovou síť.

Přeshraniční prohlídkou skrze počítačovou síť je prohlídka počítačových dat uložených na serverech cizího státu, zpravidla díky možnostem internetových sítí. Někteří ISP, jako například Hotmail, Google, Microsoft a Facebook, usazení ve Velké Británii, předávají orgánům činným v trestním řízení údaje týkající se uživatelů na základě pouhého policejního příkazu (podle místního práva není třeba příkazu soudu), a to i do zahraničí, aniž by byli vázáni zákonnou povinností.[652] Pomineme-li tuto veřejně proklamovanou vůli některých ISP dobrovolně spolupracovat s cizozemskými orgány činnými v trestním řízení, možností, jak bez mezinárodní spolupráce získat v zahraničí uložená počítačová data, není mnoho a vytvářet pro každý případ společné vyšetřovací

[651] O´FLOINN, Micheál. It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe. *Computer Law & Security Review* [online]. 2013, 29(5), str. 613. Dostupné z http://www.sciencedirect.com/science/article/pii/S0267364913001428 [cit. 2016-03-20]. Překlad autorka.
[652] Tamtéž, str. 610 – 615.

týmy není reálné. Ze závazných mezinárodních instrumentů se přeshraničním přístupem k počítačovým datům zabývá toliko čl. 32 Úmluvy o počítačové kriminalitě.

5.6.1.1. Případy veřejně dostupných dat a poskytnutí souhlasu

Úmluva o počítačové kriminalitě upravuje dva možné přeshraniční přístupy k uloženým počítačovým datům. V případě prvního jde o zřejmou možnost získat přístup k veřejně dostupným datům, bez ohledu na geografické umístění otevřeného zdroje.[653] Typickým příkladem je načtení veřejně přístupné webové stránky hostované na serveru v zahraničí. Tyto zdroje bývají označovány jako „open source", tj. otevřené zdroje. Přístup k nim má kdokoli a není důvod z něj orgány činné v trestním řízení vyloučit.

Druhá možnost opravňuje smluvní stranu Úmluvy o počítačové kriminalitě buď ze svého území za pomoci počítače získat přístup k uloženým datům umístěným na území jiné strany, anebo tato data obdržet. Podmínkou je získání právoplatného a dobrovolného souhlasu osoby, která má zákonnou pravomoc zpřístupnit druhé smluvní straně data pomocí počítače.[654] Nejasná formulace a mnohostranný výklad pojmu „právoplatný a dobrovolný souhlas" je důvodem kontroverze zmíněného ustanovení i odmítání ratifikace Úmluvy o počítačové kriminalitě ze strany některých členských států Rady Evropy. V případě Ruska je zmíněný článek všeobecně znám jako jeden z hlavních důvodů, proč se Úmluvu o počítačové kriminalitě rozhodlo neratifikovat.[655]

Co se týče práva EU, zdá se, že je natolik zaměřeno na striktní ochranu osobních údajů, že nedovoluje, aby ISP obcházeli souhlas subjektu údajů či procedury vzájemné právní pomoci mezi dotčenými státy a na místo toho přímo poskytovali orgánům cizích států žádaná digitální data. Soukromý sektor však namítá, že subjekt údajů souhlas se zpřístupněním údajů již udělil v obchodních podmínkách, kterými se poskytování konkrétní služby řídí.[656] Částečnou alternativou při vyšetřování v členských státech EU

[653] Čl. 32 písm. a) Úmluvy o počítačové kriminalitě.
[654] Čl. 32 písm. b) Úmluvy o počítačové kriminalitě.
[655] KOOPS Bert-Jaap. Cyklus přednášek z předmětu „Cybercrime" na Tilburg University v Nizozemském království, zimní semestr 2014/2015.
[656] Alespoň dle zástupců Mezinárodní obchodní komory (International Chamber of Commerce) a společnosti Symantec. Souhlas se zpracováním údajů je v právu ochrany osobních údajů a soukromí komplikovanou otázkou. Podrobněji O´FLOINN, Micheál. It wasn't all white light before Prism: Law

by mohl být evropský vyšetřovací příkaz, který umožňuje urychlené provedení vyšetřovacího úkonu orgány příslušného státu. Na druhou stranu lze očekávat, že tam, kde se spolupráce se zahraničními ISP orgánům činným v trestním řízení osvědčila, nebudou volit přeci jen zdlouhavější alternativu evropského vyšetřovacího příkazu.

Přes nastíněné komplikace lze uzavřít, že s ohledem na rozhodné právo v konkrétním případě bude dle Úmluvy o počítačové kriminalitě za právoplatný souhlas považován souhlas udělený osobou, o jejíž data se jedná, ISP nebo příslušným orgánem státu.[657]

5.6.1.2. Přeshraniční přístup k datům při neexistenci souhlasu

Poslední variantu představuje situace, kdy počítačová data nejsou veřejně dostupná a získat souhlas oprávněné osoby k jejich zpřístupnění není možné. Dovoluje mezinárodní právo veřejné získat přeshraniční prohlídkou skrze počítačovou síť přístup k takovým datům? Zajímavý rozbor problematiky nabízí Seitz.[658]

Seitz pojednává o jednom z vůbec prvních případů přeshraniční prohlídky skrze počítačovou síť – o případu „Gorshkov-Ivanov".[659] Dva ruští občané, Vasiliy Gorshkov a Alexey Ivanov, získali údaje bankovního charakteru neoprávněným přístupem do počítačových systémů bank a jiných finančních institucí v USA a zneužili je k četným podvodům. Příslušníci Federálního vyšetřovacího úřadu USA (dále též „FBI") detekovali podezřelé jako majitele počítačů nacházejících se v Čeljabinsku v Rusku. FBI poté vytvořila fiktivní společnost Invitu, specializující se na oblast počítačové bezpečnosti a jejím jménem nabídla oběma podezřelým zaměstnání. Pracovní příležitost

---

enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe. *Computer Law & Security Review* [online]. 2013, 29(5), str. 611. Dostupné z http://www.sciencedirect.com/science/article/pii/S0267364913001428 [cit. 2016-03-20]. Překlad autorka.

[657] *Explanatory report to the Convention on Cybercrime (ETS No. 185)* [online]. Treaty Office. Council of Europe, 2001, bod 294. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. [cit. 2016-02-23]. Překlad autorka.

[658] SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1). Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10]. Překlad autorka.

[659] „The Gorshkov-Ivanov case." Souhrn případu dostupný z https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/gorshkovSent.htm [cit. 2016-03-20]. Překlad autorka.

si Invita vymínila předvedením schopností obou podezřelých na území USA, konkrétně získáním přístupu do počítačové sítě společnosti Invita. Oba podezřelí, používajíce místních počítačů, vyzradili FBI přístupová hesla k vlastním počítačům v Rusku. Ihned po jejich zatčení FBI na základě příkazu k prohlídce od soudce v USA získala přístup k počítačům v Rusku, z nichž zajistila množství důkazního materiálu. Oba Rusové byli v USA odsouzeni k nepodmíněnému trestu odnětí svobody.

Stěžejní otázkou v našem případě je, zda svým postupem během získání počítačových dat FBI porušila suverenitu Ruska, popřípadě zda je omezení suverenity jiného státu za určitých případů ospravedlnitelné. Rusko vůči postupu FBI, nikoli překvapivě, protestovalo a zahájilo vůči příslušníku FBI, který vedl vyšetřování, trestní stíhání pro trestný čin spočívající v neoprávněném přístupu k počítačovému systému. USA příslušníka FBI vydat odmítly a ocenily jej za jeho přínos k dopadení pachatelů.

Všeobecně je přijímán názor, že citovaný postup FBI lze považovat za porušení principu státní suverenity, neboť dotčený stát, Rusko, k prohlídce předem nedal souhlas. Výjimkou je poskytnutí souhlasu od osoby, vůči níž je prohlídka vedena, a případy, kdy vyšetřující stát nemohl vědět, že se data ve skutečnosti nenachází v jeho teritoriu. Setkáme se i s nepříliš rozšířeným názorem, podle kterého je přeshraniční prohlídka skrze počítačovou síť bez fyzické přítomnosti aktéra jednání příliš zanedbatelné, aby konstituovalo skutečné porušení suverenity státu.[660]

Seitz dochází k závěru, že veškeré prohlídky neslučitelné s čl. 32 Úmluvy o počítačové kriminalitě odporují normám mezinárodního práva. S ohledem na neexistenci ustanovení mezinárodních smluv je nutné vyjít z praxe států, podle které je přeshraniční prohlídka skrze počítačovou síť v zásadě nepřípustná. USA však uznávají jako přípustnou prohlídku za existence výjimečných okolností, mezi které řadí hrozbu ztráty či zničení důkazních prostředků v případě závažných trestných činů nebo existenci teroristické hrozby.[661] Naproti tomu Rusko odmítá přípustnost přeshraniční

[660] SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1), str. 11- 12. Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10]. Překlad autorka.

[661] *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* [online]. Office of Legal Education Executive Office for United States Attorneys, 2009, str. 27 – 28. Dostupné z https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [cit. 2016-03-20]. Překlad autorka.

prohlídky skrze počítačovou síť bez dalšího, neboť neuznává ani výše zmíněná pravidla dle čl. 32 Úmluvy o počítačové kriminalitě.

5.6.2. Cloud computing

Cloud computing (dále též „cloud“) definujeme jako *„způsob používání počítačových technologií (služeb, programů) uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat prakticky odkudkoliv pomocí webového prohlížeče nebo jiných rozhraní – např. klienta dané aplikace.“*[662] Uživateli využívaná služba je odebírána ze vzdáleného místa, které vlastní a spravuje poskytovatel cloudu.[663] Data uživatelů služeb nejsou pod jejich fyzickou kontrolou a nachází se zpravidla na serverech rozmístěných po celém světě. Smejkal doslova uvádí: *„čím obtížněji je uchopitelný vlastník a odpovědný provozovatel cloudu, tím rizikovější situace.“*[664] Zejména u cloudu provozovaného mimo EU hrozí riziko okamžité ztráty dat, soukromí uživatelů a nevymahatelnost jakékoli právní povinnosti.[665] Charakteristické vlastnosti cloudu působí v kriminalistické praxi značné problémy, neboť maximálně snižují efektivní možnosti ohledání informačních systémů nacházejících se v cloudu kdesi v zahraničí.

