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

BAKALÁŘSKÁ PRÁCE

KYBERKRIMINALITA V ČESKÉ REPUBLICE

Autor práce: **Luděk Hrabák**

Studijní obor: **Bezpečnostně právní činnost ve veřejné správě**

Forma studia: **Kombinovaná**

Vedoucí práce: **RNDr. Růžena Ferebauerová**

Katedra: **Katedra právních oborů a bezpečnostních studií**

2019

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

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

…….

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

HRABÁK, L., DiS. *Kyberkriminalita v České republice: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2019. 70 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kybernetická kriminalita, počítačová, informační kriminalita, kyberprostor, úmluva o počítačové kriminalitě, typy protiprávních jednání kyberkriminality, získávání informací a dat při objasňování a vyšetřování kybernetické kriminality, data retention, data freezing

Práce pojednává o nové a stále se rozvíjející formě trestné činnosti, o kybernetické kriminalitě, se zaměřením na její projevy v České republice. V práci je vymezen a objasněn pojem kybernetická kriminalita na základě výsledku analýzy a komparace různých definic uvedených v odborné literatuře, historického vývoje informačních a komunikačních technologií, a vlivu nově vzniklého fenoménu virtuálního prostoru nazývaného kyberprostor. Dále jsou vymezeny základní pojmy důležité k pochopení celé problematiky. Kyberkriminalita je za využití metody výkladu a analýzy zákonných norem a mezinárodních smluv rozdělena na jednotlivé druhy (formy), které jsou zasazeny do kontextu českého trestního práva. Práce zahrnuje roli a podíl útvarů Policie České republiky podílejících se na objasňování a vyšetřování této trestné činnosti a analyzuje statistická data potvrzující, že dochází k téměř exponenciálnímu nárůstu kyberkriminality, jejíž největší podíl v České republice tvoří počítačové podvody. Dále je analyzován stávající právní rámec týkající se problematiky vyžadování a zajišťování dat a informací při prověřování a vyšetřování případů kyberkriminality a na základě této analýzy jsou navrženy konkrétní změny právních norem týkajících se povinnosti uchovávání dat ze strany poskytovatelů informačních služeb a zajišťování obsahu e-mailových schránek. V závěru práce jsou z teoretického a praxeologického hlediska autora práce popsány způsoby získání informací k facebookovým účtům podle českého práva s popisem konkrétního šetřeného případu.

ABSTRACT

HRABÁK, L., DiS. *Cybercrime in the Czech Republic: A Bachelor's Thesis.* České Budějovice: The College of European and Regional Studies, 2019. 70 pp. Thesis supervisor: RNDr. Růžena Ferebauerová.

Keywords: cybercrime, computer-oriented crime, computer crime, cyberspace, Convention on Cybercrime, types of illegal conduct in cybercrime, information and data retrieval during cybercrime investigation, data retention, data freezing

The thesis focuses on cybercrime, which is a new and continually evolving type of crime. More specifically, it deals with manifestations of this crime in the Czech Republic. The thesis determines and clarifies the concept of cybercrime based on the analysis and comparison of various definitions in the academic literature, historical development of information and communication technologies and the influence of cyberspace, which is a newly emerged phenomenon of virtual space. Furthermore, the thesis also defines basic concepts that are important to understand the issue. Using the method of interpretation and analysis of legal norms and international treaties, cybercrime is divided into different types (forms) that are put in the context of Czech criminal law. The thesis informs about the role and participation of the units of the Police of the Czech Republic involved in the investigation of this crime. It also analyses statistical data confirming that cybercrime is almost exponentially increasing – computer fraud being the most frequent in the Czech Republic. Furthermore, the thesis analyses the existing legal framework related to request and provision of data and information during investigation of cybercrime cases. Based on this analysis, it proposes specific changes to legal norms related to data retention obligations of internet service providers and provision of mailbox content. From the theoretical and praxeological view of the author, the conclusion of the thesis concentrates on ways of obtaining information on Facebook accounts under the Czech law with a description of the investigated case.

Obsah

Úvod

„Celosvětová pavučina (World Wide Web) byla vyvinuta, aby se stala místem pro ukládání lidských vědomostí. Místem, které umožňuje lidem ze vzdálených míst vyměňovat si nápady a pracovat na společných projektech.“

Tim Berners-Lee (vědec CERN, autor WWW), 1994

Druhá polovina 20. století bývá označována jako období digitální revoluce, v některých zdrojích i jako třetí průmyslová revoluce, počítačová, digitální nebo informační doba. Typickým rysem pro tuto dobu je společnost založená na integraci informačních a komunikačních technologií do všech oblastí společenského života v takové míře, že zásadně mění společenské vztahy a procesy[1].

Základním kamenem pro rozvoj této revoluce bylo rozšíření informačních a komunikačních technologií mezi široké masy uživatelů. K takovému rozšíření došlo díky cenové dostupnosti výpočetní techniky a možnosti kohokoli, se téměř kdekoliv připojit k internetu.

První oficiální připojení k internetu bylo v České republice uskutečněno v roce 1992 na půdě pražského Českého vysokého učení technického. Toto připojení bylo uskutečněno prostřednictvím v té době jediné vybudované páteřní sítě, kterou byl CESNET (Czech Educational and Scientific NETwork)[2]. První komerční poskytovatelé připojení začali vznikat v roce 1995, ale k masovému rozšíření internetu do běžných domácností došlo až po roce 1999, což je zřejmě spojeno s poklesem nákladů na připojení v té době[3]. Poté se postupem času stalo používání internetu a služeb s ním spojených (e-mail, sociální sítě, e-shopy, úložiště apod.) zcela samozřejmou a běžnou činností pro téměř všechny obyvatele napříč věkovými a sociálními skupinami. Růst počtu domácností vybavených počítači a počtu jednotlivců s připojením k internetu v České republice dokazují data Českého statistického úřadu, ze kterých vyplývá, že v roce 2005 disponovalo připojením k internetu pouze 19.1 % domácností, zatímco v roce 2017 již

[1] JONÁK, Z. Informační společnost. In KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha: Národní knihovna ČR, 2003- [cit. 2017-12-03]. Dostupné z WWW: <http://aleph.nkp.cz/F/?func=direct&doc_number=000000468&local_base=KTD>

[2] Czech Educational and Scientific NETwork – první internetová páteřní síť v České republice, která měla propojovat zejména univerzitní a akademická pracoviště.

[3] Historie internetu v ČR. Co je to internet? [online]. Copyright © 2011 [cit. 29.09.2018]. Dostupné z WWW: <http://www.imip.cz/historie-internetu-v-cr/>

77.2 % domácností. Podobné je to i u počtu uživatelů internetu, kterých v roce 2005 bylo 32.1 % z celkového počtu obyvatel a v roce 2017 již 78.8% (viz graf v příloze č. 1). Právě díky velkému počtu osob používajících internet jako zdroj informací a služeb, a využívání obrovského množství aplikacích fungujících v jeho prostředí, vznikla nová dimenze, kterou nazýváme kyberprostorem.

Jak už to v historii lidstva chodí, když je vyvinuta jakákoliv nová technologie, tak se ji lidé snaží využít ke svému prospěchu, zejména k získání maximálních zisků, a v některých případech i nelegální cestou. Právě tato lidská vlastnost vedla ke vzniku nového fenoménu, který je laickou veřejností nazýván různými pojmy, jako např. kyberkriminalita, počítačová nebo informační kriminalita.

Právě fenoménu kyberkriminality se věnuje tato bakalářská práce – zejména vymezením základních pojmů jak samotné kybernetické kriminality, tak i pojmů s ní úzce souvisejících. V práci se autor věnuje všem formám této kriminality, ale s větším zaměřením na ty, jejichž cílem není útok na samotné počítače, informační technologie, systémy nebo data, ale na formy, které zde byly již před digitální dobou, a vznik nových technologií umožnil nové způsoby jejich páchání v globálním měřítku, tedy kdekoli na světě, aniž by pachatel opustil svůj domov. Jedná se zejména o tzv. internetové podvody, tedy podvodná jednání páchaná pomocí internetu a v jeho prostředí.

Dále se práce zaobírá postižitelností projevů kyberkriminality v prostředí českého práva, složitostmi objasňování a vyšetřování těchto protiprávních jednání v rámci Policie České republiky, zejména problematikou získávání a vyžadování dat a informací.

Téma bakalářské práce bylo zvoleno nejen s ohledem na jeho aktuálnost, spočívající zejména ve stále se rozšiřujícím používání a pronikání výpočetních, informačních a komunikačních technologií a techniky do všech sfér lidského života, a s tím spojené zvýšené nebezpečí jejich zneužití k páchání protiprávních jednání, ale i kvůli služebnímu zařazení autora práce u Policie České republiky Plzeňského kraje na Oddělení analytiky a kybernetické kriminality Územního odboru v Rokycanech.

1 Cíle a metodika bakalářské práce

Cílem bakalářské práce je objasnění a vymezení pojmu kyberkriminalita, její rozdělení na jednotlivé druhy (formy) a zasazení tohoto protiprávního jednání do kontextu českého trestního práva. Dalším cílem je zhodnocení objasňování a vyšetřování kyberkriminality v rámci Policie České republiky, zejména úskalí a obtížnost získávání informací a dat, což bude zhodnoceno i na konkrétním případu.

Pro objasnění a vymezení pojmu kyberkriminalita bude použito odborných textů a literatury. Stejné metody budou použity pro definování pojmů úzce souvisejících s kyberkriminalitou, bez nichž by nebylo možné zcela objasnit zkoumanou problematiku, zejména její formy a způsoby páchání.

Zasazení popisovaného protiprávního jednání do kontextu českého trestního práva a jeho rozdělení na jednotlivé formy bude provedeno zejména za pomoci metod výkladu a analýzy zákonných norem a mezinárodních smluv, zvláště Úmluvy o počítačové kriminalitě otevřené k podpisu Výborem Rady ministrů dne 23. 11. 2001 v Budapešti (dále jen „budapešťská úmluva“)[4] , zákona č. 40/2009 Sb. (trestní zákoník), zákona č. 141/1961 Sb. (trestní řád), zákona č. 127/2005 Sb. (zákon o elektronických komunikacích), zákona č. 480/2004 Sb. (zákon o některých službách informační společnosti) a dalších.

Problematika objasňování a vyšetřování kyberkriminality, obzvláště získávání a zajišťování důkazů, bude analyzována nejprve z pohledu dle lege lata a na základě této analýzy bude navržena změna de lege ferenda. Vyhodnocení bude provedeno především na konkrétních případech z teoretického a praxeologického hlediska autora práce. Tedy na kazuistice vybraného případu se zjištěním a popisem problémů a obtížností získávání informací a dat důležitých pro důkladné prošetření skutků spojených s kyberkriminalitou.

Vedlejším cílem bakalářské práce je komparací statistických dat z databází Policie České republiky (dále jen Policie ČR) potvrdit hypotézu o téměř exponenciálním nárůstu tohoto druhu kriminality a dále určení základních kriminologických faktorů majících vliv na její vznik a rozšíření.

[4] ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 56.

2 Vymezení a definice pojmu kyberkriminalita a základních pojmů s ní souvisejících

V této kapitole bude objasněn a vymezen samotný pojem kyberkriminalita, a to jak definice tohoto termínu, tak určení jeho obsahu. Dále budou objasněny některé základní pojmy s ní související, jejichž vymezení je potřeba pro plné pochopení textu bakalářské práce.

2.1 Kyberkriminalita

Jazykovou analýzou lze odvodit, že slovo kyberkriminalita je česká obdoba anglického výrazu Cybercrime, což je slovo vzniklé axifoidní kompozicí, tzn. spojením zkráceného slova Cybernetics (česky kybernetický) a slova Crime (česky zločin). Ale jazykový rozbor, ani zkoumání původu slova, není předmětem této práce.

Veřejností jsou jako synonyma tohoto pojmu používány výrazy počítačová, informační kriminalita a někdy i kyberzločin. To je dáno především tím, že jednotné vymezení pojmu kyberkriminalita nelze v legislativě ani v odborné literatuře najít, což souvisí zejména s velkým počtem rozdílných přístupů, ale i s chápáním obsahu tohoto pojmu.

Václav Jirovský[5] například používá jako synonymum pro kybernetickou kriminalitu pojem **kybernalita**. Tímto pojmem označuje činnost, kterou je porušován nejen zákon, ale i morální pravidla společnosti. Dále uvádí, že tato kriminalita může být namířena přímo proti počítačům (hardware nebo software), sítím, datům, nebo je počítač jejím nástrojem, nebo počítačová síť a zařízení v ní zapojená jsou prostředím, kde se kriminalita odehrává. Vladimír Smejkal[6] hovoří o termínu **e-kriminalita,** a to v souvislosti s prorůstáním internetu do všech lidských činností.

Pro definování pojmu kyberkriminality, resp. vymezení jeho obsahu, je nutné si uvědomit, že společně s vývojem a zejména s růstem možností využívání informačních a komunikačních prostředků (dále jen ICT) roste i možnost jejich zneužívání k páchání trestné činnosti[7]. Používání různých pojmů je dáno tedy i historickým vývojem

[5] JIROVSKÝ, V. Kybernetická kriminalita. Praha: Grada, 2007. s. 19. ISBN 978-80-247-1561-2

[6] SMEJKAL, V. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue. Praha: C. H. Beck, 2003(6), s. 161-167. ISSN 1213-5313.

[7] KOLOUCH, J. CyberCrime. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016, s. 33. ISBN 978-80-88168-18-8.

informačních a komunikačních technologií a rozsahem jejich používání širokou veřejností a jejich zneužíváním k různým protiprávním aktivitám.

Z uvedených skutečností lze tedy odůvodnit, že se v 90. letech minulého století pro trestnou činnost, pro kterou byl společným faktorem počítač, programy a data, zažil termín počítačová kriminalita[7]. Jedná se o kriminalitu, kde je počítač nástrojem nebo předmětem útoku.

Postupem času v návaznosti na další vývoj ICT, zejména na rozšíření připojení k internetu, se v souvislosti s protiprávním jednáním začal používat pojem informační kriminalita (dále jen IT kriminalita), někdy i internetová kriminalita. Pro tuto trestnou činnost je charakteristické využívání počítačových sítí, v první řadě síť sítí internet.

Kyberkriminalita tedy pak zahrnuje oba již zmíněné pojmy a zahrnuje i trestnou činnost související s kyberprostorem. Na základě této úvahy lze konstatovat, že kybernetickou kriminalitu tvoří podmnožina informační kriminality, jejíž podmnožinou je počítačová kriminalita, tak jak uvádí i Josef Požár [8].

Obr. 1: Znázornění vztahu kyberkriminality s počítačovou a informační kriminalitou[8]

Při různorodosti pojmosloví a definice kyberkriminality považuje autor práce jako nejpřesnější a nejvýstižnější výklad uvedený ve výkladovém slovníku kybernetické bezpečnosti, který na něj odkazuje i u hesla počítačová kriminalita[9]:

„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického 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 zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž

[8] POŽÁR, J. Některé aspekty kybernetické kriminality [online]. Praha: Policejní akademie ČR, Fakulta bezpečnostního managementu, 2011 [cit. 2017-12-10]. Dostupné z: https://www.cybersecurity.cz/data/Pozar.pdf

[9] JIRÁSEK, P., NOVÁK, L., POŽÁR, J.. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, s. 57, 73 ISBN 978-80-7251-377-2.

předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“

Tedy zjednodušeně řečeno se jedná o trestnou činnost, kde je cílem útoku počítač, počítačová síť, její část nebo data a trestná činnost, při které je počítač nebo počítačová síť rozhodujícím nástrojem k jejímu páchání.

Při vnímání pojmu kybernetická kriminalita, jako ostatní pojmy kriminality, které jsou považovány za tzv. „klasickou“ kriminalitu (např. majetková, hospodářská, násilná…), kdy každá z těchto forem trestné činnosti má vždy určitý společný faktor (např. způsob provedení, předmět zájmu apod.), jde u kyberkriminality v podstatě o různorodou trestnou činnost, která má společné faktory, kterým je např. počítač, data, síť nebo program jako cíl (napadený objekt) nebo jako nástroj, prostředek ke spáchání.[10] Rozsah obsahu kybernetické kriminality je tedy velmi široký, zahrnující v sobě téměř všechny druhy „klasické“ kriminality.

2.2 Počítač

Pro tento pojem existuje mnoho definic. Podle autora práce se lze na základě společných znaků většiny těchto definic přiklonit k vysvětlení, které zastává Vladimír Smejkal[11], že počítač je každý programovatelný stroj (zařízení), který může provést naprogramovaný seznam instrukcí a reaguje na pokyny zadávané z vnějšku, přičemž zpracovává data zadaná prostřednictvím vstupných zařízení a výsledky jsou prezentovány pomocí výstupních zařízení.

Každý počítač je tvořen technickým vybavením, které nazýváme **hardware** a programovým vybavením nazývaným **software**.

Hardware můžeme dále rozdělit na:

- vnitřní vybavení počítače, kterým je např. základní deska, procesor, harddisk, grafická karta, napájecí zdroj, mechanika paměťových médií apod.,
- vnější vybavení počítače, tzv. **periferie**, tedy zařízení externě připojovaná k počítači ať kabely, nebo různými bezdrátovými metodami (např. Wi-Fi a Bluetooth).

[10]SMEJKAL, V., SOKOL, T. a VLČEK, M. Počítačové právo. Praha: C. H. Beck, 1995. s. 99. ISBN 80-7179-009-5.

[11] SMEJKAL, V. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 22- 23. ISBN 978-80-7380-501-2.

2.3 Počítačový systém

Pojem počítačový systém je používán trestním zákoníkem (§§ 182, 230, 231 a 232), aniž by byl jakkoliv v této právní normě vysvětlen. Termín byl do české práva implementován na základě „budapešťské úmluvy“, v níž je v čl. 1 písm. a) definován jako: „*Jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu“*. [12]

Podle Tomáše Gřivny[13] se jedná o funkční jednotku sestávající minimálně z jednoho technického zařízení s odpovídajícím programovým vybavením, přičemž nejméně jedno z těchto zařízení by mělo být počítačem.

Vladimír Smejkal[14] vyslovil názor, že není nutné vymýšlet odlišnosti mezi počítačem a počítačovým systémem. Vždyť z uvedených definic je možné konstatovat, že se jedná o téměř totožné pojmy. Tomáš Gřivna[15] konstatuje používání pojmu počítač jako synonymum k počítačovému sytému, ale zdůrazňuje skutečnost, že počítačový systém zahrnuje i pomocí sítě připojená zařízení nesplňující vlastnosti počítače.

2.4 Počítačová síť

Již ze samotného pojmu lze dovodit, že se bude jednat o vzájemné propojení více počítačů do jedné společné sítě s možností vzájemné komunikace – výměny dat. Toto je však velmi jednoduché pojetí.

Pro tento pojem existuje mnoho definic. Autor této práce chápe počítačovou síť tak, jak je vymezena ve slovníku kybernetické bezpečnosti[16]. Jde o soubor počítačů (počítačových systémů) propojených komunikační infrastrukturou za účelem výměny informací nebo sdílení zdrojů (dat, technických a programových prostředků).

---

[12] ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 56.

[13] GŘIVNA, T. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In ŠÁMAL, P. a kol. Trestní zákoník (EVK). 2. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 2300. ISBN 978-80-7400-428-5.

[14] SMEJKAL, V. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 25. ISBN 978-80-7380-501-2.

[15] GŘIVNA, T. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In ŠÁMAL, P. a kol. Trestní zákoník (EVK). 2. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 2300. ISBN 978-80-7400-428-5.

[16] JIRÁSEK, P., NOVÁK, L., POŽÁR, J.. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013, s. 73. ISBN 978-80-7251-377-2.

Komunikační infrastrukturu tvoří komunikační linky, technické a programové vybavení a konfigurační údaje.

Počítačové sítě lze dělit podle různých kritérií, kterými jsou např. jejich architektura (sítě peer-to-peer, klient server), topologie (sběrnicová, hvězda, kruh, strom apod.)

Podle rozsahu pokrytí se samotné sítě rozdělují na lokální síť (LAN), tedy síť zřízenou v jedné budově, firmě nebo v malé geografické oblasti (např. metropolitní síť, tzv. MAN), a vzdálenou síť (WAN), tedy rozlehlou síť, která spojuje geograficky oddělené oblasti a umožňuje komunikaci na velké vzdálenosti. Nejznámější rozlehlou celosvětovou sítí je internet.

