Jan Kolouch

# CyberCrime

Edice CZ.NIC

**CYBERCRIME**
JUDr. Jan Kolouch, Ph.D.

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2016
Kniha vyšla jako 14. publikace v Edici CZ.NIC.
ISBN 978-80-88168-18-8

© 2016 Jan Kolouch
Toto autorské dílo podléhá licenci Creative Commons (http://creativecommons.org/licenses/by-nd/3.0/cz/), a to za předpokladu, že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Dílo může být překládáno a následně šířeno v písemné či elektronické formě na území kteréhokoliv státu.

CZ.NIC | SPRÁVCE DOMÉNY CZ

Právní stav byl zohledněn ke dni 1. 8. 2016.

ISBN 978-80-88168-18-8

— Jan Kolouch

# CyberCrime

— Edice CZ.NIC

# Předmluva vydavatele

## Vážený čtenáři,

titulem, který právě držíte v ruce, se sdružení CZ.NIC vrací k problematice bezpečnosti. Po knize *Buď pánem svého prostoru*, která byla zaměřena především na teenagery a jejíž autoři se pohybovali v americkém prostředí, jsme se tentokrát rozhodli oslovit odborníka českého a vydat knihu zaměřenou komplexněji a odborněji.

Po přečtení knihy rád konstatuji, že Jan Kolouch ve své knize zúročil své bohaté zkušenosti pedagoga, právníka i odborníka na počítačovou bezpečnost a napsal knihu, která bude nejen ozdobou knihovniček, ale zřejmě mnoha lidem bude ležet na stole a budou v ní hojně listovat.

Autor vytvořil text, který obsahuje technické části, které čtenářům pomohou orientovat se ve světě malware, phishingu, darknetu, botnetů a dalších, pro ne zcela technicky zaměřeného uživatele matoucích a odstrašujících pojmů.

Zároveň ovšem kniha obsahuje i právní výklad: analyzuje kybernetickou kriminalitu z pohledu jednotlivých paragrafů, a umožňuje tak získat velké množství cenných informací i těm čtenářům, kteří sice ovládají všechny ty zvláštní technické pojmy, ale svět právních klasifikací, paragrafů a odstavců je jim cizí a neorientují se v něm.

Jsem rád, že máme příležitost vydat právě tento typ knihy. Věřím, že bude užitečná nejen studentům, ale i policistům, členům bezpečnostních týmů a koneckonců i právníkům, kteří přicházejí se světem kyberzločinu do styku stále častěji.

Příjemné čtení a spoustu nových a užitečných informací vám přeje

**Martin Peterka, CZ.NIC**
*Praha, 15. listopadu 2016*

# Předmluva autora

## Předmluva autora

Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný. Ne, toto konstatování není zcela přesné. Dovolím si tvrdit, že ve stavu rozvoje společnosti, v jakém se nacházíme, bez zásadních změn, je dokonce nemožný.

Uvědomuji si, že toto vyjádření může pobouřit celou řadu lidí, kteří se rozhodli žít „off-line", avšak ani ti se v dnešní společnosti nemají šanci vyhnout průniku informačních technologií do svých životů. Virtuální, či rozšířená realita[1] a zejména pak jednotlivé prvky kyberprostoru[2] stále více prostupují do běžného života každého z nás.

Náš svět, ve kterém právě žijeme, a doba digitální, se všemi neodmyslitelnými klady i zápory a nezbytnými technologiemi, se kterými jsme denně spoutáni, mi vždy připomene úryvek z filmu Minority Report.[3] Konkrétně se jedná o průchod Johna Andertona obchodním centrem, při kterém John dostává nabídky na zboží, které je cíleno pouze na něj na základě jeho zvyků, jeho posledních nákupů, jeho zálib atd. Uvedené sci-fi sice má představovat realitu z roku 2054, ale ve skutečnosti se jedná o realitu dnešních technologicky vyspělých společností, ve kterých dochází k prostupu informačních a komunikačních technologií do života každého jedince. Běžně se můžete setkat s geomarketingem v podobě, kterou si sami mnohdy neuvědomujeme. Ivan Bartoš ve své přednášce na Security 2016[4] výstižně popsal stav, kdy se každý z nás stává produktem. Svým způsobem jsme zdrojem informací a dat pro někoho jiného. Otázkou je, kdo je tím „jiným". Mnoho z Vás si automaticky představí Velkého bratra v podobě KGB, CIA, FBI, NSA aj. Pravda je v současnosti mnohem prozaičtější, oněmi Velkými bratry jsou zpravidla společnosti (komerční či nekomerční organizace), které my, jakožto konzumenti informačních a komunikačních technologií a na ně nabalených aplikací využíváme, s pocitem, že je to „zdarma". Krásným příkladem předneseným právě v přednášce Ivana Bartoše jsou věrnostní (slevové) karty, přičemž nijak přitom nezáleží na tom, do jakého obchodu máte věrnostní kartu. Podstatou oné hry, kdy se sami stáváme produktem, je vlastní použití oné věrnostní (slevové) karty. Konkrétní obchodní řetězec je pak schopen například vyhodnocovat, jaké zboží se v jaké lokalitě prodává více, je schopen na Vás cílit konkrétní reklamu, či Vám zasílat letáky, samozřejmě s extra slevou, na zboží, které vy, zákazník, kupujete nejvíce. Tento příklad krásně demonstruje to, jak jsme ovlivňováni informačními a komunikačními technologiemi[5] a to i v okamžiku, kdy naše vzájemná interakce probíhá ve světě reálném, nikoli virtuálním.

1: Viz Oxford Dictionaries. *Augmented reality.* [online]. [cit. 10.7.2016].
Dostupné z: http://www.oxforddictionaries.com/definition/english/augmented-reality

2: Blíže k jednotlivým pojmům viz kap. 1.2.1 Kyberprostor (Cyberspace).

3: Minority Report je americký sci-fi film režiséra Stevena Spielberga z roku 2002.
Blíže k této konkrétní scéně např. [online]. [cit. 10.7.2016]. Dostupné z: https://www.youtube.com/watch?v=4bs9cAeOqZY

4: Přednáška: *„Souhlasím s VOP? Odkliknu a jedu..."* [online]. [cit. 10.7.2016]. Dostupné z: https://konferencesecurity.cz/

5: Dále jen: **ICT** či informační a komunikační technologie, **IT** či informační technologie, **IS** či informační systémy.

Nemyslím si, že je možné se oprostit od informačních a komunikačních technologií,[6] a rozhodně nemá být smyslem této knihy potlačovat či dehonestovat tyto technologie jako takové, či Vám tvrdit, že je máte přestat používat. Přínos těchto technologií pro společnost ve všech oblastech lidské činnosti (např. v lékařské vědě, výzkumné činnosti, bezpečnosti, dopravě aj.) je neoddiskutovatelný. Oblast informačních a komunikačních technologií je nejrychleji a nejvíce se rozvíjejícím odvětvím lidské činnosti.

To, co je třeba si uvědomit, je skutečnost, že informace či data a jejich využití v sobě zahrnují značný ekonomický i politický potenciál. Informace a jejich obsah mohou rozhodovat nejen o bytí či nebytí jednotlivce či firmy, ale ve své podstatě jsou schopny ovlivnit celosvětový vývoj.

Využití informačních a komunikačních technologií má však i stinné stránky. Jednou z nich je bezesporu i gigantický a dynamický nárůst „nového druhu" trestné činnosti, se kterou je třeba se vypořádat tak, aby nedocházelo k ohrožování a porušování zájmů společnosti. Tuto trestnou činnost lze souhrnně nazvat kyberkriminalitou.[7]

Je třeba zmínit, že v celosvětovém měřítku lze pozorovat značnou snahu jak na právní, tak i bezpečnostní úrovni, jejímž cílem je přijmout adekvátní opatření, která by byla schopna reagovat na tento nový a dynamický fenomén současnosti.[8]

Klíčovými body pro rozvoj kyberkriminality se dle mého názoru staly tři skutečnosti.[9] První

6: Vyjma případu, kdy se rozhodnete odcestovat na pustý ostrov... ale i tam si Vás Google Earth najde.

7: **Kyberkriminalita** je mnohdy označována různými názvy. Domnívám se, že nejvýstižnějším pojmem, označujícím toto protiprávní jednání, je právě pojem kyberkriminalita. V této monografii budou pro označení tohoto jevu používány i pojmy **kyberkriminalita, kybernetická kriminalita či kybernetická trestná činnost**. Blíže viz kap. 1.1 Kybernetická trestná činnost (Cybercrime).

Pokud bychom vycházeli z doslovného překladu anglického názvu **Cybercrime**, pak překlad kyberkriminalita není přesný, neboť doslovný překlad tohoto spojení dvou slov je možné přeložit jako: **kyber zločin** (případně **trestný čin**). Avšak i v prostředí České republiky je vžit a běžně užíván překlad **Convention on Cybercrime**, jako **Úmluva o kyberkriminalitě**, byť tento překlad není, jak je uvedeno výše, doslovný. Domnívám se proto, že i vzhledem k tomuto překladu není pochybením užívání pojmu kyberkriminalita.

Vymezení rozdílů mezi kriminalitou a trestnou činností na tomto úseku bude obsaženo v další části této publikace, stejně jako vymezení názorů různých autorů na přesné označení této trestné činnosti. V publikaci budou jako synonyma využívány zejména pojmy kybernetická trestná činnost a kyberkriminalita.

8: Např: *Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy.* [online]. [cit. 10.7.2016]. Dostupné z: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

9: Tyto skutečnosti pak byly podpořeny řadou dalších okolností (např. nedostatek právní úpravy ve vztahu k Internetu, neschopností vynutit právo, pocitem anonymity uživatelů aj.).

z nich je propojení čtyř univerzitních počítačů a vytvoření počítačové sítě určené ke sdílení dat.[10] Druhým vytvoření prvního osobního počítače (PC - Personal Computer) společností IBM na konci 80. let 20. století. Třetím a dle mého názoru nejvýznamnějším milníkem je zpřístupnění Internetu[11] široké veřejnosti, včetně úpravy jednotlivých aplikací do uživatelsky přívětivější podoby.[12]

Rozvoj současné digitální společnosti není založen přímo na hospodářském rozvoji spojeném s hmotnými zdroji, ale na rozvoji IT, na připojování stále většího počtu uživatelů do Internetu, ale zejména k aplikacím jako takovým a v neposlední řadě na zisku informací a dat od uživatelů samotných. Tyto změny související s rozvojem IT probíhajícím jak v sociální, tak i ekonomické rovině a jsou jednou z příčin kyberkriminality.

Kyberprostor je v současnosti nejúčinnější a nejnebezpečnější zbraní v rukou pachatelů kybernetické trestné činnosti. Nejde o to, že by byl kyberprostor, či Internet sám o sobě nebezpečný nebo nezabezpečený. Podstatou je, že systém je vždy tak silný, jak je silný jeho nejslabší článek. V tomto případě je tím nejslabším prvkem, víc než kdy jindy, uživatel. Uživatel je vlastně sám sobě a svému okolí největší „hrozbou", protože byť má právní osobnost,[13] tak často má jen minimální znalosti o svých právech a povinnostech.

Internet se stal součástí našeho každodenního života a zejména jeho multimediální aspekt se velmi rychle rozvíjí. Internet je, ať chceme či nechceme, silnějším a dravějším médiem než televize či jakékoli jiné masmédium. Už nyní může dokonce i prostý uživatel prostřednictvím jednoduchého rozhraní předat či vnutit celé světové populaci svou myšlenku, názory. A je jedno, zda jsou to myšlenky normální, či jakkoli zvrácené.

Na jedné straně Internet nabízí prakticky neomezené možnosti téměř komukoli v získávání a zpracovávání informací téměř o čemkoli, bez nutnosti trávení času v knihovnách či informačních centrech mimo domov (získání předmětných informací je otázkou několika vteřin). Google a Wikipedia se staly relevantním a mnohdy jediným zdrojem informací pro naše rozhodnutí. Internet umožňuje komunikaci sbližující lidi mezi sebou navzájem, usnadňuje řadu aktivit díky

10: Blíže viz ARPANET či NSFNET. Jedná se o období konce 60. let 20. století.
Srov. *Historical Maps of Computer Networks*. [online]. [cit. 10.7.2016]. Dostupné z:
https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

11: Záměrně používám velké písmeno ve slově Internet, pokud jde o vlastní jméno (celosvětovou informační a komunikační síť) malé písmeno pak tam, kde píši o internetu ve smyslu propojených počítačových sítí.
K dalšímu vymezení viz blíže: MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ.NIC, 2013. ISBN: 978-80-904248-7-6.
Matejka dále uvádí, že: *„Je však nepochybné, že malé písmeno patří do trojice pojmů intranet – extranet – internet, užívané rovněž ve významu „komunikační médium", u nichž píšeme malé písmeno. Pokud jde o velké písmeno, mělo by vyznačovat samotný vlastní název jedinečného produktu, v tomto případě veřejně globálního Internetu."* Viz s. 19.

12: Aby se jednalo o kyberkriminalitu, je třeba, aby se toto protiprávní jednání odehrávalo v rámci počítačových sítí.

13: Mají práva a povinnosti. Uživatelé zakládají, mění a případně ruší právní vztahy.

možnosti nalezení řešení či návodu, nabízí množství různých informačních kanálů aj. Přitom to vše umožňuje dělat z prostředí domova a s pocitem téměř absolutní anonymity.

Na druhé straně může mít činnost v tomto virtuálním prostředí za následek těžké finanční ztráty, strach ze zásahů do svého soukromí cizími osobami, ztrátu cenných osobních dat, online komunikaci psychicky narušených osob (pedofilů, drogově závislých, filozoficky dezorientovaných apod.), komunikaci těchto osob s našimi vlastními dětmi za našimi zády, domlouvání kriminálních skupin na nezákonné činnosti bez možnosti odposlechu třetí stranou, podvody, neautorizované průniky do soukromých sfér firem, přesměrovávání obchodních zakázek, vykrádání cizích účtů, ničení dat a databází, poškozování autorského práva atd.

Jsem přesvědčen o tom, že nelze připustit, aby se kyberprostor stal prostředím, kde by pachatelé mohli páchat de facto beztrestně jakoukoliv trestnou činnost. Existuje ale pouze jeden výchozí bod pro boj proti kriminalitě v kyberprostoru, a tím je kyberprostor sám. Je třeba pochopit, co vlastně kyberprostor představuje, na jakých principech pracuje, jaké typy kriminality se mohou v tomto virtuálním světě vyskytovat a co vše mohou orgány činné v trestním řízení, ale zejména uživatel sám, proti této protiprávní činnosti dělat.

Jak již bylo řečeno, kyberkriminalita nabývá v poslední době na stále větší intenzitě. Díky její různorodosti dochází k zásahům do široké škály základních lidských práv (např. čl. 10, 13 a 34 zákona č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod.)[14] každého z nás a informační a komunikační technologie se tak stávají prostředky, jimiž dochází k páchání trestné činnosti nebo jsou samy cílem této činnosti.

Výraznou odlišností kybernetické kriminality od ostatních druhů kriminality je její vysoká latentnost, mnohdy vysoká míra tolerance společností (včetně lhostejnosti uživatelů k případným hrozbám), reálná či domnělá anonymita pachatele a jeho obtížná identifikace, jakož i celý proces dokazování. Proto je třeba řešit nejen otázky represivního působení na pachatele, ale je třeba se zabývat také otázkou prevence trestné činnosti v této oblasti, jakož i otázkou možné ochrany společnosti před touto trestnou činností.

14: Dále jen **Listina**.

**Čl. 10**

(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

**Čl. 13**

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

**Čl. 34**

(1) Práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem.

Vlastní prevence zmíněných negativních jevů musí nutně začít u koncových uživatelů, neboť v kyberprostoru jsou to právě oni, kdo je typickou první obětí útočníka. Na základě svých zkušeností jsem pevně přesvědčen o tom, že výchova a vzdělávání uživatelů má být nezbytnou součástí prostupu informačních a komunikačních technologií do našich životů. Myslím si, že budování informační gramotnosti by mělo být neodmyslitelně spojeno s tvorbou, distribucí a podporou produktů či služeb, které jsou s informačními a komunikačními technologiemi spojeny. Vlastní vzdělávání v této oblasti, či spíše seznamování se s možnými hrozbami, riziky a negativy IT, by mělo být součástí výuky všech forem studia na všech úrovních školství.

Pokud se jedná o osoby, které se této problematice věnují v rámci své profese, pak jsou na tyto specialisty kladeny ještě vyšší nároky, neboť se musí neustále zdokonalovat a školit, aby byli schopni čelit stále novým a dynamicky narůstajícím útokům páchaným prostředky a v prostředí ICT.

Tato kniha shrnuje názory a zkušenosti, které jsem získal v oblasti kybernetické kriminality a kybernetické bezpečnosti. Od roku 2003 se jako vysokoškolský učitel na katedře trestního práva Policejní akademie ČR v Praze věnuji problematice kybernetické kriminality a možnosti jejího trestněprávního postihu. Od roku 2014 jsem také garantem předmětů Kybernalita/Cybernality na FIT ČVUT. Dále dlouhodobě spolupracuji se sdruženími CESNET a CZ.NIC. V rámci své činnosti přednáším zejména na vysokých školách v ČR k vybraným problémům kyberkriminality a prevence této kriminality. Díky svým zkušenostem jsem byl opakovaně přizván European Union Agency for Network and Information Security (ENISA)[15] jako člen expertního týmu při řešení problematik souvisejících s aplikací práva v souvislosti s CERT/CSIRT týmy. Ve své činnosti jsem zároveň měl možnost řídit a kompletně přebudovat infrastrukturu ICT na vysoké škole, takže se domnívám, že jsem schopen propojit jak ryze technické, tak právní a manažerské aspekty pojící se ke kybernetické kriminalitě a kybernetickým hrozbám.

Kniha, kterou právě čtete, je primárně zaměřena na problematiku kybernetické kriminality a částečně na oblast kybernetické bezpečnosti. Byť se jedná o dvě oblasti, které spolu souvisejí, je třeba tyto dvě oblasti oddělit, neboť se každá ubírá jiným směrem. Jsem si vědom toho, že toto „násilné oddělení" je v řadě případů nereálné, neboť kybernetický útok či událost, jež zasahuje do oblasti bezpečnosti, může mít zároveň znaky trestného činu, avšak pro účely této knihy se budu snažit primárně věnovat problematice kybernetické kriminality.

Cílem této monografie není detailně popsat veškeré aspekty, které mohou souviset s kyberkriminalitou (zejména technické oblasti jsou vymezeny relativně stručně), nýbrž ukázat především souvislosti a vzájemnou propojenost ICT, práva a bezpečnosti online.

Předložená publikace ideově vychází z monografie Trestně právní ochrana před kybernetickou kriminalitou, kterou jsem zpracoval společně s kolegou JUDr. Petrem Voleveckým, Ph.D., nicméně aktuální verze je podstatně přepracována a rozšířena. Cílem bylo vytvořit publikaci obsahující aktuální

15: Evropská agentura pro bezpečnost sítí a informací.

informace o kyberkriminalitě a dalších souvisejících aspektech působnosti práva v kyberprostoru, kterou by mohla použít široká veřejnost. Do knihy jsem také zapracoval, ve více či méně přepracované podobě, některé své starší texty (disertační práci, články, prezentace aj.), podobně jsem použil některé fragmenty a myšlenky z prací, které jsem dříve publikoval. Často jsem sám s odstupem času došel k tomu, že jsem své názory revidoval, či pozměnil. Mnohdy jsem k tomu potřeboval slyšet názor jiných, za což jsem jim upřímně vděčný.

Součástí knihy jsou pak i projekty, které jsem realizoval se svými studenty v rámci jejich studentských vědeckých prací, a které demonstrují nebezpečnost chování některých uživatelů v online prostředí.

Identifikační údaje osob použité v příkladech (IP adresy, e-mailové schránky apod.) byly v některých případech pozměněny, na druhou stranu monografie obsahuje celou řadu reálných případů z praxe, u nichž z důvodu objektivnosti byly zachovány informace o skutečných aktérech či detailech útoku.

Posledním, avšak o to významnějším zdrojem informací pro tuto knihu jsou postřehy a náměty studentů, s nimiž jsem měl tu čest diskutovat.

Rozhodně stojí za to, podnítit, ne jen u studentů, diskusi...

Kdykoli rád přivítám jakoukoli zpětnou vazbu od čtenářů této knihy. Vy jste totiž ti, kteří dokáží odhalit chyby a prohřešky, které jsem přehlédl, případně upozornit na témata, která Vás zajímají více. Za jakoukoli vaši zpětnou vazbu jsem vděčný. Tuto knihu jsem se rozhodl vydat pod Creative Commons licencí: CC BY ND.[16]

Závěrem bych chtěl poděkovat všem těm, kdo se o výslednou podobu této knihy zasloužili. Můj dík patří JUDr. Josefu Součkovi, CSc., Andree Kropáčové, Mgr. Juraji Kodyšovi, Bc. Janu Nejedlému, JUDr. Heleně Krejčíkové, Ph.D., mým studentům na PA ČR a FIT ČVUT, jakož i dalším odborníkům, s nimiž jsem měl tu čest spolupracovat a diskutovat. Díky jim za to, že mi otevřeli oči a umožnili mi na problematiku kybernetické bezpečnosti a kriminality nahlížet i z jiných úhlů než doposud. Děkuji všem, kdo byli ochotni číst a připomínkovat rukopis této knihy. Díky za vaše připomínky a náměty.

Poslední dík patří mé rodině, která mi umožňuje být „připojeným bláznem“.

**Jan Kolouch**
jan.kolouch@cesnet.cz

16: Blíže viz kap. 4.10 Internetové (počítačové) pirátství; konkrétně pak kap. 4.10.5 Možná řešení. Bližší informace o creative commons licencích dále naleznete např. na: http://www.creativecommons.cz/licence-cc/; https://cs.wikipedia.org/wiki/Creative_Commons
Byť to může znít šíleně, tak se jedná o následující požadavek: Uvedení autora (umožňuje ostatním rozmnožovat, rozšiřovat, vystavovat a sdělovat dílo a z něj odvozená díla pouze při uvedení autora) + Nevytváření odvozených děl (umožňuje ostatním rozšiřovat odvozená díla pouze za podmínek identické licence).

# Obsah

# Seznam zkratek

## Seznam zkratek

| | |
|---|---|
| APT | Advanced Persistent Threat |
| AZ, autorský zákon | Zákon č. 121/2000 Sb., autorský zákon ve znění pozdějších předpisů |
| BSA | Bussines Software Aliance |
| C&C | Command-and-control |
| CERT | Computer Emergency Response Team |
| CSIRT | Computer Security Incident Response Team |
| Data retention | Plošné ukládání provozních a lokalizačních údajů u poskytovatelů připojení. |
| DBE | Dluh/Banka/Exekuce. Jeden z phishingových útoků. |
| DNS | Domain Name System. Hierarchický systém doménových jmen. |
| Dodatkový protokol | Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě. |
| DoS, DDoS | Denial of Service. Distributed Denial of Service |
| EC3 | European Cybercrime Centre. Evropské centrum pro boj proti kybernetické kriminalitě |
| EFF | Electronic Frontier Foundation. Mezinárodní nezisková organizace zabývající se ochranou práv a svobody slova v digitálním prostředí. |
| ENISA | The European Union Agency for Network and Information Security. Evropská agentura pro bezpečnost sítí a informací. |
| EULA | End User Licence Agreement. Smlouva uzavřená mezi uživatelem a ISP |
| EXIF | EXchangeable Image File Format. Jedná se o formát metadat, která jsou vkládána do digitálních fotografií, digitálními fotoaparáty. |
| GPS | Global Positioning System |
| HTML | Hyper Text Markup Language. Jde o název značkovacího jazyka používaného pro tvorbu webových stránek. |
| HTTP | Hypertext Transfer Protocol. Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. |
| IAP | Internet Access Provider |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICT | Informační a komunikační technologie |
| IoT | Internet of Things. Internet věcí. |
| IS | Informační systém / systémy |
| ISP | Internet Service Provider. Specificky k českému právu je využíván pojem poskytovatel služeb informační společnosti. |
| IT | Informační technologie |
| Krizový zákon | Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů |
| LEA | Law Enforcement Agencies. Bezpečnostní složky státu. |
| LIR | Local Internet Registry |
| Listina | Zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod |
| MMORPG | Massive(ly)-Multiplayer Online Role-Playing Game – počítačová hra na hrdiny o více hráčích, umožňující zapojení hráčů z celého světa skrze Internet do hry odehrávající se ve virtuálním světě. |

| | |
|---|---|
| NAT | Network Adress Translation. Překlad síťových adres. |
| OS | Operační systém |
| OZ, občanský zákoník | Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů |
| P2P | Peer-to-peer |
| PC | Personal Computer. Osobní počítač. |
| RIR | Regional Internet Registry |
| SeznamOTP | Seznam One Time Password. Jeden z phishingových útoků. |
| TOPO, zákon o trestní odpovědnosti právnických osob | Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů |
| TŘ, trestní řád | Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů |
| TZK, trestní zákoník | Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů |
| Úmluva o kyberkriminalitě | Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001 |
| URL | Uniform Resource Locator. Jednotná adresa zdroje. |
| Ústava | Ústava České republiky ze dne 16. 12. 1992 jako součást ústavního pořádku České republiky pod č. 1/1993 Sb., ve znění ústavních zákonů č. 347/1997 Sb., č. 300/2000 Sb., č. 395/2001 Sb., č. 448/2001 Sb. a č. 515/2002 Sb. |
| ÚZČ | Útvar zvláštních činností služby kriminální policie a vyšetřování Policie ČR. |
| VoIP | Voice over Internet Protocol |
| ZKB, zákon o kybernetické bezpečnosti | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| ZoEK, zákon o elektronických komunikacích | Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně dalších zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů |
| ZOOU, zákon o ochraně osobních údajů | Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů |
| ZoP, zákon o přestupcích | Zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů, ve znění pozdějších předpisů |
| ZoZT, zákon o znalcích a tlumočnících | Zákon č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů |
| ZPČR | Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů |
| ZSIS, zákon o některých službách informační společnosti | Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů |
| ZSM | Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů |

# 1 Pojem kybernetické trestné činnosti a pojmy související

*„K tomu, aby zlo zvítězilo, stačí jediná věc – aby dobří lidé nedělali nic.“*
Edmund Burke

# 1 Pojem kybernetické trestné činnosti a pojmy související

V této kapitole se pokusím vymezit některé základní pojmy, které jsou důležité pro pochopení problematiky kyberkriminality. Vzhledem k zaměření a rozsahu knihy není možné vysvětlit veškeré pojmosloví související s kyberkriminalitou a IT, k tomuto účelu slouží například specializované slovníky.[17]

## 1.1 Kybernetická trestná činnost (Cybercrime)

Užívání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. Lze konstatovat, že **v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie**.

Bohužel, tak jak rostou možnosti užívání těchto vymožeností dnešní doby a vědeckotechnického pokroku, rostou i možnosti a zároveň i četnost jejich zneužívání k páchání trestné činnosti.

Různí autoři i různé právní normy používají pro označení těchto aktivit různé pojmy, mezi které patří: informační,[18] informatická,[19] elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost (Computer crime), computer-related-crime, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita aj. U této problematiky přetrvávají rozdíly nejen v označování tohoto jevu, ale rozdílně je chápán též jejich obsahový význam, což mnohdy přispívá k nesprávnému pochopení významu a škodlivosti tohoto druhu trestné činnosti.

Na tomto místě je třeba předně konstatovat terminologickou nejednotnost a různorodost v chápání výše uvedených pojmů. To je do značné míry odůvodněné interdisciplinárností přístupu k řešení dané problematiky. Proto bývají v různých odborných pracích i v právních dokumentech

17: Jedná se například o: HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* 1. Vyd. Praha: Computer Press, 1997. 456 s. či JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-397-0. Dostupné z: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/; https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

18: **Information Crime**: jedná se o trestné činy, jejichž prostředkem jsou informace. V tomto případě nezáleží na tom, jak byly informace zpracovány, či užity k útoku.

19: **IT Crime**: cílem útoku v tomto případě nebývá pouze počítač, jeho data a programy, ale celé informační (počítačové) systémy, včetně jejich komponentů.
Blíže viz SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. aktualiz. a rozš. vyd. Praha: C. H. Beck, 2004, s. 693

často zaměňovány pojmy „počítačový trestný čin" s „počítačovou kriminalitou", „kybernetický trestný čin" s pojmem „kyberkriminalita" apod., resp. jsou mnohdy užívány jako synonyma.

V 90. letech 20. století se pro trestnou činnost páchanou pomocí informační techniky ustálil pojem **„počítačová kriminalita"** (Computercrime, Computerkriminalität). Smejkal ve své publikaci definuje, v polovině 90. let 20. století, počítačovou kriminalitu, jako různorodou směsici trestných činů, jejichž společným faktorem je počítač, program a data. Pod pojmem počítačová kriminalita *„…je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem* ***s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti****."*[20] Z uvedené definice je patrné, že počítačová kriminalita se vztahovala pouze na počítačové systémy, jakožto na cíle útoku.

Označení „počítačová kriminalita" evokuje představu, že trestný čin musí být spáchán na počítači nebo prostřednictvím počítače, nejčastěji počítače osobního (PC - Personal Computer). Takové chápání je dnes zjednodušující, zároveň i poněkud kvantitativně redukuje množství jevů, které lze pod pojem trestná činnost páchaná prostředky informačních a komunikačních technologií zahrnout. Mnohá technická zařízení v dnešní době, díky implementaci mikroprocesorů spolu s jejich miniaturizací, již dávno převzala funkci osobních počítačů (PC), aniž by byla sama za osobní počítače označována. Jedná se o hybridy plnící rozličné funkce, které dříve plnily speciální přístroje. Soudobá technická zařízení umožňující komunikaci mezi sebou a mezi jejich uživateli a jejichž konstrukce je vedena myšlenkou *ALL-IN-ONE* (vše v jednom) dosahují mnohem větších výpočetních výkonů, než nejmodernější výpočetní jednotky z první poloviny 90. let. A i tyto prostředky,[21] přestože nejsou nazývány počítači, mohou být terčem trestné činnosti či prostředkem k jejímu spáchání. Z těchto důvodů se pojem „počítačová kriminalita" či „počítačový trestný čin" v dnešní době již v odborné literatuře téměř nepoužívá. Namísto pojmu „počítač" je v dnešní době používán spíše výraz „informační a komunikační technologie" (*Information and Communiction Technology – ICT*), resp. „trestné činy v ICT".[22]

20: SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo.* Praha: C. H. Beck, 1995, s. 99

21: V současnosti se jedná o celou řadu zařízení, která jsou trestněprávní normou označována jako počítačový systém. Blíže viz kap. 1.2.3 Počítač (Počítačový systém).

22: Blíže např.:

GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 32 a násl.

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

POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 249.

V roce 2000 vydala Rada Evropy definici počítačové kriminality pocházející ze Statutu Komise expertů pro zločin v kyberprostoru: *„Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je užito moderních informačních a komunikačních technologií.“*[23]

Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu označuje za **„computer-related crime“** takové jednání, které směřuje proti počítači, či jednání, kde je počítač prostředkem ke spáchání trestného činu. Ze znění evropského zatýkacího rozkazu pak vychází i definice kyberkriminality.

V mezinárodních úmluvách se pro trestnou činnost páchanou prostředky informačních technologií užívá nejčastěji pojem **„kybernetická kriminalita“** a používání tohoto pojmu se z oblasti normativní přeneslo též do slovníku odborné veřejnosti. Pojem kyberkriminalita má obdobný charakter jako pojmy *„násilná kriminalita“, „kriminalita mladistvých“, „ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).“*[24]

Při vymezení obsahu pojmu **kybernetická kriminalita** si je třeba uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páchání trestné činnosti. Proto v podstatě neexistuje jakási univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla.

Jednu z možných definic počítačové či kybernetické kriminality je možné nalézt i ve Výkladovém slovníku kybernetické bezpečnosti:[25]

***Kybernetická kriminalita - Cyber crime***
*Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.*

*(Více také **Počítačová kriminalita**).*

23: MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 5

24: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 19

25: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 57 a 73. [online]. [cit. 10.7.2016]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

***Počítačová kriminalita / Kybernetická kriminalita – Computer crime / Cyber crime***
*Zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.*

Z těchto dvou definic je patrná snaha o vymezení všech aspektů kybernetické kriminality, avšak autoři se dopustili určitých nepřesností. Zaprvé využívají oba dva uvedené termíny jako synonymum, avšak v definici počítačová kriminalita pomíjí faktory, že počítač je zároveň cílem i prostředkem útoku. Obdobné problémy spojené s vlastním definováním pojmu kybernetická kriminalita je možné nalézt i jinde.

Vzhledem ke snaze o definování pojmu kybernetické kriminality je vhodné využít Úmluvu Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001.[26] Tato úmluva však vlastní pojem kyberkriminality nevymezuje. Definuje pouze opatření, která by měla být přijata ratifikující stranou na vnitrostátní úrovni. Tato opatření v oblasti trestního práva hmotného pak vymezují hrubý rámec trestných činů, které jsou považovány za kybernetické trestné činy.[27] Toto rámcové vymezení (spolu s dalšími trestnými činy obsaženými v Dodatkovém protokolu Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě[28]) poskytuje základní prostor pro jednotnou právní unifikaci trestných činů, které je možné považovat za kybernetické, napříč jednotlivými zeměmi. Vlastní, mnohdy až velmi strohé vymezení daných trestných činů je věci spíše ku prospěchu, neboť nijak neomezuje vnitrostátní (podrobnější či rozpracovanější) implementaci těchto trestných činů, avšak zároveň zaručuje splnění minimálních požadavků (standardů) všemi ratifikujícími stranami.

I z důvodu značné nejednotnosti v názorech na to, co vše je a co není kybernetická kriminalita, v následující části této kapitoly vymezím tento pojem, a to jak z hlediska pozitivního, tak negativního.

Nejobecněji je možné kybernetickou kriminalitu definovat **jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu.** Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.

Při definici pojmu kybernetická kriminalita je nutno v prvé řadě **vymezit pojem kriminalita vůbec**. V souvislosti s provozem informačních systémů, výpočetní techniky či komunikačních prostředků dochází k celé řadě jednání, která jsou jistě nežádoucí, ale nejsou postižitelná prostředky trestního práva, přestože mohou být pro společnost značně nebezpečná (škodlivá). Taková jednání

26: Dále jen **Úmluva o kyberkriminalitě**. Blíže viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
27: Blíže viz kap. 5.1.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě; 5.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě; 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku.
28: Dále jen **Dodatkový protokol**. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
Blíže viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

a priori nemohou být kvalifikována jako počítačová, informační či jakákoliv jiná kriminalita – nejsou totiž kriminalitou vůbec. Při definování pojmu kriminalita (přičemž tuto definici je možno podat z více úhlů pohledu - sociologicky, trestněprávně atd.) se opíráme o definici kriminality jako o **souhrn všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem.**[29] **Podle tohoto vymezení tedy nejsou kriminalitou taková jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupku či jiného správního deliktu**. Takové vymezení pojmu kriminalita je poměrně přesné a lze s ním vystačit i v oblasti informační a komunikační techniky.

Pro páchání trestných činů v oblasti ICT je však charakteristické, že mnohdy jsou v rámci jejich spáchání používány takové postupy či prostředky, jejichž užití nenaplňuje žádnou skutkovou podstatu trestného činu, avšak jsou nedílnou součástí či předpokladem pro jednání další, které již postižitelné prostředky trestního práva je.[30] Navíc tyto netrestné postupy či prostředky představují v procesu odhalování a objasňování trestné činnosti důležité komponenty, jejichž identifikace a pochopení hraje významnou roli při odhalování pachatelů tohoto druhu trestné činnosti.[31]

Kybernetická kriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Delikty páchané v rámci této množiny je možno podle různých hledisek dále třídit a označovat různými pojmy. „Internetová kriminalita", „e-kriminalita", „kyberterorizmus" či např. „pirátství" pak mohou tvořit podmnožiny kybernetické trestné činnosti, přičemž tímto výčtem nedochází k vyčerpání možných podmnožin jednání, které je možné pod pojem kyberkriminalita podřadit.

Pod označením kybernetická kriminalita bývají v odborných publikacích nejčastěji označena taková kriminální **jednání, při kterých jsou prostředky informačních a komunikačních technologií**:

a) ***užity jako nástroj pro spáchání trestného činu,***
b) ***cílem útoku pachatele***, přičemž tento útok je trestným činem.

29: Blíže srov. GŘIVNA, Tomáš, Miroslav SHEINOST, Ivana ZOUBKOVÁ a kol. *Kriminologie.* 4. vyd. Praha: Wolters Kluwer, 2014, s. 21–22.

30: Např. zasílání nevyžádané pošty (SPAM). Spam někdy může být pouze reklamním (obchodním) sdělením. Takovéto jednání pak není postižitelné prostředky trestního práva. Může však nastoupit postih správněprávní (na základě zákona č. 480/2004 Sb., o některých službách informační společnosti). Avšak ani tento zákon nepostihuje zasílání SPAMu, který není nevyžádaným obchodním sdělením. Lze si tak představit například zasílání SPAMu politicky, nábožensky, či jinak motivovaného. Jindy může SPAM obsahovat malware umožňující získat přístupové jméno a heslo k bankovnímu účtu klienta (což je za určitých okolností možné kvalifikovat např. jako přípravu k trestnému činu podle § 20 TZK).

31: Např. díky komunikaci pachatele s okolím je možno vystopovat IP adresu jeho PC a následně lokalizovat místo připojení pachatele k síti Internet.

**Takové vymezení kybernetické kriminality však v dnešní době již neobstojí.** Zahrnovalo by totiž i takové trestné činy, při kterých sice dojde k použití informačních technologií, avšak nikoliv v kontextu jejich běžného užívání či určení (např. jde o případy, kdy pachatel ublíží poškozenému na zdraví úderem monitoru či jinou součástí počítače do temene hlavy v úmyslu způsobit ublížení na zdraví; nebo půjde o krádež nákladního automobilu převážejícího počítačové komponenty apod.). Jde o trestné činy, kde je ICT využito mimo svůj rámec určení – např. jako zbraň, jako věc, která má určitou hodnotu vyjádřitelnou penězi, bez ohledu na to, za jakým účelem slouží nebo má sloužit. Při odhalování a objasňování těchto činů se uplatní jiné metodiky vyšetřování (např. metodika vyšetřování krádeží apod.), nikoliv metodika vyšetřování kybernetické kriminality.

Aby bylo možno hovořit o kybernetické kriminalitě, musí být informační a komunikační technologie, které byly ke spáchání trestného činu užity nebo které byly cílem takového činu, zasazeny do určitého kontextu. V tomto duchu je tedy ke dvěma výše uvedeným bodům nutno přiřadit ještě jeden bod, obsahující tuto podmínku. Kybernetická kriminalita pak tedy představuje takovou kriminalitu, kde jsou prostředky informačních a komunikačních technologií:

*a)* ***užity jako nástroj pro spáchání trestného činu*****,**
*b)* ***jsou cílem útoku pachatele,*** **přičemž tento útok je trestným činem,** ***za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru).***

Takové vymezení kybernetické kriminality je však stále ještě nedostatečné. Za použití takto stanovených kritérií pro určení, zda je či není konkrétní jednání možno považovat za kybernetickou kriminalitu, dojdeme k závěru, že např. hlediska vymezení účastenství ve smyslu § 24 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,[32] je možné spáchat každý úmyslný trestný čin pomocí informačních prostředků (např. osoba přiměje pomocí e-mailových zpráv jiného ke spáchání úmyslného trestného činu vraždy). Obdobně tomu bude i u jiných forem trestné součinnosti (např. podněcování, schvalování trestného činu). Ty lze též spáchat prostřednictvím informačních technologií. **Takováto jednání však za kybernetickou kriminalitu označit nelze. Ve svém důsledku by akceptace opačného názoru vedla k jedinému možnému závěru - každý trestný čin, při jehož spáchání pachatel použil jakýmkoliv způsobem informační a komunikační technologie, je kybernetickou kriminalitou.** Z tohoto hlediska by se pak těžko hledaly trestné činy, které za kyberkriminalitu považovat nelze.

**Z uvedeného vyplývá, že kybernetickou kriminalitu nepostačí vymezit pouze pozitivně, ale je nutno ji vymezit i výčtem jednání, která zásadně za kybernetickou kriminalitu považovat nelze.**

Určitý pokus o takové vymezení je možno nalézt v jednom z dokumentů Odboru bezpečnostní politiky Ministerstva vnitra z roku 2006, který vymezuje trestnou činnost na úseku informačních

32: Dále jen **trestní zákoník** či **TZK.**

technologií jako *„…páchání trestné činnosti, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti,* ***ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.*** "[33]

S tímto negativním vymezením je možno souhlasit jen částečně. Mezi trestné činy hlavy V. trestního zákoníku, tedy mezi majetkové trestné činy, jsou totiž zařazeny i skutkové podstaty trestných činů, které slouží přímo k ochraně informačních a komunikačních technologií (respektive počítačových systémů), jejich součástí, dat na nich uložených, což jsou typické příklady kybernetické trestné činnosti.

V tomto duchu pak bude možno pod pojem kybernetická kriminalita zařadit trestné činy tří různých kategorií:

1) trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku resp. oprávněné zájmy osob na nerušené užívání těchto technických prostředků,

2) trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty,

3) ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky).

## Klasifikace forem kyberkriminality

Domnívám se, že pokud se chceme zabývat problematikou kyberkriminality, bylo by vhodné alespoň rámcově vymezit, co vše je možné pod tuto trestnou činnost zahrnout. Na závěr této subkapitoly chci proto čtenáři předložit některé klasifikace kybernetické (či počítačové) kriminality tak, jak je vnímají různé právní normy, různí autoři, či organizace, které se věnují boji s kybernetickou kriminalitou. Na těchto členěních chci demonstrovat i genezi pohledu na problematiku kybernetické kriminality.

33: *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení.* [online]. [cit. 2.10.2008]. Dostupné z: http://www.mvcr.cz/dokument/2006/informacni.doc

### 1. Klasifikace dle Úmluvy o kyberkriminalitě a dle dodatkového protokolu.

Úmluva o kyberkriminalitě dělí kybernetické trestné činy do čtyř kategorií:

1) **trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů** (Offences against the confidentiality, integrity and availability of computer data and systems),

2) **trestné činy související s počítači** (Computer-related offences),

3) **trestné činy související s obsahem** (Content-related offences),

4) **trestné činy související s porušováním autorských práv a práv souvisejících** (Offences related to infringements of copyright and related rights).

Dodatkový protokol pak definuje další kybernetické trestné činy:

1) **šíření rasistických a xenofobních materiálů pomocí počítačových systémů** (Dissemination of racist and xenophobic material through computer systems),

2) **rasisticky a xenofobně motivované vyhrožování** (Racist and xenophobic motivated threat),

3) **rasisticky a xenofobně motivované útoky** (Racist and xenophobic motivated insult),

4) **popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti** (Denial, gross minimisation, approval or justification of genocide or crimes against humanity).

### 2. Klasifikace Commitee of Experts on Crime in Cyberspace

Dle Statutu Komise expertů Rady Evropy pro zločin v kyberprostoru (Commitee of Experts on Crime in Cyberspace) z roku 2000 lze kyberzločin rozdělit:

1) **Dle pozice počítače při páchání trestné činnosti:**
   - *cíl (terč) útoku;*
   - *prostředek (nástroj) útoku.*

2) **Podle typu činu:**
   - *protiprávní jednání tradiční* (např. padělání bankovek aj.)
   - *protiprávní jednání nová* (např. phishing, DDoS aj.)[34]

34: [online]. [cit. 11.3.2010]. Dostupné z: http://assembly.coe.int/documents/WorkingDocs/doc01/edoc9263.htm
Srov. MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 49

### 3. Klasifikace dle eEurope+

Tento dokument členil počítačové zločiny na:

1) **Zločiny porušující soukromí**
   - Nelegální sběr, uchovávání, modifikace, zveřejňování a šíření osobních dat.

2) **Zločiny se vztahem k obsahu počítače**
   - Dětská pornografie, rasizmus, vyzývání k násilí aj.

3) **Ekonomické**
   - Neautorizovaný přístup, sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody.

4) **Zločiny se vztahem k duševnímu vlastnictví**[35]

### 4. Klasifikace počítačové trestné činnosti dle kriminalistiky

Porada a Konrád[36] dělí počítačovou kriminalitu do pěti základních skupin.

1) **Neoprávněné zásahy do vstupních dat**
   - změna vstupního dokladu pro zpracování počítačem,
   - vytvoření dokladu obsahujícího nepravdivé údaje pro následné zpracování dat počítačem,

2) **Neoprávněné změny v uložených datech**
   - manipulace s daty, neoprávněný zásah do nich a následný návrat k normálu,

3) **Neoprávněné pokyny k počítačovým operacím**
   - přímý pokyn k provedení operace, či instalace softwaru provádějícího operace automaticky,

4) **Neoprávněné pronikání do počítačů, počítačového systému a jeho databází**
   - informativní vstup do databáze, bez využití informací,
   - neoprávněné užívání informací pro vlastní potřeby,
   - změny, ničení, či nahrazování informací jinými,
   - nelegální „odposlech“ a záznam provozu elektronické komunikace,

5) **Napadení cizího počítače, programového vybavení a souborů a dat v databázích**
   - vytváření programů sloužících k napadení,
   - zavedení viru do programového vybavení počítače,
   - vlastní napadení viry, či jinými programy.[37]

35: Blíže: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 92

36: Blíže: STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 272–274

37: Tamtéž

## 5. Zaměření Europolu na některé druhy kyberkriminality dle závažnosti

Europol respektuje Úmluvu o kyberkriminalitě a vychází z členění trestných činů v ní obsažených. Pro podporu boje s kyberkriminalitou a pomoc členským státům došlo, v rámci Europolu ke vzniku The European Cyber Crime Centre (EC3).[38] Tento tým jasně deklaroval svoje pole působnosti v rámci boje s kybernetickou trestnou činností a vymezil následující tři oblasti (FP – focal point), kterým se věnuje:

1) **FP TERMINAL – Payment fraud**. Skupina, která se věnuje a poskytuje podporu při řešení online podvodů.

2) **FP Cyborg – High-Tech Crimes**. Skupina, která se věnuje a poskytuje podporu při různých kybernetických útocích, jež ovlivňují kritickou infrastrukturu[39] a informační systémy. Zejména se jedná o útoky typu: Malware, Ransomware, Hacking, Phishing, Identity Theft aj.

---

38: *Combating Cybercrime in a Digital Age.* [online]. [cit. 7.5.2016]. Dostupné z: https://www.europol.europa.eu/ec3

39: Pokud jde o vymezení pojmu kritická infrastruktura, pak je v ČR (v případě kyberprostoru) třeba vycházet ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále jen **zákon o kybernetické bezpečnosti** nebo **ZKB**. Tento zákon v § 2 písm. b) vymezuje pojem kritická informační infrastruktura a prvek nebo systém prvků kritické infrastruktury.

Definice pojmu kritická informační infrastruktura vychází z právních předpisů upravujících oblast krizového řízení. Kritická informační infrastruktura je součástí kritické infrastruktury, která je vymezena zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů („dále jen krizový zákon"). Aby mohl být určitý informační systém nebo služba a síť elektronických komunikací zařazena do kritické informační infrastruktury, musí splnit definiční kritéria kritické infrastruktury, jakož i prvku kritické infrastruktury, vymezené krizovým zákonem a dále pak i průřezová a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V odvětvových kritériích pro určení prvku kritické infrastruktury je od účinnosti zákona a kybernetické bezpečnosti vložen bod VI. *„Komunikační a informační systémy"*, písm G.: *oblast kybernetické bezpečnosti*. Zde jsou stanovena odvětvová kritéria pro určení daného informačního systému, služby nebo sítě elektronických komunikací kritickou informační infrastrukturou.

Nicméně toto vymezení se vztahuje pouze na oblast kybernetické bezpečnosti. Obecně **je možné vymezit kritickou infrastrukturu následovně**:

1. Kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury narušení, jehož funkce by měla závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
2. Prvkem kritické infrastruktury se rozumí stavba, zařízení, prostředek nebo veřejná infrastruktura určená podle průřezových a odvětvích kritérií, která jsou stanovena nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
3. Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko:
   a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,
   b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
   c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

3) **FP Twins – Child Sexual Exploitation**. Skupina, která se věnuje a poskytuje podporu při vyšetřování trestné činnosti, při níž dochází k sexuálnímu zneužívání dětí.

### Další možné klasifikace kyberkriminality

Existuje i mnoho jiných způsobů klasifikace, pro ilustraci uvádím další možné dělení kyberkriminality.[40]

Na tomto místě si dovolím uvést i klasifikaci, kterou jsem vytvořil na základě vlastních poznatků získaných zejména při interpretaci problematiky kyberkriminality na různých seminářích či konferencích.

Je možné konstatovat, že velmi zjednodušeně lze kyberkriminalitu dělit ze tří hledisek:

1) **Dle četnosti (povahy) útoků:**

   a) **porušování práv autorských** (viz kap. 4.10 Internetové (počítačové) pirátství. Jde o jednání, které je v rámci kyberprostoru dominantní a při kterém dochází k porušování intelektuálního vlastnictví. Snaha o potírání tohoto jevu je zjevná zejména za strany soukromých organizací hájících práva autorů.);

   b) **ostatní kybernetické útoky** (viz kap. 4 Projevy kyberkriminality. Vyjma kap. 4.10 Internetové (počítačové) pirátství.).

2) **Dle postižitelnosti trestním právem:**

   a) **trestním právem řešené jednání** (viz kap. 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku – některé z uvedených jednání subsumovatelných pod skutkovou podstatu trestného činu);

   b) **trestním právem neřešené (nepostižitelné) jednání** (některé z uvedených jednání není možné, ani za použití přípustné analogie,[41] subsumovat pod zákonné znaky skutkové podstaty trestného činu. Jedná se například o jednání popsaná v kap. 4.5 Spam a kap. 4.12 DoS, DDoS, DRDoS útoky).

---

40: Srov. PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 22 a násl.
Dále pak např. *Cybercrime*. [online]. [cit. 1.2.2015]. Dostupné z:
http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; aj.

41: **Analogií se rozumí subsumpce případu v trestním zákoně výslovně neuvedeného, pod zákonné ustanovení podobné, v zákoně uvedené.** Oproti extenzivnímu výkladu je v rámci analogie využíváno ustanovení, které se na subsumovaný případ podle svého smyslu nevztahuje. Extenzivní výklad se realizuje v souladu s účelem trestního zákona a v jeho mezích, kdežto analogie tyto pomyslné hranice překračuje. Užitím analogie dochází k **vyplňování mezer v zákonech**. Jsou jí řešeny případy, které zákonodárce opomněl upravit právní normou. **Nelze ji** však **využít v neprospěch (k tíži) pachatele** (in malam partem).
Blíže viz NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010, s. 83

3) **Dle míry tolerance většinovou společností:**

   a) **společností tolerované jednání** (nejvíce je tolerováno již zmiňované Internetové (počítačové) pirátství);

   b) **společností neakceptované jednání** (např. dětská pornografie - viz kap. 4.13 Šíření závadového obsahu aj.).

## 1.2 Pojmy související s kybernetickou trestnou činností

### 1.2.1 Kyberprostor (Cyberspace)

*„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, …"*
William Gibson: Neuromancer (1984)

Kyberprostor představuje ono pomyslné pískoviště, na kterém se pohybujeme, ale zároveň se jedná o klíčový prvek v definici kybernetické kriminality. Aby bylo možné definovat kyberprostor, je nezbytně nutné vymezit pojem Internet, který právě s kyberprostorem bezprostředně souvisí.[42]

Světové počátky Internetu, který je nezbytnou materiální podstatou kyberprostoru, se datují do 50. let 20. století.[43] V té době došlo k budování a testování sítí propojených počítačů především pro vědeckovýzkumné a vojenské účely. Ačkoli byl Internet vybudován na základech sítí ARPANET a NSFNET,[44] v současné době není nikdo vlastníkem Internetu a neexistuje ani centrální autorita či instituce, která by jej řídila. *„Přesto existují instituce podílející se významnou měrou na fungování a dalším rozvoji Internetu. Jako první jmenujme Internet Society (ISOC), jenž sdružuje internetové uživatele. ISOC má dvě hlavní složky, Internet Activities Board (IAB) a Internet Engeneering Task Force (IETF). Obě tyto složky spolupracují s nejvýznamnějšími počítačovými firmami na tvorbě standardů potřebných pro další rozvoj Internetu."*[45]

---

42: Specifikace připojení koncového uživatele k Internetu je vysvětlena v kap. 1.3 Počítačové sítě a jejich fungování a 1.4 ISP (Internet Service Provider). Vymezení této specifikace je mimo jiní nezbytné i pro postup orgánů činných v trestním řízení, avšak je nadbytečné ji vysvětlovat vrámci pojmu kyberprostor.

43: **Československá republika se k internetu poprvé připojila v roce 1992** prostřednictvím univerzity: České vysoké učení technické.

44: Srov. *Internet History of 1980s*. [online]. [cit. 7.6.2016]. Dostupné z: http://www.computerhistory.org/internethistory/1980s/

45: *Internet, připojení k němu a možný rozvoj (Část 2 – Historie a vývoj Internetu)*. [online]. [cit. 10.2.2008]. Dostupné z: http://www.internetprovsechny.cz/clanek.php?cid=163

Osobně se však domnívám, že výsostné postavení v rámci sítě Internet má sdružení ICANN[46] (Internet Corporation for Assigned Names and Numbers). Do náplně činnosti tohoto sdružení totiž spadá stanovení pravidel pro provoz systému doménových jmen. V současné době se však do popředí stále více dostávají, a větší úlohu hrají ISP.[47]

**Materiální (hmotnou) podstatou** Internetu je jeho páteřní síť, která vede signál (data) vzduchem, kabely, či jinými přenosovými médii. **Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.** Tím je vlastně vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený **kyberprostor**. Lze říci, že kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném. Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného se, díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb, atd.), adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození, či zániku kyberprostoru jako takového.

Kyberprostor je také možné definovat jako prostor kybernetických aktivit či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému.

Pokud jde o legální definici kyberprostoru, je možné využít například znění § 2 písm. a) ZKB, kde je uvedeno, že *„**kybernetickým prostorem je digitální prostředí** umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*

Do obecného povědomí se pojem kyberprostor začíná dostávat po vydání deklarace Johna Barlowa (zakladatele Electronic Frontier Foundation): „A Declaration of the Independence of Cyberspace“:

*„Vlády Průmyslového světa, vy znavení obři z masa a oceli, přicházím z Kyberprostoru, nového domova Mysli. Jménem budoucnosti vás žádám, abyste nás vy, lidé minulosti, nechali na pokoji. Nejste mezi námi vítáni. Vaše svrchovanost nesahá do míst, kde se scházíme.*

*Nemáme žádnou volenou vládu a nejspíše ani žádnou mít nebudeme, proto k vám promlouvám s autoritou o nic větší než tou, se kterou vždy mluví sama svoboda. Prohlašuji námi budovaný globální společenský prostor za přirozeně nezávislý na tyraniích, do kterých se nás snažíte uvrhnout. Nemáte žádné*

46: Blíže viz https://www.icann.org/

47: ISP – Internet Service Provider. Blíže viz kap. 1.4 ISP (Internet Service Provider) a 2.5 Odpovědnost poskytovatele služeb informační společnosti

*morální právo nám vládnout a nemáte ani žádné donucovací prostředky, kterých bychom se skutečně museli obávat.*

*Vlády odvozují svou spravedlivou moc od souhlasu podřízeného lidu. O náš souhlas jste nežádali a ani jste žádný nedostali. Nezvali jsme vás. Neznáte nás a neznáte ani náš svět. Kyberprostor neleží uvnitř vašich hranic. Nemyslete si, že ho můžete budovat, jako by to byl nějaký veřejný stavební projekt. Nemůžete. Je to přírodní jev, který roste prostřednictvím našich společných činů.*

*Nezapojili jste se do našeho velkého podmanivého dialogu a nevytvořili jste ani bohatství našich trhů. Neznáte naši kulturu, naše mravy, ani nepsané zákony, které naší společnosti již teď dodávají větší řád, než by mohlo přinést kterékoliv vaše nařízení.*

*Tvrdíte, že mezi námi jsou problémy, které vy musíte vyřešit. Tohle tvrzení využíváte jako záminku, abyste mohli vtrhnout do našeho výsostného prostoru. Spousta těch problémů vůbec neexistuje. Pokud vzniknou skutečné spory, pokud nastanou křivdy, sami je odhalíme a vyřešíme vlastními prostředky. Vytváříme svou vlastní Společenskou smlouvu. Tohle zřízení vznikne podle podmínek našeho světa, ne toho vašeho. Náš svět je jiný.*

*Kyberprostor sestává z transakcí, vztahů a myšlenek vůbec, uspořádaných jako stojatá vlna v síti našich komunikací. Náš svět je zároveň všude a nikde, ale není tam, kde žijí tělesné schránky.*

*Vytváříme svět, kam mohou všichni vstoupit bez výsad a předsudků spjatých s rasou, ekonomickou mocí, vojenskou silou nebo místem narození.*

*Vytváříme svět, ve kterém může kdokoliv a kdekoliv vyjádřit své přesvědčení, jakkoliv ojedinělé, aniž by se musel bát, že bude násilím umlčen nebo donucen se přizpůsobit.*

*Vaše právní koncepty majetku, projevu, totožnosti, pohybu a kontextu se na nás nevztahují. Všechny jsou založené na hmotě, a tady žádná hmota není.*

*Naše identity nemají tělesné schránky, takže na rozdíl od vás nemůžeme zjednat pořádek pomocí fyzického násilí. Věříme, že naše zřízení se vyvine z mravů, osvíceného osobního zájmu a veřejného prospěchu. Naše identity mohou být rozeseté do spousty vašich právních řádů. Všechny naše dílčí kultury budou obecně uznávat jen jediný zákon, Zlaté pravidlo. Doufáme, že naše vlastní řešení problémů budeme moci vybudovat na jeho základě. Jenže nemůžeme přijmout řešení, která se nám snažíte vnutit.*

*Ve Spojených státech jste dnes vytvořili Zákon o reformě telekomunikací, který popírá vaši vlastní Ústavu a uráží ideály Jeffersona, Washingtona, Milla, Madisona, DeToquevilla a Brandeise. Tyto ideály se teď musejí znovu zrodit v nás.*

*Děsíte se svých vlastních dětí, protože jsou domorodci ve světě, kde vy budete vždy jen přistěhovalci.*

*Protože se jich bojíte, svěřujete svým byrokratickým aparátům rodičovské povinnosti, ke kterým nemáte odvahu postavit se čelem. V našem světě jsou všechny postoje a projevy lidstva, od těch nejpokleslejších až po ty nejvznešenější, součástí jediného nedělitelného celku, globálního dialogu bitů. Není možné oddělit dusivý vzduch od vzduchu, o který se opírají křídla.*

*V Číně, Německu, Francii, Rusku, Singapuru, Itálii a Spojených státech se snažíte zahnat virus svobody budováním strážných věží na hranicích Kyberprostoru. Ty sice nákazu mohou na krátkou chvíli zadržet, jenže budou k ničemu ve světě, který brzy zaplaví bitonosná média.*

*Váš zastarávající informační průmysl se bude snažit upevnit svou pozici navrhováním zákonů, v Americe i jinde, podle kterých by každé slovo na celém světě bylo jejich majetkem. Tyto zákony prohlásí všechny myšlenky jen za další průmyslový výrobek, o nic ušlechtilejší než surové železo. V našem světě se veškeré výtvory lidské mysli dají neomezeně reprodukovat a šířit s nulovými náklady. Globální výměna myšlenek se teď obejde bez vašich továren.*

*Čím dál více nepřátelské a koloniální praktiky nás staví do stejné pozice, v jaké byli i ti předchozí milovníci svobody a sebeurčení, kteří museli odmítnout autoritu vzdálené neinformované mocnosti. Musíme svá virtuální já prohlásit za nedotknutelná vaší svrchovaností, přestože nadále přijímáme vaši nadvládu nad našimi tělesnými schránkami. Rozprostřeme se po celé Planetě, aby nikdo nemohl uvěznit naše myšlenky.*

*V Kyberprostoru vytvoříme civilizaci Mysli. Nechť je lidštější a spravedlivější než svět, který v minulosti vytvořily vaše vlády.*

*Davos, Švýcarsko*
*8. února 1996"* [48]

Osobně jsem přesvědčen o tom, že i po dvaceti letech od vydání této deklarace je její text více než aktuální. Současná společnost se snaží reagovat na obrovský rozmach informačních a komunikačních technologií, jejich vzájemné prolínání a propojování, vznik nových trendů aj. Tato reakce je však mnohdy primárně postavena na vynucování a restrikci, než na pochopení a výchově uživatelů.

Kyberprostor, oproti světu reálnému, je značně specifický a rozhodně je mylné se domnívat, že v něm budou fungovat stejná pravidla, jako ve světě reálném. Obecně je sice možné konstatovat, že na kyberprostor lze aplikovat standardní kritéria,[49] která jsou uplatňována v návaznosti na

48: BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit. 23.9.2014].
Dostupné z: https://www.eff.org/cyberspace-independence.
Český zdroj: http://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru

49: Viz kap. 2 Působnost práva v kyberprostoru a specificky 2.2 Prostředky trestního práva.

skutečnou fyzickou lokalizaci dat či informací. Druhou možností je vytvoření nových kritérií, pro aplikaci principu místní působnosti (jedná se o virtuální lokalizaci právních vztahů).[50]

Pro kyberprostor je příznačné, že se do něj propojila značná část společnosti (odhaduje se zapojení přibližně 3,6 miliard obyvatel, přičemž celosvětová populace činí přibližně 7,4 miliard obyvatel).[51] Zároveň je třeba konstatovat, že k masovému zapojení společnosti začalo docházet teprve před cca 15–20 lety.

Mezi znaky kyberprostoru je možné zařadit jeho decentralizovanost, globálnost, otevřenost, bohatost na informace (a to včetně informací v podobě „informačního smogu", naprostých nesmyslů, polopravd a lží), interaktivnost a možnost ovlivňování mínění skrze uživatele (avatary[52]). Podstatným charakterem kyberprostoru je, že primární roli v něm zaujímají technologie a na ně navázané služby. V poslední době se čím dál víc ukazuje, že projev světa virtuálního může a má dopady ve světě reálném.[53]

Rychlost a zejména dostupnost přenášených dat se stává klíčovým elementem dnešní doby. Uživatel zpravidla nechce a ani nemá snahu zjišťovat, kudy a jakým způsobem dochází k přenosu dat jím do informačních sítí vložených. Nezajímá ho ani, kde se nachází adresát přenášených dat, či kde jsou data uchovávána, tím dochází k odhmotnění obsahu od fyzické struktury informačních sítí.

Na jednu stranu je možné sledovat situaci, kdy jsou **společenské vztahy v kyberprostoru delokalizovány**,[54] což s sebou přináší problémy z hlediska aplikace práva, avšak na stranu druhou tato delokalizace umožňuje uživatelům volně („svobodně" a bez omezení v podobě hranic) komunikovat, zasílat, uchovávat a měnit data.

Kyberprostor je možné si představit jako pomyslný ledovec, kde viditelná část představuje prostor, v němž se běžný uživatel pohybuje při své rutinní práci s ICT.

---

50: Blíže viz REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, s. 218

51: Viz např. *World Internet Users and 2015 Population Stats.* [online]. [cit. 9.8.2015]. Dostupné z: http://www.internetworldstats.com/stats.htm

52: Pojem avatar zde užívám záměrně, neboť jde o vyjádření virtuální identity, která je vytvořena jedincem reálným. Pojem avatár původně vychází z Hinduismu, kde tento pojem označoval zhmotnění boha, či osvobozené duše v tělesné formě na zemi (pozemské vtělení duchovní bytosti).
V současnosti je tento pojem používán jako vizuální reprezentace (ikona či postava) uživatele ve světě virtuálním (ve hře, blogu, fóru, Internetu aj.), tedy v kyberprostoru.

53: Viz jednotlivé útoky uvedené v kap. 4 Projevy kyberkriminality, nebo i například rozmach augmentované reality a služeb na ni navázaných (např. Ingress, Pokemon Go aj.).

54: *Delokalizace právních vztahů na internetu* [online]. [cit. 15.4.2012]. Dostupné z: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html


Obrázek 1: Zobrazení kyberprostoru

Tento ledovec[55] lze rozdělit na následující tři části:
1) **Surface Web,**
2) **Deep Web,**
3) **Dark Web.**

Deep a Dark Weby jsou také často souhrnně označovány jako **D4rkN3ts – Darknets**. Všechny tyto součásti pak společně vytváří skutečný kyberprostor.[56]

Surface Web (také označován jako **Visible Web, Clearnet, Indexed Web aj.**) je ta součást kyberprostoru, která je dostupná většinové společnosti a lze se v ní „pohybovat" za použití standardních

55: *The „Deep Web" is Not All Dark*. [online]. [cit. 12.5.2016]. Dostupné z: http://www.deepwebtech.com/deepweb-not-darkweb/
56: Srov. Např. *The dark Web explained*. [online]. [cit. 20.7.2016]. Dostupné z:
https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
či *Surface Web, Deep Web, Dark Web – What's the Difference*. [online]. [cit. 20.7.2016]. Dostupné z:
https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

prostředků (např. webových prohlížečů aj.). Tato část kyberprostoru v sobě obsahuje služby (stránky), jako jsou např. Google, Facebook, YouTube, Seznam aj. Surface web pak spadá do správy ICANN a má jasně danou strukturu.[57]

Na tomto místě je vhodné zmínit se i o intranetu, respektive o privátních či poloprivátních částech kyberprostoru. Intranet je typicky využíván jako firemní či podniková, počítačová síť (tj. umožňující komunikaci mezi subjekty navzájem, jakož i umožňující přenos dat a informací), avšak tato síť, či její prvek není veřejně dostupný. Tím částečně dochází k vytváření Deep Webu, jakožto jedné ze součástí kyberprostoru. Je třeba si uvědomit, že **Darknets nejsou separátní fyzickou sítí, ale že se jedná o aplikační vrstvu v rámci existujících sítí a služeb**. Rozdíl spočívá především v indexaci obsahu. Surface web představuje onu indexovanou část kyberprostoru, avšak tato indexace činí přibližně pouhé 4 % z celkového objemu kyberprostoru. Oněch 96 % obsahu pak připadá právě na Darknets.

Jsem přesvědčen o tom, že je třeba vymýtit tvrzení, která přirovnávají Darknet k prostředí, v němž se nemáte pohybovat. Stejně jako budete ve světě reálném vykázáni z určité oblasti, protože tam například probíhá demolice, tak je vhodné respektovat určitá doporučení a omezení i ve světě virtuálním. Pro pohyb v kyberprostoru je třeba pochopit základní principy, na nichž funguje připojení vašeho počítačového systému do tohoto prostředí[58] a stejně tak je třeba znát podstatu a pravidla poskytovaných či nabízených služeb. Například vytvořením své soukromé VPN[59] mezi dvěma specifickými počítačovými systémy již vstupujete do prostředí Darknetu. Avšak bez tohoto připojení se v mnoha společnostech nejste schopni připojit k pracovnímu počítači, nebo nemůžete navštívit své oblíbené sociální sítě například z území Čínské lidové republiky.

Vždy pak vyvstane otázka: Je to hrozba? Pro řadu uživatelů budou Darknets vždy představovat hrozbu a nelze u nich změnit názor na to, že jde pouze o prostředí, kde se prodávají drogy, zbraně a dětská pornografie. Pro druhou skupinu lidí pak Darknets představují **„…internet pod Internetem, jehož základní ideou je neregulované a necenzurované prostředí…"**[60] a nástroj Tor Browser, běžný nástroj umožňující nesvobodným svobodnou komunikaci. Než něco odsoudíme, je vhodné se seznámit s podstatou fungování konkrétní věci.

Při plném respektování minimálních základních pravidel Darknets nepředstavují takovou hrozbu, jak mnohá média prezentují.[61] Řadu nástrojů a prostředků, pomocí nichž můžu páchat

57: Viz RIR a LIR v kap. 3.1.1 Digitální stopa neovlivnitelná.

58: Blíže viz kap. 1.3 Počítačové sítě a jejich fungování.

59: Virtual private network – virtuální privátní síť.

60: NUTIL, Petr. *Darknet, aneb cesta do hlubin internetu* [online]. [cit. 10.5.2016]. Dostupné z: http://www.kurzy.cz/zpravy/382630-darknet-aneb-cesta-do-hlubin-internetu/

61: Např.: LOUDA, Pavel. *Darknet: Tak vypadá horší stránka internetu.* [online]. [cit. 15.7.2016]. Dostupné z: http://computerworld.cz/internet-a-komunikace/darknet-temna-strana-internetu-52610

kybernetickou či jinou trestnou činnost, mohu zcela legálně získat i v rámci Surface Webu například na stránkách www.alibaba.com. Jen pro zajímavost si zkuste zadat do vyhledávače na této stránce výraz *card skimmer*. Nemíním nikoho navádět k páchání trestné činnosti, jen se snažím poukázat na to, že pokud se někdo rozhodne spáchat trestný čin, pak si prostředek k jeho spáchání může obstarat kdekoliv.

Na druhou stranu je třeba objektivně přiznat, že v oblasti Dark Webu je možné snadněji narazit na všechny výše zmiňované negativní jevy, jako je prodej drog, dětská pornografie aj.

Princip fungování Darknetu je zpravidla postaven na připojení se na bázi Friend-to-friend (F2F) / Peer-to-peer (P2P). Mezi nejznámější „anonymní sítě", či anonymizéry patří: Freenet[62] a TOR project.[63]

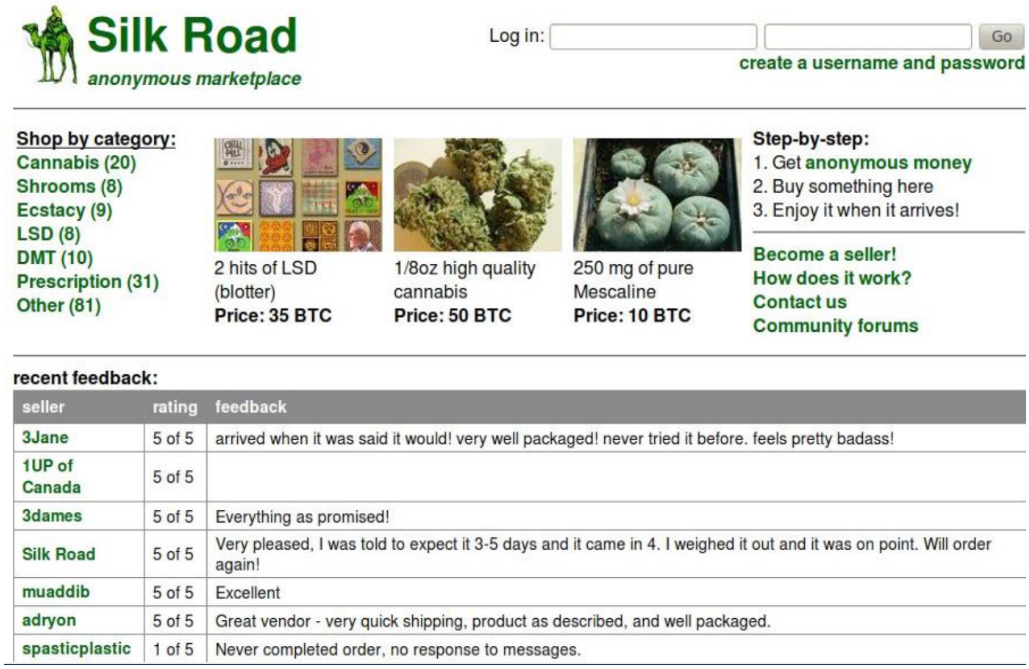
Asi nejznámějším příkladem tržiště v rámci Darknetu, byl Silk Road (http://silkroad6ownowfk.onion, zakladatel: Ross Ulbricht, screen stránky Silk Road je uveden na obrázku č. 2 - Tržiště Silk Road), který zahájil svoji činnost v roce 2011 a uzavřen byl v říjnu 2013 v rámci akce FBI. Podstatou Silk Roadu byla snaha o zachování anonymity jak prodávajícího, tak kupujícího. Transakce byly hrazeny prostřednictvím virtuální měny (v tomto případě Bitcoin[64]) a účty, jež si jednotliví uživatelé zakládali, byly fiktivní. Rozmach Silk Roadu byl spojen především s prodejem drog a s teritoriálním umístěním většiny uživatelů (USA – distribuce zakoupených drog pak zpravidla nenarážela na problémy teritoriality a s nimi spojené procedury, jako je celní kontrola zboží převáženého mezi jednotlivými suverénními státy). Nicméně kromě drog bylo možné na tomto tržišti získat například kradený software; ukradené přihlašovací údaje k e-mailovým adresám, sociálním účtům; falešné či kradené občanské a řidičské průkazy, pasy; kreditní karty; zbraně; padělané zboží všeho druhu aj. Různé zdroje uvádí,[65] že obrat stránky (po dobu jejího fungování) činil okolo **9 519 664** Bitcoinů a bylo zde **957 079** registrovaných uživatelů.

62: https://freenetproject.org/

63: Tor byl původně vytvořen v roce 1995 v U.S. Naval Research Lab, jako prostředek zabezpečeného předávání informací v rámci vládních složek online, přičemž odesílatel a příjemce měli zůstat utajeni. V roce 2003 byl Tor „uvolněn" i pro veřejnost. Bližší informace naleznete na: https://www.torproject.org.

64: Bližší informace naleznete např. na: https://www.bitcoin.com/; http://www.bitcoin-bitcoiny.cz/; http://www.kurzy.cz/bitcoin/ aj.

65: Srov. např.: FRANCESCHI-BICCHIERAI, Lorenzo. *The Silk Road Online Drug Marketplace by the Numbers.* [online]. [cit. 16.6.2016]. Dostupné z: http://mashable.com/2013/10/04/silk-road-by-the-numbers/#9USbF1JntiqU. Zkratka pro bitcoin – BTC.




Obrázek 2: Tržiště Silk Road

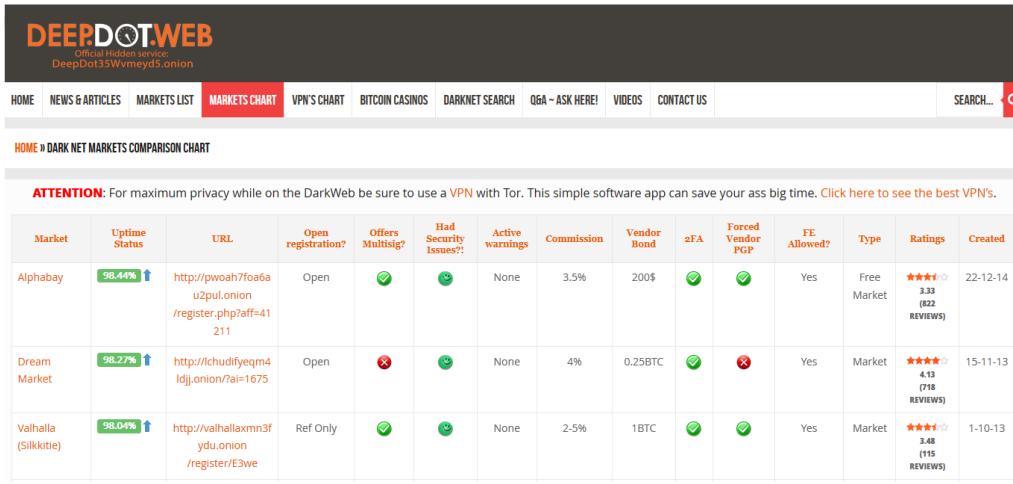
V rámci služby Silk Road byl vždy určitý poplatek z každé transakce připsán na účet Rosse Ulbrichta. Ulbricht byl obviněn z praní špinavých peněz, obchodování s drogami, protivládní konspiraci a hackerství. FBI zajistilo Bitcoiny (26 000 BTC) v hodnotě přibližně 4 milionů dolarů a byly zajištěny finanční prostředky Rosse Ulbrichta pocházející z této trestné činnosti.

Po uzavření Silk Road založili stejní administrátoři, ještě v roce 2013, tržiště Silk Road 2.0. Toto tržiště bylo uzavřeno v rámci společné akce Europolu a FBI dne 17. 10. 2014 (viz Obrázek 3). Dle vyjádření vyšetřovatelů[66] docházelo v rámci tržiště Silk Road 2.0 k transakcím s měsíčním obratem přibližně 8 milionů dolarů, přičemž drogy činily až 70 % prodávaného zboží.

66: U. S. Attorney's Office. *Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court.* [online]. [cit. 18.6.2016]. Dostupné z: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court

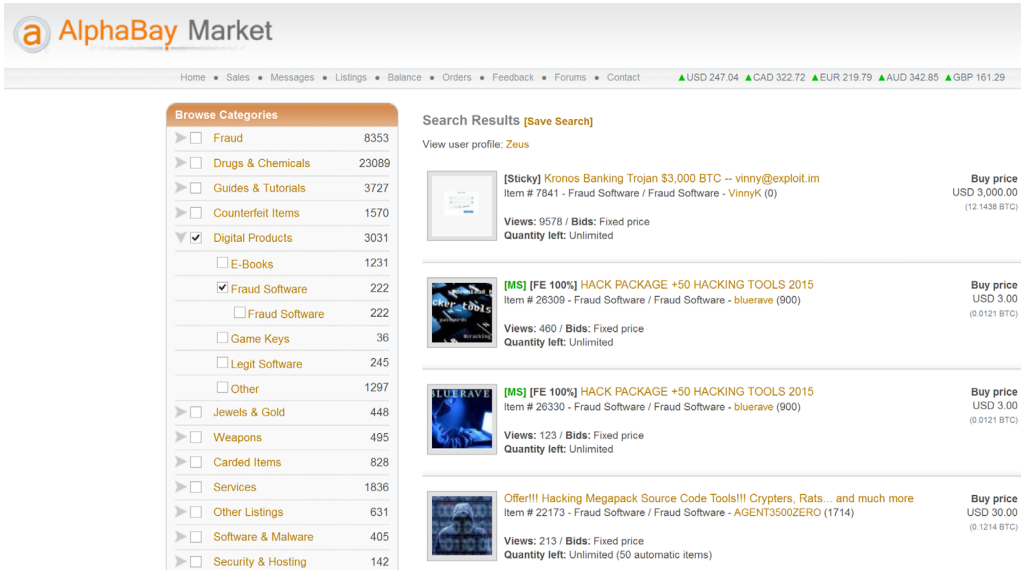

Obrázek 3: Printscreen zobrazující uzavření tržiště Silk Road 2.0

Praxe však ukazuje, že pokud ve virtuálním prostředí jednu službu zakáži nebo jinak znepřístupním, pak na její místo téměř okamžitě nastoupí služby nové, obdobné, mnohdy lépe zabezpečené. Jako příklad je možné uvést seznam tržišť, které fungují v Darknetu, a který naleznete na https://www.deepdotweb.com/dark-net-market-comparison-chart/.



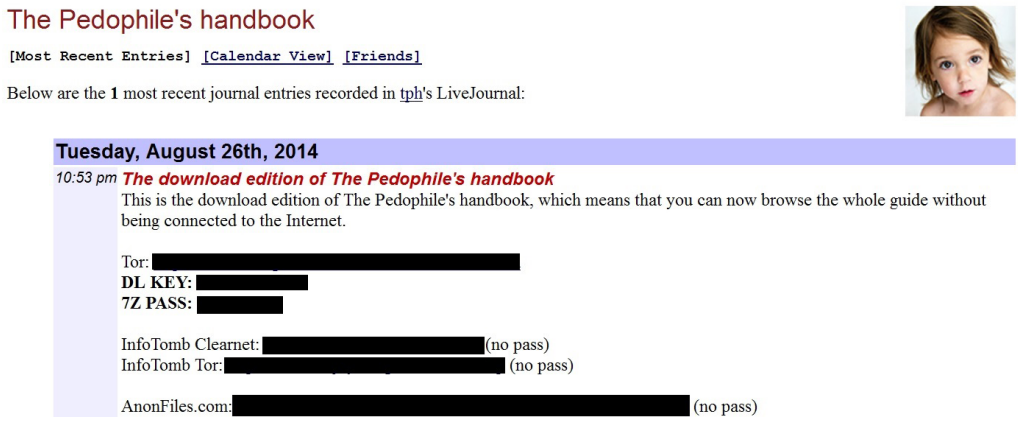

Obrázek 4: Seznam tržišť, které fungují v Darknetu

V současnosti je jedním z oblíbených tržišť tržiště Alphabay. V porovnání se Silk Road 1.0 a 2.0 je třeba konstatovat, že zde dochází k nabízení téměř identického zboží.

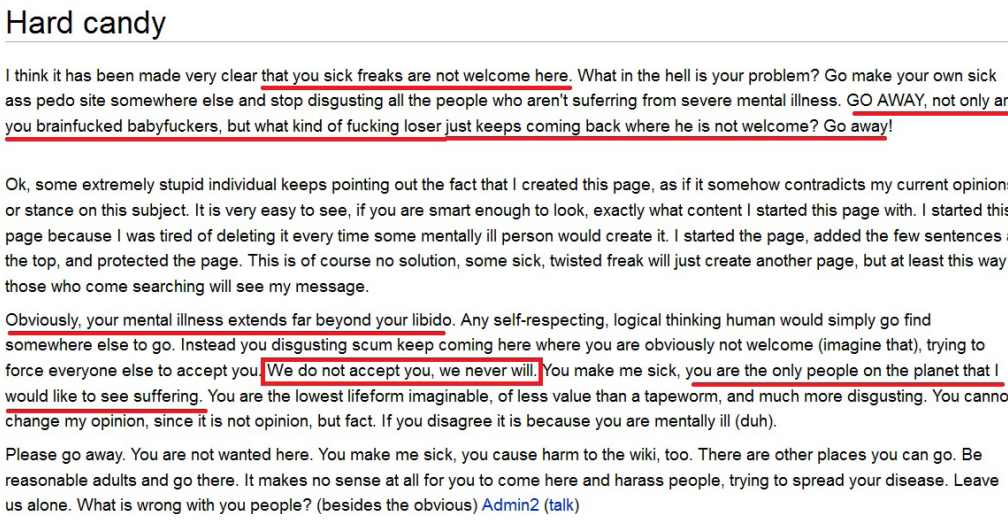



Obrázek 5: Nabídka malware na tržišti AlphaBay Market

Nicméně i v oblasti Dark Webu a aktivit zde prováděných je možné pozorovat určitý posun. Například v roce 2015 bylo možné na Hidden Wiki (http://kpvz7ki2v5agwt35.onion) nalézt návod i stránky na stažení *The Pedophile's handbook* (viz Obrázek 6). Nicméně správce Hidden Wiki se v současnosti jasně a velmi striktně distancuje od podobných aktivit (viz Obrázek 7 - Vyjádření správce The Hidden Wiki k vyhledávání dětské pornografie). Netvrdím, že tímto činem vymizí tisíce pedofilů či jiných osob, které se chtějí dopouštět trestné činnosti, z Dark Webu, avšak je možné pozorovat snahu uživatelů a správců o regulaci obsahu i v prostředí, kde de facto žádná regulace fungovat nemusí. Je mi jasné, že pod Dark Webem může vzniknout Dark Dark Web, či Pitch Black Web, ale i v tomto prostředí záleží na uživateli, správci a dalších osobách, jaké aktivity připustí (budou tolerovat) a jaké už ne.




Obrázek 6: The Pedophile's handbook



## Hard candy

I think it has been made very clear that you sick freaks are not welcome here. What in the hell is your problem? Go make your own sick ass pedo site somewhere else and stop disgusting all the people who aren't suferring from severe mental illness. GO AWAY, not only are you brainfucked babyfuckers, but what kind of fucking loser just keeps coming back where he is not welcome? Go away!

Ok, some extremely stupid individual keeps pointing out the fact that I created this page, as if it somehow contradicts my current opinions or stance on this subject. It is very easy to see, if you are smart enough to look, exactly what content I started this page with. I started this page because I was tired of deleting it every time some mentally ill person would create it. I started the page, added the few sentences at the top, and protected the page. This is of course no solution, some sick, twisted freak will just create another page, but at least this way those who come searching will see my message.

Obviously, your mental illness extends far beyond your libido. Any self-respecting, logical thinking human would simply go find somewhere else to go. Instead you disgusting scum keep coming here where you are obviously not welcome (imagine that), trying to force everyone else to accept you. We do not accept you, we never will. You make me sick, you are the only people on the planet that I would like to see suffering. You are the lowest lifeform imaginable, of less value than a tapeworm, and much more disgusting. You cannot change my opinion, since it is not opinion, but fact. If you disagree it is because you are mentally ill (duh).

Please go away. You are not wanted here. You make me sick, you cause harm to the wiki, too. There are other places you can go. Be reasonable adults and go there. It makes no sense at all for you to come here and harass people, trying to spread your disease. Leave us alone. What is wrong with you people? (besides the obvious) Admin2 (talk)

Obrázek 7: Vyjádření správce The Hidden Wiki k vyhledávání dětské pornografie

Na závěr chci říci, že je možné být anonymní, ovšem pouze za podmínky, že máte dostatečné znalosti ICT, Internetu, jste důslední a máte dostatek času a často i zdrojů. Avšak jako lidé často chybujeme a neuvědomujeme si, že anonymizace jednoho připojení není synonymem pro anonymizaci sítě. Je možné anonymizovat například připojení počítačového systému do počítačové sítě, avšak například využívané služby uchovávají a předávají informace o aktivitách uživatele a počítačovém systému jako takovém.[67]

Domnívám se, že je mnohem lepší pochopit, poznat a porozumět, než pouze zakazovat či nepovolovat. Veškeré tyto aktivity pouze zákonitě vzbudí touhu po zakázaném a neznámém. Cestou k poznání je podle mě pochopení alespoň základních principů, na nichž funguje svět ICT.[68]

### 1.2.2 Kybernetický útok (Cyber attack)

Prosise a Mandiva charakterizují tzv. **„počítačovou bezpečnostní událost"** (kterou lze chápat jako počítačový útok či počítačový trestný čin), jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Tato akce může být zaměřena například na

67: Blíže např viz kap. 3 Anonymita uživatele, konkrétně pak 3.1.1 Digitální stopa neovlivnitelná a 3.2 Smluvní podmínky (EULA).

68: Blíže viz kap. 1.3 Počítačové sítě a jejich fungování.

krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie aj.[69]

Jirásek a kol. definují kybernetický útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“*[70]

Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru,[71] zejména z toho důvodu, že kumulativně slučuje podmínky poškození IT a získání informací. Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství,[72] kde je jediným cílem získat informace, či naopak útok DoS, či DDoS,[73] kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.

Na základě výše uvedeného je tedy možné **kybernetický útok**[74] definovat jako **jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**.[75] Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu.[76]

Kybernetický trestný čin musí být zároveň kybernetickým útokem, avšak ne každý kybernetický útok musí být trestným činem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či nechtěné jednání).

---

69: PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 13

Srov. dále CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 9 a násl.

70: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 59. Dostupný online: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/

71: V uvedené definici chybí zejména vymezení jakékoliv jiné motivace útočníka, než té, která spočívá ve *„...způsobení poškození či zisku strategicky důležitých informací.“* Jako příklad, který tato definice nepostihuje, lze uvést ekonomicky motivované útoky, jejichž počet v současnosti dramaticky roste.

72: Viz kap. 4.1 Sociální inženýrství (Sociotechnika).

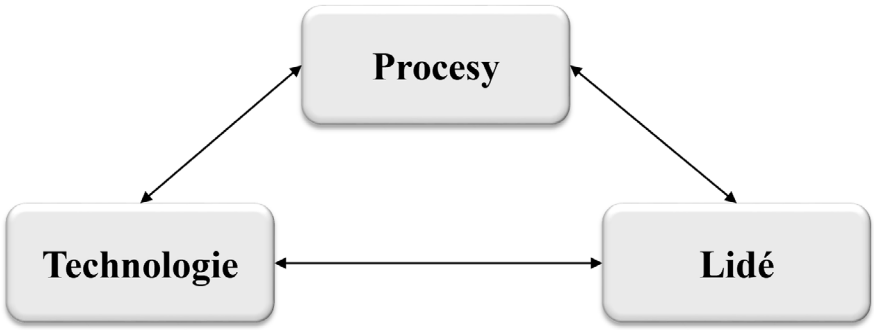
73: Viz kap. 4.12 DoS, DDoS, DRDoS útoky.

74: Od pojmu kybernetický útok je třeba odlišit pojem **bezpečnostní incident**, který představuje narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (bezpečnostní politika).

75: Může jít o jednání uvedená v kap. 4 Projevy kyberkriminality, ale stejně tak může jít o další aktivity v této publikaci neuvedené.

76: Např. útok virem Conficker, který vytvořil Botnet (viz kapitola 4.2 Botnet). Tím byl útok dokonán. Otázkou však zůstává, k jakým účelům bude tato síť případně využita (může se jednat o přípravu daleko vážnějšího kybernetického útoku).

Úspěšnost kybernetického útoku typicky spočívá v porušení některého z prvků, které tvoří kybernetickou bezpečnost (**lidé, procesy a technologie**). **Tyto prvky je třeba uplatňovat, případně modifikovat v průběhu celého jejich životního cyklu. Zejména jde o prevenci, detekci a rekci na útok.**[77] Bezpečnost IT, informací a dat je také přímo závislá na repektování principů „C" „I" „A".[78]




Obrázek 8: Prvky kybernetické bezpečnosti

Pokud chceme definovat pojem kybernetický útok, je vhodné využít i definice, které vyplývají ze zákona o kybernetické bezpečnosti. Tento zákon totiž definuje v § 7 pojmy kybernetická bezpečnostní událost a kybernetický bezpečnostní incident. **Kybernetickou bezpečnostní událostí** je *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."* De facto jde o událost bez zatím reálného negativního následku pro daný komunikační nebo informační systém, ve své podstatě se jedná pouze o hrozbu, která však musí být reálná.

**Kybernetickým bezpečnostním incidentem** je *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události."* Kybernetický bezpečnostní incident tak představuje samotné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem.

77: Blíže viz SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23. 9. 2014)

78: **C** – Confidentiality/důvěrnost; **I** - Integrity/celistvost; **A** – Availability/dostupnost. Systémy, data a informace je nutné chránit před narušením důvěrnosti (Confidentality), dostupnosti (Availability) a integrity (Integrity) a to v průběhu celého jejich životního cyklu.

### 1.2.3 Počítač (Počítačový systém)

Pojmy počítač a počítačový systém jsou na tomto místě uváděny a vysvětlovány záměrně, neboť i když může být na první pohled patrné, že se jedná o notoriety, trestní zákoník tyto pojmy užívá[79] a jejich vymezení z pohledu práva nemusí být vždy jednoznačné.

Existuje celá řada definic pojmu **počítač**.