V případě počítačové kriminality se s využíváním služeb cloudu setkáváme především u vyšetřování trestného činu porušení autorského práva, práv souvisejících s právem autorským a práv k databázi dle § 270 TZ. Běžně dochází ke sdílení autorských děl pomocí úložišť využívajících služeb cloudu. S požadavkem získat přístup k datům uloženým v cloudu se však lze setkat i u běžné trestné činnosti, přistupuje-li orgán činný v trestním řízení k e-mailové schránce obviněného, jehož ISP využívá služeb cloudu pro ukládání dat elektronické komunikace uživatelů. V řadě

[662] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 56.
[663] K jednotlivým modelům služeb cloudu a jejich kombinacím podrobněji SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 56 – 57.
[664] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, str. 57.
[665] Znám je případ úložiště Megaupload, jehož provozovatelé po celém světě po zahájení trestního stíhání v USA roku 2012 smazali ze serverů spolu s nelegálně sdíleným software i značný objem legálních soukromých dat uživatelů. Dostupné z https://en.wikipedia.org/wiki/Megaupload_legal_case [cit. 2016-03-21]. Překlad autorka.

případů mohou být ve skutečnosti požadovaná data uložena na zahraničních serverech. Nejčastěji se s podobnou situací setkáme u uživatelů rozšířených služeb společnosti Google. Bez statutární výjimky nedovolují zákony USA společnosti Google poskytnout obsah komunikace účastníka.[666] Data požadovaná orgánem dožadujícího se státu mohou být v USA uchovávána po maximální dobu 90 dní, s možností prodloužení o dalších 90 dní. Během této doby musí být dokončen proces mezinárodní právní pomoci, na jehož základě bude možné dožádání vyhovět a procesní úkon provést. Postup je natolik komplikovaný a časově náročný, že orgán činný v trestním řízení dožadujícího se státu od své žádosti obvykle zkrátka upustí.

Hodlá-li tedy orgán činný v trestním řízení získat přístup k datům nacházejícím se v cloudu, bude mít v případě dat uložených na zahraničních serverech stejné možnosti, jako v případě přeshraničního přístupu k uloženým počítačovým datům. Je-li stát smluvní stranou Úmluvy o počítačové kriminalitě, lze jej požádat dle čl. 29 Úmluvy o počítačové kriminalitě o urychlené uchování uložených počítačových dat. Úmluva o počítačové kriminalitě předpokládá aplikaci ustanovení na všechny typy služeb cloudu, vzít v potaz je ale nutné případná omezení právního řádu dožádaného státu, neboť provedení úkonu se obvykle řídí právem dožádaného státu.[667] Odlišnosti se mohou týkat zejména ochrany soukromí a práva na ochranu osobních údajů.

Závěrem kapitoly lze uvést některá doporučení Mezinárodní společnosti pro trestní právo. Žádný ze států není suverénní ve vztahu k veřejně přístupným počítačovým sítím. Státy by měly zvážit uzákonění povinnosti spolupráce pro ISP, v rámci níž by mělo být umožněno stopovat přenos dat, zpřístupnit hesla, odšifrovat data nebo instalovat vyhledávací programy za účelem vyšetřování trestného činu. Postup musí být však striktně podmíněn individuálním příkazem nezávislého soudu a dodržením principu proporcionality, při dostatečném šetření základních lidských práv a svobod. U extrateritoriálního výkonu pravomoci musí státy dodržet standardy lidskoprávní ochrany ve státě jednající autority i ve státě výkonu pravomoci. Průběh vyšetřování by měl být dokumentován, aby v případě nezákonného zásahu do základních práv a svobod bylo možno stát vést k odpovědnosti.[668]

---

[666] §§ 2702(a) Electronic Communications Privacy Act, 18 U.S.Code. Dostupné z https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121 [cit. 2017-01-29]. Překlad autorka.
[667] Srov. též § 49 ZMJS.
[668] XIX Congrès International de Droit Pénal. Société de l´information et de droit penal. Toulouse (France): La Revue Internationale de Droit Pénal, 2014, str. 620 – 623. Překlad autorka.

5.7. Předpokládaný vývoj

5.7.1. Alternativní cesty vůči mezinárodní justiční spolupráci

Pro postih počítačové kriminality v mezinárodním prostředí je stěžejní co nejrychlejší provedení procesního úkonu, kterým je nejčastěji přístup k digitálním datům. Přes časté využití se mezinárodní justiční spolupráce neukazuje nejefektivnějším prostředkem, jde-li o přístup k datům uloženým v zahraničí. Státy hledají jiné cesty, jak data získat a procesní úkon provést bez využití zdlouhavých procedur mezinárodní justiční spolupráce.

Podle Anny Marie Osuly lze tyto alternativní způsoby dosažení dat dělit do dvou skupin. Do první skupiny spadá formální i neformální spolupráce mezi státy, včetně sdílení mezinárodních informačních databází, spolupráce na úrovni společných institucí jakými je Europol, Interpol i Eurojust, ale i neformální přímá spolupráce orgánů činných v trestním řízení. Druhá skupina sestává z formální i neformální spolupráce orgánů státu s nestátními subjekty, jako jsou ISP. Spoluprací se zahraničními nestátními subjekty lze formální procedury mezinárodní spolupráce obejít a získat například přímý přeshraniční přístup k e-mailové schránce obviněného. Důsledky pro transparentnost a zákonnost trestního řízení jsou zcela jistě negativní. Dokud ovšem nebudou nedostatky rigidních forem mezinárodní justiční spolupráce vyřešeny, lze očekávat vzestupnou tendenci států ve využívání podobných operativních mechanismů, které předběžný souhlas cizího státu, z jehož území jsou data získána, nevyžadují.[669]

Právní debaty o podmínkách vyhovění ISP dožádání orgánů činných v trestním řízení cizího státu, podněcují i soudní kauzy. Ty ilustrují odlišnou interpretaci vnitrostátního i mezinárodního práva národními soudy, a to zpravidla ve prospěch potřeb vlastních orgánů činných v trestním řízení. Za povšimnutí stojí případ společnosti The Yahoo! Inc., který řešilo belgické soudnictví v roce 2013. V průběhu trestního stíhání podvodného jednání spáchaného skrze emailové účty společnosti The Yahoo! Inc., si belgický státní zástupce vyžádal dle belgického trestního řádu od ISP

[669] OSULA, Anna-Maria. *Accessing Extraterritorially Located Data: Options for States* [online]. Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2015. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options %20for%20States_Anna-Maria_Osula.pdf [cit. 2017-01-29]. Překlad autorka.

The Yahoo! Inc. informace o konkrétním uživateli emailového účtu. The Yahoo! Inc. odmítl státnímu zastupitelství požadovanou informaci poskytnout s poukázáním na skutečnost, že sídlo obchodní společnosti se nachází v USA a na území Belgie nemá společnost žádnou pobočku. Odvolací soud v Antverpách potvrdil povinnost ISP The Yahoo! Inc. poskytnout požadované údaje se zdůvodněním, že ISP se v Belgii virtuálně nachází a belgickému trestnímu právu proto podléhá, protože zde nabízí své služby elektronických komunikací.[670]

K opačnému závěru dospěl soudní spor v trestní věci týkající se příkazu k prohlídce emailového účtu spravovaného společností Microsoft Corporation, řešený soudy v USA v letech 2014 až 2016. Microsoft Corporation odmítl poskytnout na základě příkazu k prohlídce vydaného v trestním řízení v USA obsahová data uložená fyzicky na serverech společnosti v Irsku. Prvoinstanční soud The Federal District Court rozhodl o povinnosti Microsoft Corporation příkazu vyhovět s tím, že data jsou pod kontrolou společnosti. Microsoft Corporation se však odvolal a odvolací soud The United States Court of Appeals for the Second Circuit rozhodnutí prvoinstančního soudu zrušil s tím, že bez dalšího není možné příkaz k prohlídce uvedeným jednostranným způsobem mimo území USA vykonat.[671] Tímto rozhodnutím se tak postavil praxi orgánů USA popsané výše v případu Gorshkov-Ivanov.

Vzhledem k výše uvedeným skutečnostem lze očekávat, že právní debata o zákonnosti prostředků umožňujících provést v rámci trestního řízení procesní úkon mimo jurisdikci státu, aniž by došlo k využití mezinárodní justiční spolupráce, budou na mezinárodní úrovni pokračovat. Rigidní zdlouhavý proces mezinárodní justiční spolupráce nebude mít do budoucna šanci obstát, a to nejen v rámci postihu počítačové kriminality v mezinárodním prostředí. Abychom předešli různým alternativním způsobům jak data nacházející se v zahraničí získat, tedy způsobům ohrožujícím suverenitu států i zákonnost trestního řízení, bude zapotřebí novelizovat stávající formy mezinárodní justiční spolupráce tak, jak to učinila např. směrnice o útocích na

[670] OSULA, Anna-Maria. *Accessing Extraterritorially Located Data: Options for States* [online]. Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2015, str. 17. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options %20for%20States_Anna-Maria_Osula.pdf [cit. 2017-01-29]. Překlad autorka.
[671] Podrobněji https://digitalconstitution.com/2016/07/search-warrant-case-important-decision-people-everywhere/ [cit. 2017-01-29]. Překlad autorka.

informační systémy, která v členských státech EU vytvořila kontaktní síť umožňující rychlou reakci na žádost jiného členského státu EU.

5.7.2. Online sociální kontrola aneb counter-hacking

V rámci postihu počítačové kriminality stojí za povšimnutí aktivity tzv. online vigilantismu, označované i jako tzv. counter-hacking.[672] Jde o projev sociální kontroly ve virtuálním prostředí, která bývá leckdy efektivnější, nežli zakročení orgánů státní moci proti protiprávním aktivitám na Internetu. Jednotlivci i organizované supiny, které berou ochranu práva do vlastních rukou, se ovšem často dopustí protiprávní činnosti, nehledě na skutečnost, že převzetím pravomoci státních orgánů a vymáháním vlastního pojetí práva se dostávají do konfliktu se základy právního demokratického zřízení státu.

Proti některým formám počítačové trestné činnosti bojují vlastními silami jednotlivci i organizované skupiny. Čím hlubší jsou znalosti a hackerské dovednosti, tím citelnější a efektivnější je „škoda“ způsobená pachatelům v rámci „protiútoku“ ve virtuálním prostředí. Příkladem lze zmínit vyřazení z provozu webových stránek, distribuujících protiprávní škodlivý obsah (typicky dětskou pornografii). Aktivity jednotlivců a skupin v rámci online vigilantismu někdy připomínají vyřizování účtů mezi mafií, neboť jak skupiny bránící virtuální prostředí před škodlivým obsahem, tak i oběti jejich obrany, udržují leckdy aktivity v tajnosti a kybernetický útok policejním orgánům neoznamují. Obě strany se dopouští trestné činnosti, ať již jde o šíření škodlivého obsahu skrze Internet, o hacking, popřípadě o vydírání. Ani jedna ze stran nemá zájem na odhalení.