Obr. 2: Grafické znázornění počítačových sítí[17]

2.5 Internet

Internet je celosvětová počítačová síť a jedná se vlastně o celosvětový systém vzájemně propojených počítačových sítí na základě smluv mezi jejich vlastníky (provozovateli). Jedná se o jakousi síť sítí. Z technického hlediska jde o soustavu sítí, podsítí, serverů a k nim připojených počítačů. Aby počítače, resp. jednotlivé sítě, mohly spolu komunikovat, je používán protokol TCP/IP. Jedná se o zkratku anglického termínu *Transmission Control Protocol/Internet Protocol*. Jde vlastně o sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě internet. Internet z pohledu výměny informací, dat a za jeho pomoci poskytovaných a využívaných služeb

[17] Zdroj: [online]. [cit. 2017-12-28]. Dostupné z: http://pepa.zvonicek.info/inf/hlavni-rozdeleni.html

různých aplikací, má globální charakter. Internet je vlastně prostor, jež nemá žádné hranice (více viz kapitola 2.6 Kyberprostor).

Z hlediska práva nemá internet jako takový žádnou právní subjektivitu, což plyne ze skutečnosti, že není fyzickou ani právnickou osobou, a tak není subjektem práva. Internet jako takový není ani v právním smyslu věcí podle občanského zákoníku, neboť mu schází podstatné vlastnosti věci, především to, že internet si nelze jako celek přivlastnit, ani ho jako celek ovládat. Vladimír Smejkal[18] jde v analýze povahy internetu ještě dále a konstatuje, že internet není ani objektivní právní skutečností nebo právní událostí nezávislou na lidském chování.

S přihlédnutím na shora uvedeném konstatování vyvstává otázka vymahatelnosti a uplatňování práva v prostředí internetu. K odpovědi na tuto otázku je třeba si uvědomit, co internet znamená z technického hlediska. Z tohoto pohledu se jedná, jak již bylo v úvodu této kapitoly uvedeno, vlastně o celosvětovou počítačovou síť složenou z jednotlivých menších sítí, které umožňují komunikaci, přenos dat a informací a poskytování služeb mezi subjekty navzájem. Jednotlivé počítačové sítě jsou vlastněny a provozovány fyzickými či právnickými osobami. Tyto sítě je možné považovat za věc dle § 489 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů[19].

Ze shora uvedených skutečností lze vyvodit, že internet jako celek nemá majitele, ale jednotlivé části (vybudovaná infrastruktura, datová centra, servery) či služby mají své vlastníky, od kterých je již možné vyžadovat poskytnutí informací důležitých pro vyšetřování kyberkriminality. Avšak toto má svá úskalí, neboť vyžadování informací od poskytovatelů služeb, majitelů a provozovatelů infrastruktur v internetu je velmi složité hlavně kvůli samotné podstatě fungování internetu a zejména díky jeho globálnímu charakteru, neboť internet nezná hranice.

Jednotliví uživatelé přistupují na internet za využití služeb poskytovatelů internetového připojení, např. prostřednictvím telefonní linky, kabelu, přenosem po elektrické síti, různými bezdrátovými sítěmi apod. Tito poskytovatelé zajišťují konektivitu, tzn. fyzické připojení do sítě. Uživatelé rovněž využívají dalších služeb v prostředí internetu, jako jsou např. free mailové služby, datová úložiště, sociální sítě

[18] SMEJKAL, V. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 59- 60. ISBN 978-80-7380-501-2.

[19] KOLOUCH, J. CyberCrime. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016, s. 91-92. ISBN 978-80-88168-18-8.

apod. Tyto služby jsou poskytovány subjekty, které v České republice nazýváme poskytovateli služby informační společnosti.

2.5.1 Poskytovatel připojení

Jedná se o podnikatele, který zajišťuje pro své klienty fyzické připojení k internetu pomocí své vlastní nebo pronajaté infrastruktury. V české legislativě je právní rámec takového poskytovatele uveden v zákoně o elektronických komunikacích (dále jen ZoEK)[20], ze kterého vyplývá, že se jedná o osobu podnikající v elektronických komunikacích na území České republiky, za podmínek stanovených ZoEK, která splňuje obecné podmínky (bezúhonnost fyzické nebo právnické osoby, a u fyzické osoby ještě dosažení věku nejméně 18 let a plná způsobilost k právním úkonům). Oprávnění k podnikání vzniká těmto osobám dnem doručení oznámení podnikání, které splňuje náležitosti podle § 13, nestanoví-li tento zákon jinak.

Takto podnikajícím osobám pak ze ZoEK vnikají i některá práva a povinnosti, z nichž pro šetření případů kyberkriminality je nejdůležitější povinností uchovávání provozních a lokalizačních údajů po dobu šesti měsíců[21].

2.5.2 Poskytovatel informační služby

Podle § 2 písm. d) zákona o některých službách informační společnosti[22] je poskytovatelem služby: „*každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti*“.

Službou informační společnosti se pak rozumí podle § 2 písm. a) tohoto zákona: „*Jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat“*. Jak již bylo uvedeno v předchozí kapitole, jedná se např. mailové služby, datová úložiště, sociální sítě apod.

---

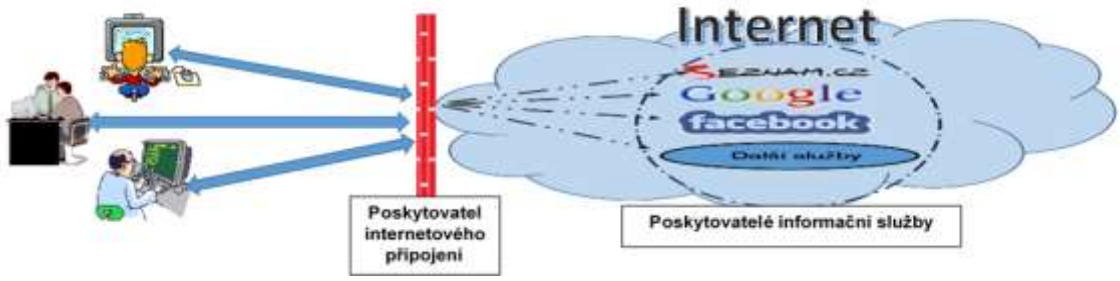
[20] ČESKO. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), § 8. In *Sbírka zákonů, Česká republika*. 2005, částka 43.

[21] ČESKO. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), § 97. In *Sbírka zákonů, Česká republika*. 2005, částka 43.

[22] ČESKO. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In *Sbírka zákonů, Česká republika*. 2004, částka 166.

Těmto poskytovatelům služeb není uložena žádná zákonná povinnost uchovávat provozní a lokalizační údaje tak, jako u poskytovatelů fyzického připojení k internetu.

Obr. 3: Grafické znázornění vztahu poskytovatel připojení versus poskytovatel informační služby[23]



2.6 Kyberprostor

Globálním propojením informačních, počítačových, komunikačních systémů a jejich aktivním využíváním uživateli napříč celým světem vzniklo prostředí, v němž je umožněno uchovávání, vytváření a výměna informací a hlavně vznik nových možností sociální komunikace a interakce. Hlavními znaky tohoto nového prostředí je, že není omezeno žádným teritoriem, a že zmenšuje vzdálenosti v procesu globalizace. Toto prostředí, které reálně fyzicky neexistuje, a které jsme si zvykli nazývat virtuální realitou (světem) nebo kyberprostorem, je nejčastěji spojováno s internetem.

Poprvé byl pojem kyberprostor (angl. Cyberspace) použit americkým prozaikem Williamem Gibsonem, který tento prostor popsal jako jakousi konsensuální datovou halucinaci vizualizovanou v podobě imaginárního prostoru, tvořeného počítačově zpracovanými daty a přístupného pouze vědomí (a nikoli fyzické tělesnosti) uživatelů[24].

Podle Kevina Robinse[25] je kyberprostor utopická představa postmoderní doby. Utopie je podle něj nikde, ale současně někde, kde je dobře. Kyberprostor tedy představuje zároveň nikde a někde.

[23] Vlastní zdroj

[24] Kyberprostor. In Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-11-04]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberprostor

[25] ROBINS, K., O. BESPERÁT, Z. KOUBÍKOVÁ, J. MACEK a M. METYKOVÁ. KYBERPROSTOR A SVĚT, VE KTERÉM ŽIJEME. REVUE PRO MÉDIA: Časopis pro kritickou reflexi médií. Spolek přátel pro vydávání časopisu HOST, 2003(5), s. 15. ISSN 1214-7494.

Termín kyberprostor nelze jednoduše definovat. V současnosti existují nejméně dvě desítky definicí. Nejznámější je nejspíše názor Johna Perry Barlowa[26], podle kterého je kyberprostor domovem nové mysli, ve kterém neexistuje žádná vláda. Jde o globální společenský prostor nezávislý na tyraniích, který neleží v žádných hranicích. Jedná se podle něj o svět, do kterého mohou vstoupit všichni bez privilegií a předsudků daných rasou, ekonomickou mocí, vojenskou silou či místem narození.

Autor této práce chápe kyberprostor jako prostor pro tvorbu, výměnu a uchovávání informací s možností neomezené komunikace a vytváření nových identit. Tento prostor je opakem světa reálného. Takový prostor představuje v současné době prostředí internetu, který právě umožňuje neomezenou komunikaci, výměnu, tvorbu a uchovávání informací a zároveň možnost si v něm zvolit libovolnou identitu, která je odlišná od té reálné. Internet i podle názoru autora práce tedy naplňuje myšlenku „zároveň nikde a někde".

2.7 Nosič informací

Pro objasnění tohoto pojmu je třeba nejdříve stanovit definici pojmů informace a data. Pro potřeby této práce bude její autor vycházet z definice, že informace jsou: *„Údaje, které byly zpracovávány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí stát informací"*.[27]

Vzhledem ke shora uvedené definici lze souhlasit s názorem Tomáše Gřivny[28], že by bylo přesnější používat termín nosič dat nebo datový nosič, nicméně trestní zákoník operuje s pojmem nosič informací. Samotný Gřivna chápe nosič informací jako: „***jakýkoli nosič dat v informační technice, tedy materiál, do kterého nebo na který lze zaznamenávat („zapsat") data, a z kterého lze data zpět získat („přečíst")***", např. pevný disk, CD, DVD, Blue-Ray, USB key apod. Za nosič informací však nelze považovat záznam zvuku nebo kinematografický záznam, popř. videozáznam, i když jsou zaznamenány např. na magnetické pásce.

[26] BARLOW, John Perry. A Declaration of the Independence of Cyberspace. In Electronic Frontier Foundation [online]. Davos, 1996 [cit. 2018-10-21]. Dostupné z WWW: https://www.eff.org/cyberspace-independence

[27] POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk), s. 24-25.). ISBN 80-868-9838-5.

[28] GŘIVNA, T. § 230 [Neoprávněný přístup k počítačovému systému a nosiči informací]. In ŠÁMAL, P. a kol. Trestní zákoník (EVK). 2. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 2300. ISBN 978-80-7400-428-5.

3 Historie kyberkriminality

Ruku v ruce s vývojem digitálních a informačních technologií se vyvíjela i počítačová kriminalita. Za počátek vzniku tohoto druhu kriminality v přibližně stejné podobě, jak jej známe dnes, můžeme označit začátek 80. let minulého století, kdy docházelo k masivnějšímu rozšíření počítačů i mezi nekomerční uživatele, zejména rok 1981, kdy byl na trh uveden první osobní počítač firmou IBM.

Autoři zabývající se historií vývoje počítačové kriminality uvádějí její různou etapizaci. Jedna z teorií dělí vývoj této kriminality do tří etap[29], které označuje a charakterizuje takto:

- **Počítačový pravěk** – období do uvedení prvního osobního počítače na trh,
- **Počítačový středověk** – období od roku 1981 do případu průniku ruské hackerské skupiny v čele s Vladimírem Levinem do systému banky City bank v roce 1994,
- **Počítačový novověk** – období od roku 1994; pro toto období je typické masové rozšíření počítačů a připojení k internetu.

Pokud budeme hovořit o počítačové kriminalitě na našem území (myšleno Česká republika, Česko-slovenská federativní republika a Československá socialistická republika), můžeme konstatovat, že se jedná o poměrně mladý jev. Je to dáno zejména tím, že do konce 80. let 20. století zde nebyly počítače pro domácí používání až tak dostupné, pokud pomineme nadšence, kteří si draze v prodejnách Tuzex[30], nebo vlastním dovozem ze zahraničí, pořizovali 8bitové počítače zn. Atari, Comodore, Sinclair, nebo některý z počítačů domácí provenience jako byl např. Ondra, Didaktik Gama nebo PMD 85.

Vůbec první případ počítačové kriminality na našem území se odehrál v 70. letech 20. století a spočíval v jednání nespokojeného pracovníka Úřadu důchodového zabezpečení, který pomocí magnetu znehodnotil záznamy na magnetických páskách. Tento pracovník byl tehdy odsouzen na 10 let odnětí svobody za trestný čin sabotáž[31].

[29] MATĚJKA, M. Počítačová kriminalita. Praha: Computer Press, 2002. s. 17-18. ISBN 80-722-6419-2.

[30] TUZEX – Podnik zahraničního obchodu, který provozoval speciální prodejny na území ČSSR, ve kterých probíhal prodej zboží všeho druhu za cizí měny nebo odběrní poukázky, tzv. bony.

[31] Smejkal, V. Informační a počítačová kriminalita v České republice, MV ČR, 1999. [online].[cit. 2017-12-09]. Dostupné z WWW: <https://web.archive.org/web/20001202015000/http://www.mvcr.cz/casopisy/studie/diskuse/analyza2.html>

4 Formy kyberkriminality

V literatuře zaměřené na počítačovou a kybernetickou kriminalitu se můžeme dočíst, že o této kriminalitě, a zejména jejich formách, se vedou čtyři diskurzy (legislativní, akademický, expertní a laický). Vzhledem k rozsahu zadání práce nebude autor podrobně rozebírat jednotlivé myšlenkové proudy, ale bude vycházet z rozdělení kyberkriminality jak jej uvádí Aleš Završnik[32], který ji v širším smyslu na základě tzv. „budapešťské úmluvy“[33] rozděluje do tří skupin:

- kriminalita spojená s integritou informačního systému a dat, kdy terčem protiprávního jednání je ohrožení důvěrnosti počítačových dat, informačního sytému nebo ohrožení jejich integrity nebo přístupnosti,
- kriminalita spojená s obsahem
  a) sexuální obsah (dětská a „extrémní“ pornografie)
  b) násilný obsah (kybernetické obtěžování a nenávistný projev)
  c) porušení práv duševního vlastnictví,
- kriminalita spojená s počítači, kdy informační a komunikační technika je nástrojem pro páchání „klasické kriminality“.

4.1 Protiprávní jednání zaměřené proti počítačům a integritě a dostupnosti dat a systémů

Jedná se o jednání, které je namířené proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů. Takovým jednáním je[33]:

- jakýkoliv úmyslný neoprávněný přístup k počítačovému sytému nebo k jeho části;
- jakýkoliv úmyslný neoprávněný, technickými prostředky provedený, odposlech neveřejného přenosu počítačových dat do počítačového systému, z něj, nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému přenášejícího taková počítačová data;
- jakékoliv úmyslné neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat;

[32] ZAVRŠNIK, A. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR), s. 16. ISBN 978-80-7552-758-5.

[33] ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 56.

- jakékoliv úmyslné neoprávněné závažné omezení funkčnosti počítačového systému vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat;
- úmyslné neoprávněné jednání spočívající v pomoci ke spáchání již shora uvedených protiprávních jednání dané:
  1) vyrobením, prodejem, opatřením za účelem použití, dovozem nebo jiným zpřístupněním zařízení, včetně počítačového programu, jehož pomocí lze spáchat shora uvedená jednání nebo zpřístupněním počítačového hesla, přístupového kódu nebo podobných dat, kterými lze získat přístup k počítačovému sytému nebo jeho části;
  2) držením jedné z položek uvedených v bodě jedna s úmyslem, že bude použito pro shora uvedená protiprávní jednání.

Nejčastějším a nejznámějším shora popisovaným protiprávním útokem je šíření a použití škodlivého softwaru, který je v současnosti označován anglickým výrazem malware. Tento pojem v sobě sdružuje veškerý škodlivý software, který známe pod různými názvy jako jsou viry, červi, Trojské koně apod. a nejčastěji bývá distribuován formou příloh e-mailové pošty. Jedná se o software, který byl vytvořen za různými účely, např. k získání přístupu do počítačového systému, nebo narušení jeho činnosti, či získání dat nebo informací.

Dalším známým jednáním jsou tzv. DoS a DDoS útoky. Jedná se o formy útoků na internetové služby nebo webové stránky vyřazením či snížením výkonu napadeného zařízení (např. serveru nebo systému) za použití opakujících se dotazů či požadavků, které má zařízení vykonat za účelem jeho zahlcení. Tento útok se pak projevuje zpomalením nebo úplnou nefunkčností webových stránek nebo internetové služby. Dle některých lidí z komunity vyznávající svobodu na internetu není DDos útok kriminálním činem, ale pouze jednáním, jehož účelem je: „*stejně jako v případě demonstrace na nějakém prostranství, upozornit na sebe, vyjádřit s něčím nesouhlas, projevit se“*.[34]

[34] WIFT. Co to je DDoS útok a jak se dělá? Diit.cz: Novinky a informace o hardware, software a internetu [online]. 24.1.2012, 2012 [cit. 2018-01-08]. ISSN 1213-2225. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

Popisované formy tohoto protiprávního jednání jsou některými autory, např. Romanem Svatošem[35], nazývány přímou počítačovou kriminalitou a ostatní formy, popisované v následujících kapitolách, jako nepřímá počítačová kriminalita.

4.2 Protiprávní jednání spojené s obsahem

Do této kategorie patří protiprávní jednání související s obsahem elektronické komunikace, např. „závadný“ obsah zveřejňovaných, ukládaných a sdílených obrazových, audiovizuálních nebo textových souborů v počítačovém systému nebo síti. „Závadným“ obsahem je myšlena pornografie, veřejné nenávistné projevy vůči příslušnosti k určitému národu, rase nebo náboženskému vyznání, nebo veřejné podněcování ke spáchání teroristického činu, či vychvalování jeho pachatele. Aleš Završnik[36] řadí do této skupiny i projevy kyberšikany a kyberstalkingu.

4.2.1 Dětská a „tvrdá“ pornografie

Podle „budapešťské úmluvy“[37] jde o úmyslné a neoprávněné jednání spočívající ve výrobě, nabízení, zpřístupnění, distribuci, přenosu nebo opatřování dětské a „tvrdé“ pornografie prostřednictvím počítačového systému. Protiprávním jednáním je ale i uchovávání dětské pornografie v počítačovém systému nebo na datovém nosiči.

Dětskou pornografií je podle této úmluvy materiál vizuálně znázorňující osobu nezletilou nebo takovou, která se jí zdá být, jak se účastní sexuálně jednoznačného chování, nebo realistické zobrazení účasti nezletilé osoby na popisovaném chování.

Pojem „tvrdé“ pornografie „budapešťská úmluva“ ani dodatky k ní nestanovuje, ale v kontextu českého právního řádu lze tento pojem chápat jako pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které znázorňuje pohlavní styk se zvířetem [38].

---

[35] SVATOŠ, Roman. Počítačová kriminalita. AUSPICIA [online]. VŠERS, 2013(1), s. 171-178 [cit. 2018-11-07]. ISSN 1214-4967. Dostupné z WWW: https://vsers.cz/wp-content/uploads/2017/02/Auspicia-2013-1.pdf

[36] ZAVRŠNIK, Aleš. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR), s. 16. ISBN 978-80-7552-758-5.

[37] ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). Oddíl 3. In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 56.

[38] GŘIVNA, T. § 191 [Šíření pornografie]. In ŠÁMAL, P. a kol. Trestní zákoník (EVK). 2.vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 1880. ISBN 978-80-7400-428-5.

4.2.2 Šíření rasistického a xenofobního materiálu

Jedná se o úmyslné rozšiřování nebo zpřístupňování rasistických nebo xenofobních materiálů veřejnosti za využití počítačového systému. Zároveň se toto dotýká úmyslného jednání spočívající ve veřejném urážení osob z důvodu příslušnosti k rase, rodovému, národnímu nebo etnickému původu a náboženskému vyznání, které je uskutečněno počítačovou sítí.