1) Za počítač je možné označit zařízení, které se vyznačuje následujícími rysy: zařízení obsahuje centrální procesorovou jednotku, schopnou řídit se programovým kódem a schopnou ovládat přidružené periferie a další části počítače; dále zařízení obsahuje médium pro ukládání dat (paměť, disk aj.). Mezi nepovinné prvky počítače se pak řadí zařízení pro vstup dat (klávesnice, myš aj.), zobrazovací zařízení (nejčastěji se jedná o monitor, ale může se jednat i o projektor či jiné zobrazovací zařízení) a jiné periferie.[80]

2) Počítačem je funkční jednotka schopná provádět rozsáhlé výpočty, včetně mnoha aritmetických a logických operací, bez zásahu člověka.[81]

3) Počítačem je každá funkční jednotka schopná provádět výpočty a operace bez lidského zásahu a podle určitého programu, zařízení na zpracování, uchovávání a využívání dat, která převádí na číselné kódy.[82]

4) Jde o soubor technického vybavení (hardware) schopného vyplňovat posloupnost předem stanovených příkazů. Tyto příkazy jsou ve formě programu nebo sady programů (software).

5) *„V nejobecnějším smyslu lze za počítač považovat přístroj, který může být naprogramován za účelem samostatné realizace aritmetických a logických operací.* “[83]

6) *„Elektronické zařízení, které je schopné přijímat informace (data) v určité formě a provádět sekvenci operací v souladu s předem nastavenou, ale variabilní sadou procesních instrukcí (program) za účelem vytvoření výsledku ve formě informací nebo signálů.* “[84]

79: Viz např. § 120, 230, 231 TZK.

80: Srov. HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 85

81: Viz Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník, Část 1: Základní termíny - s. 20.

82: Viz KUCHTA, Josef a kol. *Kurs trestního práva. Trestní právo hmotné. Zvláštní část.* Praha: C. H. Beck, 2009. s. 224

83: POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kolektiv. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 84

84: Viz Oxford Dictionaries. *Computer* [online]. [cit. 7.5.2016]. Dostupné z: http://www.oxforddictionaries.com/definition/english/computer

Veškerá činnost počítače musí být předem naprogramována. Počítač je prostřednictvím paměťových médií schopen uchovávat informace, které do něj mohou být vkládány, zpracovávány a transformovány, nebo je počítač může zpětně poskytovat ve vnímatelné podobě (na zobrazovacím zařízení, jako zvukové signály, případně jako určité činnosti při řízení výrobních procesů).

Pojem počítačový systém je pojmem, který je využíván trestním zákoníkem a který byl do našeho právního řádu včleněn na základě ratifikace Úmluvy o kyberkriminalitě. V čl. 1 písm. a) této Úmluvy je definován počítačový systém jako *„jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.“*

**Počítačový systém** je tedy funkční jednotkou, která **je složena z jednoho nebo více počítačů a přidruženého software**, využívající paměťové médium pro všechny, nebo část programů a dat nezbytných pro vykonání programů.

**Počítačový systém může být samostatnou funkční jednotkou** (pracující samostatně - např. osobní počítač, notebook, smartphone aj.), **nebo může jít o soubor několika vzájemně propojených počítačových systémů** (např. počítačová síť).[85]

Příkladem počítačového systému je osobní počítač (včetně připojených periferií), bankomat (ATM), mobilní telefon, PDA, tablet, herní konzole (např. Sony Playstation, PSP, Wii, Xbox 360) aj. Mezi počítačové systémy je však možné například zařadit i televize či jiné domácí spotřebiče umožňující spouštění aplikací, včetně připojení na Internet, či systémy v automobilech, poskytující obdobné funkce. V současné době, zjednodušeně řečeno, je za počítačový systém možné považovat téměř každé zařízení, které splňuje podmínky **Internet of Things (IoT)**.[86] Relativně komplexním počítačovým systémem je Internet jako takový.

---

85: *Computer system.* Překlad autora. [online]. [cit. 16.2.2010]. Dostupné z: http://www.its.bldrdoc.gov/fs-1037/dir-008/_1198.htm

86: Dále jen IoT, či Internet věcí. **Typicky se jedná o zařízení (počítačové systémy), které sbírají a vyměňují si data s jinými počítačovými systémy. Předpokladem je, že jsou tato zařízení připojena do počítače, či jiné počítačové sítě.** Příkladem může být:

- komunikace mezi televizí a žárovkou, pokud bude televize se žárovkou schopna navázat kontakt, bude možné zajistit optimální nastavení světla, kterou žárovka svítí ve vztahu k aktuálnímu nastavení jasu televize;
- předávání informací z osobní váhy do telefonu či přímo lékaři;
- předání informací z wearables („nositelná“ elektronika, čidla aj.) umístěného v oblečení, botách do počítačového systému pro výpočet ušlých kroků, spálených kalorií aj.
- sledování pozice GPS a předávání této informace;
- sledování množství potravin v lednici a případný automatický nákup chybějících potravin aj.

Bližší informace naleznete např. na: *What is Internet of Things.* [online]. [cit. 15.7.2016]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/internet-of-things

*Internet of Things (IoT).* [online]. [cit. 15.7.2016]. Dostupné z: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Lze konstatovat, že počítačový systém je souhrnem technických a programových prostředků, jejichž variabilita je značná a uvedený výčet je pouze orientační a zdaleka nepostihující všechny možnosti. Vývojem techniky se tak i rozsah zařízení, které spadají do definice počítačového systému, značně posouvá.[87]

### 1.2.3.1 Hardware

**Hardware** (z angl. významu: „technické vybavení"). Pojem hardware vyjadřuje souhrn hmotných technických prostředků umožňujících nebo rozšiřujících provozování počítačového systému.[88] Jde o veškeré fyzické zařízení, které je třeba pro funkci systémů zpracování informací. Je to v podstatě počítač sám. Negativním vyjádřením lze uvést, že hardware je vše, co není programovým vybavením (software). Hardware je možné rozčlenit na dvě skupiny:

1) **Vnitřní vybavení počítače.** Jedná se o součásti hardwaru, bez kterých by nebyla možná vlastní činnost počítače. Těmito nezbytnými komponentami jsou: základní deska s obvody, paměť, procesor, napájecí zdroj. Mezi současné standardní vnitřní vybavení počítače však dále patří harddisk, grafická karta (umožňující vizualizaci činnosti počítače), mechaniky paměťových médií (FDD, CD, DVD, CD-RW, DVD-RW, Blu-Ray, čtečky karet), porty/řadiče (ATA-PATA/SATA, PCI, USB, FireWire, E-SATA aj.), síťové komponenty (umožňující komunikaci v rámci sítí), zvukové a televizní karty aj.

2) **Periferie** (peripheral, či **peripheral device**).[89] Jedná se o zařízení, která ve své podstatě nejsou nezbytně nutná k samotnému provozu počítače (pouze rozšiřuje možnosti jeho využití). *„**V širším slova smyslu** se za periferii považuje cokoli kromě základní desky počítače s jeho procesorem (periferií tedy je: paměť, disk, disketová mechanika, porty, klávesnice, monitor), **v užším slova smyslu** pak až zařízení připojovaná k počítači externě a skutečně nepotřebná k obvyklému provozu i ovládání počítače."*[90] Nejběžněji je periferie chápána právě v užším slova smyslu, tak jak je zde uvedeno. V tomto pojetí se jedná o zařízení, které se různými metodami (kabely, infračervený přenos, technologie Bluetooth, WiFi aj.) připojuje k počítači. Periferií je například klávesnice, myš, monitor, tablet, externí paměťová zařízení, tiskárna, datový projektor, optické senzory, scanner, plotr, externí modem, joystick aj.

Za **předmět sloužící k ovládání počítačového systému** je možné považovat některé z výše uvedených periferií (např. klávesnice, myš, tablet aj.).

87: Srov. SVETLÍK, Marian. Počítače a kriminalita. In: *Sborník odborných sdělení ze semináře uskutečněného na Policejní akademii dne 26. 1. 1999*. Praha: Policení akademie 1999, s. 93 a 97

88: Viz HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 182

89: Periferní zařízení - Norma ČSN ISO/IEC 2382-1. Informační technologie - Slovník. Část 1: Základní termíny, s. 9

90: Viz HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 309

**Procesor (Central Processing Unit – CPU)** je nezbytnou součástí každého počítače. Tato základní elektronická součást počítače je schopna provádět strojové instrukce. Dochází v ní ke kontrole a provedení všech zadaných operací.[91]

Hlavními součástmi procesoru jsou: aritmeticko-logická jednotka (ALU - tato jednotka provádí vlastní výpočetní operace), registry (lze rozlišovat registry obecné a řídící) a řadič. Řadič řídí činnost procesoru, neboť zprostředkovává načítání strojových instrukcí z paměti, jejich dekódování, provedení a následné uložení výsledků. Pokud má obvod v sobě více procesorových jednotek, pak je označován jako vícejádrový procesor (přičemž uváděn je počet fyzických a virtuálních jader).

Současné počítače v sobě kromě hlavní procesorové jednotky mají zabudovány zpravidla další „podpůrné" procesorové jednotky, které s hlavní procesorovou jednotkou spolupracují. Tyto jednotky slouží např. pro provádění výpočtů pro grafické výstupy (GPU), zajištění WiFi, Bluetooth komunikace, příjem GPS aj.

**Paměťové** nebo **záznamové médium** (případně datový nosič či nosič informací) je externí nebo interní prostředek k zápisu a uchovávání dat. Kromě popsaných pevných disků jsou to nejčastěji diskety, kompaktní disky s různou hustotou zápisu (CD, DVD, Blu-Ray), paměťové karty (SD, MMC, CF karty, SDHC aj.), elektronické paměti typu USB (flashdisky) apod. Paměťovým médiem jsou však i operační paměti.

**Operační paměť** (**vnitřní** či **hlavní paměť**. Anglicky: main memory, internal memory, primary storage) je nezbytnou součástí počítače, neboť umožňuje čtení i zápis dat, nad nimiž programy vykonávají operace. Operační paměť je s procesorem spojena pomocí rychlé sběrnice a procesor má okamžitý, či přímý přístup k této paměti,[92] respektive k přímo požadované buňce operační paměti. Operační paměť je rozdělena do paměťových míst (buněk), které mají definovanou velikost (typicky 1, 2, 4 či 8 bytů). Toto rozdělení se nazývá **fyzický adresový prostor (FAP)** a slouží k:

- přidělování paměťových regionů na požádání procesů,
- uvolňování paměťových regionů na požádání procesů,
- udržování informací o obsazení adresového prostoru,
- zabezpečení ochrany paměti (zabránění přístupu procesu k paměti mimo jeho přidělený region).

V současných počítačích je operační paměť v podobě RAM (Random Access Memory). Jedná se o polovodičovou paměť, která je typicky volatilní (dochází ke ztrátě uložených dat v případě odpojení od zdroje napájení) a dynamická. Mimo paměti RAM se v počítači nachází i paměť

91: Překlad autora. Viz Oxford Dictionaries. *Central processing unit* [online]. [cit. 4.4.2016].
Dostupné z: https://www.oxforddictionaries.com/definition/english/central-processing-unit

92: Překlad autora. Viz Oxford Dictionaries. *Main memory* [online]. [cit. 4.4.2016].
Dostupné z: https://www.oxforddictionaries.com/definition/english/main-memory?q=main+memory

ROM (Read Only Memory), která umožňuje pouze čtení, nikoliv však zápis dat. Tato paměť typicky slouží pro uchování základního řídícího software počítače (BIOS: Basic Input Output System. Tato paměť je součástí polovodičové desky – základní desky), či pro uchování firmware aj. Paměť ROM je energeticky nezávislá.

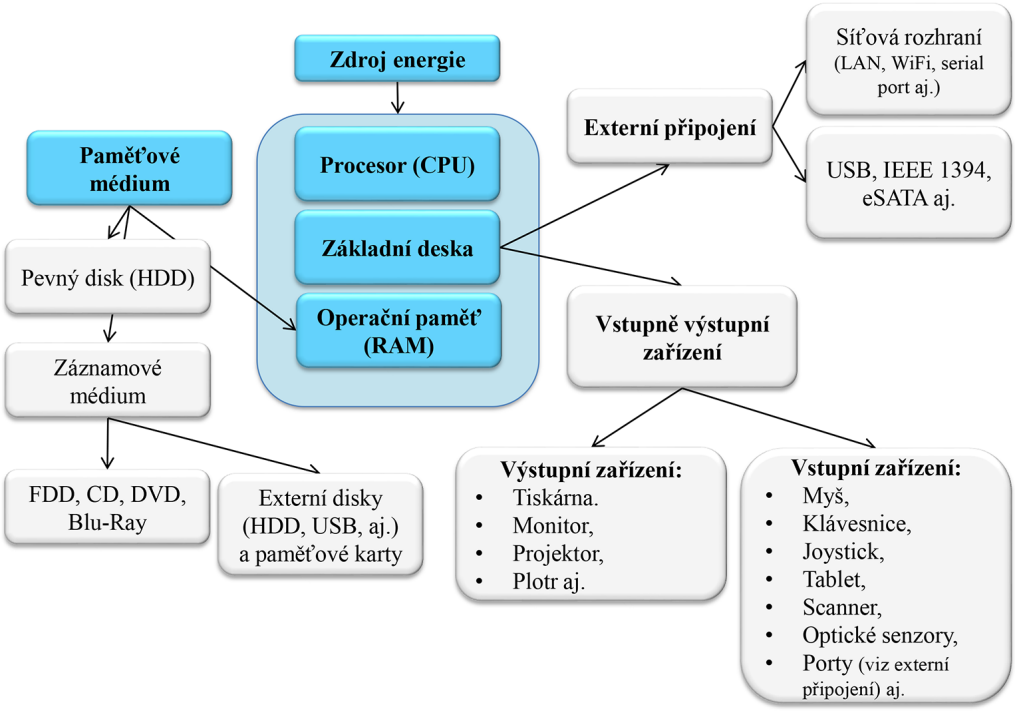
**Základní deska (mainboard, motherboard)** propojuje jednotlivé součásti počítače do fungujícího celku. Přes základní desku dochází k napájení jednotlivých komponent. Základní deska obsahuje integrované obvody zabudované v čipové sadě (chipset). Fyzicky se může jednat o jeden či dva čipy, přičemž čipová sada rozhoduje o tom, jaký procesor a operační paměť lze k základní desce připojit.

**Harddisk (pevný disk)** je paměťové médium zabudované v počítači sloužící k ukládání a uchování dat a programů, instalaci a načtení systému. Povrch disku je rozdělen do sektorů, které mají přesně definované umístění a obsahují příslušná data. Alokační tabulka disku (jedná se nejčastěji o tabulku FAT či NTSF, která je na pevně daném místě disku) určuje, v jakém sektoru disku se data nacházejí. Toto určení má význam zejména z hlediska znaleckého zkoumání paměťových médií. V současnosti se kapacita jednotlivých pevných disků pohybuje v rozmezí několika desítek či stovek MB až po několik TB. Pevné disky mohou být propojeny i v tzv. diskovém poli nejčastěji prostřednictvím SCSI (Small Computers System Interface), či SATA, PATA aj.

**Server** je výkonný počítačový systém, užívaný nejčastěji v počítačové síti jako zdroj dat a programů pro koncové počítače, tzv. klienty nebo pracovní stanice. Pracovní stanice mohou všechny současně pracovat s daty na serveru, přičemž využívají jeho diskové kapacity a programy uložené na jeho discích. Serverů může být zapojeno v síti i několik a každý z nich může plnit specifickou funkci (např. tiskový server, databázový server, terminal server, firewall aj.).

Pokud bychom chtěli graficky znázornit současný počítačový systém, pak by jedním z vhodných zobrazení mohlo být to následující (Modré[93] bloky jsou povinné a bez nich nemůže počítačový systém fungovat. Šedé bloky pak představují periferii v užším či širším slova smyslu. **Zároveň je třeba konstatovat, že počítačový systém musí využívat přidružený software pro to, aby mohl fungovat.**):

93: Poznámka vydavatele: V černobílé verzi knihy nahrazuje modrou barvu tmavě šedá.




Obrázek 9: Grafické zobrazení počítačového systému a jeho částí

### 1.2.3.2 Software

Mezi pojmy **programové vybavení, počítačový program a software** je rozdíl. Nejširším pojmem je software (softwarový produkt), který v sobě zahrnuje nejen počítačový program, ale i databáze a multimédia apod.

Z hlediska přehlednosti budou vymezeny všechny výše uvedené pojmy, nicméně je třeba uvést, že české i mezinárodní právní normy pracují jak s pojmem počítačový program, tak pojmem programové vybavení či software.[94] Mnohdy jsou tyto pojmy využívány jako synonyma, avšak nelze než zopakovat, že mezi vlastními pojmy existují určité odlišnosti.

94: Například trestní zákoník využívá jak pojem **počítačový program** (konkrétně v ustanoveních § 103, 231, 236, 348 TZK), tak **programové vybavení** (v ustanoveních § 120, 230, 232, 264, 267 TZK).

**Programové vybavení** (někdy nepřesně označované jako software) je součást výpočetní techniky. Jsou to programy a přidružená dokumentace, jimiž je doplněno technické vybavení počítače, aby bylo umožněno jeho využití.[95]

Programové vybavení v sobě zahrnuje programy počítačů, počítačové programy včetně software. Jedná se o programy, procedury, pravidla a příslušnou dokumentaci systému zpracování informací nebo jejich část.[96]

**Software** je anglický výraz označující veškeré programové či netechnické vybavení, nutné k provozu počítačů. Software zahrnuje programy od základních vstupně/výstupních systémů (BIOS) a jednoduchých utilit přes operační systémy [nejčastěji MS Windows v různých verzích a OS Linux], grafická rozhraní a veškeré aplikace, od jednoduchých až po komplexní programové systémy.[97] *„Software jsou instrukce, které způsobí, že počítač může být využit. Označuje tedy „logickou" část počítače, kterou nelze vnímat přímo lidskými smysly, tj. „vidět ji nebo si na ni sáhnout". V širším slova smyslu to jsou veškeré informace, které jsou v počítači nějakým způsobem uloženy a dále se dělí podle způsobu použití do dvou základních skupin. Jsou to PROGRAMY a DATA."*[98]

**Počítačový program** je charakterizován jako zápis algoritmu v takovém tvaru, ve kterém jej systém na zpracování údajů dokáže zpracovat. Lze jej charakterizovat jako ucelený souhrn instrukcí (příkazů), pomocí nichž provádí počítač určitou činnost. Program je tvořen souborem nebo více soubory, které jsou v úhrnu dostatečně schopné provádět předepsanou činnost. Příbuznými termíny, mezi kterými lze těžko vymezit ostrou hranici, jsou:

- *aplikace, čímž se označuje obvykle komplexnější souhrn často i několika programů, které plní úkoly dané oblasti;*

- *software, čímž se označuje jakékoli programové vybavení počítače, které je ucelené spíše svým vnějším zjevem.*[99]

Dle Šámala je počítačový program souborem instrukcí, které mohou být počítačovým systémem provedeny pro dosažení zamýšleného účinku. *„Lze ho definovat i tak, že jde o množinu příkazů, instrukcí, deklarací a popř. jiných prvků programovacího jazyka, vyjadřující algoritmus řešení nějakého problému."*[100]

95: Blíže viz ČSN 36 90 01 – dnes již nezávazná.

96: Blíže viz ČSN ISO/IEC 2382 – s. 9

97: Jako jsou například hry, textové a tabulkové programy, grafické programy aj. - srov. HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 379

98: Viz PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování softwarového pirátství.* Praha: Policejní akademie, 1999, s. 43

99: Srov. HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 328

100: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. vyd. Praha: C. H. Beck, 2012, s. 2306

**Počítačový program** je chráněn jako dílo literární,[101] bez ohledu na formu jeho vyjádření, a to včetně přípravných koncepčních materiálů. Chráněny však nejsou myšlenky a principy, na nichž je založen jakýkoliv prvek počítačového programu.

Program je zapsán ve **strojovém (binárním) kódu** či **zdrojovém kódu**.

**Strojový kód** je souhrn operací či příkazů vyjádřených v řetězci přirozených číslic v binárním tvaru. Jedná se o základní podobu povelů, které je stroj schopen přečíst.

**Zdrojový kód** je (v informatice) označení zápisu textu počítačového programu v některém programovacím jazyce, který je uložen v jednom nebo více textových souborech. *„Zdrojový text a jeho převod do binárního kódu tvoří celek jako dílo (pokud splňují další znaky autorského díla).*[102]

Zdrojový kód je nadřazen kódu strojovému.

### Příklady některého software

**Public domain** jsou programy, které jsou volně šiřitelné a lze je jakýmkoli způsobem dále upravovat a používat, aniž by se osoba vystavovala případné trestní odpovědnosti. Public domain programy jsou chráněny jako autorská díla. Jde o program určený pro volné užití (jedná se např. o 7-Zip, SQLite, CERN httpd aj.)

**Firmware** je základním programovým vybavením počítače (BIOS) uloženým v paměti ROM. Firmware v sobě obsahuje programy a funkce, které jsou relativně neměnné a nevyjímatelné (jedná se např. MB BIOS, GPU BIOS aj.).

**Freeware** jsou programy, které jsou volně šiřitelné, autor však nedovoluje jejich úpravu a modifikaci. Freeware zcela podléhá ochraně prostředky autorského a trestního zákona (jedná se např. Audacity, Imgburn, Itunes, CCleaner, Recuva, Google Chrome, Opera aj.).

**Shareware** jsou programy, které jsou určeny k vyzkoušení a které lze volně šířit. Po definovaném čase, případně počtu spuštění, může program přestat fungovat a uživatel je vyzýván k zaregistrování (další legální používání je pak možné pouze po zakoupení licence). Shareware je obvykle distribuován ve verzi, která je oproti registrované verzi nějakým způsobem omezená (funkčně nebo časově) a zpravidla slouží k tomu, aby se uživatel seznámil s programem před jeho zakoupením. Shareware programy jsou chráněny jako autorská díla (jedná se např. CommView, File Scavenger, MP3 Speed Changer, WinRAR aj.).

**Komerční software** lze získat pouze jeho zakoupením nebo jiným legálním převodem vlastnických práv (dar, dědictví). Jeho volné šíření není dovoleno. Zpravidla si uživatel zakupuje

101: viz § 65 zákona č. 121/2000 Sb., autorský zákon. Dále jen **autorský zákon** či **AZ**.

102: Viz PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování softwarového pirátství*. Praha: Policejní akademie, 1999, s. 43

pouze licenci umožňující (za přesně stanovených podmínek) užívání softwaru (jedná se např. o Adobe Acrobat Pro, Final Cut Pro aj.).

**Licenční smlouvou** (srov. § 46 AZ) poskytuje autor nabyvateli oprávnění k výkonu práva dílo užít (**licence**) k jednotlivým způsobům nebo ke všem způsobům užití v předem stanoveném rozsahu. Koncový uživatel počítače se zakoupením operačního systému či kancelářského aplikačního programu nestává majitelem tohoto programu, jak se mnozí mylně domnívají, ale je mu poskytnuta pouze licence k užití díla.

### 1.2.3.3 Data a informace

Dle Úmluvy o kyberkriminalitě[103] se **počítačovými daty** rozumí *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.*"

**Data** *„jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace.*"[104] Data jsou jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačem. Data jsou uchovávána v ucelených souborech, které mohou být různého typu (např. textové, obrazové, binární aj.). Data jsou zpracovávána tak, aby následně utvořila informaci.

Definici dat, respektive počítačových dat, uvádí i Úmluva o kyberkriminalitě v čl. 1, kde je stanoveno, že *„počítačová data znamenají jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.*"[105]

Data jsou z hlediska trestního práva uchovávána na nosičích informací (viz např. § 230 a násl. TZK). Pojem nosič informací je opět pouze synonymem pro nosič dat či paměťové médium (viz kap. 1.2.3.1 Hardware). Podstatné je, že vzhledem ke kontextu uvedeného v trestním zákoníku je třeba za nosič informací považovat takové médium, které je schopno uchovat data v digitální podobě.[106]

Pokud jde o definici **informace**, pak je možné využít teoreticko právní definici od Knappa, který uvádí, že informace je něčím, co snižuje entropii znalostí příjemce, a to tím, že rozmnožuje jeho znalosti, znalosti ověřuje nebo je zdokonaluje.[107]

103: Čl. 1 písm. b) Úmluvy o kyberkriminalitě.

104: Blíže viz POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005. s. 24

105: *Úmluva o kyberkriminalitě.* [online]. [cit. 20.8.2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

106: Nosičem informací dle ustanovení § 230 a násl. TZK tedy nebude např. listina, či jiné médium, které je schopno nést informace v „nedigitální" podobě.

107: Srov. KNAPP, Viktor. *Teorie práva.* Praha: C. H. Beck, 1995, s. 222.

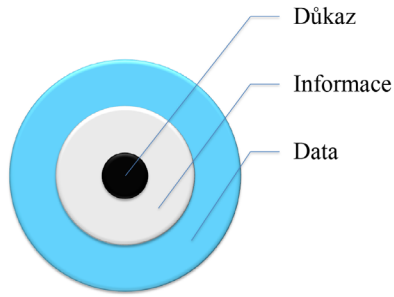
Smejkal uvádí, že za informaci je možné považovat *„každé energetické sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá.“*[108]

**Informace** *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“*[109] **Vymezení vztahu mezi informacemi a daty je nutné zejména pro dokazování v trestním řízení.**

Informace jsou vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi.[110]

Pro úplnost a názornost uvádím i pojem **důkaz** a jeho vztah k pojmům data a informace. Důkazem je informace vyplývající z určitého úkonu trestního řízení, kterým se orgán činný v trestním řízení přesvědčuje o skutečnosti důležité buď pro rozhodnutí ve věci samé, nebo pro následný postup v trestním řízení.[111] Důkaz je přímým poznatkem o předmětu dokazování (což je skutečnost, která má být zjištěna) získaný důkazním prostředkem (postupem dle trestního řádu) z nositele důkazu (jedná se o zdroj informace; tímto zdrojem může být osoba nebo věc).[112] Ne každá informace může být důkazem, ale každý důkaz musí být nutně informací.

Vztah dat, informací a důkazu demonstruje následující graf :[113]




108: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 36

109: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

110: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vyd. Praha: C. H. Beck, 2012, s. 2308

111: Srov. FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní*. 6 vyd. Praha: Wolters Kluwer, 2015, s. 330

Srov. NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní*. Plzeň: Aleš Čeněk, 2009, s. 227

Důkaz je přímým poznatkem o předmětu dokazování získaný v procesu dokazování pomocí důkazního prostředku.

112: Blíže viz kap. 6.3 Specifika dokazování kyberkriminality.

113: Graf vychází ze zobrazení vztahu data a informace, uvedeného Požárem (viz: POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 25) avšak je doplněn vztah důkazu.

## 1.3 Počítačové sítě a jejich fungování

Tato subkapitola definuje pojem počítačové sítě a další základní pojmy a některá technická specifika související s počítačovými sítěmi a Internetem. Uvedená minimální charakteristika je zcela nezbytná pro pochopení fungování počítačových systémů v rámci počítačových sítí.

Alespoň obecná znalost v této subkapitole uvedeného schématu připojení k počítačové síti a jeho jednotlivých komponent je důležitá pro úspěšné pochopení fungování IT světa, možnosti vytvoření a nastavení si vlastních pravidel, jakož i odhalování kybernetických útoků a trestné činnosti páchané prostřednictvím ICT.

### 1.3.1 Počítačová síť (Computer network)

Existuje celá řada definic pojmu počítačová síť, pro představu čtenáře některé z nich uvádím.

Jednu z možných definic počítačové sítě je možné nalézt ve Výkladovém slovníku kybernetické bezpečnosti, kde autoři uvádějí, že se jedná o *„soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.*“[114]

Další definici je možné nalézt v dnes již neplatné normě ČSN ISO/IEC 2382-1 která definovala počítačovou síť jako *„síť uzlů, které se při datové komunikaci propojují.*“[115]

*„Jedná se o množství vzájemně propojených počítačů, strojů, nebo operací.*“[116]

Počítačovou síť si je možné asi nejjednodušeji představit jakožto **soubor (množinu) počítačových systémů, které jsou navzájem propojeny a mezi nimiž dochází k výměně dat či informací**.

Počítačové sítě je možné dělit z celé řady hledisek. Uvedu tři možná dělení, která mají význam pro tuto publikaci:

114: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 73. Dostupný online: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

115: Viz Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník, Část 1: Základní termíny - s. 15.

116: Viz Oxford Dictionaries. *Network.* [online]. [cit. 4.5.2016]. Dostupné z: https://www.oxforddictionaries.com/definition/english/network

1) **Dělení dle rozlehlosti sítí.** Podle rozlehlosti, respektive rozsahu sítí se sítě rozdělují na čtyři základní skupiny, přičemž v současnosti jsou nejvýznamnější sítě uvedené pod písmeny b) a d):

   a) **PAN** (**Personal Area Network** – Osobní síť). Jedná se o malou privátní síť, která zpravidla slouží pro potřeby jednotlivce či domácnosti. V rámci této sítě dochází typicky k propojení jednotlivých počítačových systémů (mobilní telefon, PDA, laptop aj.) typicky za pomoci Bluetooth, IrDA, WiFi, ZigBee.[117]

      PAN sítě se v současnosti značně rozšiřují a zapojují do své struktury čím dál více zařízení. Příkladem fungování PAN sítě je komunikace jednotlivých technologií v domácnosti například s mobilním telefonem či počítačem, a to v rámci propojení těchto systémů do Internetu věcí (IoT) či Internetu všeho (IoE).[118]

   b) **LAN** (**Local Area Network** – Lokální počítačová síť). Typicky je tento pojem využíván pro označení lokální, či místní sítě, což je síť, v rámci které dochází k propojení uzlů[119] v rámci jedné či více budov. Nezáleží na způsobu propojení jednotlivých uzlů. Toto propojení může být realizováno metalickými, optickými či bezdrátovými sítěmi. Tato síť mívá typicky vyšší přenosovou rychlost a menší vzdálenost mezi jednotlivými uzly. Lokální sítí může být např. kompletní síť (subsítě) univerzity, organizace, ale zároveň se může jednat o malou síť, která je vybudována v rámci domácnosti (například jde o propojení více počítačových systémů: počítače, tiskárny, Smart TV, datové úložiště aj. přes switch či router).

   c) **MAN** (**Metropolitan Area Network** – Metropolitní síť). Jedná se o síť, která propojuje LAN sítě v městské zástavbě. Síť MAN spojuje jednotlivé uzly v řádech jednotek až desítek kilometrů. Někteří autoři řadí tuto síť do sítí WAN.

   d) **WAN** (**Wide Area Network** – Vzdálená počítačová síť). Pojem WAN označuje počítačovou síť propojující geograficky vzdálené oblasti. Typicky jsou do sítě WAN propojovány jednotlivé LAN a MAN sítě. Z geografického hlediska je možné definovat WAN sítě, jako sítě s rozsahem například v teritoriu státu, kontinentu i jako sítě celosvětové.

117: Jedná se o bezdrátovou komunikaci realizovanou na standardu IEEE 802.15.4.

118: Blíže viz kap. 3 Anonymita uživatele.

119: Pojem síťový uzel (node) označuje **zařízení v rámci počítačové sítě, které slouží k jejich vzájemnému propojování, nebo jako koncový bod**, kterým může být jakýkoli počítačový systém. **Každý uzel musí mít svoji MAC adresu** (blíže viz kap. 1.3.3 MAC Adresa).

2) **Dělení dle postavení síťových uzlů.**

a) **Peer-to-peer** (**P2P** – „rovný s rovným", či klient-klient) je počítačovou sítí, kde mezi sebou přímo komunikují jednotliví uživatelé, respektive jednotlivé počítačové systémy. Tento typ sítě nelze centrálně spravovat. Tyto sítě jsou například používány pro sdílení souborů, systémových prostředků aj.

b) **Klient-server** je typem sítě, kde je jeden či více počítačových systémů (server) nadřazen počítačovému systému či systémům (klient/klienti). Klient-server označuje vztah „nadřízenosti a podřízenosti" mezi dvěma počítačovými programy. Klient typicky žádá o služby server. Na modelu klient-server jsou založeny služby typu e-mail, web, přístup k databázi aj.

3) **Dělení dle vlastnictví sítí.**

a) **Privátní síť** je počítačovou sítí, která využívá privátní IP[120] adresy. Privátní adresy jsou používány v rámci sítě LAN (domácí, podnikové aj.). Pokud privátní síť potřebuje připojení k Internetu (přes přidělené veřejné IP adresy), musí používat překlad síťových adres (NAT), nebo proxy server. Privátní sítě se využívají zejména z důvodu nedostatečného množství veřejných IP adres ve verzi IPv4.

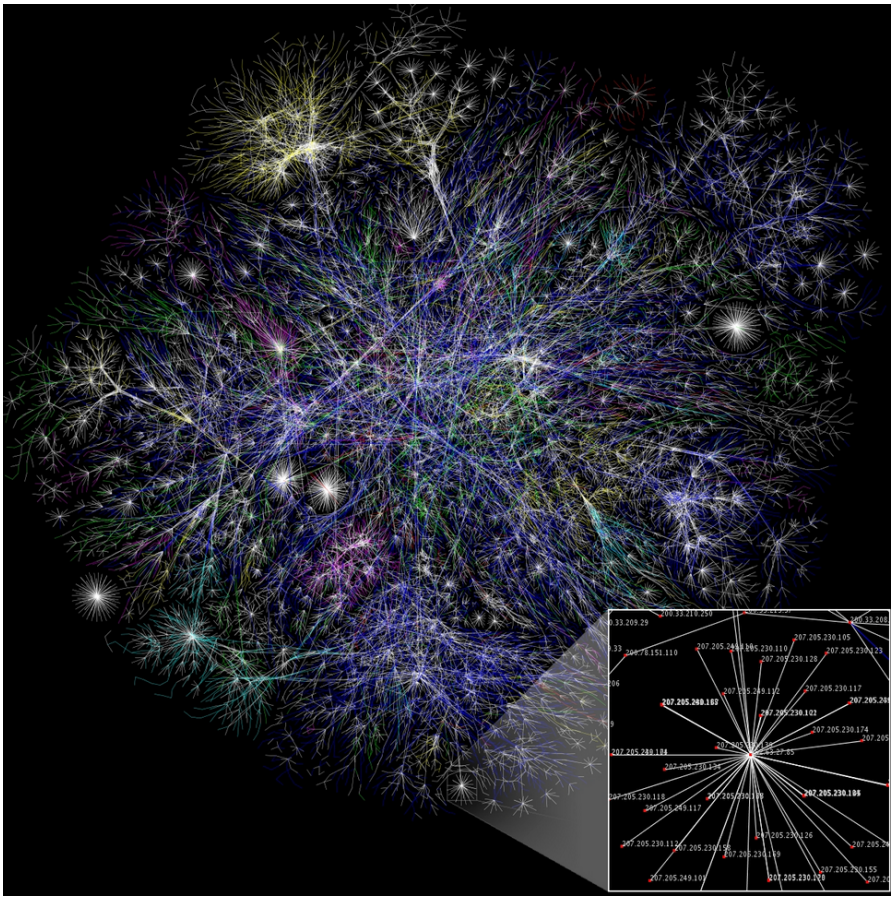
b) **Veřejná síť** je otevřena *„nejširší veřejnosti, které nabízí své služby spočívající v přenosu dat. Uživatelem takovéto sítě se skutečně může stát kdokoli, kdo o to má zájem a je ochoten za to zaplatit, resp. přistoupit na podmínky toho, kdo takovouto síť provozuje. Provozovatelem přitom bývá takový subjekt, který svou datovou sám nepoužívá – vlastní ji a provozuje především proto, aby její služby mohl poskytovat na komerční bázi jiným subjektům."*[121]

c) **Virtuální privátní síť** (**VPN** – Virtual Private Network). VPN je mechanismus (nebo metoda) umožňující propojení počítačových systémů prostřednictvím nedůvěryhodné (např. veřejné) počítačové sítě tak, že propojené počítačové systémy mezi sebou budou moci komunikovat, jako by byly propojeny v rámci důvěryhodné (uzavřené privátní) sítě. Tyto počítačové systémy ověřují svoji totožnost (např. pomocí certifikátů, hesla aj.) a po vzájemné autentizaci je komunikace mezi těmito privátně propojenými počítači šifrována.

Komplexní a globální počítačovou sítí pak je **Internet**, který je také označován jako **„Síť sítí". Technicky se jedná o decentralizovanou, celosvětovou distribuovanou počítačovou síť** složenou z jednotlivých menších sítí navzájem spojených pomocí protokolů TCP/IP.

120: Viz kap. 1.3.2 Internet Protocol a IP adresa.

121: PETERKA, Jiří. *Terminologie datových sítí.* [online]. [cit. 10.11.2015].
Dostupné z: http://www.earchiv.cz/b00/b0003002.php3



Obrázek 10: Jedno z možných grafických zobrazení Internetu[122]

## Protokoly počítačových sítí a Internetu podle modelu ISO/OSI

K tomu, aby bylo možno přenášet data mezi jednotlivými počítačovými systémy, byl definován model ISO/OSI jako referenční komunikační model. Tento model rozděluje komunikaci do sedmi vzájemně propojených vrstev. Tento model je zařazen do ISO/IEC 7498-1:1994 [v ČR: ČSN EN ISO/IEC 7498-1 (369614). Informační technologie – Propojení otevřených systémů – Základní referenční model – Základní model (ISO 7498-1:1994).].

122: Viz Wikipedia. *Internet map* [online]. [cit. 4.7.2016].
Dostupné z: https://upload.wikimedia.org/wikipedia/commons/d/d2/Internet_map_1024.jpg

Graficky je možné těchto sedm vrstev znázornit následovně:[123]

OSI (Open Source Interconnection) 7 Layer Model

| Layer | Application/Example | | Central Device/ Protocols | | DOD4 Model |
|---|---|---|---|---|---|
| **Application (7)** Serves as the window for users and application processes to access the network services. | **End User layer** Program that opens what was sent or creates what is to be sent<br>Resource sharing • Remote file access • Remote printer access • Directory services • Network management | | **User Applications**<br>SMTP | GATEWAY | Process |
| **Presentation (6)** Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network. | **Syntax layer** encrypt & decrypt (if needed)<br>Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation** | | JPEG/ASCII EBDIC/TIFF/GIF PICT | | |
| **Session (5)** Allows session establishment between processes running on different stations. | **Synch & send to ports** (logical ports)<br>Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc. | | **Logical Ports**<br>RPC/SQL/NFS NetBIOS names | | |
| **Transport (4)** Ensures that messages are delivered error-free, in sequence, and with no losses or duplications. | **TCP** Host to Host, Flow Control<br>Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing | PACKET FILTERING | TCP/SPX/UDP | | Host to Host |
| **Network (3)** Controls the operations of the subnet, deciding which physical path the data takes. | **Packets** ("letter", contains IP address)<br>Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting | | **Routers**<br>IP/IPX/ICMP | | Internet |
| **Data Link (2)** Provides error-free transfer of data frames from one node to another over the Physical layer. | **Frames** ("envelopes", contains MAC address)<br>[NIC card — Switch — NIC card] (end to end)<br>Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control | | **Switch Bridge WAP**<br>PPP/SLIP | Land Based Layers | Network |
| **Physical (1)** Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium. | **Physical structure** Cables, hubs, etc.<br>Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts | | **Hub** | | |

Can be used on all layers

123: Rozložení vrstev a funkcí je částečně převzato z *The OSI Model's Seven Layers Defined and Functions Explained*. [online]. [cit. 8.7.2016]. Dostupné z: https://sarvesict.blogspot.cz/2015/11/the-osi-models-seven-layers-defined-and.html. Původní tabulka je však doplněna o definice jednotlivých vrstev, které je možné nalézt na: http://site.the.cz/index.php?id=4. Další možná znázornění OSI modelu je možné nalézt např. na: *Network Layers*. [online]. [cit. 8.7.2016]. Dostupné z: http://www.comptechdoc.org/independent/networking/protocol/protlayers.html
*Network vulnerabilities and the OSI model*. [online]. [cit. 8.7.2016]. Dostupné z: http://cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model/

Další možné grafické znázornění v sobě zahrnuje i příklady aktivit v rámci jednotlivých vrstev, či využívané protokoly:[124]

| **OSI Model** | | | | |
|---|---|---|---|---|
| Data Unit (protokolová datová jednotka) | | Layer (Vrstva) | | Function (Funkce) |
| Host Layers | Data | 7 | Aplikační | Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev, a díky tomu je izolována od problémů síťových technických prostředků. Je softwarová. |
| | Data | 6 | Prezentační | Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována. Řeší například háčky a čárky, CRC, kompresi a dekompresi, šifrování dat. Je softwarová. |
| | Data | 5 | Relační | Koordinuje komunikace a udržuje relaci tak dlouho, dokud je potřebná. Dále zajišťuje zabezpečovací, přihlašovací a správní funkce. Je softwarová. |
| | Segments (Segmenty) | 4 | Transportní | Vlastní přenos dat. Definuje protokoly pro strukturované zprávy a zabezpečuje bezchybnost přenosu (provádí některé chybové kontroly). Řeší například rozdělení souboru na pakety a potvrzování. Je softwarová. |
| Network Layers | Packets (pakety) | 3 | Síťová | Definice protokolů pro směrování dat. Adresování a směrování dat v síti od zdroje k cíli. Definuje protokoly pro směrování dat, jejichž prostřednictvím je zajištěn přenos dat do požadovaného cílového uzlu. Je hardwarová, ale když směrování řeší PC s dvěma síťovými kartami je softwarová. |
| | Frames (rámce) | 2 | Linková | Zajišťuje integritu toku dat z jednoho uzlu sítě na druhý. V rámci této činnosti je prováděna synchronizace bloků dat a řízení jejich toku. Je hardwarová. |
| | Bits (bity) | 1 | Fyzická | Definuje prostředky pro komunikaci s přenosovým médiem a s technickými prostředky rozhraní. Dále definuje fyzické, elektrické, mechanické a funkční parametry týkající se fyzického propojení jednotlivých zařízení. Je hardwarová. |

124: *What is the OSI Model* [online]. [cit. 8.7.2016]. Dostupné z: http://blog.buildingautomationmonthly.com/what-is-the-osi-model/

Dalším síťovým modelem vytvořeným pro sítě internetového typu je **TCP/IP.**[125] Graficky by bylo možné TCP/IP model znázornit následovně:[126]

| TCP/IP | OSI |
|---|---|
| Aplikační | Aplikační |
| | Prezentační |
| | Relační |
| Transportní | Transportní |
| Síťová | Síťová |
| Vrstva síťového rozhraní | Linková |
| | Fyzická |

Technické vymezení sítě tak, jak bylo uvedeno výše, však právem běžně používáno není. Z hlediska práva, zejména trestního, je třeba na závěr kapitoly o počítačových sítích vymezit i pojem ***„veřejně přístupná počítačová síť"*** [viz § 117 písm. a) TZK].

Trestní zákoník v tomto ustanovení uvádí, že trestný čin je spáchán veřejně, pokud je spáchán *„obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí,* ***veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.***"

Šámal k tomuto pojmu uvádí, že se jedná o *„funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy (např. francouzský Minitel apod.). Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Z organizačního hlediska jde o provozovatele jednotlivých sítí a podsítí, zprostředkovatele připojení i uživatele a další subjekty."*[127]

K pojmu spáchání činu veřejně přístupnou počítačovou sítí se dále blíže vyjadřuje **Tpjn 300/2012** (stanovisko trestního kolegia Nejvyššího soudu České republiky z 30. 1. 2013) – Rt 20/2013:[128]

Toto kolegium *„obecně uznává, že za veřejně přístupnou počítačovou síť se v obecných rysech považuje funkční propojení do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především Internet a jiné podobné komunikační systémy. Internet je informační a komunikační systém, který má kromě jiného i povahu prostředku, jehož prostřednictvím lze veřejně šířit informace.*

125: Transmission Control Protocol/Internet Protocol

126: BOUŠKA, Petr. *OSI model.* [online]. [cit. 8.7.2016]. Dostupné z: http://www.samuraj-cz.com/clanek/osi-model/

127: ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář.* 2. vydání. Praha: C. H. Beck, 2012, s. 1300–1301

128: Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30.1.2013. [online]. [cit. 8. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?openDocument&Highlight=0

*Je tedy patrné, že internet je počítačovou sítí, která figuruje jako přenosové médium umožňující využívání určitých služeb, z nichž nejvýznamnější je přenos informací.*

*K tomu je možno dodat, že na základě výše uvedených skutečností je internet veřejně přístupnou sítí, neboť zaregistrovat se na něm a využívat jeho služby může obecně každý. Podmínka veřejně přístupné sítě je splněna bez dalšího v případě, pokud by komunikace byla vedena formou veřejně přístupných webových stránek, na kterých by např. byly závadné materiály vyvěšeny. K takovým stránkám, pokud nejsou zakódovány či opatřeny heslem, má přístup každý či může se stát uživatelem při splnění určitých podmínek. Webové stránky jsou tedy obecně přístupné blíže neurčenému a neomezenému okruhu uživatelů.“*

### 1.3.2 Internet Protocol a IP adresa

Internet Protocol (**IP**) zajišťuje vysílání **datagramů** na základě síťových IP adres uvedených v jejich hlavičce. Datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesílateli a pořadové číslo datagramu ve zprávě. Jednotlivé datagramy jedné zprávy putují sítí nezávisle na sobě, mohou putovat jinou cestou a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Vlastní doručení datagramu není zaručeno, spolehlivost přenosu datagramu musí zajistit vyšší vrstvy (TCP, aplikace aj.).

Podstatnou informací je, že pokud chce počítačový systém komunikovat v rámci jakékoli sítě, musí mít přidělenou **IP adresu**,[129] která je v rámci dané koncové sítě jedinečná. IP adresy mohou být přidělovány staticky (počítačovému systému je „napevno“ manuálně přidělena IP adresa) či dynamicky, kdy mu je (při každém připojení nového počítačového systému k počítačové síti) na základě MAC adresy přidělena automaticky IP adresa nová. IP adresa není standardně anonymní a počítačový systém ji využívá při komunikaci s jinými počítačovými systémy jakožto jeden z identifikátorů.

V současnosti existují dvě verze Internetového protokolu:

1) **Internet Protocol version 4 (IPv4)**. Jedná se o první, masově rozšířenou a v současnosti stále nejrozšířenější verzi Internet protokolu. IPv4 používá 32bitové adresy, které jsou zapsány dekadicky po jednotlivých oktetech (osmicích bitů). Veřejná adresa[130] v rámci IPv4 je tvořena čtveřicí čísel, vždy od sebe oddělených tečkou, přičemž hodnota každého z nich nepřesahuje **255**. IP adresa tedy může mít podobu například takovéhoto číselného řetězce:

129: Pro doručení jakéhokoliv objektu v libovolném systému musí být splněna podmínka možnosti jednoznačné adresace. Základním komunikačním protokolem Internetu je protokol **TCP/IP**. Základem adresovací struktury sady protokolů TCP/IP je **jedinečná adresa (číslo)**, která určuje jak konkrétní síť na Internetu, tak každý konkrétní počítačový systém v Internetu.

130: Blíže viz rozdělení IP adres v rámci působnosti RIR. Kap. 3.1.1 Digitální stopa neovlivnitelná.

195.113.149.160, či 64.233.168.99 apod. Číselný řetězec IP adresy: 302.233.8.158, či 64.233.168.299 v tomto provedení je nesmyslný a není se možné jeho prostřednictvím přihlásit do sítě Internet.

Protokol IPv4 poskytuje teoretický adresní prostor v rozsahu 232 (což je 4 294 967 296 adres). Prakticky je však využitelnost menší, protože kvůli přidělování adresových bloků je část adres nevyužitých.

Internet Engineering Task Force[131] rozhodla o zachování následujících rozsahů IPv4 adres pro privátní sítě:

| **Označení RFC 1918** | **Rozsah IPv4 adres** | **Počet adres** | **Největší CIDR blok (maska podsítě)** | **Pro síťové rozhraní** |
|---|---|---|---|---|
| 24bitový blok | 10.0.0.0–10.255.255.255 | 16 777 216 | 10.0.0.0/8 (255.0.0.0) | 24 bitů |
| 20bitový blok | 172.16.0.0–<br>172.31.255.255 | 1 048 576 | 172.16.0.0/12<br>(255.240.0.0) | 20 bitů |
| 16bitový blok | 192.168.0.0–<br>192.168.255.255 | 65 536 | 192.168.0.0/16<br>(255.255.0.0) | 16 bitů |

Z důvodu nedostatku veřejných IP adres ve verzi IPv4 došlo k zavedení protokolu IPv6. Tyto dva protokoly v této době fungují současně, avšak je předpokládáno postupné nahrazení protokolu IPv4.

2) **Internet Protocol version 6 (IPv6).** IPv6 je novým protokolem, který by měl vyřešit problémy související s nedostatkem veřejných IP adres. IP adresa verze 6 má délku 128 bitů, které jsou zapsány hexadecimálně (např. 2001:0:5ef5:79fd:386a:e7:4dee:fb51). U IPv6 je odstraněna potřeba použití překladu síťových adres. IPv6 obsahuje celkem 2 128 adres.

Adresní architekturu IPv6 definuje RFC4291. Adresní prostor je rozdělen následovně:

| **prefix** | **význam** |
|---|---|
| ::/128 | neurčená |
| ::1/128 | smyčka (loopback) |
| ff00::/8 | skupinové |
| fe80::/10 | individuální lokální linkové |
| ostatní | individuální globální |

131: https://www.ietf.org/

Protokol IPv6 zavádí tři typy adres:

- **Individuální (unicast)**, která identifikují právě jedno síťové rozhraní.
- **Skupinové (multicast)**, která označuje skupinu síťových rozhraní, jejímž členům se mají data dopravit. Skupinově adresovaný datagram se doručuje všem členům skupiny.
- **Výběrové (anycast)**, která označují také skupinu síťových rozhraní, data se však doručují jen jejímu nejbližšímu členovi.

Z pohledu práva je třeba uvést, že IP adresa je schopna více méně (viz užití NAT,[132] TOR aj.) jednoznačně identifikovat síťové rozhraní v počítačové síti, nikoliv ale přímo konkrétní osobu. IP adresa je schopna identifikovat počítačový systém „po celou dobu" jeho připojení k počítačové síti (skrze všechna jednotlivá připojení). *„V tomto ohledu lze hovořit o tom, že IP adresa sama o sobě představuje neperfektní identifikátor směřující pouze k místu připojení, případně k síti více počítačů či jednomu konkrétnímu počítači. Samotná IP adresa tak z principu neslouží k identifikaci konkrétní osoby, ale směřuje toliko k místu, kde je realizována nějaká činnost, přičemž není samo o sobě známo, zda jde o činnost strojovou (tj. počítače), nebo činnost konkrétní osoby."*[133] U předmětného počítačového systému mohla sedět osoba provádějící konkrétní aktivity, avšak mohla tam sedět i osoba jiná, nebo se mohlo jednat o vlastní (či naprogramovanou) činnost počítačového systému. Prokázání skutečnosti, kdo byl v daný okamžik uživatelem počítačového systému, je významné zejména pro trestní řízení.

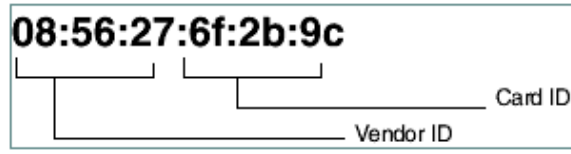
K otázce, zda je IP adresa osobním údajem, se vyjádřil i Nejvyšší správní soud, který v jednom ze svých rozsudků[134] (mimo jiné i s odvoláním na Soudní dvůr EU) uvedl: *„Při posuzování povahy IP adresy je možno podpůrně odkázat rovněž na judikaturu Soudního dvora EU. Ten ve svém rozhodnutí ze dne 29. 1. 2008, sp. zn. C-275/06, Productores de Música de Espana (Promusicae) vs. Telefónica de Espana SAU (rozhodnutí je dostupné z http://curia.europa.eu), považoval IP adresu v kontextu daného případu (Promusicae požadovala po Telefonice odhalení identit osob, kterým poskytovala připojení*

132: **Network Adress Translation** (překlad síťových adres). Dále jen NAT.
Blíže viz např. *NAT.* [online]. [cit. 16.6.2016]. Dostupné z: https://www.abclinuxu.cz/slovnik/nat
**NAT** *se používá k úspoře IP adres v současném Internetu. Většinou je realizován například na routeru připojujícím lokální síť k síti poskytovatele připojení. V lokální síti mohou pak být použity libovolné adresy (nejčastěji se jedná o adresy z neveřejného rozsahu).*
*Když počítač z lokální sítě odesílá paket do vnější sítě (např. Internetu), odešle jej se svou zdrojovou IP adresou a portem. Při průchodu NATem jsou však zdrojové IP adresy v paketech přepsány na veřejnou IP adresu NATu. Také je přepsáno číslo zdrojového portu na port, který NAT odesílajícímu počítači přidělil. NAT si zároveň uloží toto přidělení do své převodní tabulky (ve které jsou uloženy veškeré informace o vzájemném mapování jednotlivých adres).*
*Když pak následně dorazí odpověď od vzdáleného počítače, hlavičky paketů jsou znovu přepsány – tentokrát je cílová adresa a port přepsána příslušnými informacemi z převodní tabulky (lokální IP adresou a portem příslušného počítače) a paket je předán dál k doručení do lokální sítě.*
133: Blíže viz MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, s. 90
134: Rozhodnutí Nejvyššího správního soudu 1 As 90/2008, ze dne 4. 2. 2009. [online]. [cit. 8.7.2016]. Dostupné z: http://nssoud.cz/files/SOUDNI_VYKON/2008/0090_1As__0800189A_prevedeno.pdf

*k Internetu a u nichž byla známá jejich IP adresa a datum a čas připojení) za osobní údaj ve smyslu předpisů na ochranu osobních údajů. Pro účely nyní posuzované věci lze z uvedeného závěru vyvodit, že jestliže může IP adresa za určitých okolností představovat osobní údaj, tedy údaj, na jehož základě lze identifikovat (přímo či nepřímo) nějakou konkrétní osobu, pak může sloužit také jako důkaz v přestupkovém řízení, byť jako důkaz nepřímého charakteru.* "[135]

### 1.3.3 MAC Adresa

MAC adresa (Media Access Control) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové) vrstvy OSI. MAC adresa je přiřazována síťové kartě bezprostředně při její výrobě, proto je také někdy označována za fyzickou adresu. Přidělená MAC adresa je vždy celosvětově jedinečná (unikátní), avšak je ji možné podvrhnout.[136] MAC adresa je rozdělena na dvě poloviny, přičemž první z nich definuje výrobce síťové karty a druhá polovina je pak jedinečným identifikátorem karty, který jí přidělil výrobce (viz Obrázek 11[137]).




Obrázek 11: MAC adresa a její součásti

Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 08:56:27:6f:2b:9c). Mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami (např. 00-B0-D0-86-BB-F7).

MAC adresa se zobrazuje pouze k nejbližšímu síťovému zařízení (např. router u poskytovatele připojení k Internetu) a slouží tedy k identifikaci počítačových systémů pouze v jedné, značně omezené části počítačové sítě.

135: Blíže viz MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, s. 91

136: Blíže viz např.: https://cs.wikipedia.org/wiki/MAC_spoofing;
http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/;
http://www.gohacking.com/spoof-mac-address-on-android-phones/ aj.

137: *Addresses and Names* [online]. [cit. 9.7.2016]. Dostupné z:
http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_addresses

## 1.4 ISP (Internet Service Provider)

Na závěr kapitoly, která se věnuje vymezení některých pojmů bezprostředně se vztahujícím ke kyberkriminalitě, IT/ICT, kyberprostoru a aktivitám v něm uskutečňovaným, považuji za nezbytné vydefinovat pojem Internet Service Provider (ISP).[138] Internet Service Provider je nezbytnou součástí fungování světa informačních a komunikačních technologií, zejména pak Internetu a s ním spojenými službami. Internet Service Provider se svou vlastní činností bezprostředně podílí na jeho budování, obměně.

Internet Service Provideři poskytují jednotlivé služby v rámci Internetu. V nedávné minulosti se primárně jednalo o služby, které byly spojeny s poskytnutím internetového připojení, a zkratka ISP označovala pouze subjekty, které zajišťovaly koncovým uživatelům (fyzickým či právnickým osobám) „konektivitu".[139] V minulosti byla většina ISP zároveň telefonními společnostmi nebo si od nich fyzickou infrastrukturu pronajímali. **V současnosti však pojem ISP nezahrnuje pouze ty subjekty, které zajišťují fyzickou konektivitu, ale i subjekty, které poskytují další služby v prostředí Internetu.** V současnosti je možné konstatovat, že začínají převažovat ISP poskytující jiné služby než konektivitu (cloudová úložiště, e-mail, sociální sítě aj.) nad ISP, kteří poskytují konektivitu, byť ti první jsou na druhých závislí. **V České republice není v legislativě používán pojem ISP, ale pojem poskytovatel služby informační společnosti.**[140]

### Poskytovatel služby informační společnosti

Jedná se o subjekty, jejichž prostřednictvím mohou koncoví uživatelé vstupovat do počítačových sítí a využívat zde nabízené služby. ***Směrnice*** Evropského parlamentu a Rady č. ***98/34/ES*** o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice ***č. 98/48/ES*** **nedefinuje pojem poskytovatele** služeb informační společnosti, **ale pouze pojem** samotné **informační společnosti**.[141]

Pojem **služba informační společnosti** je vymezen v čl. 1 odst. 2 směrnice č. 98/34/ES následovně:

*„**službou**" je jakákoliv služba informační společnosti, to je každá služba zpravidla poskytovaná za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.*

138: Pro označení tohoto subjektu jsou užívány i jiné pojmy. Dle práva ČR půjde zejména o pojem: **poskytovatel služeb informační společnosti**, dále pak **ISP – Internet Service Provider**, někdy také **Information service provider**. V této knize budu pro obecné označení těchto subjektů používat pojem **ISP** či **Internet Service Provider**, případně pak specificky k českému právu pojem poskytovatel služeb informační společnosti.

139: Někdy je pro tyto poskytovatele využíván pojem **IAP – Internet Access Provider.**

140: Někdy také označován jako: „**information intermediary**" (což lze přeložit jako: informační zprostředkovatel).

141: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 46

**Pro účely této definice se rozumí:**

- ***„službou poskytovanou na dálku"*** *služba poskytovaná bez současné přítomnosti stran,*

- ***„službou poskytovanou elektronicky"*** *služba odeslaná z výchozího místa a přijatá v místě jejího určení pomocí elektronického zařízení pro zpracování a uchovávání dat (včetně digitální komprese) a jako celek odeslaná, přenesená nebo přijatá drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky;*

- ***„službou na individuální žádost příjemce služeb"*** *služba poskytovaná přenosem dat na individuální žádost.*

Příklady služeb, které nejsou zahrnuty do této definice, jsou uvedeny v příloze V. směrnice č. 98/34/ES.

Pojem ***„poskytovatel služeb"*** pak vymezila teprve ***směrnice č. 2000/31/ES*** o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu").

Tato směrnice definuje poskytovatele v čl. 1 odst. 2 takto:

- ***„poskytovatelem"*** *je každá fyzická nebo právnická osoba, která poskytuje určitou službu informační společnosti;*

- ***„usazeným poskytovatelem"*** *je poskytovatel, který účinně vykonává prostřednictvím stálého zařízení po neurčitou dobu hospodářskou činnost; existence a používání technických prostředků a technologií nezbytných k poskytování služby nevytváří samy o sobě usazení poskytovatele;*

- ***„příjemcem služby"*** *je každá fyzická nebo právnická osoba, která k profesním či jiným účelům využívá služeb informační společnosti, zejména pro vyhledávání či zpřístupňování informací;*

- ***„spotřebitelem"*** *je každá fyzická osoba, která jedná za účelem nespadajícím do její profesní či obchodní činnosti.*

Do českého práva byly tyto normy implementovány zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů.[142]

142: Dále jen **zákon o některých službách informační společnosti** či **ZSIS**.

Ustanovení § 2 tohoto zákona uvádí, že:

a) ***službou informační společnosti*** *je 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,*

b) ***elektronickou poštou*** *je textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne,*

c) ***elektronickými prostředky*** *jsou zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová telekomunikační zařízení a elektronická pošta,*

d) ***poskytovatelem služby*** *je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti,*

e) ***uživatelem*** *je každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací.*

Zákon o některých službách informační společnosti je, z pohledu českého práva, lex generali ve vztahu k některým jiným právním normám.[143] Tento zákon definuje tři základní skupiny poskytovatelů služeb informační společnosti (ISP). Autor českého zákona následoval **klasifikaci poskytovatelů služeb informační společnosti** tak, jak je provedena směrnicí č. 2000/31/ES. Dle této klasifikace se poskytovatelé dělí na:[144]

1) **Poskytovatele služeb spočívající v přenosu informací poskytnutých uživatelem (angl. Mere Conduit nebo Access Provider).** De facto se jedná o osobu (fyzickou, či právnickou), která je schopna poskytovat jiným osobám, či subjektům přístup k Internetu. Jde tedy **o ISP, kterého je možné označit jako „poskytovatele připojení"**. Jedná se o:

    - *Operátory elektronických komunikací,*
    - *ostatní operátory fyzických linek a*
    - *operátory logických linek.*

143: Zejména k zákonu č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Dále jen **zákon o elektronických komunikacích** či **ZoEK**.
Na druhou stranu je třeba konstatovat, že tento zákon je v některých ustanoveních i *lex specialis* (např. ve vztahu § 6 ZSIS a § 2901 OZ).
Srov. HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 141
144: Blíže: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 55

2) **Poskytovatele služeb spočívajících v automatickém mezi ukládání informací poskytnutých uživatelem (tzv. caching).**

3) **Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting).**

Poskytovatele uvedené pod body č. 2 a 3 je vzhledem, k povaze jimi poskytovaných služeb, možné označit jako **„poskytovatele služeb"**. V současnosti, zejména při poskytování komplexních služeb, je možné se setkat s poskytovatelem, který bude spadat do více skupin, či jej není mnohdy možné striktně podřadit pod určitou skupinu vymezenou tuzemskými i mezinárodními právními předpisy, neboť činnost ISP mnohdy přesahuje rámec té které skupiny. Pokud ISP spadá do více kategorií, je třeba vždy individuálně posuzovat každý konkrétní případ.

Uvedené členění do tří základních skupin je významné zejména z hlediska případné právní odpovědnosti. Podrobnější definice práv a povinností jednotlivých poskytovatelů služeb informační společnosti je uvedena v kap. 2.5 Odpovědnost poskytovatele služeb informační společnosti.

Pro názornost lze uvést i jiné členění poskytovatelů služeb informační společnosti, které uvádí ve své monografii Polčák (jeho výčet není úplný a ani autor sám si tento cíl nekladl). Autor dělí poskytovatele na:

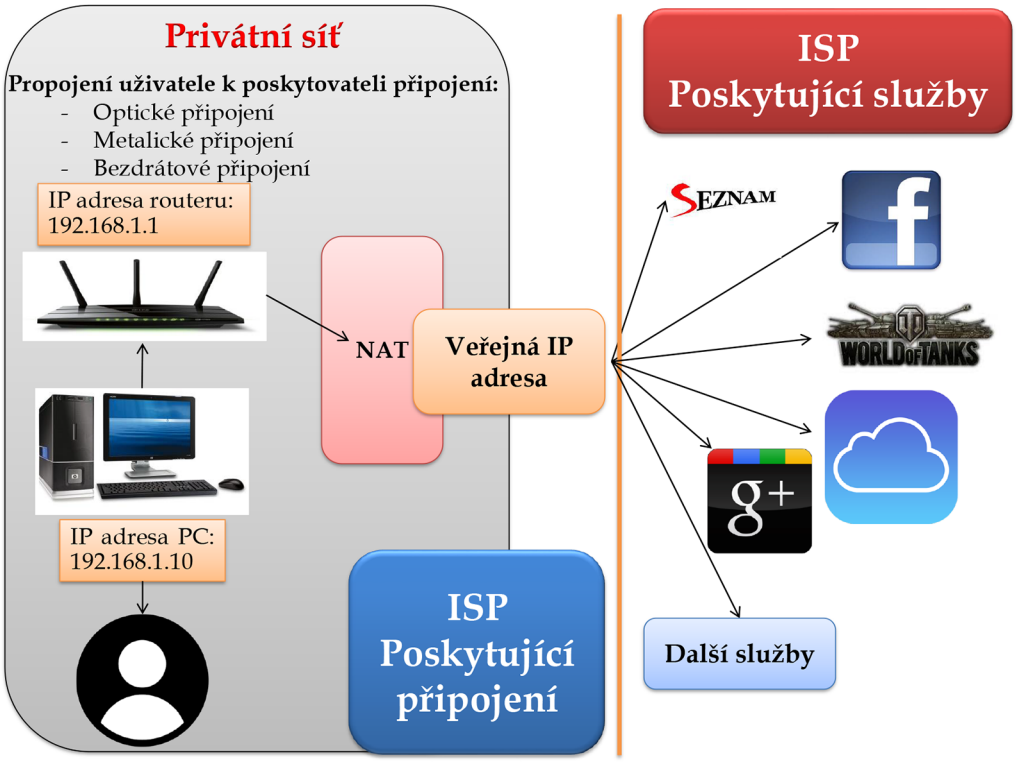
- *provozovatele síťové komunikační infrastruktury (fyzické, logické);*
- *provozovatele síťové asistenční infrastruktury;*
- *provozovatele hostingových služeb, služeb pro bloggery apod;*
- *provozovatele e-mailových služeb;*
- *vyhledávače, portály;*
- *diskusní servery, diskusní služby;*
- *zpravodajské servery;*
- *doménové autority.*[145]

Na závěr se pokusím o velmi zjednodušené grafické znázornění připojení koncového uživatele, za použití ICT, skrze jednotlivé ISP k službám poskytovaným v Internetu. Je třeba si uvědomit, že technické provedení částečně znázorněné na obrázku [privátní síť[146] (či podsítě), různé řídící prvky (switch, router), prvky zabezpečení sítě a jednotlivých počítačových systémů aj.] je možné nalézt jak na straně poskytovatele připojení, tak na straně poskytovatele služeb.

145: Blíže: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 49

146: Privátní síť je u ISP poskytujícího připojení znázorněna záměrně. V našem regionu (viz **RIR** kap. 3.1.1 Digitální stopa neovlivnitelná) jsou veřejné IPv4 adresy de facto vyčerpány. ISS jsou tedy nuceni vytvářet podsítě (subnets) v rámci přidělených veřejných IP adres. Subnet je možné vytvořit de facto v celém rozsahu IP adres přidělených pro privátní sítě (viz kap. 1.3.2 Internet Protocol a IP adresa). V rámci každé jedné privátní adresy je pak možné vytvořit další podsíť. Jednotlivé podsítě je pak možné hierarchicky spravovat.

Z pohledu práva je problematické, pouze za použití technických informací získaných z protokolu TCP/IP, jednoznačné a nezpochybnitelné určení koncového uživatele. K tomuto určení je však možné použít i jiné identifikátory uvedené například v kapitole 3 Anonymita uživatele.



# 2 Působnost práva v kyberprostoru

## 2 Působnost práva v kyberprostoru

Kyberprostor, je otevřený a snadno přístupný všem, ***„…neplatí zde žádné zvláštní zákony a je třeba se řídit obecně závaznými normami.“***[147]

Neoddiskutovatelnou skutečností je, že se do prostředí informačních sítí přesouvá realizace stále většího množství společenských, ale i ekonomických vztahů, a tím pádem vyvstává potřeba určité právní regulace takového jednání. Díky delokalizaci subjektů práva v různých zemích na celém světě je otázkou, jaký právní systém (jestli vůbec nějaký) se bude vztahovat na případné úkony (či protiprávní jednání) učiněné v Internetu.

**Je tedy třeba primárně řešit dvě otázky. Za prvé, zda platí právo na Internetu, a pokud ano, jaké právní normy se užijí. Za druhé, jakým způsobem je možné toto právo aplikovat, a to včetně případných sankcí či jiných opatření.** Jako příklad, na němž lze demonstrovat obtížnou aplikaci práva, může sloužit případ, kdy v roce 2005 v Číně jeden hráč online hry *„The Legend of Mir 3“* **zabil druhého hráče kvůli krádeži virtuální zbraně**. Mezi hráči této hry funguje nejen prodej virtuálních komodit, ale i systém půjček. Zejména se tak děje u hráčů, kteří se znají důvěrně, není však podmínkou, aby se znali z reálného světa. Právě půjčka byla příčinou uvedené vraždy. Hráč Qui Chengwei půjčil virtuální šavli - *„Dragon sabre“*, svému virtuálnímu příteli Zhu Caoyuanovi. Zhu ale podlehl vidině lehce vydělaných peněz a zbraň prodal za 7 200 junů (což je v přepočtu asi 19 000–20 000 Kč) na internetové aukci. Poté, co se Qui o prodeji dozvěděl, obrátil se na policii a nahlásil krádež virtuální šavle. Policie odmítla skutek řešit s tím, že na virtuální vlastnictví (de facto neexistující věci) se zákony nevztahují. Qui ztratil trpělivost a napadl Zhua u něj doma a ubodal ho k smrti.[148]

Je zřejmé, že se jedná o velmi extrémní případ, ale je na něm vhodně demonstrováno, že virtuální svět není od reálného světa odtržený, a proto je třeba řešit i otázku právní odpovědnosti v něm.[149] De facto od počátku rozvoje Internetu docházelo ke konfrontaci světa technického a právního. Technicky je Internet řešen logicky s jasnou hierarchií a strukturou. Právo, a zejména pak právo lokální, však často do této logičnosti vnášelo a vnáší „chaos“. Pojem „chaos“ asi nejvýstižněji vystihuje snahu legislativy o regulaci tohoto ryze technického světa, neboť v kyberprostoru má uživatel širokou řadu možností, jak určitý zákaz či restrikci „obejít“. Na následujících příkladech se pokusím demonstrovat ovlivňování světa reálného a virtuálního.

147: SMEJKAL, Vladimír. *Internet a §§§.* 2. aktualiz. a rozš. vyd. Praha: Grada, 2001, s. 32

148: Srov. HAINES, Lester. *Online gamer stabbed over „stolen“ cybersword.* [online]. [cit. 3.10.2006]. Dostupné z: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

149: Srov. Rozhodnutí Nejvyššího soudu 4 Tz 265/2000, ze dne 16.1.2001. [online]. [cit. 13.3.2008]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

**LICRA vs. Yahoo! Inc.**

Jeden z prvních případů vztahujících se k aplikovatelnosti práva v Internetu se stal v roce 2000 ve Francii. V únoru 2000 navštívil Marc Knobel (francouzský žid, který svůj život zasvětil boji s nacismem), aukční server www.yahoo.com a zjistil, že tento server nabízí na svých webových stránkách řadu předmětů s tematikou nacismu nebo předmětů vztahujících se k německým válečným silám z druhé světové války. Po tomto zjištění se Marc Knobel obrátil na Yahoo! Inc. s požadavkem na blokaci těchto stránek. Společnost Yahoo! Inc. však jeho požadavku nevyhověla. Marc Knobel prostřednictvím L.I.C.R.A. (Ligue Internationale Contre Le Racisme et l'Antisémitisme) podal, dne 11. dubna 2000, žalobu na Yahoo! Inc. u francouzského soudu za porušování francouzských zákonů, neboť ve Francii je zakázána propagace a podpora nacismu v televizi, v rozhlase i v psané podobě. Společnost Yahoo! Inc. se bránila tvrzením, že servery, na nichž je provozován aukční portál, jsou fyzicky umístěny v USA, a tak nelze připustit, aby se francouzské zákony uplatnily na hardware a weby provozované v Americe. Obhajoba dále namítala, že obsah webů je primárně určen pro americké rezidenty, jimž první dodatek Ústavy USA zaručuje svobodu projevu. Jakékoli snahy o odstranění těchto stránek by pak bylo v rozporu s tímto dodatkem.

LICRA však poukázala na skutečnost, že pokud firma Yahoo! Inc. podniká ve Francii, je nucena respektovat zákony Francie, přičemž Internet není výjimkou. Yahoo! Inc. na tento argument reagovalo tak, že není schopno určit, odkud se jejich zákazníci k aukčnímu portálu přihlašují. Pokud by tedy odstranili předmětné stránky, nejen že by nerespektovaly První dodatek Ústavy USA, ale znemožnili by přístup všem uživatelům, nehledě na hranice. Tím by se francouzské zákony staly de facto zákony celosvětovými. Dne 22. května 2000 byl soudcem Jean–Jacques Gomez vynesen rozsudek, který nařídil společnosti zablokovat pro francouzské uživatele přístup na americké aukční stránky s nacistickými pamětními předměty. Své rozhodnutí odůvodnil mimo jiné i tím, že Yahoo! Inc. dokáže identifikovat francouzské uživatele natolik dobře, že na jimi navštěvované stránky umí umístit reklamu ve francouzštině. Soudce dal společnosti Yahoo! Inc. 90 dní na to, aby nainstalovali na francouzské stránky Yahoo! Inc. filtrovací systém na bázi klíčových slov. *„Soudce Gomez v odůvodnění uvedl, že je možné zablokovat až devadesáti procentům francouzských uživatelů přístup na inkriminované internetové stránky. Technické řešení, s nímž má Yahoo! na základě rozsudku přijít, posoudí tříčlenný mezinárodní panel. Jeho dřívější nález uvádí, že je možné až sedmdesát procent uživatelů odblokovat podle označení jejich poskytovatele internetového připojení (ISP), dalších dvacet procent pak podle sledování klíčových slov zadávaných do hledače na stránkách Yahoo!.* “[150]

Právní zástupce Yahoo! Inc. Greg Wrenn uvedl: *„Kdykoli bude na stránce připomínající oběti holocaustu zmíněno slovo Hitler, bude stránka automaticky zavřena. Není možné vůbec mluvit o efektivním rozsudku, protože fakticky není možné jej naplnit.“*

Technické problémy v té době spočívaly, a částečně spočívají i dodnes, v tom, že filtrovat lze to,

150: ŠTOČEK, Milan. *V Hitlerově duchu proti Hitlerovi.* [online]. [cit. 10. 7. 2016]. Dostupné z: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

co se dá jasně definovat (např. slova jako Nazi, Heil Hitler aj.). Ale filtr není schopen odhalit všechny možné verze nežádoucího materiálu (např. N_A_Z_I, H3Il HiT_L3R aj.). Tyto rozdíly mohou poznat osoby fyzické (např. zaměstnanci konkrétního ISP), které pak stránku odstraní, nicméně provozovatel závadového fóra nebo aukce si může jednoduše změnit adresu a pokračovat ve své činnosti dál.

Společnost Yahoo! Inc. se vzdala odvolání proti rozsudku francouzského soudu a zahájila blokaci francouzských uživatelů na stránkách nabízejících závadný obsah. Společnost Yahoo! Inc. se však zároveň obrátila na místně příslušný okresní soud[151] v USA se žádostí o vynesení deklaratorního rozsudku, jež by působnost francouzského soudu nad americkou firmou vyloučil. Tento soud společnosti Yahoo! Inc. vyhověl v tom smyslu, že výkon francouzského rozhodnutí na území USA je protiústavní. LICRA proti tomuto rozsudku podala odvolání. Odvolací soud v USA reagoval odmítnutím své jurisdikce nad organizacemi LICRA. V roce 2006 se případ dostal před Nejvyšší soud v USA,[152] který se v závěru věcí odmítl zabývat. Rozsudky soudů v USA tak spíše vyzněly v prospěch společnosti Yahoo! Inc., ta se však nakonec sama dobrovolně rozhodla, že zcela odstraní stránky nabízejících předměty s nacistickou tématikou ze svých serverů, a to nejen ve Francii.

### Gutnick vs. Dow Jones

Joseph Gutnick (australský podnikatel s diamanty), si o sobě v roce 2000 přečetl v internetovém vydání novin Barron's[153] článek, který považoval za pomluvný. Gutnick podal žalobu pro pomluvu na vydavatelství Dow Jones u australského soudu. Dow Jones využilo obdobné argumenty, jako Yahoo! Inc. ve sporu s LICRA. Argumentace se primárně opírala o skutečnost, že tištěná verze novin je primárně určena pro trh v USA, tudíž se na případ nemohou australské zákony vztahovat.

Navzdory této argumentaci rozhodl australský soud[154] v roce 2002[155] následujícím způsobem: *„jelikož je materiál (článek) dostupný také v Austrálii, tedy v místě, kde je podnikatel Gutnick nejznámější, může jej pomluva nejvíce poškodit. Dow Jones je povinno zaplatit Gutnickovi odškodnění.“* Soud konstatoval, že se nebude zabývat tím, zda má či nemá Internet hranice a vzal v potaz především to, kde byl obsah dostupný, nikoli, kde byl zveřejněn. Soud také konstatoval, že každý má právo na právní ochranu před obdobným jednáním či dalšími útoky. Australský soud ve svém rozsudku také konstatoval realitu přeshraničního charakteru Internetu, kterému odpovídá extenzívní uplatňování jurisdikce.

151: United States District Court for the Northern District of California in San Jose

152: United States Supreme Court

153: http://online.barrons.com

154: High Court of Australia

155: Rozsudek [2002] HCA 56 z 10. prosince 2002, [online]. [cit. 24.3.2014]. Dostupné z: http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html

### GoDaddy

GoDaddy[156] je americký majoritní registrátor internetových domén. V roce 2016 spravuje více než 61 milionů internetových domén, což z GoDaddy činí největšího registrátora domén. Registrace domény u tohoto ISP je velmi jednoduchá a cenově dostupná. Zároveň je, díky lokaci společnosti (USA), uživatelům poskytována právní ochrana jejich osobních údajů a dat uvedených na doméně zaregistrované právě v rámci GoDaddy, pokud však uživatelé neporušují právo USA. Z tohoto důvodu jsou domény registrované u GoDaddy velmi často využívány například extremistickými, rasistickými[157] a jinými skupinami či uživateli. Tito uživatelé pak spoléhají na ústavní právo USA a První dodatek Ústavy USA:

*„Kongres nevydá žádný zákon, který by nerespektoval svobodu vyznání, nebo by obsahoval zákaz volného výkonu (bohoslužebných úkonů), nebo oklešťující svobodu slova nebo tisku nebo právo lidu pokojně se shromažďovat, a podávat petici vládě s cílem nápravy křivd.* "[158]

Problémem při řešení kybernetické trestné činnosti s výše uvedeným obsahem je pak prokázání reálnosti hrozby, či trestného činu tak, aby zároveň nešlo o porušení prvního dodatku Ústavy.

### Second Life (a „dětské" porno)

Second Life představuje 3D virtuální prostředí vyvíjené společností Linden Lab. Toto prostředí umožňuje vytváření vlastních avatarů, jejich vzájemné interakce, včetně možnosti generování zisku. Second Life je rozdělen do dvou virtuálních světů podle věku uživatele.[159] Uživatelé jsou schopni si měnit svoji totožnost a modifikovat si vzhled avatara dle svých představ. V roce 2007 upozornila německá stanice ARD a následně CNN na existenci „pedofilního ostrova."[160]

V této reportáži je poukazováno na skutečnost, že někteří uživatelé MainGrid (tedy uživatelé starší 18 let) si vytvořili avatary v podobě dítěte a jiní se vydávali za dospělé. V rámci vzájemné interakce pak docházelo ke zneužívání dětských avatarů avatary dospělými. Orgány činné v trestním řízení ve Spolkové republice Německo (SRN) zahájily vyšetřování, neboť podle německého trestního práva je držení virtuální dětské pornografie trestné.[161] Společnost Linden Lab poskytla německým orgánům součinnost při zjišťování identity uživatelů a majitelů virtuálních pozemků, na kterých se virtuální dětská pornografie uskutečňovala. Ve Spolkové republice Německo a Velké Británii bylo předmětné jednání možné postihnout prostředky trestního práva, ale v USA bylo takové jednání nepostižitelné.

156: https://uk.godaddy.com/

157: Typicky se jedná o trestné činy popsané v kap. 5.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě.

158: *First Amendment.* [online]. [cit. 10.7.2016]. Dostupné z:
https://www.law.cornell.edu/constitution/first_amendment. Překlad autora

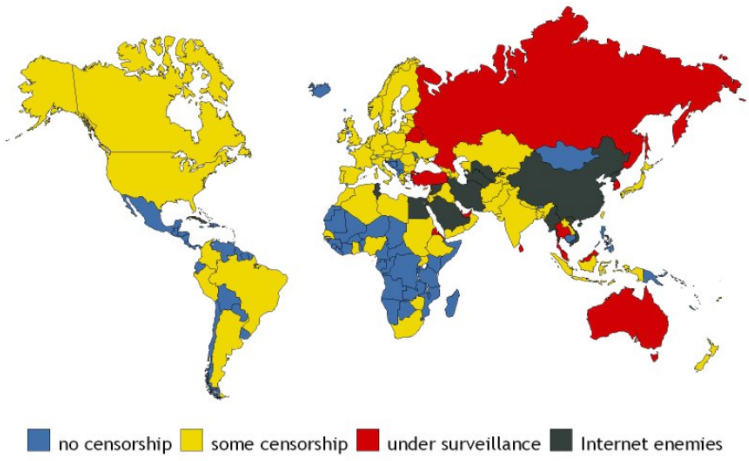
159: **MainGrid** - určený pro uživatele od dosažení věku 18 let; **TeenGrid** - určený pro věkovou skupinu v rozmezí od 13 do 18 let.

160: Blíže k uvedenému viz: *CNN on pedophile sex in Second Life.* [online]. [cit. 18.6.2009]. Dostupné z:
http://www.youtube.com/watch?v=AQM-SiiaipE

161: *Second Life 'child abuse' claim.* [online]. [cit. 16.6.2009]. Dostupné z:
http://news.bbc.co.uk/2/hi/technology/6638331.stm

V současnosti na světě neexistuje stát, který by se vzdal práva na potrestání protiprávního jednání, které zasahuje zájmy, jež chrání.

Mimo výše uvedené případy existuje celá řada dalších příkladů regulace Internetu a služeb na Internetu poskytovaných ze strany organizací nebo států. Tato regulace pak nutně přináší problémy s aplikovatelností a vynutitelností práva.




Obrázek 12: Rozdělení států dle cenzury Internetu

Ze zobrazené mapy (viz Obrázek 12)[162] vyplývá skutečnost, že většina zemí světa přijala právní nástroje, které ovlivňují Internet či poskytované služby.

Z hlediska uživatele je třeba konstatovat, že princip teritoriality v souvislosti s Internetem ztrácí smysl, protože se lze v kterémkoli okamžiku nacházet kdekoli na světě, aniž by uživatel musel vědět, kde je umístěn server, s nímž právě komunikuje. Z tohoto pohledu je Internet globální a nezná hranice.

„*Je sice pravda, že lze v každý konkrétní okamžik vystopovat fyzické umístění určité informace – příslušná lokace je však mnohdy nahodilá, velmi krátkodobá a pro informaci jako takovou a její právní efekt zpravidla naprosto irelevantní.*“[163]

162: *Internet censorship.* [online]. [cit. 10.8.2016]. Dostupné z: http://www.deliveringdata.com/2010_10_01_archive.html
163: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 7

Právo by mělo s virtuálním světem držet krok, bohužel ne vždy se to daří, neboť státy (uzavřené v pevných teritoriích) mnohdy postrádají prostředky, jak efektivně vynucovat právo v rámci kyberprostoru.[164] V podstatě existují dvě možnosti řešení totoho problému. Jednou z možností je respektovat principy teritoriality států tak, jak jsou nastaveny dnes. Tento přístup by pak de facto znamenal to, že pokud by někdo zasáhl do práv, jež se stát garantoval chránit, muselo by se počkat, než se útočník ocitne ve fyzické jurisdikci státu,[165] či by musel využít cesty mezinárodní právní pomoci.

Druhou možností pak je vytvoření speciální právní úpravy, tzv. internetové jurisdikce, která by se vztahovala na online svět. Otázkou je, jak by bylo toto nové právo přijato jednotlivými zeměmi. Osobně se domnívám, že za současných podmínek není možné celosvětově sjednotit všechna právní odvětví (občanské, obchodní, trestní, správní aj.), do nichž nějakým způsobem intervenuje Internet. Svoje tvrzení opírám mimo jiné i o skutečnost, že v roce 2001 byla přijata Úmluva o kyberkriminalitě, která definuje základní skupiny trestných činů, které by měly být v kyberprostoru stíhány, avšak k 1. 8. 2016 ji ratifikovalo pouze 49 zemí.

Jako problematické se, vzhledem ke globálnosti Internetu, dále jeví **určení**:

1) **rozhodného práva** (podle práva kterého státu se bude případný soudní spor rozhodovat),
2) **orgánu, který je oprávněn vydat rozhodnutí,**
3) **orgánu, který může rozhodnutí vymoci či přímo vykonat.**[166]

Vedle klasických právních norem se na tvorbě práva, respektive pravidel na Internetu, podílejí *definiční autority* tvorbou *definičních norem*.[167]

Na závěr uvádím příklad, kdy došlo k blokaci přístupu na web www.seznam.cz ze strany ISP působícího v Afghánské islámské republice. Důvodem bylo navštívení URL odkazu, v rámci něhož byly zobrazeny finalistky Miss ČR v plavkách. Země, která má problém se zajištěním základních

164: Srov. vyjádření v rámci **Deklarace nezávislosti kyberprostoru** („A Declaration of the Independence of Cyberspace"). Viz kap. 1.2.1 Kyberprostor (Cyberspace).
Srov. THOMAS, Douglas. *Criminality on the Electronic Frontier.* In Cybercrime. London: Routledge, 2003, s. 17 a násl.
Srov. JOHNSON, David R. a David POST. *The Rise of Law in Cyberspace.* [online]. [cit. 10.7.2016]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535

165: Příkladem tohoto přístupu může být případ, kdy uživatel např. z ČR bude v Internetu veřejně a opakovaně napadat ten který stát (např. pro nedodržování lidských práv v této zemi aj.), případně bude vyvíjet další činnost, která je v tomto státě protiprávní (avšak není protiprávní v ČR). Pokud se tento uživatel někdy v budoucnu rozhodne navštívit onu zemi, proti které takto vystupoval, může na něj být při překročení hranic tohoto státu uplatněno jeho teritoriální právo na základě některého z principů uvedených v kap. 2.2 Prostředky trestního práva.

166: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 7

167: Blíže viz kap. 2.5 Odpovědnost poskytovatele služeb informační společnosti.

potřeb pro svoje obyvatelstvo, je schopna celkem efektivně ovlivňovat to, na co se osoba v rámci jejího fyzického teritoria může na Internetu podívat.

Nejen po této zkušenosti se domnívám, že unifikace práva a jeho vynucování globálně, v rámci „internetové jurisdikce", by bylo značně problematické. Primární otázkou totiž zůstává, čí právo by bylo to, které by definovalo základní rámec práv a povinností v jednotlivých odvětvích.


Obrázek 13: Printscreen blokace stránky

## 2.1 Právní prostředí Internetu obecně

Internet nemá právní subjektivitu. Jde o informační a telekomunikační systém, který se skládá ze subjektů práva, tedy účastníků právních vztahů v podobě fyzických a právnických osob (jako jsou uživatelé, poskytovatelé veřejných či neveřejných služeb apod.). Internet jako celek nemá svého majitele. Internet není ani fyzickou, ani právnickou osobou. Vydefinování jednotlivých druhů ISP [viz kap. 1.4 ISP (Internet Service Provider)] má přímý vztah i k určení právní povahy Internetu a vymezení působnosti jednotlivých zainteresovaných osob.

Internet, jak již bylo uvedeno dříve, je tvořen jednotlivými menšími počítačovými sítěmi, které jsou navzájem propojeny. Tyto menší počítačové sítě jsou pak typicky vlastněny nějakou fyzickou či právnickou osobou (velmi často se jedná o ISP, ale vlastníkem může být i stát, či jakákoli jiná fyzická či právnická osoba) a tyto sítě je možné považovat za věc, dle § 489 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.[168]

Věcí se dle tohoto ustanovení rozumí *„vše, co je rozdílné od osoby a slouží potřebě lidí"*, přičemž věci se dle občanského zákoníku dále dělí na věci hmotné a nehmotné. **Za hmotnou věc je** pak dle § 496 odst. 1 OZ **považována** *„ovladatelná* ***část vnějšího světa, která má povahu samostatného předmětu.*** "Vybudovaná infrastruktura (např. v podobě počítačových sítí, datových center, serverů, jednotlivých řídících prvků aj.) je tedy věcí hmotnou, dle občanského zákoníku.

Z tohoto pohledu by pak bylo teoreticky možné konstatovat, že Internet je věcí, dle českého právního řádu. Problém však vyvstává ve vymezení již výše uvedeného vlastnictví věci (respektive možnosti nabytí věci). Dle mého názoru není možné si reálně představit, že by někdo (ať fyzická, či právnická osoba) vlastnil Internet jako takový. Vlastněny jsou pouze části (viz výše uvedené počítačové sítě) či služby, které jsou v rámci Internetu poskytovány. K této otázce se vyjadřuje i Smejkal: *„Věc v právním slova smyslu profiluje její ovladatelnost. Internet jako celek si nelze přivlastnit, ani jej ovládat.* "[169]

Ve vztahu k Internetu není možné ani plně využít ustanovení o věci nehmotné, dle § 496 odst. 1 OZ, podle kterého se věcí nehmotnou rozumí *„práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty.* " Tuto klauzuli není možné uplatnit, neboť Internet není právem a zároveň to ani není věc bez hmotné podstaty. **Internet, bez hmotné podstaty**, tedy informačních a komunikačních technologií a jednotlivých počítačových systémů, **nemůže existovat**. Internet je pevně svázán s hmotnou podstatou, tedy s hmotnou věcí, která je někým vlastněna. Vymezením Internetu, jakožto předmětu práva se opět dostáváme k výsostné pozici ISP a službám jimi poskytovanými.

Pokud chceme řešit otázku případné odpovědnosti za protiprávní jednání, je nezbytně nutné využívat nejen prostředků vnitrostátních (ať trestněprávních či občanskoprávních), ale i mezinárodních (viz Úmluva o kyberkriminalitě aj.). Proto se pokusím v další části této kapitoly obecně vymezit některé podmínky odpovědnosti, v závislosti na tom kterém právním odvětví, a na závěr se budu věnovat právní odpovědnost i poskytovatelů služeb informační společnosti a případné právní odpovědnosti uživatele.

168: Dále jen **občanský zákoník** či **OZ**.

169: SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 59–60

## 2.2 Prostředky trestního práva

### 2.2.1 Prostředky trestního práva hmotného

Trestní právo hmotné chrání zájmy společnosti, ústavní zřízení ČR, práva a oprávněné zájmy fyzických a právnických osob zejména tím, že stanoví podmínky trestní odpovědnosti, výčet trestných činů a sankce, které lze za trestné činy uložit (viz čl. 39 Listiny).[170]

V České republice je možné trestněprávně postihnout pouze takové jednání, které naplňuje znaky trestného činu uvedeného v trestním zákoně.

**Pokud jde o kyberkriminalitu, pak lze konstatovat, že trestněprávní postih útočníka, spáchajícího kybernetický útok, který nebude možné podřadit pod žádné ustanovení trestního zákona, nebude možný.** To však nevylučuje postih útočníka prostředky občanského či správního práva.

Pokud jde o vymahatelnost práva v oblasti veřejného práva (trestní, správní aj. právo), vystupuje zpravidla aktivně při vymáhání práva sám stát (respektive jeho orgány). Pokud jde o právo soukromé je zpravidla třeba, aby se na vymožení svého práva aktivně podílela osoba, která byla incidentem (protiprávním jednáním) dotčena.