Organizovaná skupina známá pod názvem Anonymous, jež se dlouhodobě zaměřuje na boj proti distribuci dětské pornografie na Internetu, v dubnu roku 2013 dočasně vyřadila z provozu řadu webových stránek šířících materiál dětské pornografie. Uvést lze i případ indické softwarové společnosti podnikající ve filmovém průmyslu, která sama monitorovala Internet s ohledem na výskyt pirátských kopií filmových

[672] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 5. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

snímků od spřízněných tvůrců. V případě, že společnost nalezla odkaz na nelegálně sdílený film, zaslala hostujícímu serveru svůj požadavek na odebrání obsahu porušujícího autorská práva. Pakliže požadavku společnosti vyhověno nebylo, zaútočila na server masivním kybernetickým útokem typu DDoS.[673]

Přestože o aplikaci práva v rámci virtuálního prostředí již nemáme pochyb, jeho faktická vynutitelnost zůstává přetrvávajícím problémem. Kyberprostor proto leckdy připomíná období středověku, kdy bylo právo bráno jednotlivci i skupinami ve smyslu svépomoci do vlastních rukou, neboť stát nebyl schopen zajistit obyvatelstvu odpovídající ochranu. Counter-hacking se stává prostředkem svépomoci. Můžeme se jen domnívat, že svépomoc bude s dalším přesunem společenských aktivit do virtuálního prostředí stále běžnější.

[673] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 4 - 5. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

ZÁVĚR

Právní regulace počítačové kriminality je oblastí, v níž dochází ke střetu vědeckého pokroku s mnohdy rigidní právní úpravou. Trestní právo je nuceno reagovat na technologický vývoj a bez hlubší znalosti charakteristických vlastností počítačové kriminality a kybernetického prostředí se již neobejde. Jako stěžejní se ukazuje požadavek spolupráce s odborníky z oblasti informačních a výpočetních technologií. Do budoucna bude rovněž vhodné zaměřit se na další studium počítačové kriminality a jejích projevů. Cílem výzkumu by se měla stát i osoba pachatele počítačové kriminality a jeho oběti, neboť v této oblasti hlubší poznatky již delší dobu chybí, ačkoli by bezesporu přispěly k efektivnějšímu postihu počítačové kriminality a k její prevenci.

Při postihu počítačové kriminality se střetáváme s řadou specifických situací, které jsou důsledkem typických vlastností informačních a komunikačních technologií i globálního virtuálního prostředí. Trestní právo se s technologickým vývojem a globálním dosahem virtuálního světa vyrovnává spíše pomaleji, jak dokládá i rigorózní práce v rozboru některých jeho procesních instrumentů, které dostatečně nereflektují specifika počítačové kriminality.

Počítačová trestná činnost není jen záležitostí jednotlivců pohybujících se ve sféře komunikační a výpočetní techniky. V určitých směrech lze hovořit o vývoji počítačové kriminality v trestnou činnost organizovaného charakteru, zaměřenou na dosahování co nejvyššího zisku. Kybernetickou kriminalitu v současnosti rozvíjejí pachatelé hledající v ní hlavní zdroj obživy, což vede k hlubšímu propojení s organizovaným zločinem.[674] Organizovaný zločin tedy do virtuálního prostředí pronikl a čerpá z jeho výhod stejně jako ostatní. Útoky na informační systémy mohou být vedle jednotlivců a organizovaných zločineckých skupin páchány i orgány státu. Kybernetické útoky mohou být součástí politické strategie či formou teroristického útoku. Počítačová kriminalita tedy zahrnuje širokou škálu kriminálních jevů, od trestné činnosti využívající počítače toliko jako nástroje, až k útokům spadajícím pod

[674] POŽÁR, Josef. Kybernetická kriminalita a její trendy. In: MAREŠOVÁ, Alena (eds.). *Analýza trendů kriminality v roce 2014: sborník statí pracovníků IKSP a časové řady vybraných ukazatelů kriminality*. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 72.

kyberterorismus. Podřazení kybernetického útoku pod kyberterorismus musí být striktně odůvodněno splněním všech definičních znaků činu teroristického.

Globální virtuální prostředí je spjato s počítačovou trestnou činností, u které je vzhledem k její podstatě často přítomen mezinárodní prvek. Mezinárodní společenství uznává globální charakter počítačové kriminality. Orgány činné v trestním řízení se při postihu počítačové trestné činnosti neobejdou bez spolupráce s příslušnými orgány cizích států. Ačkoli o aplikaci trestního práva na virtuální prostředí již není pochyb, problém vynutitelnosti právních norem přetrvává. Pro postih počítačové kriminality je mezinárodní spolupráce klíčová, neboť zajišťuje faktickou realizaci právních norem mimo jurisdikci daného státu. Mezinárodní spolupráce jako taková se v podstatě stává podmínkou zachování působnosti práva v globálním virtuálním prostředí.[675]

Úpravu mezinárodní justiční spolupráce nalezneme v mnohých bilaterálních i multilaterálních mezinárodních smlouvách. Zejména mezi členskými státy Evropské unie lze hovořit nejen o harmonizaci trestněprávních předpisů, nýbrž i o prohlubující se spolupráci jednotlivých států. Přesto zůstává výměna informací, dosažitelnost důkazů ze zahraničí a efektivita mezinárodní justiční spolupráce v rámci boje proti počítačové trestné činnosti hodnocena neuspokojivě. Experti z oblasti justice poukazují na nedostatečné možnosti využití přímého právního styku s cizinou, příliš formalizované způsoby mezinárodní justiční spolupráce v trestních věcech a zdlouhavý, až liknavý přístup některých států k mezinárodní právní pomoci.[676]

S problematickým uplatňováním některých forem mezinárodní justiční spolupráce se objevuje i snaha orgánů činných v trestním řízení nevyhovující tradiční právní úpravu obcházet. Uvedený přístup je již patrný u přeshraniční prohlídky skrze počítačovou síť. Procesních úkonů je dosaženo díky různým metodám neformální spolupráce, které představují alternativní a jednodušší způsob získání důkazního prostředku v podobě digitálních dat nacházejících se v zahraničí. Tato praxe však v mezinárodním prostředí ohrožuje princip suverenity a je v rozporu se základním principem trestního řízení - se zásadou řádného zákonného procesu. Jestliže se trestní právo chce vyhnout riziku rozvoje podobných metod orgánů činných v trestním řízení,

[675] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, str. 113.
[676] CEJP, Martin. Organizovaný zločin v České republice v mezinárodním kontextu. *Trestněprávní revue*. 2016, 15(4), str. 91.

rigidní zdlouhavý proces mezinárodní justiční spolupráce v rámci postihu počítačové kriminality do budoucna nemá šanci obstát.

SEZNAM PŘEDPOKLÁDANÉ LITERATURY A PRAMENŮ

Učebnice

GŘIVNA, Tomáš; SCHEINOST, Miroslav; ZOUBKOVÁ, Ivana. *Kriminologie*. 4., aktualiz. vyd. Praha: Wolters Kluwer, 2014.

JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 6. aktualizované vydání. Praha: Leges, 2016.

JELÍNEK, Jiří; DANKOVÁ, Katarína; NAVRÁTILOVÁ, Jana; PELC, Vladimír; ŘÍHA, Jiří; STEJSKAL, Vojtěch. *Trestní právo hmotné: obecná část, zvláštní část*. 5. aktualizované a doplněné vydání. Praha: Leges, 2016.

JELÍNEK, Jiří. *Trestní právo procesní*. 4. aktualiz. a dopl. vyd. Praha: Leges, 2016.

JELÍNEK, Jiří. *Trestní právo Evropské unie*. Praha: Leges, 2014.

KAMLACH, Milan; REPÍK, Bohumil. *Mezinárodní spolupráce v trestním a občanskoprávním řízení*. Praha: Panorama, 1990.

KLIP, André. *European criminal law: an integrative approach*. 2. vyd. Cambridge: Intersentia, 2012.

KLOUČKOVÁ, Světlana; FENYK, Jaroslav. *Mezinárodní justiční spolupráce v trestních věcech*. 2., aktualiz. a dopl. vyd. Praha: Linde, 2005.

KONRÁD, Zdeněk; PORADA, Viktor; STRAUS, Jiří; SUCHÁNEK, Jaroslav. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2015.

MADAR, Zdeněk. *Slovník českého práva*. 3. rozš. a podstatně přeprac. vyd. Praha: Linde, 2002.

POLČÁK, Radim; ŠKOP, Martin; MACEK, Jakub. *Normativní systémy v kyberprostoru: (úvod do studia)*. 1. vyd. Brno: Masarykova univerzita, 2005.

PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016.

PORADA, Viktor; STRAUS, Jiří. *Kriminalistika: (výzkum, pokroky, perspektivy)*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013.

ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef. *Trestní právo procesní*. 4., přeprac. vyd. V Praze: C.H. Beck, 2013.

TICHÝ, Luboš. *Evropské právo*. 5., přeprac. vyd. V Praze: C.H. Beck, 2014.

Monografie

AWAN, Imran; BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012.

BALOUN, Vladimír. *Organizovaný zločin a jeho možné projevy ve finančním sektoru ekonomiky: dílčí závěrečná studie úkolu "Výzkum organizovaného zločinu v České republice II"*. Praha: Institut pro kriminologii a sociální prevenci, 1999.

BRENNER, Susan W. *Cybercrime and the law: challenges, issues, and outcomes* [online]. Boston: Northeastern University Press, 2012. Dostupné z http://site.ebrary.com/lib/cuni/Doc?id=10620947

BRENNER, Susan. *Cyberthreats and the decline of the nation-state* [online]. Oxfordshire, England: Routledge, 2014, str. 16. ISBN 9780203709207. Dostupné z http://site.ebrary.com/lib/cuni/Doc?id=10848006

CASTELLS, Manuel. *The internet galaxy: reflections on the internet, business, and society*. 1. vyd. Oxford: Oxford University Press, 2003.

CEJP, Martin. *Vývoj organizovaného zločinu na území České republiky*. 1. vyd. Praha: Institut pro kriminologii a sociální prevenci, 2010.