V dodatku k „budapešťské úmluvě“ je definován rozsah pojmu rasistického a xenofobního materiálu jako: „*jakýkoli písemný materiál, obraz nebo jiné vyjádření myšlenek nebo teorií, který obhajuje, podporuje nebo podněcuje nenávist, diskriminaci nebo násilí, proti jakémukoli jednotlivci nebo skupině jednotlivců, na základě rasy, barvy pleti, rodového nebo národního nebo etnického původu, jakož i náboženství, pokud je použito jako záminka namísto nějakého z těchto atributů*“.[39]

4.2.3 Porušení práv duševního vlastnictví

Jedná se o neoprávněné jednání, které porušuje autorská práva, tak jak jsou definována na základě implementace mezinárodních smluv a závazků do národního práva. Předmětem ochrany jsou literární, umělecká a vědecká díla, která jsou výsledkem tvůrčí činnosti a jsou vyjádřena v jakékoliv vnímatelné podobě, včetně elektronické, a to trvale i dočasně.[40] Dle autorského zákona se za takové dílo považuje i počítačový program, fotografie a výtvor vyjádřený postupem podobným fotografii v případě, že jsou autorovým vlastním duševním výtvorem.

Nejznámějším popisovaným jednáním je stahování filmů a hudby na internetu za použití výměnných sítí peer-to-peer (P2P). Tyto sítě umožňují sdílet soubory, které velmi často představují filmy, hudbu nebo programy. To představuje riziko protiprávního jednání, neboť sdílením, tedy možností stažení, těchto dat dochází k porušování autorských práv, protože k tomu autor nedal souhlas. Mezi nejznámější P2P sítě patří např. DC++, Napster, Shareaza a další.

V poslední době došlo téměř úplně k přesunu trestné činnosti z historicky dominantního prostředí výměnných sítí do segmentu datových úložišť, přičemž pro

[39] ČESKO. Sdělení č. 9/2015 Sb.m.s., Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 3.

[40] ČESKO. Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). § 2 Předmět práva autorského. In *Sbírka zákonů, Česká republika. 2000*, částka 36.

výměnu odkazů a případně hesel ke komprimovaným materiálům s obsahem autorsky chráněných děl šířených v rozporu s autorským právem, jsou využívána tematická fóra a diskuse. Tyto odkazy jsou směrovány do datových úložišť, kde jsou tato díla tímto způsobem sdílena. V tomto směru je využíváno tzv. cloudových služeb, které jsou primárně určeny pro potřeby vzájemného sdílení dat úzce komunitních a firemních skupin.

4.3 Protiprávní jednání páchané pomocí počítače

Do této kategorie by se podle jejího pojmenování daly zařadit všechny skupiny kyberkriminality, protože všechny jsou páchány za využití počítače a počítačovými sítěmi, ale jak již bylo v úvodu kapitoly řečeno, jedná se o kriminalitu spojenou s počítači, kdy informační a komunikační technika je nástrojem pro páchání „klasické kriminality".

Jedná se zejména o podvody, tedy majetkovou kriminalitu, a krádeže identit. Nejtypičtějším příkladem je neoprávněné získání dat k platebním kartám a jejich následné zneužití k platbám na internetu. K získání těchto dat je užito velmi často podvodného jednání, které se označuje anglickým slovem phishing (rybaření).

Podvody patří k nejčastěji páchané protiprávní činnosti a tudíž i k nejčastěji šetřeným trestným činům páchaných na internetu, což dokládají statistické údaje Policie ČR (příloha č. 2). Škála podvodných jednání je velmi široká. Mezi projevy této trestné činnosti patří např. o tzv. nigerijské podvody, phishing, podvodné e-shopy nebo webové aukční (inzertní) podvody.

Při podvodné činnosti jsou pachateli poslední dobou využívány různé techniky, které jsou velmi často společně kombinovány. Jedná se v první řadě o různé způsoby jak skrýt, zamaskovat, svou pravou identitu. K tomuto slouží různé anonymizační způsoby k zakrytí své skutečné IP adresy, jako například použití spojení přes anonymní proxy servery, anonymizační aplikace (tzv. anonymizéry), použití virtuální soukromé sítě (tzv. VPN), e-mail spoofing[41], krádeže identit a další. V této kapitole budou dále přiblíženy tři nejčastěji využívané typy podvodů, u kterých jsou i popsány některé způsoby využití různých anonymizačních a podvodných technik.

[41] Email spoofing – technika použitá k tomu, aby se doručený e-mail "tvářil" jako by byl odeslán z e- mailového účtu podepsaného odesílatele.

4.3.1 Nigerijské podvody

Jedná se asi o nejstarší typ podvodného jednání v prostředí internetu, který je znám i pod označením **SCAM 419**[42]. Původně byly tyto podvody páchány mimo počítačovou síť. V této prvotní formě probíhal podvod v několika variantách. V jedné z nich tak, že byl poškozenému doručen dopis, ve kterém ho oslovil vysoký nigerijský vládní úředník s tím, že hodlá uprchnout ze země a chce si vzít sebou nakradené peníze, k čemuž potřebuje pomoc poškozeného, za kterou sliboval lákavě vysokou odměnu. Poškozený byl požádán o sdělení svých bankovních údajů, že mu bude na jeho účet převedena určitá částka, ze které si poškozený měl ponechat dohodnutou, velmi vysokou provizi, a zbylou částku poté poslat dál podle instrukcí. Jakmile poškozený souhlasil a odpověděl na dopis, začaly být od něj postupně požadovány peníze na poplatky za převod, na úplatky apod. Požadavky byly požadovány do té doby, dokud byl poškozený ochoten platit.

Rozvoj informačních technologií, zejména internetu a elektronické komunikace, umožnil za velmi nízké náklady masové rozšíření tohoto druhu podvodů. Podvody jsou páchány pod různými záminkami, ale princip vylákání peněz od obětí zůstává prakticky nezměněn. Známé jsou podvody, kdy poškozený reaguje na inzerát zveřejněný na internetovém inzertním portále s cenově výhodnou nabídkou prodeje vozidla ze zahraničí. Poškozený je nejdříve požádán o zaplacení poloviny ceny vozidla. Když tak učiní, je mu odeslán internetový odkaz na webové stránky přepravní společnosti, kde může sledovat trasu přepravovaného vozidla. Po nějaké době je e-mailem kontaktován údajnou přepravní společností, že je třeba zaplatit celní poplatky apod. Požadavky na placení různých poplatků se opět stupňují, dokud je poškozený ochoten platit.

Kromě vozidel se k prodeji nabízí např. psi či pronájem bytů. Po kladném reagování na tyto inzeráty je další postup naprosto stejný jako ve výše popsaném případu s prodejem vozidla ze zahraničí. Společným znakem těchto podvodných jednání zpravidla bývá současný pobyt prodejce v zahraničí a špatná čeština v písemném projevu.

4.3.2 Phishing

Jedná se o anglický výraz, jehož význam v češtině znamená „rybaření“[43]. Tímto termínem jsou označovány podvodné techniky s cílem například vylákat přístupové údaje

[42] Příchod hackerů: nigerijský scam „419“. Root.cz - informace nejen ze světa Linuxu [online]. Internet Info, 2014 [cit. 2019-03-05]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-nigerijsky-scam-419/

[43] Co je phishing?: Vyhněte se e-mailovým podvodům a útokům [online]. AVAST Software [cit. 2019- 03- 05]. Dostupné z: https://www.avast.com/cs-cz/c-phishing

k internetovému bankovnictví, e-mailovým účtům a k jiným účtům různých internetových služeb[44] (PayPal, Skype, Facebook, Google, eBay apod.). V těchto případech se jedná o tzv. krádeže identity, protože podvodník vždy tyto údaje zneužije ke svému majetkovému prospěchu tím způsobem, že díky získaným údajům se vydává za osobu, od které tyto údaje získal.

Podvod probíhá tak, že oběti je zaslán e-mail, který se snaží vyvolat dojem, že byl odeslán např. bankou, které je oběť klientem, s cílem vylákat od něj důvěrné informace. Toto se děje např. pod záminkou aktualizace bezpečnostních údajů, dočasného zablokování účtu nebo platební karty apod. V zaslané zprávě se pak nachází hypertextový odkaz na podvodné stránky, které se tváří jako oficiální webové stránky banky, kde je klient vyzván např. k vyplnění formuláře se zadáním přihlašovacích údajů do internetového bankovnictví.

V poslední době se množí forma „cíleného rybaření“ (anglicky **spear phishing[45]**). Tato metoda spočívá v tom, že útočník se zaměřuje na konkrétní oběť, ke které má předem zjištěné některé informace, např. firemní chování apod. Poté je zaslán e-mail adresovaný přímo vybrané osobě s tím, že pisatel v něm vystupuje typicky jako jednatel či ředitel společnosti, který prostřednictvím e-mailové komunikace požaduje provedení platby z firemního účtu na účet zahraniční. V těchto případech se doručený e-mail tváří jako by byl odeslán z e-mailového účtu podepsaného odesílatele. K tomuto je využívána další z podvodných technik, která je anglicky nazývána **e-mail spoofing**.

4.3.3 Webové aukční (inzertní) podvody

Webové aukční (inzertní) podvody již delší dobu patří mezi nejčastěji páchanou protiprávní činnost, která spočívá v nabídce prodeje určitého zboží na aukčních nebo inzertních internetových portálech, kdy po zaplacení celé ceny zboží nebo její části nedojde k jeho zaslání, nebo je zaslána jiná, zpravidla bezcenná věc.

V českém prostředí jsou pro zveřejňování podvodných nabídek využívány zvláště inzertní portály, jako Bazos.cz nebo Sbazar.cz, a v případě aukčních portálů se jedná jednoznačně o Aukro.cz. Pro ztížení své identifikace využívají pachatelé anonymní předplacené SIM karty, pomocí kterých komunikují s poškozenými a ke znemožnění

[44] Phishing - příklady. In: Support.zcu.cz/STRÁNKY UŽIVATELSKÉ PODPORY [online]. Plzeň: ZČU Plzeň [cit. 2019-03-05]. Dostupné z: https://support.zcu.cz/index.php/Phishing_-_příklady

[45] ČERMÁK, Miroslav. Spear phishing je cílený phishing, kterému se lze jen těžko bránit [online]. 2012 [cit. 2019-03-05]. Dostupné z: https://www.cleverandsmart.cz/spear-phishing-je-cileny-phishing-kteremu-se-lze-jen-tezko-branit/

dohledání podvodně vylákaných finančních prostředků využívají jeden z dalších „výdobytků“ dnešní anonymní doby – anonymní předplacené platební karty[46] (např. Blesk peněženka, biip, Napka, Cool karta a další).

Při páchání těchto podvodů jsou pachatelé stále rafinovanější, protože mnoho kupujících bývá již obezřetnějších a nedůvěřivých k platbám předem. V poslední době bylo zaznamenáno několik případů, při kterých pachatel, vystupující coby prodávající, pro zvýšení své důvěryhodnosti zašle během e-mailové komunikace s kupujícím občanský průkaz, řidičský průkaz, náhled z elektronického výpisu bankovního účtu k osobě, na kterou jsou doklady vystaveny a případně ještě pošle naskenovaný doklad, fakturu, o nákupu prodávaného zboží. Kupující takto získá důvěru a zašle požadovaný finanční obnos na bankovní účet, ale zakoupené zboží již neobdrží a prodejce se stane nekontaktním.

V takových případech pak nespokojený kupec vyhledá, nebo jinak kontaktuje, osobu, jejíž naskenované doklady obdržel, ale ten o žádném prodeji neví. Později je zjištěno, že osoba, které patří uvedené doklady, se stala nějakou dobu předtím obětí podvodného jednání, dalo by se hovořit o jakési formě phishingu, kdy například ve snaze získat půjčku kontaktoval inzerenta nabízejícího službu sjednání úvěru. Během jednání o poskytnutí této služby je od zájemce vylákán sken jeho osobních dokladů (občanský, řidičský průkaz). Pomocí takto získaných skenů dokladů jsou přes internet založeny bankovní účty u českých bank. Bankovní účty jsou později použity pro již popisované podvodné jednání. Podvodně získané finanční prostředky jsou pak z účtů za použití internetového bankovnictví směněny za virtuální měny. Směna je prováděna na různých internetových burzách, které obchodují s virtuálními měnami.

[46] COUFALOVÁ, D. Anonymní platební karty: To, že jsem paranoidní, ještě neznamená, že po mě nejdou. Ušetřeno.cz [online]. 2017 [cit. 2019-03-05]. Dostupné z: https://www.usetreno.cz/anonymni-platebni-karty/#gref

5 Postižitelnost kyberkriminality v prostředí českého práva

Česká republika se řadí mezi státy, které se snaží normativně regulovat a trestněprávně postihovat známé projevy kyberkriminality. Trestně právní odpovědnost za spáchání všech forem kyberkriminality, které byly popsány v předchozí kapitole, je v trestním právu stanovena ve zvláštní části trestního zákoníku. Jde jednak o nové trestné činy, jejichž skutkové podstaty byly do trestního zákoníku implementovány na základě mezinárodních smluv, ale i o trestné činy českému trestnímu právu již známé („klasická" kriminalita). Některé trestné činy „klasické" kriminality byly doplněny kvalifikovanými skutkovými podstatami, které reflektují na jejich spáchání pomocí nebo prostřednictvím počítače či počítačovou sítí, čímž české trestní právo poukazuje na vyšší společenskou škodlivost takového jednání.

Vzhledem ke skutečnosti, že jednání podléhající trestněprávní odpovědnosti, která jsou, nebo by mohla být, páchána pomocí nebo prostřednictvím počítače či počítačové sítě, je v českém trestním právu mnoho, budou v následujících podkapitolách popsány pouze ty, jejichž formy byly uvedeny ve předchozí kapitole.

5.1 Postižitelnost protiprávního jednání spojeného s obsahem

Skutkové podstaty trestných činů spojených s šířením „závadného" obsahu formou sdílení či zveřejněním prostřednictvím počítačové sítě jsou obsaženy ve třech hlavách zvláštní části trestního zákoníku. Jedná se o trestné činy, u nichž je dána jejich příslušnost do skupiny kyberkriminality na základě kvalifikovaných skutkových podstat, a jde tedy o zpřísnění trestní sankce za jejich spáchání pomocí nebo prostřednictvím počítačové sítě.

5.1.1 Trestné činy související s pornografií

V českém trestním právu není pojem pornografie legislativně vymezen, nicméně se pornografické dílo charakterizuje tím, že: „*zvláště intenzivním způsobem zasahuje a podněcuje sexuální pud, překračuje podle převládajících názorů ve společnosti uznávané hranice sexuální slušnosti, uráží neakceptovatelným způsobem cit pro sexuální slušnost, vyvolává pocit studu*".[47]

[47] GŘIVNA, T. § 191 [Šíření pornografie]. In ŠÁMAL, P. a kol. Trestní zákoník (EVK). 2. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 1880. ISBN 978-80-7400-428-5.

Posouzení, zda se jedná o pornografii, je na zhodnocení celkového dojmu, zejména toho, zda dílo způsobuje morální pohoršení a zda podněcuje sexuální pud. V odborné literatuře nalezneme dělení pornografie do tří skupin:

1) „tvrdou“ pornografii,
2) dětskou pornografii,
3) prostou pornografii.

Skutkové podstaty trestných činů týkajících se pornografie jsou umístěny ve zvláštní části trestního zákoníku, konkrétně v hlavě třetí. Sem zákonodárce umístil trestné činy proti lidské důstojnosti v sexuální oblasti.

Konkrétní ustanovení, která se týkají trestně právní odpovědnosti formy kyberkriminality v souvislosti s „tvrdou“ pornografií jsou obsaženy v **§ 191 (Šíření pornografie)**. V prvním odstavci je stanovena základní skutková podstata a vlastní vymezení pojmu „tvrdé“ pornografie – tedy, že jde o pornografické dílo, v němž se projevuje násilí či neúcta k člověku nebo znázorňuje pohlavní styk se zvířetem. Ve třetím odstavci je pak kvalifikovaná skutková podstata, a k tíži pachatele je přičteno, když takové pornografické dílo „*nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří*“[48] veřejně přístupnou počítačovou sítí.

Dětskou pornografií je myšleno pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, která se jeví být dítětem[49]. Trestněprávní odpovědnost je dána v **§ 192 (Výroba a jiné nakládání s dětskou pornografií),** kdy projevu kyberkriminality se týká ustanovení ve třetím odstavci písmeno b). V tomto ustanovení je kvalifikovaná skutková podstata, která k tíži pachatele přičítá to, když dětskou pornografii nabídne, činí veřejně přístupnou, zprostředkuje, uvede do oběhu, nebo prodá prostřednictvím veřejně přístupnou počítačovou sítí.

5.1.2 Trestné činy s nenávistným obsahem

Trestněprávní odpovědnost za jednání hanobící některý národ, rasu nebo etnickou skupinu a rovněž tak skupinu osob pro jejich rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, nebo pro jejich náboženské vyznání, byla již v českém trestním právu zakotvena. Vzhledem k rozšíření používání internetu, resp. jeho

[48] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 191 odst. 1. In Sbírka zákonů, Česká republika. 2009, částka 11.

[49] GŘIVNA, T. § 191 [Šíření pornografie]. In ŠÁMAL, P. a kol. Trestní zákoník (EVK). 2. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 1889. ISBN 978-80-7400-428-5.

zneužívání k šíření tohoto nenávistného obsahu, zejména možnosti přístupu obrovského množství lidí k tomuto obsahu, přidal zákonodárce, k již existujícím trestným činům, kvalifikované skutkové podstaty, které zpřísňují tresty při jeho šíření za pomoci počítačové sítě.

Skutkové podstaty těchto trestných činů jsou uvedeny ve zvláštní části trestního zákoníku, konktrétně v těchto hlavách:

Hlava IX, Díl 1 (Trestné činy proti základům České republiky, cizího státu a mezinárodní organizace)

- **§ 312e** Podpora a propagace terorismu

Hlava X., Díl 5 (Trestné činy narušující soužití lidí)

- **§ 355** Hanobení národa, rasy, etnické nebo jiné skupiny
- **§ 356** Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

Hlava XIII., Díl 1 (Trestné činy proti lidskosti)

- **§ 403** Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
- **§ 407** Podněcování útočné války

5.1.3 Kyberstalking

Anglický výraz stalking (česky pronásledování) znamená dlouhodobé, opakované, systematicky stupňované obtěžování a pronásledování. V případě kyberstalkingu se jedná o stejné jednání prováděné za pomoci informačních a komunikačních technologií[50].

V českém trestním právu je toto jednání postižitelné díky § 354 odst. 1, písm. c) trestního zákoníku (Nebezpečné pronásledování), ve kterém je stanoveno, že nebezpečného pronásledování se dopustí ten, kdo: „*jiného dlouhodobě pronásleduje tím, že jej vytrvale prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osobo jemu blízkých*“.[51]

[50] Prevence kriminality v České republice: Stalking a kyberstalking [online]. Praha: MV ČR, 2019 [cit. 2019-03-05]. Dostupné z: http://www.prevencekriminality.cz/kyberkriminalita-testovaci-provoz/clanky-informace/stalking-a-kyberstalking/

[51] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 354 odst. 1, písm. a). In *Sbírka zákonů, Česká republika*. 2009, částka 11.

5.1.4 Porušování práv duševního vlastnictví

Zvláštní skupinu představuje **kyberkriminalita spojená s porušováním práv duševního vlastnictví**. Jak již bylo řečeno v předchozí kapitole o formách této protiprávní činnosti, zařazujeme ji rovněž k trestným činům spojených s obsahem. Na rozdíl od předchozích trestných činů však nemá kvalifikovanou skutkovou podstatu v souvislosti s jejím spácháním pomocí nebo prostřednictvím počítačové sítě. V rámci českého trestního práva se jedná o trestný čin uvedený v **§ 270** trestního zákoníku[52] (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi) ve zvláštní části trestního zákoníku (**Hlava VI., Díl 4 – Trestné činy proti průmyslovým právům a proti autorskému právu**).