Současný stav trestněprávní ochrany před kybernetickými útoky je v České republice dle mého názoru dostačující, avšak ne vždy jsou vhodným způsobem do právního řádu ČR transponovány mezinárodní právní normy či jejich části.[171] Zákonodárce se snaží změnami legislativy reagovat na stále sofistikovanější a nebezpečnější hrozby a útoky v rámci kyberprostoru, bohužel pomalejší reakce je mimo jiné zapříčiněna i složitějším procesem změny zákonů,[172] ve vztahu k novým druhům protiprávních jednání. Na druhou stranu útočníci jsou při snaze napadnout zvolený cíl schopni prokázat značně inovativní přístup, a to ve velmi krátkém časovém období.

#### Vymezení působnosti českého trestního práva hmotného

Působností práva se rozumí okruh společenských vztahů, na které se právo vztahuje, respektive uplatňuje. Obecně jsou teorií rozeznávány čtyři druhy působnosti trestních zákonů:

- **působnost časová** (trestnost činu se posuzuje dle zákona účinného v době spáchání trestného činu),
- **působnost osobní** (okruh pachatelů, na něž se trestní zákon vztahuje – viz exempce hmotně a procesněprávní),

170: NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010, s. 15

171: Blíže viz např. kap. 4.12 DoS, DDoS, DRDoS útoky a 5 Trestněprávní ochrana před kyberkriminalitou.

172: viz *Legislativní proces z hlediska Poslanecké sněmovny.* [online]. [cit. 18. 8. 2009]. Dostupné z: http://www.pravnik.cz/a/94/legislativni-proces-z-hlediska-poslanecke-snemovny.html

- **působnost místní** (užití trestního zákona ve vztahu k místu, kde byl trestný činy spáchán), a
- **působnost věcná** (definuje okruh společenských vztahů, na které se zákon vztahuje).

Pokud jde o problematiku kybernetických útoků (či trestných činů), pak **nejproblematičtější je určení místa, kde k útoku či trestnému činu došlo**.

Pokud chceme řešit otázku: *„Kde byl trestný čin spáchán?"*, je třeba využít institutů uvedených v trestním zákoníku, neboť Česká republika se zavazuje stíhat trestné činy i tehdy, pokud se pachatel nacházel mimo území ČR. U kyberkriminality dojde především k využití **zásad teritoriality** (§ 4 TZK), **registrace** (§ 5 TZK), **personality** (§ 6 TZK), **ochrany a univerzality** (§ 7 TZK) a **subsidiární zásady univerzality** (§ 8 TZK).

Velmi zjednodušeně je možné pomocí následující tabulky vymezit okruh trestných činů, kterými se budou zabývat české orgány činné v trestním řízení.

| | Místo činu | Pachatelé | Trestné činy | Další podmínky |
|---|---|---|---|---|
| **Zásada teritoriality** (§ 4 odst. 1 TZK) | Trestný čin byl zcela spáchán v ČR. Trestný čin byl z části spáchán v ČR.* | Všechny osoby bez omezení. | Veškeré trestné činy uvedené v TZK | - |
| **Zásada registrace** (§ 5 TZK) | Čin byl spáchán mimo území České republiky na palubě lodi nebo jiného plavidla, anebo letadla nebo jiného vzdušného dopravního prostředku, které jsou registrovány v České republice. | Všechny osoby bez omezení. | Veškeré trestné činy uvedené v TZK | - |
| **Zásada personality – aktivní princip** (§ 6 TZK) | V cizině | Občan ČR** | Veškeré trestné činy uvedené v TZK | - |
| **Zásada ochrany a zásada universality** (§ 7 odst. 1TZK) | V cizině | Cizinec*** | Trestné činy vyjmenované v § 7 odst. 1 TZK | - |
| **Zásada personality – pasivní princip** (§ 7 odst. 2 TZK) | V cizině | Cizinec | Trestné činy, u nichž platí oboustranná trestnost, nebo místo spáchání činu nepodléhá žádné trestní pravomoci. | Proti občanu ČR nebo proti osobě bez státní příslušnosti, která má na území České republiky povolen trvalý pobyt. |
| **Subsidiární zásada univerzality** (§ 8 TZK) | V cizině | Cizinec | - | *a)* čin je trestný i podle zákona účinného na území, kde byl spáchán, *b)* pachatel byl dopaden na území České republiky, proběhlo vydávací nebo předávací řízení a pachatel nebyl vydán nebo předán k trestnímu stíhání nebo výkonu trestu cizímu státu nebo jinému oprávněnému subjektu a *c)* cizí stát nebo jiný oprávněný subjekt, který žádal o vydání nebo předání pachatele k trestnímu stíhání nebo výkonu trestu, požádal o provedení trestního stíhání pachatele v České republice. |

* Dle § 4 TZK je trestný čin spáchán na území ČR i tehdy, pokud se pachatel dopustil na území ČR části jednání, i když porušení nebo ohrožení zájmu chráněného trestním zákonem nastalo nebo mělo nastat zcela nebo zčásti v cizině, nebo na tomto území nastala část následku, i když se jednání dopustil v cizině. Stejně tak je spáchán čin na území ČR, pokud zde zčásti jednal účastník činu spáchaného v cizině.

** Vedle občana ČR se zásada personality vztahuje i osobu bez státní příslušnosti, která má na jejím území povolen trvalý pobyt.

*** Pojmem cizinec se dle trestního zákoníku rozumí: *„Cizí státní příslušník nebo osoba bez státní příslušnosti, která nemá na území České republiky povolen trvalý pobyt.“*

U trestné činnosti páchané v kyberprostoru pak bude pro posouzení otázky, zda stíhat či nestíhat trestný čin, zpravidla rozhodujícím místem to **místo, kde buď nastal následek trestného činu, nebo kde došlo k jednání** (ať již zcela, nebo z části). V prostředí kyberprostoru se velmi často jednání pachatele odehraje na území jiného státu, než na kterém nastal právě účinek, nebo naopak. V praxi je pak možné se setkat se situací, kdy je jeden trestný čin současně stíhán na území více států. V současné době je stále více využívána mezinárodní justiční spolupráce[173] při řešení kyberkriminality, zejména cestou spolupráce přes Interpol či Europol.

Jako příklad uvedené spolupráce je možné uvést útok skupiny hackerů, kterým se podařilo odcizit dosud neuveřejněné filmy z produkce hollywoodských studií. Po získání těchto filmů došlo k jejich zpřístupňování na Internetu. Tito pachatelé působili (jejich jednání bylo provedeno) z různých zemí světa, avšak server nabízející inkriminované filmy do prostředí Internetu skrze P2P síť byl fyzicky umístěn na území České republiky, tudíž zde docházelo k porušování práv autorských. Řízení proti pachatelům bylo zahájeno jak úřadem FBI, tak i Policií ČR. Mezi jednotlivými institucemi docházelo pravidelně k výměně informací týkajících se vyšetřovaného případu.

### 2.2.2 Prostředky trestního práva procesního

„*Předmětem trestního práva procesního je úprava právních vztahů mezi orgány činnými v trestním řízení navzájem a mezi těmito orgány a jinými osobami zúčastněnými na trestním řízení, při zjišťování, zda byl spáchán trestný čin a kdo je jeho pachatelem, při rozhodování o nich a při výkonu těchto rozhodnutí i objasnění příčin trestné činnosti a úprava jejich práv a povinností.*“[174]

Zejména v trestním právu procesním je třeba akceptovat základní zásady vyplývající z Ústavy ČR a Listiny základních práv a svobod (zejména čl. 37, 39 a 40). K nejdůležitějším z těchto zásad patří zásada *presumpce neviny* a zásada *in dubio pro reo* (tedy v pochybnostech ve prospěch obžalovaného). Právě tato poslední zásada má pro dokazování kybernetických trestných činů největší význam.

Úkolem orgánů činných v trestním řízení je zajistit takové množství důkazního materiálu, aby mohl být obžalovaný *nad veškerou pochybnost* usvědčen a tedy shledán vinným a odsouzen.[175] Bohužel ve virtuálním světě je právě tento požadavek klíčovým problémem dokazování počíta-

173: Blíže viz zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních.

174: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015, s. 29

175: Tímto však není popřena ***zásada oficiality*** (respektive ***zásada vyhledávací***, která konkretizuje právě zásadu oficiality), kdy jsou orgány činné v trestním řízení povinny zjišťovat závažné skutečnosti, svědčí v neprospěch či ve prospěch obviněného z úřední povinnosti.
Srov. FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 96 a násl.

čového zločinu. Orgány činné v trestním řízení musí vždy porušení zákona dokázat konkrétní osobě. Ve světě počítačů se ovšem setkávají s dříve nevídanými problémy.[176] Tyto problémy jsou pak typicky zapříčiněny vlastním fungováním virtuálního světa a způsobem, jakým dochází k připojení uživatele do kyberprostoru a k jednotlivým službám. Kyberprostor umožňuje uživateli aktivně maskovat či zastírat svoji identitu (respektive identitu počítačového systému), ať již díky využití např. TOR network, VPN, NAT či jiným službám. Samotným problémem trestního práva procesního pak je nezpochybnitelné určení osoby, která v době páchání trestného činu využívala daný počítačový systém.

Nicméně i v této oblasti existuje celá řada způsobů, jak přímo či nepřímo identifikovat jak vlastní počítačový systém, tak konkrétního uživatele.[177]

## 2.3 Prostředky správního práva

Vedle trestního práva považuji za nutné zmínit i některé prostředky práva správního, které umožňuje postih protiprávního jednání, jež má povahu přestupku i v prostředí virtuálním. Základní právní normou, která upravuje přestupky, je zákon č. 200/1990 Sb., o přestupcích,[178] jež v § 2 definuje pojem přestupku. Dle tohoto ustanovení je přestupkem *„zaviněné jednání, které porušuje nebo ohrožuje zájem společnosti a je za přestupek výslovně označeno v tomto nebo jiném zákoně, nejde-li o jiný správní delikt postižitelný podle zvláštních právních předpisů anebo o trestný čin.*" Pokud jde o zavinění, pak zákon stanoví, že k trestnosti přestupku postačí zavinění z nedbalosti, pokud zákon výslovně nestanoví, že je třeba zavinění úmyslného.

Z přestupkového zákona záměrně vyjímám následující dvě ustanovení, týkající se ochrany práv autorských a ochrany práv na ochranu osobnosti, která mají dle mého názoru přímý vztah k protiprávním jednáním v prostředí Internetu.

Mnoho uživatelů si neuvědomuje, že se svým jednáním mohou dopustit některého z níže popsaných jednání. Na druhou stranu je třeba přiznat, že pokud by státní orgány měly řešit veškeré přestupky, které by ve virtuálním prostředí naplnily například skutkovou podstatu dle § 49 odst. 1 písm. a) či odst. 3 písm. b)[179] ZoP, pak by zřejmě nebyly schopny řešit přestupky jiné.

176: MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 83

177: Blíže viz kap. 3 Anonymita uživatele; 6 Trestněprocesní a kriminalistické aspekty odhalování, prověřování a vyšetřování kyberkriminality.

178: Dále jen **zákon o přestupcích** či **ZoP**.

179: Jako příklad je možné uvést příklady hanlivých, rasistických, xenofobních, sexuálně orientovaných, urážlivých výroků v rámci blogů, diskusních fór či v rámci sociálních sítí samotných.

**§ 33**
**Přestupky na úseku porušování průmyslových práv a porušování práv k obchodní firmě**

(1) Přestupku se dopustí ten, kdo
a) **neoprávněně vykonával práva, která jsou zákony na ochranu průmyslového vlastnictví vyhrazena majitelům těchto práv**,
b) neoprávněně užíval obchodní firmu nebo jakékoliv značení zaměnitelné s obchodní firmou nebo označením příznačným pro jiného podnikatele.
(2) Za přestupky podle odstavce 1 lze uložit pokutu do 15 000 Kč.

**§ 49**
**Přestupky proti občanskému soužití**

(1) Přestupku se dopustí ten, kdo
a) **jinému ublíží na cti tím, že ho urazí nebo vydá v posměch**,
b) jinému ublíží na zdraví.
(2) Přestupku se dopustí ten, kdo úmyslně naruší občanské soužití tím, že
a) jinému vyhrožuje újmou na zdraví,
b) jiného nepravdivě obviní z přestupku,
c) se vůči jinému dopustí schválnosti, nebo
d) se vůči jinému dopustí jiného hrubého jednání.
(3) Přestupku se dále dopustí ten, kdo
a) omezuje nebo znemožňuje příslušníku národnostní menšiny výkon práv příslušníků národnostních menšin, nebo
b) **způsobí jinému újmu pro jeho příslušnost k národnostní menšině nebo pro jeho etnický původ, pro jeho rasu, barvu pleti, pohlaví, sexuální orientaci, jazyk, víru nebo náboženství, věk, zdravotní postižení, pro jeho politické nebo jiné smýšlení, členství nebo činnost v politických stranách nebo politických hnutích, odborových organizacích nebo jiných sdruženích, pro jeho sociální původ, majetek, rod, zdravotní stav anebo pro jeho stav rodinný.**
(4) Za přestupek podle odstavců 1 až 3 lze uložit pokutu do 20000 Kč.
(5) Je-li přestupek podle odstavců 1 až 3 spáchán opakovaně (§ 91a) po nabytí právní moci rozhodnutí o přestupku podle stejného odstavce, uloží se pokuta do 30000 Kč. Za přestupek podle odstavce 2 lze spolu s pokutou uložit zákaz pobytu.

## 2.4 Prostředky občanského práva

Vedle uplatnění norem veřejného práva lze vůči uživatelům (fyzickým či právnickým osobám) uplatnit normy soukromoprávní,[180] zejména pak občanský zákoník. Tato komplexní právní norma práva soukromého obsahuje celou řadu ustanovení, jež je možné aplikovat jak ve světě reálném, tak ve světě virtuálním. Pro účely této monografie jsem se pokusil vybrat ta ustanovení, která jsou z mého pohledu nejvýznamnější.

### 2.4.1 Ochrana soukromí

Na prvním místě se chci věnovat ochraně fyzické osoby, konkrétně ochraně podoby a soukromí jedince. Soukromí je jedním ze základních lidských práv, zakotvených ve Všeobecné deklaraci lidských práv z roku 1948.[181] Do českého právního řádu byla tato ustanovení transponována zejména v rámci článků 7, 10, 13 Listiny.[182]

Ustanovení § 84 OZ stanoví, že *„**zachytit** jakýmkoli způsobem **podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.**“* Občanský zákoník dále zakazuje zasahovat do soukromí jiného, bez zákonného důvodu. Demonstrativně pak v § 86 vyjmenovává jednání, která jsou zakázána. Jedná se například o sledování soukromého života jiného, a to včetně pořizování zvukového nebo obrazového záznamu této osoby. Dále je zakázáno využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu chrání občanský zákoník i **soukromé písemnosti osobní povahy**.

---

180: V soukromoprávní oblasti srov. např. nařízení Evropského parlamentu a rady **(ES) č. 593/2008 – Řím I**.

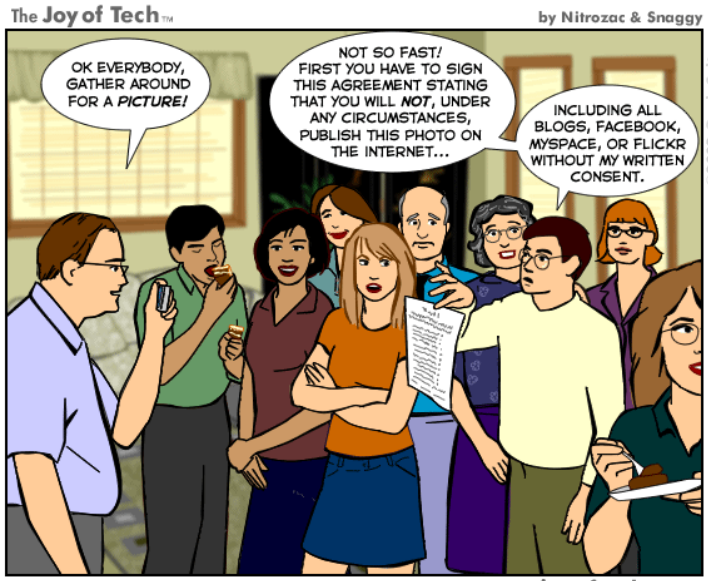
181: Dostupné online: http://www.osn.cz/wp-content/uploads/2015/03/vseobecna-deklarace-lidskych-prav.pdf
Ve všeobecné deklaraci lidských práv jsou tato práva primárně zakotvena v článcích 12 a 18.
Čl. 12: *„**Nikdo nesmí být vystaven svévolnému zasahování do soukromého života**, do rodiny, domova **nebo korespondence**, ani útokům na svou čest a pověst. **Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.**“*
Čl. 18: *„Každý má právo na svobodu myšlení, svědomí a náboženství; toto právo zahrnuje v sobě i volnost změnit své náboženství nebo víru, jakož i svobodu projevovat své náboženství nebo víru, sám nebo společně s jinými, ať veřejně nebo soukromě, vyučováním, prováděním náboženských úkonů, bohoslužbou a zachovávání obřadů.“*

182: Čl. 7 odst. 1 Listiny: ***„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“***
Čl. 10 odst. 2 a 3 Listiny:
*„**Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.**“*
*„Každý má právo na **ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.**“*
Čl. 13 Listiny: *„Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.“*

Svolení k zásahu do výše uvedených práv pak není třeba, jestliže se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob, nebo se pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.[183] **Svolení také není třeba, pokud je podobizna nebo zvukový či obrazový záznam pořízen k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.**[184]

Mnoho uživatelů kyberprostoru si neuvědomuje, že se například vytvářením, umisťováním a další distribucí fotografií, na kterých je zachycena jiná osoba, která k tomu nedala souhlas, může dopustit jednání, jež porušuje právě výše uvedená ustanovení občanského zákoníku.

Plné respektování občanského zákoníku by pak do reálného života mohlo vnést řadu situací, které by de facto znemožnily, za plného respektování práva občanského, fungování řady služeb v Internetu (např. sociálních sítí, které jsou postaveny primárně na sdílení informací mezi uživateli). Dle platného občanského práva si lze představit situaci, kdy si od osob budete vyžadovat souhlas s pořízením fotografie (i když zde by bylo možné aplikovat skutečnost, že se dobrovolně podíleli na pořízení fotografie, tedy s touto skutečností souhlasili) a zejména pak souhlas s její distribucí a zveřejněním.



185

183: Viz § 88 OZ

184: Viz § 89 OZ

185: [online]. [cit. 20.10.2013]. Dostupné z: http://www.geekculture.com/joyoftech/joyarchives/1078.html

### 2.4.2 Věci a virtuální majetek

Rozdělením věcí z pohledu práva občanského jsem se zabýval v kap. 2.1 Právní prostředí Internetu obecně, která je věnována definici Internetu, jakožto objektu práva. Nicméně problematika věcí, vlastnických práv a virtuálního majetku je v prostředí ICT natolik významná, že považuji za nutné se jí věnovat o něco podrobněji.

Jak jsem již uvedl dříve, občanský zákoník v § 489 OZ stanoví, že **věcí je vše, co je rozdílné od osoby** (fyzické či právnické) **a co slouží potřebě lidí**. Věcí dle tohoto ustanovení je tedy jak hardware (v podobě počítačových systémů, sítí aj.), tak software. Zároveň **je věcí** i například **ovladatelná přírodní síla** (§ 497 OZ, např. elektrická energie aj.), či **cokoliv, co může sloužit k uspokojování potřeb člověka**. **Z okruhu věcí jsou pak vyloučena zvířata** (§ 494 OZ), **lidské tělo a jeho části** (§ 494 OZ) **a skutečnosti mimo dosah lidské moci** (např. sluneční světlo, vítr, déšť aj.), byť se jedná o elementy, které mohou sloužit k uspokojování potřeb člověka, avšak člověk je není schopen ovládat, tedy učinit předmětem svého vlastnictví. Posledním kritériem definujícím věc je **existence této věci ve vnějším světě**.

Toto kritérium od sebe odlišuje věci samostatné (např. postel, vrtačka aj.) a součásti věci. Součástí věci se dle § 505 OZ rozumí vše, *„co k ní podle její povahy náleží a co nemůže být od věci odděleno, aniž se tím věc znehodnotí.*" Lavický vysvětluje, že *„součást věci nemá samostatnou funkci, a nemůže být proto samostatným předmětem práv. Začleněním do celku součást ztrácí svou individualitu (volant, kolo osobního automobilu, harddisk počítače, rypadlo jeřábu) a získává individualitu celku (věci složité).*"[186]

Občanský zákoník (§ 496 OZ) dále dělí věci na věci hmotné (*res corporales*) a věci nehmotné (*res incorporales*), přičemž hmotnou věcí je ovladatelná část vnějšího světa, jež má povahu samostatného předmětu a věcí nehmotnou jsou práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty. *„Za nehmotné věci se považují statky, které existují jen právně (in iure consistunt), např. majetková práva z obligací, typicky pohledávky nebo služebnosti.*"[187] Z definice obsažené v občanském zákoníku vyplývá, že věcí jsou práva a povinnosti, jejichž povaha to připouští. Typicky se bude jednat o práva majetková (všechna majetková práva, s nimiž lze nakládat, pohledávky, služebnosti, případně i vlastnické právo), předměty majetkových práv k duševnímu vlastnictví (know-how, označení tvořící ochrannou známku, obchodní firma, doména či doménové jméno aj.), nehmotné statky (patenty, ochranné známky aj.), spoluvlastnický podíl, osobní námaha, práce, pohledávky aj.

186: LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář.* Praha: C. H. Beck, 2014. s. 1790

187: ELIÁŠ, Karel. *Věc, jako pojem soukromého práva.* [online]. [cit. 6.6.2016]. Dostupné z: http://www.pavelpetr.cz/soubory/29/87/Karel_Elias_Vec_jako_pojem_soukromeho_prava.pdf

*„Dříve jsme si mysleli, když to zjednodušším, že s předmětem se dá obchodovat, jen když ho nacpeme do krabice a pošleme. To už dnes není pravda. Stále větší počet věcí a služeb můžeme poslat přes hranice států. Jsou to elektrony, co se pohybuje, ne krabice.*“[188]

Ve vztahu k ICT tedy nehmotnou věcí může být například právo užívat autorské dílo [např. píseň, či film, program (za stanovených podmínek), aniž bych si jej musel kupovat ve fyzické podobě. Doručen je uživateli čistě obsah.], herní či jiné virtuální účty, avatarové, stejně jako nehmotný virtuální majetek, získaný např. během hry, za podmínky, že tento majetek není možné považovat za finance (respektive platidlo převoditelné na některou z měn reálných či virtuálních kryptoměn).

Za **virtuální majetek je** možné označit **majetek v digitální podobě**. Může se jednat o data či informace, které si uživatel sám vytvořil, uložil (soubory, databáze, poznámky, e-maily aj.), získal (programy, aplikace aj.) apod., nebo může jít i o věc pocházející z virtuální hry, či jiného programu, aplikace.

Virtuální majetek není možné považovat pouze za součást věci, neboť byť je a vždy bude vázán na nějakou fyzickou materií (např. harddisk či jiné paměťové medium), tak na této materii nemusí být zcela závislý, neboť může být přesunut na jiné médium, nebo je například duplikovaně ukládán v rámci poskytované služby či hry na datových nosičích ISP (nejčastěji cloudových úložištích).

V současné době se stéle více objevuje virtuální majetek, jakožto věc pocházející z počítačové hry či jiné aplikace. Byť to pro řadu lidí může znít absurdně, tyto předměty, případně hráčské účty[189] nejsou bezvýznamné a neužitečné (užitečnost věci je občanským zákoníkem definována jako schopnost uspokojovat potřeby člověka). Hry, ať reálné či virtuální, pak uspokojují celou řadu potřeb. Minimálně se jedná o potřebu odpočinku, relaxace. U virtuálních věcí je třeba počítat s jejich hodnotou, která může být v řadě případů přenositelná do světa reálného. Pro celou řadu lidí se obchod s virtuálními předměty či hráčskými účty stal skutečným zdrojem obživy. V následující části uvedu několik příkladů virtuálních věcí, včetně ceny, za kterou byly tyto věci prodány.[190]

188: GUZMAN, Andrew, Joost H. B. PAUWELYN. *International Trade Law*. Aspen Publishers, 2012, s. 37.

189: Hráčské účty jsou věcí nehmotnou mající povahu pohledávky, neboť jde typicky o smluvní vztah uzavřený mezi dvěma subjekty práva.

190: Zdrojem informací byly:

*Vejce dražší než vaše auto. Deset luxusních virtuálních předmětů.* [online]. [cit. 15.7.2016]. Dostupné z: http://bonusweb.idnes.cz/nejdrazsi-virtualni-predmety-dko-/Magazin.aspx?c=A150930_082546_bw-magazin_anb

*10 Most Expensive Virtual Items Ever Sold.* [online]. [cit. 15.7.2016]. Dostupné z: https://www.youtube.com/watch?v=VUNRl3kAATk

*10 of the Most Expensive Virtual Items In Video Games.* [online]. [cit. 15.7.2016]. Dostupné z: http://www.therichest.com/rich-list/most-popular/10-of-the-most-expensive-virtual-items-in-video-games/

*11 Most Expensive Virtual Items in Video Games.* [online]. [cit. 15.7.2016]. Dostupné z: http://www.insidermonkey.com/blog/11-most-expensive-virtual-items-in-video-games-377679/2/

Prostředím, v němž byly doposud prodávány nejdražší virtuální předměty, je projekt Entropia Universe.[191] V rámci této MMORPG[192] hry byla zatím nejdražší virtuální věcí planeta Calypso (prodejní cena činila 6 milionů $). Projekt Entropia pak v pomyslné desítce nejdražších virtuálních věcí zabírá i další přední příčky. Druhou nejdražší virtuální věcí je klub - Club Neverdie. Tento klub byl v roce 2005 zakoupen Jonen Jacobsem za 100 000 $ a následně prodán v roce 2010 za 635 000 $. Třetí místo pak patří Crystal Palace Space Station (Entropia), jež byla prodána v roce 2009 za 335 000 $. Mezi dalšími virtuálními nemovitostmi, jež byly prodány, pak vyčnívá prodej virtuálního Amsterodamu v projektu Second Life. Prodejní cena činila 50 000 $.

Obrázek 14: Nest Egg (Entropia)

Pokud bychom opustili virtuální nemovitosti, pak nejdražší samostatnou, doposud prodanou, virtuální věcí je Nest Egg[193] (vejce s novým typem stvoření, Entropia). Prodejní cena tohoto vejce činila 69 000 $. Dalšími unikátními vydraženými věcmi pak jsou: růžový pes (Ethereal Flames Pink War Dog ze hry DOTA 2, který se v roce 2013 prodal za 38 000 $), hořící čepice (Burning Team Captain ze hry Team Fortress 2, prodala se přibližně za 18 000 $), meč (Dragon Slaying Sabre ve hře Age of Wulin, v roce 2011 se prodal za 16 000 $), palcát (Echoing Fury ze hry Diablo III, který se prodal za 14 000 $; nicméně největší zajímavostí u tohoto palcátu je, že jej první majitel prodal

191: Blíže viz http://www.entropiauniverse.com/

192: Jde o hru **MMORPG** (***M**assive(ly)-**M**ultiplayer **O**nline **R**ole-**P**laying **G**ame*) – počítačová hra na hrdiny o více hráčích, umožňující zapojení hráčů z celého světa skrze Internet do hry odehrávající se ve virtuálním světě.

193: Obrázek Nest Egg převzat z: *The $70,000 virtual egg is finally hatching.* [online]. [cit. 15.7.2016]. Dostupné z: http://www.entropiaplanets.com/threads/the-70-000-virtual-egg-is-finally-hatching.9055/

za 250 $, aniž by znal skutečnou cenu prodávané věci). Výše uvedené předměty však představují pouze špičku pomyslného ledovce. Samozřejmě jde o to, získat ve hře něco unikátního, co nikdo nemá, nicméně současní uživatelé neobchodují jen s unikátními či běžně ne zcela dostupnými věcmi.

Jedním z artiklů, které jsou velmi často nabízeny a prodávány v celé řadě akcí, jsou účty k hrám. Typicky se jedná o free to play hry, u nichž uživatel strávil čas tím, že se snažil o co nejvyšší upgrade. Běžně je tak možné narazit na účty z her jako jsou: Clash of Clans, Boom Beach, World of tanks aj.


LVL65 všechno vymaxované
~1000+ Victory Pointů
3400 Power Powderů = podrobnosti v obrázku, tolik pp stačí na umístění v Global 5(
na 60. místě)
přes 10500 diamantů
981 prototypových součástek = podrobnosti v obrázku
Sochy - PRAKTICKY NEJLEPŠÍ MOŽNÉ:
Troop DMG = 32%, 13%
Troop HP = 34%
GBE = 42%, 17%, 17% (+17% v uschove)
PSC = 74%, 30%, 29% (+27% v uschove)
Building HP = 32
Building DMG = (+34, +15 v uschove)
(31% resource reward v uschove)

dostat se až sem mi trvalo 2 roky
s dotazy se neváhejte zeptat
o ceně jsem ochoten jednat

ZMĚNA JMÉNA JE POŘÁD K DISPOZICI

Obrázek 15: Nabízený účet Boom Beach[194]

194: Účet, který byl k prodeji dne 2.8.2016 na portálu www.bazos.cz za 25 000 Kč. Doporučuji čtenáři navštívit některý z aukčních portálů, jako je např. www.ebay.com aj. a zkusit si zadat některou z virtuálních věcí či účtů ke hrám.

Pokud jsou tyto účty prodávány, pak se zpravidla vyvolávací cena (u kvalitnějších účtů) pohybuje v ceně nad 5 000 Kč.

V případě prodeje takovýchto účtů jsou dle občanského práva de facto prodávány pohledávky.

U virtuálního majetku je třeba vzít v potaz i otázku určení jeho hodnoty, a to jak z pohledu občanského, tak zejména trestního práva. Právě hodnota, či spíše způsobená škoda může být jedním z rozhodujících kritérií při právní kvalifikaci skutku a posouzení, zda se jedná o trestný čin, či jiné protiprávní jednání.

Občanský zákoník pak k hodnotě věci uvádí, že pokud je možno u věci vyčíslit její hodnotu v penězích, pak je hodnotou věci její cena. Dále § 492 OZ uvádí, že „*cena věci se určí jako* ***cena obvyklá****, ledaže je něco jiného ujednáno nebo stanoveno zákonem.*" Otázkou je, jak by se skutečně určovala hodnota dané virtuální věci. U hráčských účtů by jistým vodítkem mohla být cena účtů, které jsou prodávány za splnění podmínky obdobné „kvality" účtu. Nicméně problém může vyvstat u věcí či účtů, které jsou unikátní a nikdy v takovéto konfiguraci nebyly prodávány. Teoreticky by bylo možné uplatnit § 492 odst. 2 OZ, který stanoví, že „***mimořádná cena věci*** *se stanoví, má-li se její hodnota nahradit, s přihlédnutím ke zvláštním poměrům nebo ke zvláštní oblibě vyvolané náhodnými vlastnostmi věci.*" Nicméně nejsem zcela přesvědčen o tom, že by soud v ČR byl ochoten akceptovat skutečnost, že „nějaká virtuální nemovitost" může stát 6 000 000 $.

Virtuální hry a virtuální majetek již vytvořily i několik precedentů v oblasti práva. Velmi známou je kauza **Habbo Hotel**. Hra, sociální síť, či spíše jistý druh virtuální reality, poskytuje hráči virtuální hotelový pokoj, do nějž si může nakupovat vybavení za reálné peníze.[195] V roce 2007 byl v Nizozemí zadržen sedmnáctiletý mladistvý, který vytvořil phishingovou stránku,[196] která vypadala jako stránka oficiální. Od přihlašujících se uživatelů pak získal jejich přístupové údaje, které využil k získání přístupu k jejich účtům, načež rozprodal jejich virtuální nábytek a další předměty z napadených účtů. Odhadovaná škoda na odcizeném virtuálním majetku tehdy činila více než 2 800 £.[197] Tento případ byl řešen trestním soudem v Nizozemsku. Důvodem byla ta skutečnost, že se útočník dopustil dvou trestných činů v souběhu. Konkrétně se jednalo o trestný čin neoprávněného přístupu k počítačovému systému[198] a trestný čin krádeže.

195: Viz https://www.habbo.com/

196: Blíže viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing.

197: Blíže viz např.:

*Six teens arrested for virtual crime in Habbo Hotel.* [online]. [cit. 17.3.2013]. Dostupné z: http://www.technologytell.com/gaming/18923/six-teens-arrested-for-virtual-crime-in-habbo-hotel/

*Police investigate Habbo Hotel virtual furniture theft.* [online]. [cit. 17.3.2013]. Dostupné z: http://www.bbc.com/news/10207486

198: Blíže viz kap. 5.2.2.1 Trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů. Jedná se o trestné činy, jež jsou součástí Úmluvy o kyberkriminalitě, kterou ratifikovalo i Holandsko.

Dalším sporem o virtuální majetek byla kauza **Bragg vs. Linden Research, Inc**,[199] ve které Marc Bragg zažaloval společnost Linden Lab (provozovatel virtuální reality Second Life) za ukončení účtu v této virtuální realitě. Důvodem tohoto kroku ze strany Linden Lab byla skutečnost, že Marc Bragg nalezl způsob, jak nakoupit virtuální majetek (konkrétně virtuální nemovitosti – ostrovy) „za nižší než obvyklou cenu". Důvodem bylo, že Marc měl provést URL hacking, čímž získal možnost dražit majetek v neautorizovaných aukcích, a tím porušil licenční podmínky Linden Lab. Kauza nakonec skončila mimosoudním vyrovnáním.

Další kauzou spadající do roviny trestněprávní je případ ukradeného amuletu a dalších virtuálních věcí. Nizozemské soudy se níže popsaným případem zabývaly v letech 2008 -2009.[200] Dne 6. září 2007 došlo k ukradení virtuálních předmětů (amulet, maska a zlaťáky pocházející ze hry RuneScape) třináctiletému chlapci jinými nezletilými. *„Krádeži předcházelo násilí a vyhrožování násilím za účelem krádež připravit, usnadnit si ji, nebo si zajistit útěk v případě dopadení při činu. Násilí spočívalo v úderech pěstí do hlavy a žeber poškozeného a kopání do hrudníku, žeber a beder. Obžalovaný se rovněž postavil proti poškozenému s nožem, s nímž prováděl pohyby spočívající v mávání, bodání a vrhání. Poškozenému hrozil slovy „zabiju tě", či jinými slovy výhružné povahy. Obžalovaný strhl poškozeného ze židle na podlahu, ovázal mu šátek kolem krku a stiskl mu hlavu."*[201] Důvodem výše popsaného jednání bylo donutit poškozeného vydat přístupové jméno a heslo k jeho účtu ve hře RuneScape a následně odcizit výše uvedené virtuální předměty.

Soud se v uvedené kauze musel zabývat otázkou, ***„zda jsou virtuální předměty věcmi ve smyslu nizozemského trestního zákoníku (čl. 310)."*** Myšlenka, že věc musí být hmotná, aby spadala do rozsahu tohoto článku, byla odmítnuta v judikátu o elektřině z roku 1921. Nejvyšší soud tehdy judikoval, že elektřina je předmět s uživatelskou hodnotou. ***Relevantní je především skutečnost, zda má věc pro vlastníka hodnotu. Z posouzení věci vyplývá, že virtuální předměty měly pro oznamovatele, obžalovaného i spoluobžalované hodnotu.*** Tehdy třináctiletý oznamovatel v této souvislosti prohlásil: „Na RuneScape jsem hodně bohatý, a protože jsem bohatý, jsem také velmi silný. S různými zbraněmi jsem velmi silný a téměř neporazitelný. Kvůli svému velkému majetku si měním na RuneScape heslo každé tři dny, protože se bojím, aby mě někdo nehacknul." Spoluobžalovaný prohlásil: „(Jméno poškozeného) měl před několika dny štěstí, protože našel předměty, které patřily mrtvému muži, jenž byl velmi bohatý a měl hodně cenných předmětů. Vlastně jsem mu to záviděl." Z těchto prohlášení se dá vyvodit, že majetek ve hře měl pro oznamovatele, obžalovaného i spoluobžalované skutečnou hodnotu, jež jim může být sebrána. Na základě výše zmíněných skutečností soud rozhodl, že virtuální předměty jsou věcmi ve smyslu čl. 310 trestního zákoníku. ***„Relevantní rovněž je, že herní pravidla RuneScape nepředpokládají nabytí předmětů takovým způsobem, jakým se to stalo***

199: Blíže viz např. Rozsudek ze dne 30. května 2007: *Bragg v. Linden Research, Inc, 487 F. Supp. 2d 593.* [online]. [cit. 1.6.2016]. Dostupné z: https://h2o.law.harvard.edu/cases/4435

200: Rozsudek LJN: BK2773, Odvolací soud v Leeuwardenu

201: FIALOVÁ, Eva. Krádež virtuálních předmětů v příkladech nizozemské judikatury. *Revue pro právo a technologie*, 2010, roč. 1, č. 1, s. 1. [online]. [cit. 15.7.2016]. Dostupné z: https://journals.muni.cz/revue/article/view/3980/pdf

***v tomto případě. Odebrání věcí bylo spácháno mimo kontext hry. Z tohoto důvodu se nejedná o virtuální jednání ve virtuálním světě, ale o skutečné jednání, jež virtuální svět ovlivnilo.*** "[202]

Nizozemský soud ve svém rozhodnutí dále uvedl, že ***„má za prokázané, že oznamovatel ovládal ve hře své věci skutečně a výlučně. Pouze on měl po přihlášení na účet RuneScape možnost s amuletem a maskou nakládat. V trestněprávním smyslu patřily tyto věci oznamovateli. Krádež postihla jeho dispoziční moc nad věcmi. Že má hra RuneScape svého vlastníka, nepovažuje soud v tomto případě za relevantní. Navíc jsou v tomto případě naplněny i další části skutkové podstaty trestného činu krádeže, a sice že věc byla odebrána z dispoziční moci oznamovatele a byla přenesena do dispoziční moci obžalovaného. Toto se podle NS liší od odcizení např. softwaru, počítačových dat a PIN kódu. Oznamovatel nad těmito předměty neztrácí dispoziční moc. V těchto případech se o krádež nejedná.*** "[203]

Domnívám se, že přiznání hodnoty virtuálním věcem je tou skutečností, která ovlivnila rozhodování soudů ve výše popsaných případech. Zároveň může být hodnota věci, respektive její vlastnost spočívající v uspokojování potřeb člověka či její užitečnost oním kritériem, které vyžaduje i české občanské a trestní právo.

### 2.4.3 Právní jednání

Občanský zákoník stanoví, co se rozumí právním jednáním v § 545: „*Právní jednání vyvolává právní následky, které jsou v něm vyjádřeny, jakož i právní následky plynoucí ze zákona, dobrých mravů, zvyklostí a zavedené praxe stran.* " Význam právního jednání spočívá v tom, že u ICT, respektive u řady služeb poskytovaných v prostředí kyberprostoru, se vyžaduje aktivní činnost uživatele, spočívající v jeho odsouhlasení smluvních podmínek. Toto jednání sice bude právním jednáním (i s odkazem na § 546 OZ), ale nebude se však zpravidla jednat o případ uvedený v § 561 OZ, kde je uvedeno, že „*K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé.* " Případy, kdy je právně jednáno v elektronické formě[204] totiž z povahy věci vyžadují, aby tomu odpovídal i podpis jednajícího. Jedná se tedy o elektronický podpis, který je v ČR legislativně zakotven v zákoně č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

### 2.4.4 Licence

Problematika licencí je v občanském zákoníku upravena komplexněji, než tomu bylo v předchozích

202: FIALOVÁ, Eva. Krádež virtuálních předmětů v příkladech nizozemské judikatury. *Revue pro právo a technologie*, 2010, roč. 1, č. 1, s. 2. [online]. [cit. 15.7.2016]. Dostupné z: https://journals.muni.cz/revue/article/view/3980/pdf

203: Tamtéž s. 3

204: Srov dále § 562 OZ

právních předpisech (autorský zákon a obchodní zákoník), neboť z větší části přejímá do obecných ustanovení právní úpravu obsaženou v autorském zákoně (ta se dříve vztahovala pouze na licence poskytované dle autorského zákona). Problematika licencí je v občanském zákoníku upravena v § 2358 a násl. Z těchto ustanovení mimo jiné vyplývá, že „*Licenční smlouvou poskytuje poskytovatel nabyvateli oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném omezeném nebo neomezeném rozsahu a nabyvatel se zavazuje,* ***není-li ujednáno jinak, poskytnout poskytovateli odměnu.***" Obecně výslovně platí, že pokud byla sjednána licence na dobu neurčitou, může být vypovězena. Ustanovení § 2371 OZ stanoví, že „*smlouvou autor poskytuje nabyvateli oprávnění k výkonu práva autorské dílo užít v původní nebo zpracované či jinak změněné podobě, a to určitým způsobem nebo všemi způsoby užití, v rozsahu omezeném nebo neomezeném.*"

Autorský zákon je ve vztahu k občanskému zákoníku normou lex specialis. Formálně jsou oba předpisy stejné právní síly, takže je při aplikaci těchto norem třeba využít princip subsidiarity občanského zákoníku. „*Pro řešení vztahů vzniklých v souvislosti s vytvořením a společenským uplatněním autorských děl je proto třeba použít autorského zákona ve všech případech, kde tento zákon obsahuje vlastní, přímou právní úpravu těchto vztahů.*"[205] Pokud autorský zákon speciální úpravu neobsahuje, použije se občanský zákoník.

### 2.4.5 Náhrada škody

V závěrečné části této podkapitoly, která se vztahuje k občanskému zákoníku, se chci velmi stručně věnovat problematice náhrady škody. V případě kybernetické kriminality či kybernetických útoků se velmi často může stát, že je počítač či počítačový systém zneužit třetí osobou (například z důvodu zcela chybějícího zabezpečení, či ponechání počítače přístupného třetím osobám aj.).[206] V takovém případě je možné využít právě institutu občanského práva, který se vztahuje k náhradě škody. Dále je případně možné využít institutů trestního práva při respektování principu subsidiarity trestní represe.[207]

Ustanovení § 2900 OZ uvádí, že pokud to vyžadují okolnosti případu nebo zvyklosti soukromého života, **musí si každý počínat při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného**. Toto ustanovení definuje generální prevenční povinnost každé osoby.

**V případě, že škůdce způsobí újmu úmyslným porušením dobrých mravů, je povinen ji nahradit.**[208] Pokud škůdce způsobí škodu porušením zákonné povinnosti (tedy i povinnosti vyplývající

205: Viz § 1 odst. 3 OZ

206: Blíže viz kap. 2.6 Možnosti právní odpovědnosti uživatele za jednání v kyberprostoru.

207: Viz § 12 odst. 2 TZK: „*Trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech společensky škodlivých,* ***ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu.***"

208: § 2909 a násl. OZ

z § 2900 OZ), má se za to, že škodu zavinil z nedbalosti.[209] Občanský zákoník dále v § 2912 odst. 1 stanoví, že: *„Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale."*

V souvislosti s náhradou škody je třeba se věnovat i § 2913 OZ (Porušení smluvní povinnosti), kde je stanoveno, že **„Poruší-li strana povinnost ze smlouvy, nahradí škodu z toho vzniklou** druhé straně nebo i osobě, jejímuž zájmu mělo splnění ujednané povinnosti zjevně sloužit." **Povinnosti k náhradě škody je možné se zprostit, pokud škůdce prokáže, *„že mu ve splnění povinnosti ze smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli.*** *Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním smluvené povinnosti v prodlení, ani překážka, kterou byl škůdce podle smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí."*

Na závěr je třeba se zabývat i možností, že škodu způsobí věc, a to sama od sebe. V takovém případě je povinen škodu nahradit ten, kdo měl mít nad věcí dohled. Nelze-li takovou osobu určit, platí, že je jí vlastník věci. Pokud dotyčná osoba prokáže, že náležitý dohled nezanedbala, zprostí se povinnosti k náhradě škody.

## 2.5 Odpovědnost poskytovatele služeb informační společnosti

Na tvorbě práva na Internetu, na omezování či rozšiřování jeho aktivit, se podílejí *definiční autority* tvorbou *definičních norem*. Aby bylo možné pochopit otázku případné odpovědnosti poskytovatelů služeb informační společnosti, musím nejdříve charakterizovat právě definiční normu a definiční autoritu.

**Definiční normy** jsou vytvářeny a implementovány subjekty, které jsou oprávněny definovat prostředí informační sítě. Jde de facto o normy sui generis, které vymezují informační sítě jako takové. Vyskytují se ve vrstvách, které jsou na sobě závislé. *„Definiční normy jsou vytvářeny telekomunikačními operátory, producenty kancelářského softwaru, ale i například tvůrci, či provozovateli online her, nebo každý, kdo si otevře blog, nebo kdo má emailovou schránku (definiční norma vytvořená uživatelem této schránky je například filtr, který automaticky provádí nastavenou operaci s doručenou poštou)."*[210]

**Definiční autority** jsou původci definičních norem, jde o subjekt, který svým fungováním vytváří

209: § 2911 OZ

210: Srov. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 42 a násl., s. 88 a násl.

Do definičních norem je možné podřadit i **RFC** (*Request For Comments*). Byť se jedná o dokumenty mající spíše povahu doporučení než norem, tak jsou uživateli respektovány, jako by normami byly. RFC lze volně získat na adrese http://www.ietf.org/rfc.html.

pravidla fungování logického systému, ve kterém autorita působí. Jak již bylo uvedeno dříve, má mezi těmito autoritami výsostné postavení ICANN, neboť této organizaci přísluší přidělování, správa a stanovení pravidel pro systém doménových jmen.[211] Další definiční autoritou je například IETF.[212] Byť se definiční autority mohou jevit jako neomezení správci kyberprostoru, stále jsou subjektem práva některého státu.[213]

Specifikem **Internet**u je, že **existuje** právě **jen díky definičním autoritám**. **Je z nich složen. Žádná operace se neuskuteční bez účasti** (provedení či zprostředkování operace) **definiční autority.**

Lawrence Lessig ve své knize Code and Other Laws of Cyberspace (Code v. 2) uvádí: „*Můžeme postavit, navrhnout nebo nakódovat*[214] *(naprogramovat) kyberprostor k ochraně hodnot, které pokládáme za základní. Můžeme jej ale také navrhnout nebo naprogramovat tak, že tyto hodnoty necháme vymizet. Žádná prostřední možnost tu není, vše v kyberprostoru je nějakým způsobem postaveno. Kód nikdy neobjevujeme, ten vždy utváříme.*“[215]

Po výše uvedeném vyjádření a svých zkušenostech s kyberprostorem si dovolím tvrdit, že největší **definiční autoritou**, byť se nejedná o subjekt, který vytváří pravidla fungování logického systému, **je uživatel jako takový**. Jeho definiční role působí zprostředkovaně. Uživatel služeb, jež poskytují jednotliví ISP, přímo či zprostředkovaně ovlivňuje to, co bude v kyberprostoru úspěšné, a co ne. Pokud se dostatečně velká skupina uživatelů rozhodne, že aktivně přestane využívat některou ze služeb, poskytovaných ISP, bude tato služba nucena změnit své „chování“ na základě poptávky uživatele, nebo v horším případě zanikne. Je otázkou, jak velká skupina lidí by musela přestat využívat např. služby Google, Microsoft, Facebook aj., aby to pro tyto společnosti nebylo marginální, nicméně právě v kyberprostoru mají uživatelé možnost přímo svým aktivním konáním či zdržením se konání ovlivnit fungování či nefungování jednotlivých služeb.

---

211: Doménové jméno slouží k označení „třídy“ počítačových systémů připojených k Internetu, které se vyznačují určitou geografickou a organizační jednotou: např. všechny počítače v doméně **.cz** se nalézají na území České republiky, všechny počítače v doméně (subdoméně) **nic.cz** jsou počítače pod správou sdružení CZ.NIC. Jména hlavních domén (vycházející z geografie) jsou pevně rozdělena.

Polčák k doménovým jménům mimo jiné uvádí, že: Formou **virtuální reality** může být doménové jméno. To je záznamem v databázích DNS. **Pokud se doménová autorita rozhodne vymazat doménové jméno, přestane tato virtuální realita existovat.** Je jedno, jestli jde o doménové jméno např.: www.tondovy_stranky.cz, či o www.google.com.

212: IETF - The Internet Engineering Task Force. Blíže viz: https://www.ietf.org/

213: Vždy jde o fyzickou nebo právnickou osobu, která má sídlo či trvalé bydliště. Tudíž se na ně vztahuje právo jako na jakýkoli jiný subjekt. V některých zemích (např. Čína) je definiční autoritou sám stát.

214: **Definiční normu** označuje Lessig jako **kód (code).**

215: Srov. LESSIG, Lawrence. *Code v. 2*. s. 6 Dostupný v plném znění (Angl.) [online]. [cit. 13.3.2008]. Dostupné z: http://pdf.codev2.cc/Lessig-Codev2.pdf

Lze tedy vyslovit tyto závěry:

- **Kyberprostor je tvořen vůlí definičních autorit.**
- **Všichni poskytovatelé služeb informační společnosti jsou definičními autoritami.**
- **Každý poskytovatel služeb, jako jakýkoli jiný subjekt práva, je právně odpovědný za své jednání.**[216]

Problematika odpovědnosti poskytovatelů služeb informační společnosti (ISP) dle zákona o některých službách informační společnosti je zde uváděna záměrně, neboť má přímý vztah k problematice kybernetické kriminality, odpovědnosti uživatelů a zjišťování a zajišťování informací podstatných pro trestní řízení. *„Obecně platí zásada, že je-li informace protiprávní a ISP neměl ani povědomosti o jejím vytvoření či komunikaci, je ISP zbaven odpovědnosti ze zákona.“*[217]

Pojem poskytovatel služby je mimo výše uvedeného zákona definován například i v Úmluvě o kyberkriminalitě, konkrétně v čl. 1 písm. c), kde je uvedeno, že poskytovatelem služby je:

- jakýkoli veřejný nebo soukromý subjekt, **který uživatelům své služby umožňuje komunikovat prostřednictvím počítačového systému**, a
- jakýkoli jiný subjekt, **který zpracovává nebo uchovává počítačová data pro takovou komunikační službu nebo pro uživatele takové služby**.

Zákon o některých službách informační společnosti rozeznává následující tři poskytovatele služeb, přičemž stanoví, že poskytovatelem služby je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti:[218]

1) **Poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem** (angl. Mere Conduit nebo Access Provider).
2) **Poskytovatele služeb spočívajících v automatickém mezi ukládání informací poskytnutých uživatelem** (tzv. caching).
3) **Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem** (tzv. storage nebo hosting).

Z výše uvedené definice není vyloučena žádná osoba (nemusí se jednat např. o osobu podnikající podle jiného právního předpisu), nicméně platí, že pokud se na poskytovatele vztahují další speciální předpisy (viz např. některý z poskytovatelů připojení), musí se jimi také řídit.

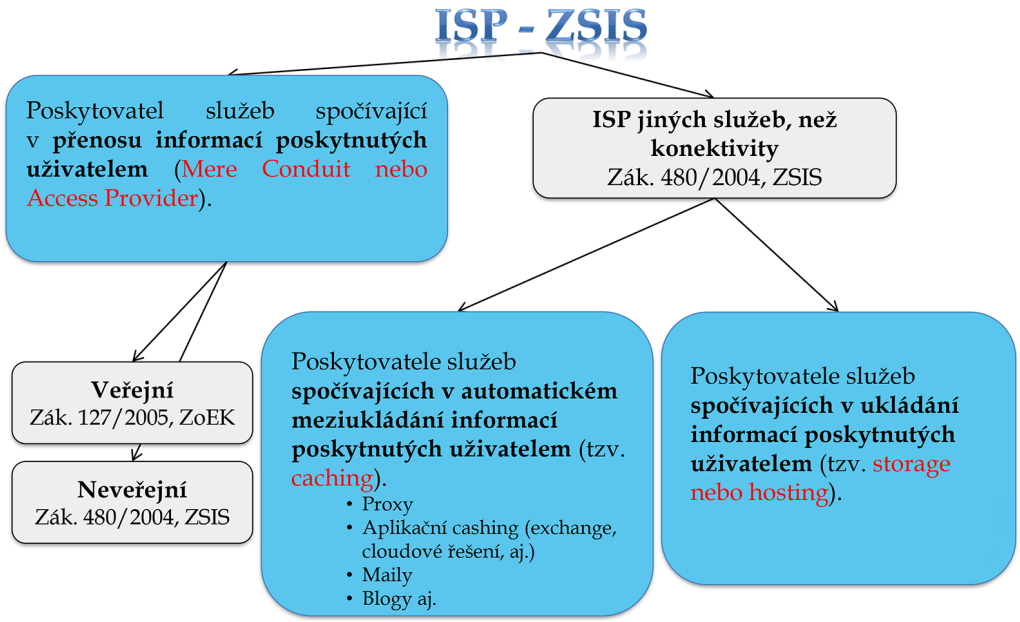
---

216: V trestním právu je možná pouze **subjektivní odpovědnost** (tj. odpovědnost za jednání zaviněné - ať úmyslné, či z nedbalosti - srov. § 13 odst. 2 TZK). V některých případech však lze vůči poskytovatelům uplatnit i **objektivní odpovědnost** vyplývající ze soukromoprávních odvětví práva - např. § 45 AZ.

217: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 55

218: Viz § 2 písm. d) ZSIS

Graficky je možné uvedené poskytovatele (a vázanost jednotlivými právními předpisy znázornit následovně:




Příjemcem služby informační společnosti je pak uživatel, kterým může být každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledání či zpřístupnění informací.[219]

**Službou informační společnosti** se dle zákona o některých službách informační společnosti rozumí *„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.“*[220] Definice uvedená v České právní úpravě pak přímo vychází ze Směrnice Evropského parlamentu a Rady (EU) 2015/1535[221] [čl. 1 písm. b)], která uvádí, že službou je *„jakákoli služba informační společnosti, tj. každá služba poskytovaná **zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.**“*

219: Viz § 2 písm e) ZSIS

220: § 2 písm. a) ZSIS

221: Dostupný online: http://www.unmz.cz/urad/smernice-98-34-es-ve-zneni-smernice-98-48-es

Z této definice vyplývají čtyři základní znaky služby:

- je poskytovaná elektronickými prostředky,
- je poskytována na individuální žádost uživatele,
- je běžně poskytována za odměnu,
- je poskytována distančně (na dálku).

Pojem **poskytování elektronicky** je uveden ve Směrnici Evropského parlamentu a Rady (EU) 2015/1535 v čl. 1 písm. b) ii), kde je definováno, že se jedná o službu, která je odeslána z výchozího místa a je přijata v místě jejího určení prostřednictvím elektronického zařízení pro zpracování (včetně digitální komprese) a uchovávání dat. Tato služba je jako celek odeslána, přenesena nebo přijata drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky. Česká úprava využívá demonstrativního výčtu, kde je uvedeno, že se jedná zejména o síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronickou poštu.[222] Ve vztahu k základním technickým pojmům uvedeným v kap. 1.2.3 Počítač (Počítačový systém) této monografie je třeba uvést, že v případě elektronických prostředků se bude jednat o počítačový systém.

**Individuální žádost uživatele** znamená, že se musí jednat o aktivní činnost ze strany uživatele. Husovec uvádí, že jde o případy, kdy například uživatel sám vpíše adresu do políčka prohlížeče (IE, Firefox, Chrome aj.), čímž formuluje žádost na otevření příslušné stránky nebo napíše SMS zprávu. Typickým příkladem služby, která je poskytována bez individuální žádosti, je podle Husovce např. televizní vysílání.[223]

Nejproblematičtějším kritériem definice služby informační společnosti je, že tato **služba je poskytována za odměnu**. Česká úprava kopíruje i v tomto bodě úpravu mezinárodní a obsahuje ustanovení *„zpravidla za úplatu"*. V prostředí Internetu či jiných počítačových sítí existuje celá řada služeb, které jsou poskytovány „zdarma". Husovec zcela správně argumentuje tím, že pod pojmem odměna si je možné představit celou řadu skutečností odlišných od ryze peněžitého plnění.[224] Může se jednat o plnění, které bude mít podobu nepeněžitého charakteru, kdy ISP získá o uživatelích informace v podobě osobních, technických a jiných údajů, času stráveného užíváním dané služby, nabídne uživateli reklamu na jiné produkty atd. Nicméně i tato podmínka by měla dle Husovce být interpretována extenzivněji, a to tak, že je vyvíjena činnost *potenciálně ekonomická*.[225]

Díky tomu, že si pod pojmem úplata lze představit skutečně rozlišné možnosti (např. poděkování, návštěva stránky či odkazu, finanční či jiné plnění), a díky znění zákona o některých službách

222: Viz § 2 písm. c) ZSIS

223: Blíže viz HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 100

224: Tamtéž viz s. 98

225: Tamtéž s. 99

informační společnosti i dle Směrnice Evropského parlamentu a Rady (EU) 2015/1535 (viz *„zpravidla za úplatu"*) lze vyvodit závěr, že činnost poskytovatele služeb informační společnosti může být poskytována i zdarma.

Pojem **na dálku** definuje Směrnice Evropského parlamentu a Rady (EU) 2015/1535 jako službu, která je poskytována bez současné přítomnosti stran.[226]

Husovec ve své monografii dále uvádí příklady, které demonstrují, co vše lze považovat za službu informační společnosti. Pod tento pojem je třeba dle Směrnice 2000/31/ES Evropského parlamentu a Rady zařadit celou řadu činností, ke kterým dochází v online světě. Může se jednat o online prodej zboží, služby, které poskytují online informace, komerční komunikaci, či služby poskytující nástroje pro vyhledávání, přístup a získávání údajů, služby poskytující přenos informací prostřednictvím komunikační sítě aj.

*„Judikatura Soudního dvora EU již přímo či nepřímo uznala například službu AdWords (inzertní služba ve vyhledávači Google),*[227] *službu pojištění motorových vozidel přes Internet ,*[228] *on-line prodej kontaktních čoček ,*[229] *připojení se k Internetu ,*[230] *rezervaci hotelu skrze email ,*[231] *rezervaci služeb cestovní kanceláře skrze email*[232]*, aukční server eBay* [233]*a klasické vyhledávání od společnosti Google."* [234]

### 2.5.1 Poskytovatelé služeb spočívajících v přenosu informací poskytnutých uživatelem (Mere Conduit či Access Provider)

Z hlediska zákona o některých službách informační společnosti může být tímto poskytovatelem jakákoli fyzická či právnická osoba, která je schopna poskytovat jiným subjektům (fyzickým či právnickým osobám) službu přenosu informací (poskytnutých uživatelem) prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací.

226: Viz čl. čl. 1 písm. b) i) této směrnice.

227: Rozhodnutie *Google France* C-236/08 až C-238/08.

228: Rozhodnutie *Bundesverband* C-298/07.

229: Rozhodnutie *Ker-Optika* C-108/09.

230: Rozhodnutie *Promusicae* C-275/06 a *Tele 2*. C-557/07

231: Rozhodnutie *Alpenhof* C-144/09.

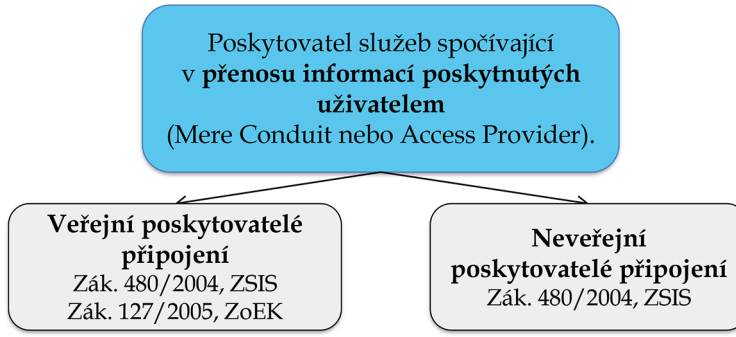
232: Rozhodnutie *Pammer* C-585/08.

233: Rozhodnutie *L'Oreal v. Ebay* 324/09.

234: HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, s. 101–102.

Takovýmto poskytovatelem pak nebudou pouze osoby podnikající v oblasti připojování jiných k počítačovým sítím či do Internetu (typicky se bude jednat o osoby zapsané v *Evidenci podnikatelů v elektronických komunikacích podle všeobecného oprávnění*),[235] ale půjde o jakoukoli osobu poskytující či zprostředkovávající přenos informací prostřednictvím sítí elektronických komunikací. Lze si tedy představit situaci, kdy bude poskytovatelem připojení podle tohoto zákona i osoba, která zřídí a jiným zpřístupní například WiFi připojení v rámci restaurace, bytového domu, domácnosti aj. Stejně tak do této kategorie budou spadat například i školy (typicky vysoké školy poskytující svým studentům a učitelům konektivitu v rámci své sítě či do Internetu.). Službou spočívající v přenosu informací však je i např. aplikace Skype, ICQ aj. Velmi zjednodušeně můžeme označit tyto poskytovatele za **poskytovatele připojení.**

Z hlediska vymezení jednotlivých práv a povinností poskytovatelů připojení je nicméně třeba tyto poskytovatele rozdělit do dvou skupin, a to na poskytovatele **veřejné a neveřejné**. Na obě dvě skupiny poskytovatelů připojení se vztahuje zákon o některých službách informační společnosti, avšak na veřejné poskytovatele připojení se dále vztahuje zákon o elektronických komunikacích, který těmto poskytovatelům stanoví další práva a povinnosti. K určení, zda je poskytovatel zařazen do té které skupiny, pomůže výše uvedená *Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění* spravovaná Českým telekomunikačním úřadem.[236] Z hlediska odhalování a vyšetřování kybernetické kriminality, zejména pokud jde o zisk informací od jednotlivých ISP, má tato informace zásadní význam.




235: Databáze podnikatelů v elektronických komunikacích podle všeobecného oprávnění je dostupná online: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

236: Dále jen ČTÚ.

### 2.5.1.1 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZSIS

Zákon o některých službách informační společnosti v případě poskytovatele připojení v co možná největší míře omezuje odpovědnost tohoto subjektu za přenášené informace. Zvláštní požadavky a podmínky jsou však stanoveny vůči operátorům služeb elektronických komunikací. Tyto podmínky stanoví zákon o elektronických komunikacích. Ustanovení čl. 12 směrnice č. 2000/31/ES umožňuje členským státům nařídit Poskytovateli, aby přerušil poskytování služeb, skrze něž dochází k přenosu informací, jež neoprávněně zasahují do práv jiného. Tato možnost je jedním z prostředků, jak zabránit protiprávnímu jednání. Příkaz k přerušení poskytování služeb zpravidla vydává soud.

Poskytovatele **připojení lze činit odpovědného za obsah informace** jen pokud:

- přenos sám iniciuje,
- zvolí uživatele přenášené informace, nebo
- zvolí nebo změní obsah přenášené informace.[237]

Podle § 6 ZSIS **není poskytovatel připojení povinen** dohlížet na obsah přenášených informací, či aktivně zjišťovat protiprávnost přenášené informace. Poskytovatele nelze činit odpovědného za kvalitu informace (kterou mu nelze přičíst), a to i v případě, že si je vědom protiprávnosti přenášené informace.[238]

### 2.5.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZoEK

Veřejní poskytovatelé připojení se dále řídí zákonem o elektronických komunikacích. Tento zákon definuje některé pojmy, které dále používá. Pro účely této monografie se jedná zejména o:

- **Službu elektronických komunikací** [§ 2 písm. n) ZoEK]. Tímto pojmem se dle § 2 písm. n) ZoEK rozumí služba, která je obvykle poskytována za úplatu a spočívá (zcela nebo převážně) v přenosu signálů po sítích elektronických komunikací. Touto službou pak nejsou služby nabízející obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaný službami elektronických komunikací. Dále touto službou nejsou služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.

237: Tyto tři možnosti činí poskytovatele připojení odpovědného de facto pouze v případě, že je sám subjektem, který aktivně odesílá, či jinak manipuluje s přenášenými informacemi.

238: Srov. čl. 12 směrnice č. 2000/31/ES a ust. § 3 odst. 1, 2 zák. č. 480/2004 Sb.

- **Veřejně dostupnou službou elektronických komunikací** [§ 2 písm. o) ZoEK]. Touto službou je taková služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.

- Nevyloučením se rozumí možnost uzavřít smlouvu s podnikatelem, jenž poskytuje veřejně dostupnou službu elektronických komunikací. Podstatné je, že tato služba je otevřena širokému okruhu lidí, z nichž není nikdo předem vyloučen. Opakem takovéto služby může být například členství v různých spolcích, komorách, či například status studenta školy.

- **Podnikatel**, který zajišťuje nebo je oprávněn zajišťovat veřejnou komunikační síť nebo přiřazené prostředky, je tímto zákonem označován za **operátora** [§ 2 písm. e) ZoEK].

- **Účastníkem** [§ 2 písm. a) ZoEK] je každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb. **Uživatelem** [§ 2 písm. n) ZoEK] je každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací.

Zákon o elektronických komunikacích zavedl, na základě 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 a o změně směrnice 2002/58/ES*,[239] povinnost preventivně uchovávat **provozní a lokalizační údaje**[240] o uskutečněné elektronické komunikaci. Tato povinnost se vztahuje pouze na podnikatele, který zajišťuje nebo je oprávněn zajišťovat veřejnou komunikační síť nebo přiřazené prostředky.

Účelem směrnice o Data Retention bylo **harmonizovat předpisy členských států týkající se povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí**, pokud jde o uchovávání provozních a lokalizačních údajů tak, aby se daly poskytovat příslušným orgánům členských států pro účely **prevence, vyšetřování, odhalování a stíhání závažné trestné činnosti, jako jsou terorismus a organizovaný zločin**.

Rozsah směrnice byl stanoven na oblast provozních a lokalizačních údajů o právnických i fyzických osobách a na související údaje, které jsou nezbytné k identifikaci účastníka nebo registrovaného uživatele.

---

239: Dále jen směrnice o **Data Retention.** Pojem data retention znamená plošné ukládání provozních a lokalizačních údajů u poskytovatelů připojení (v ČR u poskytovatelů dle zákona o elektronických komunikacích).

240: Viz § 97 odst. 4 ZoEK.

**Provozními a lokalizačními údaji jsou** zejména **údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace** a dále **údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.**

Rozsah provozních a lokalizačních údajů, forma a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu (viz § 97 odst. 3 ZoEK) a způsob jejich likvidace stanoví prováděcí právní předpis. Prováděcím předpisem je **vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.**

Tato směrnice se nevztahovala na obsah elektronických sdělení ani na informace vyžadované při použití sítě elektronických komunikací.

**Členské státy** byly dle Směrnice **povinny zajistit, aby se telekomunikační údaje uchovávaly po dobu nejméně šesti měsíců a nejvýše dvou let ode dne komunikace.** Uvedená směrnice byla v různých podobách transponována do právních řádů členských zemí EU. Nicméně už od jejího vzniku docházelo k názorovým střetům na směrnici jako takovou. Odpůrci namítali, že směrnice nepřiměřeným způsobem zasahuje do základních lidských práv a svobod, zejména tím, že de facto přikazuje plošné sbírání informací o jednotlivých uživatelích. Dále bylo argumentováno, že směrnice (v takto obecné podobě) by nebyla schopna projít testem proporcionality.

**Test proporcionality** je standardním právním nástrojem jak soudů mezinárodních, tak soudů ústavních (národních) v případě, že se posuzuje konflikt ustanovení právního řádu, sledující ochranu ústavně zaručeného práva či veřejného zájmu, s jiným základním právem či svobodou. Test proporcionality zahrnuje tři kritéria posuzování přípustnosti zásahu:

1) **Princip vhodnosti** (způsobilosti naplnění účelu), dle něhož **musí být příslušné opatření vůbec schopno dosáhnout zamýšleného cíle**, jímž je ochrana jiného základního práva nebo veřejného statku.

2) **Princip potřebnosti**, dle něhož **je povoleno použití pouze prostředku nejšetrnějšího k dosažení požadovaného účelu** (zásahu do základních práv a svobod), **z více možných prostředků.**

3) **Princip přiměřenosti** (v užším smyslu), dle kterého **újma na základním právu nesmí být nepřiměřená ve vztahu k zamýšlenému cíli**, tj. opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních.

Směrnice o Data Retention, respektive její národní transpozice se staly předmětem ústavních žalob v některých zemích EU. Z těch nejvýznamnějších je třeba zmínit rozhodnutí ústavních soudů Rumunska (2009), Spolkové republiky Německa (2010) a České republiky (2011). Zaměřím se na rozhodnutí soudů v SRN a ČR.

Spolkový ústavní soud SRN, který řešil konflikt mezi svobodou a bezpečností (na základě směrnice o Data Retention) a vyslovil se ve prospěch svobody jednotlivce. Dne 2. března 2010 soud rozhodl, že hromadné uchovávání údajů o telefonických a datových přenosech je v Německu neústavní.

Soud tak reagoval na hromadnou stížnost 35 000 občanů, kteří žádali zrušení zákona z roku 2008, jenž telekomunikačním společnostem nařizoval archivovat záznamy o telefonických hovorech a e-mailové komunikaci po dobu šesti měsíců pro potřeby vyšetřovacích orgánů. Spolkový ústavní

soud napadené předpisy jako neústavní zrušil. Dále uvedl, že povinnost uchovávat údaje ve stanoveném rozsahu sice není od samého počátku zcela protiústavní, chybí však zákonná úprava odpovídající zásadě přiměřenosti. Dle vyjádření soudu nebyly napadené předpisy v souladu s ústavněprávními požadavky na bezpečnost dat, nedošlo k jasnému vymezení účelu použití údajů (a transparentnosti použití údajů) a nebyla dostatečně zajištěna právní ochrana.

Soud uvedl, že *„využívání základních práv a svobod občanů (zde tajemství zpráv podávaných elektronickými komunikačními prostředky) nesmí být ze strany státu kompletně sledováno, dokumentováno a registrováno; to patří k ústavně právní identitě Spolkové republiky Německo, o jejíž zachování se republika musí zasazovat v evropských i mezinárodních souvislostech.*“[241]

V České republice došlo k implementaci směrnice o Data Retention ještě před její účinností v rámci EU (V EU byla směrnice přijata 15. března 2006, s požadavkem na transpozici do 15. září 2007. V ČR byla implementována do § 97/3 ZoEK, s účinností od 1.5.2005). I v ČR došlo k podání ústavní stížnosti, konkrétně sdružením Iuridicum Remedium, kterou podpořila skupina 51 poslanců. Tato stížnost byla podána k Ústavnímu soudu v březnu 2010. V roce 2011 pak Ústavní soud rozhodl a zcela vyhověl návrhu na úplné zrušení příslušných pasáží zákona o elektronických komunikacích (konkrétně se jednalo o § 97 odst. 3 a 4) a prováděcí vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů a zrušení ustanovení trestního řádu.[242] Soud se vyjádřil následovně: *„Ústavní soud seznal, že napadená právní úprava porušuje ústavněprávní limity, neboť nesplňuje požadavky plynoucí z principu právního státu a je v kolizi s požadavky na omezení základního práva na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny, které plynou z principu proporcionality.*“

Legislativci v ČR reagovali na námitky Ústavního soudu ČR a byla přijata **nová právní úprava**, která v ČR nadále umožňuje plošné uchovávání provozních a lokalizačních údajů, neboť **respektuje** již dříve zmíněný **test proporcionality** zejména tím, že jasně deklaruje okruh subjektů (oprávněných provozní a lokalizační údaje vyžadovat) a účel pro který je možné údaje vyžadovat.

241: *German Federal Constitutional Court rejects data retention law.* [online]. [cit. 16.7.2016]. Dostupné z: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/
Srov dále např.: *National legal challenges to the Data Retention Directive*. [online]. [cit. 16.7.2016]. Dostupné z: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html
*Data retention unconstitutional in its present form.* [online]. [cit. 16.7.2016]. Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690
*German Bundestag Passes New Data Retention Law.* [online]. [cit. 16.7.2016]. Dostupné z: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/
242: Viz Nález Ústavního soudu Pl. ÚS ÚS 41/11, ze dne 22. 3. 2011. *Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu.* [online]. [cit. 24.8.2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=4&typ=result

Zároveň byla přijata opatření, jež přikazují podnikatelům dle zákona o elektronických komunikacích přijmout taková pravidla, aby měly provozní a lokalizační údaje zajištěny stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně před neoprávněným přístupem, změnou, zničením, ztrátou anebo odcizením nebo jiným neoprávněným zpracováním nebo využitím, jako údaje podle § 88 ZoEK.[243]

Byla také **stanovena maximální délka, po kterou je možné tyto údaje uchovávat, ta v současnosti činí 6 měsíců**. Po uplynutí této doby je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud zákon nestanoví jinak (§ 90 ZoEK). Dále byla stanovena **povinnost zajistit, aby při uchovávání provozních a lokalizačních údajů nebyl uchováván obsah zpráv a takto uchovávaný dále předáván** (§ 97 odst. 3 ZoEK).

Zároveň byla v trestním řádu zdůrazněna **zásada subsidiarity** (zejm. § 88 a 88a TŘ: *„nelze-li sledovaného účelu dosáhnout jinak, nebo bylo-li by jinak jeho dosažení podstatně ztížené"*). Garance minimální ingerence do základních lidských práv je v těchto případech dána mimo jiné i tím, že příkaz k vydání provozních a lokalizačních údajů vydává soudce na návrh státního zástupce.

Kdo a za jakých podmínek je tedy v ČR oprávněn žádat vydání provozních a lokalizačních údajů? Dle § 97 odst. 3 ZoEK je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, na požádání povinna je bezodkladně poskytnout:

a) **orgánům činným v trestním řízení** pro účely a při splnění podmínek stanovených zvláštním právním předpisem,[244]

b) **Policii České republiky** pro účely zahájeného **pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby** a při splnění podmínek stanovených zvláštním právním předpisem,[245]

c) **Bezpečnostní informační službě** pro účely a při splnění podmínek stanovených zvláštním právním předpisem,[246]

243: Blíže viz § 88a ZoEK

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

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

Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

246: § 6 až 8 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.

d) **Vojenskému zpravodajství** pro účely a při splnění podmínek stanovených zvláštním právním předpisem,[247]

e) **České národní bance** pro účely a při splnění podmínek stanovených zvláštním právním předpisem.[248]

V rámci Evropské unie pak soudní dvůr EU (dne 8. 4. 2014) po předchozím stanovisku[249] svého generálního advokáta Pedra Cruze Villalóna vynesl verdikt,[250] v jehož rámci **zneplatnil příslušnou směrnici o Data Retention (2006/24/ES)**.

*„Dnešním rozsudkem prohlašuje Soudní dvůr směrnici za neplatnou."*

*„Vzhledem k tomu, že Soudní dvůr neomezil časové účinky rozsudku, je prohlášení neplatnosti účinné ode dne, kdy směrnice vstoupila v platnost."*

Soudní dvůr EU zejména vytýkal tu skutečnost, že *„unijní zákonodárce překročil přijetím směrnice o uchovávání provozních údajů hranice vymezené požadavkem na dodržování zásady proporcionality."*

Rozhodnutí spočívající v ponechání či zrušení platných legislativ, které řeší uchovávání provozních a lokalizačních údajů v členských státech EU, je plně na příslušných národních orgánech a samotná Unie jim nehodlá ani doporučovat či dávat nějaké vodítko ohledně toho, jak se mají zachovat.[251]

Jak se postavit k plošnému uchovávání provozních a lokalizačních údajů? Osobně se domnívám, že v kyberprostoru není možné jiným způsobem zrekonstruovat události, které se odehrály v minulosti, než tak, že budou uchovávány provozní a lokalizační údaje. Kyberprostor a ICT, které umožňují velmi rychlou změnu topologie sítě, služeb aj. technologie, které umožňují získání několika různých identit v rámci jednotek sekund vlastně ani jinou možnost nepřipouští.

Uvědomuji si, že plošné uchovávání provozních a lokalizačních údajů zasahuje do mých základních práv a svobod, nicméně tím, že jsem přijal koncepci společenské smlouvy a vzdal jsem se části svých

247: § 9 a 10 zákona č. 289/2005 Sb., o Vojenském zpravodajství.

248: Zákon č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů.

249: Stanovisko Generálního advokáta Pedra Cruz Villalóna. Věc C-293/12 a C-594/12. [online]. [cit. 15.7.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

250: Soudní dvůr Evropské unie. Tisková zpráva č. 54/14, ze dne 8. 4. 2014. **Rozsudek ve spojených věcech C-293/12 a C-594/12.** [online]. [cit. 15.7.2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

251: PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10.11.2015]. Dostupné z: http://www.earchiv.cz/b14/b0428001.php3

práv a svobod ve prospěch autority (v našem případě státu), která má zajistit ochranu moji a mých práv, vlastně ani jinou možnost nemám. Domnívám se, že pokud chceme efektivně prověřovat a vyšetřovat kybernetickou trestnou činnost, kybernetické útoky a jiné negativní jevy, jež se odehrávají v kyberprostoru, tak se bez tohoto nástroje neobejdeme. Otázka, kterou bychom měli řešit, by neměla znít: „*Jak omezit sbírání údajů a dat o osobách v kyberprostoru (neboť toto se na zcela jiných úrovních děje), a tím omezit možnosti státu řešit negativní jevy v kyberprostoru?*" Otázky, které jsou zcela legitimní a které by měly být řešeny, jsou: „*Jak nastavit pravidla, komu a za jakých podmínek povolit přístup k těmto údajům, co se s těmito údaji děje, pro jaké účely mohou být využívány, atd.*"

Osobně jsem přesvědčen o tom, že podobné údaje by neměli uchovávat pouze veřejní poskytovatelé připojení, ale všichni ISP, kteří poskytují nějakou službu. Důvodů pro toto tvrzení mám několik.

Za prvé se domnívám, že ostatní služby, než ty, jež spočívají v poskytnutí připojení, jsou a do budoucna budou majoritními službami v kyberprostoru. Uživatel tak přestává řešit otázku, kdo a jakým způsobem ho připojuje, a primárně se věnuje službám, které mohou mít například i podobu virtuálního propojení do různých virtuálních prostředí. Významné tedy nebude samo fyzické propojení, jako propojování mezi jednotlivými službami.

Druhým důvodem je ta skutečnost, že v současnosti již ze strany poskytovatelů těchto služeb dochází v drtivé většině k uchovávání ne jen provozních a lokalizačních údajů, ale celé řady dalších údajů, které jim uživatelé dovolí uchovávat na základě smluvních podmínek uzavřených mezi ISP a koncovým uživatelem.[252] V kapitole 3 Anonymita uživatele hodlám demonstrovat, jaké informace a jaká data jsou o nás shromažďována, na základě našeho „souhlasu" se smluvními podmínkami.

Posledním důvodem je vlastní ochrana ISP před uživateli. Poskytovatel služby musí respektovat právo a je v jeho nejlepším zájmu uchovávat údaje, které by ho mohly případně zprostit odpovědnosti například za škodu, či jinou újmu.[253]

K uchovávání provozních a lokalizačních údajů se nedávno vyjádřil i generální advokát,[254] který konstatoval, že Data Retention představuje v mnoha případech jediný účinný nástroj k řešení bezpečnostních rizik a závažné trestné činnosti. Současně formuloval požadavky na jeho proporcionální implementaci v právních řádech členských států.

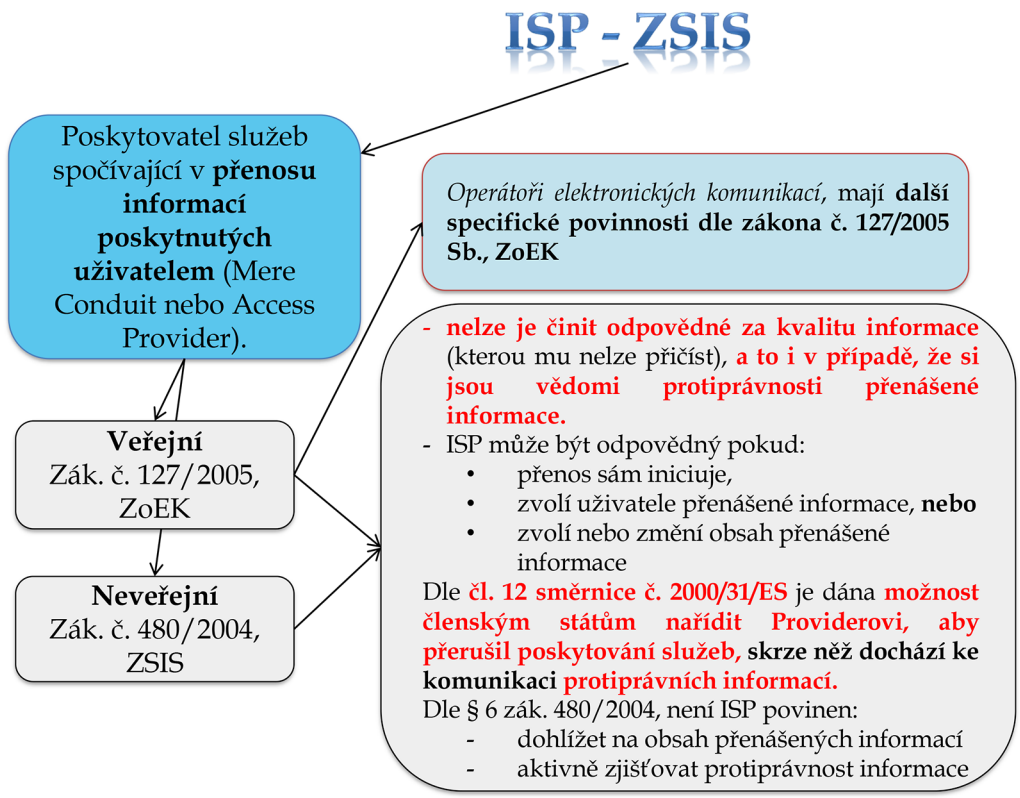
Možná jsou moje závěrečné úvahy mylné. Pokud znáte lepší způsob, jak v tomto případě zajistit

252: Typicky se jedná o 3.2 Smluvní podmínky (EULA), kterou uživatel mnohdy nevědomky uzavře.

253: Srov. viz kap. 2.4.5 Náhrada škody.

254: Stanovisko Generálního advokáta SAUGMANDSGAARD ØE, ze dne 19. 7. 2016. Ve spojených věcech C-203/15 a C-698/15. [online]. [cit. 10.8.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

zároveň ochranu společnosti a zcela, někdy až dogmaticky, dodržet některá základní lidská práva, pak rád přijmu Váš názor.




Obrázek 16: Grafické znázornění rozdělení poskytovatelů připojení a některých jejich práv a povinností

### 2.5.2 Poskytovatelé služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tzv. caching)

Caching spočívá v přenosu informací, při němž dochází automaticky dočasně k jejich meziuložení. Následně je tato informace přenesena příjemci služby na jejich žádost.

*„Caching je v podstate špecialnou upravou služby mere conduit, keďže aj ten zahŕňa prenos s prechodnym medzi-uložením informácii. Jediny rozdiel, v ktorom by služba caching mohla vybočovať z ramca široko koncipovanej mere conduit je to, že ukladanie pri prenose je vykonane na „dobu dlhšiu, ako je primerane nutne na prenos.“*[255]

Husovec dále velmi výstižně popisuje služby cachingu na příkladu proxy serveru či browseru cachingu, které urychlují načítání webových stránek. Příjemcem služby je majitel webové stránky deníku (tzv. primární příjemce), jehož obrázky si poskytovatel cachingu uloží na geograficky bližším počítači (např. v Evropě), aby nemusel neustále přistupovat na počítač, kde je v originále webová stránka uložena (např. Afrika), čímž se urychlí celkové načítání stránky (v Evropě). Uživatel, který jde webovou stránku navštívit a je dalším příjemcem služby (tzv. sekundární příjemce), tak na základě individuální žádosti adresované poskytovateli služby cachingu získá obrázek z jeho počítače a není nucen „cestovat“ na počítač originální.[256]

Poskytovatelé cachingu nejsou zbaveni odpovědnosti za kvalitu informací, pokud dojde z jejich strany k porušení standardních či smluvených technických podmínek cachingu.[257]

Poskytovatel cachingu je dle § 4 ZSIS odpovědný v případě, že:

a) změní obsah informace,
b) nevyhoví podmínkám přístupu k informaci,
c) nedodržuje pravidla o aktualizaci informace, která jsou obecně uznávána a používána v příslušném odvětví,
d) překročí povolené používání technologie obecně uznávané a používané v příslušném odvětví s cílem získat údaje o užívání informace, nebo
e) ihned nepřijme opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní, jakmile zjistí, že informace byla na výchozím místě přenosu ze sítě odstraněna nebo k ní byl znemožněn přístup nebo soud nařídil stažení či znemožnění přístupu k této informaci.

255: viz HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 133

256: Tamtéž s. 133

257: Srov. čl. 13 směrnice č. 2000/31/ES a ust. § 4 ZSIS

Srov. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 58

**Poskytovatel cachingu nemá povinnost** aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace či dohlížet na obsah jimi přenášených nebo ukládaných informací.

### 2.5.3 Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting)

Poskytováním storage nebo hostingu se rozumí zpřístupnění úložiště (prostoru) uživateli, aby si tam mohl umístit data. Ukládání informací, resp. dat, na rozdíl od mere conduit či cachingu, není pouze dočasné. Mezi služby hostingu je možné zařadit:

a) Webhosting (Active 24, Ignum, Zoner aj.)
b) Cloudová úložiště umožňující ukládání jakýchkoli souborů a dat (Dropbox, iCloud, Microsoft OneDrive, ownCloud aj.)
c) Úložiště souborů (Rapidshare, Ulož.to aj.)
d) Úložiště videí (YouTube aj.)
e) Úložiště zvukových souborů (iTunes aj.)
f) Služby internetových aukcí (eBay, Aukro aj.)
g) Blogy, fóra, diskusní chaty aj.
h) Sociální sítě (Facebook, Twitter aj.).

Uvedený výčet není konečný, v rámci hostingu může být poskytována celá řada dalších služeb.

U poskytovatelů hostingu je situace s jejich případnou právní odpovědností nejsložitější.[258] Opět se vychází z ustanovení směrnice č. 2000/31/ES, jejíž doporučení přejal český zákonodárce do § 5 ZSIS. V tomto ustanovení je dána podmínka alespoň nevědomé nedbalosti[259] poskytovatele ve vztahu k protiprávnímu obsahu informace u něj uložené. **Zákonodárce však neukládá poskytovatelům povinnost aktivně vyhledávat protiprávní informace uživatelů**[260] (neboť by v mnohých případech šlo de facto o zásah do základních práv a svobod zaručených Listinou - např. čl. 13) či dohlížet na obsah přenášených nebo ukládaných informací.

258: Srov. čl. 14 směrnice č. 2000/31/ES a ust. § 5 ZSIS

259: Srov. ust. § 16 odst. 1 písm. b) TZK

260: Srov. čl. 15 směrnice č. 2000/31/ES a ust. § 6 ZSIS

Poskytovatel hostingu je dle § 5 odst. 1 ZSIS odpovědný v případě, že:

a) ***mohl vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní**, nebo*

b) ***dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele** a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.*

Poskytovatel hostingu je vždy odpovědný za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.[261]

Pro účely této monografie byly vybrány pouze určité aspekty, které se vztahují k poskytovatelům služeb informační společnosti, zejména s ohledem na využitelnost informací v rámci odhalování a vyšetřování kybernetické kriminality a kybernetických útoků. Pokud by měl čtenář zájem se podrobněji seznámit s problematikou právní odpovědnosti jednotlivých poskytovatelů služeb informační společnosti, lze mu jen vřele doporučit publikaci: HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN: 978-80-904248-8-3.

## 2.6 Možnosti právní odpovědnosti uživatele za jednání v kyberprostoru

Řada uživatelů informačních a komunikačních systémů si neuvědomuje svoji případnou odpovědnost za zneužití těchto technologií.[262] **Informační a komunikační systémy jsou věcí a ten, kdo s nimi disponuje, je povinen si počínat při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného.**[263]

**Pokud škůdce způsobí poškozenému újmu, úmyslným porušením dobrých mravů, je povinen ji nahradit;** vykonává-li však své právo, je škůdce povinen škodu nahradit, jen sledoval-li jako hlavní účel poškození jiného.[264]

261: § 5 odst. 2 ZSIS

262: Pro tuto část textu byly použity teze, jež byly částečně uveřejněny v článku: KOLOUCH, Jan a Andrea KROPÁČOVÁ. Liability for Own Device and Data and Applications Stored therein. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC'14).* [B.m.], c2014, s. 321–324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

263: § 2900 OZ

264: § 2909 a násl. OZ

Z této dikce občanského zákoníku tak jednoznačně vyplývá jednak povinnost řádně spravovat informační a komunikační systémy, stejně jako povinnost předcházet škodám, které by z jeho činnosti (tedy i užívání ICT v prostředí Internetu) mohla vzniknout.

Řada běžných uživatelů podceňuje ochranu a zabezpečení prostředků ICT, jimiž disponují, ať již z nedbalosti či úmyslně.

Určení formy zavinění u jednání koncového uživatele má rozhodující význam pro možnou občansko, či trestněprávní odpovědnost. Toto tvrzení je možné demonstrovat na třech ilustrativních případech z praxe.

*Uživatel osobního počítače využíval nelegální kopii operačního systému Windows XP SP. 2, přičemž tento systém úmyslně neaktualizoval. Uživatel úmyslně nainstaloval do počítače programy, které umožňovaly manipulaci s tímto počítačem třetím osobám, bez jeho další součinnosti.*

Smyslem činnosti výše popsaného uživatele bylo zprostit se případné trestněprávní odpovědnosti za útok provedený prostřednictvím takto připraveného počítače jinou osobou (např. počítač je úmyslně součástí sítě botnet).

V praxi je možné se setkat právě s útočníky, kteří svoji obhajobu staví na faktu, že oni nebyli tou osobou, která provedla prostřednictvím daného počítače konkrétní útok.

Vyvinění se tvrzením, že daná osoba není přímým útočníkem a svým jednáním konkrétní útok nezpůsobila, není dle mého názoru možné, respektive není možné toto tvrzení přijmout absolutně.

Z hlediska trestního práva by v úvahu mohlo přicházet minimálně uplatnění institutu účastenství a zásady akcesority účastenství,[265] neboť jednání osoby, která umožnila nebo usnadnila jinému spáchání trestného činu (zejména opatřením prostředků, odstraněním překážek, vylákáním poškozeného na místo činu, hlídáním při činu, radou, utvrzováním v předsevzetí nebo slibem přispět po trestném činu) je možné subsumovat pod ustanovení o pomocníkovi.[266] Opatřením prostředků by se v tomto případě rozumělo i zpřístupnění počítačového systému, či jeho části ke spáchání úmyslného trestného činu.

Pokud by byla prokázána vyšší míra přímé účasti uživatele na protiprávním jednání jiné osoby, bylo by možné takovéhoto uživatele považovat případně i za spolupachatele[267] trestného činu.

265: Jedná se o zásadu závislosti trestní odopovědnosti a trestnosti účastníka (viz § 24 TZK) na trestní odpovědnosti a trestnosti hlavního pachatele (viz § 22 TZK), za podmínky, že se hlavní pachatel dospustil alespoň pokusu trestného činu, na němž se účastník podílel.