CEJP, Martin; BLATNÍKOVÁ, Šárka; HÁKOVÁ, Lucie; HOLAS, Jakub; TRÁVNÍČKOVÁ, Ivana; VLACH, Jiří. *Společenské zdroje vývoje organizovaného zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2015.

COUFALOVÁ, Tereza. *Justiční a policejní spolupráce v Evropské unii*. V Praze: Univerzita Karlova, 2015.

EICHLER, Jan. *Terorismus a války v době globalizace*. 2., dopl. vyd. Praha: Karolinum, 2010.

GLENNY, Misha. *Temný trh: kyberzloději, kyberpolicisté a vy*. 1. vyd.. Praha: Argo, 2013.

GOUNEV, Philip; RUGGIERO, Vincenzo (eds.). *Corruption and Organized Crime in Europe: Illegal partnerships*. New York: Routledge, 2012.

HERCZEG, Jiří. *Trestné činy z nenávisti: právní monografie*. 1. vyd. Praha: ASPI, 2008.

HOBBES, Thomas; CHOTAŠ, Jiří; Zdeněk, MASOPUST; BARABAS, Marina (eds.). *Leviathan, aneb, Látka, forma a moc státu církevního a politického*. 1. vyd. Překlad Karel Berka. Praha: OIKOYMENH, 2009.

JELÍNEK, Jiří; GŘIVNA, Tomáš. *Poškozený a oběť trestného činu z trestněprávního a kriminologického pohledu*. Praha: Leges, 2012.

JELÍNEK, Jiří, (ed.). *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014.

JELÍNEK, Jiří; IVOR, Jaroslav. *Trestní právo Evropské unie a jeho vliv na právní řád České republiky a Slovenské republiky*. 1. vyd. Praha: Leges, 2015.

JELÍNEK, Jiří; ŘÍHA, Jiří; SOVÁK, Zdeněk. *Rozhodnutí ve věcech trestních: se vzory rozhodnutí soudů a podání advokátů*. 3., aktualiz. a přeprac. vyd. Praha: Leges, 2015.
JELÍNEK, Jiří. *Základní zásady trestního řízení - vůdčí ideje českého trestního procesu: sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2016, trestní sekce*. Praha: Leges, 2016.
JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou: zákon o soudnictví ve věcech mládeže, zákon o trestní odpovědnosti právnických osob a řízení proti nim, advokátní tarif*. 6. aktualizované vydání. Praha: Leges, 2016.
JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007.
KOLOUCH, Jan; VOLEVECKÝ, Petr. *Trestněprávní ochrana před kybernetickou kriminalitou*. 1. vyd. Praha: Policejní akademie České republiky v Praze, 2013.
KOOPS, Bert-Jaap (ed.). *Cybercrime and jurisdiction: a global survey*. 1. vyd. The Hague: T.M.C. Asser press, 2006.
MARKUSOVÁ, Renata; NETÍK, Karel. *Výzkum pachatelů trestné činnosti spáchané v organizované skupině: dílčí studie v rámci výzkumu struktury, forem a možností postihu organizovaného zločinu v ČR*. Praha: Institut pro kriminologii a sociální prevenci, 1997.
PAOLI, Letizia (ed.). *The Oxford handbook of organized crime*. [1st ed.]. Oxford: Oxford University Press, 2014.
POLČÁK, Radim. *Právo na internetu: spam a odpovědnost ISP*. 1. vyd. Brno: Computer Press, 2007.
POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012.
REPÍK, Bohumil. *Evropská úmluva o lidských právech a trestní právo*. 1. vyd. Praha: Orac, 2002.
SCHEINOST, Miroslav; NETÍK, Karel. *Český organizovaný zločin v mezinárodním kontextu*. Praha: Institut pro kriminologii a sociální prevenci, 2010.
SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. *Počítačové právo*. 1. vyd. Praha: C.H. Beck, 1995.
SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. vyd. Praha: C.H. Beck, 2004.
SMEJKAL, Vladimír. *Kybernetická kriminalita*. 1. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015.
SOULEIMANOV, Emil. *Organizovaný zločin*. Praha: Auditorium, 2012.
WALL, David. *Cybercrime: the transformation of crime in the information age*. 1. vyd. Cambridge: Polity, 2007.
YAR, Majid. *Cybercrime and society: crime and punishment in the information age*. 2. vyd. Thousand Oaks, CA: SAGE Publications, 2013.

Komentáře

JELÍNEK, Jiří. *Zákon o obětech trestných činů: komentář s judikaturou*. 2. dopl. a rozš. vyd. Praha: Leges, 2014.
KUBÍČEK, Miroslav. *Zákon o mezinárodní justiční spolupráci ve věcech trestních: komentář*. Praha: Wolters Kluwer, 2014.
ŠÁMAL, Pavel. *Trestní zákoník I. § 1 – 138. Komentář*. 2. vyd. Praha: C.H. Beck, 2012.
ŠÁMAL, Pavel. *Trestní zákoník II. § 140 – 421. Komentář*. 2. vyd. Praha: C.H. Beck, 2012.
ŠÁMAL, Pavel. *Trestní řád I. § 1 – 156. Komentář*. 7., dopl. a přeprac. vyd. Praha: C.H. Beck, 2013.
ŠÁMAL, Pavel. *Trestní řád II. § 157 – 314s. Komentář*. 7., dopl. a přeprac. vyd. Praha: C.H. Beck, 2013.
VANGELI, Benedikt. *Zákon o Policii České republiky: komentář*. 2. vyd. V Praze: C.H. Beck, 2014.

Časopisecké články a příspěvky ve sbornících

ABELOVSKÝ, Tomáš. Zaistenie elektronického dôkazu vo svetle rekodifikácie trestného poriadku. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2015, 6(11).
ARNBAK, Axel; VAN EIJK, Nico. Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain. *TRPC* [online]. 2012. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409 [cit. 2016-04-13].
AUSTEN, John. Praktické příklady vyšetřování počítačové kriminality. *Kriminalistická společnost*. Praha, 1991, (3).
BRENNER, Susan. Cybercrime investigation and prosecution: the role of penal and procedural law. *E law* [online]. 2001, 8(2). Dostupné z http://www.austlii.edu.au/au/journals/MurUEJL/2001/8.html [cit. 2016-02-22].
BRENNER, Susan; KOOPS, Bert-Jaap. Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law* [online]. 2004, 4(1). Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507 [cit. 2016-03-10].
BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 5. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]
CEJP, Martin. Organizovaný zločin v České republice v mezinárodním kontextu. *Trestněprávní revue*. 2016, 15(4).

COUFALOVÁ, Bronislava. Organizovaný zločin – vymezení pojmu. In: JELÍNEK, Jiří, ed. *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014.
GRABOSKY, Peter. Virtual criminality: Old wine in new bottles? *Social and legal studies* [online]. 2001, (10). Dostupné z http://sls.sagepub.com/content/10/2/243.full.pdf [cit. 2016-04-15].
GŘIVNA, Tomáš. Závazky k ochraně kyberprostoru vyplývající z evropského a mezinárodního práva. *Acta Universitatis Carolinae. Iuridica*. Praha: Univerzita Karlova, 2008, 2008(4).
GŘIVNA, Tomáš. Existují virtuální trestné činy? In: VANDUCHOVÁ, Marie; GŘIVNA, Tomáš (eds.). *Pocta Otovi Novotnému k 80. narozeninám*. 1. vyd. Praha: ASPI, 2008.
GŘIVNA, Tomáš. K ustanovením Úmluvy o počítačové kriminalitě. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008.
HERCZEG, Jiří. Extremismus a hranice svobody projevu na internetu. *Acta Universitatis Carolinae. Iuridica*. Praha: Univerzita Karlova, 2008, 2008(4).
HERCZEG, Jiří. Zásada „nemo tenetur“ a práva obviněného v trestním řízení. *Bulletin advokacie*. 2010, (1 - 2).
CHMELÍK, Jan; PORADA, Viktor. Vybrané problémy vyšetřování a dokazování počítačové kriminality II. In: *Identifikace potřeb právní praxe jako teoretický základ pro rozvoj kriminalistických a právních specializací*. 1. vyd. Karlovy Vary: Vysoká škola Karlovy Vary, o. p. s., 2011.
JELÍNEK, Jiří; PELC, Vladimír. Zákon o obětech trestných činů - jeho nedostatky a možnosti řešení. *Bulletin advokacie: stavovský časopis české advokacie*. 2015, str. 19-23.
JELÍNEK, Jiří. Edwin H. Sutherland - k odkazu zakladatele moderní americké kriminologie pro studium organizované kriminality. *Pocta prof. JUDr. Květoslavu Růžičkovi, CSc. k 70. narozeninám*. Praha: Wolters Kluwer, 2016.
KENNEY, Michael. Cyber-Terrorism in a Post-Stuxnet World. *Orbis*. 2015, 59(1).
KERR, Orin. Searches and Seizures in a Digital World. *Harvard Law Review* [online]. 2005, 119(531). Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=697541 [cit. 2016-02-24].
KIGERL, Alex. Infringing Nations: Predicting Software Piracy Rates, BitTorrent Tracker Hosting, and P2P File Sharing Client. *International Journal of Cyber Criminology* [online]. 2013, 7(1). Dostupné z http://www.cybercrimejournal.com/Alex2013janijcc.pdf [cit. 2016-03-17].
KOOPS, Bert-Jaap. The Internet and its Opportunities for Cybercrime: Tilburg Law School Research Paper No. 09/2011. *Transnational Criminology Manual* [online]. Nijmegen: WLP, 2010, (1). Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1738223 [cit. 2016-02-18].
KUČERA, Pavel. Kdo není odposloucháván, jakoby nebyl. *Trestní právo*. 2014, 18(3).