5.2 Postižitelnost protiprávního jednání proti počítačům, integritě a dostupnosti dat a systémů

Jedná se převážně o trestné činy, u nichž je objektem ochrana před protiprávním jednáním proti integritě informačního systému a dat, nebo ohrožení jejich přístupnosti. Tyto trestné činy obsahuje **Hlava V. – Trestné činy proti majetku** ve zvláštní části trestního zákoníku. Jak již název této hlavy trestního zákoníku napovídá, zákonodárce zde garantuje ochranu vlastnických a majetkových práv, kterými jsou např. nerušené držení nebo užívání věci. Jsou to trestné činy, jejichž skutkové podstaty byly do českého trestního práva implementovány na základě „budapešťské úmluvy“[53] a jedná se o:

- **§ 230** Neoprávněný přístup k počítačovému systému a nosiči informací

Ustanovení tohoto trestného činu postihují jednání spočívající v neoprávněném přístupu k počítačovému systému nebo nosiči informací, který může být proveden překonáním různých bezpečnostních opatření (např. hesla, PIN, postupu apod.) nebo na základě získaného přístupu. Jak uvádí Vladimír Smejkal[54] neoprávněným přístupem, je každý přístup, který není oprávněný.

- **§ 231** Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

[52] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 270. In *Sbírka zákonů, Česká republika*. 2009, částka 11.

[53] ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 56.

[54] SMEJKAL, V. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 398. ISBN 978-80-7380-501-2.

Zde je postihováno jednání toho, kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv nebo neoprávněného přístupu k počítačovému systému a nosiči informací vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává tyto prostředky[55]:

- zařízení nebo jeho součást,
- postup pro neoprávněný přístup,
- nástroj nebo jiný prostředek,
- počítačový program,
- počítačové heslo,
- přístupový kód,
- data.

- **§ 232** Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Do skupiny této kriminality patří rovněž **protiprávní jednání související s jakýmkoliv úmyslným neoprávněným, technickými prostředky provedeným odposlechem neveřejného přenosu počítačových dat do počítačového systému**. Postižitelnost za toto protiprávní jednání je řešena ustanovením **§ 182** (Porušení tajemství dopravovaných zpráv) uvedeným ve zvláštní části trestního zákoníku**, Hlava II., Díl 2 – Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství**.

5.3 Postižitelnost protiprávního jednání páchaného pomocí počítače

Jedná se o trestné činy spojené s počítači, kdy informační a komunikační technika je hlavním a převažujícím nástrojem pro páchání tzv. „klasické“ kriminality. Jde především o majetkovou trestnou činnost, konkrétně podvodná jednání různého druhu.

5.3.1 Podvodná jednání

Byť se zdá pojem podvodné jednání známým, je třeba si jeho význam blíže objasnit. Trestní právo považuje za podvodné jednání uvedení někoho v omyl, využití něčího omylu, nebo zamlčení podstatných skutečností[56]. V § 120 trestního zákoníku pak zákonodárce pamatoval i na podvodná jednání páchaná prostřednictvím technického

[55] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 231. In Sbírka zákonů, Česká republika. 2009, částka 11.

[56] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 209. In Sbírka zákonů, Česká republika. 2009, částka 11.

zařízení. Z tohoto ustanovení vyplývá, že: „*uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným*“.[57]

Skutkové podstaty podvodu i trestně právní odpovědnost obsahuje § 209 trestního zákoníku, kde je v prvním odstavci uvedena základní skutková podstata. V dalších odstavcích tohoto ustanovení jsou uvedeny kvalifikované skutkové podstaty, ale ani jedna z nich se netýká spáchání pomocí nebo prostřednictvím počítače či počítačovou sítí.

5.4 Ostatní trestné činy

V trestním právu existují i další trestné činy obsahující kvalifikovanou skutkovou podstatu týkající se jejich spáchání prostřednictvím počítačové sítě. Jde např. o trestné činy, které svou povahou můžeme zařadit mezi formy kyberkriminality související s obsahem, ale dle názoru autora nelze z jejich skutkových podstat považovat jejich obsah za nenávistný projev nebo o obtěžování. Mezi tyto trestné činy autor práce řadí např. neoprávněné nakládání s osobními údaji dle § 180 trestního zákoníku, trestný čin pomluva dle § 184 trestního zákoníku, nebo šíření toxikománie dle § 287 trestního zákoníku. U těchto trestných činů dle jejich skutkových podstat nejde o projevy s nenávistným projevem nebo obtěžování, např. u trestného činu pomluva jde o sdělení nepravdivého údaje, který je: „*způsobilý značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu“*.[58]

Další a poměrně početnou skupinu tvoří trestné činy, které lze páchat za využití počítače či počítačové sítě, ale jejich základní ani kvalifikované skutkové podstaty neobsahují jako jeden z povinných znaků použití počítače nebo počítačové sítě jako prostředek ke spáchání protiprávního jednání. Zařadit tyto trestné činy k projevům kyberkriminality lze pouze za předpokladu, že počítač nebo počítačová síť jsou rozhodujícím nástrojem k jejich páchání a zároveň při jejich vyšetřování jsou uplatňovány stejné metody a postupy jako u vyšetřování kybernetické kriminality.

[57] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 120. In *Sbírka zákonů, Česká republika*. 2009, částka 11.

[58] ČESKO. Zákon č. 40/2009 Sb., Trestní zákoník, § 184. In *Sbírka zákonů, Česká republika*. 2009, částka 11.

6 Objasňování a vyšetřování kyberkriminality

V současné době je páchání kybernetické kriminality na vzestupu. Dá se hovořit o tom, že počet evidovaných případů roste téměř exponenciální řadou, což dokládají grafy vývoje trestné činnosti spáchané prostřednictvím internetu nebo jinými počítačovými sítěmi od roku 2011 do 2017 (příloha č. 3). Za faktory ovlivňující stoupající počet tohoto druhu protiprávního jednání můžeme označit vysoký stupeň anonymity, možnost páchání trestné činnosti z pohodlí domova, důvěřivost uživatelů internetu, a v neposlední řadě i možnost většího zisku s podstatně menšími riziky zranění, odhalení a odsouzení – viz tabulka porovnání klasického a kybernetického zločinu[59] .

Tab. 1: porovnání klasického a kybernetického zločinu[54]

Parametr	**Průměrné ozbrojené přepadení**	**Průměrný kybernetický útok**
Riziko	Pachatel riskuje, že bude zraněn či zabit	**Bez rizika fyzické újmy**
Zisk	průměrně 3 -5 tisíc USD	**Průměrně 50 - 500 tisíc USD**
Pravděpodobnost dopadení	dopadeno 50 - 60% útočníků	**dopadeno cca 10% útočníků**
Pravděpodobnost odsouzení	odsouzeno 95% dopadených útočníků	**z dopadených útočníků dojde k soudnímu projednávání pouze 15% útočníků a z nich je odsouzeno jen 50%**
Trest	průměrně 5 - 6 let, pokud pachatel při loupeži nikoho nezranil	**průměrně 2 - 4 roky**

6.1 Odbory/Oddělení analytiky a kybernetické kriminality

Na trend nárůstu počtu trestných činů a přestupků, v nichž figuruje počítač, počítačová síť, data, nebo programy, jako předmět zájmu těchto jednání, nebo jako nástroj k jeho páchání, musela tedy reagovat i Policie České republiky. Její reakce spočívá zejména v odborném školení policistů základních útvarů, kteří jako první přijímají oznámení o těchto činech, a dále pak policistů služby kriminální policie a vyšetřování, kteří se podílejí na jejich objasňování, prověřování a vyšetřování. Hlavním opatřením ze strany policie je pak především to, že ve své organizační struktuře zřídila specializované součásti věnující se této problematice jak z hlediska objasňování, tak i vyšetřování. Jedná se o součásti jak s celostátní, tak s územně vymezenou působností.

[59] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. s 30. ISBN 978-80-247-1561-2.

6.1.1 Útvary s celostátní působností

Na celostátní úrovni se jedná o Sekci kybernetické kriminality Národní centrály proti organizovanému zločinu Služby kriminální policie a vyšetřování (dále jen NCOZ). Tato sekce sestává ze dvou odborů – odboru kybernetické kriminality a odboru vyšetřování kybernetické kriminality. Zatímco vedením trestního řízení v případech spadajících do kompetence NCOZ se zabývá odbor vyšetřování, zjišťování a vyhodnocování informací a dat důležitých pro trestní řízení, metodická a poradní funkce pro ostatní útvary Policie České republiky je náplní práce odboru kybernetické kriminality.

6.1.2 Útvary v podřízenosti krajských ředitelství

Podobná pracoviště jsou zřízena i u krajských ředitelství a jim podřízených územních odborů a městských ředitelství. Rozkazem policejního prezidenta č. 45/2017[60] byly u krajských ředitelství zřízeny Odbory analytiky a kybernetické kriminality, v jejichž rámci jsou tři oddělení. Jedná se o oddělení informatické podpory, oddělení kriminálních analýz a oddělení kybernetické kriminality. Část pracovníků oddělení kybernetické kriminality se zabývá vedením trestního řízení a část se zabývá zjišťováním a vyhodnocováním informací a dat důležitých pro trestní řízení, což bychom mohli nazvat jakousi „*technickou operativou*“. K této činnost patří např. účast při zajišťování výpočetní techniky, nebo zajišťování tzv. obrazů pevných disků počítačů. Oddělení kybernetické kriminality provádí úkoly a úkony trestního řízení ve věcech jim náležejících dle věcné příslušnosti dané trestním řádem. Jedná se o případy, ve kterých koná v prvním stupni řízení krajský soud[61]. Vzhledem k situaci, že počet takto závažných trestných činů je nízký, je např. na Krajském ředitelství policie Plzeňského kraje konáno prověřování a vyšetřování i u vybraných případů, u kterých koná v prvním stupni okresní soud. Dozor nad trestním řízení vykonává místně příslušné okresní státní zastupitelství. Vybírány jsou spisy např. na základě jejich skutkové složitosti, rozsahu a závažnosti.

Na úrovni územních odborů a městských ředitelství jsou pak zřízena oddělení analytiky a kybernetické kriminality, která mohou být dále organizačně členěna na skupinu případových analýz a skupinu kybernetické kriminality.

---

[60] ČESKO. Rozkaz policejního prezidenta č. 45 ze dne 6. března 2017, kterým se stanoví vzorová systemizace služebních a pracovních míst krajského ředitelství Policie České republiky a městského ředitelství Policie České republiky. Sbírka interních aktů řízení policejního prezidenta 2017.

[61] § 17 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Podrobněji se práce zabývá strukturou a činnostmi těchto oddělení působících v rámci územních odborů Krajského ředitelství policie Plzeňského kraje a Městského ředitelství policie v Plzni[62].

Na územních odborech a Městském ředitelství policie v Plzni nejsou tato oddělení nijak dále organizačně členěna. Oddělení vznikla transformací původních skupin případových analýz, jejichž pracovníci stejně do té doby plnili úkoly jak na úseku analytickém (případové analýzy, analýzy kriminality a analýzy dat), tak na úseku objasňování projevů kyberkriminality, a to včetně metodické podpory v této oblasti pro policisty základních útvarů. Kromě Městského ředitelství policie v Plzni, kde existuje již plnohodnotné oddělení, jsou tato oddělení obsazena pouze jedním pracovníkem.

Samotné trestní řízení jako takové vedou policisté zařazení na úseku vyšetřování na odděleních obecné a hospodářské kriminality. Policisté zařazení na oddělení analytiky a kybernetické kriminality pak kromě analytické činnosti, ať již sami, nebo cestou metodické pomoci základním útvarům policie, vyžadují data a informace k prověřovaným a vyšetřovaným věcem, provádějí vyhodnocení získaných dat a informací, a sami získávají informace z otevřených zdrojů na internetu a sociálních sítích. Jak již bylo dříve řečeno, zajišťují *„technickou operativu“*, a to např. včetně nasazení a vyhodnocení odposlechu a záznamu telekomunikačního provozu, nebo sledování věci.

Specializační kurz pro policisty zařazené na těchto odděleních přímo po linii kyberkriminality v rámci Policie České republiky není, pouze jsou tito policisté vysíláni na kurz „Kriminální zpravodajská analýza“. Tento vzdělávací program se však zaměřuje pouze na získání základních znalostí a dovedností v oblasti kriminální zpravodajské analýzy a na zdokonalení využívání analytických a informačních systémů, zejména programu Analyst’s Notebook. Vzhledem k uvedeným skutečnostem jsou policisté nuceni se sami sebevzdělávat, ať již prostřednictvím odborné literatury, nebo z poznatků získaných v rámci pracovních činností. Díky tomu jsou nově získané poznatky nebo informace týkající se kyberkriminality mezi pracovníky těchto pracovišť sdíleny napříč celou Policií České republiky.

Existují však různá odborná školení organizovaná jak ze strany krajských ředitelství, tak i Policejního prezidia a NCOZ. Tato školení jsou převážně zaměřována na policisty základních útvarů, a dále pak na policisty služby kriminální policie

[62] Pozn.: autor je zařazen na Oddělení analytiky a kybernetické kriminality Územního odboru Rokycany

a vyšetřování, kteří přijímají oznámení o těchto protiprávních jednání, činí k nim prvotní opatření a podílejí se na jejich objasňování, prověřování a vyšetřování. Obsahem školení jsou především zákonné způsoby získávání a vyžadování dat a informací důležitých pro trestní řízení a objasnění šetřeného případu.

6.2 Problematika uchovávání a rozsahu provozních a lokalizačních dat

Následující kapitola je věnována problematice uchovávání a rozsahu provozních a lokalizačních dat, tedy dat poskytovaných orgánům činným v trestním řízení (dále jen OČTŘ) a týkajících se elektronické komunikace. Zmíněn bude v současnosti platný legislativní rámec ukládající povinnost uchovávat tato data, a to v daném rozsahu (pohled ***de lega lata***) a dále pak budou nastíněny možné legislativní změny norem upravujících tuto oblast (pohled ***de lega ferenda***). Ukládání vybraných dat o uskutečněné elektronické komunikaci je stěžejní pro jejich další využití při objasňování a vyšetřování jak kyberkriminality, tak i jiných trestných činů, při jejichž páchání byly použity prostředky informačních a komunikačních technologií (dále jen ICT), nebo jsou informace zjištěné z těchto dat důležité pro trestní řízení jako takové.

6.2.1 Data retention – ukládání provozních a lokalizačních údajů

V českém právním řádu je otázka ukládání a doby uchování provozních a lokalizačních údajů, řešena v § 97 zákona č. 127/2005 Sb., zákon o elektronických komunikacích (dále jen ZoEK). Rozsah uchovávaných údajů je upraven Ministerstvem průmyslu a obchodu vyhláškou č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

Ze zákona o elektronických komunikacích vyplývají povinnosti uchovávat tyto data pouze fyzickým a právnickým osobám poskytujícím veřejně dostupnou službu elektronických komunikací, podrobněji viz kapitola 2.5.1 (Poskytovatel připojení). Nejdůležitější povinností vyplývající ze ZoEK je pro vyšetřování kyberkriminality doba uchování lokalizačních a provozních údajů, kterou zákon stanovuje na šest měsíců. Subjekty, které poskytují veřejně dostupnou službu elektronických komunikací, mají povinnost údaje ukládat po stanovenou dobu a v daném rozsahu o všech proběhlých elektronických komunikacích, tedy o uskutečněné komunikaci všech účastníků využívajících jejich služeb. Proces a způsob uchovávání předmětných dat je nazýván odbornou veřejností jako data retention.

V posledních několika letech je toto „plošné“ uchovávání provozních a lokalizačních dat předmětem mnoha diskuzí, ve kterých je jeho odpůrci označováno jako tzv. „plošné šmírování“ občanů ze strany státu, což považují za nepřípustné. Hlavním argumentem odpůrců data retention je právě ta skutečnost, že jsou ze zákona povinně uchovávány provozní a lokalizační údaje o všech účastnících, což dle jejich názoru znamená, že je stát považuje všechny za podezřelé z protiprávního jednání a že se z hlediska proporcionality jedná o nepřiměřený zásah do ústavně zaručených práv a svobod v porovnání s účelem, za jakým jsou tyto údaje uchovávány – tedy za účelem vyšetřování a objasňování kriminality. Tyto osoby požadují „plošné“ uchovávání dat zrušit a nahradit jej za tzv. „data freezing“, tedy „zmrazení“ stávajícího stavu údajů u konkrétního účastníka telekomunikačního provozu (podrobněji viz následující kapitola). Přitom si však neuvědomují skutečnost, že osoby podnikající v oblasti telekomunikačních činností (dále jen operátoři) budou stejně muset většinu provozních a lokalizačních údajů uchovávat po nějakou dobu kvůli případným reklamačním sporům ohledně jimi poskytovaných služeb, či jejich vyúčtování. Situace neexistence zákonné povinnosti pro poskytovatele uchovávat tato data nastala po 22. 3. 2011, kdy Ústavní soud zrušil ustanovení § 97 odst. 3 a odst. 4 ZoEK, tedy ustanovení ukládající tuto povinnost[63].

Autor bakalářské práce chápe argumenty odpůrců plošného uchovávání provozních a lokalizačních údajů, ale na druhou stranu si je nutné uvědomit, že stále značně roste podíl využívání komunikační techniky a technologií ve společnosti a bohužel i páchání velkého množství trestné činnosti, a to nejen u té označované jako přímá kyberkriminalita, ale i té tradiční kriminality. Právě u posledně jmenované kriminality je stále stoupající počet případů, kdy jsou informační a komunikační technika a technologie jedním z hlavních nástrojů pachatele k jejímu páchání. Na tento trend reagoval i senát Soudního dvora Evropské unie v rozsudku[64], kterým zrušil platnost směrnice Evropského parlamentu a Rady 2006/24/ES[65]. Konkrétně v bodu 49 tohoto rozsudku je konstatováno: „*Pokud jde o otázku, zda je uchovávání údajů způsobilé k dosažení cíle sledovaného směrnicí 2006/24, je třeba konstatovat, že údaje, které musí*

[63] ČESKO. Nález č. 94/2011 Sb., Ústavního soudu ze dne 22.3.2011 sp. zn. Pl. ÚS 27/2010. In *Sbírka zákonů, Česká republika*. 2011, částka 35.

[64] EVROPSKÁ UNIE. SOUDNÍ DVŮR EVROPSKÉ UNIE. Rozsudek ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12. Bod č. 49. In: *Curia.europa.eu*. Číslo ECLI:EU:C:2014:238

[65] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

být uchovávány podle této směrnice, s ohledem na rostoucí význam prostředků elektronické komunikace umožňují, aby vnitrostátní orgány příslušné v oblasti trestního stíhání měly další možnosti objasnit závažné trestné činy, a jsou tedy v tomto ohledu cenným nástrojem pro vyšetřování trestných činů. Uchovávání takových údajů tak lze považovat za způsobilé k dosažení cíle sledovaného uvedenou směrnicí.“

Senát v tomto bodu ale připouští data retention pouze jako jednu z dalších možností justičních orgánů k objasnění závažných trestných činů, tedy vůbec nezvažuje možnost, že v některých případech se jedná o u možnost jedinou.

Musíme si uvědomit jednoduchou věc a to, že policie, resp. všechny OČTŘ, se dozví o skutečnosti, že se stal nějaký trestný čin až po jeho spáchání, přičemž jde často o dobu v řádech dnů. Jednoduchou logickou úvahou tedy nemohou OČTŘ dopředu tušit kdy, kde a jaký trestný čin bude spáchán, a ani kým, aby mohly být dopředu uchovávány pouze provozní a lokalizační údaje pouze této osoby, místa, nebo času.

Pokud jde o otázku, zda ponechat subjektům poskytujícím veřejně dostupnou službu elektronických komunikací zákonem danou povinnost uchovávat provozní a lokalizační data, odpověď zní ano. Ohledně doby, po kterou mají být tyto údaje uchovávány, je autor práce názoru, že současná šesti měsíční lhůta je zcela dostačující. Bez možnosti data retention by bylo vyšetřování u mnoha trestných činů velmi ztíženo, a u některých zcela znemožněno.

Z pohledu de lege ferenda by měla být zákonná povinnost uchovávat určité údaje dána i poskytovatelům informační služby. Povinnost by byla dána na uchovávání údajů o datu, čase, IP adrese a portu přístupu ke službě, a dále případných platbách za poskytnuté služby. Jedná se o data, která mohou pomoci ustanovit uživatele služby.

6.2.2 Data freezing – zálohování dat

Jak doslovný překlad anglického názvu napovídá, jde o jakési „zmražení“ dat, přesněji jde o uložení (zálohování) dat v podobě a rozsahu v době jeho provedení. Od 1. 2. 2019 je účinná novela trestního řádu, která v § 7b zakotvuje oprávnění OČTŘ nařídit v případě zabánění ztráty, zničení či pozměnění dat důležitých pro trestní řízení osobě, která tato data drží, nebo je má pod svou kontrolou, aby je uchovala v nezměněné podobě. Povinnost uchovat uvedená data je po dobu, která je uvedena v příkazu OČTŘ, ale nesmí přesáhnout 90 dnů. Druhý odstavec tohoto ustanovení trestního řádu dává dokonce možnost OČTŘ vydání příkazu k znemožnění přístupu k těmto datům, pokud je to potřeba

k zabránění pokračování v trestné činnosti nebo jejím opakování. Uchování dat je jakási forma předběžného opatření, které OČTŘ poskytuje potřebný čas k následnému zajištění dat.