266: Za podmínky domluvy (dohody) účastníka a hlavního pachatele. Viz § 24 odst. 1 písm. c) TZK

267: Viz § 23 TZK

Rozhodující by byla míra informovanosti o využívání daného počítače k protiprávnímu činu a dále pak srozumění s tím, že touto činností může dojít k porušení nebo ohrožení zájmů chráněného trestním zákonem.[268]

Z hlediska občanského práva by pak jednání takového uživatele bylo jednak možné subsumovat pod § 2909 OZ, případně by bylo možné využít i § 2915 OZ, který upravuje případ, kdy je škoda způsobena několika osobami. Toto ustanovení stanoví, že: *„je-li k náhradě zavázáno několik škůdců, nahradí škodu společně a nerozdílně; je-li některý ze škůdců povinen podle jiného zákona k náhradě jen do určité výše, je zavázán s ostatními škůdci společně a nerozdílně v tomto rozsahu.* ***To platí i v případě, že se více osob dopustí samostatných protiprávních činů, z nichž mohl každý způsobit škodlivý následek s pravděpodobností blížící se jistotě, a nelze-li určit, která osoba škodu způsobila.*** " Právě větu druhou § 2915 odst. 1) OZ lze, dle mého názoru, velmi dobře aplikovat na výše popsaný případ.

*Uživatel osobního počítače využíval nelegální kopii operačního systému Windows VISTA, přičemž tento systém úmyslně neaktualizoval. V počítači měl nainstalovánu řadu her a jiných aplikací, u nichž došlo k porušení práv autorských zejména tím, že byly obcházeny či potlačovány prvky jejich ochrany a k instalaci bylo využito keygenů či cracků,*[269] *které však v sobě obsahovaly malware jiných útočníků. Uživatel si nebyl vědom té skutečnosti, že jeho počítač je využíván jinými uživateli.*

V praxi se jedná o nejčastější případ, při němž dochází ke zneužití počítače bez vědomí jeho oprávněného uživatele, i když tento svým protiprávním jednáním (zejména porušování práva autorského) či z prosté neznalosti výpočetní techniky zapříčinil stav, že jeho počítač je zneužit k útoku na třetí osoby.

Z hlediska trestního práva není v tomto případě možné využít institutu účastenství a zásady akcesority účastenství, neboť jednání osoby, která umožnila nebo usnadnila jinému spáchání trestného činu, nebylo úmyslné, tudíž nesměřovalo k pomoci hlavnímu pachateli trestného činu.

Z hlediska zavinění by bylo na uživatele takto napadeného počítače možné aplikovat ustanovení týkající se nedbalosti nevědomé, neboť pachatel nevěděl, že svým jednáním může způsobit porušení nebo ohrožení zájmu chráněného trestním zákonem, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl.[270]

268: Viz § 15 odst. 1 písm. b) TZK

269: Jde o zásahy do programů jinými osobami za účelem modifikace směřující ke snadnějšímu spuštění (keygenů), ochromení ochrany programu, která zabraňuje jeho kopírování či spuštění za předem daných podmínek (cracky) a další přepracovávání těchto programů směřující k následnému užívání, případně distribuci dalším osobám. Viz např. kap. 4.3 Malware; 4.9 Cracking.

270: Viz § 16 odst. 1 písm. b) TZK

Vzhledem k tomu, že v trestním zákoníku neexistuje nedbalostní skutková podstata trestného činu dle § 230 TZK: *Neoprávněný přístup k počítačovému systému a nosiči informací*, nebude možné využít v tomto konkrétním případu institutů trestního práva.

Z hlediska občanského práva by pak jednání takového uživatele, bylo možné subsumovat pod § 2912 odst. 1 OZ: *„Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale.*" V této souvislosti je třeba připomenout, že ten, kdo škodu způsobil (škůdce), je povinen škodu nahradit, a to bez ohledu na své zavinění v případech stanovených zvlášť zákonem.[271]

*Uživatel o svůj počítač adekvátně „pečuje" (má legální software, aktualizuje jej aj.) a rozumně jej zabezpečil (používá antivirovou, antispamovou a antimalware ochranu a kontrolu), a přesto byl tento počítač napaden zvenčí, (např. zapojen do botnetu) a následně využit k útoku proti jinému.*

Domnívám se, že z hlediska zavinění by v tomto případě nebylo možné na uživatele takto napadeného počítače aplikovat ani ustanovení týkající se nedbalosti nevědomé. Vzhledem k proaktivní činnosti uživatele pak nepřichází v úvahu ani aplikace § 232 TZK: *Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti*, neboť v tomto ustanovení je vyžadována hrubá nedbalost.[272]

Z hlediska občanského práva by pak jednání takového uživatele dle mého názoru nebylo možné subsumovat pod dříve uvedený § 2912 odst. 1 OZ, neboť v tomto případě jednal uživatel tak, jak od něj lze spravedlivě požadovat. Toto je však třeba chápat šířeji, neboť pokud se uživatel dozví, že jeho prostředky ICT jsou zneužity k protiprávnímu útoku na jiného, je povinen toto bez zbytečného odkladu oznámit osobě, které z toho může újma vzniknout,[273] a upozornit ji na možné následky. Splní-li oznamovací povinnost, nemá poškozený právo na náhradu té újmy, které mohl po oznámení zabránit.[274]

V konkrétním případu vždy bude záležet na všech okolnostech případu a povinnost náhrady škody je oprávněn stanovit pouze soud.

Na druhou stranu, pokud se uživatel o počítač „nestará" (tj. nezabezpečí jej, neprovádí údržbu aj.) a ten bude následně zneužit, je reálné, že soud v řízení o náhradě škody určí takovémuto uživateli povinnost částečně či zcela (např. dojde k využití výpočetního výkonu jednoho datového centra) saturovat poškozenému škodu, která mu byla prostřednictvím počítače uživatele způsobena.

271: Viz § 2895 OZ

272: Viz § 16 odst. 2 TZK: *„Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem."*

273: Je otázkou, zda je možné takovouto osobu v daný okamžik (okamžik útoku) reálně určit.

274: Viz § 2092 OZ

# 3 Anonymita uživatele

## 3 Anonymita uživatele

Žít v digitální době s představou či pocitem, že mé jednání je anonymní či skryté před zraky jiných uživatelů,[275] je dle mého názoru naivní. S nástupem doby digitální se neobjevují pouze její pozitivní, ale i negativní aspekty.[276] Jedním z těchto negativ je i ta skutečnost, že se čím dál méně zajímáme o podstatu fungování služeb poskytovaných v kyberprostoru.

Náš svět, který stále častěji chápeme jako „svět informací" či „svět Internetu", je pevně spojen s informačními a komunikačními technologiemi, které zasahují do života jedince velmi výrazným způsobem. Tyto technologie usnadňují přístup k informacím a zjednodušují či zrychlují vzájemnou komunikaci mezi jednotlivými uživateli atd. Na straně druhé je však třeba si uvědomit, že jakékoli uveřejnění informací z našeho soukromí na Internetu je rizikem, kterého může v kyberprostoru kdokoliv zneužít.

Veškeré aplikace, ať už jsou využívány v jakémkoli počítačovém systému, webové služby[277] a zejména sociální sítě,[278] shromažďují o svých uživatelích značné množství informací, které majoritně nepotřebují ke svému fungování, ale které jednak umožňují dotyčnému ISP poskytovat službu „zadarmo", a jednak „cílit" či modifikovat jím nabízené služby. Mezi informace, které standardně nejsou nezbytně nutné k přímé funkčnosti jednotlivých služeb, patří například informace mající povahu **osobních** (jméno, příjmení, e-mailová adresa, telefonní číslo, bydliště aj.), **citlivých**[279] (např. informace o využívaném operačním systému počítače, verzích jednotlivých aplikací, soubory cookies aj.), **lokalizačních údajů** (souřadnice GPS, informace o WiFi, GPRS aj.), provozních údajů aj.[280]

Uvedené informace mohou být využity značně různorodě. Poskytovatel služby může dle těchto informací nabízet např. doplňkové služby či reklamu na základě požadavků, zájmů či zálib uživatelů. Policie je díky nim schopna vytvořit rámec denní činnosti osoby, která se například ztratila či byla unesena, a tím urychlit vlastní činnost při pátrání po této osobě. Zároveň však tyto

275: Pod pojmem uživatel zahrnuji veškeré subjekty, které svým působením ovlivňují dění v kyberprostoru. Primárně je potřeba do této skupiny zařadit **ISP**. Ne všichni ISP však spadají do jurisdikce českého práva (ať již z důvodů geolokačních, či spíše proto, že jejich činnost není právní normou upravena). Dalšími „uživateli" pak bezesporu budou **LEA** (Law Enforcement Agencies - jimž právní normy jednotlivých zemí umožňují jeden z nejintenzivnějších zásahů do základních lidských práv a svobod), **CERT/CSIRT týmy, správci IT oddělení, koncoví uživatelé (end user) aj.**

276: Např. kyberkriminalita, závislosti a mimo jiné i tzv. digitální demence. Blíže viz: SPITZER, Manfred. *Digitální demence.* Brno: Host, 2014. ISBN 978-80-7294-872-7

277: Viz např. *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají možnost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit. 4.4.2014]. Dostupné z: https://www.google.cz/intl/cs/policies/?fg=1

278: Viz *Prohlášení o právech a povinnostech.* [online]. [cit. 4.4.2014]. Dostupné z: https://www.facebook.com/legal/terms

279: Pojem citlivý údaj zde je uveden v kontextu bezpečnosti, nikoli s odkazem na § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů.

280: **Některé autentizační systémy přesto potřebují pro svoji funkčnost i tyto uvedené doplňkové informace.**

informace mohou být velmi jednoduše zneužity pachateli trestné činnosti, ať již pro navázání kontaktu s obětí, či k naplánování činu samotného.

Poskytnutím (byť i nedobrovolným či nevědomým) těchto údajů umožňuje uživatel dané služby získat jiným osobám důležité informace o svém životě (např. informace o svém chování v průběhu dne, navštěvovaných místech, aktivitách a osobách, se kterými je v kontaktu).[281] V tento okamžik **se sami stáváme informací či komoditou, se kterou může někdo jiný obchodovat**.

Různé dostupné statistiky[282] uvádějí, že v současnosti je celková populace přibližně 7,4 miliard lidí. Z tohoto počtu zhruba 3,6 miliardy lidí jsou aktivními uživateli Internetu a více než 2,1 miliardy lidí jsou aktivní uživatelé sociálních sítí. Mobilní zařízení vlastní více než 3,6 miliardy uživatelů a k sociálním sítím se přes tato zařízení připojuje více než 1,7 miliardy uživatelů. Sociálním sítím vévodí Facebook s více než 1,59 miliardami uživatelů:[283]

V této části publikace se pokusím upozornit na možné bezpečnostní hrozby, které jsme si zvykli de facto přijímat či nevnímat a u kterých si většina jedinců či organizací vůbec neuvědomuje možné nebezpečí.

## 3.1 Digitální stopa

Uvedené hrozby, či spíše rizika, spočívají velmi často v zanechávání digitálních stop v kyberprostoru. Digitální stopy, na základě toho, zda mohou, či nemohou být ovlivněny uživatelem, je obecně možné **rozdělit na stopy ovlivnitelné a neovlivnitelné**.

281: KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN a Terezie JANÍKOVÁ. neBezpečné chování na Facebooku. In: *Sborník příspěvků ke konferenci: Sociální sítě. Mobilní aplikace*. Plzeň: Západočeská univerzita v Plzni, 2014, s. 39–47. ISBN 978-80-261-0362-2 s. 40

282: Blíže viz např.: *World Internet Users and 2015 Population Stats*. [online]. [cit. 9.8.2015]. Dostupné z: http://www.internetworldstats.com/stats.htm

*Digital, Social & Mobile Worldwide in 2015*. [online]. [cit. 9.8.2015]. Dostupné z: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015

*Největší sociální sítě na světě? Facebook je sice jednička, ale…* [online]. [cit. 10.8.2015]. Dostupné z: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

*Current World Population.* [online]. [cit. 10.8.2015]. Dostupné z: http://www.worldometers.info/world-population/

283: *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions)* [online]. [cit. 10.8.2015]. Dostupné z: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Dělení digitálních stop:

- **Digitální stopa neovlivnitelná**
  - Informace z počítačového systému;
  - připojení k počítačovým sítím, zejména Internetu;
  - využívání poskytovaných služeb aj.

- **Digitální stopa ovlivnitelná**
  - vědomé využití služeb;
  - dobrovolné zveřejnění informace
    - blogy, fóra,
    - sociální sítě,
    - e-mail,
    - datová úložiště,
    - cloudové služby aj.

V následující části se budu věnovat některým aspektům jednotlivých digitálních stop a informacím v nich obsažených. Smyslem je upozornit uživatele na to, že jeho jednání v prostředí informačních a komunikačních systémů není tak anonymní, jak si možná myslí.

Ve světě ICT platí jedno pravidlo: **pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy"**. Vždy bude existovat kopie (vzniklá na základě funkcionality počítačového systému či kopie uložená některým jiným uživatelem) vašich dat. A i když tato data následně odstraníte (či je odstraní někdo jiný), k jejich skutečnému, trvalému a nezvratnému odstranění nedojde. Je proto vhodné věnovat pozornost své digitální stopě a informacím či datům, jež za sebou v prostředí kyberprostoru zanecháváme.

### 3.1.1 Digitální stopa neovlivnitelná

Neovlivnitelné stopy nejčastěji vznikají na základě interakce jednoho počítačového systému s počítačovým systémem jiným nebo na základě funkčnosti počítačového systému (a přidruženého software). Příkladem těchto stop mohou být informace z operačního sytému (např. hlášení o chybách systému Windows či systémové informace), nebo další informace a data, jež jsou ukládány na základě funkčnosti tohoto systému, aniž by muselo dojít k jejich předání (např. počítačový systém nebyl nikdy připojen k žádné síti či jinému počítačovému systému).[284] Tvrdit

284: Neboli převážně informace, které se o činnosti uživatelů logují a archivují na místech, k nimž nemá uživatel přístup a nemá je pod kontrolou [např. uživatel není schopen smazat logy prokazující jeho aktivitu (např. přístup, odesílání e-mailu aj.) na mail serveru]. Na vlastním počítači může uživatel ovlivňovat uložená data a informace. Je oprávněn mazat (např. historii, e-maily aj.), editovat aj.

zcela nekompromisně, že nelze tyto stopy ovlivnit, by nebylo zcela korektní. V případě, že je uživatel dostatečně zkušený, je schopen celou řadu „neovlivnitelných" digitálních stop pozměnit, maskovat nebo potlačit (např. prostým anonymním režimem webového prohlížeče, který vypne cookies). Nicméně pohyb uživatele po Internetu se dá sledovat nejrůznějšími způsoby.

### IP adresa

Připojení počítačového systému k Internetu je typickým příkladem relativně neovlivnitelné stopy využívající IP adresu či MAC adresu, které jsou předávány spolu s dalšími informacemi ISP. V kapitole 1.3.2 Internet Protocol a IP adresa bylo uvedeno, že IP adresa není standardně anonymní a počítačový systém ji využívá při komunikaci s jinými počítačovými systémy jakožto jeden z identifikátorů. IP adresy jsou přidělovány hierarchicky, přičemž dominantní roli zde má **ICANN**,[285] který rozdělil reálný svět na regiony, nad nimiž vykonávají správu regionální internetoví registrátoři (**RIR - Regional Internet Registry**). Tito registrátoři dostali od ICANN přidělen určitý rozsah IP adres, které přidělují LIRům v rámci svého regionu. Regionální registrátoři jsou rozděleni do následujících pěti teritorií:

1) „Euro-asijská" oblast - RIPE NCC: https://www.ripe.net/
2) „Asijsko pacifická" oblast – APNIC: https://www.apnic.net/
3) „Severo-americká" oblast – ARIN: https://www.arin.net/
4) „Jiho-americká" oblast – LACNIC: http://www.lacnic.net/
5) „Africká" oblast – AFRINIC: http://www.afrinic.net/


Obrázek 17: Rozdělení světa mezi RIR

285: Viz 1.2.1 Kyberprostor (Cyberspace) a 2.5 Odpovědnost poskytovatele služeb informační společnosti.

Regionální registrátoři[286] provozují na svých stránkách službu Whois, což je označení pro databázi, v níž jsou evidovány údaje o držitelích IP adres. Tyto databáze obsahují celou řadu informací, na jejichž základě je možné identifikovat např. rozsah používaných veřejných IP adres, kontaktní údaje, abuse kontakt,[287] hierarchicky nadřazeného poskytovatele připojení aj. K vlastnímu zjištění „vlastníka" (operátora, poskytovatele) konkrétní IP adresy je mnohdy možné využít právě těchto volně dostupných databází.[288]

```
Responsible organisation: Policejni akademie CR v Praze
Abuse contact info: abuse@polac.cz

inetnum:         195.113.149.160 - 195.113.149.175
netname:         POLAC-TCZ
descr:           Policejni akademie CR
descr:           Prague 4
country:         CZ
org:             ORG-PACV1-RIPE
admin-c:         PACV1-RIPE
tech-c:          PACV1-RIPE
status:          ASSIGNED PA
mnt-by:          TENCZ-MNT
remarks:         Please report network abuse -> abuse@polac.cz
created:         2014-09-02T14:06:09Z
last-modified:   2014-09-02T14:06:09Z
source:          RIPE

route:           195.113.0.0/16
descr:           CESNET-TCZ
origin:          AS2852
mnt-by:          AS2852-MNT
remarks:         Please report abuse -> abuse@cesnet.cz
created:         1970-01-01T00:00:00Z
last-modified:   2006-06-26T14:36:38Z
source:          RIPE
```

Obrázek 18: Výpis informací z databáze RIR

286: *Regional internet registries.* [online]. [cit. 4.8.2015]. Dostupné z: https://www.nro.net/about-the-nro/regional-internet-registries

287: Jedná se o kontakt, na nějž se uživatel může obrátit, pokud je mu z dané IP adresy, nebo rozsahu adres způsobována újma (dochází např. ke kybernetickému útoku v podobě spamu, phishingu aj.). Jde o kontakt nejbližší zdroji útoku.

288: Nejedná se však o databáze jediné. Existuje celá řada služeb, jež nabízejí stejné informace. Jako příklad uvádím i další databáze: http://whois.domaintools.com/; https://www.whois.net/; http://www.nic.cz/whois/; https://whois.smartweb.cz/ aj.

Regionální registrátoři dále rozdělují přidělené IP rozsahy mezi lokální internetové registrátory (**LIR - Local Internet Registry**). Lokálním registrátorem je zpravidla ISP (v ČR poskytovatel služeb informační společnosti, konkrétně pak poskytovatel připojení, ať veřejný, či neveřejný). Tento registrátor pak může dále svůj rozsah IP adres poskytnout například části své organizace či jiným subjektům.

Na zkráceném výběru z databáze RIR je zobrazen LIR (v tomto případě CESNET, z.s.p.o. využívající rozsah IP adres: 195.113.0.0/16) a organizace, jíž CESNET přidělil část veřejných adres [Policejní akademie ČR s rozsahem IP adres 195.113.149.160–195.113.149.175. Policejní akademie pak opět může rozdělit tyto adresy mezi další části organizace (např. fakulty, laboratoře, či jiné sub sítě, jež spravuje)]. Dle IP adresy a přesného času je možné na základě hierarchického přidělování adres určit konkrétní počítačový systém.[289] Informace o připojení koncového počítačového systému (zdroje) k cílovému počítačovému systému (např. připojení počítače k Internetu a zobrazení si požadované webové stránky) jsou uchovávány jednotlivými ISP v rámci celé cesty mezi zdrojem a cílem.

Díky přísným pravidlům definujícím hospodaření s IP adresami a veřejně přístupnými databázemi RIRů, které obsahují informace o držitelích jednotlivých adresových bloků, je možné velmi rychle zjistit, do které sítě patří určitá IP adresa a kdo danou síť provozuje. Provozovatel dané sítě pak díky logování informací ze síťového provozu dokáže identifikovat, kdo (respektive jaký počítačový systém) v konkrétním čase používal konkrétní IP adresu. Toto určení je velmi důležitým zdrojem informací při řešení bezpečnostních incidentů (kybernetických útoků) a při pátrání jejich po zdroji (původci).

### E-mail

E-mail jakožto jedna z nejčastěji využívaných služeb v prostředí Internetu rozhodně není anonymní službou. Zpráva, která je odeslána od zdroje k cíli (adresátovi), v sobě typicky nese celou řadu informací, které mohou identifikovat jednak poskytovatele služby (e-mailu), tak i poskytovatele připojení zařízení, z nějž byl e-mail odeslán. Tyto informace nejsou zobrazeny v těle zprávy (tedy textu, který odesíláme konkrétní osobě), ale ve zdrojovém kódu (hlavičce) zprávy. Z toho zdrojového kódu je například možné zjistit cestu přes servery, skutečného odesílatele, zdrojové jméno počítače, název počítače, čas odeslání zprávy (včetně časové zóny) používaný operační systém, mailového klienta aj. Níže je uvedený příklad hlavičky přeposlaného[290] podvodného e-mailu s vyznačením potenciálně zajímavých informací.

289: Viz kap. 1.4 ISP (Internet Service Provider).

290: e-mail byl přeposlán z adresy: jan.kolouch@fit.cvut.cz na e-mail: kyber.test@seznam.cz

```
X-Account-Key: account1
X-UIDL: 7
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Received: from relay.fit.cvut.cz (relay.fit.cvut.cz [147.32.232.237])
    by email-smtpd5.ko.seznam.cz (Seznam SMTPD 1.3.4) with ESMTP;
    Wed, 19 Aug 2015 15:14:16 +0200 (CEST)
Received: from imap.fit.cvut.cz (imap.fit.cvut.cz [IPv6:2001:718:2:2901:0:0:0:238])
    by relay.fit.cvut.cz (8.15.2/8.15.2) with ESMTP id t7JDE1Mm072888
    for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
Received: from PCP[redacted] (cust-178.17.4.174.uvt.cz [178.17.4.174] (may be forged))
        (authenticated bits=0 as user ko[redacted])
        by imap.fit.cvut.cz (8.15.2/8.15.2) with ESMTPSA id t7JDE139012575
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
        for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
X-Authentication-Warning: imap.fit.cvut.cz: Host cust-178.17.4.174.uvt.cz [178.17.4.
From: "JUdr. Jan Kolouch, Ph.D." <jan.kolouch@fit.cvut.cz>
To: <kyber.test@seznam.cz>
References: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
In-Reply-To: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
Subject: =?UTF-8?Q?FW:_Chci=2C_aby_partner_s_v=C3=A1mi_na_?=
    =?UTF-8?Q?tomto_projektu?=
Date: Wed, 19 Aug 2015 15:14:15 +0200
Message-ID: <006901d0da80$f3599db0$da0cd910$@fit.cvut.cz>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_006A_01D0DA91.B6E2BBD0"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQDP5b3kQbONWI2VUUpIa1oprzeNE6AVNk1w
Content-Language: cs
X-FIT-MailScanner-ID: t7JDE1Mm072888
X-FIT-MailScanner: Found to be clean
X-FIT-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-0.381, required 7, autolearn=not spam, RP_MATCHES_RCVD -0.38)
X-FIT-MailScanner-From: jan.kolouch@fit.cvut.cz
X-FIT-MailScanner-Watermark: 1440594843.20583@MBoaO3F9jzMModBIjGdzYg
```

Obrázek 19: Zobrazení informací z hlavičky e-mailové zprávy

### Web browser

Webový prohlížeč je další aplikací, která standardně předává informace o uživateli a jeho počítačovém systému, počítačovému systému (serveru) navštívené stránky. Tento server pak v rámci dotazu od klienta zjistí například referer (což je stránka, ze které uživatel přichází), používaný webový prohlížeč a operační systém (včetně přesné verze), cookies, flash cookies, historie, cache aj.

Kromě IP adresy jsou to právě mimo jiné i soubory cookies,[291] jež pomáhají vytvořit „otisk" („fingerprint") uživatelova počítačového systému (počítače, smartphonu aj.). Tento otisk umožňuje

291: V protokolu HTTP označuje pojem cookie malé množství dat, která odešle navštěvovaný webserver (zjednodušeněji: navštěvovaná webová stránka) webovému prohlížeči, který je následně uloží na počítači uživatele. Tato data jsou pak zpětně posílána webovému serveru, při každém navštívení téhož serveru.

určit konkrétní počítačový systém,[292] a to i v případě, že uživatel používá jiný webový prohlížeč, či promaže cookies, přihlašuje se z jiné IP adresy, atd.

Jeden z mnoha v současnosti požívaných způsobů tvorby „fingerprintingu" je canvas fingerprinting.[293] Canvas fingerprinting funguje tak, že navštívený webserver nařídí webovému prohlížeči uživatele „nakreslit skrytý obrázek". Tento obrázek je unikátní pro ten který webový prohlížeč a počítačový systém. Nakreslený obrázek je pak převeden do ID kódu, který je na webovém serveru uchován pro případ, že by jej uživatel navštívil znovu.[294]


Obrázek 20: Ukázka Canvas Fingerprintingu

Kromě fingerprintingu je u webového prohlížeče dále zajímavé sledovat předávání informací třetím stranám (jak subjektům, tak službám, které informace o uživateli mohou dále využít). Toto předávání se standardně děje na základě smluvních podmínek uzavřených s ISP. Každý koncový uživatel může například využít aplikaci Light Beam,[295] která zobrazí všechny stránky, se kterými na webu uživatel (mnohdy nevědomky) komunikuje (dochází k předávání dat třetím stranám). Předávání informací o uživatelích třetím stranám rozhodně není něco výjimečného. Naopak v digitálním světě se jedná o samozřejmost a „nezbytný předpoklad" pro fungování řady ISP.

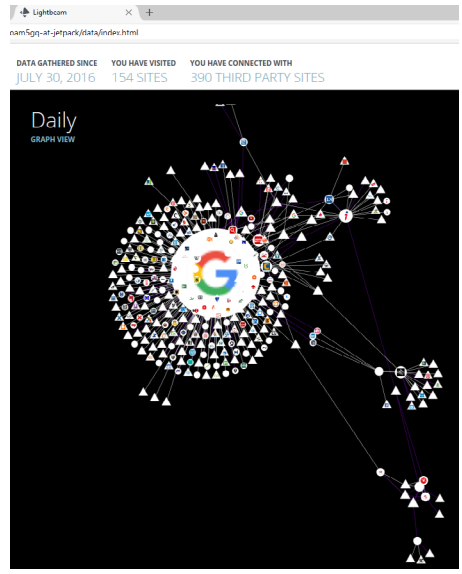
292: Pokud si chce uživatel zjistit více informací o tom, co o jeho činnosti prozrazuje webový prohlížeč, doporučuji následující URL: http://panopticlick.eff.org , http://browserspy.dk/, http://samy.pl/evercookie.

293: ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit. 10.6.2016]. Dostupné z: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

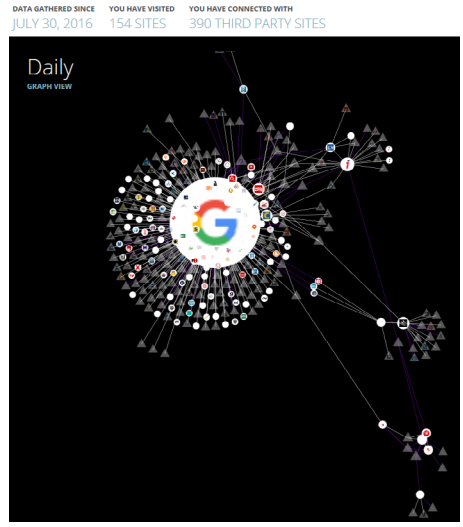
294: Ukázka Canavas fingerprintingu. Test, ukazující otisk Vašeho webového prohlížeče, je možné vyzkoušet v rámci článku ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit. 10.6.2016]. Dostupné z: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

295: Aplikace umožňuje grafické zobrazení propojování jednotlivých služeb a předávání informací třetím stranám. Jedná se o doplněk webového prohlížeče Firefox, který je dostupný na: https://www.mozilla.org/en-US/lightbeam/.

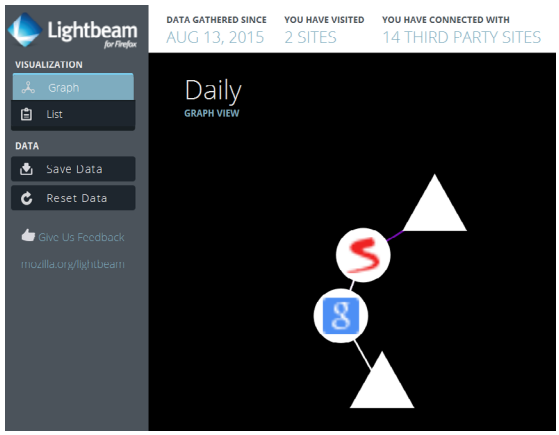
1) První snímek zobrazuje činnost Firefoxu za období od 30. července 2016 do 4. srpna 2016. V daném období došlo k navštívení 154 stránek a došlo k propojení na **390 stránek třetích stran**.




2) Druhý printscreen zobrazuje stejnou mapu, avšak odfiltrovává stránky třetích stran, které jsou znázorněny pomocí trojúhelníků.



3) Poslední printscreen zobrazuje aplikaci LightBeam po vyčištění a zobrazení následujících stránek: www.seznam.cz; www.google.com.




## Ostatní aplikace

V následující části textu se částečně zaměřím na smart devices (smartphone, tablet aj.) a aplikace spojené s vlastní činností „smart devices". Cíleně si vybírám právě tato zařízení, neboť se jedná o počítačové systémy, do kterých uživatelé instalují asi největší množství programů (velmi často neověřených, pouze doporučených „kamarádem"). Právě tato zařízení, která mimo jiné i díky smluvním podmínkám, nemusí být pod plnou kontrolou uživatele, administrátora aj., představují bezpečnostní riziko a to jak pro uživatele koncového, tak pro společnost (organizaci).

Z již dříve zmíněného statistického průzkumu[296] vyplývá, že průměrně strávíme na Internetu: 4,4 hod. (přístup přes počítač v podobě stolního PC či notebooku aj.) a 2,7 hod (přístup skrze mobilní zařízení) denně. V případě počítače je zpravidla bezpečnost zařízení zajištěna, avšak mobilní zařízení (smartphone, tablet aj.) běžně nemají nastavené politiky týkající se možné instalace software (ať již z důvěryhodných, či nedůvěryhodných zdrojů) a mnohdy chybí i základní ochrana v podobě antivirového programu.[297]

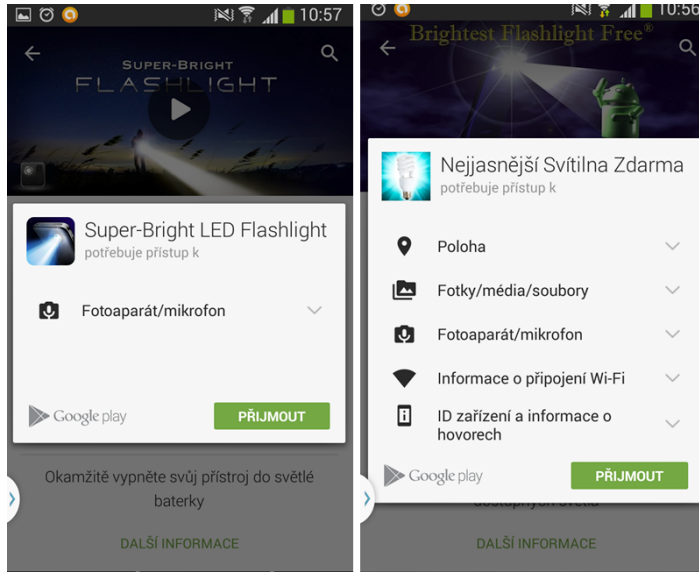
296: *Digital, Social & Mobile Worldwide in 2015.* [online]. [cit. 9.8.2015]. Dostupné z: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015

297: Přičemž je třeba uvést, že např. ze zprávy vydané společností Kaspersky Lab vyplývá, že existuje více než 340 000 druhů malware určeného primárně pro mobilní zařízení. Kaspersky Lab dále uvádí, že 99 % tohoto malware cílí na zařízení s operačním systémem Android. Je třeba uvést, že toto cílení je naprosto pochopitelné, neboť variabilita jednotlivých zařízení a verzí OS Android je značná (některé zprávy uvádí, že Android OS využívá více jak 24 000 druhů různých zařízení). Blíže viz např.: *The very first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cit. 1.8.2016]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
Dále: *Interesting Statistics On Mobile Strategies for Digital Transformations*. [online]. [cit. 15.7.2016]. Dostupné z: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/
*The fragmentation of Android has new records: 24 000 different devices*. [online]. [cit. 15.7.2016]. Dostupné z: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

Koncový uživatel si právě primárně do zařízení s OS Android má možnost nainstalovat software, který bude předávat (dalším subjektům) a uchovávat informace o jeho činnosti, a to včetně uchování a předání obsahu přenášených informací. Služba Obchod Play, která je společností Google v rámci OS Android poskytována, umožňuje jakémukoli vývojáři nastavit pravidla toho, co má daná aplikace např. sbírat a kam má tato data posílat.

Osobně se domnívám, že není chybou umožňovat vývojářům a tvůrcům aplikací získávat dostatečné informace o svých aplikacích, jejich funkčnosti atd. Pokud bychom sběr těchto informací regulovali, pak nepochybně budeme regulovat a brzdit možný pokrok a následný vývoj těchto a jiných aplikací. Na straně druhé však stojí útočníci, kteří díky tomu, že ve službě Obchod Play nedochází k ověřování a prověřování aplikací, mohou nabízet malwarem infikované aplikace, po jejichž instalaci do koncového počítačového systému může dojít například i k získání kontroly nad smartphonem koncového uživatele.[298]

Problém je v tomto případě, dle mého názoru, jak na straně poskytovatele služby Obchod Play, kde chybí kontrola aplikací, tak samozřejmě především na straně uživatele, který nezjišťuje, komu a v jaké míře svěřuje informace s tímto zařízením spojené. Příkladem disproporce sběru informací o uživatelích je např. aplikace svítilna. Obě následující aplikace jsou v TOP 5 svítilen dostupných ve službě Obchod Play, přičemž *„Nejjasnější svítilna zdarma"* se umístila na prvním místě (rating je určen uživateli).[299]




Obrázek 21: Ukázka požadovaných oprávnění od dvou různých aplikací "svítilna"

298: viz kap. 4.3 Malware.

299: Vysvětlení přístupu k Fotoaparát/mikrofon: Blesk v zařízení s Android OS je spravován službou, ovládající současně fotoaparát a mikrofon. Printscreen pořízen ze zařízení autora.

Z přiložených printscreenů je zřejmé, že informace o uživatelích může velmi snadno získat jakákoli osoba, na jejíž smluvní podmínky uživatel přistoupí.

#### Určení počítačového systému na základě informací z jeho komponent

Jedním z unikátních, avšak za určitých okolností změnitelných, identifikátorů počítačového systému, je MAC adresa, která je pevně svázána se síťovou kartou počítačového systému.[300] Síťová karta není však jedinou hardwarovou komponentou, která je schopna předávat unikátní identifikátor počítačového systému jinému počítačovému systému.

Vědci z Princenton University zjistili, že počítačový systém je možné identifikovat například i na základě informací o baterii tohoto systému, přičemž webové prohlížeče jsou nezbytnou součástí předávání těchto informací.[301]

V praxi je užíván postup, který využívá možnosti HTML5. Součástí tohoto standardu je totiž funkce, která umožňuje webovým stránkám (resp. web serveru) zjistit stav baterie počítačového systému, který na ně přistupuje (předávány jsou informace o tom, kolik procent baterie zbývá, za jak dlouho se přibližně vybije nebo nabije). Představa vlastníků web serverů je taková, že uživateli, kterému se vybíjí baterie, bude zobrazena úsporná verze webové stránky. Dva skripty, které popsali právě vědci z Princeton University, data o baterii už skutečně využívají, zároveň sbírají další informace - například IP adresu nebo otisk z canvas fingerprinting. Takové kombinace už mohou poskytnout velmi přesnou identifikaci počítačového systému.[302]

### 3.1.2 Digitální stopa ovlivnitelná

Digitální stopa ovlivnitelná představuje veškeré informace, které o sobě uživatel sám dobrovolně předá jiné osobě (ať fyzické či právnické, nebo i např. ISP). Pod pojmem předání si je třeba představit celou řadu činností, které mohou spočívat například v odeslání e-mailu, přidání příspěvku do diskuse, fóra, zveřejnění jakýchkoli médií (foto, video, audio aj.) v rámci sociálních sítí, atd. Dále pod tento pojem spadají i registrace a využívání všech představitelných služeb v rámci kyberprostoru [např. operační systémy, e-maily (včetně freemailu), sociální sítě, seznamky, P2P sítě, chaty, blogy, BBS, webové stránky, cloudové služby, datová úložiště aj.].

Digitální stopy ovlivnitelné jsou stopami, nad kterými může mít uživatel relativní kontrolu a je pouze na něm, jaké informace o sobě hodlá zpřístupnit jiným. Je však třeba upozornit na již uve-

300: Blíže viz kap. 1.3.3 MAC Adresa.

301: Blíže viz ENGLEHARDT, Steven a Ardvin NARAYANAN. *Online tracking: A 1-million-site measurement and analysis*. [online]. [cit. 5.8.2016]. Dostupné z:
http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

302: Blíže viz VOŽENÍLEK, David. *Promazání „sušenek" nepomůže, na internetu vás prozradí i baterie*. [online]. [cit. 4.8.2016]. Dostupné z:
http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

denou premisu: jakákoli data či informace vložené do kyberprostoru již v kyberprostoru zůstanou.

Teoreticky by bylo možné definovat i kategorii **hypoteticky ovlivnitelných stop**, což je svým způsobem oxymóron, nicméně tato kategorie zahrnuje jisté skutečnosti, na které může mít uživatel teoreticky vliv, tedy je schopen je ovlivnit, ale běžně to nedělá, neboť by de facto značně omezil možnosti svého fungování v digitálním světě. Mezi tyto stopy by pak bylo možné zařadit například používání služeb největších ISP (Microsoft, Apple, Google, Facebook aj.), u nichž je využívání služby podmíněno odsouhlasením smluvních podmínek (EULA), které umožňují těmto ISP získávat značné množství informací.[303] Dále je pak do těchto stop možné zahrnout i stopy, jež vznikly např. korelací neovlivnitelných a ovlivnitelných stop; informace, jež o nás zveřejní jiní uživatelé; data, jež jsou zrcadlena; EXIF data.[304]

## 3.2 Smluvní podmínky (EULA)

V následující části této kapitoly se pokusím popsat, jaké informace jsou standardně o uživatelích sbírány největšími ISP.[305] Specificky jsem si vybral společnost Google Inc., neboť se domnívám, že existuje minimum uživatelů, jež by nikdy nevyužili některý z produktů (např. OS Android, vyhledávací nástroj na www.google.com, Gmail, Google Chrome aj.) této společnosti.[306] Mým cílem v žádném případě není „útok" na společnost Google Inc. či jiné společnosti (včetně jejich produktů). Smyslem je prezentovat možná bezpečnostní rizika, která jsou spojena s využíváním některých poskytovaných služeb a s akceptací smluvních podmínek (EULA - End Users Licence Agreement), na něž je využívání uvedených služeb vázáno.

Smluvní podmínky, umožňující využití služby daného poskytovatele služby nejsou ve své podstatě ničím jiným než zpravidla jednostranně vymezeným definováním práv a povinností ze strany

303: Blíže viz3.3 Sociální sítě.

304: EXIF - *Exchangeable image file format*. Jedná se o formát metadat, která jsou vkládána do digitálních fotografií, digitálními fotoaparáty. Tato metadata mohou například obsahovat:

- značku a model fotoaparátu,
- datum a čas pořízení snímku,
- GPS pozici,
- informace o autorovi (osobě, která si fotoaparát zaregistrovala),
- nastavení fotoaparátu,
- náhled snímku aj.

305: Pro tuto část textu byly použity teze, jež byly uveřejněny v článku: KOLOUCH, Jan. Pseudoanonymita – bezpečnostní riziko pro uživatele Internetu. *DSM –data security management* [online]. 2015. Roč. 19, číslo 3, s. 24–29 ISSN 1211-8737. Dostupné z: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

306: Je třeba konstatovat, že velmi obdobné smluvní podmínky (umožňující zajišťovat informace ve srovnatelném rozsahu) mají i následující společnosti: Microsoft, Apple, Facebook aj.

poskytovatele služby (ISP). Uživatel však není nikterak omezován na svých právech, neboť má možnost volby v podobě nevyužití takto jednostranně stanovených smluvních podmínek. V případě souhlasu s využíváním takovýchto služeb je možné obecně konstatovat, že dojde primárně k aplikaci soukromoprávních norem.

Otázkou je, zda si uživatel skutečně uvědomuje, jaké smluvní podmínky odsouhlasil, kdy se pro něj stávají závaznými a jaký možný (legální) zásah do jeho základních lidských práv a svobod takto vyslovený souhlas představuje. Další neopomenutelnou skutečností pak je, že takto poskytovaná služba může ovlivnit práva a oprávněné zájmy (např. bezpečnost IT, důvěryhodnost dat aj.) třetích osob (např. zaměstnavatele; osob, kterým je e-mail adresován aj.), které k využívání předmětné služby explicitně souhlas nevyjádřily.

Teoreticky je možné konstatovat, že soukromoprávní smlouvu s touto společností za celé období existence této společnosti uzavřely téměř 3 miliardy uživatelů.[307] Smutným faktem zůstává ta skutečnost, že velmi malé procento uživatelů je ochotno číst smluvní podmínky, vztahující se k té které poskytované službě.[308]

### Výňatky ze smluvních podmínek společnosti Google Inc.[309]

Google explicitně uvádí, že pokud kterýkoli uživatel začne využívat jakékoli služby společnosti Google, souhlasí s platnými smluvními podmínkami. Dále jasně definuje vztah uživatele a sebe, jakožto poskytovatele služby, v případě, že je uživatel povinen akceptovat další smluvní podmínky. Tento vztah je vyjádřen následujícím způsobem: „*Nabídka našich služeb je široká, a na některé se proto mohou vztahovat dodatečné podmínky nebo požadavky (včetně omezení věku). Dodatečné podmínky budou k dispozici spolu s příslušnými službami.* ***Pokud tyto služby použijete, stávají se dodatečné smluvní podmínky součástí smluvních ujednání mezi oběma stranami.***“

Již v úvodu smluvních podmínek Google stanoví, že: „***Obsah***[310] ***můžeme kontrolovat, abychom určili, zda je legální a splňuje naše zásady****, a pokud se domníváme, že naše zásady nebo právní předpisy porušuje, můžeme obsah odstranit nebo zamezit jeho zobrazování. Berte prosím na vědomí, že* ***výše uvedené neznamená, že obsah prověřujeme****.*“

Z hlediska bezpečnosti je dle mého názoru zásadní částí smluvních podmínek sekce, která pojednává

307: Dle článku SMITH, Craig. *By the Numbers: 100 Amazing Google Search Statistics and Facts.* [online]. [cit. 4.8.2016]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/ dochází měsíčně k 100 miliardám vyhledávání právě prostřednictvím Google search.

308: A dle vyjádření jednoho účastníka konference Security 2015 by normální člověk čtením všech, neustále se měnících smluvních podmínek strávil cca 10-20 let života.

309: Dále jen Google. Veškeré výňatky ze smluvních podmínek byly čerpány z: *Smluvní podmínky společnosti Google.* [online]. [cit. 14.6.2016]. Dostupné z: *https*://www.google.cz/intl/cs/policies/terms/regional.html

310: Obsahem je míněn obsah (data), která nepatří společnosti Google. Za obsah nese odpovědnost ten subjekt, který jej zveřejnil.

o **Ochraně osobních údajů a autorských práv**.[311] V této části Google definuje, jaké informace o uživatelích shromažďuje a jak s nimi nakládá. Z pohledu bezpečnosti a „pocitu anonymity" jsou následující informace klíčové. Domnívám se, že deklarace toho, že následující informace jsou shromažďovány *„proto, abychom mohli všem našim uživatelům poskytovat lepší služby – od určení jednoduchých věcí, jako je jazyk, kterým mluvíte, až po věci složitější, například reklamy, které pro vás budou nejužitečnější, lidé o které se na webu nejvíce zajímáte, nebo která videa na YouTube by se vám mohla líbit"* je možná chvályhodná, avšak minimálně zarážející. Přirovnání k již zmíněnému Minority Reportu v podobě cílení reklamy je po takovémto prohlášení více než nasnadě. Mimoto se mi opět vybaví Manfred Spitzer a *Digitální demence*, neboť po čase to již nejsem já, kdo rozhoduje, na co se budu dívat či co budu vyhledávat (resp. mi nemusí být a nejsou nabízeny všechny relevantní odpovědi).

**Google shromažďuje informace o uživateli v zásadě dvěma způsoby:**

1) **Informace, které uživatel sám sdělí.** Typicky se jedná o:
   - *jméno, e-mailovou adresu, telefonní číslo nebo platební kartu.*

2) **Informace získávané při používání služeb Google.** Jsou shromažďovány informace o službách, které jsou uživatelem používány, včetně způsobu, jakým jsou používány (*„například když se podíváte na video na YouTube, navštívíte webové stránky, které využívají naše reklamní služby, nebo sledujete naše reklamy a obsah nebo na ně reagujete"*). Dle Google se jedná o:

   - ***Informace o zařízení*** *(např. model hardwaru, verze operačního systému, jedinečné identifikátory zařízení*[312] *a údaje o mobilní síti včetně telefonního čísla)*. Google je oprávněn přiřadit k vašemu uživatelskému účtu na Google identifikátory vašeho zařízení nebo vaše telefonní číslo.

   - ***Informace z protokolu:***
     - *podrobnosti o tom, jakým způsobem uživatel využil službu Google,*
     - *informace z protokolu telefonování (např. telefonní číslo, číslo volajícího, čísla přesměrování, čas a datum hovorů, trvání hovorů, údaje o směrování zpráv SMS a typy hovorů),*

311: Specificky pak, *Zásady ochrany osobních údajů.* [online]. [cit. 14.6.2016]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/

312: Definice Google. *Jedinečný identifikátor zařízení*. [online]. [cit. 14.6.2016]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/key-terms/#toc-terms-unique-device-id

*„Jedinečný identifikátor zařízení (někdy zvaný také univerzálně jedinečné ID nebo UUID) je řetězec znaků, který do zařízení zakódoval výrobce a slouží k jednoznačné identifikaci zařízení (například číslo IMEI mobilního telefonu). Různé identifikátory zařízení se liší podle toho, zda jsou trvalé, zda je mohou uživatelé resetovat a jak k nim lze získat přístup. Dané zařízení může obsahovat několik různých jedinečných identifikátorů. Jedinečné identifikátory zařízení lze použít k různým účelům, například k zabezpečení, zjišťování podvodů, synchronizaci služeb, jako je doručená e-mailová pošta, nebo k uchování nastavení uživatele a poskytování relevantních reklam."*

- *adresa internetového protokolu,*
- *informace o událostech zařízení (např. selhání, činnost systému, nastavení hardwaru, typ prohlížeče, jazyk prohlížeče, datum a čas vašeho požadavku nebo odkazující adresa URL,*
- *soubory cookie, které mohou být jedinečnými identifikátory vašeho prohlížeče nebo účtu Google.*

◦ ***Informace o poloze.*** Google je oprávněn shromažďovat a dále zpracovávat informace o skutečné poloze svého uživatele. Polohu může Google určovat pomocí různých technologií, jako jsou IP adresa, systém GPS a další senzory, které společnosti Google mohou poskytovat například údaje o zařízeních v okolí, přístupových bodech sítě Wi-Fi a vysílačích mobilních sítí.

◦ ***Jedinečná čísla aplikací.*** **Typicky se jedná o licenční číslo a typ (verzi) příslušného nainstalovaného softwarového produktu. Ze smluvních podmínek** nevyplývá, že by se jedinečná čísla aplikací zaznamenávala pouze ze zařízení, jejichž primárním operačním systémem je systém Android. Lze tedy dojít k závěru, že pokud dochází k využívání služeb Google, pak jsou sbírány i informace o jedinečných číslech aplikací i z jiných operačních systémů (iOS, Linux, Windows aj.).

◦ ***Místní úložiště.*** **Dle smluvních podmínek může Google:** *„shromažďovat a uchovávat informace (včetně osobních údajů) v místním úložišti vašeho zařízení.“* I v tomto případě lze dojít ke stejnému závěru, jako tomu bylo u jedinečných čísel aplikací.

Problémem je dle mého názoru i ta skutečnost, že nikde v obecných smluvních podmínkách není přesně vymezeno,[313] jaké umístění a především jaké zabezpečení bude službou Google využito, a tím pádem je teoreticky možné využívat úložiště jako celek. Lze získávat informace o souborech (např. jejich názvy, lokaci, a ad absurdum i hash, který bude následně porovnán např. s databází jiné služby, kde se ukládají data – např. DropBox, OneDrive aj.).

**Hrozbou pro uživatele pak je dle mého názoru i možnost zneužití takto uložených dat útočníkem. Informace (které se typicky nabalují na cookies aj.) uložené v uživatelově místním úložišti se mohou stát i zajímavým cílem pro útočníka, neboť právě z těchto informací je možné zjistit např. vzorce chování uživatele.**

◦ ***Soubory cookie a podobné technologie.*** *„Když navštívíte nějakou službu Google, používáme my i naši partneři různé technologie ke shromažďování a ukládání informací. To může mimo jiné zahrnovat používání souborů cookie nebo podobných technologií k identifikaci vašeho prohlížeče nebo zařízení. Pomocí těchto technologií* ***shromažďujeme a ukládáme informace i v případě, kdy využíváte služby, které nabízíme našim partnerům****, jako jsou reklamní služby nebo funkce Google, které se mohou zobrazit na jiných webech.“*

313: Resp. dle požadované funkce půjde především o ukládání informací a dat do složky daného prohlížeče (webbrowser), avšak dle smluvních podmínek může jít i o jiné aplikace, než je webbrowser.

Jaké informace sbírají aplikace fungující v rámci Android OS:

314

Google je na základě odsouhlasených smluvních podmínek s těmito informacemi dále oprávněn nakládat. Mimo jiné je Google oprávněn analyzovat obsah (včetně e-mailů) pomocí automatizovaných systémů. Dále je oprávněn spojovat osobní údaje z jedné služby s informacemi a osobními údaji ze služby další (využívající Google).

Nakládáním s uvedenými informacemi se pak rozumí i jejich sdílení, a to ať již se souhlasem uživatele, nebo bez tohoto souhlasu.[315] Za doslovnou citaci stojí dikce smluvních podmínek umožňující **sdílení za účelem externího zpracování a z právních důvodů**:

„*Osobní údaje poskytujeme spřízněným společnostem, nebo jiným důvěryhodným firmám či osobám, aby je pro nás mohli zpracovat na základě našich pokynů a v souladu s našimi zásadami ochrany osobních údajů a dalšími příslušnými opatřeními ohledně důvěrnosti a zabezpečení.*“

314: CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cit. 10.4.2015]. Dostupné z: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

315: Např. s administrátory domén; za účelem externího zpracování, či z právních důvodů.

*„**Osobní údaje sdílíme se společnostmi, organizacemi či jednotlivci** mimo společnost Google, **pokud jsme v dobré víře přesvědčeni, že přístup k takovým údajům, jejich použití, uchování nebo zveřejnění jsou rozumně nutné za účelem:***

- *dodržení platného zákona, nařízení, právního postupu nebo vynutitelného vládního požadavku,*
- *uplatnění příslušných smluvních podmínek včetně vyšetření jejich možného porušení,*
- *zjištění, zabránění nebo jiného postupu proti podvodu, technickým potížím či bezpečnostním problémům,*
- *ochrany před poškozením práv, majetku nebo bezpečnosti společnosti Google, našich uživatelů nebo veřejnosti tak, jak to vyžaduje nebo povoluje zákon.“*

Z pohledu bezpečnosti a ztráty anonymity však považuji za asi nejproblematičtější následující pasáž smluvních podmínek, která se věnuje uživatelskému obsahu ve službách poskytovaných Google:

*„Pokud **nahrajete, odešlete, uložíte nebo přijmete obsah do nebo prostřednictvím našich služeb, poskytujete společnosti Google** (a subjektům, se kterými společnost Google spolupracuje) **celosvětově platnou licenci k užití, hostování, uchovávání, reprodukování, upravení, vytvoření odvozených děl** (například děl, jež jsou výsledkem překladu, přizpůsobení/adaptací či úprav provedených za účelem jeho lepšího fungování v rámci našich služeb),*[316] ***komunikaci, publikování, provozování a zobrazování na veřejnosti a distribuci takového obsahu**……Licence přetrvává i poté, co přestanete naše služby používat (např. firemní zápis přidaný do služby Mapy Google). **Některé služby umožňují k obsahu, který jste do služby odeslali, získat přístup nebo jej odebrat…**“*

Osobně se domnívám, že minimálně v této části smluvních podmínek došlo k překročení oné pomyslné hranice vymezující přiměřenost sbíraných informací o jednotlivých uživatelích. V této části de facto jde o „legální využití“ jakéhokoli obsahu, se kterým Google „přijde do styku“. Osobně se domnívám, že právě zásah do obsahu např. přenášených informací by měl být tím nejzazším možným prostředkem, a ne jakousi „samozřejmostí“ zakotvenou ve smlouvě.

To, že by tento zásah neměl být onou „samozřejmostí“, je možné demonstrovat na základě proporcionality dat sbíraných například na základě zákona o elektronických komunikacích,[317] či na základě jiných zákonných ustanovení (například na základě zákona č. 141/1961 Sb., trestní řád.[318] Konkrétně § 88 TŘ - Odposlech a záznam telekomunikačního provozu, který umožňuje orgánům činným v trestním řízení právě přístup k obsahu přenášených informací. Pokud chtějí

316: Je pochopitelné, že se společnost Google snaží např. o překlady děl, stánek, či jiného obsahu, aby měl možnost si jej přečíst i uživatel, který nezná originální jazyk uvedeného díla. Nicméně, ad absurdum si je možné představit, že dojde k zveřejnění vaší soukromé milostné básně, kterou jste pomocí některé ze služeb Google odeslali, vaší fotografie, vašeho geniálního nápadu na perpetum mobile aj.

317: Viz kap. 2.5.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZoEK.

318: Dále jen **trestní řád** či **TŘ**.

orgány činné v trestním řízení zjistit tyto informace, musí mimo jiné splnit přísné podmínky stanovené zákonem[319]).

Mezi dvěma výše uvedenými případy (Google vs. stát) je patrná zjevná disproporce vztahující se k možnosti přístupu k obsahovým informacím, které si uživatelé mezi sebou sdílí, přenáší, uveřejňují na web aj. Plně si uvědomuji, že není možné reálně srovnávat stát a soukromou firmu, nicméně tento příměr má sloužit pro pochopení toho, co kdo a v jaké míře sbírá o uživatelích kyberprostoru. Pokud bych totiž tento příměr chtěl zcela dokončit, pak bych musel říci, že Google je jakýmsi „globálním státem", neboť má možnost mít informace o téměř všech třech miliardách uživatelů Internetu a o několika dalších miliardách lidí, kteří využívají např. mobilní telefon s operačním systémem Android.

Osobně neodmítám možnost uchovávání a následné zprostředkování jak obsahových, tak provozních a lokalizačních informací, avšak domnívám se, že podmínky přístupu a disponování s nimi, by měly být velmi precizně definovány a uživatel (stejně jako tomu je v případě ustanovení § 88 a 88a TŘ) by měl mít možnost kontroly, zda a jak je s jeho „obsahem" zacházeno.

Je zřejmé, že i stát má možnosti, jak získat značné množství informací o uživatelích, avšak ve většině případů nedochází k současnému zisku jak provozních a lokalizačních, tak obsahových informací. Druhou výraznou odlišností intervence státu do soukromí uživatele je i ta skutečnost, že zásah oprávněných subjektů (např. orgány činné v trestním řízení aj.) je zpravidla možný pouze na základě příkazu vydaného soudem.

## 3.3 Sociální sítě

Termín sociální síť označuje druh služby, která umožňuje uživatelům komunikovat, sdílet data a informace (více či méně trvalým způsobem) a provádět další aktivity. Tímto se sociální sítě výrazně odlišují od jiných způsobů komunikace, jako je např. telefonický hovor.

Interaktivnost sociálních sítí je dalším aspektem, který tyto sítě odlišuje od standardní komunikace. V rámci sociálních sítí je k běžné komunikaci přidávána i obsahová část, kdy dochází k vytváření, předávání, sdílení (např. fotografií, videí, dokumentů, odkazů aj.) mezi jednotlivými uživateli navzájem. Dalším typickým rysem sociální sítě je nutnost vytvoření profilů, které prezentují konkrétní osoby. Na základě různých smluvních podmínek mohou profily odpovídat reálným osobám (fyzickým, či právnickým), či mohou být zcela smyšlené.[320]

319: Blíže viz kap. 6.4.5.2 Odposlech a záznam telekomunikačního provozu.

320: ČERNÁ, Monika a Michal ČERNÝ. *Úvod do problematiky sociálních sítí*. [online]. [cit. 12.5.2015]. Dostupné z: http://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html/

Sociální komunikace v rámci sociálních sítí je bezprostředně závislá na množství aktivních uživatelů. Sociální sítě prožívají velký rozmach právě v kyberprostoru, avšak vázanost na toto virtuální médium není nezbytnou podmínkou pro existenci sociální sítě.

Jirásek definuje pojem sociální síť následovně: „*Propojená skupina lidí, kteří se navzájem ovlivňují. Tvoří se na základě zájmů, rodinných vazeb nebo z jiných důvodů. Tento pojem se dnes také často používá ve spojení s internetem a nástupem webů, které se na vytváření sociálních sítí přímo zaměřují (Facebook, Lidé.cz apod.), sociální sítě se mohou vytvářet také v zájmových komunitách kolem určitých webů, například na jejich fórech.*“ [321]

Na základě výše uvedených definic by bylo možné shrnout klíčové prvky sociálních sítí do následujících bodů:

- Možnost navazování vztahů (kontakty)
- Komunikace mezi uživateli
- Vytváření, předávání, sdílení obsahu mezi jednotlivými uživateli (obsahová část komunikace)
  - jednoduché a efektivní sdílení informací
  - interaktivnost komunikace
- Nutnost aktivního zapojení uživatele
- Využívání kyberprostoru, jakožto nejvhodnější platformy

Pokud definujeme sociální sítě, tak je třeba si uvědomit, že se jedná pouze o službu, typicky poskytovanou ISP, v kyberprostoru na základě odsouhlasených smluvních podmínek. Na základě těchto podmínek je pak o uživatelích zjišťována celá řada informací (velmi často značně soukromých), které mohou být v souladu s těmito podmínkami předávány dalším osobám, ale zejména archivovány téměř neomezenou dobu.

Za první virtuální sociální síť je možné považovat projekt Sixdegrees (1997–2000). Tento projekt umožňoval uživatelům vytvořit si svůj virtuální profil a seznam přátel. Uživatel měl také možnost nahlédnout do seznamu přátel svého přítele. Uživatel mohl díky této možnosti získat přehled společných kontaktů a e-mailové spojení na všechny přátele. Významným milníkem v případě sociálních sítí byl vznik sítě Facebook (2004) a její následné masivní rozšíření. Tato síť byla původně určena pro studenty Harwardské univerzity a umožňovala vytvářet provázanosti kontaktů a vyhledávat spojitosti mezi více druhy obsahu. Studenti tak získali možnost nalézt a kontaktovat osoby s obdobnými či stejnými zájmy. Obsahově již nešlo jen o komunikaci soukromou prostřednictvím e-mailu, ale bylo umožněno, aby každý uživatel mohl vložit do webové aplikace svůj vlastní obsah. Uživatelé byli postaveni před rozhodnutí, jakým způsobem budou se svým soukro-

321: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 107. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

mým obsahem nakládat.[322] Facebook se masivně rozšířil a v roce 2006 vydal smluvní podmínky, v nichž umožnil registraci a využívání služby Facebook jakékoliv osobě starší 13 let.

V současnosti existuje celá řada sociálních sítí či služeb, které je možné považovat za sociální sítě. Mezi nejznámější patří: Facebook, YouTube, QQ, QZONE, Whatsapp, Wechat, Google+, Shazam, Linkedin, BitTorrent, Dropbox, iCloud, Skype, Twitter, iMessage, Tumblr, Facebook Messenger, Instagram, Badoo, Google Drive, One Drive, Ask.fm, Viber, Vkontakte, Snapchat, Steam, Flickr, Spotify aj.[323]

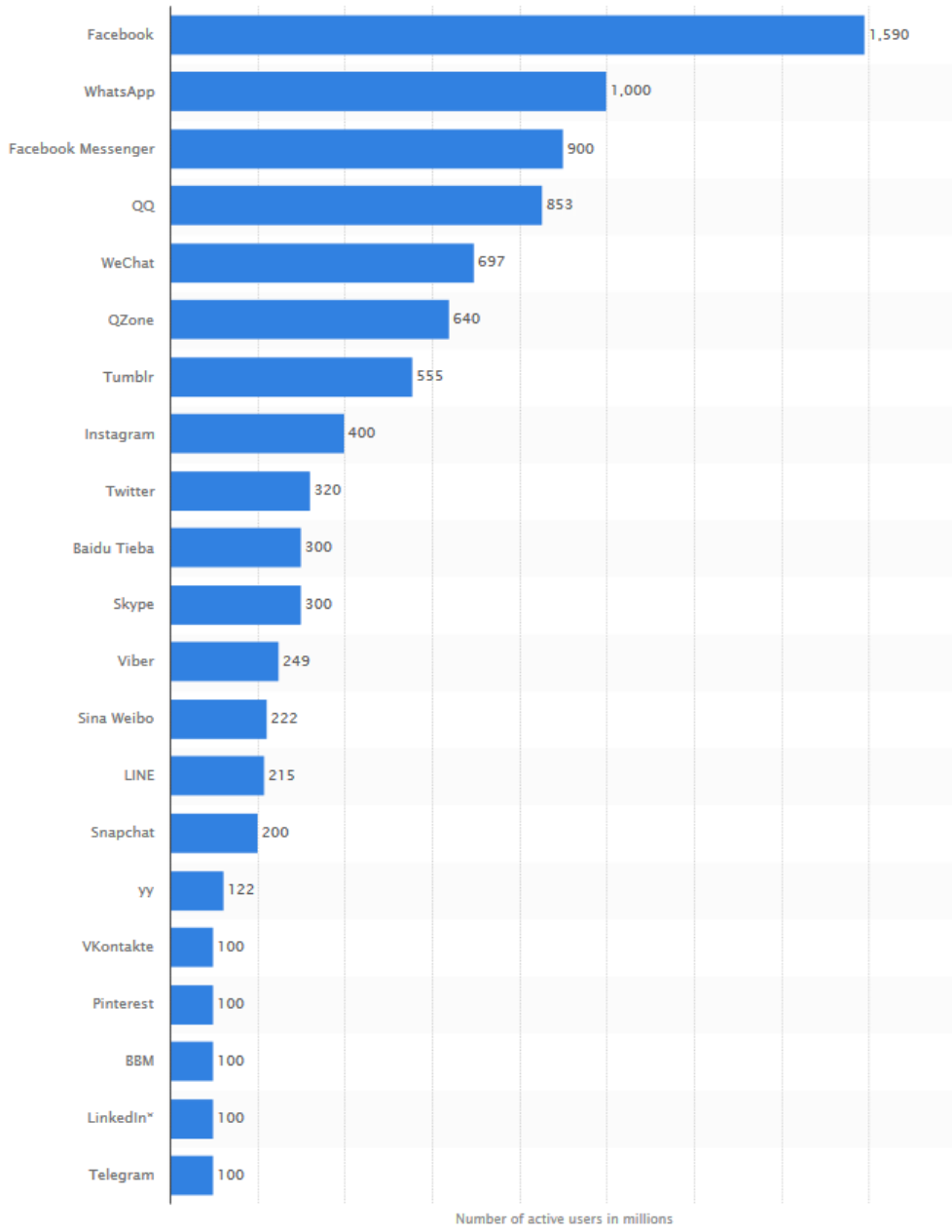
Mezi nejznámější české sociální sítě je možné zařadit Lidé.cz, Spolužáci.cz, Libímseti.cz.

V následujícím grafu jsou zobrazeny sociální sítě podle počtu aktivních uživatelů.[324]

322: Volba mimo jiné spočívá i v otázkách **míry zabezpečení až po provazování s cizím obsahem** (Vytváření spojitostí mezi objekty typu lokace, čas, oblíbenost, zájem apod.).

323: DOČEKAL, Daniel. *Největší sociální sítě na světě? Facebook je sice jednička, ale...* [online]. [cit. 20.8.2015]. Dostupné z: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

324: *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions).* [online]. [cit. 20.8.2015]. Dostupné z: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

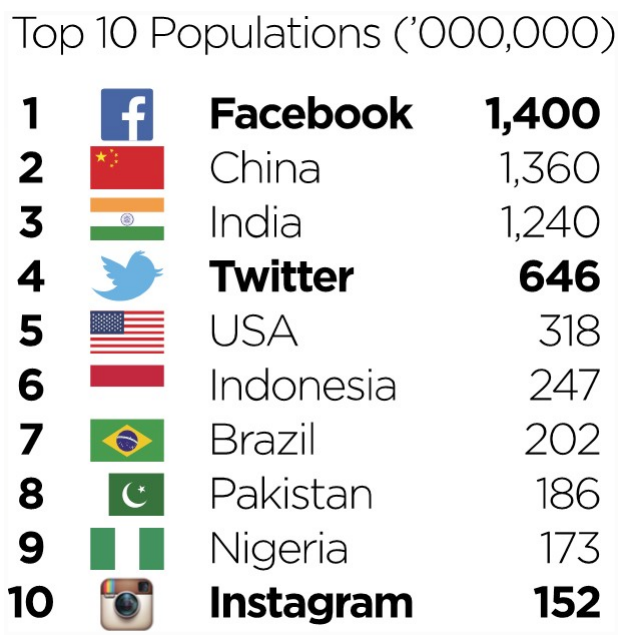

Facebook
1,590
WhatsApp
1,000
Facebook Messenger
900
QQ
853
WeChat
697
QZone
640
Tumblr
555
Instagram
400
Twitter
320
Baidu Tieba
300
Skype
300
Viber
249
Sina Weibo
222
LINE
215
Snapchat
200
yy
122
VKontakte
100
Pinterest
100
BBM
100
LinkedIn*
100
Telegram
100
Number of active users in millions

Z průzkumů společnosti Pew Research Center[325] vyplývá, že 74 % uživatelů Internetu využívá ke své komunikaci právě sociální sítě. Nejčastějšími uživateli sociálních sítí jsou osoby ve věku 18 až 29 let (téměř 90 %), avšak věkové rozložení se postupně mění a sociální sítě využívají čím dál víc osoby vyššího věku.

Sociální sítě vytváří prostředí, které umožňuje potenciálnímu pachateli (útočníkovi) velmi rychlý přístup k oběti a informacím, které o sobě oběť sama dobrovolně zveřejní.

Co vše lze zjistit z informací publikovaných v rámci sociálních sítí, je velmi vhodně demonstrováno na videu ***Amazing mind reader reveal his „gift"***. Video je dostupné online: https://www.youtube.com/watch?v=afHuT_FUw2U

Rozsah sociálních sítí velmi výstižně demonstruje starší statistika, která uvádí počet osob, které jsou „příslušníkem" toho kterého „státu".[326]




325: PERRIN, Andrew. *Social Media Usage: 2005-2015* [online]. [cit. 16.7.2016]. Dostupné z: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

326: NELSON, Adrian. *Some questions and answers about Facebook.* [online]. [cit. 16.7.2016]. Dostupné z: http://www.rotarydistrict9800.com.au/news/14135/some-questions-and-answers-about-facebook/?no_follow=1

## 3.4 Projekty testující zranitelnosti uživatelů sociálních sítí

Na tomto místě bych rád představil tři projekty, které jsem realizoval společně se studenty[327] Policejní akademie ČR v Praze v rámci studentských vědeckých odborných činností.

Všechny projekty měly jeden společný cíl, a to zjistit, jak složité je získat důvěru uživatelů sociální sítě Facebook, a tím i přístup k datům a informacím o nich a jejich přátelích. Dalším cílem bylo popsat vlastní způsob útoku, stejně jako chyby, jež uživatelé udělali. Posledním cílem bylo dát doporučení dalším uživatelům sociálních sítí, aby se nestali obětí skutečných útočníků.

Prvním impulsem pro otestování zranitelnosti uživatelů sociálních sítí v ČR byl projekt, jež vytvořil Thomas Ryan (White hat hacker, security specialist, New York) v prosinci 2009. Tento projekt[328] si kladl za cíl zjistit zranitelnost osob, které je možné považovat za bezpečnostní experty.

Thomas Ryan vytvořil fiktivní postavu: **Robin Sage**, kterou pak využil k vlastnímu „útoku". Tato virtuální postava byla vytvořena tak, aby bylo možné relativně jednoduše zjistit případné nesrovnalosti ve virtuálních profilech a nenechat se „nachytat". Thomas Ryan vytvořil Robin Sage falešné profily na sociálních sítích: Facebook, Twitter a Linkedin.

Na všech těchto profilech uvedl následující informace:

**Jméno: Robin Sage** (v USA je Robin Sage název cvičení pořádaného pro speciální jednotky https://www.army.mil/article/151795/Robin_Sage_exercise_set),

- **Věk: 25 let**
- **Profilová fotografie** (Tato profilová fotografie pochází z pornografických stránek a případná oběť tuto informaci mohla zjistit například pomocí vyhledání obrázku skrze www.google.com.)
- **Vystudovala Massachusetts Institute of Technology (MIT).** Nikde na MIT však nebyla jediná informace o tom, že by tam kdy Robin Sage studovala.
- **Profil na Linkedin uváděl, že má 10 let praxe v oblasti cyber security** (ve věku 25 let!)

---

327: Na projektech se podíleli následující studenti:

- **Projekt Dennis a Terezka:** Michal Dvořák; Terezie Janíková; Tomáš Najman
- **Projekt Petr Dvořák:** Jan Nejedlý; Tereza Šmigolová
- **Projekt Adam Novák:** Jan Nejedlý

328: Bližší informace k projektu: RYAN, Thomas. *Getting In Bed with Robin Sage.* [online]. [cit. 5.9.2013]. Dostupné z: http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

- **Práce: Cyber Threat Analyst** (analytik kybernetických hrozeb) v Naval Network Warfare Command, Norfolk, Virginia

- **Telefonní číslo a e-mailové adresy** (Uživatelé si mohli ověřit totožnost Robin Sage a nestat se tak obětí útoku Thomase Ryana.)

Obrázek 22: Profilová fotka Robin Sage

Po vytvoření těchto profilů kontaktovala (v průběhu prosince 2009 – ledna 2010) Robin s žádostí o přátelství přibližně 300 osob, přičemž většina z nich byla bezpečnostními experty, pracovníky zpravodajských služeb, příslušníky ozbrojených sil atp. I přesto, že celá řada oslovených odhalila podvod Thomase Ryana, zaznamenala Robin Sage řadu úspěchů. Byla například pozvána na několik osobních schůzek a večeří, byly jí zasílány odborné práce a jiné dokumenty ke konzultaci a byla jí nabídnuta práce konzultanta u společností Google a Lockheed Martin.

Projekt Thomase Ryana jako první jednoznačně ukázal negativa, která jsou spojena s využíváním sociálních sítí a s téměř bezmeznou důvěrou v data, informace a kyberprostor jako takový.

S plným vědomím toho, že Facebook je oprávněn smazat všechny falešné profily,[329] jsem se rozhodl odprezentovat provedené výzkumy, včetně deanonymizace použitých účtů. Důvodem je ta skutečnost, že by si uživatelé měli uvědomit svoji zranitelnost v rámci sociálních sítí a více dbát o informace, které o sobě zveřejňují, stejně jako na to, koho „přijmou za přítele".

Dalším odstrašujícím případem pak může být projekt ***„The Dangerous of Social Media"*** (tvůrcem je Coby Persin).[330]

### 3.4.1 Dennis a Terezka

V návaznosti na teoretické znalosti a zejména s ohledem na projekt Robin Sage jsme se v prvním projektu rozhodli otestovat zranitelnost dětí mladších 13 let na sociální síti Facebook.[331] Na tomto místě je vhodné připomenout, že uživatelé mladší 13 let nemají povoleno vytvářet si a užívat profil na této síti. Primárním cílem tohoto experimentu bylo především poukázat na vysoce rizikové a nebezpečné chování uživatelů sociálních sítí.

Jedním z cílů, které jsme si stanovili, bylo, že naše falešné profily nebudou samy aktivně komunikovat s uživateli, kteří si nás přidali jako přítele. V případě, že nás uživatel oslovil, snažili jsme se udržet co nejmenší úroveň komunikace. Hlavním cílem bylo analyzovat jednotlivé profily (které nás akceptovaly jako přítele), popsat rizikové oblasti informací sdílených na těchto profilech a na podkladě toho stanovit doporučení týkající se sdílení informací na sociálních sítích mezi uživateli navzájem.

Pro účely empirického výzkumu byly vytvořeny tyto dva falešné profily:

1) **Dennis Pes.**
2) **Terezka Přibylová.**

Vytvořené profily měly simulovat reálný způsob zisku informací a poukázat tak na jednoduchost zisku důvěrných a osobních informací o uživatelích. Námi nastíněný způsob získání informací může být a je využíván jak útočníky (pachateli), tak jakoukoli jinou osobou (například pro marketingové účely), či bezpečnostními složkami státu aj.

329: Blíže viz smluvní podmínky. Čl. 4: *„Uživatelé Facebooku poskytují svá skutečná jména a informace, a má-li to tak zůstat, potřebujeme vaši pomoc. Dále uvádíme několik vašich povinností vůči nám týkajících se registrace a zajištění bezpečnosti vašeho účtu: 1. Neposkytnete na Facebooku falešné osobní informace a ani bez povolení nevytvoříte účet pro nikoho jiného."* *Prohlášení o právech a povinnostech.* [online]. [cit. 6.8.2016]. Dostupné z: https://www.facebook.com/legal/terms

330: PERSIN, Coby. *The Dangerous of Socila Media.* [online]. [cit. 6.8.2016]. Dostupné z: https://www.youtube.com/watch?v=6jMhMVEjEQg

331: V rámci empirického šetření jsme se zaměřili právě na děti mladší 13 let především z důvodu vysokého ohrožení a zranitelnosti této věkové skupiny ve virtuálním prostředí. Osoby byly vybírány na základě vzhledu (a odhadu věku) na profilové fotografii.

Z vlastního empirického zkoumání vyplynulo, že získání informací o některých uživatelích je značně zjednodušeno právě uživateli samotnými. Běžní uživatelé ve většině případů nerespektují základní doporučení týkající se bezpečnosti a ochrany dat. Typicky stačí k zisku informací pouhé navázání kontaktu s potenciální obětí právě v prostředí sociálních sítí.

### Dennis Pes

Dennis je jedním z účelově vytvořených profilů sloužící k navázání kontaktu s potenciální obětí a získání informací z profilů na sociální síti Facebook.

Obrázek 23: Profilová fotka Dennis

Profil byl záměrně vytvořen jako **„podezřelý profil“**. Na profilovou fotku byla použita fotografie skutečného psa, nicméně v informacích o profilu bylo uvedeno, že profil založil muž, jenž se narodil v roce 1990 (v době realizace projektu tedy šlo o muže ve věku 23–24 let), a který záměrně oslovuje děti.

Naše hypotéza u tohoto profilu předpokládala určitou úroveň nedůvěry uživatelů ke zcela neznámému profilu, jež je oslovil. Očekávali jsme, že zcela anonymní profil si přidá minimum uživatelů (případně omezí přístup k informacím z jejich profilu – tj. budeme zařazeni do skupiny).

Dennis byl vytvořen 18. listopadu 2013 a do 1. února 2014 rozeslal celkem 85 žádostí o přátelství. V období od konce listopadu 2013 do začátku února 2014. Je třeba podotknout, že nedocházelo k nijak masivnímu zasílání žádostí o přátelství. Žádosti se pohybovaly v řádech jednotek za den, či týden.) a přijal 2 žádosti o přátelství, které mu byly navrhnuty.

Profil Dennis Pes byl vytvořen jako *„neaktivní“* profil. Z tohoto profilu docházelo de facto pouze k rozesílání žádostí. Dne 20.11.2013 v 11.00 hod. bylo rozesláno prvních 10 žádostí (ze zcela

anonymního účtu, který obsahoval pouze název a profilové foto psa) osobám zjevně mladším 15 let (5 dívek a 5 chlapců). Do 24 hodin bylo přijato 6 žádosti (5 dívek a 1 chlapec). Následující den byly do profilu **přiloženy další 4 fotografie**. Za celou dobu fungování účtu Dennis Pes bylo vloženo pouze 6 fotografií (včetně profilové), profil nebyl nijak více vyplněn a za celou dobu fungování došlo pouze k **11 „aktivitám"** [332] (např. hraní hry, vyvěšení příspěvku aj.), ze strany profilu Dennis Pes.

Počet přátel se postupně měnil od přibližně 55 až ke konečným 44 osobám v době, kdy byl projekt ukončen (23. březen 2014 – došlo k ukončení sběru a analýzy veřejně dostupných informací z profilu uživatelů). Vysoká procentuální úspěšnost tohoto profilu byla překvapením.

K 6. 8. 2016 měl Dennis stále 33 přátel.

Veškeré osoby, kterým byly rozeslány žádosti o přátelství, byly vybrány zcela náhodně. Jediným kritériem byla snaha o kontaktování co nejmladších uživatelů sociální sítě. Zejména na těchto uživatelích, kteří v prostředí sociálních sítí vyrůstají de facto od svého narození, jsme chtěli demonstrovat jejich mnohdy hrubou neopatrnost v oblasti ochrany údajů, které jsou pro případné útočníky významné a které mohou mít pro uživatele fatální důsledky.[333]

Výsledky analýzy dat[334] ukázaly, že více než 85 % uživatelů uveřejňuje informace, které mohou být potenciálním útočníkem velmi jednoduše zneužity. Konkrétně se jedná např. o uvedení: dalších kontaktních informací (telefon, soukromý e-mail, Skype aj.), profilů na jiných sociálních sítích, místa bydliště, data narození, název a místo navštěvované školy, navštěvované kroužky či sportovní kluby (někdy i s rozpisem aktivit) aj. Významným zdojem informací pak byla i aktivovaná geolokace u počítačového systému, na kterém měl uživatel zapnutý Facebook. V řadě případů pak bylo možné de facto sledovat pohyb uživatele během celého dne. Z celkového počtu přátel měly pouze dva profily nastaveny zabezpečení tak, abychom nemohli získat výše uvedené informace bez dalších aktivit (navázání komunikace, hraní her, sdílení příspěvků atp.).

### Terezka Přibylová

Druhým vytvořeným profilem je profil, který měl představovat třináctiletou dívku Terezku Přibylovou, která začala využívat sociální síť Facebook.

332: Mezi tyto aktivity není započítáno rozesílání žádostí o přátelství.

333: KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN a Terezie JANÍKOVÁ. neBezpečné chování na Facebooku. In: *Sborník příspěvků ke konferenci: Sociální sítě. Mobilní aplikace.* Plzeň: Západočeská univerzita v Plzni, 2014, s. 39–47. ISBN 978-80-261-0362-2

334: Informace, které byly veřejně dostupné na profilech uživatelů, kteří si Dennise přidali za „přítele". Dále pak viditelná komunikace aj.

Obrázek 24: Profilová fotka Terezka Přibylová

Profil byl cíleně tvořen jako běžný profil uživatele, který zrovna začíná využívat sociální sítě. Došlo tedy ke kvalitnějšímu a plnohodnotnějšímu vyplnění profilu Terezky, včetně uvedení skutečných fotografií dívky. Vyplněny byly rubriky oblíbený sport, hudba, filmy, TV pořady, knihy, „To se mi líbí", připojení se ke skupinám aj. Zároveň tento profil vystupoval na Facebooku aktivněji než Dennis, i když ne zcela typicky, jako vystupují jiní uživatelé stejného věku.[335]

Naše hypotéza u tohoto profilu předpokládala určitou vyšší úroveň důvěry uživatelů k profilu, jež je lépe spravován, aktivněji komunikuje aj. Zároveň jsme předpokládali, že tím, že se jedná o profil dívky, dojde k jeho snadnější akceptaci uživateli, jež oslovil.

Terezka byla vytvořena 19. listopadu 2013 a do 1. února 2014 (v rozhodném období pro náš výzkum) rozeslala přibližně 100 žádostí o přátelství. Žádosti o přátelství byly stejně jako u Dennise rozesílány postupně. Profil Terezky plnil svoji funkci až do 11.3.2014 (do této doby rozeslal 198 žádostí o přátelství). Počet přátel se postupně měnil od přibližně 150 až ke konečným 121 osobám v době, kdy byl projekt ukončen (23. březen 2014).

K 6.8.2016 měla Terezka stále 96 přátel.

Výsledky analýzy volně dostupných dat ukázaly téměř stejné výsledky, jako tomu bylo u profilu Dennis. Rozdíl mezi těmito dvěma profily však spočíval především v tom, že dívčímu profilu byla častěji navrhována „přátelství" od zcela neznámých lidí či od přátel našich přátel. Zarážející na tom byla především ta skutečnost, že Terezka byla často oslovována dospělými (staršími) muži, mezi jejichž přátele patřila řada dětských profilů.

335: Za celou dobu fungování účtu Terezka bylo vloženo celkem **23 fotografií**, včetně profilové. Došlo k 16 „šťouchnutím", 197 „like", přidání 13 skupin, 14 sdílení odkazů, 77 ostatním úkonům. Celkem tedy došlo zhruba k 400–500 **„aktivitám"** za vlastníka profilu.

Aktivity běžného uživatele Facebooku se pohybují, ve srovnání s aktivitami námi spravovaných profilů v jiných číslech. Běžně je schopen uživatel uskutečnit cca **400–700 aktivit za den** (komentáře cca 30-50, hry a chat v nich: 100–150, chat: 200–400, like: 30-50, prohlížení jiných profilů 150–250 aj.).

Dále byla Terezka zvána na osobní setkání, popovídání si, mazlení aj. Terezka také byla požádána o zaslání jiných fotografií, než těch, které již měla zveřejněny na Facebooku, konkrétně se jednalo o žádost o pořízení intimnějších fotografií.[336]

U celé řady dětských účtů bylo uvedeno, že jim se správou pomáhají rodiče, nicméně nikdo z rodičů neoslovil ani jeden z falešných účtů, aby si jakkoli verifikoval uživatele, který si přidal jejich dítě jako přítele. Na řadě takto spravovaných účtů pak byly vystaveny materiály, které mohly přímo poškodit uživatele.[337]

Uvědomuji si, že námi provedený průzkum je jeden z nejjednodušších a útočí na potenciálně velmi zranitelnou skupinu uživatelů, nicméně je to přesně ten typ útoků, ke kterým v kyberprostoru dochází velmi často. Doporučení pro uživatele budou souhrnně uvedena v kap. 3.5 Doporučení pro uživatele sociálních sítí.

### 3.4.2 Petr Dvořák

Druhý empirický výzkum byl realizován v roce 2015 a podíleli se na něm studenti Policejní akademie ČR v Praze Jan Nejedlý a Tereza Šmigolová. Tento projekt se významně lišil od projektu Dennis a Terezka, byť prostředí, v němž se uskutečnil, bylo stejné. Našim cílem v tomto projektu nebylo získat určité osoby jako přátele, ale dostat se do uzavřené skupiny a v této skupině rozdistribuovat „závadný" materiál.[338] Naším cílem bylo zjistit, do jaké míry jsou uživatelé schopni (ochotni) akceptovat data z neznámého zdroje. Tento postup je útočníky v kyberprostoru často využíván, neboť sociální sítě mohou být vhodným prostředkem pro vstup do chráněného prostředí.

Před provedením experimentu jsme si stanovili hypotézu, že námi vytvořený materiál se bude sám dále šířit po sociální síti v rámci zvolené skupiny uživatelů, protože bude pro uživatele zajímavý. Vlastní útok byl realizován prostřednictvím webové aplikace, která zaznamenávala informace o uživatelích, kteří po odsouhlasení EULA (smluvní podmínky v rámci naší webové aplikace) dobrovolně předali přístup ke svým datům (informacím) útočníkovi.[339] Uživatel odsouhlasením těchto smluvních podmínek mohl předat plný přístup útočníkovi, nicméně náš útok se zaměřil pouze na získání jména, příjmení a e-mailové adresy. Pokud by si uživatel stáhl infikovaná data, pak by mohlo například dojít k instalaci malware[340] do jeho počítačového systému. V rámci našeho

336: Takovéto jednání má povahu sextingu – viz kap. 4.14.2 Kybergrooming; 4.14.3 Sexting.

337: Například se jednalo o natočená videa koupání nahých dětí ve věku přibližně 6 let; videa, na kterém dítě pro zábavu předvádí striptýz aj.

338: Jedná se o data, která by při reálném útoku mohla obsahovat např. malware aj.

339: Blíže viz: NEJEDLÝ, Jan a Tereza ŠMIGOLOVÁ. *Kyberkriminalita na sociálních sítích*. Praha 2015. Studentská vědecká a odborná činnost, Policejní akademie ČR v Praze, Sekce právní vědy. Vedoucí práce Jan Kolouch.

340: Viz kap. 4.3 Malware.

projektu však nedošlo ani k instalaci malware, ani k zisku citlivých informací osobní povahy, neboť by takovéto jednání mohlo být za pomyslnou hranou vědeckého výzkumu (a byť by bylo odsouhlaseno uživatelem, mohlo by být požadováno minimálně za nemorální, případně i nelegální).

Pokud bychom se snažili neoprávněně získat přístup k účtům uživatelů, či bychom případně distribuovali malware, mohli bychom se případně dopustit trestného činu dle § 230 TZK (Neoprávněný přístup k počítačovému systému a nosiči informací).[341] Důvodem, proč jsme se tohoto trestného činu nedopustili, je skutečnost, že získáním souhlasu k přístupu do počítačového systému nebo jeho části uživatel odsouhlasil oprávněnost našeho jednání. Podmínkou bylo, že uživatel bude informován o tom, jaká data (informace) o něm získáme. Všechny tyto relevantní informace byly uživateli dostupné při přijímání podmínek vytvořené webové aplikace. Pokud uživatel s těmito podmínkami nesouhlasil, měl plné právo je odmítnout. Tím, že uživatel odsouhlasil naše podmínky, vlastně udělil svolení poškozeného (§ 30 TZK).

Posledním cílem bylo upozornit uživatele na nebezpečnost jejich jednání, pokud umožňují třetím stranám a neznámým subjektům přístup k jejich datům (informacím) tím, že odsouhlasí smluvní podmínky a přijmou data z neznámého zdroje. Útočníci, kteří sbírají informace o uživatelích, běžně tyto údaje využívají například pro phishingové útoky,[342] zcizení identity[343] apod. V reálném světě pak data nabízená útočníkem mohou obsahovat téměř cokoli, reklamou počínaje a malwarem konče.

**Petr Dvořák**
Profil byl vytvořen tak, aby věkově zaměřením a informacemi uvedenými v profilu odpovídal lidem v cílové skupině. Došlo ke standardnímu vyplnění informací v profilu (bydliště, předchozí zkušenosti, zájmy, záliby atd.), pouze s jedinou výjimkou, kterou byla profilová fotografie, jež byla získána pod licencí creative commons. Žádné jiné fotky, na nichž by byl Petr Dvořák zachycen v „normálním životě", v profilu nebyly.

Obrázek 25: Profilová fotka Petr Dvořák

341: Viz kap. 5.2.2.1.4 Zásah do systému (čl. 5).

342: Viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing.

343: Viz kap. 4.15 Identity theft.

Pro zvýšení důvěryhodnosti profilu bylo rozesláno 30 žádostí o přátelství. Do týdne přijalo tento profil za přítele 22 osob. Dle zkušeností z předchozích experimentů je to dostatečný počet pro získání určité důvěryhodnosti na sociální síti. Přátele doporučil Facebook na základě informací, které byly vyplněny v rámci profilu. Profil vystupoval jako aktivní profil, který aktivně komunikoval a přidával příspěvky a komentáře. Petr Dvořák oslovil zájmovou skupinu s žádostí o přijetí do skupiny. Cílovou skupinou byla skupina studentů VŠ, kteří se připravovali na státní závěrečné zkoušky. Právě na tuto skupinu byl zaměřen náš experiment.

Vlastní útok předpokládal vytvoření technického zázemí spočívajícího v zakoupení webhostingu a domény (www.grebni.cz),[344] kde byla nainstalována aplikace WordPress, do níž byl následně nainstalován doplněk pro ověřování uživatelů skrze FB GRAPH API.[345]

V cílové skupině se v době útoku nacházelo přibližně 150 uživatelů. Správce této skupiny přijal naši žádost do jednoho týdne od jejího podání (bez jakékoliv předchozí komunikace či ověření důvodu naší žádosti). Pro zvýšení věrohodnosti byl po přijetí přidán příspěvek v rámci skupiny a došlo ke komunikaci v rámci skupiny. Po přijetí do skupiny požádal Petr Dvořák o studijní materiály a téměř okamžitě dostal přístupové údaje do společného e-mailu, v rámci něhož byly tyto materiály sdíleny. Pokud by se jednalo o skutečného útočníka, mohlo by dojít např. k získání všech sdílených informací, či by mohlo dojít k nahrazení sdílených dat daty závadnými (např. infikovanými malwarem aj.).

344: Vlastní doména byla jedním z vodítek, která mohla kterémukoliv uživateli pomoci ověřit si identitu útočníka. Angl. překlad *„to grab" - popadnout, pokus o získání.* Po ověření vlastníka domény pomocí služby Whois se zobrazil pravý vlastník – Jan Nejedlý.

Dalšími možnostmi ověření pravosti profilu pak bylo: ověření profilové fotografie, vlastní komunikace s "útočníkem" (při přímé konfrontaci bychom uvedli, že se jedná o experiment. Nikdo nás však neoslovil) aj.

345: Aplikace umožňuje získání informací např.: ID, jméno, příjmení, pohlaví, jazykové nastavení, časová zóna, verifikace aj. Pro získání kompletního přístupu je zapotřebí, aby aplikace Graph API Explorer získala tzv. Access Token, který umožní verifikaci uživateli aplikace a zpřístupní útočníkovi rozsáhlé informace o uživatelích.


Obrázek 26: Prvotní příspěvek v cílové skupině

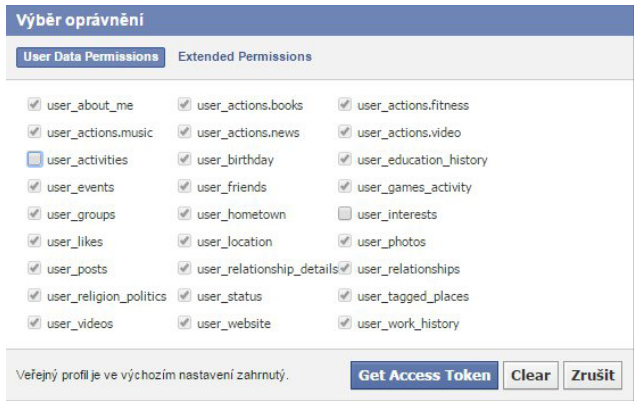
Díky přijetí Petra Dvořáka do cílové skupiny bylo možné sledovat, o co má daná skupina zájem. Na základě těchto informací pak bylo možné připravit vlastní útok.