LASTOWKA, Greg; HUNTER, Dan. Virtual Crime. *New York Law School Law Review* [online]. 2004. Dostupné z http://ssrn.com/abstract=564801 [cit. 2016-02-17].
LYC, Chan. *Cybercrime in the Greater China Region: Regulatory Response and Crime Prevention across the Taiwan Strait* [online]. Edward Elgar, 2012. [cit. 2016-12-29].
MENDEL, Aleš. Vyšetřování počítačové kriminality. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008.
O´FLOINN, Micheál. It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe. *Computer Law & Security Review* [online]. 2013, 29(5). Dostupné z http://www.sciencedirect.com/science/article/pii/S0267364913001428 [cit. 2016-03-20].
OSULA, Anna-Maria. *Accessing Extraterritorially Located Data: Options for States* [online]. Tallin: NATO Cooperative Cyber Defence Centre of Excellence, 2015. Dostupné z https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options %20for%20States_Anna-Maria_Osula.pdf [cit. 2017-01-29].
PAVLIKOVÁ, Miroslava. Estonsko-ruský incident v kontextu kyberterorismu. *Global Politics: Časopis pro politiku a mezinárodní vztahy* [online]. 2014. Dostupné z http://www.globalpolitics.cz/clanky/estonsko-rusky-incident-v-kontextu-kyberterorismu [cit. 2016-04-09].
PICOTTI, Lorenzo. *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l´informatique*. Ramonville Sainte Agne: Révue internationale de droit pénal, 2006.
PODGOR, Ellen. Computer Crimes and the USA Patriot Act. *Criminal Justice Magazine* [online]. 2002, 17(2). Dostupné z http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_17_2_crimes.html [cit. 2016-03-10].
POLČÁK, Radim. K problému působnosti trestního práva na internetu. *Acta Universitatis Carolinae. Iuridica*. 2008, 2008(4).
POLČÁK, Radim. Autoritativní regulace kyberprostoru a legitimita trestního práva. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. 1. vyd. Praha: Auditorium, 2008.
POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2015, 6(11).
PORADA, Viktor (ed.). *Identifikace potřeb právní praxe jako teoretický základ pro rozvoj kriminalistických a právních specializací: Identifying the requirements of legal practice as a theoretical basis for advancing criminalistic and legal specializations : sborník vědeckých prací*. 1. vyd. Karlovy Vary: Vysoká škola Karlovy Vary, 2011.
PORADA, Viktor; ŠEDIVÝ, Petr. Kriminalistické a forenzní aspekty počítačové (kybernetické) kriminality. *Karlovarská právní revue*. 2011, 7(2).

POŠÍKOVÁ, Lenka. Získání telekomunikačních dat jako nástroj v boji s internetovou kriminalitou. *Acta Universitatis Carolinae. Iuridica*. 2013, 2012(4).
POŽÁR, Josef. Příspěvek k rozvoji informatiky v oblasti kybernetické kriminality. *Bezpečnostní teorie a praxe: periodikum Policejní akademie České republiky*. 2008, Díl I.(Zvláštní číslo).
POŽÁR, Josef. Kybernetická kriminalita a její trendy. In: MAREŠOVÁ, Alena (eds.). *Analýza trendů kriminality v roce 2014: sborník statí pracovníků IKSP a časové řady vybraných ukazatelů kriminality*. Praha: Institut pro kriminologii a sociální prevenci, 2015.
REDIKER, Ezekiel. The Incitement of Terrorism on the Internet: Legal Standards, Enforcement, and the Role of the European Union. *Michigan Journal of International Law*. 2015, 36(2).
SEITZ, Nicolai. Transborder Search: A New Perspective in Law Enforcement? *Yale Journal of Law and Technology* [online]. 2005, 7(1). Dostupné z http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1016&context=yjolt [cit. 2016-03-10].
SIEBER, Ulrich. *General report on Internet crimes: for the 18th International Congress of the International Academy of Comparative Law*. Washington D.C.: International Academy of Comparative Law, 2010.
SOTOLÁŘ, Alexander; PÚRY, František; WORATSCHOVÁ, Vladana. Posuzování policejní provokace. *Trestněprávní revue*. 2002, 1(11).
STUPKOVÁ, Lucie. Institut spolupracujícího obviněného a korunního svědka ve světle základních zásad trestního práva procesního. In: JELÍNEK, Jiří (ed.). *Základní zásady trestního řízení – vůdčí ideje českého trestního procesu.* Praha: Leges, 2016.
SVOBODA, Pavel. Kadi 2013: tečka za jednou kapitolou protiteroristické judikatury SDEU? *Právní rozhledy*. 2013, (23 - 24).
SZABOVÁ, Eva. Boj s organizovanou kriminalitou na úrovni Európskej únie – aktuálny vývoj. In: JELÍNEK, Jiří, (ed.). *Organizovaný zločin: (trestněprávní, trestněprocesní a kriminologické aspekty) : sborník příspěvků z mezinárodní vědecké konference Olomoucké právnické dny, květen 2014, trestní sekce*. Praha: Leges, 2014.
TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy*. Brno: Masarykova univerzita, 2010, 1(1).
VON LAMPE, Klaus. Explaining the Emergence of the Cigarette Black Market in Germany. In: VAN DUYNE, Petrus; VON LAMPE, Klaus; VAN DIJCK, Maarten; NEWELL, James (eds.). *The Organised Crime Economy*. Wolfe Legal, 2005.
WALDEN, Ian. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Queen Mary School of Law Legal Studies Research Paper No. 74/2011* [online]. 2011. Dostupné z http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067 [cit. 2016-03-21].

ZAVRŠNIK, Aleš. Definiční problémy a kriminologická specifika kyberzločinu. In: GŘIVNA, Tomáš; POLČÁK, Radim (eds.). *Kyberkriminalita a právo*. Praha: Auditorium, 2008.

Internetové zdroje

DANCHEV, Dancho. Study finds an average price for renting a botnet [online]. Dostupné z http://www.zdnet.com/article/study-finds-the-average-price-for-renting-a-botnet/ [cit. 2016-02-16].
EUROPOL. Changes in modus operandi of Islamic State terrorist attacks.[online]. The Hague, 2016 Dostupné z https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-terrorist-attacks [cit. 2017-01-31]
FATF. Veřejné prohlášení ze dne 21. října 2016 – rizikové jurisdikce. Dostupné z http://www.mfcr.cz/cs/archiv/agenda-financniho-analytickeho-utvaru/novinky-fau/2016/verejne-prohlaseni-fatf-z-21-rijna-2016-26767 [cit. 2017-01-09].
JARRET, Marshall; BAILIE, Michael. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations [online]. Office of Legal Education Executive Office for United States Attorneys, 2009. Dostupné z https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [cit. 2016-03-20].
KAISER, Robert. The birth of cyberwar. *Political Geography* [online]. 2015, 46(5), str. 11 - 20 Dostupné z http://www.sciencedirect.com.ezproxy.techlib.cz/science/article/pii/S0962629814000961 [cit. 2016-11-20]
KONDRATOVA, Irina Kiri. Darknet - Internetové podsvětí [online]. Dostupné z http://cemolid.blogspot.cz/2015/04/darknet-internetove-podsveti.html [cit. 2016-03-17].
LAPRES, Daniel Arthur. Webliography on the Yahoo case [online]. Dostupné z http://www.lapres.net/yahweb.html [cit. 2016-03-15].
LEYDEN, John. UK finally ratifies Cybercrime Convention during Obama visit: No Russia + No China = No point. *The Register* [online]. Dostupné z http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/ [cit. 2016-03-18].
OWANO, Nancy. Samsung Smart TVs subject of blog on traffic intercept findings [online]. Dostupné z http://techxplore.com/news/2015-02-samsung-smart-tvs-subject-blog.html [cit. 2016-02-18].
SINGER, Miroslav. Bezpečnost internetových plateb a virtuální „měny“ z pohledu ČNB. Fórum Zlaté koruny, ČNB, 2015. Dostupné na http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/verejnost/pro_media/konferen

ce_projevy/vystoupeni_projevy/download/singer_20150421_zlata_koruna.pdf [cit. 2017-01-09].
STARR, Michelle. First man convicted in child predator sting with virtual girl Sweetie [online]. Dostupné z http://www.cnet.com/news/first-man-convicted-in-child-predator-sting-with-virtual-girl-sweetie/ [cit. 2016-03-26].

Judikatura a rozhodovací praxe (řazena dle instituce a chronologicky)

Evropský soud pro lidská práva:
Rozsudek Evropského soudu pro lidská práva ve věci Saunders v. The United Kingdom ze dne 17. 12. 1996.
Soudní dvůr Evropské unie:
Rozhodnutí Soudního dvora EU ve spojených věcech C-293/12 a C-594/12, ze dne 8. 4. 2014.
Ústavní soud ČR:
Nález Ústavního soudu, sp. zn. I. ÚS 290/98, ze dne 7. 12. 1999.
Nález Ústavního soudu, sp. zn. III. ÚS 597/99, ze dne 22. 6. 2000.
Nález Ústavního soudu, sp. zn. II. ÚS 502/2000, ze dne 22. 1. 2001.
Usnesení Ústavního soudu, sp. zn. IV. ÚS 2/02, ze dne 28. 3. 2002.
Nález Ústavního soudu ČR, sp. zn. I ÚS 3038/07-1, ze dne 29. 2. 2008.
Nález Ústavního soudu, sp. zn. Pl. ÚS 24/10, ze dne 22. 3. 2011.
Usnesení Ústavního soudu, sp. zn. IV. ÚS 3225/09, ze dne 14. 12. 2011.
Nález Ústavního soudu, sp. zn. Pl. ÚS 24/11, ze dne 20. 12. 2011.
Nejvyšší soud ČR:
Usnesení Nejvyššího soudu České republiky, sp. zn. 2 Tzn 63/95, ze dne 14. 12. 1995.
Rozsudek Nejvyššího soudu, sp. zn. 4 Tz 265/2000, ze dne 16. 1. 2001.
Rozsudek Nejvyššího soudu, sp. zn. 4 Tz 106/2002, ze dne 26. 3. 2003.
Usnesení Nejvyššího soudu, sp. zn. 5 Tdo 794/2004, ze dne 15. 7. 2004.
Usnesení Nejvyššího soudu, sp. zn. 11 Tcu 29/2006, ze dne 24. 5. 2006.
Usnesení Nejvyššího soudu, sp. zn. 4 Pzo 1/2010, ze dne 10. 14. 2010.
Usnesení Nejvyššího soudu, sp. zn. 8 Tdo 1584/2010, ze dne 26. 1. 2011.
Stanovisko Nejvyššího soudu, sp. zn. Tpjn 306/2014, ze dne 25. 6. 2015, uveřejněné pod číslem 35/2015 Sbírky soudních rozhodnutí a stanovisek.
Vrchní soudy ČR:
Usnesení Vrchního soudu v Olomouci, sp. zn. 5 To 202/2002, ze dne 22. 7. 2003.
Krajské soudy ČR:
Usnesení Krajského soudu v Hradci Králové, sp. zn. 23Co 500/2007, ze dne 27. 10. 2007.
Cizozemské soudy:
Rozhodnutí Permanent Court of International Justice, Ser. A, No. 10, 1927.