V praxi to např. znamená, že když OČTŘ v rámci prověřování nebo vyšetřování zjistí nezbytnost zajištění obsahu některého e-mailového účtu, nařídí provozovateli mailové služby, aby jej uložil v podobě, jakou má v době obdržení příkazu. Uživatel e-mailového účtu pak může jeho obsah klidně vymazat, ale OČTŘ budou mít k dispozici jeho obsah v původním rozsahu před smazáním.

Dalším názorným případem může být situace, kdy OČTŘ zjistí nutnost zajištění údajů o uskutečněném telekomunikačním provozu, ale doba, po kterou mohou být uchovávány, se blíží ke svému konci, a než by byl vydán příkaz ve smyslu § 88a trestního řádu, by již uplynula.

Jedná se o ustanovení, po kterém již OČTŘ dlouhou dobu volaly. Do trestního řádu bylo implementováno na základě článků 16 a 29 „budapešťské úmluvy“[66].

Společně s novelou trestního řádu byl rovněž novelizován zákon č. 104/2013 Sb.[67], který umožňuje OČTŘ žádat o provedení zálohy dat i subjekty působící v zahraničí. Konkrétně se jedná o ustanovení § 65a (Uchovávání dat na žádost České republiky), které je obdobou § 7b trestního řádu. Toto ustanovení bylo rovněž implementováno do českého práva na základě článku 29 „budapešťské úmluvy“. Jedná se o opatření předběžného charakteru, které má stejně jako ustanovení § 7b trestního řádu zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení. V těchto případech útvar Policie ČR, který plní funkci kontaktního pracoviště, po předchozím souhlasu státního zástupce požádá pracoviště druhého státu, aby nařídilo, nebo jinak zajistilo urychlené uchování dat uložených prostřednictvím počítačového systému, který je umístěn na jeho území, a která mají být předmětem následné žádosti dožadující strany o justiční spolupráci za účelem prohlídky, zajištění nebo zpřístupnění uchovaných dat. Data jsou na žádost pouze uchována (zálohována), aniž by došlo k jejich zpřístupnění, a dožadující straně jsou předána až na základě následné žádosti o justiční spolupráci nebo

[66] ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). In Sbírka mezinárodních smluv, Česká republika. 2013, částka 56.

[67] ČESKO. Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních. In *Sbírka zákonů, Česká republika*. 2013, částka 47.

evropského vyšetřovacího příkazu. Přínosem novely je, že se nemusí jednat pouze o stát, který je jednou ze stran mezinárodní „budapešťské úmluvy“.

Kontaktním pracovištěm Policie ČR je podle článku 35 „budapešťské úmluvy“ Odbor kybernetické kriminality Sekce kybernetické kriminality Národní centrály proti organizovanému zločinu Služby kriminální policie a vyšetřování.

Orgán činný v trestním řízení při nutnosti uchování dat z uvedených zákonných důvodů tak zašle žádost adresovanou kontaktnímu pracovišti Policie ČR, která bude obsahovat veškeré náležitosti podle § 65a zákona č. 104/2013 Sb.[68], a to specifikaci orgánu, žádajícího o uchování dat, uvedení trestného činu, pro který se o uchování dat žádá, stručný popis skutku, specifikaci dat, ohledně nichž je požadováno uchování a jejich souvislost se skutkem, pro který se vede trestní řízení, jejich umístění nebo označení osoby, která je má v držení nebo pod kontrolou a uvedení, z jakého důvodu je uchování potřebné pro účely trestního řízení (např. jako důkaz, k identifikaci pachatele apod.). V žádosti je dále nutné uvést údaje o státním zástupci (jméno, adresa sídla, telefonní spojení) a datu, kdy udělil souhlas s provedením uchování dat. Bez tohoto souhlasu nelze žádat.

Zákon č. 104/2013 Sb. rovněž umožňuje provést uchování dat na žádost cizího státu. Toto oprávnění je zakotveno v § 65b citovaného zákona. Podle tohoto ustanovení nesmí být příkaz k uchování dat vydán na dobu kratší než 60 dnů a delší než 90 dnů. Tuto dobu lze prodloužit novým příkazem o dalších 90 dnů.

6.3 Zákonná ustanovení k získávání a vyžadování informací

V této kapitole bude věnována pozornost nejčastěji používaným způsobům získávání a vyžadování dat a informací v rámci prověřování trestné činnosti páchané počítači nebo prostřednictvím internetu. Vzhledem k velkému rozsahu způsobů a možností budou popsány pouze postupy vyžadování údajů o již proběhlé elektronické komunikaci – tedy provozních a lokalizačních údajů – tedy údajů podléhajících telekomunikačnímu tajemství, a zákonné prostředky k jejich vyžadování.

Před samotným popisem jednotlivých způsobů vyžadování informací a dat je důležité zmínit skutečnost, že významnou roli v tomto procesu hraje Útvar zvláštních činností Služba kriminální policie a vyšetřování (dále jen ÚZČ SKPV), a to v návaznosti

[68] ČESKO. Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních. In *Sbírka zákonů, Česká republika*. 2013, částka 47.

na ustanovení § 97 odst. 4 ZoEK. Zde je stanoveno, že forma a způsob předávání údajů jsou prováděny na základě zvláštního právního předpisu. Tímto zvláštním právním předpisem je Vyhláška č. 357/2012 Sb. ze dne 17. října 2012, vydaná na základě ustanovení § 150 odst. 3 ZoEK. Ustanovení § 3 odst. 1 zmiňované vyhlášky ukládá, že o údaje o uskutečněném telekomunikačním provozu oprávněný orgán žádá výhradně prostřednictvím kontaktního pracoviště, kterým je v případě policie ÚZČ SKPV. Postup vyžadování informací o uskutečněném telekomunikačním provozu je stanoven interním aktem řízení, kterým je Závazný pokyn policejního prezidenta číslo 186/2011[69].

6.3.1 Vyžadování údajů o uskutečněném telekomunikačním provozu

Většina zjišťovaných informací a dat při šetření kyberkriminality se týká údajů o uskutečněném telekomunikačním provozu. Jde zejména o zjištění provozu IP adres a internetových sítí, s cílem zjištění, resp. dohledání, konkrétního koncového přípojného bodu, kterým může být účastnické číslo, server, router apod. Jedná se tedy o provozní a lokalizační údaje, jak jsou stanoveny vyhláškou č. 357/2012 Sb. **Získání a zákonné vyžadování těchto informací lze provádět pouze na základě ustanovení § 88a trestního.** Uplatňovat toto ustanovení lze pouze na základě písemného příkazu soudce v rámci trestního řízení vedeného pro úmyslný trestný čin, pro který zákon stanoví trest odnětí svobody s horní hranicí nejméně tři roky nebo taxativně vyjmenované trestné činy, kterými jsou:

- porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku)
- podvod (§ 209 trestního zákoníku)
- neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 trestního zákoníku)
- opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku)
- nebezpečné vyhrožování (§ 353 trestního zákoníku)
- nebezpečné pronásledování (§ 354 trestního zákoníku)
- šíření poplašné zprávy (§ 357 trestního zákoníku)
- podněcování k trestnému činu (§ 364 trestního zákoníku)
- schvalování trestného činu (§ 365 trestního zákoníku),

[69] ČESKO. Závazný pokyn policejního prezidenta č. 186 ze dne 7. 10. 2011, o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu.

- úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána.

Bez příkazu soudce lze údaje o uskutečněném telekomunikačním provozu získat pouze na základě souhlasu uživatele telekomunikačního zařízení, ke kterému se údaje vztahují.

Je potřebné vysvětlit, že v tomto případě se jedná o vyžádání provozních a lokalizačních dat v rozsahu daném vyhláškou č. 357/2012 Sb., tak jak je popsáno v kapitole 6.2.1 (Data retention – ukládání provozních a lokalizačních údajů). Nejedná se tedy v žádném případě o obsah komunikace, lustraci v databázích účastníků ani o poskytnutí registračních údajů či údajů o smlouvách mezi poskytovatelem a účastníkem. Tyto údaje jsou vyžadovány na základě jiných právních ustanovení.

6.3.2 Vyžadování a získávání obsahu uložené e-mailové schránky

Problematika vyžadování a zajišťování obsahu e-mailové schránky (myšleny zejména free mailové účty) nebyla dlouhou dobu nijak právně řešena. Do doby, než Nejvyšší státní zastupitelství vydalo stanovisko č. 1/2015[70], existovaly v rámci státních zastupitelství napříč celou ČR rozdílné přístupy k vyžadování obsahu mailových účtů. Cílem stanoviska bylo proto sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Ve stanovisku byly na základě velmi podrobného rozboru právních norem učiněny závěry a doporučení k zajišťování a vyžadování obsahů e-mailových účtů, nosičů dat a mobilních telefonů.

Podle stanoviska není třeba ke zjišťování obsahu a dat elektronické komunikace uskutečněné ještě před tím, než datový nosič, počítač, počítačový sytém či mobilní telefon získaly do své moci OČTŘ vyžadovat příkaz soudce, pokud byly tyto přístroje zajištěny jako věc důležitá pro trestní řízení postupem odpovídajícím trestnímu řádu (např. podle § 78, § 79, § 82, § 113 trestního řádu a dalších).

Pokud se zjištění bude týkat údajů nebo obsahu elektronické komunikace v době po zajištění přístrojů, nebo zejména nejsou-li vůbec v moci OČTŘ, je nutné postupovat na základě příkazu soudce vydaného podle § 88a trestního řádu. Pokud jde o zjištění

[70] ČESKO. Nejvyšší státní zastupitelství. Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Brno. 2015. In Sbírka výkladových stanovisek Nejvyššího státního zastupitelství. Číslo 1/2015.

obsahu v době jeho přenosu (od volajícího k volanému, od odesílatele k adresátovi) je potřeba postupovat podle § 88 trestního řádu, tedy na základě příkazu vydaného soudcem k odposlechu a záznamu telekomunikačního provozu.

Složitější otázkou bylo najít právní normy umožňující zajištění obsahu e-mailových účtů, protože tento problém neřeší přímo žádné ustanovení trestního řádu. Rozsah obsahu mailového účtu záleží na vůli jeho uživatele – pouze on může mazat doručené a odeslané zprávy, měnit údaje o nastavení filtrů, doplňovat, nebo mazat kontakty. Tato situace se dá přirovnat např. k uložení dopisů a dokumentů v bytě. I zde jeho obyvatel rozhoduje, zda dokument (dopis) zničí, uchová, nebo si ho ani nepřečte. Jedná se tedy o listiny uchovávané v soukromí, na které se vztahuje právo ochrany listovního tajemství zaručeného v č. 13 Listiny základních práv a svobod (dále jen LSP)[71] s výjimkou případů a způsobem, který stanový zákon. Stejně je tomu i u obsahu mailové schránky. Proto v tomto případě nelze uplatňovat ustanovení § 88a nebo § 88 trestního řádu, neboť se nejedná o zjištění obsahu v době jeho přenosu (§ 88) a ani o zjištění provozních a lokalizačních údajů o již uskutečněné a skončené komunikaci (§ 88a). Nejvyšší státní zastupitelství došlo zcela logicky k závěru, že jako jedinou současnou možnou zákonnou licencí prolamující ústavně zaručené právo na ochranu záznamů uložených v soukromí, tedy nacházejících v e-mailové schránce, je postup podle § 158d odst. 3 trestního řádu. Toto ustanovení lze uplatňovat v řízení pro kterýkoli úmyslný trestný čin.

Od doby vydání tohoto stanoviska uplynul nějaký čas a praxe vyžadování obsahu e-mailových schránek se sjednotila. Argumentaci v něm uvedenou dokonce akceptují i soudy, které návrhy na povolení sledování podle § 158d odst. 3 trestního řádu v těchto případech vydávají. Častým problémem byl, a někdy se občas ještě objeví, s uvedením doby, na kterou se povolení vydává. Zpočátku u některých státních zástupců a soudců docházelo k pochopení, že doba, na kterou se povolení vydává, se nevztahuje k době uskutečněného doručení či odeslání zpráv, ale na dobu, ve které je umožněno porušit právo na ochranu listovního tajemství týkající se písemností a záznamů uchovávaných v soukromí („vniknutí“ do schránky a pořízení její kopie).

Z pohledu de lege ferenda by bylo potřeba novelizovat trestní řád o ustanovení, které by jednoznačně a jasně definovalo právo OČTŘ zajišťovat obsahy e-mailových účtů

[71] ČESKO. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny ze základních práv a svobod jako součásti ústavního pořádku České republiky In Sbírka zákonů, Česká republika. 1993, částka 1.

a jim podobným službám, jako jsou např. různá úložiště. Nová norma by mohla mít toto znění:

odst. 1

„Je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin zajistit data, která jsou uložena v počítačovém systému, nosiči informací, e-mailové schránce, účtu sociální sítě nebo účtu v internetovém úložišti, a nelze-li sledovaného účelu dosáhnout jinak, nebo bylo-li by jinak jeho dosažení podstatně ztíženo, lze nařídit osobě, která uvedená data drží, nebo je má pod svojí kontrolou, aby taková data vydala orgánů činným v trestním řízení.“

odst. 2

„Vydání dat podle odst. 1 nařídí v řízení před soudem předseda senátu a v přípravném řízení soudce na návrh státního zástupce nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu. Příkaz musí být vydán písemně a odůvodněn.“

odst. 3

„Příkazu podle odst. 2 není třeba, pokud uživatel počítačového systému, nosiče informací, e-mailové schránky, účtu sociální sítě nebo účtu internetového úložiště, dá souhlas a umožní orgánům činných v trestním řízení po dobu provedení zajištění dat přístup k těmto datům sám, nebo poskytnutím přihlašovacích údajů.“

6.3.3 Získávání, vyžadovaní dat a informací od zahraničních subjektů

Jak již bylo v kapitole 2.5 (Internet) této práce konstatováno, nemá internet jako celek právní subjektivitu a majitele, ale jeho jednotlivé části, jako je vybudovaná infrastruktura jednotlivých sítí, datová centra, servery a další, vlastníky mají. Rovněž služby poskytované v prostředí internetu mají své provozovatele. Právě od těchto vlastníků a provozovatelů je již možné vyžadovat poskytnutí informací důležitých pro trestní řízení na základě zákonné licence dané právními normami. Avšak toto má svá úskalí, neboť vyžadování informací od poskytovatelů služeb, majitelů a provozovatelů infrastruktur v internetu je velmi složité, zejména kvůli samotné podstatě fungování internetu a jeho globálnímu charakteru – internet nezná hranice. Hlavním problémem je určit, na základě jaké právní normy a jakým způsobem tyto informace vyžadovat a hlavně vymáhat, protože majitel infrastruktury, datového centra nebo serveru může služby provozovat mimo území České republiky a to tak, že sám má právní subjektivitu v zahraničí, nebo jsou tam umístěna uvedená zařízení.

Podle českých právních norem lze vymáhat poskytnutí informací pouze po fyzických a právnických osobách s právní subjektivitou na území České republiky. U ostatních pouze na základě mezinárodní právní pomoci mezi justičními orgány dané na základě mezinárodních smluv nebo bilaterálních ujednání. V rámci většiny zemí Evropské unie i na základě evropského vyšetřovacího příkazu.

Kromě vyžadování informací od zahraničních subjektů cestou státního zastupitelství formou mezinárodní právní pomoci mezi justičními orgány a evropského vyšetřovacího příkazu existují ještě další možnosti jejich získání, které se běžně uplatňují v policejní praxi.

Jednou z možností je přímé oslovení tohoto subjektu, např. elektronickou komunikací, a spoléhat na to, že zahraniční subjekt tyto informace poskytne. Procesní hodnota takto získaných informací je však nejistá a většinou slouží pouze jako operativní informace k provedení dalšího šetření a zabránění ztrátě dalších dat a informací. Právě rychlost zajištění dat a informací je při objasňování kyberkriminality jednou z nejdůležitějších a jejich vyžadování cestou mezinárodní právní spolupráce bývá zpravidla zdlouhavější.

Dalším způsobem získání informací a dat jsou dohody uzavřené mezi zahraničními poskytovateli služeb a Policií České republiky. Garantem a partnerem za policii je v případě sociálních sítí Facebook, Instagram, WhatsApp a Skype Odbor kybernetické kriminality Národní centrály proti organizovanému zločinu (dále jen OKK NCOZ). V případě spol. Google Inc. a Microsoftu je to ÚZČ SKPV. Tímto způsobem je žádáno na podkladě zákonného oprávnění policejního orgánu daného trestním řádem tak, jak je tomu u subjektů poskytující připojení a služby internetu v České republice.

V praxi to pak probíhá tak, že státní zástupce na podnět policejního orgánu podá příslušnému soudu návrh na vydání příkazu k poskytnutí údajů o uskutečněném telekomunikačním provozu ve smyslu § 88a trestního řádu. Pokud soudce tento návrh akceptuje a vydá příkaz, nechá jej policejní orgán přeložit do anglického jazyka. Přeložený příkaz pak policejní orgán doručí zahraničnímu subjektu cestou specializovaného pracoviště policie, které je v s ním v kontaktu, viz přechozí kapitoly.

7 Kazuistika

V této kapitole bude popsán postup při prověřování trestního oznámení o údajném neoprávněném přístupu k facebookovému účtu a vyhodnocení informací zjištěných ze souboru se zálohou účtu získaného se souhlasem uživatele.

Úvodem, před samotným popisem a rozborem případu, je třeba objasnit povahu sociální sítě Facebook z pohledu ochrany soukromí a možnosti získání informací a dat k facebookovým profilům z pozice Policie České republiky.

Podle nálezu Ústavního soudu ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13, není povaha sociální sítě Facebook jednoznačně soukromá či veřejná. Vždy záleží na konkrétních uživatelích, jakým způsobem si míru soukromí na svém profilu, případně přímo u jednotlivých příspěvků, nastaví. Prostřednictvím této sítě může uživatel komunikovat pouze s jediným dalším uživatelem, a to, aniž by tuto komunikaci mohli vidět či do ní zasahovat ostatní uživatelé. Taková komunikace by pak jistě mohla být považována za ryze soukromou, byť uskutečněnou prostřednictvím sociální sítě využívané miliardou uživatelů.

Dle citovaného nálezu Ústavního soudu je povinností orgánů činných v trestním řízení při zjišťování těchto informací dodržovat rámec stanovený právními předpisy a respektovat obecné principy, na nichž je založena činnost státních orgánů, zejména v maximální možné míře musí šetřit ústavně zaručená práva a svobody dotčených osob.

V současné praxi existují tři způsoby získání některých informací týkajících se facebookového účtu.

1) Na základě příkazu vydaného podle § 88a trestního řádu

a) <u>cestou mezinárodní právní pomoci</u>

Pro tento postup je třeba ve věci zahájit úkony trestního řízení podle § 158 odst. 3 trestního řádu. Mezinárodní právní pomoc se realizuje cestou dozorujícího státního zástupce prostřednictvím Nejvyššího státního zastupitelství ČR, které kontaktuje příslušný justiční orgán Irské republiky. Postup vyšetřovacím evropským příkazem není možný, protože se Irsko nezavázalo k jeho plnění.

b) <u>mimo mezinárodní právní pomoc</u>

Tímto postupem je možné získat přehled logů (IP adres) přístupů do profilu na základě úředně přeloženého příkazu soudu dle § 88a odst. 1 trestního řádu. Tento způsob získání informací je popsán v předchozí kapitole.

2) Bez soudního příkazu v tzv. „Emergency“ případech

Jedná se o naléhavé případy jako např. terorismus, pohřešování dítěte, bezprostřední ohrožení života apod. Facebook i bez soudního příkazu údaje poskytuje neprodleně (lze mít výsledek např. i do 10 minut od požádání) – poskytnutými údaji jsou pak údaje o přihlášeních do profilu a vybrané základní informace o uživateli účtu. U případů bombových útoků, nebo jiných teroristických hrozeb, je podmínkou zaslat žádost v den, kdy došlo k rozhodné události. V případě zaslání žádosti se zpožděním požaduje Facebook soudní příkaz.