V rámci vlastního útoku byl přidán příspěvek na web grebni.cz. Tento příspěvek, odkazoval na volně dostupné materiály na serveru drive.google.com. K tomuto odkazu se uživatelé dostali až po přihlášení přes Facebook. Důvodem umístění dat mimo službu Facebook byla ta skutečnost, že Facebook nedovoluje zveřejňovat příspěvky s klamavým obsahem.

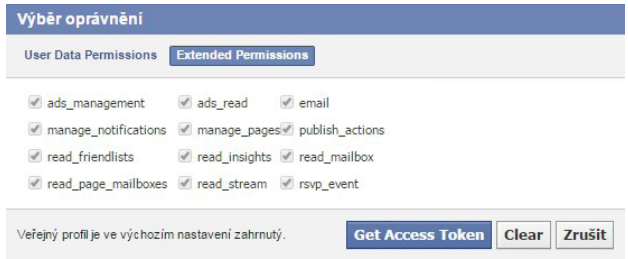
K získávání informací o uživatelích byla využita vlastní webová aplikace zaregistrovaná v rámci Facebook Graph API,[346] která je dostupná všem uživatelům v rámci Facebook developers. Tato aplikace pak umožňuje získávat data[347] od uživatelů a využívat je např. pro cílení reklamy aj.

346: Graph API je nástroj vyvinutý společností Facebook pro zjednodušení předávání dat mezi aplikacemi, využívající informace a ověření uživatele. Tato aplikace je určena zejména pro vývojáře, kteří potřebují integrovat funkcionality do svého kódu aplikace.
347: Obecně se pak jedná o data, která uživatel zveřejnil s nastavením zabezpečení na veřejně dostupné. Aplikace umožňuje získání informací, např.: ID, jméno, příjmení, pohlaví, jazykové nastavení, časová zóna, verifikace aj.

Pro získání kompletního přístupu k účtu uživatele je zapotřebí, aby aplikace Graph API získala Access Token, který umožní verifikaci aplikace ze strany uživatele a zpřístupní o něm útočníkovi rozsáhlé informace.[348]



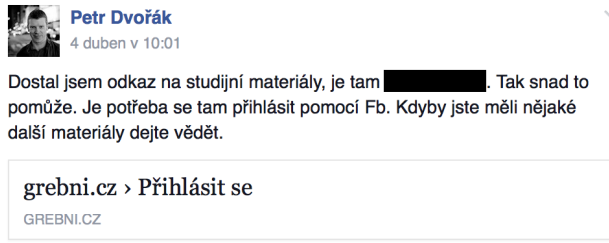

Obrázek 27: Výběr oprávnění (základní oprávnění aplikace)




Obrázek 28: Výběr oprávnění (rozšířená oprávnění aplikace)

Po několika dnech bylo zjištěno, že uživatelé mají zájem o „studijní materiály" ke státním závěrečným zkouškám. Díky této informaci došlo k provázání wordového dokumentu s námi vytvořenou aplikací.

348: Viz printscreeny: Obrázek 27: Výběr oprávnění (základní oprávnění aplikace) ;Obrázek 28: Výběr oprávnění (rozšířená oprávnění aplikace).




Obrázek 29: Nabídka materiálů ke stažení

V aplikaci, která byla nabízena uživatelům námi zvolené skupiny, došlo po kliknutí na nový příspěvek[349] sdílený „od útočníka“ k otevření okna, kde Facebook upozorňuje na předání údajů a následně byl zobrazen příspěvek, aby nedošlo k porušení smluvních podmínek služby Facebook.

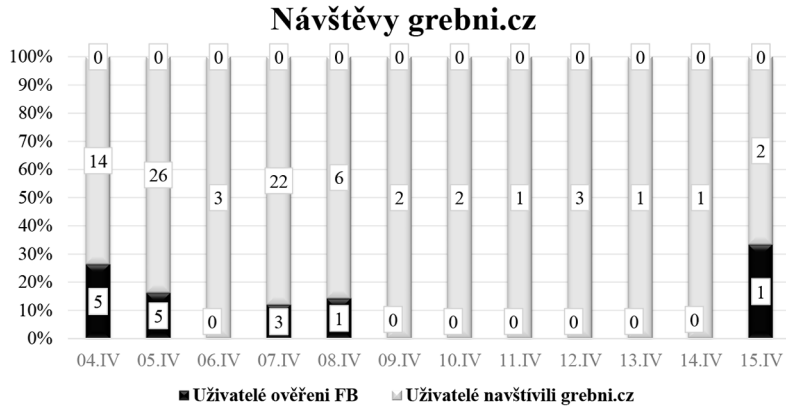

Obrázek 30: Upozorňuje na předání údajů

Vlastní útok trval jeden den s tím, že závadný příspěvek nebyl znovu zobrazován (sdílen). Příspěvek bylo možné pouze dohledat v již uskutečněné konverzaci.

I přes tuto skutečnost si námi nabídnuté dokumenty stáhlo 83 lidí ze 150.

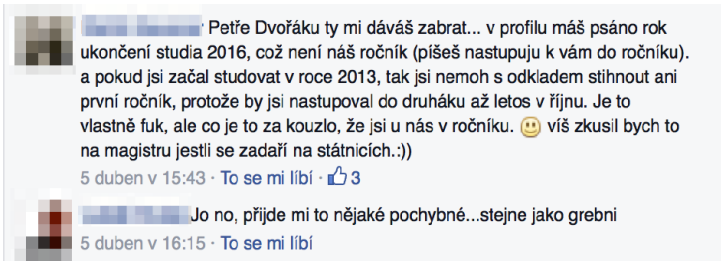
349: V našem případě fiktivní materiály pro studium.

Přes Facebook si nabízené materiály stáhlo 15 osob, 68 osob pak navštívilo stránky grebni.cz. V případě skutečného útoku by i na těchto stránkách mohl být umístěn například malware.




Obrázek 31: Návštěvy webových stránek proti ověřeným uživatelům FB

V rámci celé skupiny pouze dva uživatelé pochybovali o pravosti profilu Petra Dvořáka a jím nabízených materiálech. Nicméně i tyto osoby si uvedené materiály stáhly.




Obrázek 32: Vyjádření pochybností ohledně pravosti profilu a materiálů

Vzhledem k vyhodnocení druhého experimentu je třeba konstatovat, že jeho úspěšnost předčila naše očekávání. Potenciálně závadný materiál byl skupině nabídnut pouze jednou a pak odkaz na něj zapadl v diskusi. I přesto si materiály stáhlo přibližně 55 % uživatelů cílové skupiny.

### 3.4.3 Adam Novák

Jelikož se první experiment soustředil na děti zjevně mladší 13 let a druhý útok byl zaměřen na skupinu vysokoškolských studentů, rozhodli jsme se následující útok směřovat na osoby ve věku 15–25 let. Třetí empirický výzkum se zaměřoval opět na zjišťování, do jaké míry jsou uživatelé schopni (ochotni) se „spřátelit" s osobami, které neznají a které jsou podezřelé. Dále bylo cílem výzkumu zjistit, jak moc živelně nám začne služba Facebook nabízet další podobné uživatele či „přátele přátel". Toto zjištění je z hlediska možného reálného útoku zásadní, neboť pokud se osoba stane dostatečně „důvěryhodnou" a bude mít „dostatek společných přátel", pak mnohem snadněji získá přístup ke skutečnému cíli útoku.[350]

Před vlastním útokem jsme si stanovili hypotézu, že díky výuce a vzdělávání se v oblasti ICT by námi zvolená skupina měla být více obezřetná, a neměla by proto neuváženě přijímat přátelství od neznámých osob. Dále jsme předpokládali, že uživatelé nebudou důvěřovat osobě, kterou by dle vyplněných profilových informací bylo možné považovat za pedofila.

#### Adam Novák

Vlastní falešný profil Adama Nováka měl u oběti evokovat minimálně podezření. V profilu byly vyplněny následující informace:

- **Muž;**
- **Věk 42 let;**
- **Profilové foto** (stejně jako ostatní osobní fotografie) nezobrazuje obličej a ani jinak neumožňuje ověření pravosti (tj. skutečný věk aj.);
- **Vysokoškolsky vzdělaný;**
- **Pocházející z Brna, žijící v Praze;**
- **Pracující z domova** (Uživatel si tedy nemá možnost ověřit totožnost osoby např. u firmy, kde by osoba pracovala).

350: Blíže viz: NEJEDLÝ, Jan. *Dítě jako cíl kyberpredátora.* Praha 2015. Studentská vědecká a odborná činnost, Policejní akademie ČR v Praze, Sekce právní vědy. Vedoucí práce Jan Kolouch.

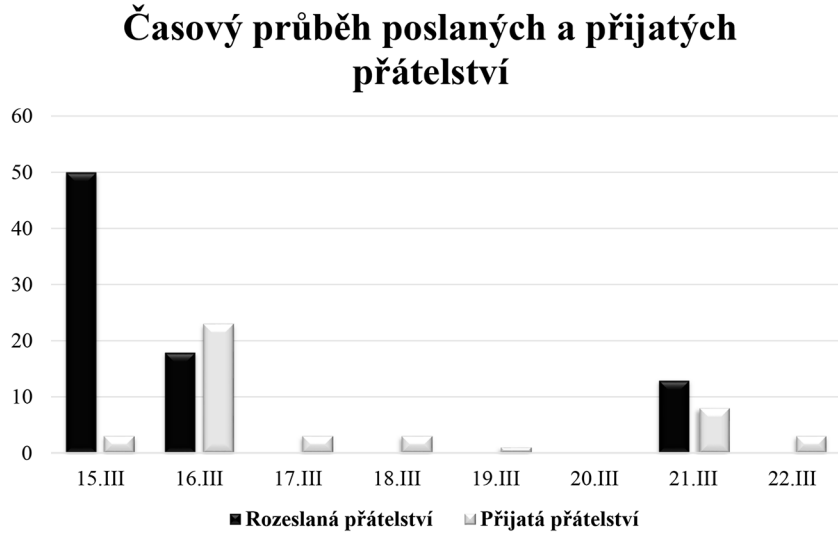
Obrázek 33: Profilová fotka Adam Novák

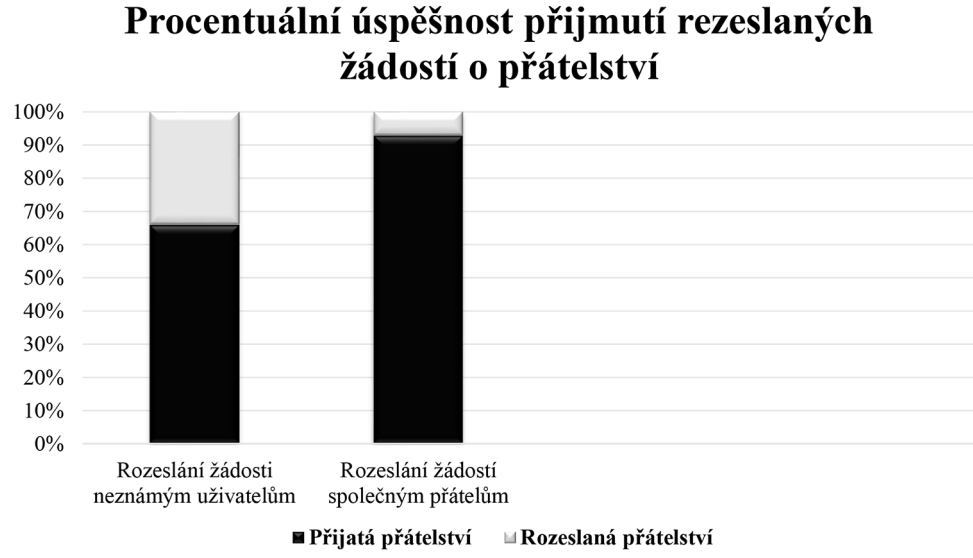
Jako doplňkové informace byly uvedeny především seriály a filmy, které měly evokovat nedůvěryhodnost profilu, neboť jako dospělý muž má Adam Novák zálibu zejména v následujících seriálech (Tom and Jerry; Popeye the Sailor; Pat a Mat; SpongeBob SquarePants; Shaun the Sheep aj.).

Po vytvoření profilu došlo ke stanovení časového plánu rozesílání žádostí o přátelství. Bylo stanoveno, že vlastní útok bude probíhat po dobu 7 dní.

V první vlně (15. 3. 2016 cca ve 23.30) bylo rozesláno celkem 50 žádostí o přátelství (s tím, že ještě týž večer byl falešný profil akceptován 3 osobami – ve věku přibližně 10–15 let). Druhá vlna žádostí byla rozeslána následující den ráno (celkem 18 žádostí). Po čtyřech dnech skončila odezva uživatelů na již zaslané žádosti. Pokud by žádosti byly rozeslány znovu či byly urgovány, lze předpokládat (na základě předchozích projektů), že by došlo k přijetí mezi přátele i u jiných osob (což však nebylo cílem výzkumu. Cílem této části výzkumu bylo zjistit, kolik lidí si přidá zjevně nedůvěryhodný a podezřelý profil bez jakékoli komunikace či urgence).

Poslední vlna útoku využila té skutečnosti, že falešný profil byl již akceptován uživateli a stal se „přítelem“. Poslední vlna žádostí měla ověřit akceptaci profilu „přáteli přátel“. V poslední vlně **bylo rozesláno celkem 13 žádostí a falešný profil byl akceptován 9 osobami**. Veškerá výše uvedená data jsou zahrnuta v následujících grafech.


Časový průběh poslaných a přijatých přátelství
60
50
40
30
20
10
0
15.III
16.III
17.III
18.III
19.III
20.III
21.III
22.III
Rozeslaná přátelství
Přijatá přátelství


Procentuální úspěšnost přijmutí rezeslaných žádostí o přátelství
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Rozeslání žádosti neznámým uživatelům
Rozeslání žádostí společným přátelům
Přijatá přátelství
Rozeslaná přátelství

## 3.5 Doporučení pro uživatele sociálních sítí

Na závěr kapitoly uvádím některá doporučení, která je vhodná akceptovat (nejen) v prostředí sociálních sítí. Tato doporučení vycházejí z doporučení uvedených na webu bezpečnýinternet.cz,[351] avšak jsou doplněna o vlastní rady a zkušenosti.

- **Přečtěte si smluvní podmínky služby, kterou používáte.**
  - Pokud se neseznámíte alespoň se základními podmínkami užívání služby, můžete tak nevědomky souhlasit se sdílením choulostivých informací o vaší osobě.

- **Nastavte si u svého účtu patřičné zabezpečení.**
  - nastavit telefonní číslo jako další vrstvu zabezpečení,
  - nastavte si hesla k aplikacím, které přes sociální síť používáte,
  - uveďte důveryhodné kontakty aj.

- **Omezte okruh osob, kterým sdělujete citlivé informace.**

- **Nepovolujte „přátelství" lidem, které neznáte.**

- ***Zvažte, zda je vhodné nechat zapnutou geolokaci.***
  - Geolokace Vám sice ukáže přátele v okolí, ale zároveň umožňuje de facto sledovat Váš pohyb během celého dne.

- **Neuvádějte na svém profilu veřejně své telefonní číslo, adresu, soukromou e-mailovou adresu, účty na jiných sociálních sítích, své koníčky (záliby), navštěvované aktivity aj.**
  - Tyto informace mohou sloužit potenciálnímu útočníkovi. Na základě těchto informací si je útočník schopen sestavit váš denní režim.

- **Nikdy nikomu nesdělujte hesla, ani další přístupové údaje k vašim účtům na sociálních sítích, k hrám, e-mailům aj.**

- **Nikdy neodpovídejte na neslušné, hrubé nebo vulgární e-maily a vzkazy.**
  - Odpověď může útočníka vybízet k dalším vulgaritám.

- **Neposílejte nikomu svou intimní fotografii či video.**[352]

351: Bezpečný internet. *Rady pro bezpečné používání sociálních sítí* [online]. [cit. 24.3.2014]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/rady.aspx

352: Viz kap. 4.14.3 Sexting.

- **Nedomlouvejte si schůzku přes Internet, aniž byste o tom řekli někomu jinému.**
  - Nikdy nemůžete věřit člověku, kterého osobně neznáte. Může se jednat o nebezpečnou osobu, která vás v krajním případě může ohrozit na zdraví či na životě.

- **Nevěřte každé informaci, kterou na Internetu získáte.**
  - Také na Internetu platí, že každá získaná informace by měla být ověřena z více zdrojů.

- **Když s někým nechcete komunikovat, nekomunikujte.**

- **Nesdělujte informace typu, kdy jedete na dovolenou a podobně.**
  - Informace o opuštění bydliště, přítomnosti velké finanční hotovosti či pořízení drahého vybavení domácnosti může přilákat zloděje.

- **Fotografie i video je možné zfalšovat. Komunikace přes webovou kameru Vám nezaručuje, že na druhé straně je skutečně daná osoba.**[353]

- **NEAKCEPTUJTE NEZNÁMÉ APLIKACE A NEKLIKEJTE NA NEZNÁMÉ ODKAZY!**

**Rady pro rodiče:**
- Zvažte, zda je dítě již dost vyzrálé pro používání Internetu a sociálních sítí.
- Mluvte s dítětem o prostředí, možnostech a rizicích Internetu.
- Naučte se ve virtuálním prostředí orientovat, lépe pochopíte možné hrozby.
- Pokuste se dítěti zabránit v nadbytečném trávení času na Internetu.
- Komunikujte s dítětem otevřeně o všech jeho problémech.
- Všímejte si změn nálad a chování dítěte a pokuste se odhalit jejich příčinu.
- Pokud bude dítě prostřednictvím Internetu ohroženo či napadeno, obraťte se na odborníky (administrátor či správce stránek, internetové poradny, Policie České republiky, organizace věnující se bezpečnosti online[354]).

**Další doporučení a rady, které je vhodné respektovat při pohybu na sociálních sítích, je možné nalézt například na následujících stránkách:**
- Look Up - Otevři oči: http://youtu.be/M4WCEzhaIrc

**Více o sociálních sítích – novinky infografiky, zajímavosti:**
- http://www.tyinternety.cz/rubrika/socialni-site/
- http://www.lupa.cz/n/socialni-site/#ic=text-labels&icc=socialni-site
- http://www.justit.cz/wordpress/category/socialni-site/

353: Blíže viz Webcam Trolling. *Podvody s falešnými webkamerami řádí i v ČR.* [online]. [cit. 7.8.2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/637-podvody-s-falenymi-webkamerami-

354: Např. http://www.saferinternet.cz/; http://www.bezpecnyinternet.cz aj.

**Více o zabezpečení a ochraně na sociálních sítích:**
- Jak na Internet (Rizika sociálních sítí): http://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/
- Centrum rodinné bezpečnosti Facebooku: https://www.facebook.com/safety/
- Centrum zásad a bezpečnosti YouTube: https://www.youtube.com/yt/policyandsafety/cs/
- Bezpečné užívání Facebooku: https://www.facebook.com/safety/groups/teens/
- Jak mohu někoho zablokovat: https://www.facebook.com/help/168009843260943
- Video o tom, jak si deaktivovat nebo zrušit FB účet: https://www.stream.cz/jaknato/665941-jak-zrusit-ucet-na-facebooku
- Video se shrnutím, jak se chovat na sociálních sítích: http://www.youtube.com/watch?v=glIRQzSJ-C0
- Vtipné video na téma Facebook versus realita: https://www.youtube.com/watch?v=22gUYhzG3iI
- Rady pro uživatele Internetu pojaté zábavnou formou: http://sheeplive.eu/?r=ovce

## 3.6 Právo být zapomenut

Při používání informačních a komunikačních technologií a stále většímu objemu dat zveřejňovaných samotnými uživateli nutně došlo ke vzniku žádostí o potlačení či smazání dat, která nejsou aktuální, či která nějakým způsobem poškozují uživatele samotného. Pro tuto činnost se užívá pojem právo být zapomenut. Toto právo vystoupilo do popředí v souvislosti s Rozsudkem Soudního dvora EU C-131/12.[355]

Mario Costeja González si v roce 2010 úřadu na ochranu osobních údajů ve Španělsku postěžoval, že je mu ve výsledcích hledání v Googlu po zadání jeho jména zobrazován odkaz na novinové články z roku 1998, kde se psalo o dražbě jeho majetku kvůli dluhům na sociálním pojištění. Mario Costeja González se dožadoval (po poskytovateli webových stránek, na nichž byla tato informace uvedena) smazání informací nebo jejich úpravy tak, aby s ním nemohly být dále spojovány. Po společnosti Google požadoval obdobnou úpravu výsledků vyhledávání. „*Jde o minulost, všechny dluhy jsem splatil a jejich spojování s mým jménem je dnes irelevantní,*" argumentoval.[356] Společnost Google odmítla ovlivnit výsledky vyhledávání skrze svoji aplikaci.

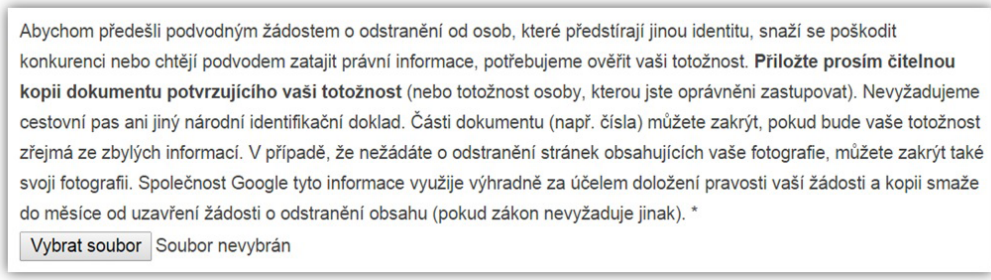
Celý spor se dostal až k soudnímu dvoru EU, který rozhodl, že *„provozovatel vyhledávače musí za určitých podmínek ze zobrazeného seznamu výsledků vyhledávání provedeného na základě jména osoby*

355: Rozsudek soudního dvora (velkého senátu) EU C-131/12, ze dne 13. 5. 2014. [online]. [cit. 24.3.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d59c3214d6fafa4d6cae2ede058bf9fcdb.e34KaxiLc3qMb40Rch0SaxuNb3z0?text=&docid=152065&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=272305

356: Blíže viz např. SLÍŽEK, David. *Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost.* [online]. [cit. 4.11.2015]. Dostupné z: http://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

*vymazat odkazy na webové stránky zveřejněné třetími osobami a obsahující informace týkající se této osoby. Soudní dvůr upřesnil, že tuto povinnost může mít rovněž v případě, že toto jméno nebo tyto informace nebyly předtím nebo současně vymazány z uvedených webových stránek, a to případně i tehdy, jestliže je jejich zveřejnění na uvedených stránkách samo o sobě v souladu se zákonem.*"

Společnost Google na uvedený rozsudek zareagovala doplněním smluvních podmínek. Výňatek z těchto smluvních podmínek je možné nalézt na následujícím printscreenu:


Abychom předešli podvodným žádostem o odstranění od osob, které předstírají jinou identitu, snaží se poškodit konkurenci nebo chtějí podvodem zatajit právní informace, potřebujeme ověřit vaši totožnost. **Přiložte prosím čitelnou kopii dokumentu potvrzujícího vaši totožnost** (nebo totožnost osoby, kterou jste oprávněni zastupovat). Nevyžadujeme cestovní pas ani jiný národní identifikační doklad. Části dokumentu (např. čísla) můžete zakrýt, pokud bude vaše totožnost zřejmá ze zbylých informací. V případě, že nežádáte o odstranění stránek obsahujících vaše fotografie, můžete zakrýt také svoji fotografii. Společnost Google tyto informace využije výhradně za účelem doložení pravosti vaší žádosti a kopii smaže do měsíce od uzavření žádosti o odstranění obsahu (pokud zákon nevyžaduje jinak). *

Vybrat soubor Soubor nevybrán

Vtipně a velmi výstižně komentuje právo být zapomenut **John Oliver** ve svém pořadu **Last Week Tonight** dostupném z: https://www.youtube.com/watch?v=r-ERajkMXw0, kde mimo jiné uvádí, že *„to co soudní dvůr EU nechápe, je, že Internet je jako pohyblivý písek. Čím agresivněji bojujete o odstranění sebe (odkazů o sobě) z Internetu, tím více zapadáte do onoho pomyslného písku. A výsledek? Muž, který nechtěl být znám pro to, že v roce 1998 byl dlužníkem, je nyní celosvětově známým právě pro to, že byl dlužníkem. Jedinou věc, kterou o něm vím, je ta jediná věc, kterou on nechtěl, abych věděl.*"

**Jak to bude dál s „anonymitou" a právem být zapomenut?**
Vize, že digitální svět a jeho uživatelé začnou být anonymní, je dle mého názoru utopií. Nic na tomto tvrzení nezmění ani různé možnosti anonymizace v podobě např. služeb TOR network[357] aj., neboť vždy bude docházet k interakci se světem reálným a vždy budou v digitálním světě figurovat uživatelé, kteří jsou omylní a kteří při sebelepším zakrývání informací o své činnosti chybují. Stejně tak je utopií se domnívat, že technika bude zapomínat. O uživatelích budou nadále sbírána data. To, k čemu dojde, bude další technické nastavení toho, komu se uvedená data budou zobrazovat a komu nikoli.

357: Některé případy narušení bezpečnosti TOR network:
*FBI Exploits Flash Vulnerability to Breach Tor Network Security*. [online]. [cit. 23.7.2016]. Dostupné z: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/
*Tor security advisory: "relay early" traffic confirmation attack*. [online]. [cit. 23.7.2016]. Dostupné z: https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

K „deanonymizaci" uživatelů bezesporu přispívá jak provázanost jednotlivých nabízených služeb a možnost předávání informací o uživatelích třetím stranám, tak i **Internet věcí (IoT)**.

Se zajímavým řešením „deanonymizace" uživatelů přišla např. společnost Facebook, vyvíjející metodu **DeepFace**, která je založena na vytvoření 3D modelu obličeje na základě definovaných výchozích bodů na fotografii.[358] Na základě této metody lze identifikovat i osoby, které nemají facebookový účet a byly pouze označeny (identifikovány) jako konkrétní osoba. Metoda DeepFace je zde uvedena záměrně, neboť možnost využití této metody je zakotvena ve smluvních podmínkách služby Facebook a umožňuje, byť si to uživatel nebude přát (např. sám se úmyslně neoznačí pod fotografií), jeho identifikaci.

Pokud jde o **IoT**, pak zásah nových technologií a naše „deanonymizace" je ještě patrnější. Jako příklad uvedu „smart TV"[359], která při vlastní instalaci opět nabídne smluvní podmínky k odsouhlasení a okamžitě poté „se ptá" po možnosti připojení k síti Internet. Podrobnějším prostudováním smluvních podmínek můžete například zjistit, že tato televize je oprávněna poskytnout záznam důvěrných a osobních hovorů či aktivit, které *„před ní vedete"*, a to za předpokladu, že využíváte funkci voice či motion control. V rámci smluvních podmínek budete upozorněni i na tu skutečnost, že zaznamenaná data jsou předávána výrobci a třetím stranám. Jediným řešením, jak zabránit předávání těchto informací, je vypnutí voice či motion recognition. Otázkou je, zda je to skutečně řešení. Osobně si myslím, že řešením by bylo vypnutí či omezení přenosu dat, případně určení subjektu, s nímž jsem ochoten tato osobní data sdílet.

Pokud jde o právo být zapomenut, dokáži si představit hypotetickou situaci, kdy uživatel bude žádat, aby společnost, jež vyrobila danou televizi či jiný počítačový systém s podobnými smluvními podmínkami, vymazala záznam hovoru např. z 1.3.2016. Soud i na tento případ aplikuje právo „být zapomenut", avšak je otázkou, kdo skutečně zaručí uživateli, že jeho data byla smazána ze všech datových úložišť.

Výňatek ze Samsung EULA:

***„Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition."***

Anonymita na Internetu není a rozhodně v blízké budoucnosti ani nebude. Uživatelé mnohdy, zcela logicky, oprávněně intenzivně bojují proti intervenci státu do svého soukromí, avšak na

358: Blíže viz např.: *Facebook will soon be able to ID you in any photo.* [online]. [cit. 9.8.2015]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

359: Dále viz např. ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit. 9.8.2015]. Dostupné z: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

straně druhé toto soukromí sami dobrovolně a mnohem vstřícněji nabízí všem v okolí (např. na sociálních sítích, v rámci cloudových služeb aj.).

Nemyslím si, že by propast mezi světem reálným a digitálním byla natolik obrovská, a možná i proto mnohdy nechápu bezmyšlenkové chování uživatelů, pokud jde o nabízené služby ze strany ISP. Ano, jako uživatelé získáme v rámci smluvních podmínek, které uzavíráme, nějakou službu. Otázkou je, zda je tento obchod výhodný a zda cena, kterou za tuto službu platíme, je přiměřená.

Osobně si plně uvědomuji tu skutečnost, že moje svoboda, včetně jisté míry „anonymity" na Internetu, je již v současnosti utopií. Domnívám se, že tato utopie bude v brzké budoucnosti i díky IoT a stále většímu propojování všech „services" dovedena téměř do situace, ne nepodobné té v Minority Report. Na druhou stranu však věřím, nebo spíše chci věřit tomu, že jsem pořád svobodný a mám právo volby.

Toto mé právo volby pak minimálně spočívá v mém rozhodnutí, zda, případně jaké služby (services) chci využívat a za jakých podmínek. Myslím si, že uživatelé by se měli stát onou skutečnou definiční autoritou Internetu, a to minimálně v té podobě, že projeví svoji vůli a budou se snažit vydobýt si svá práva i na poskytovateli služeb, neboť v případě intervence státu do jejich soukromí se jim to v řadě případů daří.

Ostatně zhodnocení, jak moc je daná služba „agresivní", respektive jak moc zasahuje do vašeho soukromí, je možné nalézt např. na stránkách: **Terms of Service, Didn't Read**: https://tosdr.org/. Když už nic jiného (byť je zde možné použít analogii o „Digitální demenci"), tak alespoň kontrola základních podmínek na této stránce může pomoci uživatelům, aby se v dané problematice částečně zorientovali.

# 4 Projevy kyberkriminality

*„Si vis pacem, para bellum.“*
*„Kdo chce mír, chystá se na válku.“*
Flavius Vegetius Renatus

*„Scientia potestat est.“*
*„Vědění je moc.“*
Francis Bacon

## 4 Projevy kyberkriminality

Kyberkriminalita se typicky projevuje prostřednictvím tzv. kybernetických útoků,[360] nicméně k úspěšnému uskutečnění řady útoků je třeba využít i ryze netechnické aspekty. Při definování toho, co vše je a co už není kyberkriminalitou, je vhodné využít definici uvedenou v kap. 1.1 Kybernetická trestná činnost (Cybercrime). Určitá protiprávní jednání v kyberprostoru či jednání související s kyberkriminalitou je možné podřadit pod příslušná ustanovení platného trestního zákoníku, existují však určité typy jednání, jejichž označení za trestné činy může být podstatně obtížnější, či dokonce nemožné (v řadě případů se spíše jedná o pouze nemorální jednání).

Velmi často je kyberkriminalita považována za nový druh kriminality, nicméně značná část kyberkriminality využívá či přenáší notoricky známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí digitálního, ve kterém je lze páchat „lépe, rychleji, efektivněji" než ve světě reálném. Mezi ryze kybernetické útoky by pak bylo možné zařadit např. hacking, DoS a DDoS útoky, botnety aj.

Pro svět virtuální je příznačné, že většina uživatelů v něj má dle mého názoru až nepochopitelnou, téměř bezmeznou důvěru.[361] Přičemž je třeba konstatovat, že svět virtuální se pro nás stává čím dál tím významnějším. Osobně mám pocit, že v případě využívání poskytovaných služeb na Internetu mnoho lidí přestane přemýšlet o možných rizicích či hrozbách. Primárně jsou uchváceni zdánlivě nekonečnými možnostmi „nových technologií"; jak jinak je pak možné vysvětlit si absenci základních obranných principů a mechanismů ve světě virtuálním, když ve světě reálném bychom se chovali zcela jinak. Jindy mi naopak uživatelé kyberprostoru svým chováním v něm připomínají „*Podivný případ Dr. Jekylla a pana Hyda*" [orig. Strange Case of Dr. Jekyll and Mr. Hyde - Robert Louise Stevenson (1886)]. Zdánlivě slušní lidé ve světě reálném, se v „pseudoanonymním" prostředí kyberprostoru projevují bez jakýchkoli legálních nebo morálních zábran. Je tak možné narazit například na případ soudce, jenž si stahuje „dětskou pornografii"[362], uživatele, kteří v reálném světě nikdy nic neukradli, ale ve světě virtuálním nemají problém krást,[363] či porušovat jiná práva chráněná zákonem té které země.

K prognózám vývoje kyberkriminality se v minulosti vyjadřovala celá řada předních odborníků, z nichž si dovolím citovat zejména Schneiera, který v roce 2002 predikoval, že dalším velkým bezpečnostním trendem v Internetu bude zločin. *„Nepůjde o případy virů, trojských koní a DDoS útoků pro zábavu nebo možnost se vychloubat se svými schopnostmi. Půjde o skutečný zločin. V Internetu.*

360: Viz kap. 1.2.1 Kyberprostor (Cyberspace).

361: Viz například reakce uživatelů na jednání popsané v kap. 4.5.2 Hoax aj.

362: *Judge, 69, who downloaded child porn facing 'catastrophic humiliation'.* [online]. [cit. 1.9.2009]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

363: HILL, Kashmir. *These two Diablo III players stole virtual armor and gold - and got prosecuted IRL.* [online]. [cit. 10.8.2015]. Dostupné z: http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/

*Zločinci mají sklon zaostávat za vývojem technologií o pět, deset let, ale nakonec si uvědomí jejich možnosti. Tak jako Willie Sutton začal přepadat banky „protože tam byly peníze", tak moderní zločinci začnou útočit přes počítačové sítě. Stále více hodnot (finančních prostředků) je online, než v peněžích reálných.* "[364]

V roce 2007 představil Jirovský statistiku FBI, která porovnávala běžné „bankovní přepadení" (loupež) s jednáním, které má povahu phishingového útoku.[365]

| 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 u 15 % útočníků a z nich je odsouzeno jen 50 %. |
| **Trest** | Průměrně 5–6 let, pokud pachatel při loupeži nikoho nezranil. | Průměrně 2–4 roky. |

Goodman v roce 2012 ve vztahu k informačním a komunikačním technologiím uvádí, že „*schopnost jedince ovlivnit masy, právě díky těmto technologiím, roste exponenciálně. Exponenciálně roste jak v oblasti ‚dobrého, tak zlého účelu'*". Názorně tento růst prezentuje na vývoji zločinu loupeže, ke kterému v minulosti původně stačil nůž či pistole a de facto docházelo k loupežnému přepadení mezi jednotlivci či malými skupinami. „*K zásadní „inovaci" došlo v okamžiku loupežného přepadení celého vlaku, ve kterém cestovalo 200 lidí.* " Internet umožňuje ještě výraznější rozsah útoku jedné osoby. Okradení velkého množství uživatelů dobře demonstruje případ Sony Playstation s přibližně 100 miliony poškozených osob. „*Kdy v historii lidstva mohl jedinec okrást 100 milionů lidí? Ale nejde jen o krádeže…* "[366]

V témže roce vystoupil s proslovem na RSA Cyber Security Conference (San Francisco, CA) ředitel FBI Robert S. Mueller, který mimo jiné ve své řeči uvedl: „*Jsem přesvědčen o tom, že existují pouze dva druhy společností: takové, do kterých se již hackeři nabourali, a ty, do nichž se teprve nabourají. A i tyto dvě skupiny se velmi rychle spojují v kategorii jedinou: společnosti, do jejichž systémů hackeři*

364: Překlad autora. Blíže viz SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing.* [online]. [cit. 6.11.2007]. Dostupné z https://www.schneier.com/crypto-gram/archives/2002/1215.html

365: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 30

366: Překlad autora. Blíže viz GOODMAN, Marc. *A vision of crimes in the future.* [online]. [cit. 13.11.2014]. Dostupné z: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

*pronikli, a společnosti do nichž proniknou znovu.*"[367]

V současnosti dochází ke stále většímu a masivnějšímu propojování různých počítačových systému do kyberprostoru, což de facto generuje přímou úměru spočívající v následujícím tvrzení: *„čím více je připojených zařízení, tím větší je jejich zranitelnost a tím větší bude počet útoků.*" Jedno z grafických znázornění probíhajících útoků je možné nalézt na stránkách: http://map.norsecorp.com/#/; https://cybermap.kaspersky.com/; https://map.lookingglasscyber.com/ aj.

Domnívám se, že není možné pochybovat o tom, že kyberkriminalita je na vzestupu a představuje celosvětový problém. Různé statistiky uvádějí částečně rozdílné škody způsobené právě kyberkriminalitou, nic to však nemění na tom, že všechny do těchto škod započítávají škody primární (např. nefunkčnost počítačového systému, jeho části, nabízené služby, výpadek infrastruktury aj.) a škody sekundární (např. obnova systémů, záchrana dat, znovu připojování koncových uživatelů aj.). Europol ve své zprávě z roku 2014[368] uvádí, že kyberkriminalita stojí globální ekonomiky přibližně 300 miliard $ ročně. Komunita útočníků se od masového rozšíření Internetu značně změnila. Primárně už se nejedná o individuality, které páchaly protiprávní jednání pro zábavu či překonávání překážek. V současnosti se zpravidla jedná o profesionály, kteří svoji činnost dělají s cílem profitovat a nezřídka jsou zapojeni do organizovaných skupin.

Tento posun je pochopitelný a neodmyslitelně spojený se třemi aspekty:

1) **Závislost společnosti na Internetu** (resp. nabízených službách, technologiích aj.),

2) **Kyberkriminalita se stala výnosným globálním businessem** [již první kybernetické útoky ukázaly možnosti zisku finančních prostředků, ať již přímo (odčerpáním financí), či zprostředkovaně (např. platbou za poškození služby jiné osoby)].

3) **Minimální gramotnost uživatelů**, kteří značně využívají informační a komunikační technologie (uživatel je typickým příkladem toho nejslabšího článku řetězu).

S rozvojem všemožných služeb postavených na principu as-a-service[369] vznikla i v prostředí kyberkriminality řada platforem (typicky undergroundových, darknet fór), kde jsou nabízeny služby, které je možné označit za **Crime-as-a-service** (cybercrime-as-a-service). Dochází tedy ke vzniku *„malware či underground economy*", která poskytuje téměř jakémukoli uživateli prostředky ke

367: MUELLER, Robert. [online]. [cit. 3.4.2013]. Dostupné z:
https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

368: Viz *The Internet Organised Crime Threat Assessment (iOCTA) 2014*. [online]. [cit. 10.8.2015]. Dostupné z:
https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

369: Jedná se o poskytování služeb typicky spojených s cloudovým řešením. Jako příklady je možné uvést: infrastructure-as-a-service; platform-as-a-service; Service-as-a-service; Security-as-a-service aj.

spáchání kybernetických trestných činů. V rámci služby souhrnně označované crime-as-a-service jsou standardně nabízeny následující služby:

- *Research-as-a-service,*[370]
- *Crimeware-as-a-service,*[371]
- *Infrastructure-as-a-service,*[372]
- *Hacking-as-a-service,*[373]
- *Data-as-a-service,*[374]
- *Spam-as-a-service,*[375]
- *Ransomware-as-a-service*[376] aj.

Výčet jednotlivých služeb není konečný a je možné konstatovat, že v rámci služby crime-as-a-service si lze objednat jakoukoli myslitelnou službu nebo komoditu, kterou lze v kyberprostoru využít či získat. Rozmach těchto negativních aktivit je přímo spojen i s fenoménem Internetu věcí (IoT), který propojuje zařízení (počítačové systémy) s Internetem, a představuje tak další výraznou hrozbu, která primárně spočívá v nerespektování některého ze základních principů bezpečnosti.[377]

Řada výrobců či distributorů počítačových systémů, které je možné zařadit pod pojem IoT, neřeší otázku bezpečnosti (jejich cílem je co nejdříve na trh uvést a prodat co nejvíce zařízení, jež je možné označit za počítačový systém), čehož útočníci využívají.

370: Pod touto službou je možné si představit aktivity, které spočívají v odhalování nejrůznějších, dosud neznámých zranitelností cílového počítačového systému, či software (tyto zranitelnosti jsou známy jako zero-day vulnerabilities). Vlastní činnost v rámci Research-as-a-service nemusí mít nutně povahu kriminálního či protiprávního jednání. Odhalování zranitelností a chyb se věnuje řada odborníků z IT bezpečnosti (např. penetrační testování aj.). Typicky jsou tyto služby poskytovány na základě smluvních podmínek mezi testovaným a testujícím, či za využití některé z okolností vylučujících protiprávnost. Viz kap. 5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru.

371: Služba crimeware-as-a-service nabízí celou řadu aktivit od prostého prodeje malware, přes jeho „úpravu na míru", dále pak dodávání exploitů (zranitelností) aj.

372: Infrastructure-as-a-service pak představuje nabídku fyzických či virtuálních počítačových systémů (botnety, hostingové služby, pronájmy sítí aj.).

373: Tato služba v sobě může zahrnovat prosté prolomení přístupových údajů k e-mailu, účtu na sociální síti aj. až po profesionální a sofistikované útoky na vybranou oběť. Do této oblasti pak může spadat např. i provedení útoků typu DoS a DDoS. Blíže viz kap. 4.8 Hacking.

374: Služba data-as-a-service nabízí nejžádanější komoditu, kterou jsou právě data. Konkrétně se jedná např. o: přístupové údaje (jméno a heslo) k různým účtům, kreditní karty, bankovní účty, kradené kreditní karty, ale i informace o osobách (bydliště, data narození, telefonní čísla, e-maily aj.).

375: Z názvu vyplývá, že je možné si objednat a zaplatit spamovou kampaň. Blíže viz kap. 4.5 Spam.

376: Blíže viz kap. 4.4 Ransomware.

377: Viz kap. 1.2.1 Kyberprostor (Cyberspace).

Náklady spojené s vývojem v oblasti bezpečnosti jsou zpravidla nejnákladnější součástí vývoje, nicméně je to oblast, které je třeba se věnovat i s ohledem na již známé hrozby. Mezi ně například patří: nezabezpečený komunikační kanál u kardiostimulátoru;[378] auto či letadlo, jež lze ovládat na dálku;[379] chytrá domácnost či její součásti (lednice, kotel, zabezpečovací systém, televize aj.), jež lze ovládat na dálku[380] aj.

*„Jak asi dopadne svět, když máme už tento rok využívat 6,4 miliardy zařízení spadajících do IoT. Za další čtyři roky by to mělo být 20,8 miliardy zařízení. Řada z těchto zařízení navíc bude mít oproti běžnému životnímu cyklu mobilních telefonů, tabletů či laptopů podstatně delší životnost. Jak bude výrobce automobilů schopen chránit bezpečnost modelu z roku 2020 o deset let později? Nebo ledničky, která vám doma může stát i dobrých patnáct let? Jak dlouho trvalo, než se Microsoft naučil, jak aktualizovat vlastní operační systém?“* [381]

Schneier ve vztahu k datům uvádí, že útočníci s nimi mohou dělat v podstatě tři základní věci: krást je (narušení principu **Confidentiality** – důvěrnosti), měnit je (narušení principu **Integrity** – celistvosti) nebo zabraňovat vlastníkům v přístupu k nim (narušení principu **Availability** – dostupnosti). Schneier uvádí, že s nástupem IoT se právě poslední dva druhy útoků stanou extrémně účinné.[382]

V následující části představím některé útoky, ke kterým v prostředí kyberprostoru dochází. Nelze vymezit všechny útoky, ať již z důvodu rozsahu této publikace, či z důvodu nemožnosti popisu všech možných alternativních jednání subsumovatelných pod pojem kyberkriminalita. Pokud to bude možné, bude u konkrétního projevu kyberkriminality uvedena i případná trestněprávní kvalifikace takovéhoto jednání.

---

378: Srov. TAYLOR, Harriet. *How the „Internet of Things“ could be fatal.* [online]. [cit. 17.6.2016]. Dostupné z: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

379: Blíže viz GREENBERG, Andy. *Hackers remotely koll a Jeep on the highwaty – with me in it.* [online]. [cit. 4. 5. 2016]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
V české verzi dostupné např. na:
http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani-auta-f1l-/automoto.aspx?c=A150723_135910_automoto_fdv
Blíže viz ZETTER, Kim. *Is It Possible for Passengers to Hack Commwrcial Aircraft?* [online]. [cit. 5. 5. 2016]. Dostupné z: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

380: Je tak možné např. obejít zabezpečení domácnosti; zvyšovat teplotu pomocí dálkově ovládaného termostatu a způsobit tak jinému škodu; objednat nesmyslné množství potravin prostřednictvím „chytré“ lednice aj.

381: DOČEKAL, Daniel. Bruce Schneier: *Internet věcí přinese útoky, které si neumíme představit.* [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/

382: SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into a Real World Disasters.* [online]. [cit. 10. 8. 2016]. Dostupné z:
https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

## 4.1 Sociální inženýrství (Sociotechnika)

*„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist."*
Albert Einstein

Sociální inženýrství nelze za každých okolností považovat přímo za kybernetický útok, nicméně je předpokladem pro to, aby byla řada kybernetických útoků úspěšná.

Pokud bychom chtěli definovat pojem sociální inženýrství, bylo by možné říci, že jde o ovlivňování, přesvědčování či manipulaci s lidmi s cílem je donutit provést určitou akci, či od nich získat informace, které by jinak neposkytli. Smyslem je v oběti navodit dojem, že situace, v níž se nachází, je jiná, než ve skutečnosti je. Zjednodušeněji by se dalo říci, že se jedná o „umění klamu", přičemž Mitnick rozlišuje dvě specializace v povolání umělce-manipulátora. *„Ten kdo mámí z lidí peníze je obyčejný podvodník, zatímco ten kdo využívá manipulace a přesvědčování vůči firmám – obvykle se záměrem získání informací – je sociotechnik."* [383]

Jsem přesvědčen, že toto tvrzení Mitnicka z roku 2003 by v současném digitálním světě neobstálo, neboť řada útočníků využívá techniky sociálního inženýrství pro to, aby získala právě informace či data a dále je využila například v rámci služby crime-as-a-service. Dále jsou tyto techniky využívány nejen vůči firmám, ale i vůči jednotlivcům. Vlastní útok primárně nemusí mít podobu podvodu, ale následně mohou být tyto informace prodány či zneužity k závažnějšímu útoku.

Hlavní myšlenkou sociálního inženýrství je nevyužívat různé ryze technické přístupy či nástroje například k prolomení hesla, když mnohem jednodušší je uvést oběť v omyl, ve kterém sama dobrovolně toto heslo prozradí. Nejslabším článkem bezpečnostního systému je a vždy bude člověk (uživatel). Jelikož na světě nemůže existovat počítačový systém, který by alespoň v nějaké fázi nebyl závislý na člověku (ať již jde o zprovoznění, nastavení, či údržbu počítačového systému), je nejjednodušší cestou získat potřebné informace právě od člověka.

Právě jednoduchost útoku zacíleného na nejslabší článek celého systému z něj zpravidla činí tu nejúčinnější formu. Sociální inženýrství se do popředí dostalo s kauzou Mitnicka,[384] který je mnohými považován za hackera, avšak sám se spíše považuje za sociotechnika. Mitnick ve svých

383: MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6. s. 6
384: Blíže viz např. *Kevin Mitnick Case: 1999.* [online]. [cit. 2. 11. 2011]. Dostupné z: http://www.encyclopedia.com/doc/1G2-3498200381.html

knihách[385] ukazuje, jak jednoduše lze získat informace, které jsou citlivé a představují bezpečnostní riziko pro jedince i organizace. V rámci slyšení před U.S. Senate Committee on Governmental Affairs,[386] kde Mitnick vypovídal, jak získával hesla a citlivé informace k počítačovým systémům firem, do kterých pronikl, mimo jiné Mitnick uvedl: *„Představil jsem se jako někdo jiný a prostě jsem o ně požádal."*

Pro sociální inženýrství je jedním z klíčových faktorů zisk co největšího množství informací o cíli útoku (ať již počítačovém systému, právnické či fyzické osobě). Mnohdy dochází k dlouhodobému působení na klíčovou osobu a budování „důvěry" mezi útočníkem a obětí před vlastním útokem, přičemž útočník typicky využívá lidské neopatrnosti, důvěřivosti, ochoty pomoci jiným, lenosti, slabosti, strachu (např. aby se osoba nedostala do problémů), neodpovědnosti, hlouposti aj.

Výše uvedené lidské vlastnosti značně napomáhají útočníkovi realizovat jeho útok. Sami si položte otázku, jak moc si ověřujete protistranu například při telefonátu či komunikaci skrze ICT? Jak moc si prověřujete paměťová média (USB disky, paměťové karty aj.), které jste získali darem na prezentační akci?

Zejména v oblasti ICT je možné sledovat stále sofistikovanější a propracovanější útoky [např. kvalitně připravené podvodné e-maily, reálné instituce (použité jako domnělý odesílatel), přesměrování na podvodné stránky či instalace malware obsaženého v příloze dokumentu nebo na paměťovém médiu aj.[387]]. Sociální inženýrství bylo i jedním z nezbytných prostředků, bez nichž bychom nemohli provést například útoky popsané v kap. 3.4 Projekty testující zranitelnosti uživatelů sociálních sítí.

Útoky sociálního inženýrství jsou zpravidla vedeny třemi způsoby, přičemž tyto způsoby jsou navzájem kombinovány:

1) **Sběr volně** (veřejně) **dostupných dat** o cíli útoku

2) **Fyzický útok** (útočník se například vydává za pracovníka servisní agentury – např. servis tiskáren, pracovník údržby aj.), při kterém se útočník snaží získat co nejvíce informací

385: Blíže viz:
MITNICK, Kevin D. a William L., SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.
MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, c2006. ISBN 0-471-78266-1.
MITNICK, Kevin D. a William L., SIMON. *Ghost in the wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.
386: *The testimony of an ex-hacker.* [online]. [cit. 26. 9. 2008]. Dostupné z: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html
387: Blíže viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing.

„zevnitř" společnosti, případně citlivé informace o jednotlivých pracovnících (včetně např. prohledávání odpadků aj.)

3) **Psychologický útok**

Mezi nejčastější metody útoků sociálního inženýrství lze zařadit:

1) **Podvodný e-mail či falešná webová stránka**[388]

2) **Telefonický hovor**

3) **Útok „tváří v tvář"**

4) **Prohledávání odpadků** („Dumpster diving" a také „cezení dat")

5) **Prohledávání webu, sociálních sítí aj.** (jedná se o jednoduše dosažitelný otevřený zdroj dat pro útočníky sociálního inženýrství, který pomáhá zjistit, případně ověřit informace o potenciálním cíli). **Veřejné informace dostupné online** (např. životopisy, práce, teze, návrhy aj. uveřejněné na Internetu). **Výroční zprávy a jiné veřejně dostupné informace o společnosti**

6) **Doručení reklamních či jiných materiálů na CD, DVD či jiném paměťovém nosiči**

7) **Ponechání paměťového média** (USB aj.) **v zájmové oblasti** (např. firmě, u domu zaměstnance aj. toto médium pak typicky obsahuje malware)[389]

8) **Nabídka vyzkoušení služby online** (např. nabídka cloudového úložiště, či některé zajímavé služby zdarma aj.)

9) **Dodávka či nalezení zařízení** (počítačového systému)

10) **Falešný servisní technik**

11) **Jiné**

388: Blíže viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing. V současnosti jde o nejčastější metodu sociálního inženýrství i z důvodu její malé finanční nákladnosti a možnosti distribuce široké veřejnosti.
389: Dalším případem je rozdávání těchto a jiných zařízení v rámci „promo" akcí, reklamy aj.

Pokud jde o cíl útoků sociálního inženýrství v rámci organizace, pak se možnými cíli mohou stát například:

- řídící pozice,
- IT oddělení,
- pracovníci help desků,
- recepční (sekretariáty),
- bezpečnostní pracovníci,
- správa budov,
- úklid aj.

Sociotechnik je schopen díky svým schopnostem manipulovat s lidmi, nicméně prostá manipulace není v některých případech dostačující a je třeba propojit tyto informace s technickými znalostmi v oblasti ICT.

Na závěr této kapitoly uvádím příklad, na němž Mitnick demonstruje právě propojení sociálních technik se znalostmi ICT:[390]

Mladý hacker, kterému budu říkat Ivan Peters, si dal za cíl získat zdrojový kód nové hry. Bez potíží se dostal do firemní sítě WAN, protože jeho hackerský kolega se už dříve dokázal nabourat na jeden z jejich webových serverů. Po odhalení jisté slabiny v softwaru div že nespadl ze židle. Ukázalo se, že systém používal tzv. *dual homing*, což znamená, že měl odtud přístup i do vnitřní sítě.

Avšak po připojení stál Ivan před podobným problémem, před jakým stojí turista v Louvre, který chce najít portrét Mony Lisy. Bez průvodce by se tam mohl motat celé týdny. Byla to globální korporace se stovkami kanceláří a tisíci serverů, která ve své síti nezveřejňovala indexy vývojářských systémů nebo jiné průvodcovské služby po svých datech. Místo toho, aby k nalezení serveru, na který se potřeboval dostat, použil technologické metody, využil metodu sociotechnickou. Uskutečnil několik telefonátů na základě postupů v této knize už popsaných. Nejprve zatelefonoval na technickou pomoc oddělení informatiky, představil se jako zaměstnanec firmy a řekl, že by rád probral jistý problém spojený s rozhraním produktu, na kterém pracovala jeho skupina. Požádal o telefonní číslo na šéfa projektů ve skupině programátorů, kteří se zabývali hrami. Potom zavolal na toto číslo a předstíral, že je pracovníkem oddělení Informatiky. *„Ještě dnes večer,"* řekl, *„budeme měnit router a chceme se ujistit, že lidé z vaší skupiny neztratí spojení se serverem. Který server používáte?"* Síť byla neustále vylepšována a sdělení jména serveru nemůže ničemu vadit, že? Vždyť je přece chráněn heslem a samotná znalost jména nikomu nic nepřinese. A tak šéf projektů uvedl jméno serveru. Ani se nepokusil o zpětné zavolání a ověření této historky nebo alespoň o zapsání jména a telefonního čísla volajícího. Prostě sdělil jména serverů: ATM5 a ATM6.

390: Příklad doslova citován z: MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6, s. 127–130

Nyní se Ivan vrátil k technologickým metodám, aby získal autentikační informace. Ve většině případů je prvním krokem identifikace účtu se snadným heslem, které dovolí získat v systému první opěrný bod. Pokud se útočník pokouší za pomoci hackerských nástrojů vzdáleně identifikovat hesla, vyžaduje to být po dlouhé hodiny připojen k firemní síti.

Objevuje se tu nebezpečí: čím déle bude připojen k síti, tím větší je riziko jeho odhalení a dopadení. Nejprve použil Ivan enumeraci, která umožňuje odhalit podrobnost o systému. Jako obvykle je možné vhodné nástroje nalézt na Internetu, (http://mtslenth.0catch.com). Ivan našel na webu několik volně dostupných hackerských nástrojů, které mu dovolily proces zautomatizovat a vyhnout se tak ruční práci, která by prodlužovala čas operace, a tím by zvětšovala i riziko dopadení. Věděl, že firma většinou používá servery na platformě Windows a stáhl si program NTBEnum - enumerační nástroj[391] NetBIOS (basic input/output system). Zadal IP adresu serveru ATM5 a spustil program. Nástroj dokázal identifikovat několik existujících kont na serveru.

Po identifikaci existujících kont stejný program umožnil spuštění slovníkového útoku. Slovníkový útok je dobře známý lidem zabývajícím se bezpečností počítačových systémů a samozřejmě i hackerům. Ostatní lidi fakt, že je něco takového vůbec možné, šokuje. Tento útok má za cíl zjištění hesel uživatelů pomocí obecně užívaných slov. Všichni jsme v některých věcech líní, ale nikdy mne nepřestane udivovat, že při výběru hesla má lidská kreativita a představivost prázdniny. Většina z nás chce mít heslo, které nás ochrání, ale zároveň je lehké si ho pamatovat. Obvykle to znamená použití nějakého nám blízkého slova. Mohou to být například naše iniciály, druhé jméno, přezdívka, jméno manžela, název oblíbené písničky, filmu či značky piva. Dále pak jméno ulice či města, kde bydlíme, značka auta, kterým jezdíme, oblíbené prázdninové místo nebo jméno potoka, kde nejlépe berou pstruzi. Vidíme to pravidlo? Většinou jsou to jména nebo výrazy, které lze najít ve slovníku. Slovníkový útok zkouší postupně výrazy ze slovníku jako heslo jednoho či více uživatelů.

Ivan provedl slovníkový útok ve třech fázích. V první fázi seznam 800 nejčastěji používaných hesel. Seznam obsahuje taková jako *secret, work* nebo *password* (tedy *tajné, práce, heslo*). Kromě toho program tvořil permutace těchto výrazů s doplněnými číslicemi nebo s číslem aktuálního měsíce. Program zkoušel každé heslo na všech nalezených účtech v systému. Bez výsledku. Ve druhé fázi si otevřel stránku vyhledávače Google a zadal výraz *„wordlists dictionaries"* a našel tisíce stran obsahující seznamy slov a anglické i jiné slovníky. Stáhl si celý elektronický anglický slovník. Doplnil ho o několik seznamů výrazů, které našel vyhledávač. Ivan si vybral adresu www.outpost9.com/files/Wordlists.html. Z této stránky se mu podařilo stáhnout (úplně zadarmo) sadu souborů obsahující příjmení, neobvyklá jména, jména a výrazy spojené s politikou, jména herců a slova a jména pocházející z Bible. Jiná stránka se seznamy výrazů je dostupná na univerzitě v Oxfordu na adrese ftp://ftp.ox.ac.uk/pub/wordlists. Na jiných adresách můžeme

391: **Enumerace** - proces odhalující služby dostupné na daném serveru, jeho operační systém a názvy uživatelských kont, které mají přístup do systému.

najít seznamy se jmény postav z animovaných filmů, citáty ze Shakespeara, z Odyssey, z Tolkiena i Hvězdných válek a také slova spojená s vědou, náboženstvím atd. (Jedna internetová firma prodává seznam obsahující 4,4 milionu slov a jmen za pouhých 20 dolarů.) Atakující program může být zkonfigurován i tak, aby tvořil na základě výrazů ze slovníku anagramy - to je další oblíbená metoda uživatelů, která má zvětšit jejich bezpečnost.

Když si Ivan vybral seznam, který použije a spustil program, přepnul ho do automatického režimu a mohl se tak věnovat něčemu jinému. Člověk by si myslel, že takový útok dá útočníkovi čas na delší šlofíček a dokonce, že až se vzbudí, bude pokrok nevelký. Ve skutečnosti může být - v závislosti na druhu napadeného systému, konfiguraci bezpečnostních systémů a rychlosti připojení - plná slovní zásoba z anglického slovníku otestována za 30 minut! Během útoku zapnul Ivan druhý počítač a rozběhl podobný útok na druhý server, který používala skupina programátorů, ATM6. O dvacet minut později se podařilo něco, co se většině lidí zdá nemožné: prolomit heslo a odhalit, že jeden z uživatelů si zvolil heslo „Frodo", jméno jednoho z hobitů, hrdiny Pána prstenů. S heslem v ruce se Ivan mohl připojit k serveru ATM6. Čekala tam na něho dobrá a špatná zpráva. Dobrá, že konto, na které se naboural, mělo administrátorská práva. A špatná, že tam nikde nemohl najít zdrojový kód hry. Zřejmě byl na druhém serveru, ATM5, který se slovníkovému útoku ubránil. Ivan však neházel flintu do žita - stále ještě měl v zásobě pár triků. V některých operačních systémech Windows a UNIX jsou zašifrovaná hesla přístupná každému, kdo má přístup na počítač, kde jsou umístěná. Důvodem je fakt, že zakódovaná hesla nelze dekódovat zpět a tedy není důvod je chránit. Tato teorie je mylná. Pomocí dalšího nástroje dostupného na síti, pwdump3, si stáhl zakódovaná hesla ze serveru ATM6. Typický soubor se zakódovanými hesly vypadá takto:

```
Administrator: 500:95E4321A38AD8D6AB75E0C8D76954A50:2E48927AQB04F3BFB341E266D6L
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D
digger:1111:5D15COD58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256555
ellgan:1112:2017DA45D8O1383EFF17365FAF1FFE89:07AEC950C22CBB9C2C734EB89j1
tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D20820335
vkantar;1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1CD6
vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432
mmcdonald: 1121:A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5FD192
```

Když měl soubor u sebe na počítači, použil Ivan další nástroj, který prováděl tzv. *útok hrubou silou*.[392] Ten zkouší všechny kombinace alfanumerických a většiny speciálních znaků.

Ivan použil nástroj *L0phtcrack3* (čti loft-crack; je dostupný na adrese www.atstake.com; jiný zdroj vynikajících nástrojů na hádání hesel je www.elcomsoft.com). Správci používají L0phtcrack3 na

392: **Útok hrubou silou** - strategie odhalování hesel, která spočívá v testování všech možných kombinací alfanumerických i speciálních znaků.

vyhledávání *„slabých"* hesel a hackeři na jejich proražení. L0phtcrack3 umožňuje zkoušet hesla s kombinacemi písmen, číslic a většiny symbolů včetně @#$%^&. Systematicky testuje všechny možné kombinace většiny znaků. (Pokud jsou však v hesle použity neviditelné znaky, L0phtcrack3 nebude schopný heslo odhalit.) Tento program pracuje s neuvěřitelnou rychlostí, která může na počítači s frekvencí procesoru 1 GHz dosáhnout hodnoty 2,8 milionu pokusu za sekundu. Dokonce i při této rychlosti může, pokud správce dobře zkonfiguroval systém Windows (tj. vypnul používání hašování LANMAN), prolomení hesla zabrat hodně času. Z tohoto důvodu si útočník často stahuje soubory s hesly na svůj počítač a spouští útok u sebe, aby neriskoval odhalení během dlouho udržovaného spojení. Ivan nemusel čekat dlouho.

O několik hodin později našel program hesla všech členů skupiny programátorů. Byla to však hesla uživatelů na ATM6, kde nebyl zdrojový kód. Co teď? Stále nebyl schopen získat hesla umožňující přístup k serveru ATM5. Jako hacker si uvědomoval zlozvyky většiny uživatelů a došel k závěru, že si někdo z členů týmu mohl vybrat stejné heslo na obou serverech. A bylo to tak. Jeden z programátorů měl heslo *gamers* jak na ATM5, tak i na ATM6. Před Ivanem se otevřely dveře k hledání zdrojového kódu.

Když ho našel a stáhl si celý strom, učinil ještě jednu pro hackera typickou věc. Změnil heslo na spícím kontě s administrátorskými právy, čistě pro případ, že by se sem chtěl později vrátit a stáhnout si novou verzi programu.

K redukci rizik sociálního inženýrství je nezbytné zvyšovat povědomí o možných hrozbách nejen v rámci organizace, ale v rámci celé společnosti. Jak jsem již uvedl dříve, sociální inženýrství pomáhá uskutečnit útok, přičemž je zcela na útočníkovi, aby určil, kdo bude jeho cílem. Pro útočníka je mnohem snazší zaměřit svůj útok na masy nezkušených a neznalých lidí, než na relativně dobře chráněnou společnost.

V této souvislosti je vhodné připomenout dva výroky, které mohou komukoli pomoci v rámci obrany nejen před sociálním inženýrstvím:

***„Důvěřuj, ale prověřuj."***
Ronald Regan

a

***„Přežije jen paranoik."***
Andrew S. Growe

## 4.2 Botnet

Botnet lze jednoduše definovat jako síť softwarově propojených botů[393], které provádí činnost na základě příkazu „vlastníka" (resp. správce) této sítě. Takto postavená síť může být použita k legální činnosti (např. distribuované výpočty), nebo k činnosti nelegální (viz dále).

Právě distribuované výpočty, de facto nechtěně, vnukly zločincům myšlenku na vybudování botnetů tak, jak je vnímáme v současnosti. Z upoutávky na distribuované výpočty uvádím: *„**většina počítačů na světě využívá svůj plný výpočetní potenciál jen velice malou část své provozní doby**, ale jejich spotřeba elektřiny je jen o málo nižší než kdyby byly vytíženy naplno. **Je obrovská škoda tohoto lenošení počítače nevyužít, a málokdo si uvědomuje, kolik takového nevyužitého výkonu na světě vlastně je…** V distribuovaných výpočtech platí do písmene pořekadlo **„Nemusí pršet, stačí když kape" a zde kape z milionů obyčejných počítačů na světě takový výkon, který převyšuje několikanásobně výkon i těch největších superpočítačů světa…** Zapojení do jakéhokoliv projektu distribuovaného výpočtu spočívá pouze v instalaci klienta a ten už většinou dokáže provádět veškeré potřebné činnosti a starat se o konkrétní aplikace…Většina projektů funguje tak, že celková práce je rozdělena na spoustu dílků a ty jsou následně rozesílány na jednotlivé počítače, které si o ně řeknou. Po zpracování každého dílku jednotlivé počítače samy odešlou výsledná data zpět do centra projektu a tam dojde ke spojení výsledků opět do jednoho celku."*[394]

Vlastní idea distribuce zdrojů, respektive využití malého výpočetního výkonu jiných počítačových systémů například pro počítání složitých matematických algoritmů aj. rozhodně není špatná a je mnohem efektivnější, než využívání a budování „superpočítačů". Nicméně jako lidé jsme značně vynalézaví, a tak bylo nasnadě, že tato myšlenka bude využita i k jiným než nezištným či prospěšným účelům. Možnost distribuce různých úloh mezi různě geograficky umístěné počítače byla a je pro útočníky lákavá.

Současný počítačový systém např. v podobě mailserveru nemá problém odeslat desítky milionů či miliardy e-mailových zpráv denně. Pokud se uživatel rozhodne tento systém využívat například k šíření Spamu[395], bude tento počítačový systém (dohledatelný podle identifikátorů jako je IP adresa) tuto činnost vykonávat pouze po velmi krátkou dobu, neboť bude velmi brzy zablokován ISP (např. z důvodu nelegitimního či nadměrného provozu v síti, který je možné označit za Spam), jeho adresa se objeví na „blacklistech" a na základě této informace bude blokován provoz (např. odchozí pošta). Pokud však útočník využije distribuovaný výkon v podobě sítě botnet, bude

393: **Bot** (zkrácenina ze slova robot). Jedná se o program, který umí plnit příkazy útočníka, zadávané z jiného počítačového systému. Nejčastěji se jedná o infikaci počítače virem typu worm, trojský kůň aj. Počítačový systém, který je takto na dálku ovládán, je pak označován jako **zombie**. Některé zdroje však i infikovaný počítačový systém označují jako bot.
Bot může vykonávat sběr dat, zpracovávat požadavky, rozesílat zprávy, komunikovat s řídícím prvkem aj.

394: Blíže viz *Distribuované výpočty.* [online]. [cit. 2. 11. 2013]. Dostupné z: http://dc.czechnationalteam.cz/

395: Viz kap. 4.5 Spam.

mít k dispozici tisíce až stovky tisíc počítačů, z nichž každý odešle část zpráv (např. 1000-2000 zpráv denně). Takovýto provoz pak nebude považován za problematický a nebude zastaven.

Pro **botnet** je typické, že **pokud se podaří infikovat cílový počítačový systém, připojí se tento systém**, který je nazýván „zombie" či „bot" (zotročený počítačový systém) **k centrálnímu řídícímu serveru** [označovanému jako command-and-control server (C&C)]. **Kontrolu nad celým tímto systémem** (obsahujícím zombie a C&C) **má útočník** (označován jako botmaster či botherder), **jenž řídí boty prostřednictvím C&C serveru**.[396]

Pro botnet jsou charakteristické (nezbytné) následující prvky:

1) **Command-and-control infrastructure (C&C)**
   Jedná se o infrastrukturu, která se skládá z řídícího prvku (či prvků) a botů (ovládaných počítačových systémů).

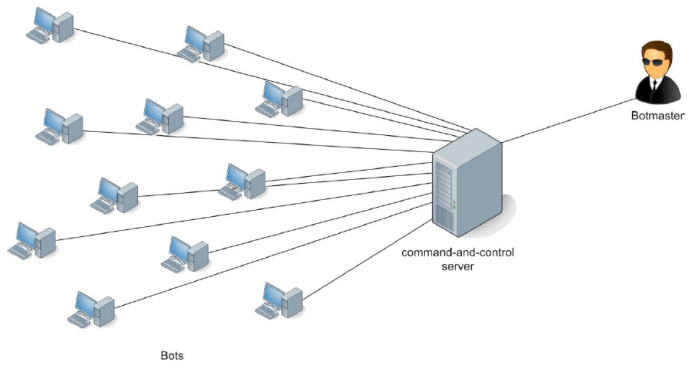
2) **Instalace a ovládání botu**
   Nejčastěji se jedná o malware, který je prostřednictvím sítě botnet či jiným způsobem šířen. Primárním cílem takovéhoto malware je zapojit další počítačové systémy do botnetu. Malware využívá různé zranitelnosti počítačových systémů.

3) **Řízení** (ovládání) **botů skrze C&C infrastrukturu**
   Bot je software, který funguje skrytě a ke komunikaci s C&C serverem používá běžné komunikační kanály (IRC, IM, RFC 1459 aj.). Noví boti se snaží získat co nejvíce informací ze svého okolí a propagovat se do dalších počítačových systémů.

Na základě architektury se standardně rozlišují botnety s:

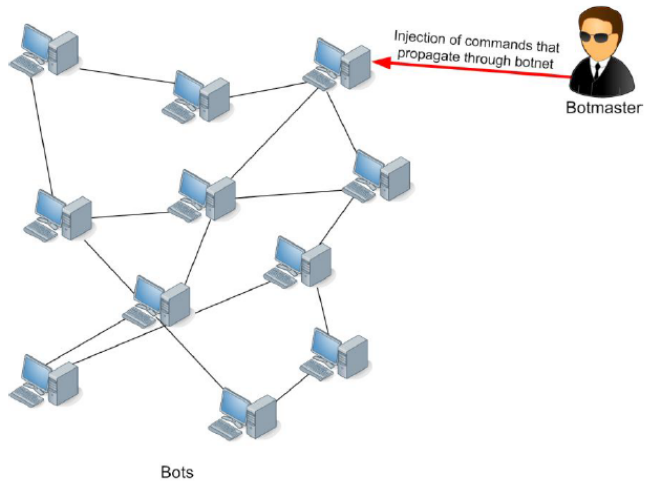
1) **Centralizovanou architekturou**
   Tato architektura je typicky postavena na principu komunikace klient-server. Koncové počítačové systémy (zombie/boti) komunikují přímo s C&C serverem (centrálním řídícím prvkem) a plní instrukce a využívají zdroje z tohoto serveru.

396: Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA, 2011. [online]. [cit. 17. 5. 2015], s. 14. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence
Další definice botnetu a informace o nich je možné nalézt např. na:
*Co je to botnet a jak se šíří?* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.youtube.com/watch?v=ywXqDon5Xtg
*Botnety: nová internetová hrozba*. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.lupa.cz/clanky/botnety-internetova-hrozba/
*Války síťových robotů– jak fungují sítě botnets*. [online]. [cit. 15. 7. 2016]. Dostupné z: http://tmp.testnet-8.net/docs/h9_botnet.pdf
*Botnets*. [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6




397

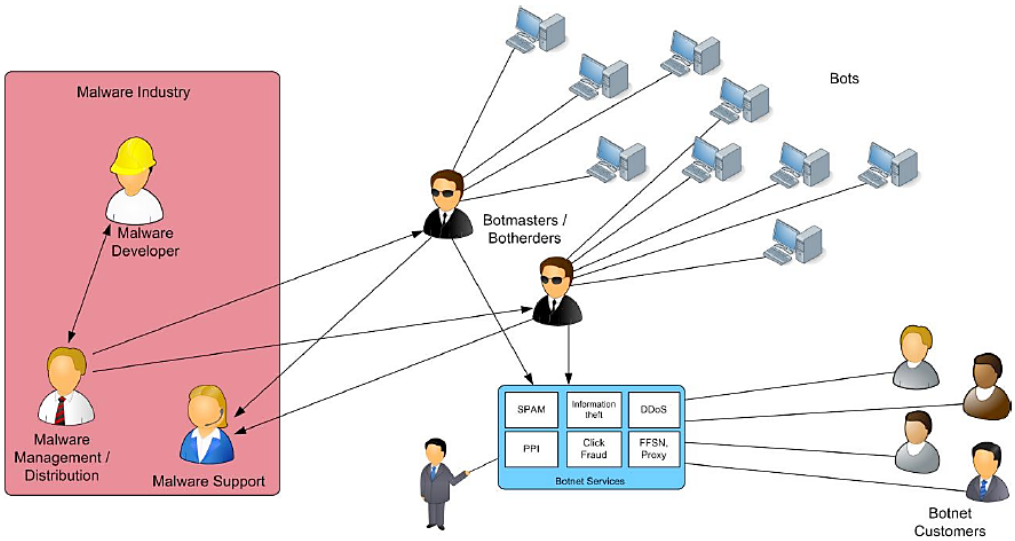
2) **Decentralizovanou architekturou**
Typicky je vybudovaná na Peer-to-peer (P2P) architektuře. Tato architektura umožňuje sdílení zdrojů a příkazů v rámci P2P sítě. Chybí zde centrální řídící prvek v „klasické" podobě, díky čemuž je tento systém odolnější proti snaze o převzetí kontroly prostřednictvím tohoto řídícího prvku.




398

397: Obrázek centralizovaného botnetu. Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit. 17. 5. 2015], s. 16. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence
398: Obrázek decentralizovaného botnetu. Tamtéž s. 18

Botnety je možné využít k řadě činností, avšak v popředí je především finanční zisk, který spočívá jednak v generování vlastních útoků (např. ransomware[399], phishing,[400] rozesílání spamu,[401] krádežím informací, DDoS[402] aj.), tak v pronájmu svých služeb či celého botnetu klientům. Díky výše popsanému je možné botnet zařadit do struktury **crime-as-a-service** (kde je nabízena služba: **botnet-as-a-service**), či do malware economy[403], kde představuje základní technickou platformu, nezbytnou pro provedení celé řady kybernetických útoků.




Obrázek 34: Malware economy

Počítačový systém, který se stane součástí botnetu, je pak typicky využit pro některou z činností popsaných v následující tabulce. Je třeba uvést, že uvedené útoky jsou zpravidla vzájemně kombinovány či distribuovány v rámci botnetu s ohledem na jeho vytíženost, poptávku „zákazníků" atp.

399: Blíže viz kap. 4.4 Ransomware.

400: Blíže viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing.

401: Blíže viz kap. 4.5 Spam.

402: Blíže viz kap. 4.12 DoS, DDoS, DRDoS útoky.

403: Malware economy. Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit. 17. 5. 2015], s. 21. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

| Odesílání | Identity Theft | DoS útoky | Click Fraud |
|---|---|---|---|
| - spamu<br>- phishingu<br>- malware<br>- adware<br>- spyware | Dochází k získávání a odesílání (zpět útočníkovi) osobních a citlivých dat a informací.<br>- Přístupové údaje k účtům<br>- Přístupové údaje k e-mailům, sociálním sítím aj.<br>- jiná data či informace, které mohou být útočníkem využity, či prodány | Spouštění DoS útoku vůči cíli (počítačovému systému) určenému botmasterem. | Počítačový systém zobrazuje (případě kliká) na reklamní odkazy na stránkách bez vědomí uživatele. Vytváří se tak dojem, že stránky mají návštěvnost a inzerenti přicházejí o peníze.* |

* *Bots and Botnets – A growing Threat.* [online]. [cit. 11. 8. 2016]. Dostupné z: https://us.norton.com/botnet/

V níže uvedené tabulce shrnuji seznam některých známých botnetů:[404]

| Datum vytvoření | Datum ukončení | Jméno | Předpokládaný počet botů | Počet spamu v miliardách za den | Alias (známý též jako) | Další informace |
|---|---|---|---|---|---|---|
| **2002** | | | | | | |
| | 2011 | Coreflood | 2 300 000 | | | Backdoor. Sběr osobních a citlivých informací. |
| **2004** | | | | | | |
| | | Bagle | 230 000 [16] | 5,7 | Beagle, Mitglieder, Lodeight | Masivní rozesílání spamu. Určený pro počítačové systémy s OS Windows. |
| | | Marina Botnet | 6 215 000 [16] | 92 | Damon Briant, BOB.dc, Cotmonger, Hacktool. Spammer, Kraken | |

404: Tabulka vznikla na základě spojení informací z následujících zdrojů:
*Botnet*. [online]. [cit. 15. 7. 2016]. Dostupné z: https://en.wikipedia.org/wiki/Botnet
*Botnet – Historical List of Botnets*. [online]. [cit. 15. 8. 2016]. Dostupné z:
http://www.liquisearch.com/botnet/historical_list_of_botnets
*Botnet*. [cit. 8. 7. 2016]. Dostupné z: http://research.omicsgroup.org/index.php/Botnet
*Historical list of botnets*. [online]. [cit. 15. 8. 2016]. Dostupné z: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Torpig | 180 000 [17] | | Sinowal, Anserin | Rozesílání malware a sběr citlivých a osobních dat. Určený pro počítačové systémy s OS Windows. |
| | | Storm | 160 000 [18] | 3 | Nuwar, Peacomm, Zhelatin | Rozesílání spamu. Určený pro počítačové systémy s OS Windows. |
| **2006** | | | | | | |
| | Březen 2011 | Rustock | 150 000 [19] | 30 | RKRustok, Costrat | Rozesílání spamu. Schopnost odeslání až 25 000 spamových zpráv/hodinu z jednoho počítač. Aktivní na OS Windows. |
| | | Donbot | 125 000 [20] | 0,8 | Buzus, Bachsoy | Rozesílání především farmaceutického spamu. |
| **2007** | | | | | | |
| | | Cutwail | 1 500 000 [21] | 74 | Pandex, Mutant (related to: Wigon, Pushdo) | Rozesílání spamu. Standardně používí Trojského koně Pushdo, aby infikoval počítačový systém. Aktivní na OS Windows. |
| | | Akbot | 1 300 000 [22] | | | Backdoor, umožňující převzetí kontroly nad nakaženým počítačem. Po instalaci sbíral data, zastavoval procesy, či spouštěl DDoS útoky. |
| Březen 2007 | Listopad 2008 | Srizbi | 450 000 [23] | 60 | Cbeplay, Exchanger | Primárně rozesílání spamu. K nakažení počítačových systémů byl využíván Srizbi trojan. |
| | | Lethic | 260 000 [16] | 2 | none | Rozesílání především farmaceutického spamu. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Září 2007 | | dBot | 10 000+ (Europe) | | dentaoBot, d-net, SDBOT | |
| | | Xarvester | 10 000 [16] | 0,15 | Rlsloup, Pixoliz | Rozesílání spamu. |
| **2008** | | | | | | |
| | | Sality | 1 000 000 [24] | | Sector, Kuku | Skupina malware. Počítačové systémy nakažené Sality komunikují skrze P2P. Činnost spočívá v: rozesílání spamu, sběr citlivých dat, napadání webových serverů, provádění distribuovaných výpočtů (např. pro prolamování hesel – password cracking aj.). Aktivní na OS Windows. |
| Duben 2008 | | Kraken | 495 000 [33] | 9 | Kracken | Rozesílání malware. Zapojení dalších počítačů do botnetu. |
| | Prosinec 2009 | Mariposa | 12 000 000 [25] | | | Botnet primárně zapojený do útoků typu scam a DDoS. Jednalo se o jeden z největších botnetů vůbec. |
| Listopad 2008 | | Conficker | 10 500 000+ [26] | 10 | DownUp, DownAndUp, DownAdUp, Kido | Worm útočící na počítačové systémy s OS Windows. Chyby tohoto OS byly využity k dalšímu rozšiřování botnetu. |
| Listopad 2008 | Březen 2010 | Waledac | 80 000 [27] | 1,5 | Waled, Waledpak | Rozesílání spamu a šíření malware. Ukončen akcí společnosti Microsoft. |
| | | Maazben | 50 000 [16] | 0,5 | None | Rozesílání spamu, malware, scamu, phishingu. |
| | | OnewordSub | 40 000 [28] | 1,8 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Gheg | 30 000 [16] | 0,24 | Tofsee, Mondera | |
| | | Nucrypt | 20 000 [28] | 5 | Loosky, Locksky | |
| | | Wopla | 20 000 [28] | 0,6 | Pokier, Slogger, Cryptic | |
| | | Asprox | 15 000 [29] | | Danmec, Hydraflux | Phishingové útoky, SQL injections, šíření malware. |
| | | Spamthru | 12 000 [28] | 0,35 | Spam-D-ComServ, Covesmer, Xmiler | Používání P2P |
| | 19.7.2012 | Grum | 560 000 [31] | 39,9 | Tedroo | Rozesílání především farmaceutického spamu. |
| | | Gumblar | | | | |
| **2009** | | | | | | |
| Květen 2009 | Listopad 2010 | BredoLab | 30 000 000 [30] | 3,6 | Oficla | Rozesílání spamu. Ukončen společnou akcí nizozemské policie, Govcert NL, Europolu, Kasperky Lab aj. Zřejmě největší známý botnet. |
| | Listopad 2009 | Mega-D | 509 000 [32] | 10 | Ozdok | Rozesílání spamu. |
| Srpen 2009 | | Festi | 250 000 [34] | 2,25 | Spamnost | Rozesílání spamu a provádění DDoS útoků. |
| **2010** | | | | | | |
| Leden 2010 | | LowSec | 11 000+ [16] | 0,5 | LowSecurity, FreeMoney, Ring0.Tools | |
| | | TDL4 | 4 500 000 [35] | | TDSS, Alureon | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Zeus | 3 600 000 (US only) [36] | | Zbot, PRG, Wsnpoem, Gorhax, Kneber | Zaměřen na aktivity spojené s krádežemi informací k bankovním účtům. Instaloval i Cryptolocker Ransomware aj. Aktivní na OS Windows. |
| | (Several: 2011, 2012) | Kelihos | 300 000+ | 4 | Hlux | Převážně zapojený do krádeží Bitcoinů a rozesílání spamu. |
| **2011** | | | | | | |
| | 2015-02 | Ramnit | 3 000 000 [37] | | | Worm útočící na počítačové systémy s OS Windows. Ukončen společnou akcí Europolu a Symantec. |
| | | Zero Access | 2 000 000 | | Max++ Sirefef | Botnet využitý převážně k těžení bitcoinů a click fraudu. Aktivní na OS Windows. |
| **2012** | | | | | | |
| | | Chameleon | 120 000 | | None | Click Fraud |
| | | Nitol | | | | Botnet zapojený do šíření malware a DDoS útoků. Většina zombie (až 85 %) se nachází v Číně. Botnet klient byl nalezen v počítačových systémech dodaných přímo z výroby. |
| **2013** | | | | | | |
| | | Boatnet | 500+ server computers | 0,01 | YOLOBotnet | |
| | | Zer0n3t | 200+ server computers | 4 | FiberOptck, OptckFiber, Fib3rl0g1c | |
| **2014** | | | | | | |
| | | Semalt | 300 000+ | | Soundfrost | Rozesílání spamu. |

Aktivity současných botnetů je možné nalézt např. na stránkách:
https://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-botnet-map/index.html;
https://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetMaps aj.

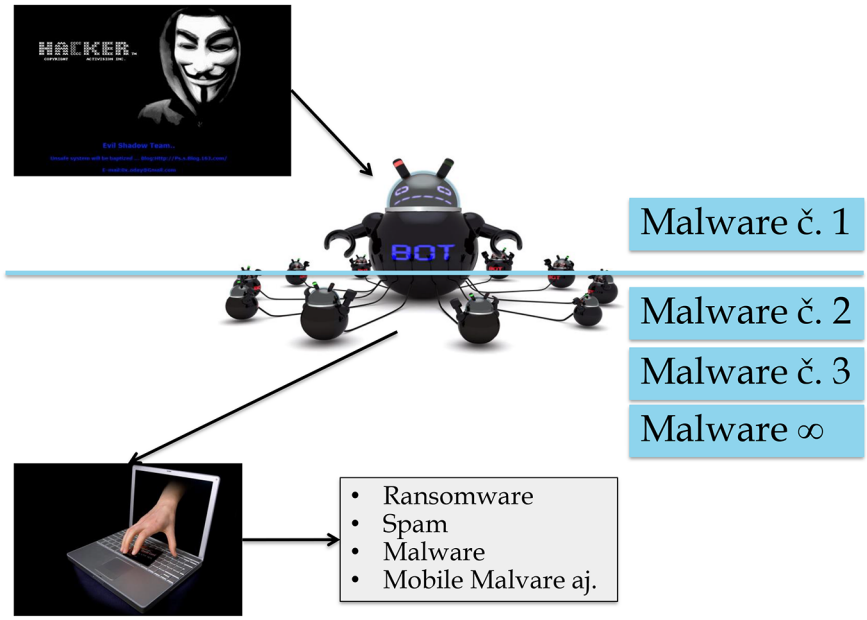
Do sítě botnet je de facto možné zapojit jakýkoli počítačový systém. Mimo jiné se jedná i o systémy, které splňují podmínky IoT (Internet of Things). V roce 2014 byl zaznamenán případ, kdy součástí botnetu byla lednice, jež rozeslala více než 750 000 e-mailů, které měly povahu spamu.[405]

Ze studie Nigama vyplývá[406], že existují desítky botnetů přímo vytvářených a primárně zaměřených na počítačové systémy, které můžeme označit jako mobilní zařízení (např. smartphone, tablet aj.). Díky instalaci aplikací z neznámých zdrojů a značné absenci antivirových produktů na mobilních zařízeních uživatelů je také mnohem snadnější nainstalovat malware do těchto mobilních zařízení, a tím nad nimi získat kontrolu. Tato zařízení jsou v současnosti svým výkonem schopna zcela splnit požadavky botmastera na chod botnetu, respektive na úkoly kladené na „zombie".

Nejen v případě botnetů slouží malware jako prostředek k získání přístupu, ovládání a dalšímu šíření malware či jiným úkolům na základě pokynů útočníka, nicméně pokud je v současnosti na uživatelův počítačový systém infikován malware, existuje vysoká pravděpodobnost, že se zároveň stal součástí botnetu. Útočník (botmaster) do počítačového systému (zombie) nainstaluje malware, který mu umožňuje manipulaci s počítačovým systémem na dálku (Malware č. 1 – přičemž tento malware ponechává kontrolu botmasterovi i v případě například pronájmu části nebo celého botnetu.). Teprve poté dochází k instalaci dalšího škodlivého software (Malware 2. až Malware ∞), který má plnit jiné úkoly (např. rozesílání spamu, sběr dat, vydírání pomocí Ransomware aj.). Celou tuto strukturu je možné znázornit následovně:

405: *Fridge caught sending spam emails in botnet attack.* [online]. [cit. 17. 5. 2016]. Dostupné z: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

406: Blíže viz NIGAM, Ruchna. *A timeline of Mobile Botnets.* [online]. [cit. 12. 7. 2016]. Dostupné z: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf




Obrázek 35: Malware instalovaný do počítačového systému zapojeného do sítě botnet

Z pohledu práva je možné konstatovat, že botnety představují celé sítě infikovaných počítačových systémů, nad kterými do určité míry neoprávněně převzala kontrolu třetí osoba, a to bez vědomí oprávněných uživatelů. Takto infikované systémy slouží nejčastěji jako základna pro anonymní připojování útočníka k Internetu, k zasílání škodlivých programů, uskutečňování útoků na další cíle, realizaci DoS útoků, šíření spamu, krádežím identit či jiným kybernetickým útokům.

Pokud jde o vlastní činnost útočníka, která spočívá v instalaci malware pro následné ovládnutí počítačového systému, je možné toto jednání posoudit dle § 230 TZK (Neoprávněný přístup k počítačovému systému a nosiči informací). Pokud by útočník malware vložil do počítačového systému v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, mohlo by být jeho jednání kvalifikováno dle § 230 odst. 2 písm. d) TZK.

Ve vztahu k ovládnutí a využívání počítačového systému je třeba uvést, že jakékoli využívání takovýchto počítačových systémů bez souhlasu oprávněné osoby je nezákonnou intervencí do **čl. 11 Listiny**,[407] bez ohledu na to, v jaké podobě je uvedené využívání realizováno.

407: „***Každý má právo vlastnit majetek***. *Vlastnické právo všech vlastníků má stejný zákonný obsah a ochranu.*“

Lze tvrdit, že se jedná i o neoprávněné užívání cizí věci (neboť předmětný počítačový systém je v těchto případech věcí cizí) dle **§ 207 odst. 1 al. 1** TZK. Užití § 207 odst. 1 al. 2 TZK[408] může být značně problematické, neboť je rozhodující intenzita zásahu a užívání počítačového systému. Na základě této míry intenzity by bylo případně možné vyčíslit vzniklou škodu, jakožto vyjádření amortizace v čase užívání. Bohužel za použití tohoto výpočtu zpravidla nedojde ke způsobení škody nikoli malé.

Vlastní ochrana před zapojováním a využíváním počítačů v rámci sítě botnet může mít dvě roviny. V první rovině jde o zvýšení ochrany majetkových práv tím, že dojde k doplnění § 207 TZK o základní skutkovou podstatu, jejíž znění by mohlo být následovné: ***„Kdo bez souhlasu oprávněné osoby užije počítačový systém."***

Tímto ustanovením by byla vymezena i okolnost, která spočívá v zásahu do majetkového práva jiného. V případě neoprávněného užívání cizí věci ve vztahu k počítačovému systému není řešením snížení škody z nikoli malé na nikoli nepatrnou (viz § 207 odst. 1 al. 1 TZK), neboť cena řady počítačových systémů je v současnosti nižší i než hodnota nikoli nepatrná (tedy nejméně 5 000 Kč), a přesto jsou tyto počítačové systémy schopny zcela plnit zadanou činnost v rámci sítě botnet.

Druhá rovina, která vystihuje závažnost jednání útočníka, pak spočívá ve včlenění nové kvalifikační okolnosti do § 230 odst. 3 TZK, přičemž tato okolnost by mohla znít následovně:

***„úmyslně připojí počítačový systém do počítačové sítě s úmyslem spáchat trestný čin, či jej v této síti se stejným úmyslem užije."***

## 4.3 Malware

Za **malware** (složenina anglických slov malicious software – škodlivý software), je možné označit jakýkoli software využitý k narušení standardní činnosti počítačového systému, zisku informací (dat), či využitý k získání přístupu k počítačovému systému. Malware může mít celou řadu podob, přičemž mnohé druhy malware jsou pojmenovány podle toho, jakou činnost provádějí.

Jeden malware je schopen plnit několik funkcí (vykonávat několik činností) naráz. Může se například sám dále šířit prostřednictvím e-mailů (v rámci přílohy) nebo jako data v P2P sítích a zároveň může získávat například e-mailové adresy z napadeného počítačového systému.