Rozsudek Tribunal de Grande Instance de Paris, ve věci Yahoo!, Inc., ze dne 20. 11. 2000.
Rozhodnutí Bundesgerichtshof, sp. zn. 1 StR 184/00, ze dne 12. 12. 2000.
Rozhodnutí Královského soudního dvora, sp. zn. 2009.04020 B5, ze dne 29. 1. 2010.

Právní předpisy (ve znění pozdějších předpisů)

Veškeré právní předpisy Evropské unie jsou dostupné na http://eur-lex.europa.eu/homepage.html?locale=cs.

ČESKO. Ústavní zákon č. 1 ze dne 28. prosince 1992 Ústava České republiky. In: *Sbírka zákonů České republiky*. 1993, částka 1.
ČESKO. Usnesení předsednictva České národní rady č. 2 ze dne 28. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů České republiky*. 1993, částka 1.
ČESKO. Zákon č. 141 ze dne 9. prosince 1961 o trestním řízení soudním (trestní řád). In: *Sbírka zákonů České republiky*. 1961, částka 66.
ČESKO. Zákon č. 40 ze dne 9. února 2009 trestní zákoník. In: *Sbírka zákonů České republiky*. 2009, částka 11.
ČESKO. Zákon č. 104 ze dne 20. března 2013 o mezinárodní justiční spolupráci ve věcech trestních. In: *Sbírka zákonů České republiky*. 2013, částka 47.
ČESKO. Zákon č. 218 ze dne 25. června 2003 o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže). In: *Sbírka zákonů České republiky*. 2003, částka 79.
ČESKO. Zákon č. 36 ze dne 6. dubna 1967 o znalcích a tlumočnících. In: *Sbírka zákonů České republiky*. 1967, částka 14.
ČESKO. Zákon č. 127 ze dne 31. března 2005 o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *Sbírka zákonů České republiky*. 2005, částka 43.
ČESKO. Zákon č. 273 ze dne 11. srpna 2008 o Policii České republiky. In: *Sbírka zákonů České republiky*. 2008, částka 91.
ČESKO. Zákon č. 181 ze dne 29. srpna 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2014, částka 75.
ČESKO. Zákon č. 412 ze dne 18. října 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005, částka 143.
ČESKO. Zákon č. 45 ze dne 30. ledna 2013 o obětech trestných činů a o změně některých zákonů. In: *Sbírka zákonů České republiky*. 2013, částka 20.
ČESKO. Zákon č. 480 ze dne 7. září 2004 o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In: *Sbírka zákonů České republiky*. 2004, částka 166.

ČESKO. Zákon č. 86 ze dne 17. dubna 2015, kterým se mění zákon č. 279/2003 Sb., o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony. In: *Sbírka zákonů České republiky*. 2015, částka 37.
ČESKO. Zákon č. 121 ze dne 7. dubna 2000 o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). In: *Sbírka zákonů České republiky*. 2000, částka 1658.
ČESKO. Zákon č. 89 ze dne 22. března 2012 občanský zákoník. In: *Sbírka zákonů České republiky*. 2012, částka 33.
ČESKO. Zákon č. 101 ze dne 4. dubna 2000 o ochraně osobních údajů. In: *Sbírka zákonů České republiky*. 2000, částka 32.
ČESKO. Zákon č. 289 ze dne 16. června 2005 o Vojenském zpravodajství. In: *Sbírka zákonů České republiky*. 2005, částka 104.
ČESKO. Zákon č. 154 ze dne 7. července 1994 o Bezpečnostní informační službě. In: *Sbírka zákonů České republiky*. 1994, částka 49.
EVROPSKÁ UNIE. Smlouva ze dne 26. října 2012 o fungování Evropské unie.
EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV.
EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2011/92/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje Rámcové rozhodnutí Rady 2004/68/SVV.
EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech.
EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2014/42/EU ze dne 3. dubna 2014 o zajišťování a konfiskaci nástrojů a výnosů z trestné činnosti v Evropské unii.
EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).
EVROPSKÁ UNIE. Rámcové rozhodnutí Rady EU 2002/475/SVV ze dne 13. června 2002 o boji proti terorismu.
EVROPSKÁ UNIE. Rámcové rozhodnutí Rady EU 2008/919/SVV ze dne 28. listopadu 2008, kterým se mění rámcové rozhodnutí 2002/475/SVV o boji proti terorismu.
EVROPSKÁ UNIE. Rozhodnutí Rady 2005/671/SVV ze dne 20. září 2005 o výměně informací a spolupráci v oblasti teroristických trestných činů.
EVROPSKÁ UNIE. Úmluva ze dne 29. května 2000 o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 55/2006 Sb. m. s.
EVROPSKÁ UNIE. Protokol ze dne 16. října 2001 k Úmluvě o vzájemné pomoci v trestních věcech mezi členskými státy Evropské unie. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 56/2006 Sb. m. s.

EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2005/60/ES ze dne 26. října 2005 o předcházení zneužití finančního systému k praní peněz a financování terorismu.
EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2015/849/EU ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady 648/2012/EU a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES.
EVROPSKÁ UNIE. Návrh směrnice Evropského parlamentu a Rady o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí 2002/475/SVV o boji proti terorismu.
RADA EVROPY. Úmluva Rady Evropy č. 5 ze dne 4. listopadu 1950 o ochraně lidských práv a základních svobod. Federálním ministerstvem zahraničních věcí ČSFR vyhlášena pod č. 209/1992 Sb.
RADA EVROPY. Úmluva Rady Evropy č. 30 ze dne 20. dubna 1959, Evropská úmluva o vzájemné pomoci ve věcech trestních. Federálním ministerstvem zahraničních věcí ČSFR vyhlášena pod č. 550/1992 Sb.
RADA EVROPY. Úmluva Rady Evropy č. 99 ze dne 17. března 1978, Dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 31/1997 Sb.
RADA EVROPY. Úmluva Rady Evropy č. 182 ze dne 8. listopadu 2001, Druhý dodatkový protokol k Evropské úmluvě o vzájemné pomoci ve věcech trestních. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 48/2006 Sb. m. s.
RADA EVROPY. Úmluva Rady Evropy č. 185 ze dne 23. listopadu 2001 o počítačové kriminalitě. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 104/2013 Sb. m. s.
RADA EVROPY. Dodatkový protokol č. 189 ze dne 28. ledna 2003 k Úmluvě o počítačové kriminalitě, o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 9/2015 Sb. m. s.
RADA EVROPY. Úmluva Rady Evropy č. 201 ze dne 25. října 2007 o ochraně dětí před sexuálním vykořisťováním a zneužíváním. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 59/2016 Sb. m. s.
RADA EVROPY. Úmluva Rady Evropy č. 90 ze dne 27. ledna 1977 o potlačování terorismu. Sdělení federálního ministerstva zahraničních věcí ČSFR č. 552/1992 Sb.
RADA EVROPY. Úmluva Rady Evropy č. 196 ze dne 16. května 2005 o prevenci terorismu. Dostupná z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196/signatures?p_auth=GS4aFhEO [cit. 2017-01-31].
RADA EVROPY. Úmluva Rady Evropy č. 217 ze dne 22. října 2015, dodatkový protokol k Úmluvě Rady Evropy o prevenci terorismu. Dostupný z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/217 [cit. 2017-01-31].

ORGANIZACE SPOJENÝCH NÁRODŮ. Opční protokol ze dne 19. prosince 2011 k Úmluvě OSN o právech dítěte. Ministerstvem zahraničních věcí ČR vyhlášen pod č. 28/2016 Sb. m. s.
ORGANIZACE SPOJENÝCH NÁRODŮ. Úmluva OSN ze dne 15. listopadu 2000 proti nadnárodnímu organizovanému zločinu. Ministerstvem zahraničních věcí ČR vyhlášena pod č. 75/2013 Sb. m. s.

Ostatní

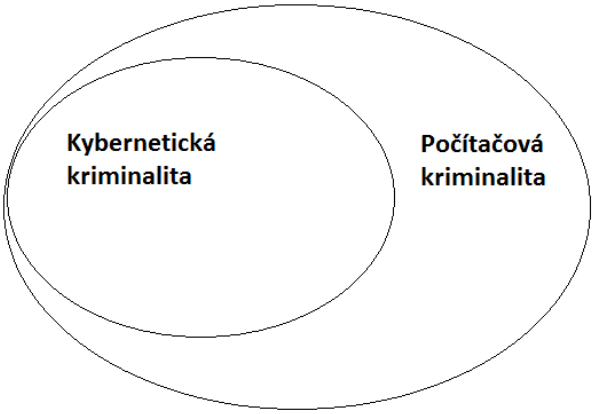
BARLOW, John Perry. A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation: Defending your rights in the digital world* [online]. Dostupné z https://www.eff.org/cyberspace-independence [cit. 2016-03-08].
COUNCIL OF EUROPE. Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems [online]. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d37ae [cit. 2016-03-15].
COUNCIL OF EUROPE. Explanatory report to the Convention on Cybercrime (ETS No. 185) [online]. Dostupné z https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b [cit. 2016-02-23].
COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime [online]. Dostupné z http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=gf19uMUq [cit. 2016-03-22].
ČESKO. Co je Národní centrum kybernetické bezpečnosti (NCKB) [online]. Dostupné z http://www.govcert.cz/cs/ [cit. 2016-03-04].
ČESKO. Mezinárodní spolupráce v boji proti informační kriminalitě. *Ministerstvo vnitra České republiky: Výsledky projektů v rámci bezpečnostního výzkumu* [online].
ČESKO. Vládní návrh zákona, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství [online]. Dostupné z http://www.mvcr.cz/clanek/vysledky-projektu.aspx [cit. 2016-03-17].
z http://www.psp.cz/sqw/text/tiskt.sqw?O=7&CT=931&CT1=0
ČESKO. Vládní návrh zákona, kterým se mění zákon č. 279/2003 Sb., o výkonu zajištění majetku a věcí v trestním řízení a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony [online]. Dostupné z http://www.psp.cz/sqw/tisky.sqw [cit. 2016-03-27].
ČESKO. Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2014 [online]. Dostupné z www.mvcr.cz [cit. 2016-04-09].