Vyžadování se v tomto případě realizuje cestou Odboru kybernetické kriminality NCOZ.

3) Se souhlasem uživatele účtu

Jedná se o případy, kdy je znám uživatel facebookového účtu a ten je ochoten dát policii souhlas s provedením zálohy účtu. Stažení zálohy účtu umožňuje jedna z funkcí, které jsou k dispozici uživateli po přihlášení do účtu. Jedná se prakticky o data, která jsou provozovatelem aplikace facebook k němu uložena.

Při tomto postupu je nutná součinnost uživatele, který poskytne přihlašovací údaje (login a heslo), nebo účet sám zpřístupní. Při provádění této zálohy se osvědčil písemný souhlas uživatele, pro který byl vytvořen formulář (příloha č. 4). O provedení zálohy se poté zpracuje protokol o provedení úkonu důležitého pro trestní řízení dle § 55 trestního řádu (v případě trestního řízení), nebo úřední záznam o pořízení zálohy facebookového účtu (dále jen FB účtu), který obsahuje stejné údaje jako protokol (příloha č. 5).

Záloha facebookového profilu je provozovatelem sociální sítě poskytnuta ve formě komprimovaného souboru formátu ZIP, který je pojmenován podle profilového jména daného profilu. V současné době lze určit, které složky dat budou staženy (např. jen zprávy, fotografie apod.), v nedávné době byla možnost stažení kompletní zálohy profilu. Obsah staženého archivu tvoří samostatný soubor formátu HTML, „index.html“, po jehož spuštění se zobrazí uživatelský profil se zobrazením základních informací o uživateli a odkazy do dalších složek.

7.1 Údajný neoprávněný přístup k facebookovému účtu

Na SKPV Územního odboru Policie České republiky v Rokycanech se dostavila Karolína K., která oznámila podezření na to, že se jí někdo neoprávněně přihlásil do jejího profilu v sociální síti Facebook. Toto podezření pojala na základě e-mailové zprávy, která jí byla od Facebooku zaslána. Jednalo se o zprávu s upozorněním, že došlo k přihlášení

do jejího profilu z prohlížeče nebo zařízení, ze kterého k přihlašování obvykle nedochází, a aby si zkontrolovala, zda se jedná o přihlášení její.

S oznamovatelkou byl sepsán protokol o trestním oznámení. Policista přijímající oznámení po provedeném výslechu rozhodl, že věc bude zatím šetřena ve smyslu § 158 odst. 1 trestního řádu, tedy že nebudou zatím zahájeny úkony trestního řízení dle § 158 odst. 3 trestního řádu.

7.1.1 Průběh šetření

Zpracovatel případu se obrátil na Oddělení analytiky a kybernetické kriminality Územního odboru policie Rokycany. Pracovník tohoto oddělení kontaktoval oznamovatelku, aby poskytla policejnímu orgánu zprávu s upozorněním od Facebooku ve své e-mailové schránce (viz příloha č. 6). Z této zprávy po zpřístupnění policejní orgán zjistil, že uživatel profilu byl přihlášen dne 26. 3. 2017 v 22:18 hod. z IP adresy 62.XXX.XXX.118. Následně byla Karolína K. dotázána, přes jakého poskytovatele přistupuje do sítě internet (dále jen ISP). Uvedla, že se jedná o společnost Mxxxt s.r.o. Provedenou lustrací v databázi Whois použité IP adresy bylo zjištěno, že tato je přidělena v rozsahu užívání společnosti Mxxxt s.r.o. Dále byla Karolína dotázána, jak přistupuje ke svému profilu v sociální síti Facebook. Uvedla, že pomocí svého mobilního telefonu zn. HONOR 7 Lite, který začala používat teprve v průběhu měsíce února 2017. V tomto telefonu je k sociální síti připojena téměř neustále.

Oznamovatelka Karolína K. dala policejnímu orgánu souhlas s pořízením zálohy jejího facebookového profilu a poskytla přístupové heslo k tomuto účtu, aby mohla být tato záloha provedena.

Záloha byla stažena v souboru facebook-kajcaxxxxxx.zip, který obsahoval soubor *security.htm* (v současné době jsou data obsažená v tomto souboru v adresáři: *security_and_login_information*, ve kterém jsou data rozdělena do několika HTML souborů). V tomto souboru byla uložena data o některých aktivitách na facebookovém profilu. Vyhodnocením těchto údajů bylo zjištěno, že dne 26. 3. 2017 ve 22:20 hod. došlo k odhlášení z tohoto profilu z IP adresy: 62.XXX.XXX.118 a následně z této IP adresy došlo ve 22:22 hod. ke změně přístupového hesla a následnému odhlášení.

Z dat o aktivitách na FB profilu bylo zjištěno, že tyto byly prováděny za použití prohlížeče instalovaném v přístroji HONOR Lite 7 (v datech uváděno HONOR NEM – L21). Logy o použitém prohlížeči a telefonním přístroji jsou uvedeny v příloze č. 6.

7.1.2 Vyhodnocení výsledků šetření a rozhodnutí

Ze zjištěných informací byl dán závěr, že dne 26. 3. 2017 nedošlo k neoprávněnému přístupu k FB profilu Karolíny K., ale byla to právě ona sama, kdo provedl přihlášení i odhlášení k tomuto FB profilu. Zjištění je dáno zejména:

- přístupovou IP adresou 62.XXX.XXX.118, která je používána ISP: Mxxxt s.r.o., tedy poskytovatelem, jehož služby využívá oznamovatelka,
- telefonním přístrojem HONOR Lite 7, který byl k přístupu použit, tedy stejné značky typu, který používá oznamovatelka,
- skutečností, že se v mobilním telefonu z aplikace připojení k sociální síti Facebook neodhlašuje a v uvedenou dobu i před ní bylo přihlášení pouze z telefonního přístroje HONOR Lite 7.

Na základě zjištěných skutečností zpracovatel spisu konstatoval, že nedošlo k žádnému protiprávnímu jednání, a proto oznámení založil ad acta.

Závěr

V bakalářské práci byl vymezen a objasněn pojem kybernetická kriminalita na základě výsledku analýzy a komparace různých definic uvedených v odborné literatuře, historického vývoje informačních a komunikačních technologií, a vlivu nově vzniklého fenoménu virtuálního prostoru nazývaného kyberprostor. Rovněž byl pojem kyberkriminality zasazen do kontextu ostatních druhů kriminality označované jako kriminalita klasická. Vedle tohoto klíčového pojmu byly vysvětleny další základní pojmy s ním související. Vzhledem k zadanému rozsahu práce však nemohly být vymezeny a vysvětleny všechny pojmy, protože by to bylo téma na samostatnou práci.

Rovněž bylo provedeno rozdělení kyberkriminality na jednotlivé druhy (formy). Její projevy byly rozděleny do tří základních skupin tak, jak je autor chápe na základě jejich působení a širšího pojetí rozdělení podle „budapešťské úmluvy“. U každé z forem byly uvedeny konkrétní příklady, které ji nejlépe vystihují, a rovněž byla popsána trestněprávní odpovědnost v prostředí českého práva.

V šesté kapitole a jejích podkapitolách byla popsána role a podíl útvarů Policie České republiky, které se podílejí na objasňování a vyšetřování této trestné činnosti s bližším zaměřením na Krajské ředitelství policie Plzeňského kraje. Rovněž byly nastíněny problémy se získáváním a zajišťováním dat a informací, kdy byly uvedeny nejčastěji používané zákonné postupy, tak aby byla v maximální možné míře šetřena ústavně zaručená práva a svobody dotčených osob.

Kromě popisu stávajícího právního rámce týkajícího se vyžadování a zajišťování dat a informací v průběhu prověřování a vyšetřování případů kyberkriminality, byly vysloveny konkrétní návrhy z pohledu dle lege ferenda na jejich změnu či doplnění, a to na základě vyhodnocení teoretického a praxeologického hlediska autora práce.

V závěrečné kapitole je prezentován případ údajného neoprávněného přístupu do facebookového účtu, na kterém je uveden stručný popis praktického získávání a vyžadovaní informací k profilům sociální sítě Facebook jak po stránce technické, tak po stránce právní.

Jak z celé práce vyplývá, stává se z kyberkriminality výrazně významný fenomén, který se bude i nadále stále vyvíjet. Analýzou statistických dat bylo zjištěno, že počet evidovaných případů spáchaných prostřednictvím internetu nebo jinými počítačovými sítěmi, narůstá každý rok geometrickou řadou. Nejvíce je stále evidováno protiprávní jednání páchané formou webových aukčních (inzertních) podvodů. K páchání této

činnosti ani není zapotřebí větších znalostí fungování výpočetní techniky a internetu, postačí pouze základní uživatelské schopnosti. Případy podvodných jednání různých druhů páchaných za využití internetu patří mezi nejčastěji prověřované. Co velmi napomáhá k rozšíření této trestné činnosti? Je to velká anonymita, malé riziko odhalení a zejména možnost oslovení naráz většího množství osob a tím i možnost získání většího finančního prospěchu, aniž by pachatel musel opustit svůj domov.

Objasňování a vyšetřování všech forem kyberkriminality je velmi náročné a obtížné, zejména získávání dat a informací, které po jejich zajištění a vyhodnocení mohou sloužit jako důkazy. Policie České republiky sice reagovala na nárůst kriminality spojené s počítači a počítačovými sítěmi tím, že zřídila specializované útvary na všech úrovních, které ale leckde nejsou dostatečně personálně obsazené. Rovněž chybí specializační vzdělávání všech policistů, zejména těch, kteří přijímají oznámení o této trestné činnosti, a měli by tedy jako první provádět prvotní opatření k jejímu zdárnému vyšetření.

Autor si uvědomuje, že popis a rozbor pojmů, forem, trestněprávní odpovědnosti kyberkriminality a postupů při jejím vyšetřování je velmi stručný, ale podrobnější popis a vyhodnocení všech souvisejících projevů by značně překročil zadaný rozsah práce. Proto byly vystiženy nejzákladnější pojmy a problémy spojené s tímto protiprávním jednáním. Cíle práce zvolené na jejím začátku byly splněny.

Seznam použitých zdrojů

Knihy a monografie:

1. HENDRYCH, D. a kol. Právnický slovník. 3. vydání. Praha: Nakladatelství C. H. Beck, 2009. 1481 s. ISBN 978-80-7400-059-1.
2. JIROVSKÝ, V. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007.284 s. ISBN 978-80-247-1561-2.
3. KOLOUCH, J. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. 524 s. ISBN 978-80-88168-15-7.
4. MAISNER, M.: Zákon o některých službách informační společnosti. Komentář. 1. vydání. Praha: C. H. Beck, 2016, 223 s. ISBN 978-80-7400-449-0.
5. MATĚJKA, M. Počítačová kriminalita. Praha: Computer Press, 2002. 106 s. ISBN 80-722-6419-2.
6. POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). 309 s. ISBN 80-868-9838-5.
7. SMEJKAL, V. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. 640 s. ISBN 978-80-7380-501-2.
8. SMEJKAL, V., SOKOL T. a VLČEK M. Počítačové právo. Praha: C.H. Beck, 1995. Právo a hospodářství (C.H. Beck). 264 s. ISBN 80-717-9009-5.
9. ŠÁMAL, P. a kol. Trestní zákoník, 2. vydání, Praha: C.H.Beck, 2012, 3614 s. ISBN 978-80-7400-428-5.
10. ŠÁMAL, P. a kol. Trestní řád. Komentář. 7. vydání, Praha: C.H.Beck, 2013, 4700 s. ISBN 978-80-7400-465-0.
11. VLACHOVÁ, B. Zákon o elektronických komunikacích. Komentář. 1. vydání. Praha: C. H. Beck, 2017, 530 s. ISBN 978-80-7400-632-6.
12. ZAVRŠNIK, A. Kyberkriminalita. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR), 148 s. ISBN 978-80-7552-758-5.

Periodika:

1. AUSPICIA: Recenzovaný vědecký časopis pro otázky společenských věd [online]. VŠERS, 2013(1) [cit. 2018-11-07]. ISSN 1214-4967. Dostupné z: https://vsers.cz/wp-content/uploads/2017/02/Auspicia-2013-1.pdf
2. REVUE PRO MÉDIA: Časopis pro kritickou reflexi médií. Brno: Spolek přátel pro vydávání časopisu HOST, **2003**(5). ISSN 1214-7494. Dostupné z: http://rpm.fss.muni.cz/Revue/Revue05/archiv_05.htm
3. Trestněprávní revue. Praha: C. H. Beck, 2003(6). ISSN 1213-5313.

Elektronické zdroje:

1. BARLOW, John Perry. A Declaration of the Independence of Cyberspace. In Electronic Frontier Foundation [online]. Davos, 1996 [cit. 2018-10-21]. Dostupné z: https://www.eff.org/cyberspace-independence
2. Co je phishing?: Vyhněte se e-mailovým podvodům a útokům [online]. AVAST Software [cit. 2019-03-05]. Dostupné z: https://www.avast.com/cs-cz/c-phishing
3. COUFALOVÁ, D. Anonymní platební karty: To, že jsem paranoidní, ještě neznamená, že po mě nejdou. Ušetřeno.cz [online]. 2017 [cit. 2019-03-05]. Dostupné z: https://www.usetreno.cz/anonymni-platebni-karty/#gref
4. JIRÁSEK, P., NOVÁK L., POŽÁR J. Výkladový slovník kybernetické bezpečnosti: první oficiální verze slovníku kybernetické bezpečnosti [online]. Vyd. 1. elektronické. Praha: Policejní akademie České republiky, 2012 [cit. 2017-12-10]. ISBN 978-80-7251-377-2. Dostupné z:

   https://www.govcert.cz/download/aktuality/container-nodeid-548/slovnikv231nbuwebcolor.pdf
5. JONÁK, Z. Informační společnost. In KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV) [online]. Praha: Národní knihovna ČR, 2003- [cit. 2017-12-03]. Dostupné z:

   http://aleph.nkp.cz/F/?func=direct&doc_number=000000468&local_base=KTD
6. POŽÁR, J. Některé aspekty kybernetické kriminality [online]. Praha: Policejní akademie ČR, Fakulta bezpečnostního managementu, 2011 [cit. 2017-12-10]. Dostupné z: https://www.cybersecurity.cz/data/Pozar.pdf

7. Prevence kriminality v České republice: Stalking a kyberstalking [online]. Praha: MV ČR, 2019 [cit. 2019-03-05]. Dostupné z: http://www.prevencekriminality.cz/kyberkriminalita-testovaci-provoz/clanky-informace/stalking-a-kyberstalking/

8. Příchod hackerů: nigerijský scam „419“. Root.cz - informace nejen ze světa Linuxu [online]. Internet Info, 2014 [cit. 2019-03-05]. ISSN 1212-8309. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-nigerijsky-scam-419/

9. Smejkal, V., Informační a počítačová kriminalita v České republice, MV ČR, 1999. [online].[cit. 2017-12-09]. Dostupné z: https://web.archive.org/web/20001202015000/http://www.mvcr.cz/casopisy/studie/diskuse/analyza2.html

10. Support.zcu.cz. STRÁNKY UŽIVATELSKÉ PODPORY [online]. Plzeň: ZČU Plzeň [cit. 2019-03-05]. Dostupné z: https://support.zcu.cz/index.php

11. [WIFT]. Co to je DDoS útok a jak se dělá? Diit.cz: Novinky a informace o hardware, software a internetu [online]. 24. 1. 2012, 2012 [cit. 2018-01-08]. ISSN 1213-2225. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

12. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-2018 [cit. 2018-11-04]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberprostor

Legislativní dokumenty:

1. ČESKO. Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny ze základních práv a svobod jako součásti ústavního pořádku České republiky In *Sbírka zákonů, Česká republika*. 1993, částka 1.

2. ČESKO. Zákon č. 89/2012 Sb., občanský zákoník. In *Sbírka zákonů, Česká republika*. 2012, částka 33.

3. ČESKO. Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). In *Sbírka zákonů, Česká republika*. 2000, částka 36.

4. ČESKO. Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních. In *Sbírka zákonů, Česká republika*. 2013, částka 47.

5. ČESKO. Sdělení č. 104/2013 Sb.m.s., Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě (Úmluva o počítačové kriminalitě). In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 56.

6. ČESKO. Sdělení č. 9/2015 Sb.m.s., Ministerstva zahraničních věcí o sjednání Dodatkového protokolu k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů. In *Sbírka mezinárodních smluv, Česká republika*. 2013, částka 3.

7. ČESKO. Nález Ústavního soudu ze dne 30. 10. 2014, sp. zn. III. ÚS 3844/13. In *Sbírka nálezů a usnesení Ústavního soudu, Česká republika*. 2014, Číslo N 201/75 SbNU 259.

8. EVROPSKÁ UNIE. SOUDNÍ DVŮR EVROPSKÉ UNIE. Rozsudek ze dne 8. dubna 2014 ve spojených věcech C 293/12 a C 594/12. Bod č. 49. In: Curia.europa.eu. Číslo ECLI:EU:C:2014:238 Lucembursko. 2014.

9. EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32006L0024&from=PL

10. ČESKO. Rozkaz policejního prezidenta č. 45 ze dne 6. března 2017, kterým se stanoví vzorová systemizace služebních a pracovních míst krajského ředitelství Policie České republiky a městského ředitelství Policie České republiky. In *Sbírka interních aktů řízení Policejního prezidia České republiky*. 2017, částka 48.

11. ČESKO. Závazný pokyn policejního prezidenta č. 186 ze dne 7. října. 2011, o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu. In *Sbírka interních aktů řízení Policejního prezidia České republiky*. 2011, částka 202.

12. ČESKO. Nejvyšší státní zastupitelství. Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek. Brno. 2015. In *Sbírka výkladových stanovisek Nejvyššího státního zastupitelství*. Číslo 1/2015.

Seznam zkratek

CESNET - angl. ***C**zech **E**ducational and **S**cientific **NET**work* – sdružení založené veřejnými vysokými školami a Akademií věd v roce 1996, které provozovalo první internetovou páteřní síť v České republice. Síť měla propojovat zejména univerzitní a akademická pracoviště. V současné době sdružení provozuje a rozvíjí národní e-infrastrukturu pro vědu, výzkum a vzdělávání.

CD - angl. ***C**ompact **D**isc* – kompaktní disk, jedná se o paměťové médium, optický disk určený pro ukládání digitálních dat

DVD - angl. **D**igital **V**ersatile **D**isc nebo **D**igital **V**ideo **D**isc – digitální optický datový nosič pro ukládání filmů ve vysoké obrazové a zvukové kvalitě nebo jiných dat

ESSK - **E**videnčně **s**tatistický **s**ystém **k**riminality

ICT - Informační a komunikační technologie

ISP - Internet Service Provider (poskytovatel připojení nebo poskytovatel informační služby)

LAN - angl. ***L**ocal **A**rea **N**etwork* (lokální síť)

LSP - Listina základních práv a svobod

MAN - angl. ***M**etropolitan **A**rea **N**etwork* (městská síť)

MŘ - Městské ředitelství

NCOZ - **N**árodní **c**entrála boje s **o**rganizovaným **z**ločinem

OAKK - **O**dbor (oddělení) **a**nalytiky a **k**ybernetické **k**riminality

OČTŘ - Orgán činný v trestním řízení

OKK - **O**dbor (oddělení) **k**ybernetické **k**riminality

P2P - angl. ***P**eer-to-**p**eer* (rovný s rovným); označení počítačových sítí, ve kterých komunikují jednotliví klienti přímo spolu (klient ⇆ klient)

PIN - angl. ***P**ersonal **I**dentification **Numbe**r* – osobní identifikační číslo, jde o identifikátor, kterým jsou autorizovány např. vstupní kódy, platební karty nebo mobilní telefony.

PČR - Policie České republiky

SIM - angl. ***S**ubscriber **I**dentity **M**odule*; Karta aktivující funkce mobilního telefonu a nesoucí účastnické telefonní číslo; každá SIM karta má přiděleno jedinečné sériové číslo označované jako ICCID

TCP/IP - angl. ***T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol*. Jde o sadu protokolů pro komunikaci v počítačové síti.

ÚZČ SKPV - Útvar zvláštních činností Služby kriminální policie a vyšetřování

VPN - angl. ***V**irtual **P**rivate **N**etwork* (virtuální privátní síť); prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě.