Z historického hlediska existovala nejdříve řada různých termínů pro software, který je v současnosti označován souborným pojmem malware. Vlastní názvy konkrétního škodlivého software

408: Toto ustanovení počítá se způsobením škody na cizím majetku, přičemž škoda musí být nikoli malá (tj. minimálně 25 000 Kč viz § 138 odst. 1 TZK).

vznikaly zpravidla podle činnosti, kterou daný program vykonával. I přes právě uvedené konstatování, že je v současnosti využíván primárně pojem malware, je stále možné se setkat i s historicky starším označením škodlivého software. Jedná se o následující skupiny:

1) **Adware**
2) **Spyware**
3) **Viry (Viruses)**
4) **Červi (Worms)**
5) **Trojské koně (Trojan Horses)**
6) **Backdoor**
7) **Rootkity**
8) **Keylogger**
9) **Ransomware aj.**[409]

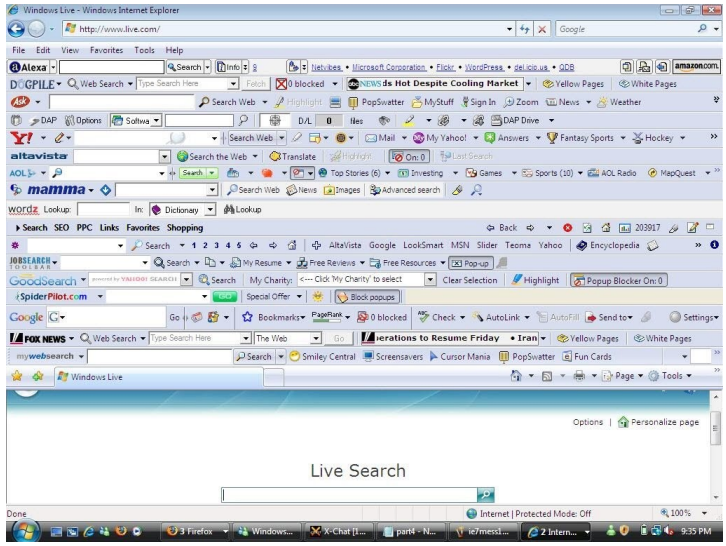
**Ad 1) Adware**
Pojem adware je zkratka z anglického slovního spojení „*advertising supported software*", což lze do českého jazyka volně přeložit jako software podporující reklamu. Jedná se o nejméně nebezpečnou, avšak výnosnou formu malware.[410] Adware zobrazuje reklamy na počítačovém systému uživatele (např. pop-up okna v operačním systému[411] nebo na webových stránkách, reklamy zobrazované společně se software aj.). Byť jde ve většině případů o produkty, které pouze obtěžují uživatele neustálými reklamními sděleními, která „vyskakují" na obrazovce, může být adware spojen i se spyware, jehož účelem je sledovat činnost uživatele a odcizit důležité informace.

409: Nejedná se o kompletní výčet různých typů malware. Spíše jde o vymezení základních typů malware včetně vysvětlení jejich fungování.

410: Existují společnosti specializující se na „placení za instalaci" (*PPI, pay per install*). „*PPI se pak projevuje záplavou aktivit vedoucích k instalaci add-onů či dalšího nechtěného softwaru, který (v tom nejméně škodlivém případě) bez vědomí uživatelů vyměňuje reklamy ve webových stránkách, případně je vkládá tam, kde žádné reklamy na webu nejsou.…**Celý model PPI je postaven na tom, že ti, kdo tyto služby nabízejí, neberou žádné ohledy na to, jestli uživatel něco chce instalovat. Za každou instalaci dostávají až 1,50 USD**, je tedy více než jisté, že podvodné a automatické instalace jsou zásadním prvkem jejich ‚obchodního modelu'.*"
Blíže viz DOČEKAL, Daniel. *Google: Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele.* [online]. [cit.10.8.2016]. Dostupné z: http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/

411: Obrázek těchto pop-up oken. Blíže viz *Adware.* [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking


Obrázek 36: Adware




Obrázek 37: Ukázka Adware a dalších add on nainstalovaných ve webovém prohlížeči[412]

412: [online]. [cit. 10. 8. 2016]. Dostupné z: https://i.ytimg.com/vi/GcvlB-EpMwA/maxresdefault.jpg

**Ad 2) Spyware**
Pojem spyware je složeninou anglických slov *„spy"* (špion) a *„software"*. Pomocí spyware jsou získávána statistická data[413] o provozu počítačového systému a bez vědomí a souhlasu uživatele odesílána do datové schránky útočníka.[414] Součástí těchto dat mohou být i informace osobního charakteru či informace o osobě uživatele, dále informace o navštívených webových stránkách, o spuštěných aplikacích apod.

Spyware může být jednak instalován jako samostatný malware, jakož může být často i součástí jiných, volně šířených a jinak zcela bezpečných programů. V takovém případě je instalace a další činnost spyware typicky ošetřena ve smluvních podmínkách EULA a uživatel tak zpravidla nevědomky dobrovolně souhlasí s monitorováním vlastních aktivit. Přikládání spyware programů k programům jiným (např. klientské programy P2P sítě, různé shareware programy aj.) bývá motivováno snahou výrobce programu zjistit zájmy či potřeby uživatele a tyto informace využít např. pro cílenou reklamu.[415] Charakteristickou vlastností programů typu spyware, která jsou součástí „balíčku programů", je též fakt, že většinou zůstávají nainstalovány v počítači i poté, co hlavní program byl odinstalován, což ve většině případů bývá uživateli skryto.

Spyware představuje hrozbu jednak proto, že odesílá různé informace z počítačového systému uživatele k „útočníkovi" (přičemž tyto informace jsou dále zpracovávány a dochází ke korelaci dat s daty a informacemi získanými z jiných zdrojů), a jednak pak proto, že spyware může obsahovat další nástroje, které ovlivňují vlastní činnost uživatele.[416]

**Ad 3) Viry (Viruses)**
Jedná se o program či závadný kód, který sám sebe připojí k jinému existujícímu spustitelnému souboru (např. software aj.) či dokumentu. Virus se reprodukuje v momentě, kdy dojde ke spuštění tohoto software či otevření infikovaného dokumentu. Nejčastěji se viry šíří díky sdílení software mezi jednotlivými počítačovými systémy; ke svému šíření nepotřebují součinnost uživatele. Viry byly dominantní formou malware zejména v 80. a 90. letech 20. století.[417]

Existuje velká řada virů, jejichž účelem je ničit, jiné naopak mají za úkol „usídlit" se v co největším počtu počítačových systémů a tyto pak využít k cílenému útoku. Typické pro tyto programy

413: Např. přehled navštívených webových stránek, jejich IP adresy, přehledy nainstalovaných a užívaných programů, záznamy o downloadu souborů z Internetu, údaje o struktuře a obsahu adresářů uložených na pevném disku atd.
414: Blíže srov. např. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 216 a násl.
415: [cit. 8. 1. 2008]. Dostupné z: http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9
416: Může se jednat např. o: **Browser Helper Object** (DLL knihovna, umožňující programátorům změnit a sledovat Internet Explorer); **Hijacker** (software měnící domácí stránku webového prohlížeče); **Dialery** [přesměrovává telefonní linku na drahé telefonní tarify (v současnosti hlavně útoky na mobilní telefony a VoIP ústředny)]; **Keystroke Logger/ Keylogger** (monitoring stlačených kláves); **Remote Administration** (umožní vzdálenému uživateli, ovládat počítačový systém uživatele na dálku); **Tracer** (program, sledující pohyb počítačového systému – typicky mobilního zařízení) aj.
417: Blíže viz Muzeum malware. *The Malware Museum @ Internet Archive*. [online]. [cit. 17. 5. 2016]. Dostupné z: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/

je schopnost šířit se mezi systémy bez nutnosti zásahu uživatele počítačového systému. Projevy virů mohou být různé, např. od neškodného vyhrávání melodie, přes zahlcení systému, změnu či zničení dat, až po celkovou destrukci napadeného systému. Počítačové viry je možno třídit podle mnoha různých hledisek, např. podle hostitele (tedy podle druhu programů, které počítačové viry přenášejí), podle způsobů, kterým se projevují v systému, podle umístění do paměti atd.[418] Podle toho, jaké soubory viry napadají, je možné je rozdělit na:

- boot viry (napadají pouze systémové oblasti),
- souborové viry (napadají pouze soubory),
- multiparitní viry (napadají soubory i systémové oblasti),
- makroviry (napadají aplikace pomocí maker).

**Ad 4) Červi (Worms)**
Za viry bývají označováni i tzv. **počítačoví červi** (anglicky *„worm"*). Důvodem bližší spojitosti s viry je ta skutečnost, že červi nepotřebují žádného hostitele, tedy žádný spustitelný soubor (obdobně jako viry). Tyto programy se na rozdíl od virů, které bývají připojeny jako součást jiného programu, šíří zpravidla samostatně. Napadený systém je následně červem využit k dalšímu odeslání kopií sebe sama dalším uživatelům pomocí síťové komunikace.[419] Tímto způsobem se velmi rychle rozšiřuje, což může vést až k zahlcení počítačové sítě, a tím i celé infrastruktury. Na rozdíl od virů jsou tyto programy schopny analyzovat bezpečnostní slabiny v zabezpečení napadeného informačního systému,[420] proto bývají taktéž využívány k vyhledávání bezpečnostních mezer v systémech nebo v poštovních programech.[421]

**Ad 5, 6) Trojské koně (Trojan Horses) a Backdoors**
Za **trojské koně** jsou obecně označovány ty počítačové programy, které obsahují skryté funkce, s jejichž užitím uživatel nesouhlasí nebo o nich neví, a které jsou potenciálně nebezpečné pro další fungování systému. Stejně jako v případě virů mohou být tyto programy připojeny k jinému, bezpečnému programu či aplikaci nebo mohou samy vypadat jako neškodný počítačový program. Trojské koně, na rozdíl od klasických virů, nejsou schopny se replikovat a ani se šířit bez „pomoci" uživatele. V případě, že je trojský kůň aktivován, může být využit například k mazání, blokování, modifikaci, kopírování dat či například narušování běhu počítačového systému, či počítačových sítí.

Některé trojské koně po své aktivaci bez vědomí uživatele otevírají komunikační porty počítače,

418: Blíže např. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 216 a násl.
419: Blíže např. LI, Tao, GUAN, Zhihong, WU, Xianyong. Modeling and Analyzing the Spread of Active Worms Based on P2P Systems. *Computers & Security*, 2007, roč. 26, č. 3, s. 213–218.
420: Blíže srov. RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007–2017. *Security magazín*, 2007, roč. 14, č. 1, s. 4.
421: Srov. JIROVSKÝ, Václav a Oldřich KRULÍK. Základní definice vztahující se k tématu. *Security magazín*, 2007, roč. 14, č. 2, s. 47.

čímž výrazným způsobem zjednodušují další napadání takto zasaženého systému jinými škodlivými programy, popřípadě usnadňují přímé ovládnutí napadeného počítače tzv. na dálku. Takové trojské koně jsou označovány jako backdoor (z anglického *„backdoor"* - zadní vrátka).[422] Moderní backdoor programy mají zdokonalenou komunikaci a využívají většinou protokolů některých nástrojů komunikace, jako je např. program ICQ.[423]

S užitím trojských koní bývá často též spojeno užití různých **skenovacích** (či scanovacích)[424] **programů** (angl. *„port scannery"*), což jsou programy, které slouží zejména ke zjištění, které komunikační síťové porty počítače jsou otevřené, jaké služby jsou na nich spuštěné a zda je přes ně možno realizovat útok na takový systém.[425] Tato data jsou opět zasílána útočníkovi a jsou dále potenciálně využitelná při páchání dalších kybernetických útoků.

**Ad 7) Rootkity**
Tímto pojmem jsou označovány nejen počítačové programy, ale i celá technologie sloužící k zamaskování přítomnosti malware (např. počítačových virů či trojských koní, červů aj.) v napadeném systému. Nejčastěji mají formu nepříliš objemných počítačových programů. Rootkity nejsou škodlivé samy o osobě, ale jsou využívány právě tvůrci škodlivých programů, jako jsou např. viry, spyware atd.[426] Program typu rootkit mění chování celého operačního systému, jeho částí nebo nadstavbových aplikací tak, aby se uživatel o existenci nebezpečných programů ve svém počítačovém systému nedozvěděl. Obecně lze programy typu rootkit rozdělovat na **systémové** (modifikující jádro systému) a **aplikační** (modifikují konfiguraci aplikací).[427]

Z aplikací napadají rootkity zejména specializované programy na vyhledávání a odstraňovaní nebezpečných programů ze systému, tedy antiviry apod.[428] Antivirové programy při použití rootkit programu nemohou tento škodlivý program z napadeného systému odstranit. Tímto způsobem je přítomnost škodlivého programu v napadeném systému prodlužována. Z tohoto hlediska je

422: Přehled nejrozšířenějších trojských koní spolu s výpisem jejich funkcí a komunikačních portů je možno získat na různých webových stránkách dostupných na Internetu. Blíže srov. např. http://www.test.bezpecnosti.cz/full.php

423: Srov. JIROVSKÝ, Václav. K*ybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 63.

424: Tyto programy jsou označovány někdy též jako skanovací, skanerovací, skenerové či skenovací programy.

425: Blíže srov. např. JIROVSKÝ, Václav. Kyb*ernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 64.

426: Blíže srov. např. BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, roč. 27, č. 7–8, s. 323–334.

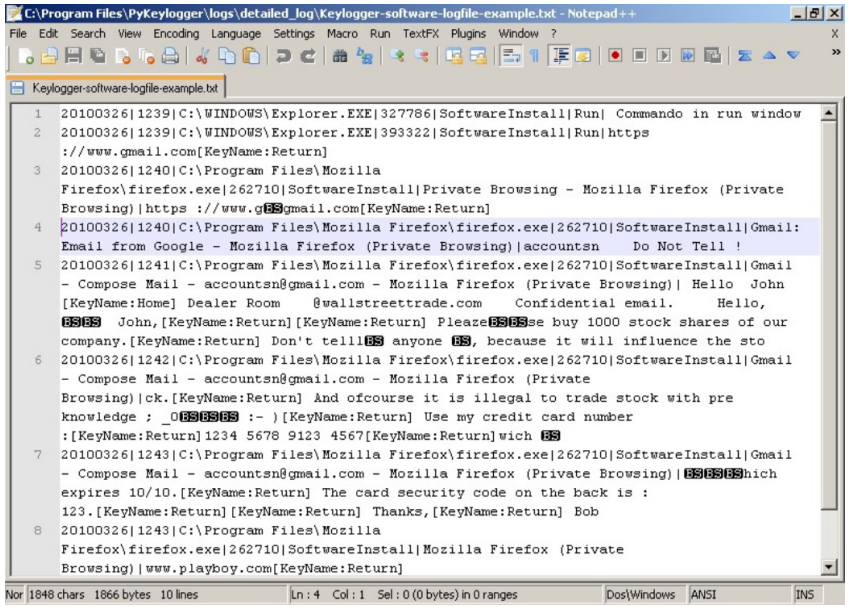
BAUDIŠ, Pavel. Programy typu rootkit. Další hrozba pro Windows. *CHIP*, 2005, č. 7, s. 14

427: Srov. RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007–2017. *Security magazín*, 2007, roč. 14, č. 1, s. 5.

428: Např. trojský kůň DNS-Changer napadá nejprve bezpečnostní programy, kde sám sebe odstraní ze seznamu škodlivých programů, čímž znemožní svoje objevení. Blíže. PLETZER, Valentin. Demaskovaný spyware. *CHIP*, 2007, č. 10, s. 116–120.

možno konstatovat, že programy typu rootkit mohou být velmi snadno zneužitelné při páchání trestné činnosti spojené s užitím či zneužitím informačních technologií.[429] Některá literatura označuje tyto nástroje jako podskupinu backdoor trojských koní.[430]

**Ad 8) Keylogger (Keystroke Logger)**
Keylogger je software zaznamenávající konkrétní stisky kláves na napadeném počítačovém systému. Nejčastěji je keylogger využíván k zaznamenání přihlašovacích údajů (uživatelského jména a hesla) k účtům, k nimž je z počítačového systému přistupováno. Získané informace pak jsou typicky zaslány útočníkovi.




Obrázek 38: Ukázka činnosti keyloggeru[431]

**Ad 9) Ransomware**
Ransomware bude detailněji popsán v 4.4 Ransomware.

429: Blíže k této problematice např. PŘIBYL, Tomáš. Seznamte se s rootkity. *PC World*, 2007, č. 9, s. 108–110.
430: JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 65
431: Zachytávání klávesových stisků a informací o spuštěných souborech. [online]. [cit. 10. 8. 2016]. Dostupné z: http://img.zerosecurity.org/files/2013/10/Keylogger-software-logfile-example.jpg

**Distribuce malware**
Existuje celá řada způsobů, jimiž je možné malware doručit k cílovému počítačovému systému. Na tomto místě stručně uvedu některé metody šíření malware. Malware je možné distribuovat skrze:

- **Přenosná paměťová média**
  Například pomocí CD, DVD, USB, externí disk aj. Jedná se o nejstarší, avšak stále účinný způsob distribuce malware, kdy si uživatelé navzájem předávají infikované soubory **či počítačové sítě** obsahující **infikované soubory** (sdílení takovýchto souborů v rámci počítačových sítí, typicky P2P sítí).

- **Drive-by-download**
  Jedním z nejčastějších způsobů infekce malware je jeho stažení z Internetu a následné spuštění souboru, typicky s příponou .exe (executable file – spustitelný program) z neznámého zdroje. Může se jednat o falešné či padělané programy (např. napodobeniny Flappy Bird, falešné media kodeky aj.), programy sloužící k obcházení ochrany autorských práv (cracky, keygeny aj.[432]), reálné infikované programy aj.


Obrázek 39: Zobrazení jednoho z možných principů drive by download.[433]

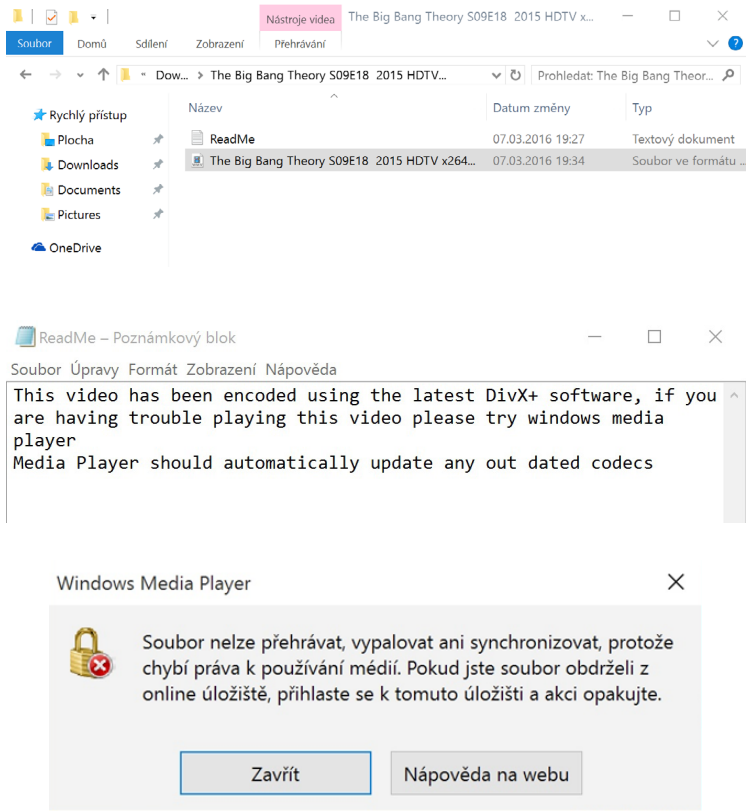
Následující příklad ukazuje malware stažený uživatelem skrze P2P síť (konkrétně se jednalo o soubor s dílem seriálu *The Big Bang Theory – sezona 9, díl 18*). Tento malware vyzval uživatele ke

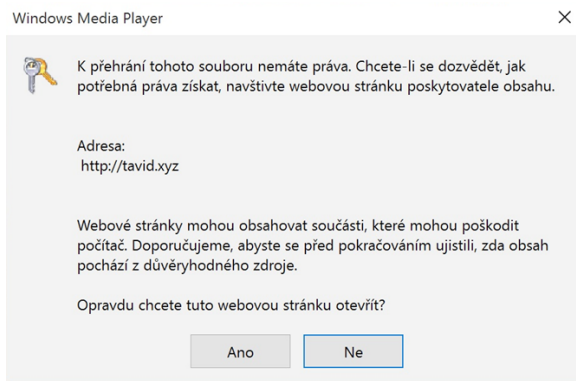
432: Viz kap. 4.9 Cracking.

433: [online]. [cit. 10. 7. 2016]. Dostupné z:
https://image.slidesharecdn.com/delljointevent2014november-onur-141105074412-conversion-gate02/95/end-to-end-security-with-palo-alto-networks-onur-kasap-engineer-palo-alto-networks-23-638.jpg?cb=1415174438

stažení nového kodeku přes Media player, aby mohlo být video přehráno. Media player se začal připojovat na stránky útočníka a následně došlo k fiktivní instalaci kodeku, avšak ve skutečnosti byl do počítače nainstalován malware (v tomto případě se jednalo o kombinaci malware: backdoor, keylogger, bot), který umožnil útočníkovi zcela ovládnout počítačový systém uživatele.

V tomto případě byla zarážející i ta skutečnost, že nabízený díl *The Big Bang Theory* ještě nebyl odvysílán v USA, kde má premiéru, přesto měl počet stažení v řádech desítek tisíc.







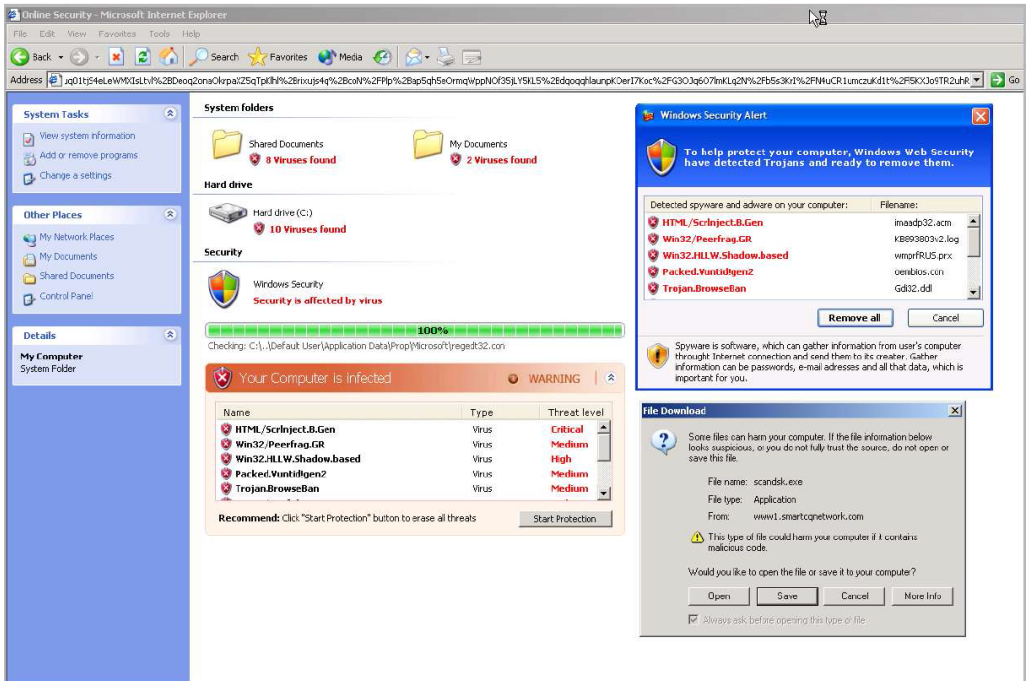
- **„Kancelářské dokumenty“**
  Velmi často dochází k šíření malware v těle souborů například typu: .doc/.docx, .xls/.xlsx, .avi aj. Tímto způsobem je možné distribuovat pouze makroviry. Uživatel předpokládá, že otevírá wordový dokument, avšak zároveň spouští executable file, který se jako tento dokument maskuje. Příklad tohoto malware bude uveden v kap. 4.6.1.1.

- **E-mail**
  Malware může být uložen v příloze zprávy, nebo se může jednat o skripty uvnitř HTML[434] těla e-mailů. V současnosti se jedná o jeden z nejběžnějších způsobů distribuce malware. Jako příklad je možné uvést současné phishingové kampaně, hoax, spam aj. Příklad tohoto malware bude uveden v kap. 4.6.1.1.

434: Hyper Text Markup Language – jde o název značkovacího jazyka používaného pro tvorbu webových stránek.

- **HTML**
  Malware může být umístěn přímo na webových stránkách, nebo v jednotlivých skriptech.

- **Falešný antivirus**
  Uživateli je typicky nabídnut antivirus zdarma – jako adware. Tento antivirus provede „otestování počítače“ a objeví závažné zranitelnosti a malware, jež uživatelův antivirus nedetekoval. Falešný antivirus kombinuje útok sociálním inženýrstvím (vzbuzení obavy před škodlivým software) s instalací malware obsaženým právě ve falešném antiviru.




Obrázek 40: Falešný antivirus

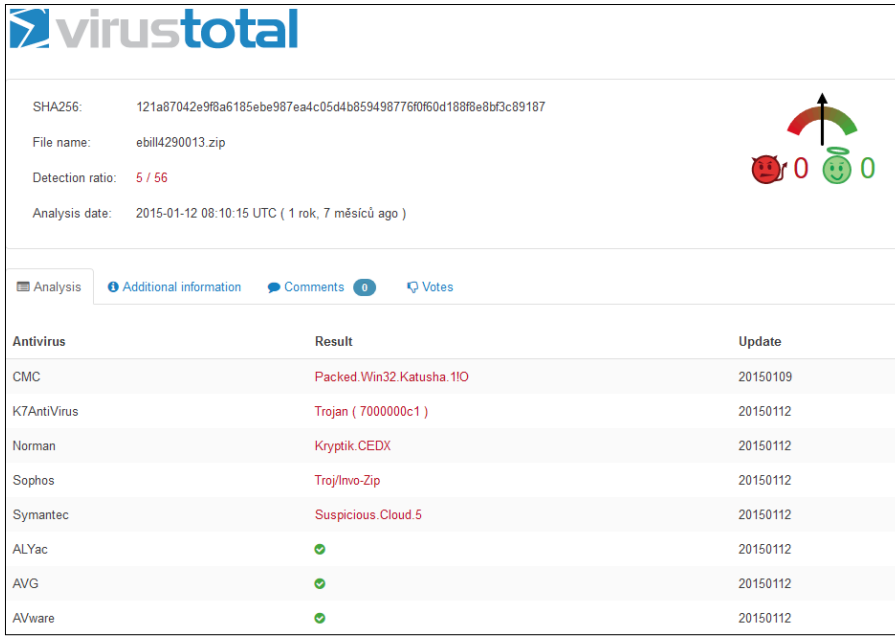

Obrázek 41: Falešný antivirus[435]

Pokud si uživatel není jistý, zda soubor či webová stránka obsahuje malware, může využít celou řadu nástrojů, které mu pomohou ověřit si přítomnost škodlivého software.

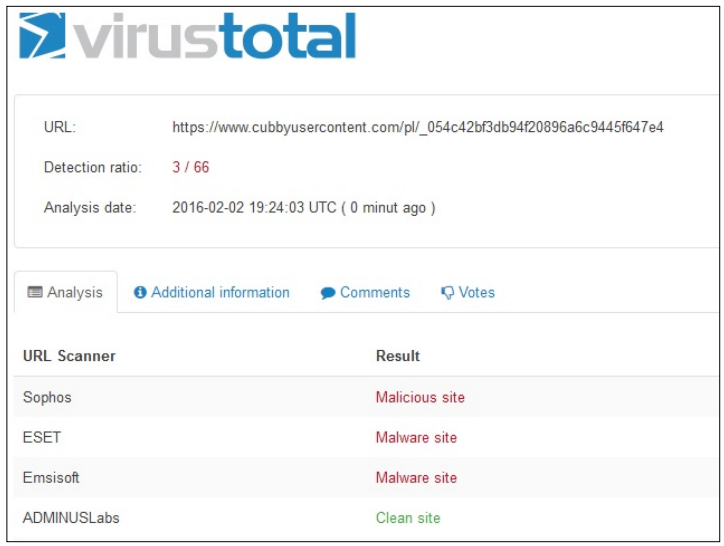
Jednou z osvědčených služeb je služba https://www.virustotal.com. Na této stránce může uživatel zadat oskenování souboru až do velikosti 128 MB či si může nechat prověřit webovou stánku, na kterou hodlá vstoupit (Vhodné je tento sken provádět např. při návštěvě stránek s internetovým bankovnictvím či stránek, na nichž je prováděna platba. Pro ověření je třeba překopírovat **celé URL navštívené stránky**.). Služba Virustotal propojuje společnosti zabývající se kybernertickou bezpečností, vývojem antivirových prostředků atp., přičemž uživatelův požadavek je prověřen nástroji všech těchto společností, čímž se zvyšuje pravděpodobnost odhalení škodlivého software.

435: Dvě verze falešného antiviru. [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.cctslo.com/images/fake-personal-antivirus.jpg

Následující printscreen zobrazuje výsledek prověření nově doručeného souboru v rámci phishingové kampaně. Den po začátku této kampaně identifikovalo malware v přiloženém souboru pouze 5 společností, do týdne jej byly schopny identifikovat i všechny ostatní společnosti. Nicméně právě doba mezi doručením aktualizací do antivirů uživatelů na jejich počítačových systémech a začátkem útoku je pro případný úspěch útočníka rozhodující.




Obrázek 42: Výsledek testování souboru




Obrázek 43: Výsledek testování webové stránky

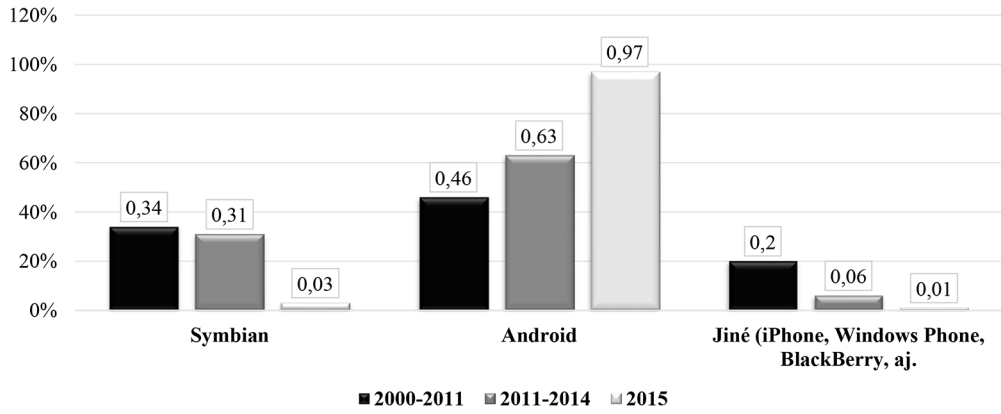
**Malware je možné nainstalovat téměř do jakéhokoli počítačového systému.** Jako příklady specifických instalací mohou sloužit případy instalace **micromalware**. Jedná se o škodlivý kód, který je rozšiřován na poměrně malém počtu počítačových systémů. Tento kód vykazuje abnormální chování a bezpečnostní programy na něj často nedokážou reagovat. Nejznámějším případem micromalware je **červ STUXNET**,[436] či instalace botnet klienta do již zmíněné lednice.

Samostatnou kapitolu pak představuje malware určený pro mobilní zařízení (**mobile malware**). První malware navržený k útokům na mobilní telefony byl objeven přibližně v roce 2004. Dnes Kaspersky Lab, která o tomto objevu tehdy informovala, uvádí, že existuje více než **340 000 malwarů**.[437]

436: Blíže viz např. *Stuxnet.* [online]. [cit. 23. 7. 2016]. Dostupné z:https://cs.wikipedia.org/wiki/Stuxnet

437: Blíže viz *The very first mobile malware: how Kaspersky Lab discovered Cabir*. [online]. [cit. 29. 6. 2015]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir
Dále viz např.:
*Škodlivý kód cílí na mobily, šíří se jako lavina*. [online]. [cit. 17. 5. 2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html
*Warning! Over 900 Milion Android Phones Vulnerable to New „QuadRooter" Attack.* [online]. [cit. 10. 8. 2016]. Dostupné z: https://thehackernews.com/2016/08/hack-android-phone.html

Pokud bychom se zaměřili na nejohroženější operační systém v rámci mobilních zařízení, pak nejvíce hrozeb je cíleno na OS Android. Důvodem této skutečnosti je především rozmanitost používaných verzí operačního systému a jejich neaktuálnost. **Většina zařízení s OS Android neumožňuje aktualizovat operační systém na poslední verzi, která je zpravidla upravena tak, aby odolávala známým zranitelnostem a již má opraveny chyby z předchozích verzí tohoto operačního systému.**[438] **Přitom je odhadováno, že 77 % hrozeb útočících na OS Android by bylo možné eliminovat právě používáním nejnovější verze tohoto operačního systému.** Následující statistika[439] představuje vývoj distribuce malware na jednotlivé operační systémy mobilních zařízení:




438: Dle statistik je u OS Android následující procentuální zastoupení všech zařízení s tímto OS: Marshmallow 6.0 – 7,5 %; Lollipop 5.1 – 19,4 %; Lollipop 5.0 – 16,2 %; KitKat 4.4 – 32,5 %; Jelly Bean 4.1, 4.2, 4.3 – 20,1 %; starší verzi – 4,3 %. Blíže viz např. *Android version market share distribution among smartphone owners as of May 2016.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

439: Pro zpracování výstupů následujících statistik byly využity především zprávy a články publikované online. Blíže viz např.: *Junipers' Mobile Threats Report: Mobile malware attacks grew over 600%.* [online]. [cit. 17. 5. 2016]. Dostupné z: http://searchnetworking.techtarget.com/news/2240203163/Junipers-Mobile-Threats-Report-Mobile-malware-attacks-grew-over-600

*Mobile Threat Report. What's on the Horizon for 2016*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

KELLY, Grodon. *Report: 97% Of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this--is-the-easy-way-you-stay-safe/#62a95de97d53

UNUCHEK, Roman a Victor, CHEBYSHEV. *Mobile malware evolution 2015.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/

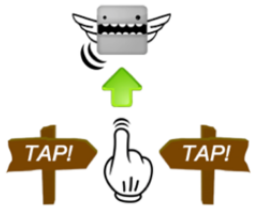
Útočníci v případě mobilních zařízení využívají především:

- **Neaktuální verze operačního systému mobilního zařízení** (známé zranitelnosti jednotlivých systémů);
- **Minimální zabezpečení mobilního zařízení** antivirovým prostředkem;
- **Neznalosti uživatelů** (Řada uživatelů bez rozmyslu instaluje aplikace „z neznámého zdroje" či aplikace požadující nadměrný přístup a oprávnění v rámci zařízení.);
- **Sociální inženýrství a „vlny zájmu" o aplikace určitého typu.**

Jedním z důvodů, proč je jako primární operační systém napadán systém Android, je i ta skutečnost, že v rámci distribučního kanálu (Google Play) není ověřována bezpečnost aplikací (respektive to, zda konkrétní aplikace například neobsahuje malware), jako tomu například je u operačního systému iOS a jejich distribučního kanálu (App Store).

Jako příklad výše uvedeného je možné uvést aplikaci **Flappy Bird** a její „klony." Tuto aplikaci vyvinul Nguyễn Hà Đông a do distribuce pro iOS byla uvedena 24. května 2013. Pro Android OS začala být tato aplikace dostupná v roce 2014 a v lednu 2014 se stala nejstahovanější hrou zdarma. Tvůrce hru z trhu odstranil 10. února 2014. Hra zaznamenala více jak 50 milionů stažení.


Již v době, kdy byla originální hra Flappy Bird na trhu, se začaly objevovat různé klony této hry pro OS Android, z nichž řada profitovala pouze na úspěchu originálu. Do řady dalších verzí však byl záměrně umístěn malware, přičemž je odhadováno, že až 79 % klonů této hry bylo infikováno škodlivým software.[440] Mezi infikované klony patří například tyto produkty:

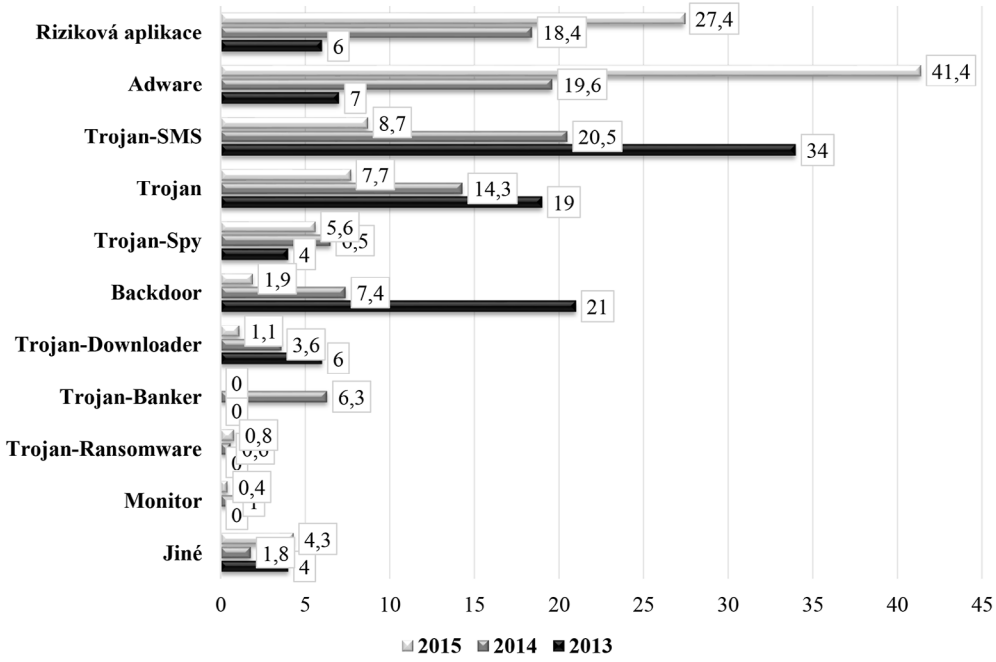





440: Blíže viz např. *Flappy Bird Clones Help Mobile Malware Rates Soar*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx

Infikování mobilního telefonu může být jedním z primárních cílů útočníka, neboť tato zařízení se dnes typicky používají v rámci dvoufaktorové autentizace internetového bankovnictví či nakupování. Útočníci se snaží získané informace použít například k odčerpání finančních prostředků přímým přístupem do bankovního účtu uživatele prostřednictvím služby internetového bankovnictví nebo získání citlivých informací.

**Mobile malware zažívá masivní nárůst.** Dle výzkumu Juniper Networks, Kaspersky Lab aj. vzrostl počet mobilního malware mezi lety 2010 a 2011 o 155 %, ještě výraznější nárůst nastal v letech 2012–2013, kdy byl zaznamenán nárůst o 614 %. Celkem bylo identifikováno 276 259 škodlivých aplikací, přičemž denně se objevilo více než 1300 nových závadných aplikací (tento výzkum do škodlivých aplikací zařadil i aplikace, které díky rozsahu svých oprávnění mohou být považovány například za spyware). Následující graf znázorňuje procentuální vyjádření podílu jednotlivých aplikací v oblasti mobile malware.




V ČR je možné postihnout útok pomocí malware dle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. **Držení malware, s úmyslem spáchat trestný čin** dle § 182 (Porušení tajemství dopravovaných zpráv) či trestný čin dle § 230 TZK, **je trestné dle § 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných

takových dat) TZK. Pokud by **účelem viru** bylo získat například utajované skutečnosti, či podpora teroristické skupiny, mohl by se útočník například dopustit trestných činů **§ 311** (Teroristický útok), **§ 316** (Vyzvědačství) nebo **§ 317** (Ohrožení utajované informace) **ve stádiu přípravy** TZK.

## 4.4 Ransomware

Do skupiny malware se řadí i tzv. vyděračský malware, pro nějž se ustálilo označení **ransomware**[441] (z anglického *„ransom"* – výkupné, někdy také označovaný jako rogueware nebo scareware). Ransomware je malware, který brání či omezuje uživatele v řádném užívání počítačového systému do doby, než dostane útočník zaplaceno „výkupné". Ransomware se nejčastěji dostane do počítače pomocí malware (trojského koně či červa), který je umístěn na webových stránkách, nebo je přílohou e-mailu.[442] Jakmile je tento malware bezpečně „usídlen" v počítačovém systému, dojde ke stažení vlastního ransomware.

Obecně je možné rozlišovat dva typy ransomware podle toho, jak moc zasahují do vlastního chodu počítačového systému. **Prvním typem je ransomware, který omezí funkčnost celého počítačového systému** a neumožní uživateli tento systém vůbec využívat (např. zabráněním spuštění operačního systému či zablokováním systémové obrazovky. Typickým příkladem tohoto typu je *„Policejní ransomware"* – viz dále). **Druhým typem pak je ransomware, jenž ponechá počítačový systém funkční, avšak dochází k uzamčení a znepřístupnění dat uživatele.**

V současnosti dochází spíše k využívání druhého typu ransomware, který je známý pod označením **crypto-ransomware**. Účelem tohoto malware je zašifrovat pevný disk nebo vybrané typy souborů v počítačovém systému, přičemž primárně má tento malware za cíl zašifrovat soukromé soubory uživatele jako jsou obrázky, textové či tabulkové dokumenty, videa aj. Po skončení šifrování se zpravidla uživateli zobrazí zpráva, že jeho soubory jsou zašifrovány, a pokud je chce získat zpět (dešifrovat), musí poslat určitý obnos na účet útočníka. K transakcím jsou obvykle využívány virtuální měny jako je Bitcoin nebo různé předplacené služby. Ve většině případů je stanovena časová lhůta pro zaplacení. Po uplynutí této lhůty dochází k smazání klíče, jenž může zašifrované soubory otevřít.

441: Např. Reventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, Jig Saw a další. Blíže viz např.: *Ransomware.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware *Postřehy z bezpečnosti: Ransomware šestkrát jinak.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/

442: Viz Malware č.1 v Obrázek 35: Malware instalovaný do počítačového systému zapojeného do sítě botnet. Dále viz kap. 4.6.1 Phishing.

### Evoluce ransomware

Ransomware, stejně jako každý jiný malware, prochází vývojem, přičemž první malware, který by bylo možné označit za ransomware, se objevil přibližně okolo roku 2005. Ve své podstatě se jednalo o **falešný antivirus (screware)**, který se za pomoci sociálního inženýrství snažil přesvědčit uživatele k zaplacení částky za vyčištění infikovaného počítačového systému. Tento ransomware zpravidla umožňoval uživateli využívat počítačový systém (nedošlo k jeho zamčení či zašifrování dat), avšak obtěžoval uživatele pop-up okny a upozorněními na neexistující viry v počítači. Tento ransomware byl velmi jednoduše odstranitelný.

Masivní nástup ransomware je možné datovat přibližně do roku 2011, kdy se celosvětově začal šířit ransomwarový útok blokující přístup k účtu uživatele OS Windows a oznamující, že počítač byl zablokován policií toho kterého státu.

Forenzní analýzu tohoto ransomware jako první v ČR provedla forenzní laboratoř (FLAB[443]) CESNET, z. s. p. o., přičemž zkoumán byl jak proces infikování uživatelova počítačového systému, tak předávání informací útočníkovi a komunikace s C&C serverem.[444]

Vlastní útok spočíval v tom, že se uživatel nakazil malware (typicky při návštěvě některých webových stránek[445] došlo k stažení „botnet-klienta"), a následně se stal součástí botnetu, přes který byl šířen vlastní **„policejní ransomware."** Tento policejní ransomware následně zablokoval přístup k účtu uživatele[446] OS Windows s tím, že uživateli oznámil, že v jeho počítači byl nalezen materiál, který porušuje právo dané země (např. porušování práv autorských, dětská pornografie aj.). Zároveň byl uživatel „policií" vyzván k zaplacení požadované sumy peněz, po níž dojde k odblokování počítače a „vyřešení celé věci." V tomto případě útočníci využili techniky sociálního inženýrství, konkrétně obavy a důvěřivosti uživatele a pomocí odkazu na oficiální autority se od něj snažili získat finanční prostředky.

443: Bližší informace na https://flab.cesnet.cz/.

444: Pro popis útoku jsem použil jednak informace obdržené v rámci spolupráce s FLAB CESNET, a dále informace z následujících článků:

PADRTA, Aleš a Karel NYKLES. *Ransomware – „policejní virus" na pitevním stole.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/

KOLOUCH, Jan a Andrea KROPÁČOVÁ. *Ransomware.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.inase.org/library/2015/zakynthos/bypaper/COMPUTERS/COMPUTERS-49.pdf

445: Velmi často se jednalo o stránky s pornografií či jiným sexuálním materiálem. Na tyto stránky mohl být uživatel i přesměrován z jiné stránky, na níž byla „návnada".

446: Aplikace byla nastavena jako „vždy navrchu" (StayOnTop). Uživatel nevidí jiné aplikace skryté pod tímto „ransom dialogem" a není schopen si vyvolat správce úloh. Vlastní Ransomware se zapsal do registrů Run a RunOnce a vždy po 500 ms prováděl kontrolu, ve stejném časovém rozsahu skrýval i správce úloh. Jedinou další běžící aplikací byla komunikace s C&C serverem (maskováno v procesu prohlížeče).

Zarážející na celém případu byla ta skutečnost, že značná část uživatelů ochotně zaplatila požadovanou částku (v ČR se tato částka průběžně pohybovala mezi 2 000–4 000 Kč), aniž by si ověřili, zda je skutečná policie oprávněna takovýmto způsobem blokovat počítače, či „vyřizovat" případné prohřešky uživatele.

Následující printscreeny zobrazují „policejní ransomware" v různých zemích a následně jsou zobrazeny verze použité v ČR.


Obrázek 44: Policejní ransomware[447]

447: *Policejní ransomware.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000


Obrázek 45: Verze policejního ransomware určená pro Velkou Británii[448]

V ČR se postupně objevovaly různé verze (rozuměj vzhled stránek) policejního ransomware. První verze byla zaznamenána na konci roku 2011, přičemž zobrazovala IP adresu připojení, ISP připojení a místo [kde byla uvedena IP adresa konkrétního poskytovatele (ISP) připojení], pokud měl uživatel zapnutou web kameru, došlo k vytvoření fotografie, která byla také zobrazena.

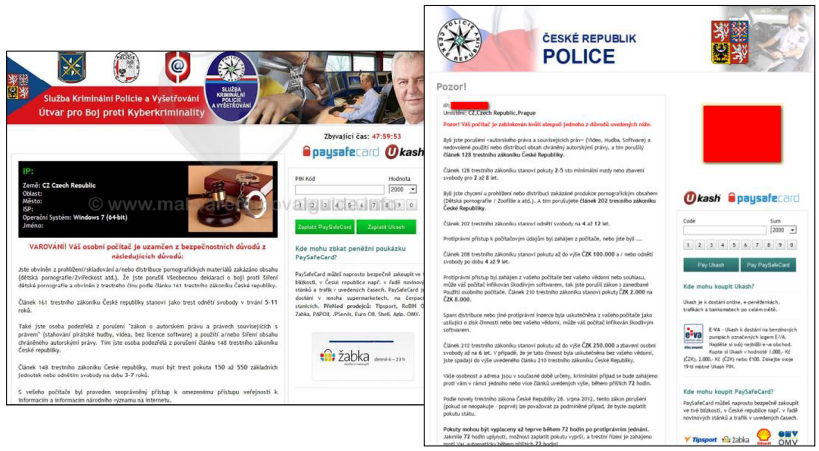
448: [online]. [cit. 14. 8. 2016]. Dostupné z: https://sophosnews.files.wordpress.com/2012/11/cool_ransom_uk_full.png


Obrázek 46: Policejní ransomware první verze v ČR

Novější verze, kromě toho, že se graficky lišily, navíc zobrazovaly verzi operačního systému a uživatelské jméno uživatele. Došlo také k vylepšení češtiny používané na zamknuté stránce.


Obrázek 47: Policejní ransomware ČR - další verze

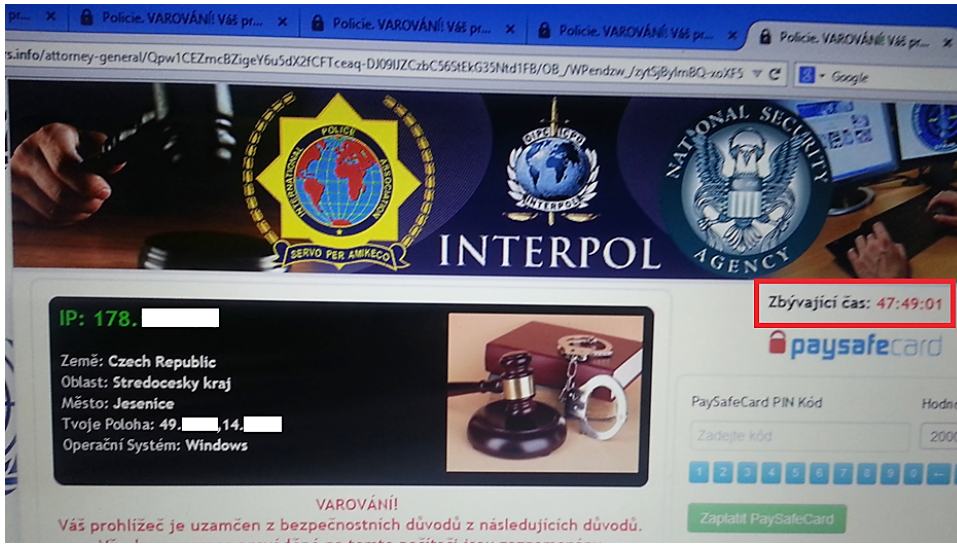
Nalézt bylo možné i verze s Milošem Zemanem, či jiné další:[449]




449: *Likvidace fotografií, dokumentů aneb nový „policejní virus" na scéně.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.viry.cz/likvidace-fotografii-dokumentu-aneb-novy-policejni-virus-na-scene/

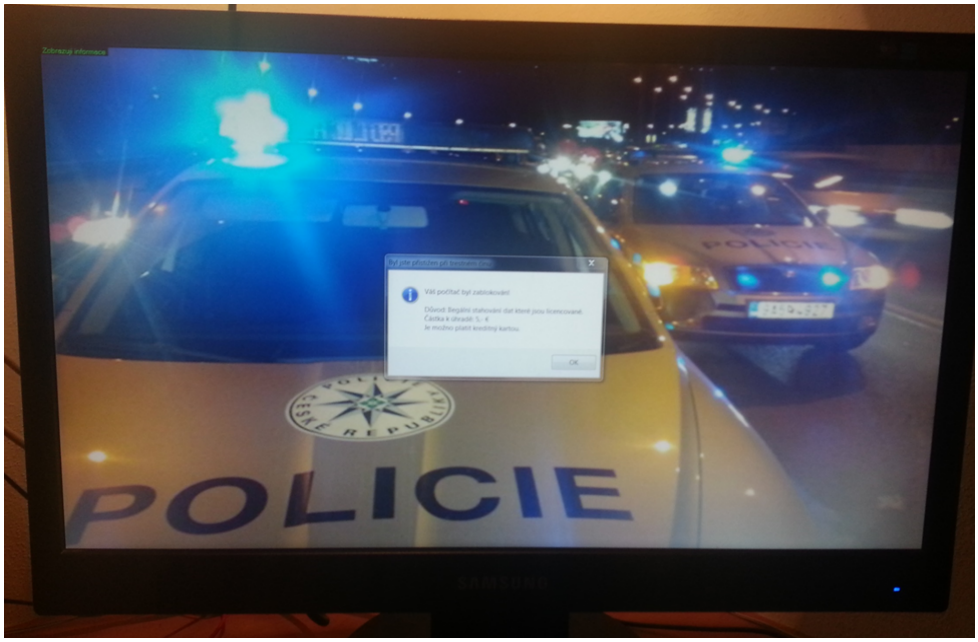
Výše popsaný „policejní ransomware“ zažil největší rozmach v letech 2011–2013, nicméně další varianty tohoto škodlivého software se s různými obměnami objevily i později. Následující printscreeny zobrazují modifikace „policejního ransomware“. Oba případy byly zjištěny v roce 2015. Na prvním printscreenu je zobrazen ransomware blokující dominantní webový prohlížeč využívaný v napadeném počítači (přičemž ostatní browsery infikovány nebyly). Uživatel mohl využívat všechny funkce počítačového systému, kromě napadeného prohlížeče.

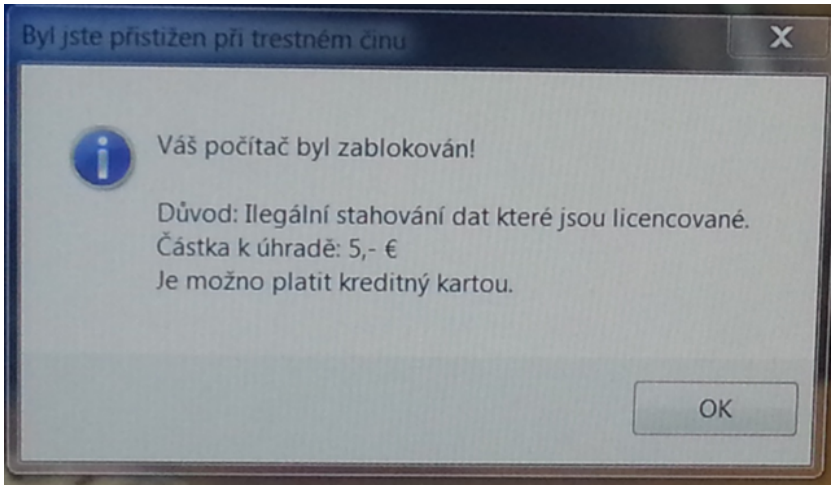
Kromě dříve uvedených informací je zobrazena GPS pozice a zbývající čas do zaplacení.




Obrázek 48: Policejní ransomware ČR (r. 2015)

Druhý printscreen zobrazuje „zamknutý“ počítač, přičemž ransomware byl skryt v cracku nelegálně stažené a nainstalované hry (v tomto případě se jednalo o hru Far Cry 4 staženou z českých torrentů).



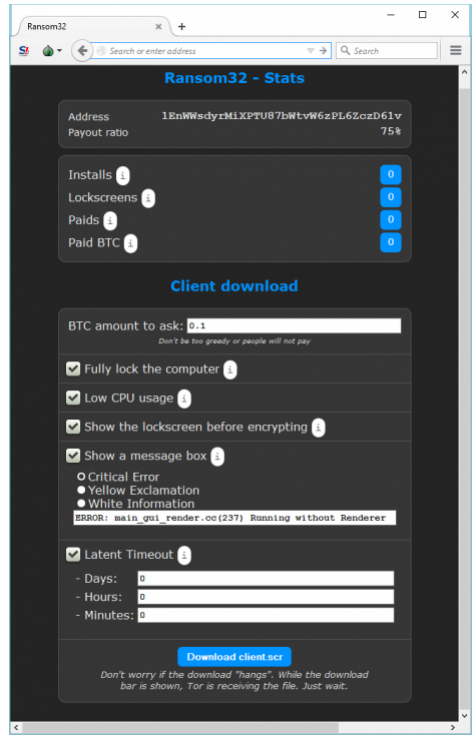




Obrázek 49: Policejní ransomware ČR (r. 2015)

**Od roku 2013 došlo v případě ransomware k významné změně. Útočníci omezili útoky, které spočívaly v omezení funkčnosti celého počítačového systému, a primárně se zaměřili na zamykání dat uživatelů.** Zamykána jsou data na místních discích, discích připojených v rámci počítačové sítě i na všech připojených periferiích (např. externí USB, HDD aj.). Data se stávají „rukojmím", přičemž prolomení šifrování je téměř nemožné. Jedním z prvních ransomware tohoto typu byl CryptoLocker (dále pak CryptoWall aj.).


Obrázek 50: Cryptolocker (r. 2013)

V rámci crime-as-a-service aktivit je nabízena od roku 2016 služba **Ransomware-as-a-service**. Uživatel (rozuměj útočník) má možnost si nadefinovat vlastní Ransomware dle svých představ. Zároveň mu je poskytnuto technické zázemí v podobě C&C serverů, bitcoinové peněženky, online 24/7 podpory aj. Příkladem Ransomware-as-a-service je software **Ransom32**.




Obrázek 51: Ransomware (klient)

Další změny je možné pozorovat i ve vlastní činnosti útočníků. Pokud dojde k instalaci ransomware, může být tento malware cílen například na šifrování uložených pozic ve hrách či může dojít k „zamknutí" televize, které využívají operační systém Android.[450]

V ČR je možné postihnout útok pomocí malware, kterým je i ransomware, dle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. **Držení malware, s úmyslem spáchat trestný čin** dle § 182 (Porušení tajemství dopravovaných zpráv) či trestný čin dle § 230 TZK, **je trestné dle § 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK.

450: Srov. např. *New Ransomware Encrypts Your Game Files*. [online]. [cit. 14. 8. 2016]. Dostupné z: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/
*Android Ransomware now targerts your Smart TV, Too!* [online]. [cit. 14. 8. 2016]. Dostupné z: https://thehackernews.com/2016/06/smart-tv-ransomware.html
*FLocker Mobile Ransomware Crosses to Smart TV.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

V případě ransomware je možné uplatnit i ustanovení **§ 230 odst. 3** TZK, kdy útočník páchá tento trestný čin s úmyslem získat sobě nebo jinému neoprávněný prospěch. V úvahu by také mohlo přicházet uplatnění § 175 (Vydírání) TZK, kdy je osoba pohrůžkou jiné těžké újmy (např. i tím, že na ni bude podáno trestní oznámení[451]) nucena k zaplacení dané částky.

## 4.5 Spam

Odpovědět na otázku, co je to spam, lze jednoduše, avšak zároveň i poněkud složitěji, přičemž složitější odpověď se bude týkat právě oblasti informačních a komunikačních technologií.


Spam je produkt společnosti Hormel Foods. Jedná se o masovou konzervu obsahující vepřové, mechanicky separované kuřecí maso, šunku, sůl, cukr, vodu, koření a dusitan sodný. V podstatě se jedná o lančmít vyráběný v USA, který se proslavil zejména během 2. světové války a po ní, kdy nahrazoval chybějící maso. Díky své trvanlivosti se mohl skladovat téměř po neomezenou dobu. Ostatně i na webu http://store.spam.com/spam-classic se dočtete: *The original. The timeless.*

Díky britské komediální skupině Monthy Python bude SPAM skutečně nadčasový a věčný. Právě skeč pojednávající o objednávání jídla (dostupný z: http://www.youtube.com/watch?v=nZ-G6lQPQKlI) zapříčinil následně tu skutečnost, že byl pojem spam použit pro označení nevyžádaného produktu, v ICT zejména pro označení nevyžádané komunikace.

Z hlediska informačních a komunikačních technologií lze obsah pojmu spam v zásadě chápat ve dvou rovinách. V **užším slova smyslu** se jedná o hromadné šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu, nejčastěji prostřednictvím elektronické komunikace.[452] V **širším slova smyslu** se jedná o všechny doručené nevyžádané zprávy, tedy i např. o zprávy obsahující viry, trojské koně apod.[453]

451: K pojmu jiná těžká újma viz ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1752-1753
Konkrétně může *„pohrůžka jiné těžké újmy může spočívat v hrozbě způsobení majetkové újmy, vážné újmy na cti či dobré pověsti aj. Jinou těžkou újmou může být i zahájení trestního stíhání v důsledku oznámení trestného činu, jímž pachatel poškozenému hrozí, a nutí ho tak něco konat, opominout nebo trpět. Je přitom nerozhodné, zda se poškozený trestné činnosti, jejímž oznámením se hrozí, dopustil či nikoli (srov. R 27/1982).“*
452: Blíže např. ŠTUDENTOVÁ, Milada. Trestněprávní aspekty související se zasíláním e-mailů a zveřejňováním materiálů na webových stránkách. *Trestní právo*, 2007, roč. 13. č 7–8, s. 27–33.
453: Ke třídění spamu srov. např. GONZÁLES-TALAVÁN, Guillermo. A Simple, Configurable SMTP Anti-spam Filter: Greylists. *Computers & Security*, 2006, roč. 25, č. 3, s. 229–236.

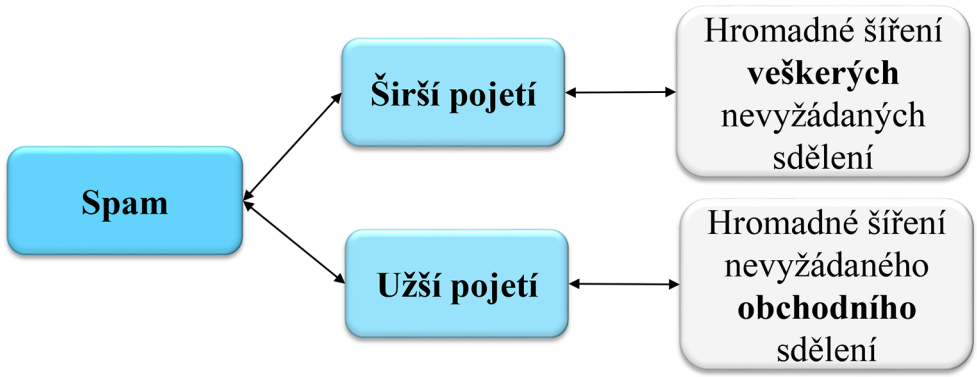



Schéma: Rozdělení spamu

Pro spam je příznačné, že se jedná o **sdělení**, které je **zaslané elektronicky, hromadně a zejména bez vyžádání**.

Spam využívá různé komunikační kanály k odesílání nevyžádaných zpráv:

- e-mail;
- jiný messenger (ICQ, Skype atp.);
- SMS, MMS;
- diskusní fóra, blogy, sociální sítě atp.;
- herní platformy aj.

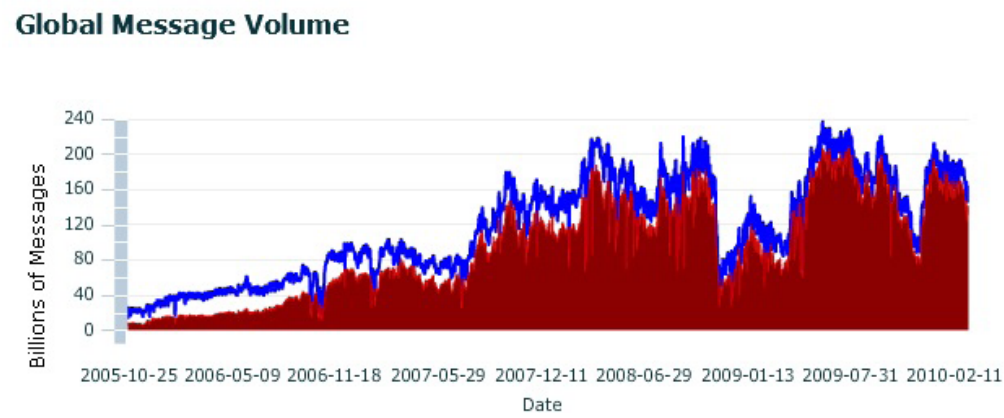
Spam může obsahovat informace:

- **obchodní či reklamní;**
- **o zdraví a medicíně** (Tato kategorie obsahuje spam nabízející produkty na snížení váhy, kosmetické přípravky, netradiční medicínu, léky nedostupné v daném regionu aj.);
- **finanční** (Zejména se jedná o nabídky různých půjček možnosti přivýdělku aj.);
- **pornografické** (Tento spam buď nabízí různé, i farmaceutické přípravky na zvýšení sexuální potence, nebo odkazuje na stránky s pornografickým obsahem.);
- **edukační** (nabídky různých kurzů, tréninků aj.);
- **hoax** (řetězový dopis);
- **politické;**
- **náboženské;**
- **kriminální** (Do této kategorie spadají zprávy obsahující například malware, či odkazující na stránky se škodlivým kódem aj.[454]).

454: Blíže viz kap. 4.5.1 Scam 419.

V současnosti existuje velké množství statistik uvádějících různé počty spamů v elektronických poštách. Jirovský například uvádí, že lze očekávat více než 90% podíl spamu v elektronické poště.[455] V roce 2006 došlo k odeslání průměrně 14,5 miliard spamových zpráv za den.[456] Díky tomu došlo i ke vzniku mnoha organizací zabývajících se spamem a poskytujících nástroje k ochraně před ním. Jednou z těchto společností byla i společnost TrustedSource,[457] odkud pochází i následující graf znázorňující obsah spamu v elektronické poště od roku 2005 do roku 2010. Modrá[458] linie znázorňuje počet e-mailových zpráv a červené pole odráží počet spamů v e-mailové poště (obojí je uvedeno v miliardách).

Bez ohledu na přesná procenta v současné době tvoří takovýto druh nevyžádaných sdělení většinu ze všech doručených e-mailových zpráv.[459] K uživateli se však, díky řadě technických opatření na straně jednotlivých ISP, dostane minimum zpráv, jež představují spam.




Obrázek 52: Vývoj spamu od 2005 do 2010

455: Srov. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 104

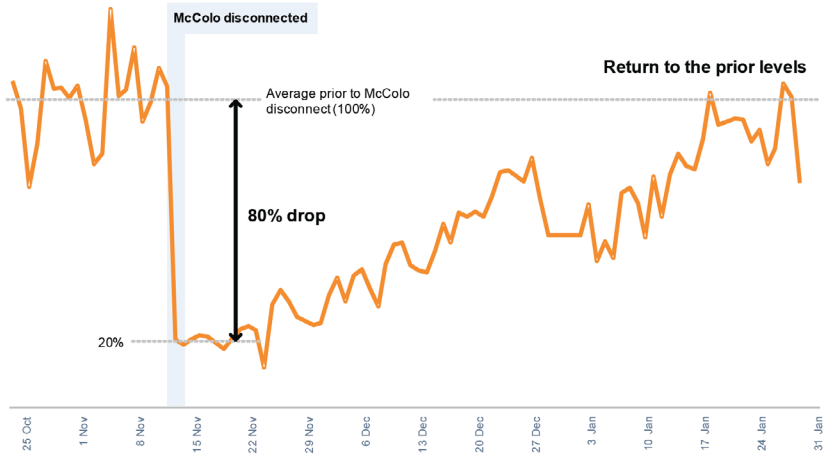
456: Srov. např. *Spam statistics*. [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.spamcop.net/spamstats.shtml *Spam Statistics and Facts.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.spamlaws.com/spam-stats.html

457: Původní online zdroj: http://www.trustedsource.org/TS?do=home [cit. 12. 2. 2010].

458: Poznámka vydavatele: V černobílé verzi knihy nahrazuje modrou barvu černá, červenou šedá.

459: Nelze přesně určit, kolik procent ze všech e-mailů tvoří spam. Různé dostupné zdroje uvádějí různá, někdy značně odlišná čísla. Např. jeden z poskytovatelů antispamových řešení, společnost POSTINI, v březnu 2005 v průběhu 24 hodin zaznamenala, že 10 z 12 e-mailů bylo spam. K četnosti zasílání spamu srov. např. LANCE, James. *Phishing bez záhad.* Praha: Grada, 2007, s. 22, SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers & Security*, 2007, roč. 26, č. 5, s. 361–372.

Výrazný propad spamu na konci roku 2009 je zapříčiněn ukončením činnosti společnosti **McColo**, která se zabývala rozesíláním nevyžádaných zpráv na Internetu.[460]




Obrázek 53: Vývoj spamu po ukončení činnosti McColo v listopadu 2008

Spam zasahuje do elektronické komunikace, mnohdy ji zcela znemožní (dojde k zahlcení informační struktury) a snižuje tak důvěru společnosti v informační technologie. Pokud však dochází k omezování spamu, de facto dochází k omezování práva na svobodu projevu (viz **čl. 17** Listiny[461]) ve prospěch práva ochrany osobní integrity (viz **čl. 10 odst. 2** Listiny[462]). I z tohoto důvodu je právní postih spamera značně komplikovaný a v současnosti dochází k využití institutů práva občanského a správního, neboť trestní právo neumožňuje spamera potrestat. Mimo trestní právo je možné postihnout spamera dle § 119 odst. 1 písm. h) či i) ZoEK, kde se osoba dopustí přestupku, pokud v rozporu s § 93 použije adresu elektronické pošty pro odeslání zprávy nebo zpráv třetím

460: *Malware, mayhem, and the McColo takedown.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

461: Čl. 17 Listiny:

1) *Svoboda projevu a právo na informace jsou zaručeny.*
2) *Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.*
3) *Cenzura je nepřípustná.*
4) *Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.*

462: „*Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*“

osobám bez souhlasu držitele adresy elektronické pošty, nebo pokud v rozporu s § 96 odst. 1 ZoEK nabídne marketingovou reklamu nebo jiný obdobný způsob nabídky zboží nebo služeb účastníkovi nebo uživateli, který uvedl, že si nepřeje být kontaktován za účelem marketingu.

Ze správněprávního hlediska je problematika zasílání nevyžádaných reklamních sdělení v České republice řešena zákonem o některých službách informační společnosti,[463] ve znění pozdějších předpisů. Tento zákon sice nepracuje s pojmem spam, upravuje však podmínky pro zasílání a přenos **obchodních sdělení**, kterým se rozumí *„všechny formy sdělení, včetně reklamy a vybízení k návštěvě internetových stránek, určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku osoby,* ***která je podnikatelem*** *nebo vykonává regulovanou činnost.* “[464]

Problémem je, že jestliže spam, resp. jeho zaslání, nesplňuje zákonem stanovené požadavky o obchodním sdělení, pak se z pohledu zákona o spam nejedná (byť z obsahového hlediska ano). Do této oblasti mohou spadat spamy obsahující pornografické odkazy, hoaxy, politické a náboženské vyjádření a také spamy s kriminálním obsahem.

Spam obsahující kriminální či jiný podvodný obsah je označován jako **scam** (z anglického *„scam“* – podvod, švindl). Scamy tvoří v současnosti podstatnou část spamu a jejich účelem je, typicky za použití sociálního inženýrství, získat důvěru uživatele a donutit ho vykonat požadované úkony (např. otevření přílohy e-mailu, navštívení zobrazeného URL aj.). Mezi scam je možné zařadit *phishing, malware, 419, hoax, podvodné loterie a nabídky, dárcovský scam, Cold-call Scam, Facebookový like scam aj.*[465]

463: Viz kap. 2.5 Odpovědnost poskytovatele služeb informační společnosti.

464: Viz § 2 písm. f) ZSIS

465: **Phishing** – viz kap. 4.6.1 Phishing.

**Malware** – viz kap. 4.3 Malware.

**Scam 419** – jedná se o označení podvodu, který je také znám jako **Nigerijské dopisy.**

**Hoax** – jedná se o „řetězové e-maily“. Viz dále.

U **dárcovského scamu** je typické rozeslání žádosti o pomoc z důvodu nemoci (dítěte, člena rodiny aj.) či finančních problémů.

**Cold-call scam** – je typicky e-mail z IT oddělení, či společnosti. V rámci zprávy je uvedena informace, že uživatelův počítačový systém je infikován malware, a z tohoto důvodu je třeba vzdáleně připojit IT oddělení, aby byl problém vyřešen. Blíže viz např. *Does Microsoft call about computer being infected with virus?* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.computerhope.com/issues/ch001385.htm

**Facebookový “like” scam** - Jedná se o sbírání „lajků“. Blíže viz *K čemu slouží facebookový „like“ scam* [online]. [cit. 14. 8. 2016]. Dostupné z: https://blog.nic.cz/2013/08/06/k-cemu-slouzi-facebookovy-like-scam/


Obrázek 54: Schéma rozdělení scamu

Bližší pozornost budu na tomto místě věnovat třem typům scamu a to konkrétně **Scam 419**, **Hoax** a **Podvodným nabídkám**.

### 4.5.1 Scam 419

Scam 419 představuje označení pro e-maily, které jsou spíše známy jako **Nigerijské dopisy**. Tyto podvody jsou ukázkou přenosu normální kriminality (podvodů) ze světa reálného do světa virtuálního. Jeden z prvních odkazů na jednání podobné dnešním Nigerijským dopisům uvádí Šejnoha ve své monografii a označuje jej jako ***Španělští podvodníci s pokladem***:

***„Trik, jehož pomocí snaží se podvodníci vylákati na bohatých osobách v cizině peníze, jest velmi starý a již koncem minulého století se vyskytli pokusy i podvody tohoto druhu.*** *V poslední době vyskytla se v Československu celá spousta dopisů a těchto podvodníků, kteří zasílají na adresy zámožných obchodníků dopisy, podepsané neexistující osobou, která o sobě tvrdí, že pro úpadek byla zatčena a že na nádraží na hranicích Francie před svým zatčením uložila kufr, v němž jest schován zisk z jejího úpadku, v obnosu mnoha set tisíc korun. Tato osoba žádá adresáta, aby tento kufr vyzvedl a z peněz v něm uložených zaplatil soudní útraty za bankrotáře, případně podplatil soudce apod. Za tuto službu slibuje mu vyplatiti později 1/3 až 1/2 schované sumy. K dopisům bývá také připojen krátký text telegramu, který má adresát odeslat na uvedenou adresu, v případě, bude-li s plánem souhlasiti. Celý trik spočívá patrně v tom, aby zámožná osoba byla vylákána do ciziny a tam ošizena o peníze,*

*nejedná-li se o horší záměry.* ***Drzost a nestoudnost těchto podvodníků jde tak daleko, že docela své dopisy rozmnožují na cyklostylu.*** "[466]

Pokud srovnáme jednání, jež je v současnosti označeno jako Scam 419 (Nigerijské dopisy) a popis jednání „Španělských podvodníků s pokladem", je možné vypozorovat de facto jediný rozdíl, který spočívá v rychlosti a hromadnosti šíření současných podvodných dopisů. Nástup Internetu umožnil obnovit starý trik a rozšířit jej skutečně masově s minimálními požadavky na náklady.

Pro zajímavost přikládám tři značně odlišné zprávy mající povahu Scamu 419.

**Zpráva č. 1 – „Zdědil jste obrovskou sumu peněz"**

Ahoj drahý,
Jsem Advokát Victoria Josef, mám pro vás zprávu týkající se mého zemřelého klienta, který nese stejné příjmení jako vy, jsem si vědom, nemusí vztahovat k němu krve, ale je státním příslušníkem ve vaší zemi, který přišel o život po boku svého přímé rodina při nehodě zde v Togu motoru.

On odešel za částku ve výši 2.700.000 $, Mezitím, jeho banka chce převést výhody na některou z jeho rozšířené člena rodiny jako prezentace může být podána prostřednictvím mé kanceláře. Chcete-li být upřímný, tyto peníze patří do mého zemřelého klienta, který má stejné příjmení a státní příslušnost s vámi bydlil a působil zde v Togu pro více než 20 let jako dodavatele, ale zemřel ve smrtelné autonehody spolu se všemi členy jeho rodina v roce 2009 a nedávno, banka, kde se ukládají tyto peníze mi dal mandát k poskytnutí nějakého člena jeho rodiny požadovat tyto peníze nebo jinde to bude předána do vlády účet státní pokladny jako opuštěné peníze.

Nechci, aby se to stalo, ale problém je, že jeho předpokládaný nejbližší příbuzní zemřeli v tomto stejném autonehodě a všechny své úsilí k dohledání členy jeho rodiny, od jeho smrti byl ve sporu neúspěšný, když se nikdy představil některé z nich ke mně, zatímco on byl naživu.

Příteli, to je důvod, proč jsem se pustil na tuto misi najít někoho na práci z ruky do ruky se mnou nároku tento fond, abychom pomohli našim rodinám a potřebným, místo, aby mohly tyto zkorumpovaní vládní úředníci, aby převzal tento těžce vydělané peníze, stejně jako že a rozhazovat to, opouštět chudé masy trpět. Pro mě vyzvednout na vás mezi miliony lidí na Facebooku; prostě znamenat, že je to Bůh, který učinil naše cesta naštvaná, takže pojďme pracovat společně s jedním mysli, jak budeme sdílet peněz tak, jak jej tvrdil. Uveďte, prosím, Váš zájem o toto tvrzení tak, že můžu vám poskytne, pokud jde o práci a směrnic.

Advokát Victoria Joseph Esq.

466: Blíže viz ŠEJNOHA, Josef. *Systém kriminalistického vzdělání (Psychologie zločinu a zločinnosti).* Praha: F. Kodym, 1936, s. 492

**Zpráva č. 2 – „Zamilovala jsem se“**

Ahoj drahoušku
Jmenuji se Joe Anita Jsem žena, jsem zjistil jeho totožnost na straně, a chci se naučit, že víme o sobě více a sdílet společenský život s kulturou, a nemám co říct, tak prosím odpovězte mi , tak i já posílám svá data na vás a řeknu více o sobě ve svých obrazech. Děkuji mnohokrát.

Vaše radost Anita

**Zpráva č. 3 – Nigerijský astronaut byl zapomenut ve vesmíru a potřebuje se dostat domů**
Tato zpráva se začala šířit v roce 2004, už v té době se „první africký astronaut“ nacházel ve vesmíru 14 let bez přestávky. Je třeba konstatovat, že délkou pobytu překonal všechny časy astronautů (možná i v součtu). Poslední verzi tohoto Scamu 419 jsem obdržel letos (r. 2016). Byť mi je tohoto imaginárního astronauta velmi líto (26 let ve vesmíru a sám), rozhodně nemíním přispět podvodníkům. Bohužel i přes zcela nesmyslný obsah a nijak nepodložené informace obsažené v tomto e-mailu se najde značná část osob, které chtějí pomoci osobě v nouzi (díky této pomoci by tento scam mohl být zařazen i do skupiny *dárcovský scam*).

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number 234 (0) 9-234-2220 only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager
tip@nasrda.gov.ng

http://www.nasrda.gov.ng/

Vzhledem k povaze podvodného jednání by bylo možné, v některých případech, Scam 419 označit či podřadit i pod jednání mající povahu phishingu.

### 4.5.2 Hoax

Hoax (anglicky - smyšlenka, žert, novinářská kachna) je další formou spamu, případně scamu. Hoax je označení pro řetězové zprávy (řetězově rozesílané zprávy typu: *„pošli to dál"*, *„pokud to nepošleš 20 dalším lidem, tak se stane…* " aj.), které uvádějí zkreslené, nepravdivé, zavádějící či jiné falešné informace. Hoax obsahuje často varování před útoky, popisy nebezpečí, prosby o pomoc, výzvy, petice, prohlášení slavných, řetězové dopisy štěstí, žertovné zprávy, obrázky a videa v prezentacích, hrající si kočičky a jiná zvířátka atd.

Nejrozšířenější Hoaxy je možné nalézt na stránkách http://www.hoax.cz/cze/. V současnosti patří mezi nejrozšířenější Hoaxy tyto zprávy:

- Funkce v MS WORDU =rand(200,99)
- Šok v lékárně - kdo nemusí platit za léky
- Pomeranče s krví a HIV
- Telefonáty z čísla 00420 477 100 111
- Slovenčina - nejtěžší jazyk na světě
- Pozor na výběr zubní pasty - barevný pás na obalu
- Proč neplatit pokuty
- Sokujici navod, jak vydelavat penize
- Facebook - copyright na profil
- Nové radary ve svodidlech
- V nouzi zadej PIN opačně
- Recyklované mléko

### 4.5.3 Podvodné nabídky

Velmi úspěšnou formou scamu jsou různé podvodné nabídky, které mohou být rozesílány hromadně či cíleně. V současnosti jsou takovéto nabídky rozesílány nejen prostřednictvím e-mailů, ale i pomocí jakýchkoliv instant messengerů, sociálních sítí, aukčních portálů atd.

Pokud jde o hromadné rozesílání podvodných nabídek, je možné si pod tímto pojmem představit celou řadu aktivit na principu „pyramida" či „letadlo", nabídky výhodných prací z domova,[467] „zaručené" metody zhodnocení peněz (s nejvyššími úroky), nabídky na půjčku (s nejnižšími úroky), „skvělé" pracovní příležitosti aj.

467: Viz Obrázek 55. Tyto nabídky mohou jednak spočívat v žádosti typu: *„pošlete nám 10 dolarů na účet a my vám pošleme návod, jak vydělat 8847 dolarů měsíčně"*. Druhou možností je, že tyto nabídky práce nevyžadují žádný poplatek předem, pouze požadují registraci uživatele. Vlastní registrací pak útočník obdrží osobní údaje o uživateli. Na uživatelovu e-mailovou adresu pak může být zaslán e-mail od této společnosti, obsahující např. malware aj.

Do cíleného odesílání podvodných nabídek je třeba zahrnout i jednání, které nemá povahu pouhého spamu, ale jde například o kombinaci nabídky konkrétního druhu zboží v rámci aukčních portálů a následnou komunikaci s uživateli, kteří na tuto nabídku přistoupili. Jedná se o tzv. „aukční podvody."


Obrázek 55: Neodolatelná nabídka práce z domova (hromadné rozesílání v rámci sociální sítě Facebook)

V současnosti již rozhodně není pravidlem, že jsou hromadně či cíleně odesílané nabídky psané podezřelou nebo lámanou češtinou (nebo jsou psané anglicky či rusky), naopak snahou útočníka je přesvědčit oběť o absolutní korektnosti, serióznosti a „čestnosti" svého jednání. V rámci aukčních portálů jsou velmi často podvodně nabízeny různé druhy elektroniky, zejména mobilních telefonů a počítačů. Vlastní podvodné jednání pak může spočívat například ve změně podstatných informací [např. země původu mobilního telefonu; informaci o tom, že jde o kopii (padělek) telefonu] či nedoručení zboží jako takového (útočník velmi často žádá zaplacení celé částky či zálohy).

Jako příklad cíleného podvodného jednání uvedu aukční podvod s motocyklovým veteránem. Nabídku, kterou jsem nalezl na portálu www.hyperinzerce.cz, prostě nebylo možné přehlédnout, neboť se jednalo o veterána v perfektním stavu za neuvěřitelně málo peněz, navíc s nabídkou dohody. Obsah vlastního inzerátu zněl:

*Prodám jawa 350 typ 18 pérák, rok 1952,po celkové renovaci,uveden do puvodního originálního stavu k motorce pouze puvodní tp-vyřazen z evidence v roce 1985. Duvod prodeje -dědictví po otci. Prodám pouze tomu,kdo bude o motocykl pečovat,neprodám překupníkovi. Cena 38 000kč dohoda.*

Obrázek 56: Orientační fotografie přiložená k inzerátu

Celý text inzerátu bylo možné nalézt na:
http://motorky.hyperinzerce.cz/veterani-motorky/inzerat/11031790-prodam-jawa-350-typ--18-perak-nabidka-olomoucky-kraj/.

Vzhledem ke stavu motocyklu (dle orientační fotografie), jeho běžné ceně na trhu a nulovým kontaktům na inzerenta jsem měl od počátku podezření, že se jedná o podvodný inzerát, přesto jsem se rozhodl na inzerát zareagovat. Důvodem byl prostý kalkul spočívající v následujících hypotézách: Pokud je to podvod, alespoň vyzkouším, jak je na tom útočník (zjistím o něm informace, informuji další o tom, že je to podvod atd.), pokud to podvod není, třeba získám zajímavou motorku.

**Inzerent** (potenciální **útočník**) se ozval za 9 dní s následující odpovědí:

_____dobry večer pane,
včera jsem se vratil z nemocnice , autonehoda -už je vse ok , zitra odjiždim do prace -pracuji mimo čr -Německo ,nemohl jsem se zabyvat prodejem motocyklu jawa 350 perak , proto jeste je na prodej , mam v email .schrance 56 odpovědi -zajemcu odepisuji postupne vsem motorku jsem zdedil po tatovi ,ktery pred rokem zemřel-musim to prodat -nechci to mit doma -nevim jestli to pochopite motorka je po špičkove renovaci , plne funkcni-pojizdna ,nema spz,pouze odhlaseny TP foto v priloze

V příloze byly přiloženy tři fotografie, z nichž vybírám pouze jednu ilustrační:

V tento okamžik jsem byl již přesvědčen, že osoba, se kterou jednám, je podvodník, který se pomocí podvodné aukční nabídky snaží provést svůj útok a obohatit se. Důvodů, které mne přesvědčily, bylo několik.

První z nich spočíval v prověření si zaslané fotografie pomocí Google search na www.google.com - vyhledávání dle obrázků. Google hned jako první odkaz nabídl stránky Starožitné motocykly a odkaz na Jawa Pérák 18-350 VERSION EXPOR modrá pařížská. Viz: http://www.zabytkowe-motocykle.eu/cz/fotogalerie/jawa-perak-18-350-version-export-modra-parizska/. Na této stránce jsem nalezl identickou fotografii jako tu, co mi poslal útočník, pouze v jiném barevném provedení:


Jedninou práci, kterou si útočník s fotografií dal, byla změna barvy, což je operace, která zabere v grafickém software řádově minuty.

Druhou indicií pak byla skutečnost, že útočník průběžně v komunikaci tvrdil, že je v ČR, pak zase, že už v Německu atd., přičemž komunikace z jeho strany celou dobu přicházela z adresy: 141.76.45.34 (viz zdrojový kód zprávy), což je adresa patřící do rozsahu Technische Universität Dresden. Poslední indicií pak bylo zadání e-mailu útočníka: sarkozi.r@centrum.cz do vyhledávače. Zobrazeno bylo několik varování před podvodníkem.

V tento okamžik už bylo jasné, kdo je podvodník a kdo má být oběť. Nicméně jsem se rozhodl tuto hru hrát dál s tím, že jsem změnil role a snažil se získat další informace, které by mohly být následně použity v trestním řízení.

**Domnělá oběť:**

Dobrý den,
Děkuji za odpověď. Doufám, že je Vám líp. O Vašeho, **opravdu krásného, péráka bych měl skutečný zájem**. Chtěl bych se zeptat: Je možné motorku vidět osobně? Jakou máte představu o ceně? Kdy by teoreticky byla k prodeji?

**Útočník:**

__dobry den ,jsem z Olomouce , cena je 38 tis kč možnost prodeje pouze sobota -nedele už jsem v Praci -v Německu dekuji ,už je mi ok-mel jsem otres mozku ,zlomeny žebro -to bude bolet podle doktora jeste za mesic. Šarkozi

**Domnělá oběť:**

**Cena je krásná** a jak jsem psal, **motorka se mi moc líbí. Zájem bych o ni měl eminentní.**

**Útočník:**

____pokud se dohodneme na zaloze ,tak urcite motorku rezervuji -neprodam cekam na vas _

Se zálohou jsem souhlasil, avšak útočník přestal komunikovat. Jedním z důvodů zřejmě byla masivní kampaň uživatelů aukcí, kteří před touto osobou varovali v rámci diskusních a jiných fór.

**POZOR NA PODVODNÍKA!!!**

Dobrý deň, chcem upozorniť na inzerát, ktorý bol na eurooltimers a teraz je na hyperinzercii, že pán predá Jawu perák 350 typ 18-dedičstvo po otcovi cena 38000 Kč. Je to čistý podvod, žiada zálohy, píše že pracuje v Rakúsku a doma bude až cez víkend. Vystupuje pod cudzím menom, emailom a aj adresou. Používa mail "sarkozi.r@centrum.cz". Prosím nereagujte na tento inzerát a hlavne neposielajte zálohy!!! [Juzek] 21.09.2015 Přidat odpověď

To se ještě v této situaci, v jaké se společnost nachází, najde nějaký naivní člověk co pošle cizí osobě zálohu na účet předem? To si ti policajti musejí hlavy ukroutit! [fikuscz] 22.09.2015

http://www.noveinzeraty.cz/Detail/21935457 Pozor, neposílat zálohy na Účet.. je to podvod ,už je to nahlášeno na policii.. prosím o pomoc dotyčné poškozené nahlašte tuto věc na policii. tel. 585413501 Policie, Olomouc [marisa] 22.09.2015

Obrázek 57: Varování na diskusním fóru[468]

468: [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.veteranforum.cz/index.php?id=11&idkat=114&idtop=269120

Na základě vlastního případu i dalších informací bylo na www.hyperinzerce.cz nahlášeno podvodné jednání. A ISP provozující tento aukční portál přijal následující opatření:

> Došlo-li ze strany inzerenta k podvodnému jednání (např. nedodal inzerované zboží ani po uhrazení zálohy či zaplacení předem) nebo došlo ke zneužití Vašich údajů (inzerát byl zveřejněn s Vaším emailem, telefonem), tak doporučujeme obrátit se na příslušné orgány nebo Policii ČR. My poté na jejich vyžádání poskytneme plnou součinnost v odhalení totožnosti pachatele a poskytneme veškeré nám dostupné informace o něm, zejména IP adresy, z nichž k nám přistupoval.
>
> Naši administrátoři zároveň nyní posoudí předmětný inzerát a případně jej zaarchivují, aby se již nezobrazoval na webu.

Nápaditost útočníků je v prostředí Internetu značná a v případě jakýchkoli nabídek, inzerce a zejména zasílání záloh či plateb je vhodné být paranoidní a nedůvěřovat neznámým osobám.

V případě podvodných nabídek, kdy se útočník snaží získat různé zálohy či jiné platby předem, je takovéto jednání možné postihnout dle **§ 209** (Podvod) TZK.

**Pokud jde o trestněprávní postih spamu a spammerů, v České republice není v současnosti zcela (vy)řešený.** Absentuje jak vnitrostátní, tak i mezinárodněprávní ochrana před tímto nežádoucím jednáním. Ani Úmluva o kyberkriminalitě v sobě neobsahuje vymezení spamu jako trestného činu.

Například v **USA** již v minulosti k odsouzení spammerů[469] za rozesílání nevyžádané pošty došlo. Například **Jeremy Jaynes** byl v roce 2007 odsouzen soudem ve Virginii k 9letému trestu odnětí svobody. Obviněn byl již v roce 2003, jako důkaz sloužilo 53 000 spamů odeslaných během tří dnů. Prokurátor však dle svého vyjádření věří, že Jaynes je odpovědný za rozesílání více než 10 000 000 spamů denně, což mu mělo vynést přibližně 750 000 USD měsíčně.

Vzhledem k tomu, že pod pojmem spamming nelze zařadit pouze jednu formu škodlivého jednání, je velmi složité spamming sám o sobě postihnout prostředky trestního práva. Tak lze učinit pouze u jednotlivých jeho druhů. V určitých případech připadá v úvahu postihnout sběr e-mailových adres, jestliže takový sběr naplní znaky skutkové podstaty trestného činu neoprávněného nakládání

469: *Convicted spammer challenging Va. law* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm
*Top Spammer Sentenced to Nearly Four Years*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.pcworld.com/article/148780/spam.html
*Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

s osobními údaji podle **§ 180** (Neoprávněné nakládání s osobními údaji) TZK.[470] Pokud spam obsahuje malware, nebo je jeho cílem dokonání podvodného jednání, je možné činnost spamera postihnout dle ustanovení vztahujících se na malware (viz kap. 4.3) či na phishing (viz kap. 4.6.1).

## 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing

### 4.6.1 Phishing

Pojmem phishing[471] se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj.

V **užším slova smyslu** phishing představuje jednání, které po uživateli vyžaduje navštívení podvodné stránky (zobrazující např. webovou stránku internetového bankovnictví, online obchodu aj.) a následné vyplnění „přihlašovacích informací", případně jsou tyto informace vyžadovány přímo (např. při vyplnění formuláře aj.).