ČESKO. Kybernetická bezpečnost: Rozšíření působnosti zákona má posílit bezpečnost sítí a informačních systémů. *Právní zpravodaj Ministerstva spravedlnosti ČR* ze dne 12. ledna 2017.
EVROPSKÁ UNIE. Společné akce 98/733/JHA ze dne 21. prosince 1998 přijaté Radou na základě článku K. 3 Smlouvy o Evropské unii, kterou se stanoví, že účast na zločinném spolčení je v členských státech Evropské unie trestným činem. Dostupná z http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31998F0733&from=EN [cit. 2016-12-22].
EVROPSKÁ UNIE. Společný postoj Rady 2001/931/SZBP ze dne 27. prosince 2001 o uplatnění zvláštních opatření k boji proti terorismu.
EVROPSKÁ UNIE. Společná akce 98/699/SVV ze dne 3. prosince 1998 přijatá Radou na základě článku K. 3 Smlouvy o Evropské unii o praní peněz, identifikaci, vysledování, zmrazení, zajištění a propadnutí nástrojů trestné činnosti a výnosů z ní.
EVROPSKÁ UNIE. Tisková zpráva Rady EU č. 716/16 ze dne 5. prosince 2016. Dostupná z http://www.consilium.europa.eu/cs/press/press-releases/2016/12/05-combatting-terrorism/ [cit. 2017-02-24].
LEAGUE OF ARAB STATES. Arab Convention on Combating Information Technology Offences [online]. Dostupné z http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences [cit. 2016-03-10].
Merriam-Webster Dictionary. [online]. Dostupné z http://www.merriam-webster.com/dictionary/spam [cit. 2016-04-17].
NATO. Cyber defence [online]. Dostupné z http://www.nato.int/cps/en/natohq/topics_78170.htm [cit. 2016-03-18].
Slovník výpočetní techniky. 1. vyd. Praha: Microsoft Press, Plus s.r.o., 1993.
UNITED NATIONS. Comprehensive Study on Cybercrime [online]. Dostupné z https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [cit. 2016-03-10].
UNITED NATIONS. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. *Twelfth United Nations Congress on Crime Prevention and Criminal Justice: Salvador, Brazil, 12 - 19 April 2010* [online]. Dostupné z https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf [cit. 2016-03-17].
UNITED STATES OF AMERICA. *Odhad nezákonných finančních toků plynoucích z obchodu s drogami a jiného nadnárodního organizovaného zločinu: výzkumná zpráva*

Úřadu Spojených národů pro drogy a kriminalitu. Praha: Institut pro kriminologii a sociální prevenci, 2013.
UNITED STATES OF AMERICA. *The First Amendment of the Constitution of the United States* [online]. Dostupné z https://www.law.cornell.edu/constitution/first_amendment [cit. 2016-03-15].
UNITED STATES OF AMERICA. Restatement (Third) of Foreign Relations Law of the United States [online]. Dostupné z http://www.macalester.edu/courses/intl114/docs/restatement.pdf [cit. 2016-03-11].
U. S. DEPARTMENT OF JUSTICE. Russian Computer Hacker Sentenced To Three Years In Prison (October 4, 2002) [online]. Dostupné z https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/gorshkovSent.htm [cit. 2016-03-20].
U. S. DEPARTMENT OF JUSTICE. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* [online]. Office of Legal Education Executive Office for United States Attorneys, 2009, str. 27 – 28. Dostupné z https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [cit. 2016-03-20].

SEZNAM PŘÍLOH

1) Příloha č. 1: Vztah kybernetické a počítačové kriminality.

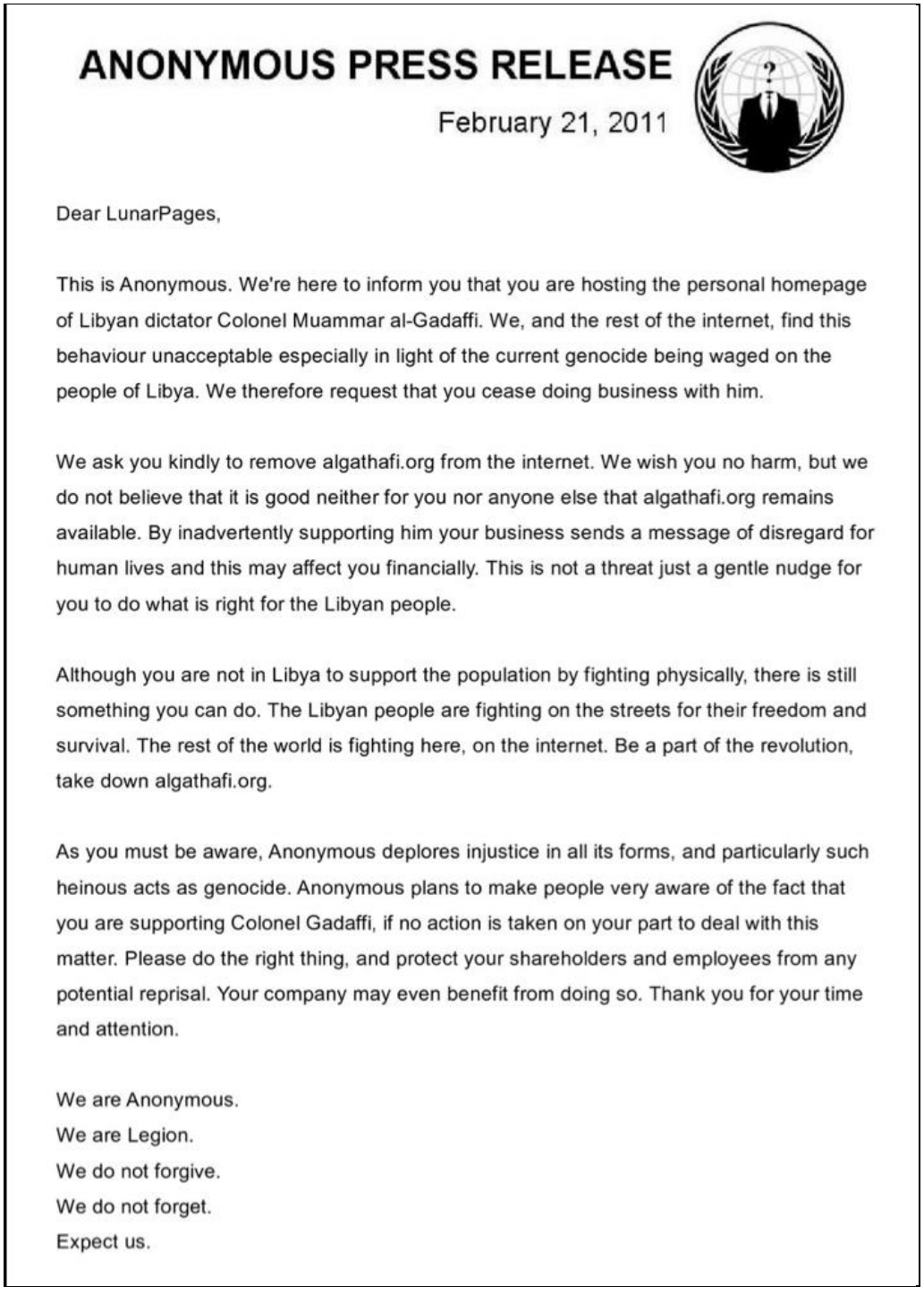


2) Příloha č. 2: Srovnání klasického a kybernetického trestného činu.[677]

Parametr	Průměrné ozbrojené přepadení	Průměrný kybernetický útok
Riziko	pachatel riskuje zranění či zabití	bez rizika fyzického zranění
Zisk	průměrně 3 až 5 tis. USD	od 50 až 500 tis. USD
Pravděpodobnost dopadení	dopadeno 50 až 60% útočníků	dopadeno cca 10% útočníků
Pravděpodobnost odsouzení	odsouzeno 95% dopadených útočníků	z dopadených útočníků je pouze 15% soudně projednáno a z nich je odsouzeno jen 50%
Trest	průměrně 5 až 6 let, pokud pachatel někoho zranil	průměrně 2 až 4 roky

[677] Převzato z JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, str. 30.

3) Příloha č. 3: Dopis hnutí Anonymous adresovaný ISP s požadavkem ukončit hostování webové stránky lybijského diktátora plukovníka Muammara Kaddáfího.[678]



ANONYMOUS PRESS RELEASE

February 21, 2011

Dear LunarPages,

This is Anonymous. We're here to inform you that you are hosting the personal homepage of Libyan dictator Colonel Muammar al-Gadaffi. We, and the rest of the internet, find this behaviour unacceptable especially in light of the current genocide being waged on the people of Libya. We therefore request that you cease doing business with him.

We ask you kindly to remove algathafi.org from the internet. We wish you no harm, but we do not believe that it is good neither for you nor anyone else that algathafi.org remains available. By inadvertently supporting him your business sends a message of disregard for human lives and this may affect you financially. This is not a threat just a gentle nudge for you to do what is right for the Libyan people.