WAN - angl. ***W**ide **A**rea **N**etwork* (rozlehlá síť)

WWW - angl. ***W**orld **W**ide **W**eb* (v doslovném překladu „světově rozsáhlá pavučina“); česky zkráceně web; označení pro systém umožňující prohlížení, ukládání a odkazování na dokumenty v internetu

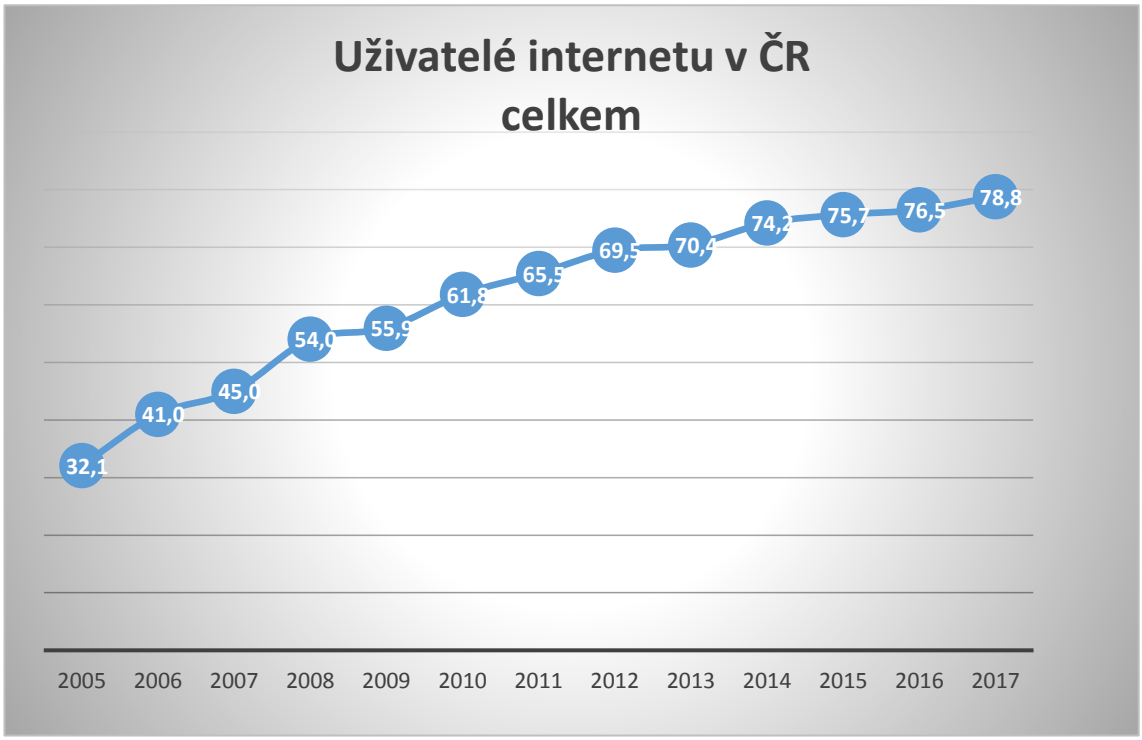
ZoEK - **Z**ákon **o** **e**lektronických **k**omunikacích (zákon č. 127/2005 Sb.)

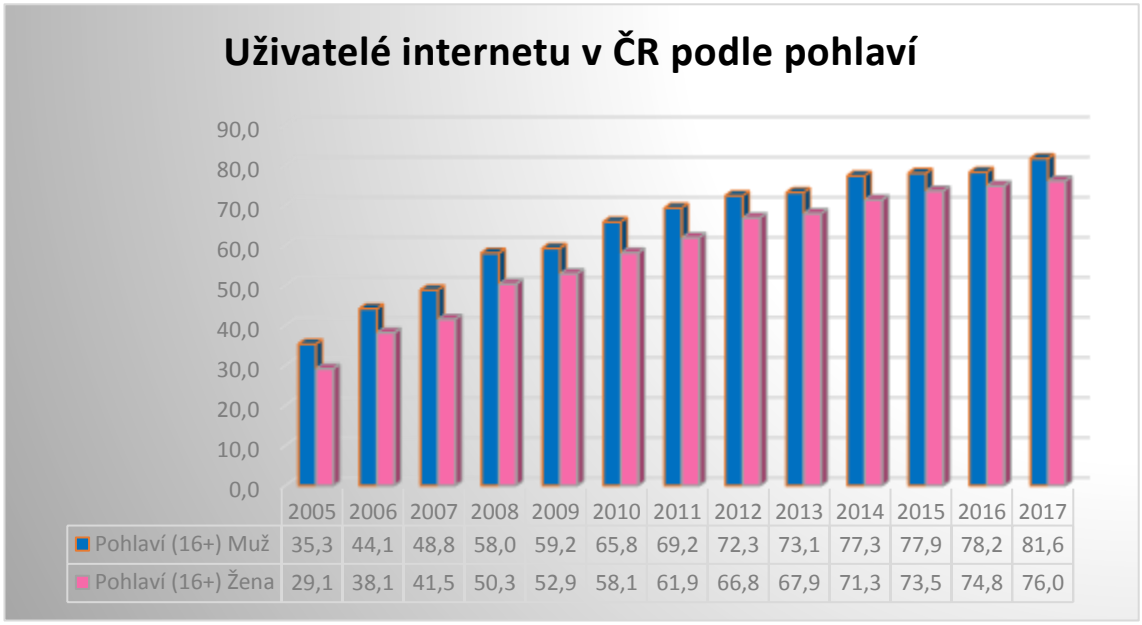
Seznam obrázků, grafů a tabulek

Seznam příloh

Příloha č. 1

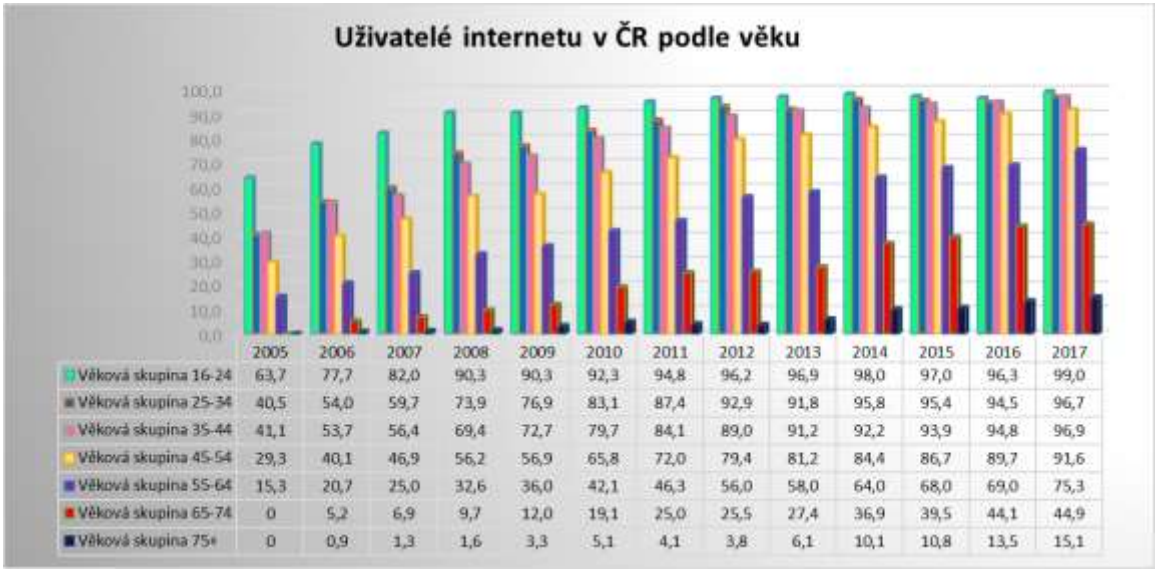
Grafy počtů uživatelů internetu v České republice[72]



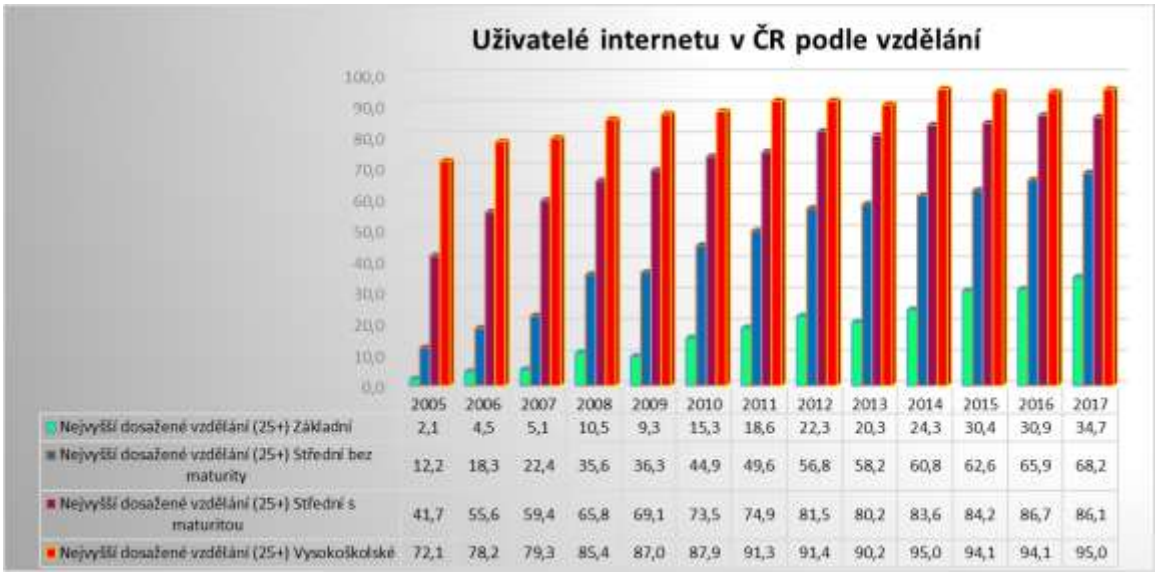


	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Pohlaví (16+) Muž	35,3	44,1	48,8	58,0	59,2	65,8	69,2	72,3	73,1	77,3	77,9	78,2	81,6
Pohlaví (16+) Žena	29,1	38,1	41,5	50,3	52,9	58,1	61,9	66,8	67,9	71,3	73,5	74,8	76,0

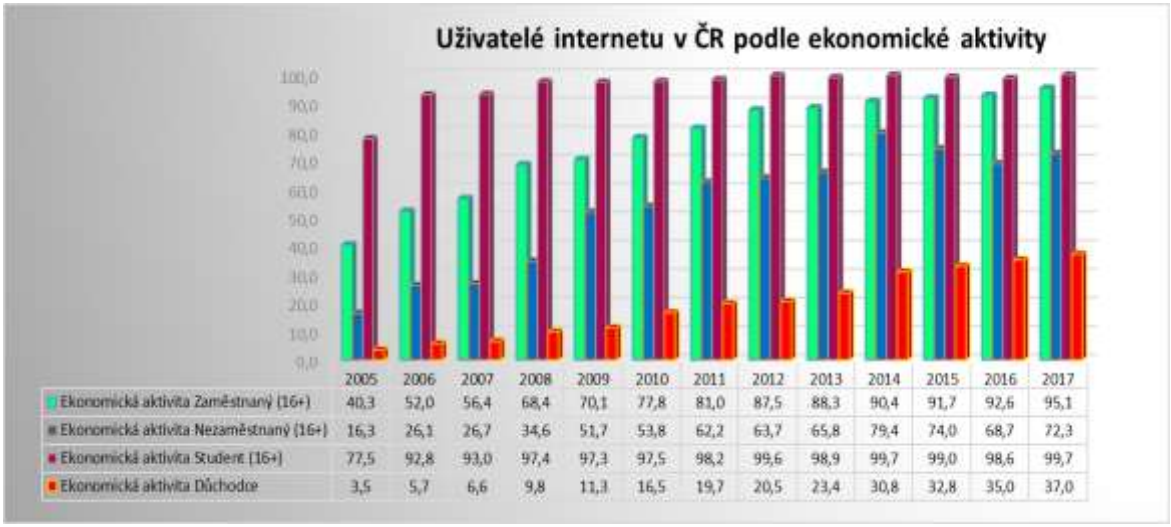
[72] Zdroj: Český statistický úřad, Veřejná databáze. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt&z=T&f=TABULKA&katalog=31031&pvo=ICT04&&str=v149&kodjaz=203



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Věková skupina 16-24	63,7	77,7	82,0	90,3	90,3	92,3	94,8	96,2	96,9	98,0	97,0	96,3	99,0
Věková skupina 25-34	40,5	54,0	59,7	73,9	76,9	83,1	87,4	92,9	91,8	95,8	95,4	94,5	96,7
Věková skupina 35-44	41,1	53,7	56,4	69,4	72,7	79,7	84,1	89,0	91,2	92,2	93,9	94,8	96,9
Věková skupina 45-54	29,3	40,1	46,9	56,2	56,9	65,8	72,0	79,4	81,2	84,4	86,7	89,7	91,6
Věková skupina 55-64	15,3	20,7	25,0	32,6	36,0	42,1	46,3	56,0	58,0	64,0	68,0	69,0	75,3
Věková skupina 65-74	0	5,2	6,9	9,7	12,0	19,1	25,0	25,5	27,4	36,9	39,5	44,1	44,9
Věková skupina 75+	0	0,9	1,3	1,6	3,3	5,1	4,1	3,8	6,1	10,1	10,8	13,5	15,1



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Nejvyšší dosažené vzdělání (25+) Základní	2,1	4,5	5,1	10,5	9,3	15,3	18,6	22,3	20,3	24,3	30,4	30,9	34,7
Nejvyšší dosažené vzdělání (25+) Střední bez maturity	12,2	18,3	22,4	35,6	36,3	44,9	49,6	56,8	58,2	60,8	62,6	65,9	68,2
Nejvyšší dosažené vzdělání (25+) Střední s maturitou	41,7	55,6	59,4	65,8	69,1	73,5	74,9	81,5	80,2	83,6	84,2	86,7	86,1
Nejvyšší dosažené vzdělání (25+) Vysokoškolské	72,1	78,2	79,3	85,4	87,0	87,9	91,3	91,4	90,2	95,0	94,1	94,1	95,0

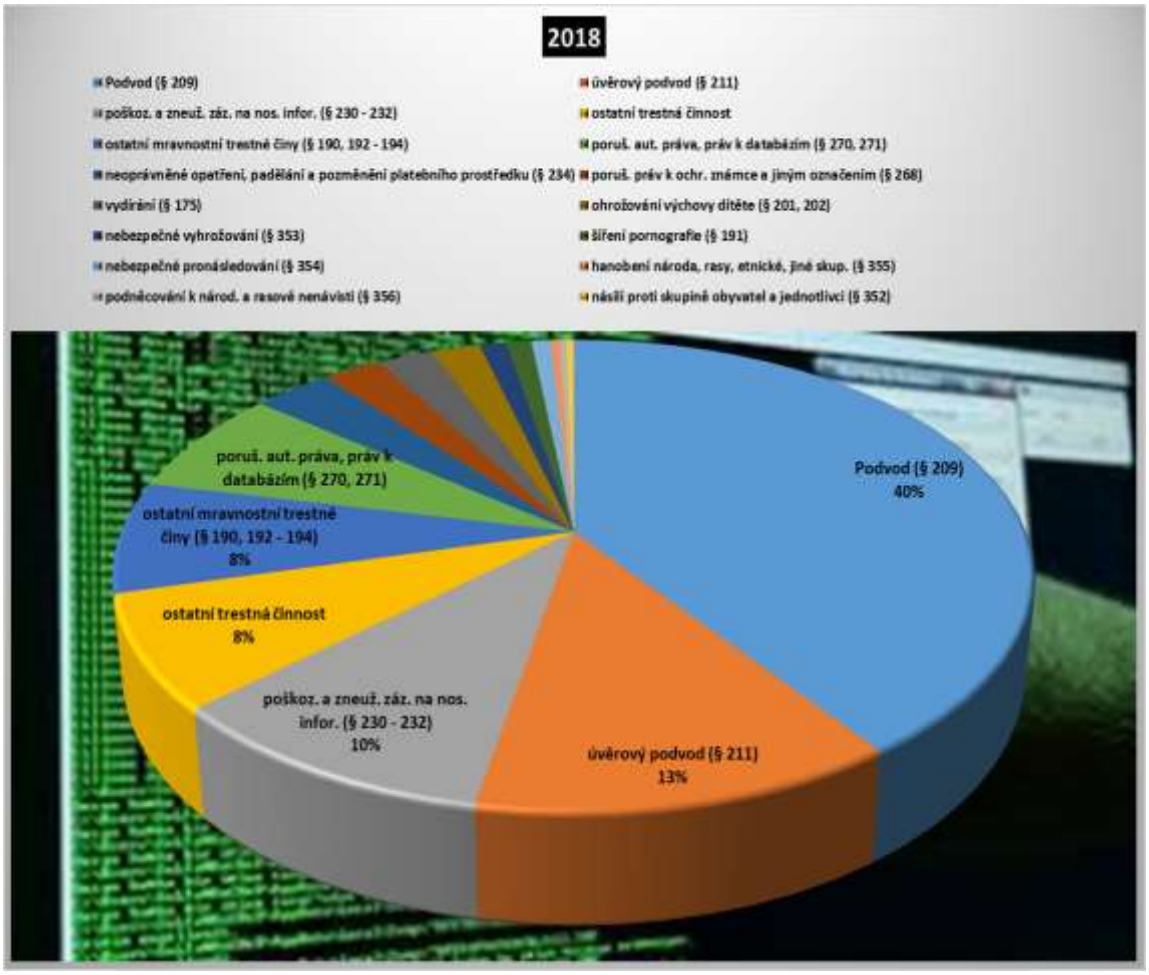


	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Ekonomická aktivita Zaměstnaný (16+)	40,3	52,0	56,4	68,4	70,1	77,8	81,0	87,5	88,3	90,4	91,7	92,6	95,1
Ekonomická aktivita Nezaměstnaný (16+)	16,3	26,1	26,7	34,6	51,7	53,8	62,2	63,7	65,8	79,4	74,0	68,7	72,3
Ekonomická aktivita Student (16+)	77,5	92,8	93,0	97,4	97,3	97,5	98,2	99,6	98,9	99,7	99,0	98,6	99,7
Ekonomická aktivita Důchodce	3,5	5,7	6,6	9,8	11,3	16,5	19,7	20,5	23,4	30,8	32,8	35,0	37,0

Příloha č. 2

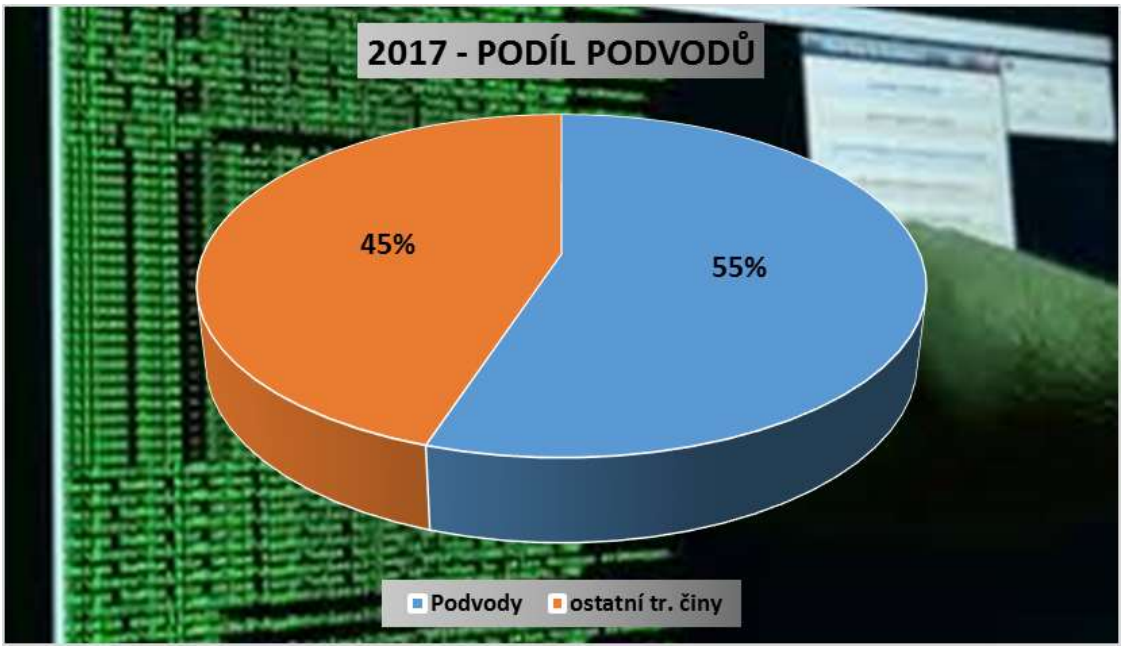
Tabulka a graf s přehledem počtu jednotlivých druhů trestných činů spáchaných prostřednictvím internetu nebo jinými počítačovými sítěmi (Česká republika rok 2018)[73].