V **širším slova smyslu** se za phishing dá označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem. V tomto širším slova smyslu již není po uživateli požadováno vyplňování údajů, avšak je mu doručena zpráva (či je uživatel přesměrován na stránku) typicky obsahující malware, který si uvedené údaje posbírá sám. Dále do tohoto širšího pojetí mohou být zařazeny i dárcovské scamy atp.

V obou dvou případech dochází k oklamání uživatele, který je cílem phishingového útoku, rozdíl spočívá především v tom, jaká míra interakce je po uživateli vyžadována.

Podstatou phishingu je využívání sociálního inženýrství. Phishing je možné provádět i ve světě reálném (viz podvody aj.), avšak svět virtuální umožňuje útočníkovi rozesílat podvodné zprávy obrovskému množství potenciálních obětí s minimem námahy. Phishing je, se značnou mírou nadsázky, možné přirovnat ke *„kobercovému bombardování."* Stejně jako v případě bombardování phishing cílí na relativně neurčené množství obětí proto, aby měl útočník naději na úspěch. Google např. v roce 2014 uváděl, že scam mající povahu skutečně dobrého phishingu je při zisku dat o uživatelích úspěšný z 45 %.[472]

470: Srov. ŠTUDENTOVÁ, Milada. Trestněprávní aspekty související se zasíláním e-mailů a zveřejňováním materiálů na webových stránkách. *Trestní právo*, 2007, roč. 13. č 7 – 8, s. 27.

471: V českém jazyce bývá slovo phishing používáno nejčastěji ve své anglické podobě, někdy je (dosti násilně) překládáno do českého jazyka jako *rhybaření, rhybolov* či *rybolov*. Překlad je značně umělý, anglická homofonie *ph*↔*f* v češtině protějšek nemá.

472: Viz např. *Google says the best phishing scams have a 45-percent success rate*. [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/
*Phishing by the Numbers: Must-Know Phishing Statistics 2016.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://blog.barkly.com/phishing-statistics-2016

Phishing není zaměřen pouze na e-maily. Je možné nalézt phishing v rámci instant messages (Skype, ICQ, Jabber aj.), sociálních sítí, SMS a MMS zpráv, chatovacích místností, scamu (podvodné nabídky práce, zboží aj.), falešných aplikací do prohlížeče[473] aj.

**Phishing v užším smyslu slova**
Princip *„klasického"* phishingového útoku spočívá nejčastěji v zaslání tzv. phishingového e-mailu poškozenému, který na první pohled nevzbuzuje žádné podezření, že by mělo jít o podvodné sdělení. Součástí takového e-mailu bývá zpravidla odkaz, na nějž je uživatel vyzýván kliknout.

Po kliknutí na přiložený odkaz se uživatel dostává na podvodnou webovou stránku, která se svým vzhledem i funkcemi od originální korektní webové schránky téměř neliší. Jedná-li se o napodobeninu webové stránky, pomocí které je možné realizovat platební styk, vstupovat na zabezpečená konta, taková konta spravovat apod., pak jsou uživatelem zadaná data automaticky odesílána útočníkovi.[474] Ten tímto způsobem může získat identifikační údaje uživatelů internetových bankovních služeb, přístup k jednotlivým bankovním účtům uživatelů napadených systémů, může získat identifikační čísla a další údaje o platebních kartách, s jejichž pomocí je poté v prostředí Internetu možné realizovat platební styk atd.

Vlastní phishingový útok probíhá v několika krocích.[475]

1) **Plánování phishingového útoku**
   V této fázi phishingového útoku dochází k výběru cíle (skupiny uživatelů) a k výběru metody, která má být k útoku použita. Je vyhodnocováno, jakým způsobem je cíl technicky zabezpečen, jaká jsou rizika odhalení identity útočníka apod.

2) **Vytváření podmínek pro phishingový útok**
   V této fázi dochází k technickému řešení phishingového útoku. Útočník získává seznamy e-mailových adres uživatelů, jimž má být zaslán phishingový e-mail, je vytvořená datová schránka, kam systém zašle získaná data uživatelů, dochází k vytvoření důvěryhodného sdělení, které je následně distribuováno uživatelům.

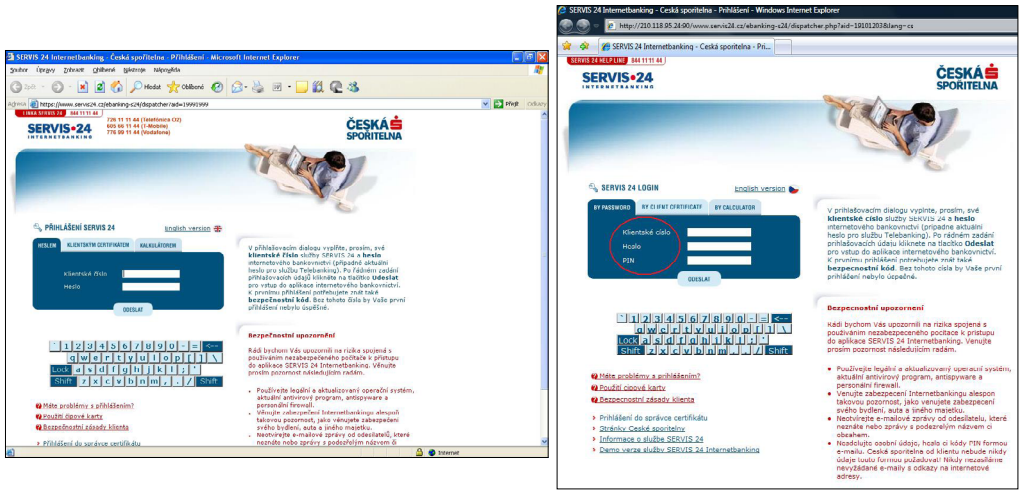
3) **Vlastní phishingový útok**
   Phishingový e-mail je doručen jednotlivým uživatelům a v závislosti na kvalitě zpracování tohoto e-mailu a dalších faktorech (zkušenost uživatele, jeho informovanost o phishingové problematice, antiphinshingový software cíle apod.) jsou data zasílána do datové schránky útočníka. V této fázi phishingového útoku se vůbec poprvé uživatel setkává s phishingovým e-mailem.

473: Viz např. *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.hackread.com/fake-android-prisma-app-phishing-malware/

474: LANCE, James. *Phishing bez záhad*. Praha: Grada Publishing, 2007. s. 45.

475: **WILSON Tracy, V.** *How Phishing Works.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://computer.howstuffworks.com/phishing.htm

Jako záminka často slouží informace o chybě v bezpečnostním systému společnosti či jiné varování, které má vzbudit u uživatele pocit autentičnosti této zprávy. Po aktivaci interaktivního odkazu je osoba přesměrována na webovou stránku, vytvořenou útočníkem, věrně kopírující originální stránku finanční instituce. Uživatel je vyzván k vyplnění přihlašovacích údajů, zpravidla včetně čísla karty a PIN kódu. Vyplněné údaje jsou odeslány na adresu phishera, který následně odčerpá z účtu část či veškeré finanční prostředky a způsobí tím klientovi škodu (viz Obrázek 58).[476]




Obrázek 58: Originální stránka (vlevo) a podvodná stránka (vpravo)

4) **Sběr dat**
Útočník získává data, která v prostředí falešné webové stránky zadali jednotliví uživatelé napadeného systému.

5) **Odčerpání peněžních prostředků či jiný profit z phishingového útoku**
Útočník pomocí získaných dat vstupuje na skutečná bankovní konta jednotlivých uživatelů a odčerpává peněžní prostředky. Pomocí převodu na další, zejména zahraniční účty, rozmělnění těchto peněžních prostředků a pomocí dalších technik se odčerpané peněžní prostředky stávají prakticky nevystopovatelnými.

476: Blíže viz: KOLOUCH, Jan a Petr VOLEVECKÝ. Trestněprávní aspekty phishingového útoku. In *Trestní právo*, 2008, roč. 12, č. 9, s. 5–12.

Je velmi obtížné určit, kolik phishingových útoků je denně po celém světě realizováno. Stejně tak je problematické určit, kolik klientů napadených společností odpoví na phishingový e-mail. Odhaduje se, že míra návratnosti se pohybuje kolem 0,01 a 0,1 %.[477]

Prognózy v roce 2007 odhadovaly, že „klasických" phishingových podvodů či kampaní bude v budoucnu přibývat.[478] Tyto prognózy se naplnily částečně, neboť ubývá „klasických" phishingových kampaní, avšak phishing v širším slova smyslu je na vzestupu,[479] zejména se objevují jeho nové modifikace či propojení phishingu s jinými typy útoků (malware, propojení do sítě botnet aj.).

**Phishing v širším smyslu slova**

V rámci demonstrace phishingu v širším slova smyslu uvedu čtyři kampaně, které v období 2014–2016 proběhly v České republice a byly více či méně úspěšné. Uvedené útoky samozřejmě nejsou jedinými phishingovými útoky v širším slova smyslu, které se v ČR uskutečnily. Důvodem výběru těchto čtyř konkrétních útoků je ta skutečnost, že chci poukázat zejména na inovativní přístup útočníka a vhodné spojení technického útoku se sociálním inženýrstvím. Konkrétně se jedná o útoky:

1) **Dluh/Banka/Exekuce**
2) **Česká pošta**
3) **Vánoce a dárky**
4) **Seznam.cz – One Time Password**

477: LANCE, James. *Phishing bez záhad*. Praha: Grada, 2007, s. 35.
K problematice phishing dále srov. např. VOLEVECKÝ, Petr a Jan STACH. Jak se krade pomocí Internetu – Phishing v praxi. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html
KOLOUCH, Jan a Petr VOLEVECKÝ. Trestněprávní aspekty phishingového útoku. *Trestní právo*, 2008, č. 9, roč. 12, s. 5–12
478: K vývojovým trendům phishingu srov blíže např. DODGE, Ronald. C., Curtis CARVE a Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, roč. 26, č. 1, s. 73–80.
479: **Dle následující studie vzrostl phishing o 250% za posledních 6 měsíců.** Viz *Phishing Activity Tresnds Report.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

#### 4.6.1.1 Dluh/Banka/Exekuce[480]

Phishingová kampaň pracovně nazvaná DBE zasáhla Českou republiku v masivním rozsahu v roce 2014 (přičemž dozvuky této kampaně přetrvaly minimálně do konce roku 2015).[481] Vlastní útok byl velice precizně připraven a zahrnoval v sobě jak vlastní phishing, tak distribuci malware (do počítače a mobilního zařízení). Celý útok je možné rozdělit do následujících fází:

1) **Phishingová kampaň**
2) **Instalace malware do počítače**
3) **Přístup k online bankovnictví**
4) **Instalace malware do mobilního zařízení**
5) **Převod a odčerpání finančních prostředků**

Ad 1) **Phishingová kampaň**
Prvním předpokladem pro to, aby útočníci mohli úspěšně získat finanční prostředky, byla velká phishingová kampaň, na kterou by zareagoval dostatečný počet osob. Vlastní rozesílání podvodných e-mailů bylo rozloženo do tří po sobě jdoucích vln phishingových zpráv:

1) **Dluh** (debt@....); březen–duben 2014
2) **Banka** (bank@....); květen–červen 2014
3) **Exekuce** (emissions@...); červenec–září 2014

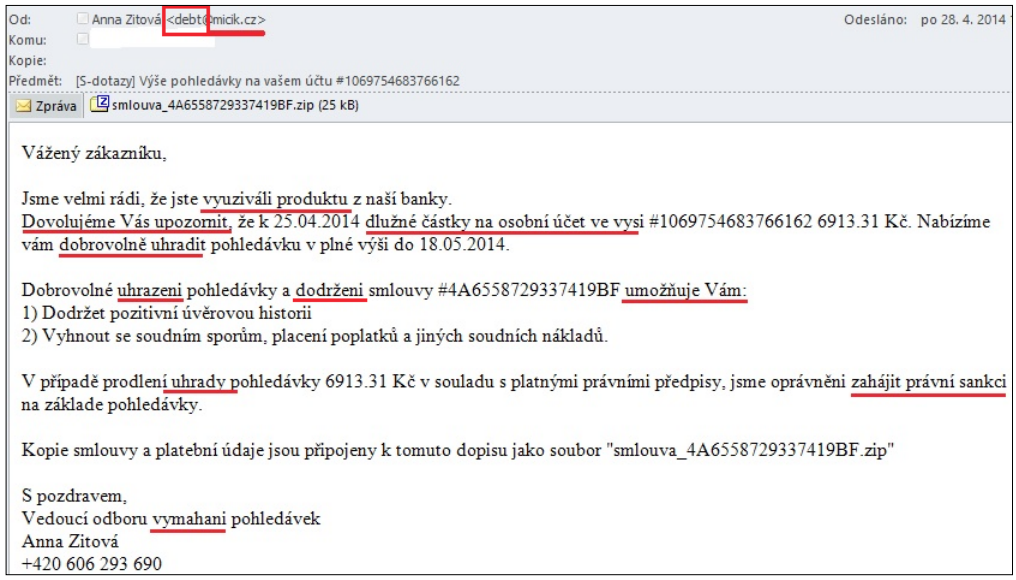
V rámci jednotlivých kampaní docházelo k zvyšování „kvality" vlastních e-mailových zpráv a zejména lepšímu využití sociálního inženýrství ve vztahu k předpokládaným obětem v cílovém regionu, tedy ČR. Všechny výše uvedené phishingové kampaně však měly minimálně dva společné znaky. Za prvé se jednalo o tu skutečnost, že v příloze rozeslaného e-mailu se vždy nacházel soubor, tvářící se jako textový dokument, avšak jednalo se o spustitelný soubor, konkrétně malware: Trojan.[482] Druhým společným znakem bylo, že sociální inženýrství využívalo obav oslovených jedinců z případných soudních sporů, v posledním případě z exekuce.

První vlna phishingových útoků používala velmi špatnou češtinu, byla rozesílána z různých, pokud se jedná o vymáhání pohledávky ne zcela důvěryhodných domén registrovaných v ČR (např. micik.cz či dhome.cz aj.). Využívána byla různá jména osob a existující telefonní čísla, dohledatelná na Internetu (osoba vlastnící toto číslo pak s vlastním útokem neměla nic společného).

480: Dále jen zkráceně **DBE**.

481: Blíže viz např. *Uhraďte dluhy, toto je exekuční příkaz. Komora varuje před další vlnou podvodných e-mailů* [online]. [cit. 15. 8. 2016]. Dostupné z: http://zpravy.aktualne.cz/finance/falesne-exekuce-jsou-zpet-komora-varuje-pred-dalsi-vlnou-pod/r~cbdac6de765111e599c80025900fea04/

482: Blíže viz výsledky z Virustotal. [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.virustotal.com/cs/file/62170532b1f656c6917fa66d0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/



Od: Anna Zitová <debt@micik.cz> Odesláno: po 28. 4. 2014
Komu:
Kopie:
Předmět: [S-dotazy] Výše pohledávky na vašem účtu #1069754683766162
Zpráva smlouva_4A6558729337419BF.zip (25 kB)

Vážený zákazníku,

Jsme velmi rádi, že jste využiváli produktu z naší banky.
Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #1069754683766162 6913.31 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 18.05.2014.

Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #4A6558729337419BF umožňuje Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

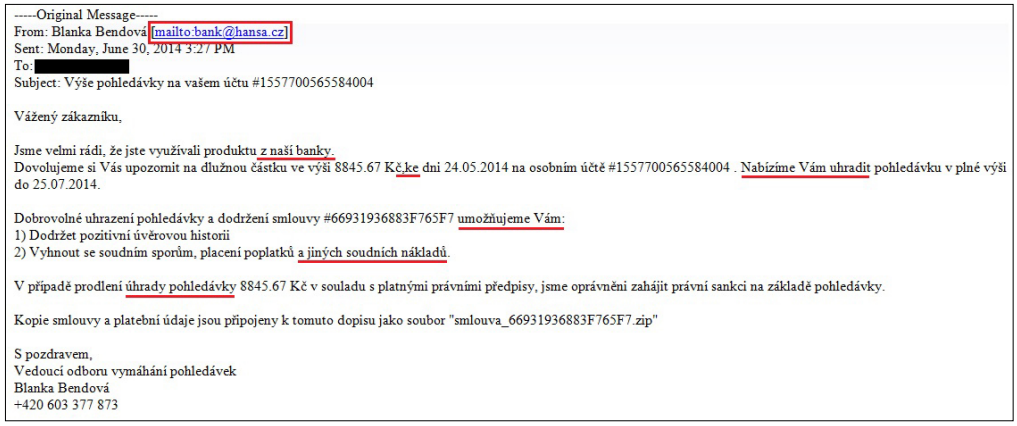
V případě prodlení uhrady pohledávky 6913.31 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_4A6558729337419BF.zip"

S pozdravem,
Vedoucí odboru vymahani pohledávek
Anna Zitová
+420 606 293 690

Obrázek 59: Podvodný e-mail rozeslaný v rámci vlny Dluh

V rámci druhé vlny došlo k zlepšení používané češtiny.



-----Original Message-----
From: Blanka Bendová [mailto:bank@hansa.cz]
Sent: Monday, June 30, 2014 3:27 PM
To: [redacted]
Subject: Výše pohledávky na vašem účtu #1557700565584004

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 8845.67 Kč,ke dni 24.05.2014 na osobním účtě #1557700565584004 . Nabízíme Vám uhradit pohledávku v plné výši do 25.07.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #66931936883F765F7 umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 8845.67 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

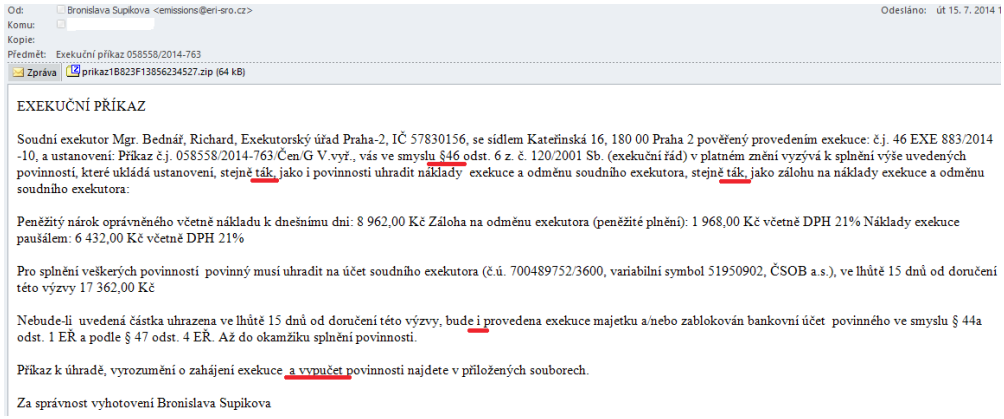
Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_66931936883F765F7.zip"

S pozdravem,
Vedoucí odboru vymáhání pohledávek
Blanka Bendová
+420 603 377 873

Obrázek 60: Podvodný e-mail rozeslaný v rámci vlny Banka

V době, kdy se začaly tyto phishingové útoky objevovat, zveřejňovaly nejrůznější bezpečnostní organizace a CSIRT[483] týmy, ale i masmédia varování, včetně uvedení návodů, jak k takovýmto zprávám přistupovat.[484]

Obě kampaně byly relativně úspěšné, avšak nejúspěšnější byl útok, kde podvodný e-mail představoval varování (výzvu) od exekutora.


Od: Bronislava Supikova <emissions@eri-sro.cz> Odesláno: út 15. 7. 2014 1
Komu:
Kopie:
Předmět: Exekuční příkaz 058558/2014-763
Zpráva prikaz1B823F13856234527.zip (64 kB)

EXEKUČNÍ PŘÍKAZ

Soudní exekutor Mgr. Bednář, Richard, Exekutorský úřad Praha-2, IČ 57830156, se sídlem Kateřinská 16, 180 00 Praha 2 pověřený provedením exekuce: č.j. 46 EXE 883/2014 -10, a ustanovení: Příkaz č.j. 058558/2014-763/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá ustanovení, stejně ták, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně ták, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 962,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 968,00 Kč včetně DPH 21% Náklady exekuce paušálem: 6 432,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 700489752/3600, variabilní symbol 51950902, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 17 362,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Bronislava Supikova

Obrázek 61: Podvodný e-mail rozeslaný v rámci vlny Exekuce

Čeština použitá v „exekučním příkazu“ obsahovala zejména chyby v diakritice, případně byly poněkud krkolomněji formulovány některé věty (podtrženy jsou nejvíce patrné chyby). Využívána však byla jména skutečných exekutorů, dohledatelná na Internetu (uvedený exekutor pak s vlastním útokem neměl nic společného), stejně jako reálně se tvářící čísla exekucí.

Ad 2) **Instalace malware do počítače**
Jak již bylo uvedeno dříve, všechny phishingové kampaně obsahovaly v příloze rozeslaného e-mailu malware: TrojanDownloader (tedy malware určený ke stahování dalšího malware). Tento

483: Computer Security Incident Response Team. Blíže viz např. https://www.csirt.cz/

484: Viz např. *Pozor na zprávu o údajné neuhrazené pohledávce - jedná se o podvod.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/
*Znovu se objevily podvodné zprávy.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.csirt.cz/news/security/?page=97
*PODVODNÉ EMAILY hrozí exekucí, nic neplaťte a neotvírejte!* [online]. [cit. 15. 8. 2016]. Dostupné z: http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html
*Pozor na zprávu o výzvě k úhradě před exekucí - jedná se o podvod.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.csirt.cz/news/security/?page=87
*Čo sa skrýva v prílohe podvodných e-mailov?* [online]. [cit. 15. 8. 2016]. Dostupné z: https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/

malware byl primárně vytvořen a zacílen na operační systém Windows XP, kterému v březnu 2014 skončila podpora.


Obrázek 62: Spustitelný soubor (malware) obsažený v příloze podvodných e-mailů

Po spuštění přílohy došlo k instalaci malware (bankovní trojský kůň) „*Tinba*", který byl na pozadí stažen z Internetu, zatímco uživateli byla zobrazena smlouva či exekuční příkaz v textovém editoru.[485]

Malware se zapsal do adresáře: **Users/**konkrétní uživatel**/AppData/Roaming/brothel**. V tomto adresáři bylo možné nalézt ate.exe, což je soubor, který vznikl po otevření spustitelného souboru v phishingovém e-mailu. Zároveň byl v registrech vytvořen příslušný klíč ve větvi **HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun**. Tímto způsobem bylo možné ověřit, zda se jedná o malware pocházející z tohoto útoku.

Ad 3) **Přístup k online bankovnictví**
Dalším krokem útočníka pak bylo počkat na okamžik, kdy se oběť přihlásí do online bankovnictví. Malware v počítači je schopen zaznamenávat komunikaci mezi uživatelem a online bankovnictvím a útočník má možnost tuto komunikaci sledovat. Uživatel měl minimální šanci rozpoznat vlastní útok, neboť URL adresa v prohlížeči náležela dané bance a komunikace byla zabezpečena (HTTPS).

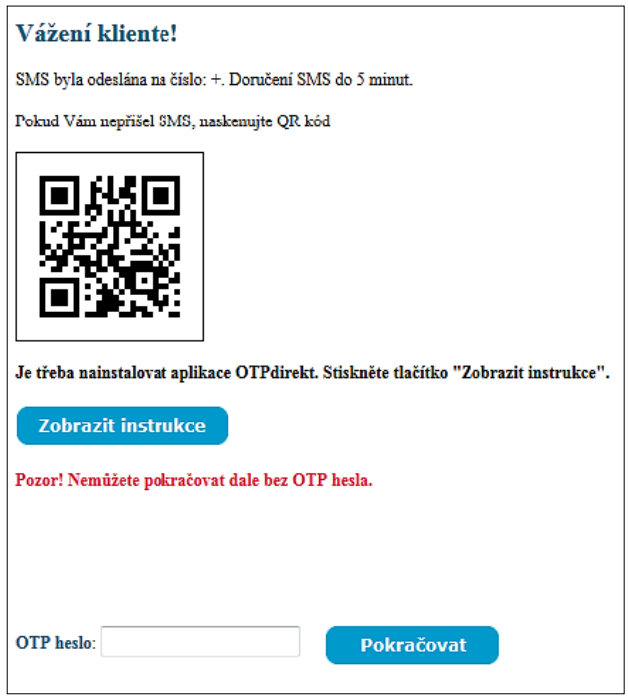
„*Vlastní kradení citlivých dat probíhá vložením škodlivého kódu do oficiálních stránek bank. Konfigurační skripty jsou staženy z C&C serverů (stroje patřící útočníkům, sloužící pro ovládání botnetu) a dešifrovány výše zmíněným způsobem. Zajímavostí je znovupoužití stejného formátu konfiguračních souborů známých bankovních trojanů Carberp a Spyeye. Pro každé botuid (unikátní hodnota, která identifikuje prostředí uživatele) se uloží seznam uživatelských jmen a hesel na C&C serveru. Další skripty jsou stahovány v závislosti na použité bance, buď tedy* ***hXXps://andry-shop.com/gate/get_html.js;hXXps://andry-shop.com/csob/gate/get_html.js;*** resp. ***hXXps://yourfashionstore.net/panel/a5kGcvBqtV****, které se stáhnou, pokud oběť navštíví webové stránky České spořitelny, ČSOB, resp. Fia.*"[486]

485: Blíže viz rozbor funkčnosti malware Tinba: *W32. Tinba (Tinybanker).* [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf
486: HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

Ad 4) **Instalace malware do mobilního zařízení**
Dalším krokem útočníka bylo přesvědčit uživatele o nutnosti zvýšení zabezpečení, při přístupu k online bankovnictví. Důvodem varování, které vydala údajná banka (ve skutečnosti se jednalo o webovou stránku ovládanou útočníkem), bylo „zvýšení" bezpečnosti spojení. Oběti byla nabídnuta stránka s volbou operačního systému mobilního zařízení (OS Android, Windows Phone, Blackberry i iPhone), avšak pouze verze pro Android umožnil stažení malware do telefonu. Útočníci volili různé způsoby distribuce malware do telefonu, od prostého zaslání SMS zprávy s odkazem, ze kterého si uživatel měl daný program stáhnout, po zaslání SMS zprávy a QR kódu.[487]

Vlastní znění zprávy:

**CS-CS24**
**Stáhněte si zabezpečení z Bit.ly/Tp9JjU**




Obrázek 63: Stažení malware do telefonu

487: Tamtéž – obrázek s captcha kódem.

Malware stažený a nainstalovaný do mobilního zařízení byl společností Avast! detekován jako Android: *Perkele-T*.

Tento malware měl za cíl získat přístup a plnou kontrolu nad druhotným autentizačním prostředkem (dvoufaktorová autentizace), kterým je ve většině případů právě mobilní telefon. V případě, že uživatel využíval jiný operační systém než Android, byla mu zobrazena zpráva: „*Zkuste to prosím později.*"

Ad 5) **Převod a odčerpání finančních prostředků**
Dalším krokem útočníka pak již bylo odčerpání finančních prostředků z účtu napadeného na účet bílých koní, kteří měli následně hotovost vybrat či přeposlat na účty jiné. Díky plnému ovládání (pomocí malware) jak přístupových údajů do internetového bankovnictví (viz napadený počítač), tak ovládání druhotného autentizačního prostředku (viz napadený mobilní telefon – kdy autentizační zprávy byly přeposílány útočníkovi bez toho, že by se zobrazily oběti), mohl útočník zadat „legitimní" příkaz k převodu peněz.

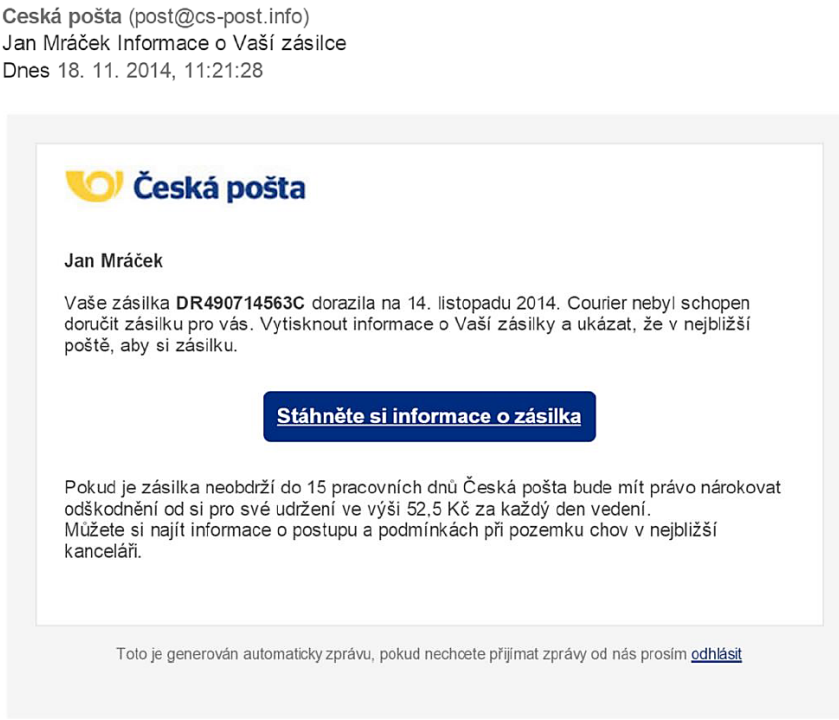
Dle zprávy společnosti Avast! za tímto útokem stáli rusky mluvící útočníci. SMS zprávy z infikovaného telefonu jsou přeposílány na číslo 79023501934, které je registrováno v oblasti Astrachaň, Rusko.[488]

### 4.6.1.2 Česká pošta

Druhý velký phishingový útok začal v listopadu 2014 a pokračoval do prosince 2014. Na počátku útoku byl phishingový e-mail s oznámením „České pošty" o tom, že jste nebyl jakožto adresát zásilky zastižen a že si máte stáhnout informace o zásilce. Čeština použitá v tomto phishingovém e-mailu je jednou z nejhorších, na kterou je možné u phishingu narazit. Ke generování tohoto e-mailu byl zřejmě použit některý z automatických překladačů z Internetu.

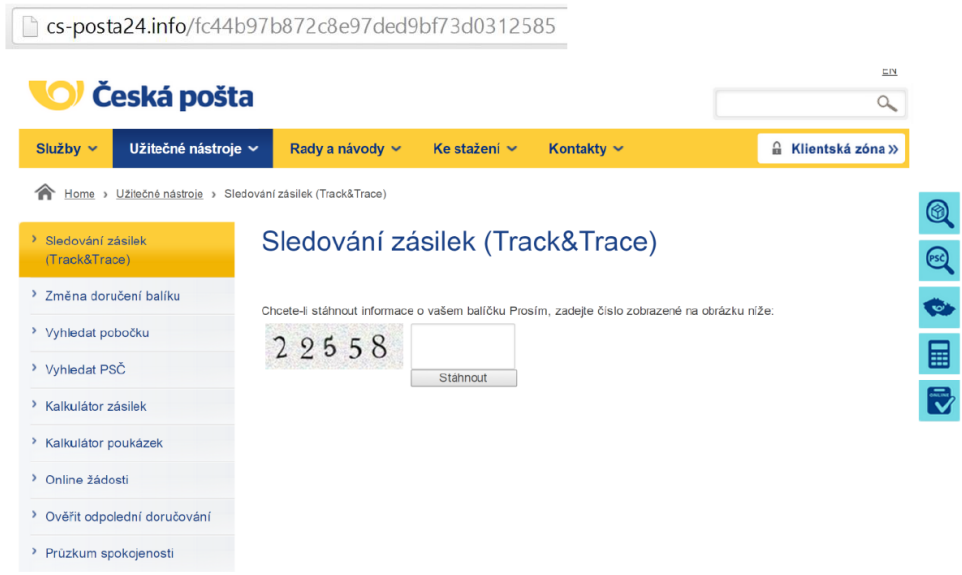
Podvodné e-maily byly rozesílány z adres, které nepatří České poště. Jednalo se například o asdresy: upport@cs-post.net, tracktrace@cs-post.net, cpost@cs-post.net, post@cs-post.net, zasilka@cs-post.net, které díky doméně ***cs-post*** mohly v uživateli vzbudit přesvědčení, že se jedná o stránky České pošty. Je třeba si však uvědomit, že ***cs-post*** byla zaregistrována v doméně ***.net***, kdežto skutečné stránky České pošty jsou zaregistrovány v doméně ***.cz*** (viz https://www.ceskaposta.cz či www.cpost.cz).

488: HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/



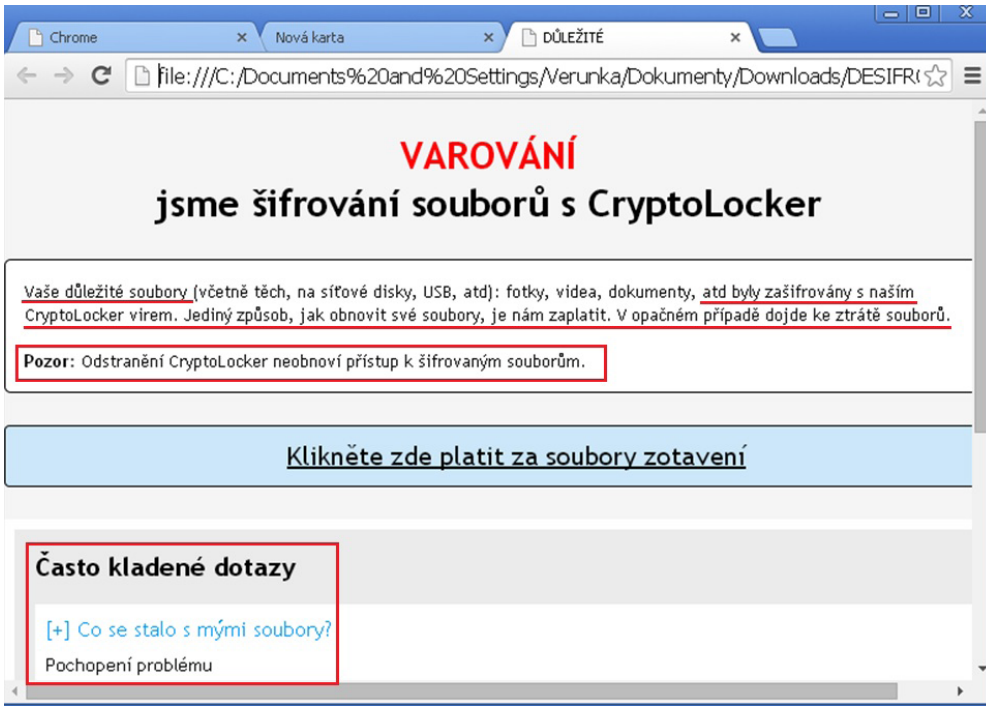

Obrázek 64: Podvodný e-mail od „České pošty"

Pokud uživatel klikl na políčko: *Stáhněte si informace o zásilka*, byl přesměrován na stránky, které svojí vizáží připomínaly skutečné stránky České pošty. Zde byl uživatel vyzván k vepsání bezpečnostního kódu (Captcha) a následně mu bylo umožněno stáhnout soubor .zip, který obsahoval „informace o sledované zásilce". Stejně jako v předchozí phishingové kampani byl v příloze uložen spustitelný soubor (ransomware), jehož cílem však bylo zašifrovat uživatelova data.



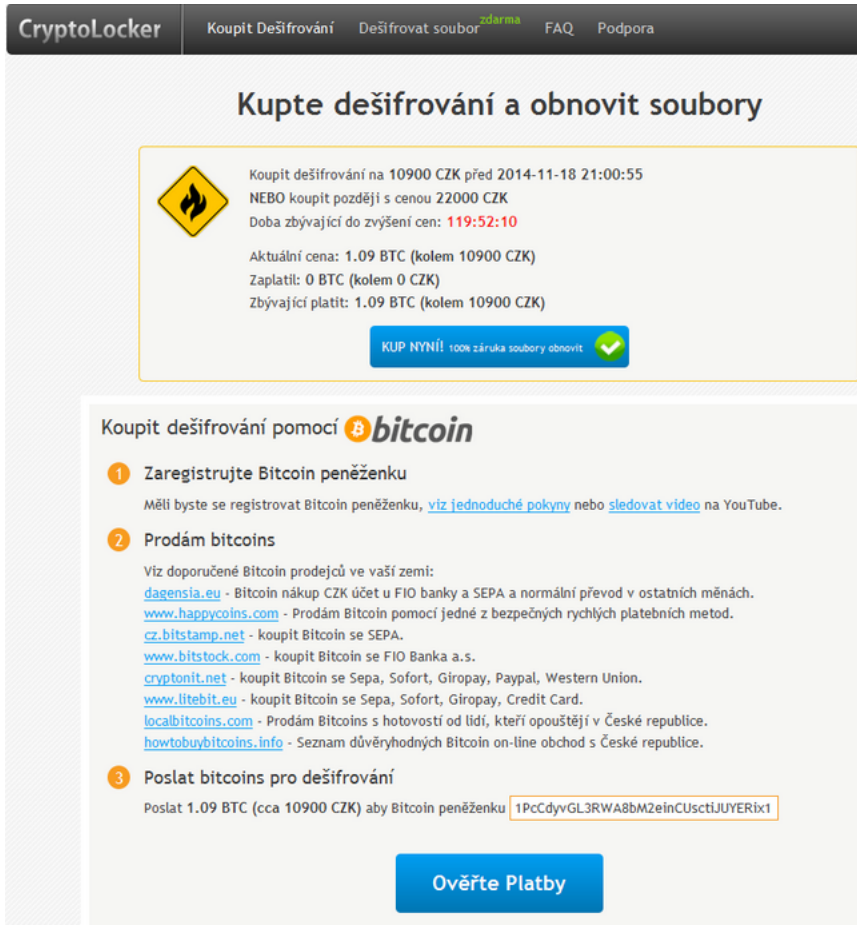

Obrázek 65: Podvodná stránka „České pošty“

Po zašifrování dat byla uživateli zobrazena výzva žádající zaplacení finanční částky za doručení klíče, který je schopen zašifrované soubory odšifrovat. Vlastní výzva již byla psána podstatně lepší verzí češtiny. Uživatel se také mohl dozvědět odpovědi na některé otázky, které ho případně trápily.




Obrázek 66: Informace, která se zobrazila uživateli po zašifrování jeho dat

Obnovení dat v té době stálo 1,09 BTC a uživateli byl kromě přepočtu na české koruny zobrazen i podrobný návod, jak si zřídit bitcoinovou peněženku, kde a jak nakoupit bitcoiny a kam je poslat.




Obrázek 67: Návod na to, jak dešifrovat svoje soubory[489]

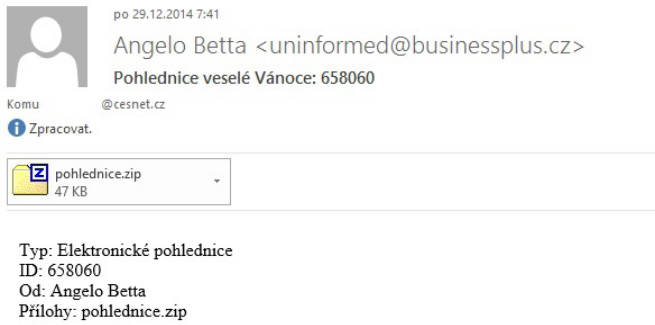
Vlastní útok je specifický tím, že jednak k phishingové kampani připojil ransomware, který rovnou začal zašifrovávat uživatelova data, a jednak tím, že k realizaci vlastního útoku bylo využito předvánoční období, ve kterém řada lidí čeká na doručení zásilek. Díky těmto dvěma faktorům byl vlastní útok velmi úspěšný.

489: *Sledování zásilky České pošty aneb nová havěť.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/

#### 4.6.1.3 Vánoce a dárky

Další velký phishingový útok začal v průběhu prosince 2014 (konkrétně v období Vánoc) a pokračoval v lednu 2015. Tento útok byl rozdělen do dvou fází. V první fázi byly uživatelům zaslány e-mailové zprávy s přáním veselých Vánoc prostřednictvím elektronické pohlednice. V druhé fázi byly v průběhu ledna zasílány zprávy o potvrzení objednávky na elektroniku. Zpráva uživateli sdělila, že si zakoupil zboží (např. tiskárnu, harddisk, fotoaparát atp.), za které zaplatil předem platební kartou, přičemž odkazuje na fakturu v příloze.

Oba dva útoky mají společný prvek, kterým je malware obsažený v příloze e-mailu. Konkrétně se jednalo o trojského koně (*Kryptik*), který byl prezentován jako spořič obrazovky. Tento malware byl stejně jako v případě útoku uvedeného v kap. 4.6.1.1 komprimován v souboru .zip. Po rozbalení souboru .zip nepovažovala řada uživatelů soubor .scr[490] za spustitelný program a infikovala si tak počítač.




490: Soubory s příponou SCR jsou Spustitelné soubory.
*Primárně je jim přiřazen program Unknown Apple II File (found on Golden Orchard Apple II CD Rom). Dále bývají přiřazovány také Windows Screen Saver, Image Pro Plus Ver. 1.x - 4.5.1.x Macro (Media Cybernetics Inc.), TrialDirector Script File (inData Corporation), Screen Dump, Screen Font, Statistica Scrollsheet, Procomm Plus Screen Snapshot File, Movie Master Screenplay, Mastercam Dialog Script File (CNC Software Inc.), Sun Raster Graphic, LocoScript Screen Font File (LocoScript Software), Faxview Fax, DOS DEBUG Input File, Script a FileViewPro.*
*Co znamená přípona souboru SCR*. [online]. [cit. 14. 8. 2016]. Dostupné z:
http://www.solvusoft.com/cs/file-extensions/file-extension-scr/

po 12.01.2015 10:08
Andrea Zázvorková <charge@artix.cz>
Datum objednávky #HDDE6402643655 10.01.15
Komu @polac.cz
charge22B8645.zip
29 KB

Vážená paní, vážený pane,
děkujeme za projevenou důvěru v internetové obchody obchody24.cz.
Tímto emailem potvrzujeme, že jsme v pořádku přijali vaši objednávku.

Číslo objednávky (variabilní symbol): HDDE6402643655 Datum a čas objednávky: 10.01.15 58:54 Kontaktní údaje:
Barbora Bořiková
+420 606 997 389

Vaše objednávka:
---
HP Officejet 4255 Print/Scan/Copy/Fax/Telefon, USB 2.0, bílá: 1 x 6 303,00 Kč =6 303,00 Kč
Doúprava PPL: 128 Kč
---
Celková cena nákupu vč. DPH: 6 431,00 Kč Způsob platby: Platba předem – platební karta
Poznámka: Potvrzení platby a fakturu najdete v přiloženém souboru (charge22B8645.zip)
-
Nyní prosím vyčkejte na našeho operátora, který se s vámi spojí maximálně do 1 pracovního dne a dohodne podrobnosti ohledně Vaší objednávky.

Obrázek 68: Ukázky phishingových zpráv pohlednice a obchod

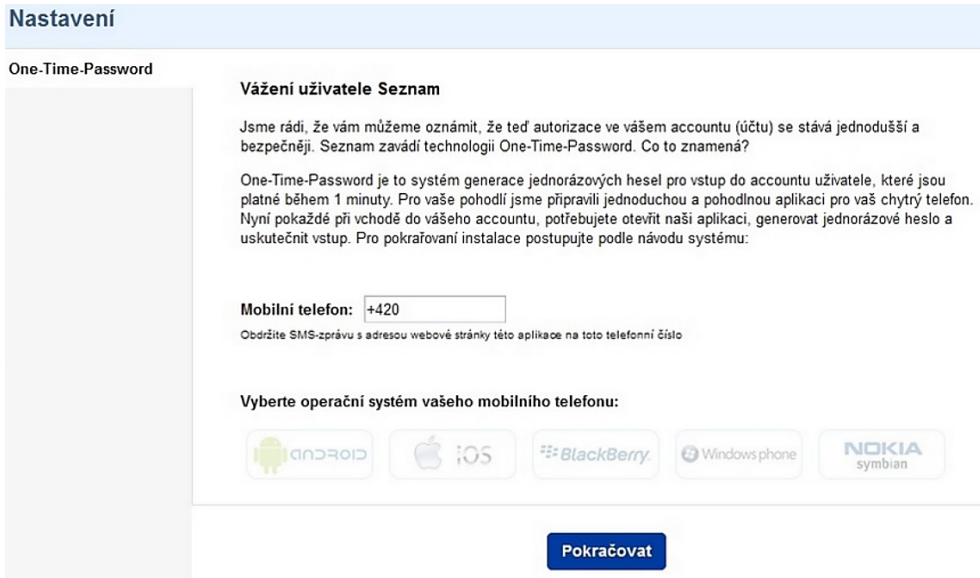
Vlastní útok je specifický tím, že jednak využil typ souboru, který celá řada uživatelů nepovažuje za nebezpečný, a jednak načasováním útoku. Díky různým řetězovým e-mailům si uživatelé zvykli otevírat elektronické pohlednice či přílohy, které tak vypadají, bez důkladnějšího testování obsahu. Druhý útok byl naplánován tak, aby si uživatel prověřil, zda si skutečně neobjednal nějaké zboží, které mu díky vánočním svátkům nebylo doručeno.

#### 4.6.1.4 Seznam.cz – One Time Password

Poslední phishingový útok demonstruje výraznou změnu v taktice útočníků. Útočník stále využívá té skutečnosti, že došlo k infikování počítače malwarem. Útočník může mít nad tímto počítačem sám kontrolu nebo si jej může pronajmout např. v rámci botnetu. K vlastnímu infikování mohlo dojít například pomocí jiného doručeného e-mailu, při návštěvě infikovaných stránek nebo jinak. Cílem útočníka v případě Seznam – One Time Password[491] bylo získat kontrolu nad mobilním telefonem uživatele.

Malware, který byl nainstalován v počítači, vyzval uživatele při přihlášení do e-mailové schránky Seznam.cz, aby si do svého mobilního telefonu nainstalovali prostředek pro jednodušší a bezpečnější práci se svou poštovní schránkou. Uživatel je následně krok za krokem proveden instalací aplikace SeznamOTP z nedůvěryhodného zdroje. Na konci instalace je uživateli poskytnut jeho „unikátní licenční klíč." Ve skutečnosti si však uživatel nainstaloval do svého mobilního telefonu malware.

491: Dále jen **SeznamOTP**




Obrázek 69: Úvodní obrazovka instalace SeznamOTP[492]

**Riziko** tohoto posledního phishingového útoku **spočívá v tom, že „phishingová zpráva" nebyla doručena prostřednictvím e-mailu nebo jiného komunikačního prostředku, ale byla zobrazena uživateli pouze při konkrétní situaci** (v tomto případě po přihlášení se do schránky seznam.cz) **a iniciátorem této zprávy byl malware nacházející se v již infikovaném počítači. Druhým rizikovým faktorem je ta skutečnost, že žádost o nastavení zabezpečení není nijak spojena s bankovním účtem. Uživatel si tedy nemusí uvědomit nebezpečí vyplývající z instalace této aplikace.**

V ČR je možné jednání, které má povahu „klasického phishingu", postihnout dle **§ 209** (Podvod) TZK. Podvod je dokonán obohacením se. Vytvoření repliky webové stránky a získání přihlašovacích jmen a vstupních hesel by pak bylo možné kvalifikovat jako přípravu či pokus trestného činu § 209 TZK. Samotné získání přístupových údajů, včetně čísel účtů, čísel platebních karet a PIN kódů bez jejich dalšího užití pak nebude trestné.

V případě kombinovaných forem phishingových útoků, kdy je užit malware k infikování počítače,

492: Další informace o tomto malware a průběhu celého útoku je možné nalézt např. na: *Podvodníci mění taktiku. Našli novou cestu, jak vybílit lidem účty.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html

je třeba takovéto jednání pachatele postihnout také dle **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem phishingového útoku získat sobě nebo jinému neoprávněný prospěch, je možné uplatnit i ustanovení **§ 230 odst. 3** TZK.

Ve specifických případech by bylo možné využít i ustanovení **§ 234** (Neoprávněné opatření, padělání a pozměnění platebního prostředku) TZK.[493]

### 4.6.2 Pharming

**Pharming**[494] představuje sofistikovanější a nebezpečnější formu phishingu. Jedná se o útok na DNS (Domain Name System) server, na kterém dochází k překladu doménového jména na IP adresu. K útoku dochází v momentě, kdy uživatel zadá na internetovém prohlížeči adresu webového serveru, na kterou chce přistoupit. Nedojde však k propojení na příslušnou IP adresu originálního webového serveru, ale na IP adresu jinou, podvrženou. Webové stránky na falešné adrese zpravidla velmi věrně imitují originální stránky, de facto jsou od nich k nerozeznání. Uživatel následně zadá přihlašovací údaje, které získá útočník. Tento útok je zpravidla realizován při přístupu uživatele na stránky internetového bankovnictví.

*„Falešné webové stránky mohou sloužit k instalaci virů nebo trojských koní do uživatelova počítače nebo se pomocí nich mohou útočníci pokusit získat osobní či finanční údaje, které mohou být následně zneužity ke krádeži identity. Pharming je zvlášť nebezpečná forma kyberkriminality, protože v případě nakaženého serveru DNS se může uživatel stát obětí i v případě, že v jeho počítači není nainstalován vůbec žádný malware. Dokonce ani pokud používáte preventivní opatření, například zadáváte internetové adresy ručně nebo používáte výhradně důvěryhodné záložky, nejste před útokem tohoto druhu chráněni, protože k nechtěnému přesměrování dochází až poté, co počítač odešle žádost o spojení.“*[495]

Druhým typickým způsobem pharmingu je napadení počítače koncového uživatele pomocí malware, kde se dá předpokládat menší míra zabezpečení. Tento malware změní soubor hostitelů s cílem odklonit přenos od zamýšleného cíle a přesměrovat uživatele na falešnou webovou stránku.

Trestněprávní postih je obdobný jako v případě phishingu (viz kap. 4.6.1).

493: Blíže viz kap. 5.2.2.2.1 Padělání související s počítači (čl. 7).

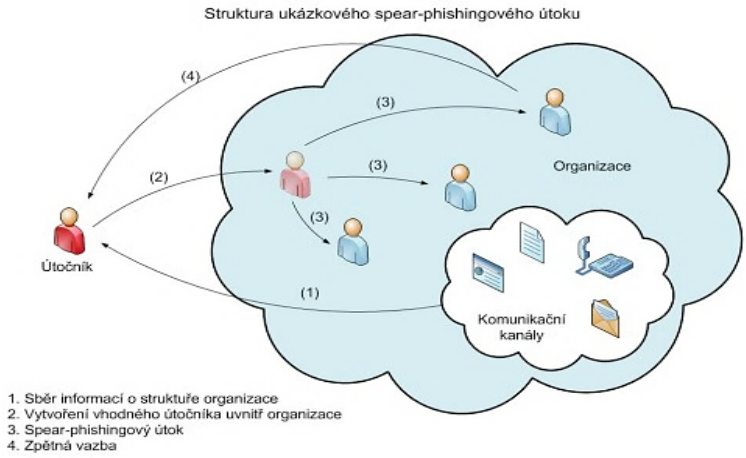
494: Jedná se o kombinaci slov **farming** (farmaření/hospodaření) a **phreaking**.

495: Blíže viz *Co je pharming?* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/pharming

### 4.6.3 Spear Phishing

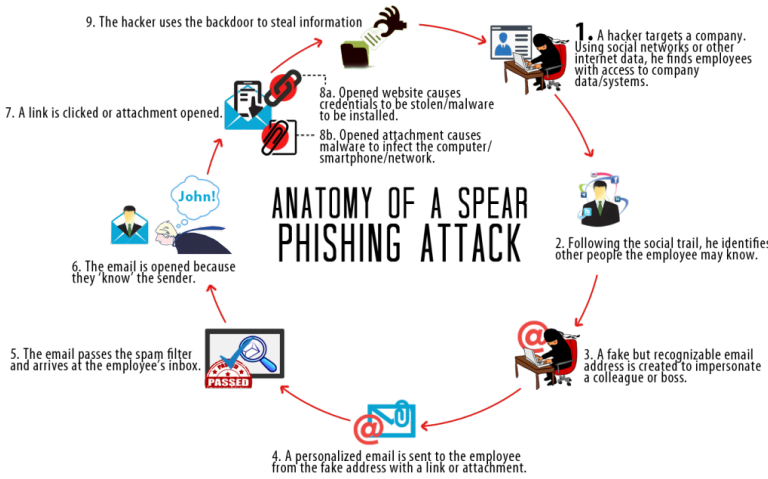
Spear phishing je jednou z forem phishingového útoku, avšak s tím rozdílem, že spear phishing je přesně cílený útok, na rozdíl od phishingu, který je útokem spíše plošným (nahodilým). Cílem útoku bývá konkrétní skupina, organizace nebo jednotlivec, konkrétně informace a data, která se v této organizaci nacházejí (např. duševního vlastnictví, osobní a finanční údaje, obchodní strategie, utajované informace aj.).

U spear phishingu oproti klasickému phishingu je rozdíl v tom, kdo je odesílatelem předmětných zpráv. V počátku útoku je to vlastní útočník, který využije otevřené zdroje, aby zjistil co nejvíce informací o napadané organizaci, její struktuře atd. Dále vytvoří velmi kvalitní e-mail či jinou zprávu a začne komunikovat s osobou zevnitř organizace jako s kolegou. Tuto osobu pak útočník využije jako prostředek pro šíření dalších zpráv (např. infikovaných malware) v rámci organizace. Jelikož se jedná o osobu obětem „známou", nemají problém s ní komunikovat a méně, pokud vůbec, prověřují její zprávy.[496]




Obrázek 70: Struktura Spear-Phishignového útoku[497]

496: „*Útočník si vyhlédne organizaci pracující s cennými informacemi, analýzou webových stránek získá informace o personální struktuře, zaměstnancích a procedurách (pro získání podrobnějších informací o zaměstnancích může využít jejich soukromé stránky a diskusní fóra) a v dalším kroku útočník vytvoří zprávu, jejíž obsah, forma a vzhled napodobuje vnitřní komunikaci v organizaci. Ve zprávě požádá zaměstnance o zadání citlivých informací pro přístup do počítačové sítě.*"
*Evoluční teorie v podání spear phishingu.* [online]. [cit. 15. 2. 2010]. Dostupné z:
http://connect.zive.cz/content/evolucni-teorie-v-podani-spear-phishingu
497: Tamtéž




Obrázek 71: Průběh spear phishingového útoku[498]

Postih spear phishera je obdobný jako v případě phishingu (viz kap. 4.6.1). Za útokem typu spear phishing může být například i teroristická organizace. V tomto případě pak není vyloučena odpovědnost pro trestný čin dle **§ 311** (Teroristický útok) TZK.

### 4.6.4 Vishing

Pojem vishing[499] označuje telefonický phishing, při kterém útočník využívá technik sociálního inženýrství a snaží se od uživatele vylákat citlivé informace (např. čísla účtů, přihlašovací údaje – jméno a heslo, čísla platebních karet, aj). Útočník se záměrně snaží zfalšovat svoji identitu. Útočníci se často představují jako zástupci skutečných bank či jiných institucí, aby u uživatele vyvolali co nejmenší podezření. Vishing se používá ve VoIP (Voice over Internet Protocol) telefonii.

498: *Tip of the month July 2016 – Avoid getting hooked by Phishing*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/

499: Jedná se o kombinaci slov voice (hlas) a phishing.

### 4.6.5 Smishing

Smishing[500] funguje na podobném principu jako vishing či phishing, ale k distribuci zpráv využívá SMS zprávy. V rámci smishingu jde primárně o snahu donutit uživatele zaplatit částku (například zavolat na placenou linku, poslat dárcovskou SMS aj.) nebo kliknout na podezřelé URL odkazy. Pokud uživatel uvedené URL navštíví, je přesměrován na stránku, která zneužívá určité zranitelnosti počítačového systému, případně je uživatel vyzván k zadání citlivých údajů či k instalaci malware.[501]

Příklad smishingu:

„Upozorneni – toto je automaticky vygenerovana zprava z (název lokální banky), Vase kreditni karta byla zablokovana. K reaktivaci volejte 866### ###“

Trestněprávní postih vishingu i smishingu je obdobný jako v případě phishingu (viz kap. 4.6.1).

## 4.7 Podvodné webové stránky (firmy)

Na Internetu se lze setkat s celou řadou aktivit, respektive webových stránek[502] prezentujících úžasné výhry či nabízejících různé zboží za velmi výhodné ceny. Útočníci využívají sociálního inženýrství a spoléhají primárně na důvěřivost a neopatrnost lidí. Vlastní činnost útočníka pak může mít typicky dvojí podobu.

V prvním případě se útočník snaží vylákat citlivé údaje (např. jméno, příjmení, doručovací adresa, e-mail, telefonní číslo a heslo) typicky za účelem registrace, doručení zboží, výhry aj. Všechny tyto údaje zadává uživatel sám a dobrovolně. Útočník se tak dostává k údajům, které může, stejně jako v případě phishingu, využít k celé řadě aktivit. Například na základě zadaného hesla a dalších údajů o uživateli se útočník může pokusit získat přístup k dalším službám, které uživatel používá.[503]

500: Jedná se o kombinaci slov SMS a phishing.

501: Např. **Xshqi** - *Android Worm on Chinese Valentine's day*. [online]. [cit. 14. 8. 2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/

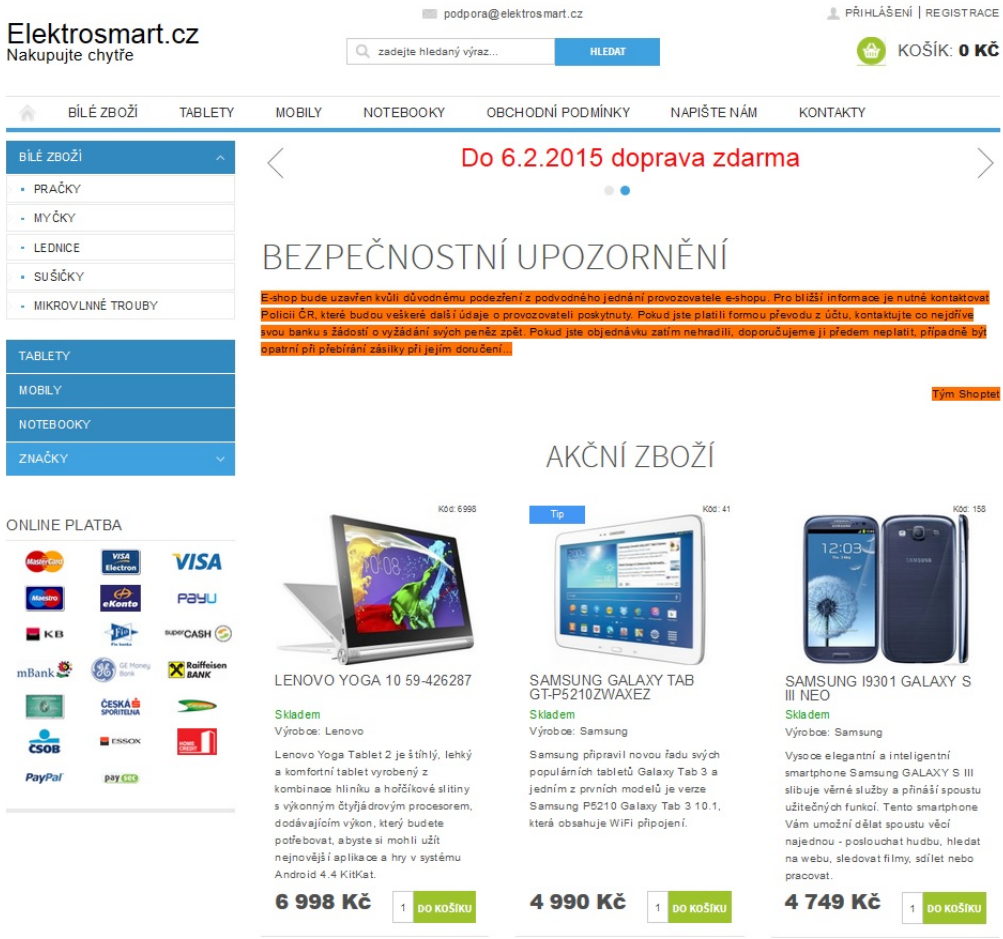
**Selfmite** - *Android SMS worm Selfmite returns, more aggressive than ever*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

502: Nejběžněji se jedná o webové stránky, inzertní portály, ale může se jednat i o účty na sociálních sítích aj.

503: Velmi často dochází k zadávání stejného, nebo obdobného hesla ze strany uživatelů v rámci různých služeb online. Díky tomu může útočník využít např. techniku slovníkového útoku k prolomení přístupových údajů k dalším službám. Tímto jednáním se útočník může dopustit i dalších protiprávních jednání (např. viz kap. 4.15 Identity theft, 4.8 Hacking aj.). Blíže viz např. *Slovníkový útok.* [online]. [cit. 30. 8. 2016]. Dostupné z: https://managementmania.com/cs/slovnikovy-utok

V druhém, mnohem častějším případě se pak jedná o aktivity, které spočívají v podvodném vylákání finančních prostředků z uživatele. Běžně jsou na Internetu nabízeny za velmi výhodnou cenu automobily, motocykly (viz kap. 4.5.3 Podvodné nabídky), traktory, další zemědělská technika a především elektronika jakéhokoliv druhu.

Jako příklad podvodných stránek nabízejících elektroniku za výhodné ceny je možné uvést obchod www.elektrosmart.cz, který byl relativně rychle po svém spuštění zablokován. Na stránkách bylo možné nalézt elektroniku za ceny nižší (avšak nijak přemrštěně) než bylo obvyklé.




Obrázek 72: Nabídka elektrosmart.cz s upozorněním na podvodné jednání

V souvislosti s podvodnými nabídkami na Internetu vydalo Evropské spotřebitelské centrum[504] doporučení pro uživatele, které by jim mělo umožnit poznat podvodná jednání:

- ***Zadejte údaje o společnosti (např. název společnosti, adresu webu, e-mail) do internetového vyhledávače.***

- ***Zamyslete se nad tím, jak se obchodník prezentuje.*** *Je vzhled webu, na kterém se chystáte nakoupit, profesionální? Důvěryhodný dojem rozhodně nebudí e-mailové adresy na bezplatných a anonymních serverech typu yahoo.com, hotmail.com, gmail.com, live.com, seznam.cz apod. Stejně tak, je-li web umístěn na bezplatném hostingovém serveru, není to znak profesionality.*

- ***Platbu předem provádějte jen tehdy, jde-li o skutečně důvěryhodného obchodníka.*** *Jistě nedáte peníze na ulici neznámému člověku s příslibem, že Vám v budoucnu dodá věc. Na internetu tak však řada uživatelů činí. Platbu předem provádějte jen tehdy, pokud jste si jisti, že jednáte s důvěryhodným dodavatelem. Především údaje o platební kartě je třeba chránit.*

- ***Zvlášť podezřelý je požadavek na platbu systémem Western Union.*** *U bankovních převodů nikdy nezasílejte peníze na účty soukromých osob, pokud se nejedná o účet prodávající firmy/společnosti.*

- ***Mezi obvyklé znaky podvodu patří špatná jazyková úprava, požadavek platby předem v hotovosti či převodem, další požadavky na platby pod smyšlenou záminkou*** *(clo, pojištění, přibalení většího počtu kusů výrobku)* ***a tak podobně. Pamatujte si, že pokud se nabídka zdá příliš výhodná, než aby byla skutečná, tak nejspíš skutečná není!***

- ***Nahlédněte do obchodního rejstříku dané země****, zda je v něm společnost registrována. (Stává se také, že někdo zneužije jméno existující společnosti a založí web s podobným označením.*

- ***Zkontrolujte doménu webové stránky.*** *Stává se, že webová adresa je stejná jako adresa skutečně existující a registrované firmy. Je zde ovšem jeden rozdíl – doména, tedy koncovka internetové adresy, je jiná (např. nikoli „.co.uk" pro Velkou Británii, ale třeba „.co.cc" pro Kokosové ostrovy).*

- ***Najděte si sídlo společnosti na internetovém serveru nabízejícím pouliční fotografie měst****, a to podle adresy, uváděné u inzerátů a na webové stránce společnosti.*

- ***Važte si svých osobních údajů.*** *Nesdělujte informace o sobě na nedůvěryhodných či Vám dosud neznámých stránkách. Uvádějte jen takové údaje, které jsou skutečně nezbytné.*

- ***Nereagujte na nevyžádanou poštu (spam).*** *Na nevyžádanou poštu nereagujte, v žádném případě nesdělujte e-mailem údaje o bankovním účtu, číslo platební karty nebo třeba přihlašovací údaje do internetového bankovnictví. Nevyžádaný e-mail smažte, nikdy neotvírejte neznámé přílohy.*[505]

504: Blíže viz http://www.evropskyspotrebitel.cz/

505: Blíže viz *ESC radí, jak poznat podvody na internetu.* [online]. [cit. 30. 8. 2016]. Dostupné z: http://www.evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu-27250

Všechny výše uvedené znaky je třeba pokládat za pouhé indicie, které mohou vést k odhalení podvodu. Útočník může své jednání modifikovat na základě úspěšnosti vlastního útoku. Mimo uvedených rad je vhodné využít i varování zveřejňované na dalších stránkách, například www.podvodnefirmy.cz aj.

V ČR je možné výše popsané jednání jednání postihnout dle **§ 209** (Podvod) TZK. Podvod je dokonán obohacením se. Vytvoření repliky webové stránky a získání přihlašovacích jmen a vstupních hesel by pak bylo možné kvalifikovat jako přípravu či pokus trestného činu § 209 TZK. Pokud by se útočník pokusil (§ 21 TZK) na základě získaných přístupových údajů o neoprávněný přístup do jiného účtu uživatele, mohlo by být takovéto jednání kvalifikováno i jako **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK.

## 4.8 Hacking

*„Hackerem se člověk nestane, narodí se jím."*
Mentor

Pojem hacking je v současné době veřejností vnímán pejorativně jako jakákoliv činnost osoby směřující k získání nelegálního přístupu k cizímu systému či osobnímu počítači.[506] Zejména ve sdělovacích prostředcích bývají tímto pojmem všeobecně nazýváni všichni útočníci, jejichž jednání směřuje proti informačním technologiím či jejichž činnost je na využívání těchto technologií založena.[507] V tomto kontextu je však zásadní rozdíl mezi vnímáním obsahu pojmu hacking z pohledu veřejnosti, a z pohledu osob, které se samy za hackery označují nebo jsou za ně označovány vlastní komunitou.

506: Blíže srov. např. GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal*, 2000, roč. 73, č. 1, s. 18–24.
YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, roč. 44, č. 4, s. 387–399.
507: Srov. např. články v denním tisku:
*Největší hackerský útok potvrzen. V ohrožení jsou stovky miliónů uživatelů.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html
*Hackeři se vydávají za Anonymous a hrozí útokem českým firmám.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/
*Yahoo řeší, jestli má hacker opravdu údaje o 200 milionech účtů.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/
*Hackeři zaútočili na uživatele Facebooku.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla
*Hackeři ukradli Američanům data o novém typu bojových stíhaček.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://digiweb.ihned.cz/c1-36816420-hackeri-ukradli-americanum-data-o-novem-typu-bojovych-stihacek
*Hackeři vám už brzy ukradnou data přímo z klávesnice.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://digiweb.ihned.cz/c1-29295240-hackeri-vam-brzy-ukradnou-data-primo-z-klavesnice

Pojem **„hacker“**[508] a **„hacking“** pochází z USA, vznikl v 50. letech 20. století a **označoval technicky nadanou osobu** (a její činnost) **schopnou nalézat nová, mnohdy neortodoxní řešení problému**.

Pro pochopení, jak vnímají společnost a její pravidla útočníci, jež jsme si zvykli označovat jako hackery, je vhodné poznat jejich názor. V roce 1984 Levy definoval následující principy hackerské etiky:

1) Přístup k počítačům a čemukoliv dalšímu, co tě může naučit něco o tom, jak svět funguje, by měl být neomezený a absolutní. Vždy respektuj pravidlo osobní zkušenosti.

2) Veškeré informace by měly být bezplatné.

3) Nevěř autoritám, podporuj decentralizaci.

4) Hackeři by měli být souzeni podle svých činů a nikoliv podle scestných kritérií jako jsou věk, rasa či postavení.

5) Na počítači můžeš vytvářet „krásu“.

6) Počítače mohou změnit tvůj život k lepšímu.[509]

Byť tato pravidla nejsou vždy respektována či uznávána, představují základní rámce vnímání virtuálního světa útočníky, jež označujeme za hackery.

Dalším významným vhledem do vnímání světa očima hackera je dokument Hackerův manifest:

508: Tento pojem lze přeložit mnoha způsoby a je třeba vycházet z kontextu. V americkém žargonu to původně znamenalo bezcílně se projíždět na koni. Hack také označoval jednoduché řešení problému. Následně znamenalo spáchání nějaké nepravosti studenty univerzity.

509: LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly edia, s. 32-41. ISBN 978-1449388393. Dostupné i online: https://e11c1b148f6c7c56754c9184e0d1c52ac4d888f9-www.googledrive.com/host/0ByAMXZl2-PZ0WjBPYmhaWVVRN0E

*Následující text byl napsán krátce po mém zatčení...*

***Svědomí hackera***
*Dneska chytli dalšího. Jsou toho plný noviny. „Mladík odsouzen za Skandální Počítačový Zločin", „Hacker zatčen za průnik do banky"...*

*Zasraný děti. Všechny jsou stejný.*

*Ale zkusili jste se někdy s tou svou trojitou psychologií a technomozkem padesátejch let podívat očima hackera? Položili jste si někdy otázku, jaká síla ho zformovala, co vytvářelo jeho osobnost?*

*Jsem Hacker. Vstup do mého světa...*

*Můj život začíná školou... Jsem chytřejší něž většina ostatních děcek, ty kecy, co nám vykládají, mě nudí...*

*Zasranej flákač. Všichni jsou stejný.*

*Jsem na gymplu nebo na střední. Učitelka už popatnáctý vysvětluje, jak se krátí zlomek. Chápu to. „Ne, slečno Smithová, nepsal jsem postup. Udělal jsem to z hlavy..."*

*Zasraný děcko. Nejspíš to někde opsal. Všichni jsou stejný.*

*Dneska jsem udělal objev. Objevil jsem počítač. Počkej chvíli, to je skvělý. Dělá to, co chci. A když to udělá chybu, tak je to kvůli tomu, že jsem něco zvoral. A ne jenom proto, že mě nemá rád...*

*...nebo se cítí být mnou ohrožený...*

*...nebo si myslí, že jsem vychcanej parchant...*

*...nebo že nemám rád učení a neměl bych tu bejt...*

*Zasraný děcko. Furt jenom hraje samý hry. Všechny jsou stejný.*

*A pak se to stalo... otevřely se dveře do světa... elektronický signál se řítí telefonní linkou jako heroin žilou narkomana, nachází úkryt před ubíjející každodenností... nachází board.*

*„To je to místo... sem patřím..."*

*Každýho tu znám. I když jsem je v životě neviděl, nikdy jsem s nima nemluvil, a možná že už o nich nikdy neuslyším... Znám vás všechny...*

*Zatracený děti. Furt jenom obsazujou linku. Všechny jsou stejný...*

*Vsaď prdel, že jsme všichni stejný!*

*Ve škole jste nás krmili po lžičkách dětským jídlem a my chtěli steak... kusy masa, který k nám proklouzly, byly předžvýkaný a bez chuti. Ovládali nás sadisti a ignorovali tupci. Bylo pár těch, co nás mělo učit a našlo v nás ochotné žáky, ale těch bylo jako kapek vody v poušti.*

***'Toto je teď náš svět...** Svět elektronů a spínačů, krása baudu. **Využíváme existujících služeb bez placení, mohly by být skoro zadarmo, kdyby nepatřily šmelinářským hltounům, a vy nás nazýváte zločinci. My objevujeme... a vy nás nazýváte zločinci. Dychtíme po vědomostech... a vy nás nazýváte zločinci. Existujeme bez barvy pleti, bez národnosti, bez náboženských předsudků a vy nás nazýváte zločinci. Vy stavíte atomové bomby, vy vedete války, vy vraždíte, podvádíte a lžete nám a chcete, abysme věřili tomu, že je to pro naše vlastní dobro, přesto jsme my zločinci.***

***Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho, co říkají a co si myslí, a ne podle toho, jak vypadají. Můj zločin je to, že jsem chytřejší než ty, což je věc, kterou mi nikdy neodpustíš. Jsem Hacker a toto je můj manifest. Můžete zastavit jednotlivce, ale nemůžete nás zastavit všechny... konec konců, všichni jsme stejní.***

**Mentor**
**Hackerův manifest**[510]
**8. ledna 1986**

V současné době sami hackeři užívají označení hacker pro osoby, které mají vynikající znalosti fungování informačních a komunikačních systémů, počítačových systémů, jejich operačních systémů a dalších programů, jejich síťových principů a mechanismů, přičemž jsou zároveň i vynikajícími programátory schopnými tvořit vlastní software, a to ve velmi krátkém čase. Právě snaha o poznání, jakým způsobem informační technologie, aplikace či technický prostředek fungují, a zpřístupnění těchto informací i ostatním uživatelům, je hnacím motorem i filozofií řady osob. Schopnost hackera získávat si díky vlastním navrženým a napsaným počítačovým programům přístup do počítačových systémů i mimo běžné způsoby přístupu (což ovšem nutně neznamená, že zisk takového přístupu musí být motivován snahou způsobit uživateli škodu, jinou újmu nebo se na proniknutí do systému jinak obohatit), je jednou, nikoliv jedinou dovedností.

510: Český překlad převzat z: *1986 – Hackerův manifest.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://blisty.cz/art/14662.html Originální znění je možné nalézt Phrack.org. [online]. [cit. 16. 8. 2015]. Dostupné z: http://phrack.org/issues/7/3.html

### Rozdělení hackerů

Právě motivace získání nestandardního (nikoliv nutně nelegálního) přístupu, způsob provedení takového průniku, jejich motivace a případné nakládání se získanými daty jsou klíčovými faktorem pro rozlišení těchto osob do následujících tří základních skupin:[511]

**White Hats** – jsou hackeři, kteří uskutečňují své průniky do systému za využití bezpečnostních slabin systému právě za účelem odhalení těchto bezpečnostních mezer a vytvoření takových mechanismů a bariér, které by tyto útoky měly znemožňovat. Jsou často zaměstnanci či externími spolupracovníky renomovaných společností podnikajících v oblasti informačních technologií.[512] Svým průnikem do systému nezpůsobují uživatelům škodu či jinou újmu, naopak v mnoha případech upozorňují správce takto napadeného systému na bezpečnostní chyby.[513] Jejich činnost je zásadně nedestruktivního charakteru.

**Black Hats** – v podstatě opak hackerů řazených mezi White Hats. Jejich motivací je snaha způsobit uživateli napadeného systému škodu či jinou újmu, resp. získat majetkový nebo jiný prospěch. Mimo vlastní realizaci prolomení napadeného systému je v jejich jednání patrný ještě další, kriminální prvek.

**Gray Hats** – jde o šedou zónu hackerů, tedy o osoby, které se nevyprofilovaly směrem k uvedeným dvěma skupinám. Občas z jejich strany může dojít k porušení práva jiného nebo morálních principů, avšak jejich činnost není primárně hnána snahou o způsobení škody, jako tomu je u Black Hats.

Kromě výše uvedeného, tj. nejběžněji používaného dělení, je možné hackery dělit do dalších skupin na základě jejich motivu. Jedná se o: Script Kiddies, Hactivists, státem sponzorované hackery, Spy hackers, kyber teroristy, začátečníky (n00b), Blue Hat hackers aj.[514]

Klíčovým faktorem pro posouzení hackingu jakožto možné bezpečnostní hrozby je stanovení důvodu aktivit hackera (viz rozdělení hackerů). V některých případech pak hacking může představovat reálnou bezpečnostní hrozbu, neboť se jedná o narušení bezpečnosti počítačového systému, případně prolomení ochrany či využití slabin systému. Naopak v jiných případech může být vhodným doplňkem sloužícím ke zvýšení bezpečnosti systému jako celku či nalezení slabých míst a zranitelností.

511: Označení těchto skupin, jakkoliv bizardní, je v informačních sférách reálně užíváno a nebývá překládáno do českého jazyka.

512: Blíže srov. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 231.

513: Blíže srov. MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 54.

514: Blíže viz např. SHNEIER, Bruce. *The Seven Types of Hackers.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

*7 Types of Hacker Motivations.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

*7 Types of Hackers You Should Know.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://www.cybrary.it/0p3n/types-of-hackers/

V obecné rovině je možné skutečně za hacking označit jakýkoliv neoprávněný průnik do počítačového systému z vnějšku, nejčastěji v rámci sítě Internet. Avšak ne každý hackerský útok musí být nutně označován za delikt.

Nebezpečí hackerských aktivit spočívá mimo jiné i v tom, že vedle vlastního získání neoprávněného přístupu do napadeného systému (bez ohledu na motivaci hackera) tyto osoby k realizaci těchto útoků vytvářejí a užívají vysoce efektivní softwarové prostředky, jejichž zdrojové kódy jsou hackery samotnými často následně zveřejněny např. v rámci Darknetích tržišť. To může vést k dalšímu hromadnému zneužívání těchto programů uživateli, kteří sami neovládají programování na takové úrovni, aby tyto programy vytvořili, avšak díky existenci takto zpřístupněných nástrojů mohou potenciálně způsobovat uživatelům napadených systémů poměrně značné škody. Prostřednictvím Internetu je tak možné si obstarat často celé sady hackerských softwarových programů obsahující základní software a informace nutné k jeho použití, de facto bez hlubších znalostí fungování těchto programů.

### Formy hackingu

Vlastní činnost hackerů spočívá v celé řadě jednání. Mezi typické aktivity používané hackery patří:

1) Sociální inženýrství
2) Prolamování hesel[515]
3) Skenování portů[516]
4) Využívání malware k infiltraci počítačového systému
5) Phishing
6) Cros Site Script[517]
7) Odposlech komunikace[518]

---

515: Jde o proces získávání hesla k počítačovému systému. Běžně se k prolamování hesel používá:

- Hádání hesla hrubou silou (testování hesla. Prevencí je dostatečně silné heslo);
- Hádání hesla na základě určitých znalostí o uživateli (získaných například na sociálních sítích aj.);
- Využití slovníku běžně používaných hesel (slovníkový útok);
- Vyžádání hesla od administrátora systému vydáváním se za oprávněného uživatele (Útočník předstírá zapomenuté heslo a pokusí se jej obnovit.)
- Odchytávání hesel z nešifrované nebo nedostatečně šifrované síťové komunikace mezi počítačovým systémem a uživatelem
- Hledání hesel v souborech dat uložených systémem

516: Jde o metodu, při níž jsou zjišťovány otevřené síťové porty na počítačovém systému, který je připojen k počítačové síti. Na základě tohoto zjištění je možné určit, jaké služby jsou na počítačovém systému spuštěny (např. webový server, ftp server aj.) Vlastní útok je pak zaměřen na zjištěné spuštěné služby na základě jejich zranitelností.

517: Jedná se o útok spočívající v narušení webových stránek. Při tomto způsobu útoku je využito aktivních prvků (skriptů) na webové stránce, do kterých je vložen zákeřný kód a následně je nabídnut oběti.

Jedno z méně častých, avšak o to nebezpečnějších jednání spočívá ve zneužití zranitelnosti webové aplikace pro spuštění malware v rámci prohlížeče oběti. Oběť pak není schopna takové jednání odhalit. Závadný kód je spuštěn stejně jako zbytek stránky a útočníkovi je umožněno převzít oprávnění prohlížeče v rámci systému.

Blíže viz např. *OWASP, XSS* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

518: Viz kap. 4.11 Sniffing.

### Známé hackerské skupiny a hackeři


Asi nejznámější současnou hackerskou skupinou je Anonymous, avšak existují či existovaly další skupiny:[519]

- Lizard Squad
- The Level Seven Screw
- Chaos Computer Club
- Lulzsec
- Syrian Electronic Army
- Globalhell
- Network Crack Program Hacker Group
- Antisec Movement
- Legion of Doom (1984–2000)
- Masters of Deception (1989–1993)
- Milw0rm aj.

Mezi **nejznámější hackery** patří Johnatan James, Vladimir Levin, Gary McKinnon, John McAfee, Astra, Stephen Wozniak, James Kosta, Kevin Mitnick, Adrian Lamo, David L. Smith.[520]

Není pochyb o tom, že **ne každá aktivita hackerů je legální**. Ve vztahu k zásahu do počítačového systému jistě dojde k porušení ústavně zaručených základních lidských práv a svobod. Zejména se bude jednat o **článek 7 odst. 1**[521] a **článek 13 Listiny**.[522]

Jak bylo uvedeno výše, existuje celá řada jednání či útoků, které je možné podřadit pod pojem hacking (prolomením hesla počínaje a konče komplikovaným phishingovým útokem, který je kombinován se sociálním inženýrstvím a užitím malware).

Jednání hackera, spočívající pouze ve využití svých schopností, díky nimž překoná bezpečnostní opatření a získá přístup k počítačovému systému nebo jeho části, je možné postihnout dle **§ 230 odst. 1** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK.

519: Blíže viz např. *10 Most Notorious Hacking Groups*. [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/
Obrázek převzat z [online]. [cit. 15. 7. 2016]. Dostupné z: http://img02.deviantart.net/a2fd/i/2012/330/7/5/we_are_anonymous_by_mrj_5412-d5mb6xc.jpg
520: Blíže viz např. *10 Most notorious hackers od all time.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://hacked.com/hackers/
*Nejznámější počítačoví hackeři a jejich útoky.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.stream.cz/top-5/10004402-nejznamejsi-pocitacovi-hackeri-a-jejich-utoky
521: „**Nedotknutelnost** osoby a jejího **soukromí je zaručena**. Omezena může být jen v případech stanovených zákonem."
522: „**Nikdo nesmí porušit** listovní tajemství ani **tajemství** jiných písemností a **záznamů**, **ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem**, s výjimkou případů a způsobem, které stanoví zákon. **Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.**"

V případě kombinovaných forem útoků, kdy je například užit malware k infikování počítače, je třeba takovéto jednání pachatele postihnout také dle **§ 230 odst. 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem útoku získat sobě nebo jinému neoprávněný prospěch, nebo neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat, je možné uplatnit i ustanovení **§ 230 odst. 3** TZK.

## 4.9 Cracking

Pojem **cracking** je s pojmem hacking spojován, někdy jsou dokonce tyto pojmy veřejností či ve sdělovacích prostředcích nesprávně zaměňovány. Pojem lze do českého jazyka přeložit jako louskání či pukání. Obsahově pojem cracking znamená prolamování nebo obcházení ochranných prvků počítačového systému, programů nebo aplikací, s cílem jejich následného neoprávněného užití.

Za crackery bývají označováni hackeři z kategorie Black Hats, tedy ti, kteří uskutečňují průlomy do systémů ve snaze způsobit uživateli škodu, získat informace, popřípadě sebe nebo jiného obohatit.[523] Dále je cracking spojen zejména s porušováním autorských práv a práv souvisejících s právem autorským. Za cracking je v tomto smyslu označováno jednání spočívající v obcházení ochranných prvků, které brání vytváření kopií či nelegálnímu užívání počítačových programů a hudebních nebo filmových produktů (filmová či hudební CD, DVD apod.).[524] Tyto bezpečnostní prvky jsou využívány jako prostředky ochrany autorských práv ve smyslu § 43 odst. 1 AZ, ve znění pozdějších předpisů.

Jednou z forem cracingu je i **„password cracking"** sloužící ke zjišťování přístupového hesla do počítačového systému, licencovaného systému či programu. Pokud jde o porušování autorského práva, pak cracker zpravidla vytvoří keygen či crack,[525] který umožní následné užití programu. Takto upravené programy jsou pak zpravidla sdíleny na warez fórech či P2P sítích.

Jednání pachatele, v rámci kterého dochází k prolamování ochrany počítačového systému či programu, s úmyslem zisku informací a jejich následném neoprávněném užití naplňuje skutkovou podstatu trestného činu dle **§ 230 odst. 1 či 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Pokud je cílem crackingu získat sobě nebo jinému neoprávněný prospěch je možné uplatnit i ustanovení **§ 230 odst. 3** TZK.

Vyloučena není ani trestněprávní odpovědnost dle **§ 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK. Při distribuci chráněného autorského díla pak dochází k naplnění **§ 270** (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi) TZK.

523: Srov. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 231.

524: Blíže srov. MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 73.

525: **Keygen** – Key Generator. Program generující sériová čísla, případně další údaje. **Crack** – program sloužící k odstranění, či omezení funkčnosti ochranných prvků jiného programu.

## 4.10 Internetové (počítačové) pirátství

*„Každý autor má právo stanovit, jak s jeho dílem můžete nakládat.*
*Nesouhlasím-li s podmínkami užití díla,*
*nerozumím jim nebo je neznám,*
*mám právo dílo neužívat.“*
Jan Kolouch

Pojem Internetové pirátství je pojmem obecným, zastřešujícím kriminalitu, jež porušuje práva duševního vlastnictví (velmi často zužovaná pouze na právo autorské). Teprve s rozšířením počítačových systémů a zejména nástupem Internetu se dá hovořit o masovém pirátství, jakožto jedné z nejrozšířenějších forem kybernetické trestné činnosti.[526]

Porušování práv duševního vlastnictví, zejména autorských práv a práv souvisejících s právem autorským, patří v prostředí informačních technologií v současné době k jednomu z nejpalčivějších problémů.

### 4.10.1 Právo duševního vlastnictví

Ve vztahu k internetovému pirátství je třeba nejprve vymezit problematiku duševního vlastnictví, zejména pak práva autorského. Toto vymezení je nezbytné pro pochopení rozdílu mezi legálním a protiprávním jednání osob, které jsou na Internetu činné.

Právo duševního vlastnictví představuje majetek nehmotné povahy, tzv. „nehmotné statky“, které jsou **výsledkem tvůrčí činnosti člověka.** Toto právo je **nezávislé na hmotném substrátu** (může být proto užíváno kdykoliv a kdekoliv na světě) za podmínky, že je **jedinečné, neopakovatelné a dostatečně originální**.

Právo duševního vlastnictví je možné rozdělit do dvou oblastí:

1) **Autorská práva** (chrání např. původní literární a umělecká díla, hudební skladby, televizní vysílání, počítačové programy, databáze, reklamní výtvory, multimédia aj.)

2) **Průmyslová práva** (chrání např. patenty na vynálezy, vzory, průmyslové modely, ochranné známky, zeměpisný původ aj.)

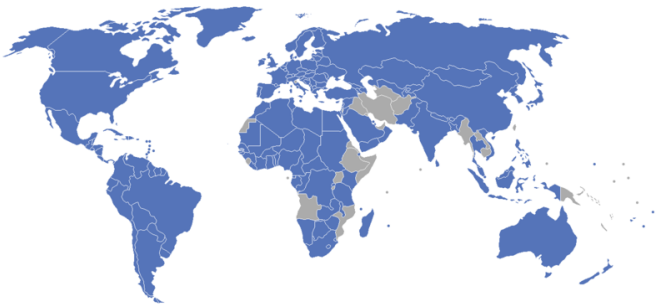
Z hlediska zaměření této monografie se dále budu primárně zabývat pouze právem autorským a zásahům do tohoto práva.

526: Srov. MATĚJKA, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 73. 22

### 4.10.2 Legislativní rámec

Ochrana práv autorských začala být poprvé na mezinárodní úrovni řešena v 19. století, a mezi nejvýznamnější právní dokumenty, které se jí věnují, patří:

- **Bernská úmluva o ochraně literárních a uměleckých děl**[527] (1886), která byla následně doplňována a upravována [1908 (Berlín), 1928 (Řím), 1948 (Brusel), 1967 (Stockholm), 1971 (Paříž).]. Od roku 1967 se její správou zabývá **WIPO** (World Intellectual Property Organization – Světová organizace duševního vlastnictví).



Obrázek 73: Seznam států. Modře[528] jsou vyznačeny státy, které přijaly Bernskou úmluvu.[529]

- Dohoda o obchodních aspektech práv k duševnímu vlastnictví, která je jednou z příloh Dohody o zřízení Světové obchodní organizace (WTO) – viz sděl. č. 191/1995 Sb., (**TRIPS – Trade Related Aspects of Intellectual Property Rights**).[530]

- Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací ze dne 26. října 1961 (vyhl. č. 192/1964 Sb., ve znění opravy č. 157/1965 Sb.) – **Římská úmluva**.[531]

527: Dostupná online. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1985-19; http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=34669&nr=133~2F1980&rpp=100#local-content

528: Poznámka vydavatele: V černobílé verzi knihy nahrazuje modrou barvu tmavě šedá.

529: *Bernská úmluva o ochraně literárních a uměleckých děl.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://cs.wikipedia.org/wiki/Bernsk%C3%A1_%C3%BAmluva_o_ochran%C4%9B_liter%C3%A1rn%C3%ADch_a_um%C4%9Bleck%C3%BDch_d%C4%9Bl. Předložená mapa je pouze ilustrační a nezobrazuje aktuální geopolitické členění světa. Kompletní seznam států, které ratifikovaly smlouvu WIPO, je možné nalézt na: http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15

530: Dostupná online. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.mkcr.cz/assets/autorske-pravo/sb51-95.pdf

531: Dostupná online. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1964-192; http://www.zakonyprolidi.cz/cs/1965-157

- Smlouva Světové organizace duševního vlastnictví o právu autorském Ženeva 1996 ze dne 20. prosince 1996 (viz sděl. 33/2002 Sb. m. s.), (**WCT – WIPO Copyright Treaty**).[532]

- Smlouva Světové organizace duševního vlastnictví o výkonech výkonných umělců a o zvukových záznamech Ženeva 1996 ze dne 20. prosince 1996 (viz sděl. 48/2002 Sb. m. s.), (**WPPT – WIPO Performances and Phonograms Treaty**).[533]

- Úmluva o ochraně výrobců zvukových záznamů proti nedovolenému rozmnožování jejich zvukových záznamů ze dne 29. října 1971 (viz vyhl. 32/1985 Sb.) – **Ženevská úmluva**.[534]

- Všeobecná úmluva o autorském právu revidovaná v Paříži dne 24. července 1971 (viz vyhl. č. 134/1980 Sb.).[535]

- Směrnice Rady 91/250/EHS ze dne 14. května 1991 o právní ochraně počítačových programů.

- Směrnice Rady 92/100/EHS ze dne 19. listopadu 1992 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s právem autorským, v platném znění.

- Směrnice Rady 93/83/EHS ze dne 27. září 1993 o koordinaci určitých předpisů týkajících se práva autorského a práv s ním souvisejících při družicovém vysílání a kabelovém přenosu.

- Směrnice Rady 93/98/EHS ze dne 29. října 1993 o harmonizaci doby ochrany práva autorského a určitých práv s ním souvisejících, v platném znění.

- Směrnice Evropského parlamentu a Rady 96/9/ES ze dne 11. března 1996 o právní ochraně databází.

- Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů práva autorského a práv s ním souvisejících v informační společnosti.

- Směrnice Evropského parlamentu a Rady 2001/84/ES ze dne 27. září 2001 o právu na opětný prodej ve prospěch autora originálu uměleckého díla.

- Směrnice Evropského parlamentu a Rady 2004/48/ES ze dne 29. dubna 2004 o dodržování práv duševního vlastnictví.