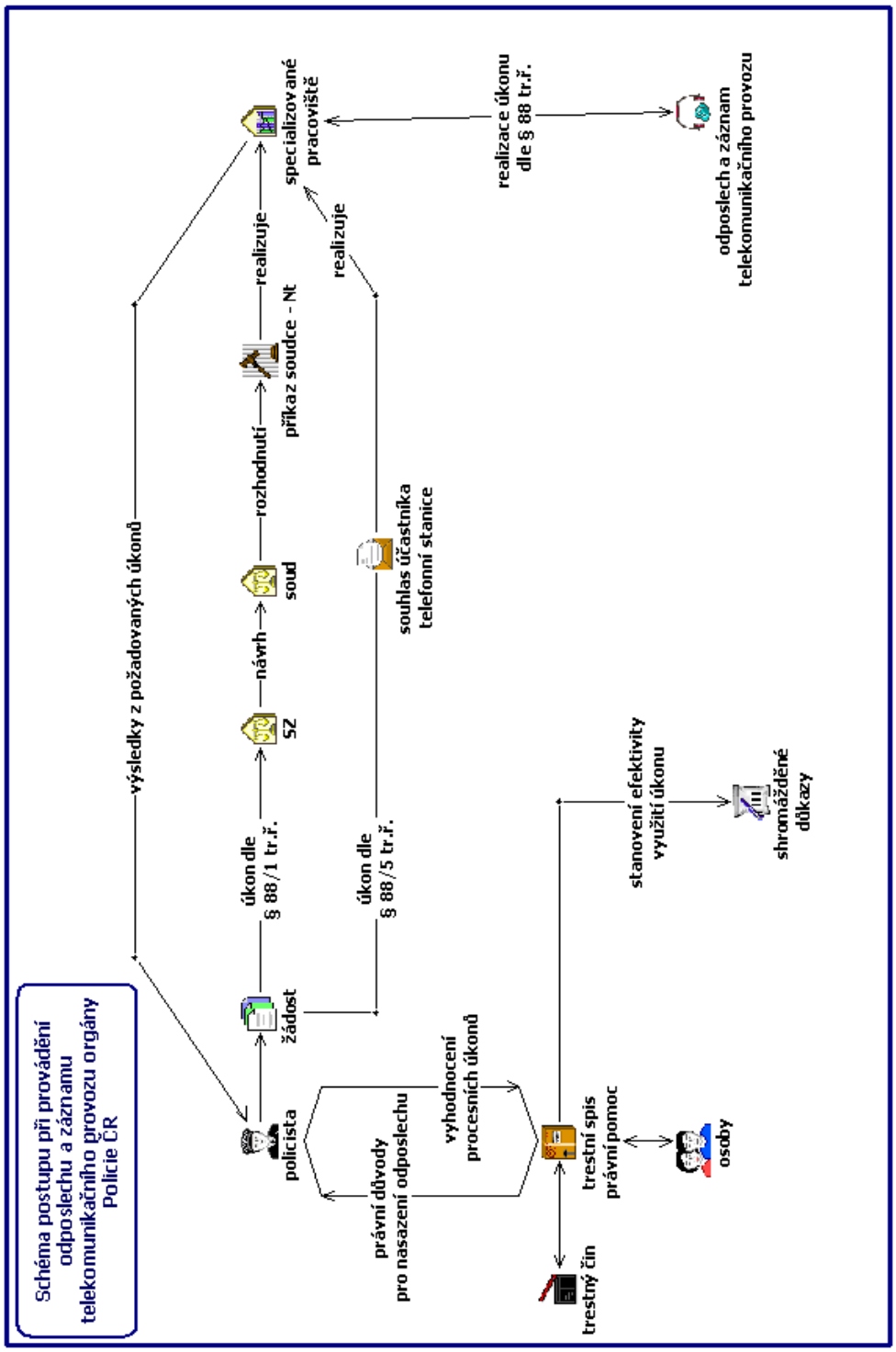
Although you are not in Libya to support the population by fighting physically, there is still something you can do. The Libyan people are fighting on the streets for their freedom and survival. The rest of the world is fighting here, on the internet. Be a part of the revolution, take down algathafi.org.

As you must be aware, Anonymous deplores injustice in all its forms, and particularly such heinous acts as genocide. Anonymous plans to make people very aware of the fact that you are supporting Colonel Gadaffi, if no action is taken on your part to deal with this matter. Please do the right thing, and protect your shareholders and employees from any potential reprisal. Your company may even benefit from doing so. Thank you for your time and attention.

We are Anonymous.
We are Legion.
We do not forgive.
We do not forget.
Expect us.

[678] BROADHURST, Roderic; GRABOSKY, Peter; ALAZAB, Mamoun; BOUHOURS, Brigitte; CHON, Steve; DA, Chen. *Crime in Cyberspace: Offenders and the Role of Organized Crime Groups* [online]. Australian National University Cybercrime Observatory, 2013, (May 16), str. 7. Dostupné z: http://ssrn.com/abstract=2211842 [cit. 2016-12-27]. Překlad autorka.

4) Příloha č. 4: Schéma postupu při provádění odposlechu a záznamu telekomunikačního provozu orgány Policie ČR.[679]



[679] Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2014 [online]. Dostupné z www.mvcr.cz [cit. 2016-04-09].

5) Příloha č. 5: Odhad expertů pro pořadí aktivit organizovaného zločinu pro rok 2020.[680]

Původní aktivity organizovaného zločinu	Novodobé/současné podoby aktivit organizovaného zločinu
• **místní sázky, loterie a hazard (gambling), herny**	➢ **gambling na mezinárodních internetových stránkách (www)**
• **obchod s heroinem a kokainem**	➢ **syntetické drogy (odpadají problémy se zásobováním, dovozem materiálu k výrobě)**
• **pouliční prostituce**	➢ **prostituce a obchod s lidmi s využitím Internetu**
• **vymáhání peněz od místních obchodníků za jejich ochranu**	➢ **vydírání společností, korporací, únosy**
• **lichva**	➢ **praní špinavých peněz, obchod s drahými kameny, surovinami**
• **překupníci kradeného zboží**	➢ **krádeže duševního majetku**

[680] CEJP, Martin; BLATNÍKOVÁ, Šárka; HÁKOVÁ, Lucie; HOLAS, Jakub; TRÁVNÍČKOVÁ, Ivana; VLACH, Jiří. *Společenské zdroje vývoje organizovaného zločinu*. Praha: Institut pro kriminologii a sociální prevenci, 2015, str. 16.

SEZNAM POUŽITÝCH ZKRATEK

ČAK	Česká advokátní komora
ČNB	Česká národní banka
ČR	Česká republika
EU	Evropská unie
EÚLP	Úmluva Rady Evropy č. 5 ze dne 4. listopadu 1950 o ochraně lidských práv a základních svobod
ICT	Informační a komunikační technologie
ISP	Poskytovatel služby informační společnosti
IoT	Koncept „Internet of Things“
Listina	Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
Sb.	Sbírka zákonů
TŘ	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
TZ	Zákon č. 40/2009 Sb., trestní zákoník (trestní zákoník)
trestní zákon	Zákon č. 140/1961 Sb., trestní zákon
Úmluva o počítačové kriminalitě	Úmluva Rady Evropy č. 185 ze dne 23. listopadu 2001 o počítačové kriminalitě
USA	Spojené státy americké
Ústava ČR	Ústavní zákon č. 1/1993 Sb., Ústava České republiky
Warez	Výroba a distribuce ilegálního software, představující trestnou činnost proti autorskému právu
ZBZ	Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
ZEK	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
ZMJS	Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních
ZPČR	Zákon č. 273/2008 Sb., o Policii ČR
ZSVM	Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)
ZZT	Zákon č. 36/1967 Sb., o znalcích a tlumočnících

NÁZEV PRÁCE V ANGLICKÉM JAZYCE

Cybercrime: Selected issues of prosecution in international environment

ABSTRAKT

Rigorózní práce pojednává o postihu počítačové kriminality v mezinárodním prostředí. Zaměřuje se na problematické situace, s nimiž se orgány činné v trestním řízení v rámci postihu počítačové kriminality setkávají. Text se soustředí především na proces odhalování a vyšetřování počítačové trestné činnosti v širším kriminalistickém smyslu.

Počítačová kriminalita je v textu vymezena široce – jako jev zahrnující i kybernetickou kriminalitu. Vzhledem k charakteristickým vlastnostem informačních a komunikačních technologií definuje práce počítačovou kriminalitu jako veskrze globální problém, při jehož postihu se ukazuje mezinárodní spolupráce orgánů činných v trestním řízení jako klíčová.

První kapitola je obecným úvodem do problematiky počítačové trestné činnosti. Představuje základní terminologii počítačové trestné činnosti, ukazuje na historickém vývoji její transformaci, stručně seznamuje s širokým spektrem jednání. Kapitola shrnuje rovněž z kriminologického hlediska dostupné poznatky o pachatelích a obětech počítačové kriminality. Ve druhé kapitole následuje rozbor působnosti a vynutitelnosti trestněprávní normy v kyberprostoru. Text se zaměřuje na uplatnění pravomoci orgánů činných v trestním řízení v rámci pravidel místní působnosti trestněprávních norem. Rozebírá jurisdikční konflikty a představuje možné způsoby jejich řešení. Třetí kapitola se věnuje propojení počítačové kriminality se závažnou trestnou činností, jako je organizovaný zločin a terorismus. Hledá odpověď na otázku, proč a jak zneužívají pachatelé organizovaného zločinu a terorismu informačních a komunikačních technologií. Pojednává též o právních nástrojích mezinárodního a evropského práva usnadňujících postih uvedených forem přeshraniční počítačové trestné činnosti. Čtvrtá kapitola rozebírá vybrané procesní instrumenty českého trestního práva ovlivňující odhalování a vyšetřování počítačové kriminality a poukazuje na některé jejich nedostatky. Jádrem práce je pátá kapitola, pojednávající o mezinárodní spolupráci v trestních věcech. Důraz je kladen na mezinárodní právní pomoc. Stav právní úpravy v oblasti zásadně ovlivní postih počítačové kriminality v mezinárodním prostředí. Text rozebírá úpravu obsaženou v zákoně č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních i nástroje mezinárodní spolupráce na úrovni univerzální a

regionální. Poukazuje rovněž na problematické aspekty mezinárodní spolupráce při postihu počítačové kriminality a varuje před některými alternativními přístupy mezinárodní praxe vůči rigidním formám mezinárodní spolupráce. Závěrem se vyjadřuje k předpokládanému vývoji v oblasti.

KLÍČOVÁ SLOVA

počítačová kriminalita, kybernetická kriminalita, kyberterorismus, mezinárodní justiční spolupráce

ABSTRACT

The thesis deals with an issue of cybercrime prosecution in international environment. The text focuses on particular problems met by law enforcement agencies when prosecuting cybercrime. Within the prosecution, the emphasis is put on the aspects of detection and investigation of cybercrime.

Within the thesis, cybercrime is understood as a part of computer crime. Computer crime is approached rather as global crime due to typical characteristics of information and communication technologies. Therefore, the international cooperation of law enforcement agencies is considered crucial.

First chapter introduces the issue of computer crime, including adopted terminology. It discusses the transformation of computer crime and cybercrime following its historical development and broad forms of modus operandi. Criminological findings about perpetrators and victims of computer crime are discussed likewise. Second chapter deals with criminal law jurisdiction and enforcement within cyberspace. The accent is put on local applicability of criminal law and related jurisdictional conflicts with possible remedies. Third chapter concentrates on the interconnection of computer crime and organized crime, as well as computer crime and terrorism. Why and how are the perpetrators of organized crime and terrorism abusing information and communication technologies is the question. Relating international legal instruments on both universal and regional level are discussed as well. Fourth chapter focuses on selected procedural powers of law enforcement agencies according to Czech Criminal Procedure Act and reveals several shortcomings. The core of the thesis is the fifth chapter which deals with international judicial cooperation within the scope of criminal law. The stress is put on particular form of cooperation - international legal assistance. The state of regulation influences greatly the prosecution of computer crime in international environment. The chapter deals with Czech International Judicial Cooperation in Criminal Matters Act as well as related international legal instruments on universal and regional level. Several problems of international cooperation within the prosecution of computer crime are discussed. The chapter warns before the practise of finding particular alternative ways to rigid methods of international cooperation and comments on expected development in the field.

KEYWORDS

computer crime, cybercrime, cyberterrorism, international judicial cooperation