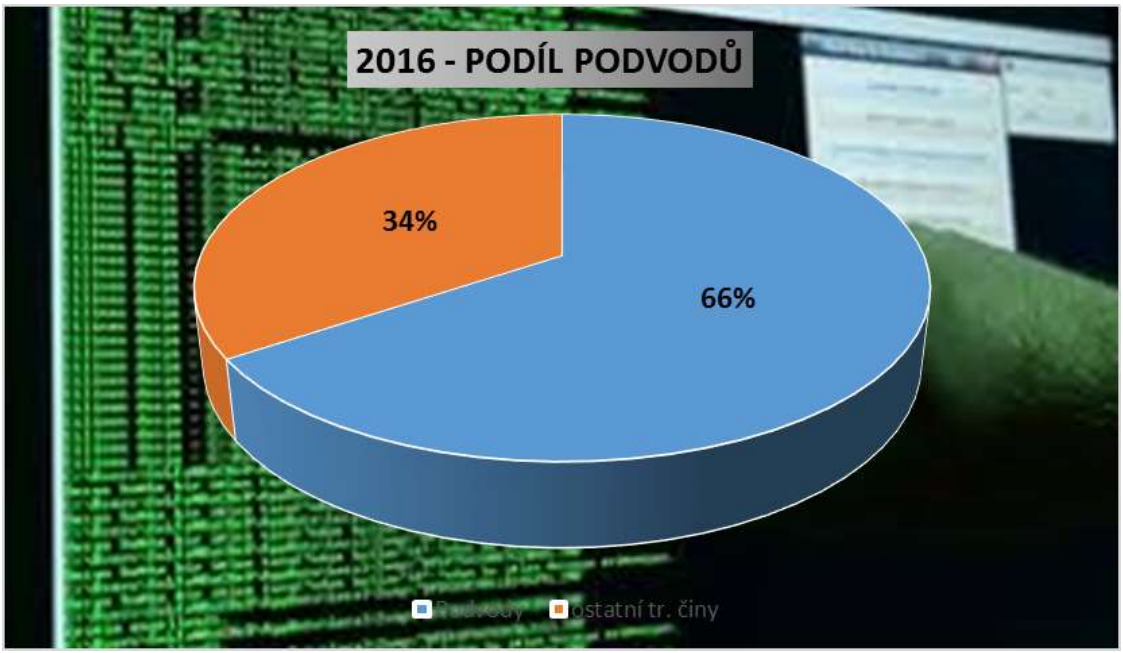
Druh TČ	Počet
Podvod (§ 209)	2743
úvěrový podvod (§ 211)	860
poškoz. a zneuž. záz. na nos. infor. (§ 230 - 232)	696
ostatní trestná činnost	529
ostatní mravnostní trestné činy (§ 190, 192 - 194)	523
poruš. aut. práva, práv k databázím (§ 270, 271)	500
neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234)	225
poruš. práv k ochr. známce a jiným označením (§ 268)	170
vydírání (§ 175)	159
ohrožování výchovy dítěte (§ 201, 202)	140
nebezpečné vyhrožování (§ 353)	77
šíření pornografie (§ 191)	72
nebezpečné pronásledování (§ 354)	54
hanobení národa, rasy, etnické, jiné skup. (§ 355)	26
podněcování k národ. a rasové nenávisti (§ 356)	21
násilí proti skupině obyvatel a jednotlivci (§ 352)	20



[73] Zdroj: Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, Odbor informatiky a provozu informačních technologií, měsíční statistiky ESSK

Grafy znázorňující podíl podvodů (§ 209 + § 211 – úvěrový podvod) spáchaných prostřednictvím internetu nebo jinými počítačovými sítěmi (Česká republika rok 2017 a 2016)[74]





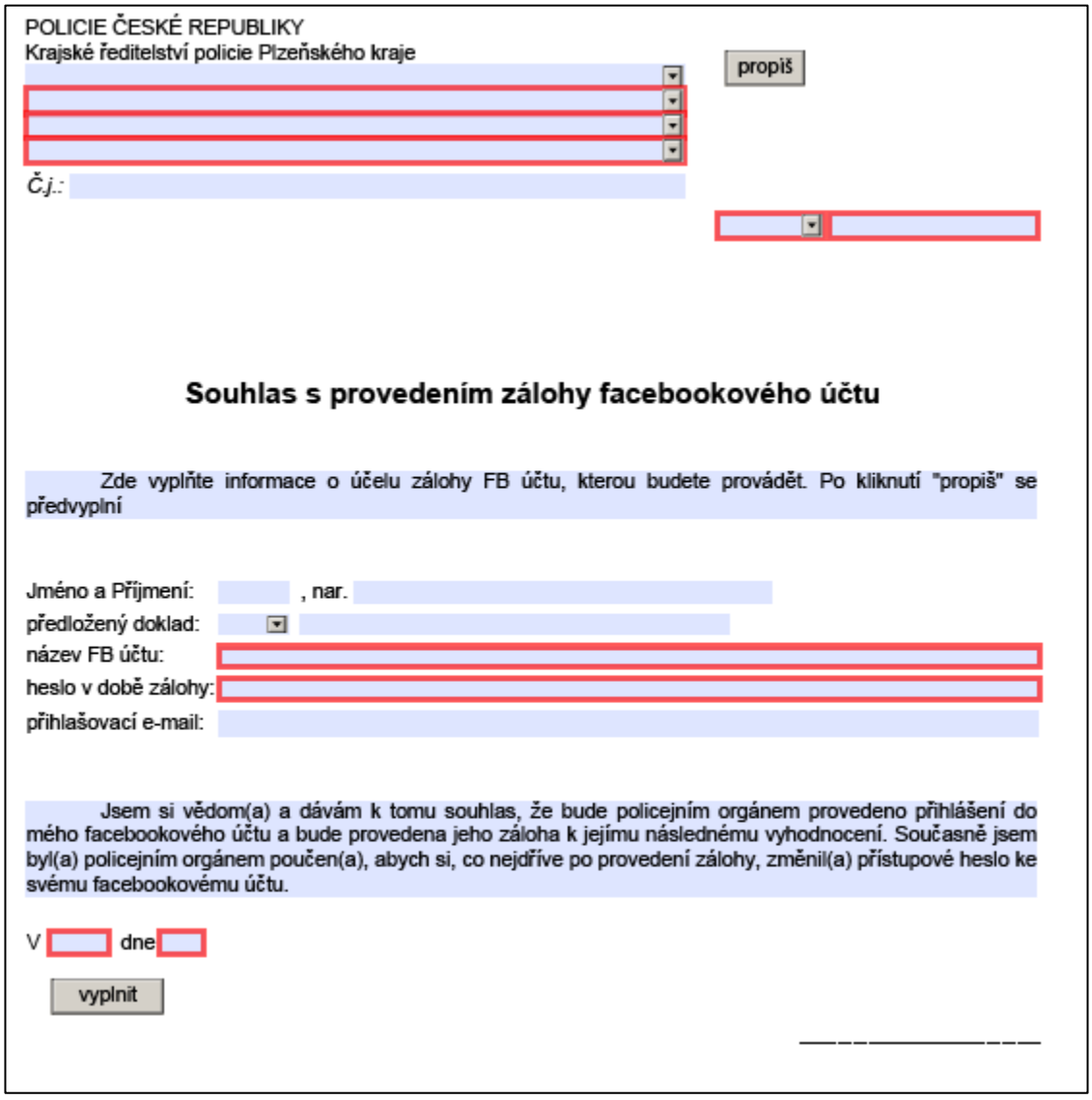
[74] Zdroj: Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, Odbor informatiky a provozu informačních technologií, měsíční statistiky ESSK

Příloha č. 3

Grafy vývoje evidovaných trestných činů spáchaných v síti Internet v r. 2011 – 2018[75]

[75] Zdroj: Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, Odbor informatiky a provozu informačních technologií, měsíční statistiky ESSK

Příloha č. 4[76]



POLICIE ČESKÉ REPUBLIKY
Krajské ředitelství policie Plzeňského kraje

propiš

Čj.:

Souhlas s provedením zálohy facebookového účtu

Zde vyplňte informace o účelu zálohy FB účtu, kterou budete provádět. Po kliknutí "propiš" se předvyplní

Jméno a Příjmení: , nar.
předložený doklad:
název FB účtu:
heslo v době zálohy:
přihlašovací e-mail:

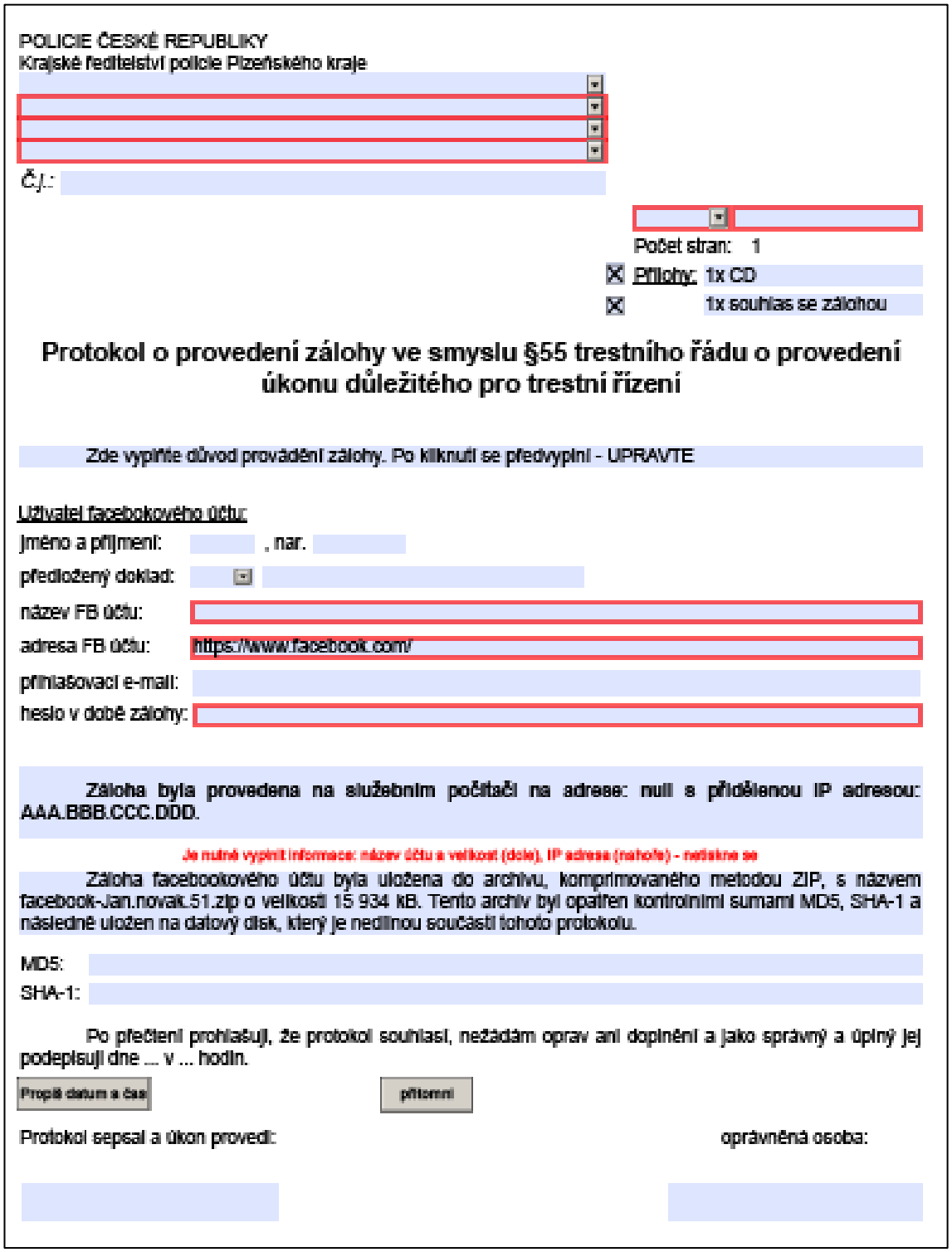
Jsem si vědom(a) a dávám k tomu souhlas, že bude policejním orgánem provedeno přihlášení do mého facebookového účtu a bude provedena jeho záloha k jejímu následnému vyhodnocení. Současně jsem byl(a) policejním orgánem poučen(a), abych si, co nejdříve po provedení zálohy, změnil(a) přístupové heslo ke svému facebookovému účtu.

V dne

vyplnit

[76] Vlastní zdroj

Příloha č. 5[77]



POLICIE ČESKÉ REPUBLIKY
Krajské ředitelství policie Plzeňského kraje

Č.j.:

Počet stran: 1

Přílohy: 1x CD

1x souhlas se zálohou

Protokol o provedení zálohy ve smyslu §55 trestního řádu o provedení úkonu důležitého pro trestní řízení

Zde vyplňte důvod provádění zálohy. Po kliknutí se předvyplní - UPRAVTE

Uživatel facebookového účtu:

jméno a příjmení: , nar.

předložený doklad:

název FB účtu:

adresa FB účtu: https://www.facebook.com/

přihlašovací e-mail:

heslo v době zálohy:

Záloha byla provedena na služebním počítači na adrese: null s přidělenou IP adresou: AAA.BBB.CCC.DDD.

Je nutné vyplnit informace: název účtu a velikost (dole), IP adresa (nahoře) - netiskne se

Záloha facebookového účtu byla uložena do archivu, komprimovaného metodou ZIP, s názvem facebook-Jan.novak.51.zip o velikosti 15 934 kB. Tento archiv byl opatřen kontrolními sumami MD5, SHA-1 a následně uložen na datový disk, který je nedílnou součástí tohoto protokolu.

MD5:

SHA-1:

Po přečtení prohlašuji, že protokol souhlasí, nežádám oprav ani doplnění a jako správný a úplný jej podepisuji dne ... v ... hodin.

Propiš datum a čas

přítomni

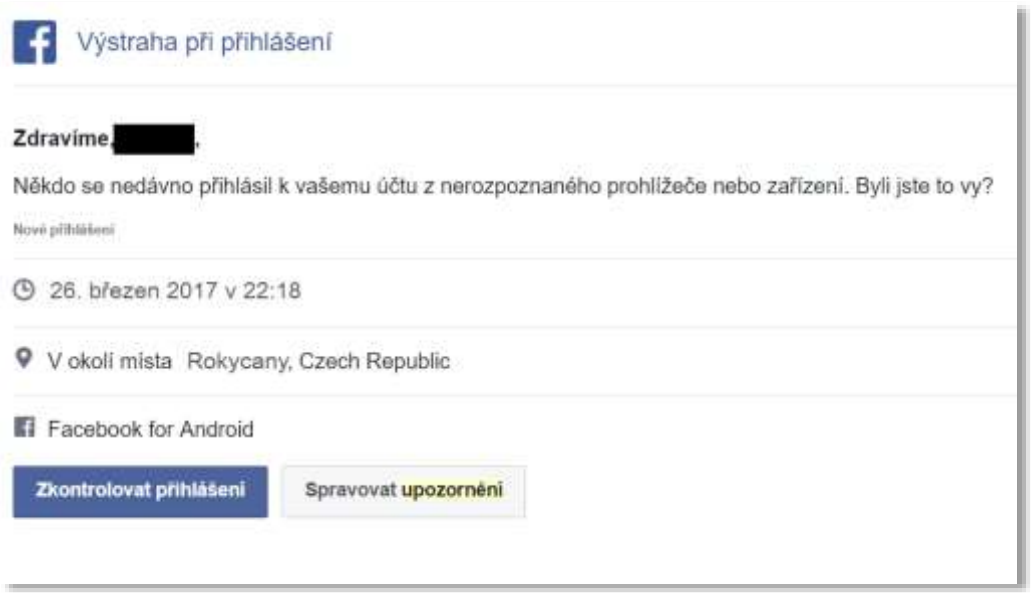
Protokol sepsal a úkon provedl:

oprávněná osoba:

[77] Vlastní zdroj

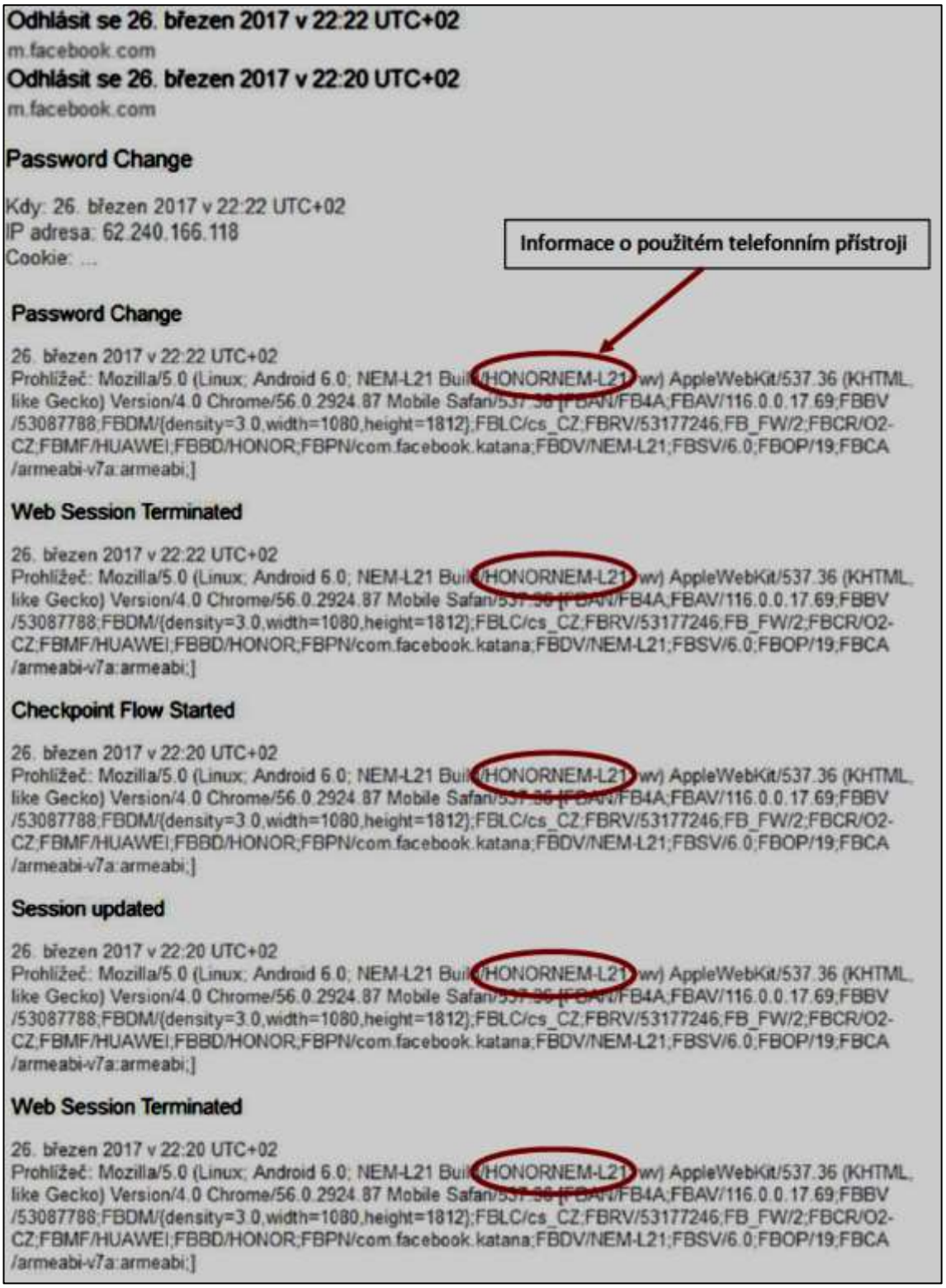
Příloha č. 6

Náhled upozornění zaslaného na e-mail[78]



[78] Zdroj: spisový materiál Policie ČR

Příloha č. 7[79]



[79] Zdroj: spisový materiál Policie ČR