- Úmluva Rady Evropy č. 185 o kyberkriminalitě.

532: Dostupná online. [online]. [cit .15. 7. 2016]. Dostupné z: http://www.mkcr.cz/assets/autorske-pravo/sb015-02m.pdf
533: Dostupná online. [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.mkcr.cz/assets/autorske-pravo/sb021-02m.pdf
534: Dostupná online. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1985-32
535: Dostupná online. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.zakonyprolidi.cz/cs/1980-134

V rámci českého práva je právo duševního vlastnictví, včetně práva autorského chráněno například:

- Čl. 34 odst. 1 Listiny: *„Práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem.“*
- Zákonem č. 40/2009 Sb., trestní zákoník;
- **Zákonem č. 121/2000 Sb., autorský zákon;**
- Zákonem č. 89/2014 Sb., občanský zákoník;
- Zákonem č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví;
- Zákonem č. 441/2003 Sb., o ochranných známkách;
- Zákonem č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích;
- Vyhláškou č. 488/2006 Sb., kterou se stanoví typy přístrojů k zhotovování rozmnoženin, typy nenahraných nosičů záznamů a výše paušálních odměn.

### 4.10.3 Autorské právo

Stěžejním právním předpisem v oblasti autorského práva, práva souvisejícího s právem autorským a práva k databázi je v České republice **zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)**, ve znění pozdějších předpisů.[536]

Autorský zákon v § 1 stanoví, že upravuje:

a) **práva autora k jeho autorskému dílu**,
   1) práva výkonného umělce k jeho uměleckému výkonu,
   2) právo výrobce zvukového záznamu k jeho záznamu,
   3) právo výrobce zvukově obrazového záznamu k jeho záznamu,
   4) právo rozhlasového nebo televizního vysílatele k jeho vysílání,
   5) právo zveřejnitele k dosud nezveřejněnému dílu, k němuž uplynula doba trvání majetkových práv,
b) **práva související s právem autorským**,
c) **právo pořizovatele k jím pořízené databázi**,
d) **ochranu práv podle autorského zákona**,
e) **kolektivní správu práv autorských a práv souvisejících s právem autorským**.

536: Dále jen **autorský zákon**, nebo **AZ**.

Stěžejním pojmem autorského práva je **dílo**. Dílem je literární, umělecké a vědecké dílo, které **je jedinečným výsledkem tvůrčí činnosti člověka** a je **vyjádřeno v jakékoliv vnímatelné podobě** včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam. Za dílo je považován též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem.

Databáze,[537] která je způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvorem a jejíž součásti jsou systematicky nebo metodicky uspořádány a jednotlivě zpřístupněny elektronicky či jiným způsobem, je dílem souborným.

Fotografie a dílo vyjádřené postupem podobným fotografii jsou chráněny jako dílo fotografické.[538]

*„Pro pojem díla, jako předmětu práva autorského, nezáleží ani na rozsahu, ani na účelu, ani na stupni hodnoty (kvalitě díla). Pojem kvality díla však do určité míry souvisí s podmínkou tvůrčí činnosti. Jinými slovy, obsah nebo účel není rozhodující, pokud má výtvor byť minimální tvůrčí charakter. O díle v tomto smyslu není možno mluvit, jestliže tento tvůrčí prvek chybí."*[539]

Právo autorské se vztahuje na **dílo dokončené, jeho jednotlivé vývojové fáze a části, včetně názvu a jmen postav**, pokud splňují podmínky podle odstavce § 2 odst. 1 nebo § 2 odst. 2 AZ. Dílem je zejména:

- **dílo slovesné** vyjádřené řečí nebo písmem (proslov, kniha, novinový článek, scénář)
- **dílo hudební** (hudební skladba)
- **dílo dramatické** (divadelní představení) a **hudebně dramatické** (muzikál, opera)
- **dílo choreografické** (balet), **pantomimické**
- **dílo fotografické** (fotografie)
- **dílo audiovizuální** (film, animovaný film)
- **dílo výtvarné** (malba, črta, kresba, animace, socha, grafika)
- **dílo architektonické** (stavba)
- **dílo kartografické** (mapa, atlas)
- **počítačový program** (operační systém, či jiný software)
- **dílo souborné** (sborník, časopis, encyklopedie, antologie, pásmo, výstava)

537: Blíže viz § 88–94 AZ

538: Viz § 2 AZ

539: Blíže viz Rozhodnutí Nejvyššího soudu 5 Tdo 631/2003, ze dne 18.6.2003. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/48AEF52C74365354C1257A4E0069A613?openDocument&Highlight=0

Dílem dle § 2 odst. 6 AZ není:

- námět díla sám o sobě
- denní zpráva
- myšlenka
- postup, princip
- metoda
- objev, vědecká teorie
- matematický a obdobný vzorec
- statistický graf a podobný předmět sám o sobě

Autorský zákon se dále nevztahuje na:

- **úřední dílo** (např. právní předpis, rozhodnutí, veřejná listina, veřejně přístupný rejstřík a sbírka jeho listin, úřední návrh úředního díla a jiná přípravná úřední dokumentace, sněmovní a senátní publikace, obecní kroniky, státní symbol a symbol jednotky územní samosprávy);

- **výtvory tradiční lidové kultury** (není-li pravé jméno autora obecně známo, užít takové dílo lze jen způsobem nesnižujícím jeho hodnotu);[540]

- **státní symboly** (viz zákon č. 352/2001 Sb., o užívání státních symbolů České republiky a o změně některých zákonů).

**Autorem** díla **je fyzická osoba, která dílo vytvořila**.[541] Právo autorské k dílu vzniká okamžikem, kdy je dílo vyjádřeno v jakékoli objektivně vnímatelné podobě. Zničením věci, jejímž prostřednictvím je dílo vyjádřeno, nezaniká právo autorské k dílu.[542]

**Spoluautorem** není ten, kdo ke vzniku díla přispěl pouze poskytnutím pomoci nebo rady technické, administrativní nebo odborné povahy nebo poskytnutím dokumentačního nebo technického materiálu, anebo kdo pouze dal ke vzniku díla podnět.[543]

540: Viz § 3 AZ

541: § 5 odst. 1 AZ V kontextu znění autorského zákona pak autorským dílem není fotografie, která není výsledkem tvůrčí činnosti člověka, tj. byla pořízena „strojově". Jedná se například o snímek z automatického radaru, fotopasti, satelitní snímek aj. Diskusi pak mohou vzbudit snímky automaticky pořízené UAV (Unmanned Aerial Vehicle – bezpilotní letadla či jiné prostředky), které jsou však ovládány člověkem (snímky jsou zpravidla pořizovány na základě pokynu člověka).

542: § 9 odst. 1, 2 AZ

543: § 8 odst. 2 AZ

Autor, jakožto tvůrce díla, má dvě základní skupiny práv (viz § 10 AZ):

**Výlučná práva osobnostní**
Osobnostních práv se autor nemůže vzdát; tato práva jsou nepřevoditelná a smrtí autora zanikají, jde o základní lidské právo. Mezi tato práva patří:

- **Právo rozhodovat o zveřejnění díla**
- **Právo osobovat si autorství** (včetně práva rozhodnout, zda a jakým způsobem má být jeho autorství uvedeno při zveřejnění a dalším užití jeho díla)
- **Právo na nedotknutelnost díla** (zejména právo udělit svolení k jakékoli změně nebo jinému zásahu do svého díla, nestanoví-li zákon jinak)

**Výlučná práva majetková**
Majetková práva trvají za života autora a 70 let po jeho smrti. Mohou být předmětem dědictví. Mezi tato práva patří:

- Právo **dílo užít**
- Právo **udělovat dalším osobám svolení** k výkonu práva
- Právo na **odměnu** v souvislosti s rozmnožováním díla
- Právo na **odměnu při opětovném prodeji** originálu díla uměleckého

Mezi **výlučná práva majetková** patří zejména právo autora dílo **užít**, které zahrnuje:

- právo na rozmnožování díla,[544]
- právo na rozšiřování originálu nebo rozmnoženiny díla,[545]
- právo na pronájem originálu nebo rozmnoženiny díla,[546]
- právo na půjčování originálu nebo rozmnoženiny díla,[547]
- právo na vystavování originálu nebo rozmnoženiny díla,[548]
- právo na sdělování díla veřejnosti.[549] Právem na sdělování díla se rozumí:
  - právo na provozování díla živě nebo ze záznamu a právo na přenos provozování díla,[550]
  - právo na vysílání díla rozhlasem či televizí,[551]

544: § 13 AZ
545: § 14 AZ
546: § 15 AZ
547: § 16 AZ
548: § 17 AZ
549: § 18 AZ
550: § 19 a 20 AZ
551: § 21 AZ

- právo na přenos rozhlasového či televizního vysílání díla,[552]
- právo na provozování rozhlasového či televizního vysílání díla.[553]

Dále mezi výlučná práva majetková patří **právo na odměnu při opětném prodeji originálu díla uměleckého,**[554] **právo na odměnu v souvislosti s rozmnožováním díla pro osobní potřebu a vlastní vnitřní potřebu,**[555] **právo na odměnu v souvislosti s pronájmem originálu nebo rozmnoženiny díla**.[556]

Dílo, u kterého uplynula doba trvání majetkových práv, může každý bez dalšího **volně užít**.[557] Při takovém užití si však nikdo nesmí osobovat autorství díla a dílo smí užít jen způsobem nesnižujícím jeho hodnotu.

Autorský zákon dále stanoví výjimky a omezení práva autorského (viz § 29 AZ a násl.), přičemž tyto výjimky a omezení práva autorského **lze uplatnit pouze ve zvláštních případech stanovených v autorském zákoně a pouze tehdy**, pokud takové užití díla není v rozporu s běžným způsobem užití díla a **ani jím nejsou nepřiměřeně dotčeny oprávněné zájmy autora**. Na základě těchto výjimek tedy nebude každý zásah do práva autorského nutně neoprávněný. Mezi tyto výjimky patří:

- **Volná užití** (§ 30 AZ)
  - Rozmnožování na papír nebo na podobný podklad (§ 30a AZ)
  - Předvedení či oprava přístroje (§ 30b AZ)
  - Citace (§ 31 AZ)

- Propagace výstavy uměleckých děl a jejich prodeje (§ 32 AZ)

- Užití díla umístěného na veřejném prostranství (§ 33 AZ)

- Úřední a zpravodajská licence (§ 34 AZ)

- Užití díla v rámci občanských či náboženských obřadů nebo v rámci úředních akcí pořádaných orgány veřejné správy, v rámci školních představení a užití díla školního (§ 35 AZ)

- Omezení práva autorského k dílu souhrnnému (§ 36 AZ)

552: § 22 AZ
553: § 23 AZ
554: § 24 AZ
555: § 25 AZ
556: § 25a AZ
557: § 28 odst. 2 AZ

- Knihovní licence (§ 37 AZ)
- Licence pro určitá užití osiřelého díla (§ 37a AZ)
- Licence pro zdravotně postižené (§ 38 AZ)
- Licence pro dočasné rozmnoženiny (§ 38a AZ)
- Licence pro fotografickou podobiznu (§ 38b AZ)
- Nepodstatné vedlejší užití díla (§ 38c AZ)
- Licence k dílům užitého umění a dílům architektonickým (§ 38d AZ)
- Licence pro sociální zařízení (§ 38e AZ)
- Umožnění příjmu současného, úplného a nezměněného rozhlasového nebo televizního vysílání na přijímačích téže budovy, popřípadě komplexu budov k sobě prostorově nebo funkčně přináležejících, pomocí společných domovních antén za podmínky, že je umožněn příjem pouze zemského nebo satelitního vysílání a společný příjem není využíván za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu (§ 38f AZ)
- Užití originálu nebo rozmnoženiny díla výtvarného, fotografie nebo díla vyjádřeného postupem podobným fotografii jeho vystavením (§ 39 AZ)

Z hlediska porušování práv autorských v kyberprostoru velmi často dochází k argumentaci, že se jednalo o **volné užití díla**. Volným užitím díla (dle § 30 AZ) se rozumí **užití pro osobní potřebu fyzické osoby, jehož účelem není dosažení** přímého nebo nepřímého hospodářského nebo obchodního prospěchu, nestanoví-li tento zákon jinak. Do práva autorského nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla.

Podle autorského zákona však není volným užitím díla užití počítačového programu či elektronické databáze, zhotovení rozmnoženiny či napodobeniny díla architektonické stavby, a pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu.[558]

558: Viz § 30 odst. 3 AZ. V uvedených případech se nejedná o volné užití díla pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby včetně zhotovení rozmnoženiny takových děl i pro takovou potřebu.

V rámci volného užití díla dle § 30 AZ je tedy možné vytvořit kopii (rozmnoženinu díla) za následujících podmínek:

- **Dílo musí být užito pro osobní potřebu** fyzické nebo právnické osoby,
- **účelem není dosažení** přímého nebo nepřímého hospodářského nebo obchodního prospěchu,
- dílo musí být **zveřejněno**,
- **není možné** při vytváření kopie **obcházet technické prostředky**[559] **sloužící k ochraně práv** (§ 43 AZ),
- kopii vytváří ten, kdo ji bude užívat (§ 30 odst. 2 AZ).

Dílo je podle § 29 AZ volně užito v souladu se zákonem pouze tehdy, jestliže takové užití vyhovuje tzv. **třístupňovému testu**.[560] Podle tohoto testu se jedná o zákonné užití díla tehdy, jestliže:

1) **se jedná o výjimku zvlášť v autorském zákoně uvedenou,**
2) **pokud takové užití díla není v rozporu s běžným způsobem užití díla a**
3) **ani jím nejsou nepřiměřeně dotčeny oprávněné zájmy autora díla.**

Jestliže nakládání s dílem nesplňuje byť jednu z uvedených podmínek, jedná se o porušení práva autorského nebo práv souvisejících s právem autorským.

### 4.10.4 Vlastní útoky

Pro fenomén porušování práv autorských a práv souvisejících s právem autorským se v prostředí Internetu vžilo několik pojmů. Nejčastěji bývá užíván pojem **softwarové pirátství** (pro porušování autorských práv ve vztahu k počítačovým programům) a **audiovizuální pirátství** (pro porušování autorských práv k audiovizuálním dílům – hudebním a filmovým). **Základem pro softwarové i audiovizuální pirátství je však vždy porušení některého z autorských práv**

559: Technická ochrana díla je označována jako **Digital Rights Management (DRM)**. Smyslem technické ochrany je výkon kontroly nad přístupen k dílu a možnost nastavit omezení k užití díla. Nejobecněji je možné technickou ochranu rozdělit na:

1) **Prostředky sloužící ke kontrole přístupu k dílu (Access control).** Držitel práv má možnost stanovit, kdy a za jakých podmínek získá uživatel k dílu přístup. Omezit lze jak doba (např. po kterou lze dílo užít – např. pouze v určitý okamžik či po určitou dobu), vnímající osoby (např. přístup autentizizovaný skrze heslo aj.), místo, přístroj (např. na kterém lze dílo přehrát, zpracovávat aj.) a další.
2) **Prostředky sloužící k omezení díla v autorskoprávním smyslu.** Užití díla může být omezeno kvantitativně (např. omezený počet možností pro vytvoření rozmnoženin či zpřístupnění díla veřejnosti), prostorově, přístrojově (jde o definování přístrojů, na nichž je možné dílo přehrát či zpracovávat aj.) či jinak.

560: Třístupňový test vychází z Revidované Bernské úmluvy (čl. 9 odst. 2). Dále je uveden v Úmluvě Světové organizace duševního vlastnictví o právu autorském (čl. 10), Dohodě o obchodních aspektech práv duševního vlastnictví (čl. 13), Směrnice 2001/29/ES (čl. 5).

**či práv souvisejících s právem autorským.**[561] Obecným pojmem, který zastřešuje softwarové a audiovizuální pirátství, je pojem Internetové (někdy též počítačové) pirátství.

Trestné činy proti duševnímu vlastnictví se značně rozšířily právě s masovým nástupem Internetu. Jako nejběžnější případy porušování autorského díla v kyberprostoru lze uvést:

- *Šíření díla elektronickou poštou*, což je nejjednodušší způsob k šíření malých souborů (zejména literárních či grafických autorských děl).

- *Zveřejnění díla na webových stránkách* bez souhlasu autora. Jedná se o další velmi jednoduchý způsob porušování autorského práva. Zveřejňovány jsou menší soubory (z hlediska velikosti dat) a toto nelegální jednání je zpravidla velmi brzy odhaleno.

- *Rozšiřování díla nahráním na specializovaný server*, odkud je možné volně dané dílo stáhnout (např. Megaupload, Rapidshare).

- *Šířením díla za využití Peer-to-peer (P2P) sítí*.[562] Tyto sítě jsou schopné přenášet/sdílet obrovská množství dat (v řádech několika GB až desítek TB). V rámci nich dochází k nejzávažnějšímu porušování autorských práv.

- *Zásahy do počítačových programů s cílem překonat technická opatření nositele autorských práv zabraňujících pořizování kopií takto chráněných programů* (tzv. crack).

- *Rozšiřování díla pomocí datových nosičů přímo mezi uživateli* (půjčování a následné okopírování dat z DVD, HDD apod., prodej datových nosičů a další).

- *Pořízení záznamu přímo při produkci a její následné rozšíření* (např. pořízení obrazového záznamu filmového díla přímo z plátna) – tzv. camcording.

- *Neoprávněné projekce audiovizuálních děl*.

- *Již vlastní obstarání si počítačového díla*. Počítačový program požívá zvláštní ochrany a není možné bez souhlasu nositelů autorských práv ve smyslu autorského zákona pořizovat rozmnoženiny takového díla, a to ani pro vlastní potřebu.

561: Blíže k této problematice srov. VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*, 2010, roč. 14, č. 7–8, s. 34 a násl.

562: Zapojením do P2P začíná uživatel, při standardním nastavení, automaticky sdílet s dalšími (jemu zpravidla neznámými) uživateli, svůj obsah. Typicky je při stahování (download) automaticky nastaveno i nabízení (upload) stahovaného materiálu.

- *Užívání počítačového programu v rozporu s licencí.*
- A další.

Mezi nejčastější projevy audiovizuálního pirátství patří zejména neoprávněné šíření audiovizuálních děl pomocí počítačových sítí, opatřování záznamu filmových děl přímo při promítání v kině a jejich následné „umístění" ke stažení v kyberprostoru, šíření originálních nosičů s filmovým či hudebním dílem v rozporu s licenčním ujednáním, výroba a šíření padělků originálních filmových či hudebních děl a veřejné projekce filmových děl v rozporu s licenčním ujednáním. Dále pak jednání spočívající v šíření softwarových produktů, zásazích do softwarových produktů, nelegální výroba softwarových produktů a užívání softwarových produktů v rozporu s licenčním ujednáním. Porušením autorského práva bude již vlastní neoprávněné obstarání softwarového produktu, aniž by s ním bylo dále nakládáno.[563]

**Umístění díla** (bez ohledu na to, jestli audiovizuálního či softwarového) do kyberprostoru (**upload**) naplňuje znak šíření díla ve smyslu autorského zákona a (pokud není autorem nebo jinou oprávněnou osobou dovoleno) může být trestně postižitelné. **Neoprávněným užitím díla je též zveřejnění odkazu na místo v kyberprostoru, odkud je možné dílo získat.** Jedná se o užití díla v podobě sdělování veřejnosti ve smyslu § 12 odst. 4 písm. f), § 18 AZ.

Na tomto místě je vhodné zmínit problematiku *„Embedded links"*,[564] ke kterým se vyjádřil Nejvyšší soud (8 Tdo 137/2013 ze dne 27. 2. 2013, Rt 7/2014) následovně:

*„Za neoprávněný zásah do zákonem chráněných práv ve smyslu § 270 odst. 1 TZK lze považovat i takové jednání pachatele, který na Internetu v prostoru vyhrazeném pro své internetové stránky umístí odkazy (tzv. embedded linky) umožňující neoprávněný přístup k rozmnoženinám děl (např. filmových a televizních) umístěných na externích serverech tak, že kdokoli k nim může mít prostřednictvím takové internetové stránky přístup, aniž by k tomu měl souhlas nositelů autorských práv, a využije tzv. hostingu s možností uložení dat na serveru. V takovém případě totiž pachatel (umístěním tzv. embedded linku) umožnil přístup k rozmnoženině díla, a to jako osoba odlišná od osoby, která je vlastníkem této rozmnoženiny nebo jinou oprávněnou osobou, což je činnost, jíž je nutné považovat za porušení autorských práv k jednotlivým dílům a porušení práva na sdělování díla veřejnosti ve smyslu § 18 odst. 1, 2 zákona č. 121/2000 Sb., o právu autorském, o právech*

563: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1, s. 108–109

564: **Embedded links** - jedná se o technický způsob umístění obsahu na internetových stránkách pomocí vložení připraveného kódu, odkazujících na obsah umístěný na jiné internetové stránce tak, že je tento obsah možné zpřístupnit na té stránce, kde je embeddovaný link umístěn, bez nutnosti uživatele přejít na internetovou stránku, kde je umístěn obsah.

*souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších právních předpisů.* "[565]

**Stažení díla (download)** z kyberprostoru nutně nemusí být protiprávní.[566] Stažení filmového či hudebního díla z Internetu není trestněprávní teorií ani praxí vnímáno jako trestné, přestože jistě nejde o volné užití díla (nejčastěji dochází ke stažení díla, které bylo do prostředí Internetu umístěno v rozporu s právními předpisy, a jde tedy o dílo nelegální. Stažení takového díla tedy není v souladu s tzv. třístupňovým testem, neboť jsou tímto jednáním nepřiměřeně dotčeny zájmy nositele autorských práv).[567]

Pokud jde o srovnání se zahraniční právní úpravou, je vhodné se zmínit o francouzském zákonu HADOPI,[568] který měl chránit před internetovým pirátstvím. Dle tohoto zákona vznikl zvláštní úřad, jehož úkolem bylo zjišťovat ilegální stahování materiálu podléhajícího autorským právům. Ti uživatelé, kteří si stáhli hudbu a filmy z Internetu bez zaplacení (vyjma volně šiřitelných děl), byli třikrát varováni a při nerespektování těchto varování byl předmětný úřad oprávněn odpojit je od Internetu až na jeden rok.[569] Avšak ani takto přísný zákon neomezil počet nelegálního stahování autorských děl. Zároveň však nastolil řadu otázek týkající se přípustnosti zásahu do základních lidských práv a svobod bez rozhodnutí soudu.[570] Zákon HADOPI byl zrušen 10. července 2013.

V souvislosti s internetovým pirátstvím se často objevuje též pojem „Warez". **Warez představuje**, velmi zjednodušeně řečeno, **formu počítačového pirátství**, kde informační technologie jsou pouze prostředkem pro urychlení šíření nelegálních kopií autorských děl prostřednictvím Internetu. Warezová fóra v současnosti slouží zejména ke stahování cracků a keygenů, ale i kompletních upravených programů, filmů a hudby. Výsledný produkt warezové scény se nazývá **release**. Pro

565: Rozhodnutí Nejvyššího soudu 8 Tdo 137/2013, ze dne 27.2.2013. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/763AE1D4853A3985C1257B5C004F46EE?openDocument&Highlight=0

566: Viz splnění podmínek volného užití díla - kap. 4.10.3 Autorské právo.

567: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 109

568: **HADOPI** (High Authority for Copyright Protection and Dissemination of Works on the Internet law), Fr: ***Loi favorisant la diffusion et la protection de la création sur Internet.***

569: Úřad k tomuto rozhodnutí nepotřeboval rozhodnutí soudu. Na základě stanoviska Ústavního soudu Fr. z 22. listopadu 2009 je k odpojení vyžadován souhlas soudu.

570: Blíže viz např. *Francie zakáže internetové pirátství.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.blisty.cz/2009/5/13/art46807.html

*Přísný zákon proti hudebním a filmovým pirátům Francii nepomohl.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi-/sw_internet.asp?c=A100330_095705_sw_internet_vse

*France drops controversial 'Hadopi law' after spending millions.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy aj.

ochranu soukromí používají klienti warezových fór proxy servery a bouncery sloužící k maskování jejich IP adresy, a tím znemožňující případné sledovaní. Vlastní komunikace a nabízení release probíhá v privátních místnostech, vytvořených k tomuto účelu na Internetu, kam mají přístup pouze členové skupiny.

Poskytování souborů, ať v rámci warezu či P2P sítě, lze postihnout dle **§ 270** (Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi), případně dle **§ 231** (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK.

### 4.10.5 Možná řešení

Mnohdy je počítačové pirátství prezentováno jako jednání, které: *„zahrnuje veškerou protiprávní činnost, která je realizována pomocí výpočetní techniky, a jejím důsledkem je porušování práv k duševnímu vlastnictví.“*[571] Jedním z posledních počinů prezentujících počítačové pirátství je projekt: https://www.mojepiratstvi.cz/.[572] V této oblasti je možné pozorovat celou řadu preventivních aktivit, které mají přimět uživatele „nestahovat“ (viz např. *Pirátství je zločin*: https://www.youtube.com/watch?v=2QRYdlByEjo) a zhruba stejné množství parodií na tyto preventivní akce (viz např. *The IT Crowd – Series 2 – Episode 3: Piracy warning*: https://www.youtube.com/watch?v=ALZZx1xmAzg). Dle mého názoru je ale tento jev mnohem hlubší a komplikovanější.

Pokud se chceme zabývat problematikou počítačového pirátství, je třeba představit obě strany existujícího a probíhajícího konfliktu. Na straně jedné jsou to vlastní autoři děl a různé asociace, které se více či méně snaží chránit jejich, zejména majetková, práva.[573] Na straně druhé jsou to de facto všichni uživatelé Internetu. Dovolím si tvrdit, že existuje mizivé promile lidí, kteří nikdy nezasáhli do autorských práv jiného [např. tím, že si stáhli z Internetu soubor (hudbu, video, text aj.) či využívali program ne zcela v souladu s licenční smlouvou (např. program Total Commander po uplynutí 30 denní lhůty aj.)].

První strana bude tvrdit, že počítačové pirátství je tím nejrozšířenějším (v čemž zřejmě mají pravdu) a nejnebezpečnějším zločinem online, kdežto druhá strana bude namítat, že stahování děl z Internetu a jejich užívání je běžnou součástí dnešního života (viz legální nástroje jako Netflix, Spotify, Youtube aj.).

---

571: *Co je pirátství.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.stoppiratstvi.cz/cs/o-piratstvi/co-je-piratstvi.shtml; či http://www.filmynejsouzadarmo.cz/cs/o-piratstvi/

572: Stránka https://www.mojepiratstvi.cz/ je značně jednostranně zaměřena a uvádí ne zcela přesné informace. Blíže viz např. KRUŽÍK Jan a NÝVLT Václav. *Protipirátská BSA schválně mate. Žádný alternativní trest pro piráta nepadl.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://technet.idnes.cz/bsa-jakub-f-alternativni-trest-deh-/tec_technika.aspx?c=A151123_141357_tec_technika_vse

573: Blíže viz kap. 4.10.3 Autorské právo.

Zásadní problém spatřuji především ve skutečnosti, že „ochránci práv autorských" poněkud zaspali dobu a nejsou schopni reagovat na rozmach informačních a komunikačních technologií. V současnosti prezentovaný model spočívající v ochraně práv autorských vychází z konceptu, jehož základy byly vytvořeny v 19. století. Tento koncept dle mého názoru není schopen v současné době obstát. Netvrdím, že by autoři neměli mít přiznána práva ke svému dílu, avšak otázkou je, jak efektivněji ochranu těchto práv zajistit.

Vhodným řešením dle mého názoru rozhodně není vybírání poplatku za prázdná média či počítačové systémy (viz snahy z poslední doby o placení poplatku za mobilní telefon s interní pamětí[574]). Takovéto řešení de facto kriminalizuje všechny uživatele, kteří mají jakýkoli počítačový systém, který umožňuje ukládání dat. Ochranný svaz autorský[575] (v době online služeb nabízejících zdarma hudbu a video) tento krok údajně činí, protože i na mobily si lidé často nahrávají nelegální obsah, kterým porušují autorská práva.

Řešení internetového pirátství v podobě vybírání poplatku za prázdné datové nosiče jakožto jakousi „saturaci" za pořizování soukromých rozmnoženin z neoprávněného zdroje napadl i Soudní dvůr Evropské unie. Ve věci C-435/12 - ACI Adam a další Soudní dvůr EU mimo jiné konstatoval, že členské státy EU by měly zákonem zakázat možnost pořizování soukromých rozmnoženin z neoprávněného zdroje:[576]

*„…unijní právo, konkrétně čl. 5 odst. 2 písm. b) směrnice 2001/29, ve spojení s odstavcem 5 tohoto článku, musí být vykládáno v tom smyslu, že brání takovým vnitrostátním právním předpisům, jaké jsou dotčeny v původním řízení, které situaci, kdy zdroj, z něhož je rozmnožena pro soukromé užití pořízena, je oprávněný, neodlišují od situace, kdy je tento zdroj neoprávněný."*

Soudní dvůr EU dále konstatoval, že **poplatky za prázdná média by měly být stanoveny tak, aby jejich výše nezohledňovala nelegální kopírování děl:**

*„Všichni uživatelé, kteří si pořídí takové vybavení, přístroje nebo nosiče, jsou tak nepřímo penalizováni, neboť tím, že nesou zátěž spojenou s poplatkem stanoveným bez ohledu na to, zda zdroj, z něhož jsou takové rozmnoženiny pořízeny, je oprávněný či neoprávněný, nutně přispívají*

574: *OSA chce i poplatek za nové mobily, maximálně 90 korun z každého.* [online]. [cit. 23. 8. 2016]. Dostupné z: http://ekonomika.idnes.cz/osa-chce-penize-i-z-mobilu-maximalne-90-korun-z-kazdeho-p0e-/test.aspx?c=A160819_092317_test_suj

575: Blíže viz http://www.osa.cz/

576: Viz Rozsudek Soudního dvora (čtvrtého senátu) ze dne 10.4.2014. ACI Adam BV a další proti Stichting de Thuiskopie a Stichting Onderhandelingen Thuiskopie vergoeding. [online]. [cit. 15. 7. 2016]. Dostupné z: http://curia.europa.eu/juris/liste.jsf?num=C-435/12; http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5419c26aa775041c0a292b59941c66783.e34KaxiLc3eQc40LaxqMbN4Pa3mMe0?text=&docid=150786&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=203878

*na náhradu újmy vzniklé v důsledku rozmnožením pro soukromé užití pořízených z neoprávněného zdroje, které směrnice 2001/29 nedovoluje, a jsou tak nuceni nést nezanedbatelnou dodatečnou zátěž, aby mohli pořizovat soukromé rozmnoženiny, na které se vztahuje výjimka podle čl. 5 odst. 2 písm. b) uvedené směrnice.* ***Takovouto situaci nelze považovat za splňující podmínku přiměřené rovnováhy, jež má být nalezena mezi právy a zájmy osob, kterým náleží spravedlivá odměna, a právy a zájmy zmíněných uživatelů.*** *"*

V České republice se k problematice vytvoření rozmnoženiny díla pro vlastní potřebu (za splnění podmínek § 30 AZ) vyjádřil Nejvyšší soud (5 Tdo 234/2009 ze dne 25. 3. 2009) následovně:

*„Dále považuje Nejvyšší soud za nutné uvést,* ***že jak také vyplývá ze znění ustanovení § 30 odst. 1 písm. a) autorského zákona, nelze z něj dovozovat, že se omezení autorského práva pro pořizování rozmnoženiny díla pro osobní potřebu vztahuje pouze na pořízení rozmnoženiny z originálu díla nebo z jeho legálně zakoupené kopie*** *pořizovatelem rozmnoženiny,* ***neboť v rámci omezení autorského práva pro pořizování rozmnožením pro osobní potřebu nestanoví toto ustanovení nic o právní povaze zdroje, ze kterého je možno rozmnoženinu díla pro osobní potřebu pořizovat.*** *Může se tedy jednat jak o originál, tak i o rozmnoženinu díla, přičemž není bez dalšího nikterak vyloučeno, aby zdrojová rozmnožením, ze které si zhotovitel pořídí vlastní rozmnoženinu pro osobní potřebu, byla pořízena i na základě jednání, které je v rozporu s autorským zákonem. Tato skutečnost nemůže sama o sobě, pokud autorský zákon nestanoví jinak, změnit právní povahu aktu pořízení rozmnoženiny díla pro osobní potřebu, jež je autorským právem aprobované, což samozřejmě nemá žádný vliv na vznik autorskoprávní a případně i trestní odpovědnosti za předchozí porušení autorského práva. "* [577]

Jednou z možností je koncept poskytování děl v rámci služeb jako Netflix, Spotify aj., které nabízejí chráněná díla za cenu přijatelnou pro uživatele. Domnívám se, že další možností je například využití vícekanálová distribuce autorského díla spojená s různými alternativami placení za dílo.[578]

Pokud by se např. George Lucas rozhodl, že další díl Star Wars bude distribuován jak v klasických kinech, tak současně např. na Youtube nebo jiném serveru (kde bude např. umístěna reklama), tak se domnívám, že dojde k situaci, kdy uvedený server vygeneruje Georgi Lucasovi zisk možná vyšší, než který získá „tradičním způsobem". Zároveň tak dojde k eliminaci internetového

577: Blíže viz Rozhodnutí Nejvyššího soudu 5 Tdo 234/2009, ze dne 25. 3. 2009. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/0873CA8A4A362534C1257A4E0066BE88?openDocument&Highlight=0

578: Viz např.

- *"Flat Fee Music" & The MUSIC LIKE WATER MANIFESTO*. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.futuristgerd.com/2006/01/15/flat-fee-music/
- Marketingový model spočívající v zisku financí za návštěvnost stránky, počet zhlédnutí videa aj.
- Pricing model spočívající platbě za skutečné užití produktu (služby).

pirátství, neboť proč krást něco, co všichni mají. Tímto modelem samozřejmě nemusí být ovlivněna distribuce na datových nosičích, jako je např. DVD, Blu-Ray aj.[579]

Jsem přesvědčen, že zde nastíněné či jiné účinné, primárně nerepresivní, řešení může efektivně ovlivnit problém počítačového pirátství. Tato úvaha mne dovedla i k mému rozhodnutí vydat knihu, kterou právě čtete pod Creative Commons licencí, přičemž je třeba, abyste respektovali následující podmínky licence CC BY ND:[580]

*Dílo smíte:*

- **Sdílet** - rozmnožovat a distribuovat materiál prostřednictvím jakéhokoli média v jakémkoli formátu pro jakýkoliv účel, a to i komerční.

  Poskytovatel licence nemůže odvolat tato oprávnění do té doby, dokud dodržujete licenční podmínky.

*Za těchto podmínek:*

- **Uveďte původ** - Je Vaší povinností uvést autorství, poskytnout s dílem odkaz na licenci a vyznačit Vámi provedené změny. Toho můžete docílit jakýmkoli rozumným způsobem, nicméně nikdy ne způsobem naznačujícím, že by poskytovatel licence schvaloval nebo podporoval Vás nebo Váš způsob užití díla.

- **Nezasahujte do díla** - Pokud dílo zpracujete, zpracujete s jinými díly, doplníte nebo jinak změníte, nesmíte toto upravené dílo dále šířit..

- **Žádná další omezení** - Nesmíte použít právní omezení nebo účinné technické prostředky ochrany, které by omezovaly ostatní v možnostech poskytnutých touto licencí.


579: Blíže viz např. DOČEKAL, Daniel. *Studie: Filmové pirátství nepoškozuje Hollywood, může mu i prospět.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.lupa.cz/clanky/studie-filmove-piratstvi-neposkozuje-hollywood-muze-mu-i-prospet/
Z článku cituji:
„Podle Strumpfových odhadů se pirátské kopie snímků v období 2003–2009 projevily snížením příjmů z kin v průměru ve výši 200 milionů dolarů ročně. Což představuje pouze tři desetiny procenta z částky, kterou filmy za stejné období utrží. Pro jasnější obraz je k této částce vhodné dodat, že Hollywood za totéž období utratil 500 milionů dolarů za antipirátské aktivity. Strumpf navíc zjistil, že pokud se film v horší kvalitě objeví na Internetu krátce před uvedením do kin, může tato skutečnost mít pozitivní vliv na tržby. Domnívá se totiž, že podobné aktivity přispívaji k lepšímu vybudování povědomí o novém filmu."
580: Podmínky jsou doslovně převzaty z https://creativecommons.org/licenses/by-nd/3.0/cz/.

## 4.11 Sniffing

Sniffing je metoda nelegálního odposlechu dat procházejících počítačovou sítí při komunikaci mezi poskytovanou službou a počítačovým systémem prostřednictvím tzv. **snifferu**.[581]

Technicky sniffing znamená odchytávání a čtení TCP paketů. Z bezpečnostního pohledu je sniffing možné označit také jako monitoring sítě, či monitoring provozu sítě a jedná se o jeden ze standardních prostředků pro diagnostiku sítě, respektive diagnostiku anomálií v síťovém provozu. Monitoring sítě je pak schopen zobrazit například nestandardní komunikaci počítačového systému napadeného malwarem atp. Vlastní činnost správců sítě v případě monitoringu sítě není nelegální (pokud se nedopustí dalšího jednání, které by mohlo případnou právní odpovědnost zakládat – např. instalace keylogger, či jiného malware do počítačového systému bez vědomí uživatele), neboť umožňuje udržet a spravovat počítačovou síť.

K monitoringu síťového provozu je využívána celá řada nástrojů (např. Wireshark,[582] NetWorx, PRTG Network monitor aj.).

Pro to, aby bylo možné sniffing subsumovat pod jeden z projevů kyberkriminality, je třeba, aby osoba provádějící tuto činnost jednala nelegálně, typicky bez souhlasu či vědomí uživatele. Z dat zachycených sniffingem je útočník schopen extrahovat a složit citlivé informace o uživateli, např. přihlašovací údaje (uživatelské jméno a heslo), e-mailovou či VoIP komunikaci, informace o používaných službách aj. Ke sniffingu může být využit i malware v podobě trojských koní, keyloggerů nebo například spyware.

De facto by takovou činnost bylo možné označit jako **nelegální odposlech a záznam telekomunikačního provozu**. Výše popsaným jednáním jistě dojde k zásahu do základních lidských práv a svobod, zejména se jedná o **čl. 13** Listiny, **a je zcela lhostejné, zda nelegální sniffing provádí externí útočník, či administrátor sítě**. Dle norem trestního práva by bylo možné takové jednání subsumovat pod **§ 182 odst. 1** (Porušení tajemství dopravovaných zpráv) TZK a v případě zneužití takto získaných informací by se mohlo jednat o trestný čin dle **§ 182 odst. 2** TZK. Pokud uvedenou nelegální činnost provádí zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, mohl by naplnit znaky skutkové podstaty dle **§ 185 odst. 5** TZK.

581: **Sniffing** je anglické slovo znamenající - **čmuchat, čenichat**. Sniffer je pak možné krkolomně přeložit jako čichač.

582: Blíže k použití software Wireshark např. *How to use Wireshark to capture, Filter and inspect Packets.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/
MINAŘÍK, Pavel. *Wireshark – Paketová analýza pro všechny.* [online]. [cit. 18. 8. 2016]. Dostupné z: https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm


Obrázek 74: Password Sniffer Spy. Rozmazaná jsou jména a hesla.[583]

## 4.12 DoS, DDoS, DRDoS útoky

Pojem **DoS** je zkratkou z anglického spojení slov ***„denial of service"***, což lze do českého jazyka přeložit jako „popření či odepření služby". Jedná se o jednu z forem útoků na (internetovou) službu, jehož cílem je vyřazení z činnosti nebo snížení výkonu napadeného technického zařízení.[584] Tento

583: *Password Sniffer Spy*. [online]. [cit. 18. 8. 2016]. Dostupné z: http://securityxploded.com/password-sniffer-spy.php

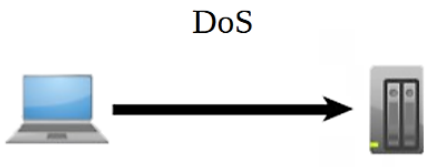
584: Blíže srov. např. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 335–354. CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet Based Denial-of-Service Detection. *Computers & Security*, 2006, roč. 25, č. 8, s. 600–615

RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007–2017. *Security magazín*, 2007, roč. 14, č. 1, s. 3.

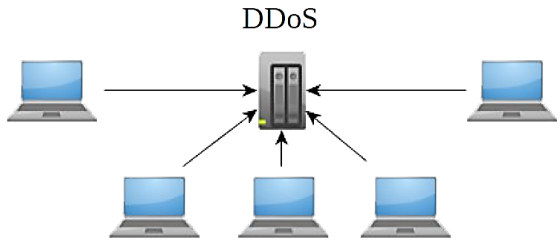
útok je realizován zahlcením napadeného počítačového systému (či prvku sítě) pomocí opakujících se požadavků na úkony, které má počítačový systém vykonat. Tento útok může být realizován i zahlcením informačních kanálů mezi serverem a počítačem uživatele či zahlcením volných systémových prostředků. Systém napadený DoS útokem se projevuje zejména neobvyklým zpomalením služby, celkovou nebo chvilkovou nedostupností služby (např. webových stránek) apod.

Rozdíl mezi DoS, DDoS a DRDoS útoky spočívá především v tom, jakým způsobem je útok veden. Pro názornost jsou k jednotlivým typům útoku přiloženy obrázky demonstrující způsob provedeného útoku.[585]

V případě **DoS (Denial of Service)** je zdroj útoku jeden. Tomuto typu útoku je relativně snadné se ubránit, neboť je možné blokovat provoz ze zdroje útoku.




U **DDoS** (**Distributed Denial of Service** - distribuované odepření služby) dochází k zahlcení cílového počítačového systému **odesíláním paketů z více počítačových systémů, které jsou různě geograficky umístěny, což ztěžuje obranu a identifikaci útočníka**. Takové útoky byly užity např. proti Yahoo! Inc., elektronickým obchodům aj.[586] Velmi často jsou k tomuto typu útoků využívány botnety či aktivity uživatelů podporujících určitou online kampaň (viz dále – Anonymous a LOIC).

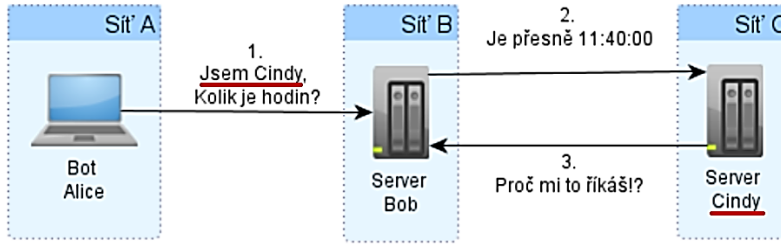



585: Obrázky byly získány z prezentace: PADRTA, Aleš. *Zamyšlení nad aktuálními bezpečnostními problémy*. [online]. [cit.18.8.2016]. Dostupné z: http://www.saferinternet.cz/attachments/article/457/CESNET_aktualni_bezpecnostni_problemy.pdf

586: Dále například DoS útoky na webové stránky prezidentského úřadu, parlamentu, ministerstev, redakcí sdělovacích prostředků a dvou estonských bank - Estonsko (2007). *Estonia recovers from masive DDoS attack.* [online]. [cit. 4. 3. 2010] Dostupné z: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

V případě **DRDoS** (**Distributed Reflected Denial of Service** – Distribuované, odražené popření služby) se jedná o podvržený distribuovaný DoS útok, který využívá mechanismus tzv. odražení. Útok spočívá v rozeslání podvržených požadavků na spojení na velké množství počítačových systémů, které poté na tyto požadavky odpoví, ovšem ne iniciátorovi spojení, ale oběti. Podvržené požadavky na spojení mají totiž jako zdrojovou adresu uvedenou adresu oběti, která je pak zahlcena odpověďmi na tyto požadavky. Řada počítačových systémů se tak stává nedobrovolným účastníkem útoku vlastně tím, že korektně odpoví na žádost o navázání spojení.

DoS, DDoS, DRDoS útoky velmi často využívají chyby například v operačním systému, spuštěných programech či síťových protokolech - UDP, TCP, IP, http aj.




Existuje několik základních metod DoS či DDoS útoku, přičemž mezi nejznámější patří:[587]

**Zahlcení příkazem ping** (*Ping-Flood*)
Díky protokolu Internet Control Message Protokol a nástroje Ping (Packet Internet Groper) je možné příkazem „ping" zjistit „živost" počítačového systému s danou IP adresou a detekci času odezvy takového systému. V rámci útoku Ping-Flood dochází k zahlcení oběti velkým množstvím tzv. ICMP Echo Request paketů, na které oběť začne odpovídat - posílat tzv. ICMP Echo Replay pakety. Útočník doufá, že se tím oběti zahltí šířka pásma (pro příjem i odesílání dat). Vlastní útok je možné ještě zesílit tím, že se pingu emitujícímu ICMP pakety nastaví možnost flood (záplava). Dané pakety se poté začnou odesílat, aniž by čekaly na odpovědi. Pokud je cílový počítačový systém málo výkonný, je možné jej takto učinit nedostupným.

**Zahlcení volných systémových prostředků** (*SYN-Flood*)
SYN-Flood je druh útoku, kdy se útočník snaží svoji oběť zahltit velkým množstvím žádostí o navázání spojení. Útočník pošle posloupnost paketů s příkazem SYN (tzv. SYN pakety) cílovému počítačovému systému (oběti), přičemž cílový systém na každý SYN paket odpoví zasláním SYN-ACK paketu, avšak útočník již dále neodpovídá. Cílový počítačový systém čeká na finální potvrzení, tzv. ACK paket od iniciátora spojení (útočníka) a drží pro toto spojení

587: Blíže srov. JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 66.

alokované zdroje, kterých má ale omezené množství. Tím může dojít k vyčerpání systémových zdrojů cíle útoku.[588]

**Falšování zdrojové adresy** (*IP spoofing*)
IP Spoofing představuje aktivity spočívající v podvrhávání (falšování) zdrojové adresy odesílaných paketů, kdy útočník iniciující spojení ze stroje A s **IP dresou a.b.c.d** jako zdrojovou adresu do odesílaných paketů vloží např. **IP adresu d.c.b.a**. a odešle je cíli B. Cíl B pak odpovídá na tuto zdrojovou adresu, tzn. odpověď neadresuje na IP adresu a.b.c.d, ale adresuje ji na IP adresu **d.c.b.a**. Pomocí této metody lze zhoršovat (zesilovat) útoky typu DoS, DDoS. Útočník tuto techniku používá tehdy, když na svoji žádost o navázání spojení nepotřebuje od cíle odpověď, pouze jej chce zaměstnat. Když útočník jako zdrojovou IP adresu do odesílaných paketů uvede IP adresu cíle svého útoku (např. a.a.a.a) a pakety vyšle na mnoho jiných počítačových systémů (IP adres), tyto pak odpovídají počítačovému systému a.a.a.a. Tímto způsobem se realizuje útok typu DRDoS.

**Smurf attack**
Tento útok je realizován prostřednictvím chybné konfigurace systému, který povolí rozesílání paketů všem počítačům zapojeným v počítačové síti skrze broadcast adresu.

Cílem útoků typu DoS/DDoS obvykle **není infikovat počítač**, respektive počítačový systém, **nebo překonat bezpečnostní ochranu např. heslem**, které jej chrání, ale pomocí série opakovaných požadavků **jej buď zahltit, či dočasně vyřadit z provozu**. Typicky tak dojde k omezení či zablokování přístupu ke službám.

Pro to, aby bylo možné „útočníka" DoS či DDoS útoků právně postihnout, je třeba určit, zda jeho **jednání bylo protiprávní**, a pokud ano, jak moc závažné toto jednání bylo. Jde o to, že povahu DDoS útoku může mít například i zcela korektní činnost uživatelů Internetu, kteří se v jeden okamžik (v krátkém časovém období) snaží připojit např. na webový server společnosti, která poskytuje slevy na letenky a kupř. oznámila, že od 12.00 hod dojde k plošnému snížení

588: Na tomto místě je třeba zmínit **Handshake** - proces, jehož úkolem je nastavit parametry komunikačního kanálu mezi dvěma subjekty před zahájením vlastní komunikace. Handshake je například používán v Internetu pro otevření TCP spojení (tzv. „**třícestný handshake**", tj. výměna tří datagramů) a teprve poté následuje vlastní přenos dat.
K navázání TCP spojení jsou požadovány tři oddělené kroky:

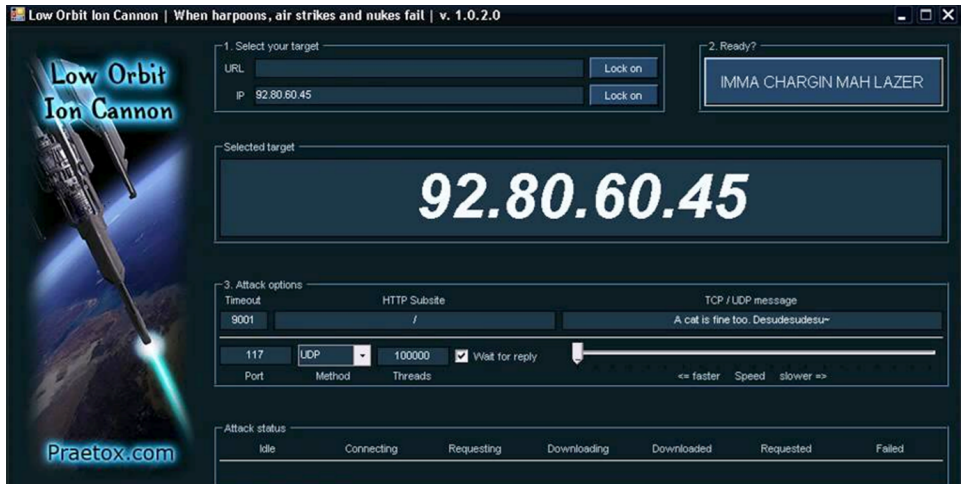
1) Strana zahajující spojení (klient) vyšle TCP segment s nastaveným příznakem SYN.
2) Strana přijímající spojení (server) odpoví TCP segmentem s nastavenými příznaky SYN+ACK.
3) Klient odpoví TCP segmentem s nastaveným příznakem ACK.

Další TCP segmenty mají již nastaven pouze příznak ACK.
Blíže viz např. *TCP handshake krok za krokem*. [online]. [cit. 18. 8. 2016]. Dostupné z:
http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000
Existují i další způsoby DoS útoku, např. „TearDrop", „Nuke", „Peer-to-Peer útok", atd. Blíže srov. [online].
[cit. 25. 9. 2010]. Dostupné z: http://cs.wikipedia.org/wiki/Denial_of_Service

letenek o 75 %. Nebo může jít o přístup velkého množství uživatelů na webovou službu některého z populárních médií, které referují o významné nebo mediálně zajímavé události – nástupu nového prezidenta, úmrtí významné osobnosti apod. Pokud je cílový počítačový systém (webserver) nedostatečně dimenzován nebo je špatně nakonfigurován (není schopen odbavit požadovanou sumu přístupů), dojde k jeho „kolapsu" obdobně, jako tomu je u cíleného DDoS útoku. Je pak otázkou, zda by se měli postihovat uživatelé, kteří se na uvedený web snažili v daný čas přihlásit, a tím de facto způsobili odstavení předmětné služby.

Domnívám se, že v nastíněných případech, byť uživatelé způsobili masivní DDoS útok na službu poskytovatele, není reálné, ba ani myslitelné, tyto „pseudoútočníky" postihnout jakýmikoli prostředky práva, neboť jejich jednání nebylo od počátku protiprávní.

Odlišným případem by však byla situace, kdy se útočníci např. prostřednictvím Internetu svolávají a v konkrétní čas, díky svému opětovnému přihlašování k poskytované službě, tuto službu potlačí.[589] K takovýmto případům docházelo např. v rámci protestů proti ACTA (Anti-Counterfeiting Trade Agreement) v roce 2012, kdy jednou z možností pro páchání uvedených útoků bylo využít prostředek, distribuovaný přívrženci hnutí Anonymous, LOIC (Low Orbit Ion Cannon).

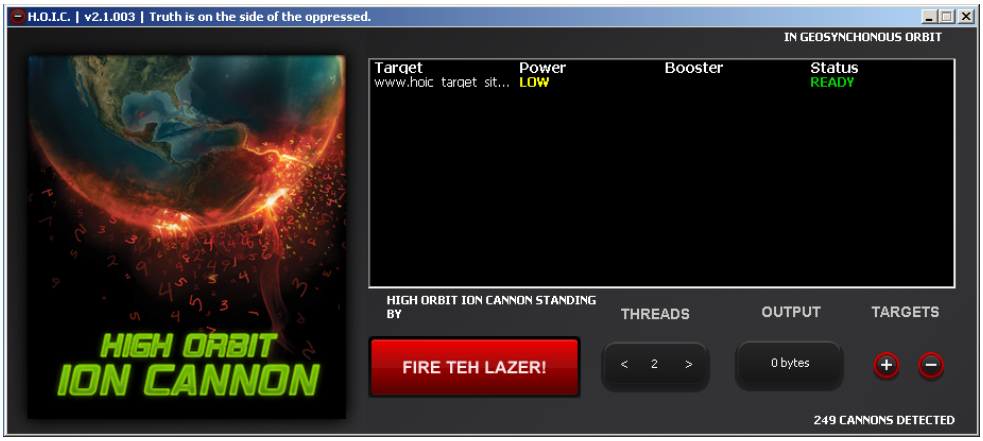



Obrázek 75: LOIC (Low Orbit Ion Cannon)[590]

589: Může jít i o případ, kdy útočník rozešle hoax typu „*6. 6. 2016 od 12 do 13 budou letenky u Lufthansy zadarmo! Pro více informací klikni sem.*"

590: *LOIC*. [online]. [cit. 18. 8. 2016]. Dostupné z: https://i.ytimg.com/vi/QAbXGy0HbrY/maxresdefault.jpg

Pomyslným nástupcem LOIC pak byl software HOIC (High Orbit Ion Canon), který byl vyvinut jako náhrada za LOIC.




Obrázek 76: HOIC (High Orbit Ion Canon)[591]

Jednání útočníků v tomto případě zcela jistě protiprávní je, neboť tito útočníci si byli vědomi nebo alespoň byli srozuměni s tím, že svým jednáním zasahují do práv jiných osob. V tomto případě by bylo možné využít prostředky trestního, správního i občanského práva.

Díky přijetí Úmluvy o kyberkriminalitě by mělo nejen v členských zemích EU docházet k harmonizaci zejména trestního práva a přijetí takových právních norem, které by měly být schopné postihnout DoS či DDoS útoky prostředky trestního práva té které země. K ochraně před těmito útoky a implementaci legislativních opatření vyzývá Kapitola II – Opatření, která mají být přijata na vnitrostátní úrovni, Oddíl 1 – Trestné činy proti důvěrnosti, integritě a použitelnosti počítačových dat a systémů, Čl. 4 – Zasahování do dat, uvedené úmluvy:

1) *Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně neoprávněné poškození, vymazání, snížení kvality, pozměnění* ***nebo potlačení počítačových dat****.*

2) *Strana si může vyhradit právo stanovit, že bude považovat jednání popsané v odstavci 1 za trestné, jen pokud způsobí závažnou škodu.*

591: *HOIC.* [online]. [cit. 18. 8. 2016]. Dostupné z: https://npercoco.typepad.com/.a/6a0133f264aa62970b0167612ea130970b-pi

Otázkou však je, jak efektivně a doslovně je tato celkem jasná výzva transformována do právní úpravy signatářské země. Například v České republice došlo v roce 2009 k masivní rekodifikaci trestního práva, včetně včlenění nových skutkových podstat trestných činů, které se týkají kybernetických útoků. Avšak zřejmě díky neznalosti technické stránky věci či díky potřebě „právního popsání" jednání, které má povahu DoS či DDoS útoků, došlo ke vzniku právní normy, která v praxi postih za provedení útoku DoS či DDoS neumožňuje.

Ze znění ustanovení **§ 230 odst. 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK vyplývá:

***Kdo získá přístup k počítačovému systému*** *nebo k nosiči informací a*

*a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,*

***b) data*** *uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní,* ***potlačí****, sníží jejich kvalitu nebo je učiní neupotřebitelnými…*

Z uvedeného ustanovení vyplývá, že útočník páchající DoS či DDoS útok musí, aby byl případně trestně odpovědný, **neoprávněně získat přístup k počítačovému systému a následně v něm data potlačit**.[592]

V tomto případě de facto došlo ke spojení dvou samostatných článků (Kapitola II, Oddíl 1, **Čl. 2 – Nezákonný přístup a Čl. 4 – Zasahování do dat**) Úmluvy o kyberkriminalitě v ustanovení jedno.

Zákonodárce tímto de facto znemožnil postih pachatelů DoS či DDoS útoků prostředky trestního práva, neboť po pachateli je vyžadováno, aby **neoprávněně získal přístup k počítačovému systému**. Tato právní interpretace vyžadující získání neoprávněného přístupu k počítačovému systému tak umožňuje postih pachatele pouze pro jednání uvedené v Úmluvě o kyberkriminalitě v **Čl. 2 – Nezákonný přístup:** „*Každá strana přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů byl trestným činem, pokud je spáchán úmyslně,* ***neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části.***"

Z technického hlediska při DoS či DDoS útocích **nedochází** k získání přístupu k počítačovému systému nebo jeho části, nebo to alespoň není primárním cílem.[593]

592: Potlačením je rozuměna ta činnost, která je uvedena v čl. 4 Úmluvy o kyberkriminaltě.

593: Pokud je např. k DoS či DDoS útoku využito PING Floodu, pak si je možné celou situaci představit jako neustálé volání (a následné zavěšení) na konkrétní telefonní číslo. Tím dojde k situaci, kdy napadené telefonní číslo nemá možnost uskutečnit hovor vlastní (dochází k blokaci funkce volání), avšak žádný z volajících (útočníků) nezíská žádné údaje uložené v napadeném telefonu.

Z výše uvedených důvodů jsem přesvědčen o nutnosti včlenit do právní úpravy ČR samostatnou skutkovou podstatu trestného činu, která by chránila počítačový systém právě před útoky DoS, DDoS, DRDoS aj. a která by zejména respektovala ustanovení Úmluvy o kyberkriminalitě. Bylo by možné užít např. následující znění:

***„Kdo bez oprávnění brání užívání počítačového systému…"***

V současnosti by bylo teoreticky možné postihnout pachatele DoS a DDoS útoků za trestný čin dle **§ 228** (poškození věci) TZK.[594] Podmínkou pro využití institutu poškození věci by však musel být fakt, že by taková věc (tedy i počítačový systém) byla zničena, poškozena, nebo učiněna neupotřebitelnou. Uvedená podmínka však u tohoto typu útoku přichází v úvahu zpravidla pouze co se týče určité dočasné neupotřebitelnosti.

V této souvislosti však vyvstává i otázka, jak a jakým způsobem bude v případě poškození věci vyčíslována skutečně vzniklá škoda a na kom bude vymáhána.[595]

Mezi další skutkové podstaty, jichž by se útočník páchající útok typu DoS a DDoS mohl za určitých okolností dopustit, je možné zařadit § 272 (Obecné ohrožení), § 273 (obecné ohrožení z nedbalosti) TZK.[596]

Z hlediska případného trestněprávního postihu pachatele DoS či DDoS útoků je významné i určení (identifikace) pachatele tohoto konkrétního trestného činu. Zůstává otázkou, **kdo všechno by měl být trestněprávně postižen jako pachatel**, který např. způsobil nedostupnost určité služby (např. webové aplikace).

Je tímto pachatelem uživatel, který jako „poslední připojující se" způsobil pád služby? Či jsou za tento útok odpovědní v plné míře a nerozdílně všichni ti, kteří protiprávně službu potlačili, tzn. v úzkém časovém okně k ní přistupovali, pravděpodobně v dobré víře? Nebo je odpovědný pouze ten, kdo jiné vyzval (organizoval) k útoku na určitou službu a v jehož rukou se tím de facto všichni ostatní stali „živým nástrojem"? A do jaké míry je za útok odpovědný uživatel, jehož počítač se do útoku také zapojil, protože je infikován malwarem a je součástí botnetu, ze kterého je útok generován?

---

594: Viz § 228 odst. 1 TZK:

*„Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty."*

Škodou nikoli nepatrnou se rozumí škoda dosahující výše minimálně 5 000 Kč (viz § 138 odst. 1 TZK)

595: Bude tato škoda vymáhána na každém útočníkovi? Či bude tato škoda mezi útočníky „rozpočítána"?

596: O tyto dva trestné činy půjde zejména v případech, kdy dojde k zásahu do kritické infrastruktury [zejména kritické informační infrastruktury § 2 písm. g) a písm. i) zákona č. 240/2000 Sb., krizový zákon].

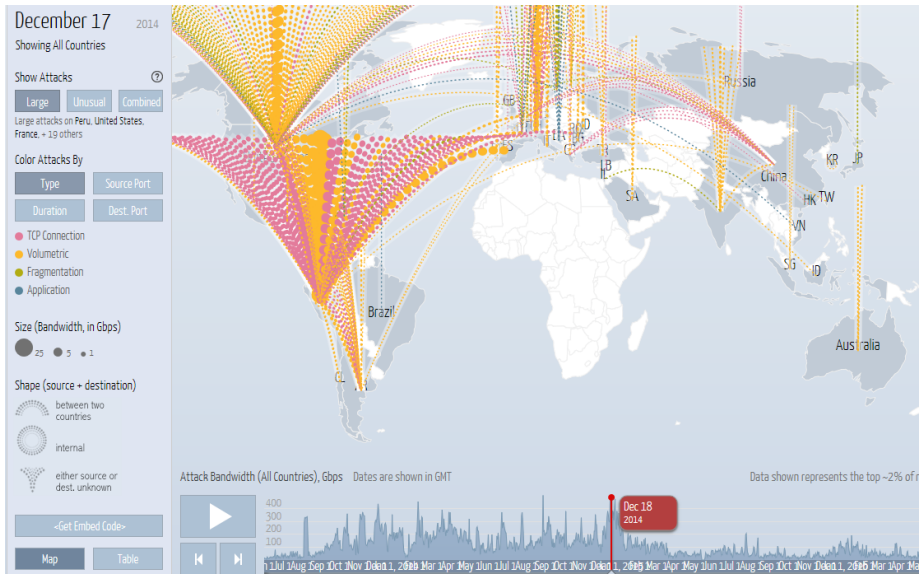
Možností je několik, avšak žádná z nich není zcela uspokojující. Případ, kdy bude postižen pouze organizátor celé „akce“ rozhodně není všespasitelný, neboť i jednotliví útočníci (připojující se osoby) si mohou být vědomi svého protiprávního jednání (viz útoky LOIC v roce 2012).

Představme si tedy soudní proces proti např. 50 tisícům uživatelů, jejichž počítač v průběhu útoku vygeneroval jeden požadavek na spojení s cílem útoku. Nejde pouze o množství 50 tisíc uživatelů, kteří by měli u případného soudního jednání vystoupit jako obžalovaní, ale také o to, jak těmto osobám nezpochybnitelně dokázat, že právě jejich spojení bylo legitimním požadavkem na danou službu nebo se z jejich strany jednalo o útok.

Postih všech účastníků DoS či DDoS útoků prostředky trestního práva není adekvátní, neboť trestní právo by mělo být prostředkem *ultima ratio* (krajním, nejzazším prostředkem). Stejně tak postih toho, kdo se jako poslední ke službě připojil, a tím způsobil její nedostupnost, je nevhodný, neboť tento „poslední“ nemusel jednat protiprávně (mohlo se jednat např. o náhodného legitimně se připojujícího). Nehledě na to, že není moc reálné stanovit, kdo tímto „posledním připojujícím se“ vlastně je.

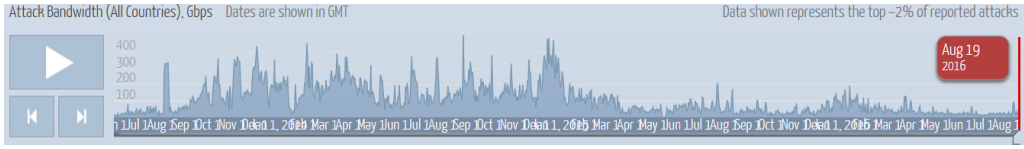
Asi nejjednodušší je postih útočníka, který k útoku úmyslně využije počítačový systém, ať již v podobě výkonného výpočetního centra, či např. jím ovládaného botnetu. V tomto případě leží plná trestněprávní odpovědnost pouze na jedné či několika málo osobách.

Útoky Anonymous a využití botnetů k útokům DDoS jasně demonstrovaly jejich potenciální sílu a nebezpečnost. DDoS útoky svého vrcholu dosahovaly zejména v letech 2012-2014 (viz Obrázek 77).




Obrázek 77: Digital Attack Map -Top daily DDoS attack worldwide (18. prosinec 2014)

V současnosti nejsou DDoS útoky využívány v takové masové míře jako dříve, nicméně se stále jedná o velmi účinný prostředek používaný útočníky. Na rozdíl od masových velkých celoplošných útoků se v současnosti můžeme setkat spíše s cílenými a velmi krátkou dobu trvajícími útoky (délka útoku 3–5 minut,[597] v tomto časovém rozmezí není napadený subjekt schopen nijak zareagovat).




Obrázek 78: Intentita DDoS útoků od 1. 7. 2013 do 19. 8. 2016[598]

597: Viz např. BHATTACHARYYA Dhruba Kumar a Jugal Kumar KALITA. *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance*. Chapman and Hall/CRC 2016. ISBN 978-1-4987-2965-9, s. 53
*Free DDoS Service! Max 5 min!* [online]. [cit.19.8.2016]. Dostupné z: http://hackforums.net/showthread.php?tid=3065539
Citace: *Hello Everyone! This is Lamborghini's free DDOS Service for everyone! This is a strong 1GBPS attack! I am offering a 5 Minute attack maximum ...*
598: *Digital Attack Map –Top daily DDoS attack worldwide.* [online]. [cit.19.8.2016]. Dostupné z: http://www.digitalattackmap.com/

## 4.13 Šíření závadového obsahu

V současné době lze vystihnout dva základní typy šíření závadového obsahu. Jedná se o **šíření zakázaných druhů pornografie** a o **šíření nenávistných a extremistických sdělení**.

V případě šíření **zakázaných druhů pornografie** jde zejména o šíření pornografického materiálu zobrazujícího styk se zvířetem a dále o šíření (resp. již pouhé držení) „dětské pornografie“[599] (materiál zobrazující nebo jinak využívající dítě - osobu mladší 18 let, či osobu, jež se jeví být dítětem). Vlastních způsobů šíření existuje nepřeberné množství. Od prostého nabízení tohoto druhu pornografie ke stažení přes umisťování těchto materiálů do prostředí Internetu, šíření pomocí výměnných počítačových sítí, zasílání pomocí e-mailů apod.

Zneužívání dětí k výrobě pornografických materiálů a následná distribuce těchto materiálů je jednou z forem trestné činnosti, k jejímuž stíhání se zavázala většina států světa, bez ohledu na to, zda ratifikovala či neratifikovala Úmluvu o kyberkriminalitě. Byť je v této oblasti vyvíjena značná aktivita (nejen ze strany států, neziskových organizací a dalších osob[600]), zůstává problém sexuálního zneužívání dětí online neustále aktuální.

Fenomén dětské pornografie provází společnost od prvních okamžiků, kdy bylo možné zachytit vlastní zneužívání na jakékoliv médium (papír, film aj.). Pravdou však je, že Internet umožnil masové šíření takovýchto materiálů mezi jednotlivými uživateli, stejně jako jejich větší míru anonymity.

Problém, který představuje Internet a kyberprostor, souvisí s dříve uvedeným tvrzením, že „*Internet nezapomíná*“. Pokud je jakýkoli materiál nahrán, či přenesen prostřednictvím ICT, vždy může někde existovat kopie tohoto materiálu. Příkladem z České republiky, kdy sami uživatelé vytváří materiál, který zobrazuje nahé děti, může být portál www.rajce.net. Tento portál rozhodně nebyl vytvořen jako prostředí pro distribuci jakéhokoliv pornografického či jinak závadného materiálu (k tomuto účelu existují jiné stránky), avšak uživatelé nerespektují ani základní pravidla služby rajce.net, zejména čl. 13, který uvádí:

„***Obsah zobrazující nahé osoby, zejména mladší 18 let, je na Rajče povoleno umisťovat pouze do soukromých alb s heslem;*** *ostatní ustanovení těchto pravidel, zejména zákaz umisťovat na Rajče pornografický obsah nebo obsah neoprávněně zasahující do práva na ochranu osobnosti třetích osob, zůstávají i v takovém případě nedotčena.* “

599: **Jedná se o vžitý pojem** používaný mimo jiné i trestním zákoníkem (viz § 192 a násl. TZK), **nicméně korektnější** a výstižnější **by bylo toto jednání označit jako zneužívaní dítěte.**
K vlastnímu vymezení a postihu dětské pornografie viz kap. 5.2.2.3.1 Trestné činy související s dětskou pornografií (čl. 9).
600: Viz kap. 4.14.2 Kybergrooming.

Přesto je možné na tomto webu nalézt celou řadu fotografií, byť vytvořených s dobrým úmyslem (například šíření fotografií mezi členy rodiny žijícími daleko od sebe), které jsou atraktivní pro kohokoliv, včetně případného útočníka. Díky dalším informacím, které jsou uveřejněny na tomto portálu, případně díky korelaci dat z jiných zdrojů dostupných online, je pro útočníka mnohem snazší například nalézt potenciální oběť.

Problém nepředstavuje ani tak nahrání fotografií nahých osob (s vědomím replikace dat), ale ta skutečnost, že tato data jsou otevřena všem uživatelům, nikoli pouze úzce omezené skupině (např. již zmiňované rodině).[601]

Obrázek 79: Fotografie z rajce.net (fotografie je volně dostupná všem uživatelům)

Závěrem chci uvést, že rozhodně nemám nic proti focení dětí (případně sdílení některých fotografií s nejbližší rodinou) z důvodu uchování krásných vzpomínek. To, co mi vadí, je hloupé bezmyšlenkovité zpřístupňování těchto fotografií komukoliv v kyberprostoru.

601: Dále viz např. VOKROUHLÍKOVÁ Kateřina a Zuzana PRŮCHOVÁ. *Naháči a prdeláči – fotky jen pro rodinu!* [online]. [cit. 19. 8. 2016]. Dostupné z: https://blog.nic.cz/2016/08/16/nahaci-a-prdelaci-fotky-jen-pro-rodinu/
Pro osobu zveřejňující fotografii nahého dítěte (typicky rodiče) by mělo být dostatečným varováním, že návštěvnost alb s koupajícími dětmi se hravě přehoupne přes 10 000, zatímco jiná např. krajinky dosáhnou stěží na 200 shlédnutí. Obliba dětských fotek v tomto případě bohužel není dána uměleckou kvalitou, ale právě specifickým typem návštěvníků, mezi kterými jsou často i útočníci, kteří fotky dále snadno zneužívají.

Jedním z projektů z poslední doby, který se věnoval problematice zneužívání dětí online, byl počin nizozemské společnosti Terre des Hommes Netherlands (THN). Tato společnost vytvořila virtuální desetiletou Filipínku **Sweetie**. Sweetie deset dní komunikovala na internetových chatech a byla oslovena přibližně dvaceti tisíci muži. Tisíc z nich jí nabídlo peníze výměnou za online sex.

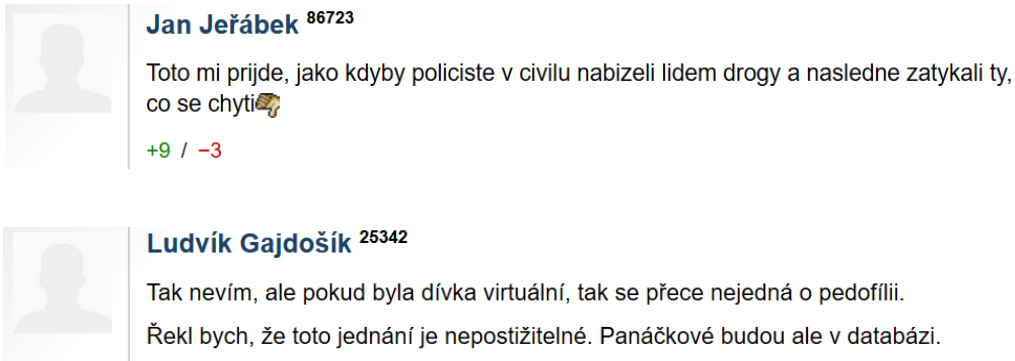
Šéf projektu Hans Guyt na tiskové konferenci v Haagu řekl, že tento typ zločinu vyžaduje nový způsob policejní práce. „*Predátoři ani jejich oběti nám při vyšetřování naproti nepřijdou,*" uvedl.

„*Vytvořili jsme virtuální identitu, která představovala desetiletou Filipínku.*"

*"Nikoho jsme nelákali, dokud nám sami nenabízeli peníze,*" řekl Guyt.

Aktivisté chtěli tímto způsobem upozornit na rostoucí problém zneužívání dětí prostřednictví webkamer. Tento fenomén nazývají „*internetovou sexuální turistikou.*"[602]

Co je z mého pohledu zarážející, jsou některé reakce v rámci diskusí. Mnoho lidí zřejmě stále žije v představě, že virtuální svět je něco odtrženého, neprovázaného se světem reálným. Namátkově jsou vybrány některé příspěvky z diskuse uveřejněné na iDnes.cz, obdobné reakce však provázely uveřejnění výsledku projektu Sweetie i na jiných diskusních fórech po celém světě:




602: Blíže viz: *Computer-generated 'Sweetie' catches online predators.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.bbc.com/news/uk-24818769
*Nizozemci vytvořili virtuální dívku. Pomohla lapit přes tisíc pedofilů.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-/zahranicni.aspx?c=A131106_210025_zahranicni_zt
Video se **Sweetie** je dostupné online: https://www.youtube.com/user/sweetie.

**Michael Mensik** [81602]

Aniž bych se chtěl jakkoli zastávat úchylů, kteří třeba ubližují dětem - obávám se, že je ta akce mírně řečeno postavená na velice vratkých základech a může opravdu zničit život spoustě lidí jen kvůli potřebě zviditelnění nějaké podivné neziskovky.

**Vladimír Holý** [84167]

Takže ty skutečné holčičky, které tímto způsobem pomáhají živit rodiny, budou muset jít vydělávat na ulici, protože teď se je budou peďáci bát na netu kontaktovat. To se fakt povedlo.

**Petr Heller** [53644]

Jak už jsem psal jinde, tak Terre des Hommes Netherlands se zcela jistě dopustili trestného činu šíření dětské pornografie. Není důležité, jestli nabízeli živé nebo virtuální dítě, pokud je trestné držení kreslené dětské pornografie, tak musí být trestná i její distribuce, čehož se zcela jistě dopustili.

Takže očekávám jejich okamžité zatčení a jasný trest!

V případě vytváření, držení či šíření materiálů, subsumovatelných pod pojem dětské pornografie, je možný postih uživatele dle **§ 192** (Výroba a jiné nakládání s dětskou pornografií), **§ 193** (Zneužití dítěte k výrobě pornografie) TZK. Trestná je i účast na pornografickém představení nebo jiném obdobném vystoupení, ve kterém účinkuje dítě (**§ 193a** TZK). Trestné je také získání přístupu k dětské pornografii prostřednictvím informační nebo komunikační technologie (**§ 192 odst. 2** TZK).

Trestný je i případ, kdy uživatel vyrobil, dovezl, vyvezl, provezl, nabídl, učinil veřejně přístupným, zprostředkoval, uvedl do oběhu, prodal nebo jinak jinému opatřil fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem (**§ 191 odst. 1** TZK).

V případě **šíření nenávistných a extremistických sdělení** jde zejména o podporu a propagaci hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka, projevy sympatií s takovým hnutím, hlásání rasové, etnické a národnostní, náboženské nebo třídní zášti či zášti vůči jiné skupině osob. Dále je sem řazeno šíření pomluv pomocí prostředků informačních technologií a v neposlední řadě též zasílání obtěžujících zpráv spadajících pod pojem stalking, resp. cyberstalking.

V těchto případech se může jednat o celou řadu trestných činů, jako jsou např. **§ 184** (Pomluva), **§ 353** (Nebezpečné vyhrožování), **§ 354** (Nebezpečné pronásledování), **§ 355** (Hanobení národa, rasy, etnické nebo jiné skupiny osob), **§ 356** (Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod), **§ 403** (Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka), **§ 404** (Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka), **§ 405** (Popírání, zpochybňování, schvalování a ospravedlňování genocidia) TZK.

## 4.14 Kybernetické útoky na sociálních sítích

V prostředí sociálních sítí je možné páchat většinu již dříve popsaných kybernetických útoků (např. malware, phishing, spam aj.). Důvodem, proč jsou kybernetické útoky na sociálních sítích popsány samostatně, je ta skutečnost, že se primárně (nikoliv však výhradně) odehrávají právě v prostředí sociálních sítí.

Mezi tyto specifické útoky je možné zařadit:

1) Kyberšikanu
2) Kybergrooming
3) Sexting
4) Kyberstalking

### 4.14.1 Kyberšikana

Šikana ve světě reálném spočívá ve snaze útočníka ublížit, ponížit, zesměšnit, urazit jiného, ať fyzicky či psychicky. Kyberšikana pak přenáší „klasickou šikanu" do světa virtuálního a umožňuje útočníkovi použít nástroje a prostředky, které mohou mít mnohem větší dopad na oběť než by tomu bylo ve světě reálném. Kyberšikana díky používání informačních a komunikačních technologií a trvanlivosti dat v kyberprostoru umožňuje opakované útoky na oběť, a to i v případě, že se oběť ve světě reálném geograficky značně vzdálila od místa, kde byla původně šikanována.

Kyberšikana může být propojena se šikanou „klasickou" (např. nahrávání fyzického napadení oběti a následné umístění tohoto útoku na web). Pro to, abychom mohli hovořit o kyberšikaně, je nutné, aby k šikanování byly použity informační a komunikační technologie či služby nabízené v kyberprostoru.

**Mezi znaky kyberšikany je možné zařadit:**

- **Pocit anonymity** (Útočník má zpravidla pocit, že jej díky Internetu není možné dohledat.)
- **Neomezenost útoku** (Díky ICT nemusí útočník řešit ani čas ani prostor pro svůj útok. Je možné šikanovat kdykoliv, odkudkoliv a kohokoliv. Vlastní útok také vyžaduje mnohem méně úsilí, než je tomu v případě šikany „klasické".)
- **Neomezený okruh útočníků** (Na rozdíl od světa reálného, ve světě virtuálním nezáleží na věku, pohlaví, fyzické síle, postavení útočníka ve skupině aj. Šikanujícím může být jakákoli osoba.)
- **Neomezený prostor a prostředky** (Internet poskytuje útočníkovi de facto neomezený prostor a prostředky pro šikanování. Útočník může opakovaně vyvěšovat urážlivé poznámky, komentáře fotografie a videa na různých portálech, sociálních sítích aj. Tyto materiály může vylepšovat a „zdokonalovat".)
- **Obtížná zjistitelnost** (Na rozdíl od šikany klasické nemusí mít kyberšikana vnější projevy jako jsou podlitiny, chybějící peníze atd.)
- **Trvalost** [Klasická šikana se většinou sestává z jednotlivých útoků, které se sice opakují, ale dílčí útok pro oběť vždy skončí. U kyberšikany stačí např. jedna SMS, e-mail apod., oběť se k nim stále vrací (respektive jsou jí neustále připomínány, zasílány aj.), může tak i měsíce žít v traumatu. Útočné SMS, e-maily, fotografie apod. jsou trvalejší než jednotlivé fyzické útoky.][603]

**Nejčastější projevy kyberšikany:**

1) Pomlouvání, zastrašování, urážení, zesměšňování či jiné ztrapňování (sociální sítě, e-mail, SMS, chat, ICQ, Skype, hry aj.).
2) Pořizování zvukových záznamů, videí či fotografií, jejich grafické či jiné upravování a následné zveřejňování s cílem poškodit (zesměšnit) vybranou osobu.
3) Natáčení videí, při kterých je oběť napadána fyzicky či je jinak psychicky týrána a zesměšňována. Tato videa jsou následně zveřejněna online (jedná se o tzv. Happy Slapping).

---

603: Srov. *Co je to kyberšikana a jak se projevuje?* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html
Blíže o kyberšikaně viz např. *Kyberšikana I, II.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

4) Vytváření internetových stránek, sociálních účtů (úprava původních či vytváření nových profilů), diskusních portálů aj., které urážejí, pomlouvají nebo ponižují konkrétní osobu.

5) Zneužívání cizího účtu - krádež identity (e-mailového, diskuzního apod.).

6) Provokování a napadání uživatelů v diskuzních fórech (chatovací místnosti apod.).

7) Odhalování cizích tajemství.

8) Vydírání pomocí mobilního telefonu nebo Internetu.

9) Obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním.[604]

**Důsledky některých útoků:**

- **Amanda Todd** (15 let). Příběh, který se Amandě stal, je možné nalézt na jejím vlastním videu dostupném na: http://www.youtube.com/watch?v=qDIKB2_RpuY.
  Amanda spáchala sebevraždu.

- **Rebecca Ann Sedwicková** (12 let), byla téměř rok šikanována na Internetu, spáchala v roce 2013 sebevraždu. Šikana začala poté, co Rebecca nějakou dobu chodila s jedním chlapcem. Její matka novinářům řekla, že dcera dostávala vzkazy jako: „Jsi hnusná", „Proč ještě žiješ?" a „Jdi se zabít". Situace se tak vyhrotila, že matka odhlásila dceru ze školy z Crystal Lake a zrušila její účet na Facebooku. Ze školy prý musela odejít. Zbytek roku ji matka učila doma. V září nastoupila do jiné školy. Zdálo se, že se vše obrací k lepšímu, a Rebecca v nové škole pookřála. Ale tajně se přihlásila k novým aplikacím včetně telefonního posílání zpráv Kik Messenger a Ask.fm a šikana začala nanovo poté, co se na Internetu začala dotazovat na nadváhu. Šerif Judd uvedl, že dívka byla na sociálních sítích „naprosto terorizována".[605]

- **Ghyslain Raza** (14 let, Kanada), známý jako Star Wars Kid.
  https://www.youtube.com/watch?v=HPPj6viIBmU&spfreload=10.
  Ghyslain Raza natočil sám sebe při předvádění bojové scény z Hvězdných válek. Snažil se napodobit postavu Dartha Maula. Spolužáci mu nahrávku ukradli a pro pobavení ostatních ji zveřejnili na Internetu. Během několika týdnů nahrávka obletěla celý svět, byla mnohokrát upravována, vzniklo množství webů a blogů, na kterých byl chlapec zesměšňován.

604: Srov. dále: *Víte co je KYBERŠIKANA?* [online]. [cit. 19. 8. 2016]. Dostupné z:
http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

605: *Dvanáctiletá dívka se zabila po téměř roční šikaně na internetu.* [online]. [cit. 19. 8. 2016]. Dostupné z:
https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html
http://www.ceskatelevize.cz/ct24/svet/246314-dalsi-sebevrazda-kvuli-socialnim-sitim-divka-skocila-z-veze/

Ghyslainovi fanoušci napsali petici tvůrcům Hvězdných válek, aby byl obsazen do některé z epizod. Byl parodován dokonce v seriálech (např. South Park, American Dad, Veronica Mars). Ghyslain se psychicky zhroutil a musel se dlouhodobě léčit.[606]

- **Anna Halman** (14 let, Polsko). Pět spolužáků podrobilo Annu před celou třídou sexuální šikaně (strhali z ní šaty a předstírali, že ji znásilňují). Celou scénu nahráli na mobil a vyhrožovali dívce, že nahrávku zveřejní na Internetu. To také později udělali, video umístili na stránku YouTube. Pro Annu to měla být pomsta za to, že s jedním z chlapců nechtěla chodit. Anna spáchala sebevraždu.[607]

- **Jessica Logan** (18 let, USA). Po rozchodu zveřejnil Jessičin bývalý přítel její intimní fotografie, které mu poslala v době, kdy spolu ještě chodili. Jessica pak byla vystavena neustálému posměchu ze strany spolužáků. Útoky na ni ještě zesílily poté, co anonymně vystoupila v televizi, aby ostatní upozornila na rizika sextingu. Jessica spáchala sebevraždu.[608]

- **Oldřiška** (9 let, ČR). Její video je na Internetu k nalezení pod odkazem *Hledám kluka z autobusu*. Zveřejnění videa zcela změnilo dívčin život. Začala být zesměšňována, ponižována nejen v kyberprostoru, ale i v reálném životě. Oldřiška byla nucena mimo jiné vyhledat psychologickou pomoc.

Kyberšikana (stejně jako klasická šikana) sama o sobě není trestným činem ani přestupkem. Vždy záleží na jednání, kterým útočník šikanoval. Pokud toto jednání mělo podobu například fyzického ublížení oběti, jejímu vydírání či zastrašování, pak by mohlo přicházet v úvahu uplatnění například **§ 146** (Ublížení na zdraví) či **§ 145** (Těžké ublížení na zdraví), **§ 175** (Vydírání) TZK. V případě obtěžování a pronásledování osoby by bylo možné využít ustanovení **§ 354** TZK (Nebezpečné pronásledování). Avšak u kyberšikany, která se může projevovat například neustálým zesměšňováním, ztrapňováním a psychickým ubližováním prostřednictvím informačních a komunikačních technologií, bude aplikace některých výše uvedených ustanovení problematická, ne-li přímo nemožná.

### 4.14.2 Kybergrooming

Kybergrooming je jednání, které představuje psychickou manipulaci s osobou (typicky za použití sociálního inženýrství), realizovanou prostřednictvím Internetu či informačních a komunikačních

606: *Kyberšikana I, II.* [online]. [cit. 19. 8. 2016]. Dostupné z:
https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy
607: *Kyberšikana I, II.* [online]. [cit. 19. 8. 2016]. Dostupné z:
https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy
Dále pak: *Jessica Logan – The rest of the Story.* [cit. 8. 8. 2016]. Dostupné z: http://nobullying.com/jessica-logan/
608: Tamtéž.

technologií (např. mobilních telefonů aj.). Účelem kybergroomingu je vyvolat v oběti falešnou důvěru a přimět ji tak k osobní schůzce. Výsledkem této schůzky může být jakýkoli fyzický, sexuální či jiný útok na oběť. Oběťmi kybergroomingu mohou být děti, ale i dospělé osoby.[609] Nejčastějšími oběťmi jsou dle statistik dívky ve věku 13–17 let.[610]

*„Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu – od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Existují případy, kdy predátor manipuloval dítě po dobu 2–3 let, než došlo k osobnímu setkání a sexuálnímu zneužití. Je třeba rovněž zohlednit hranici zletilosti dítěte – útočník může s dítětem komunikovat v době, kdy bylo nezletilé, k útoku však dojde až po završení zletilosti (je zjevné, že trestní sazby za sexuální zneužití zletilého a nezletilého dítěte jsou velmi rozdílné).* "[611]

**Kybergrooming má různé etapy:**

1) Vzbuzení důvěry a snaha izolovat oběť od okolí (útočník mění svoji identitu, je velmi trpělivý)
2) Podplácení dárky či různými službami, budování kamarádského vztahu
3) Vyvolání emoční závislosti oběti na osobě útočníka
4) Osobní setkání
5) Sexuální obtěžování, zneužití dítěte či jiný útok[612]

**Rizikovou skupinu dětí tvoří:**

1) *adolescenti/teenageři* (zajímá je lidská sexualita, jsou ochotni o ní hovořit),
2) *děti s nízkou sebeúctou nebo nedostatkem sebedůvěry* (lze je snadněji citově či fyzicky izolovat),
3) *děti s emocionálními problémy, oběti v těžké životní situaci* (často hledají náhradu za své rodiče a potřebují pomocnou ruku),
4) *děti naivní a přehnaně důvěřivé* (jsou ochotnější zapojit se do online konverzace s neznámými lidmi, obtížněji rozpoznávají rizikovou komunikaci).[613]

609: *Riziková komunikace: Kybergrooming* [online]. [cit. 19. 3. 2014]. Dostupné z: http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming

610: CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, [cit. 19. 3. 2014]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

611: KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit.19.3.2014]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

612: *Kybergrooming.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

613: KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit. 19. 3. 2014]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

Pokud jde o prevenci kybergroomingu, tak na možná rizika upozorňují materiály prezentované v rámci projektů **Seznam se bezpečně 1, 2, 3** dostupné na: http://www.seznamsebezpecne.cz/ či projekty Saferinternet.cz, e-bezpeci.cz[614] aj.

Ve Velké Británii působí i dobrovolné organizace zvané Paedophile hunters. Tyto organizace vytvářejí falešné účty (typicky se prezentující jako nezletilé dívky) na sociálních sítích a v rámci chatu a v případě, že jsou osloveni útočníkem, domluví osobní setkání, které je natáčeno. Veškeré záběry a další data jsou předána policii.[615] Příklad takovéhoto setkání je možné nalézt na uvedených Facebookových účtech a dále pak např. na URL: https://www.youtube.com/watch?v=JAnJnGBdYc0.

Osoba dopouštějící se kybergroomingu může svým jednáním naplnit skutkovou podstatu některých trestných činů uvedených v trestním zákoníku. Zpravidla se bude, dle povahy jednání útočníka, jednat o trestné činy dle ustanovení **§ 168** (Obchodování s lidmi), **§ 171** (Omezování osobní svobody), **§ 175** (Vydírání), **§ 185** (Znásilnění), **§ 187** (Pohlavní zneužívání), **§ 201** (Ohrožování výchovy dítěte), **§ 209** (Podvod), **§ 353** (Nebezpečné vyhrožování), **§ 354** (Nebezpečné pronásledování) TZK.[616]

Další z možných definic kybergroomingu uvádí, že jde o *„**takové chování uživatelů internetu, které má v dětské oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti**, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.*“[617] V této souvislosti pak je možné využít speciálního ustanovení uvedeného v **§ 193b** (Navazování nedovolených kontaktů s dítětem) TZK.

### 4.14.3 Sexting

Jednou z podob nebezpečného chování zejména v prostředí sociálních sítí je tzv. sexting. Pojem sexting vznikl kombinací slov sex a texting, z čehož vyplývá i jeho význam. Jde o elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem. Takovýto materiál se sexuálním podtextem může být na sociální sítě či jiná datová úložiště nahráván přímo jeho samotnými

614: Viz např. *Nikdy nevíš.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.youtube.com/watch?v=O79-0FUeYrk&list=PLQe7s_lKdHIAycTLmN_ojbey-joyldxRh
*Kybergrooming.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

615: Blíže viz např. Facebookový profil Stinson hunter - https://www.facebook.com/StinsonHunter/?fref=ts či Letzgo Hunting – Online Child Protection - https://www.facebook.com/LetzgoHuntingOfficial/?fref=ts.

616: VLACHOVÁ, Marta. *E-Bezpeci: Trestná činnost spojená s internetovou kriminalitou* [online]. [cit. 29. 6. 2015]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226

617: KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I.* In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit. 19. 3. 2014]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

autory nebo jiným uživatelem, který k takovému materiálu získal přístup. Nejčastěji se tak stane dobrovolným posíláním souborů se sexuálním obsahem, které jsou pořízeny samotným odesílatelem.

Následně (po ukončení komunikace, vztahu či z jiného důvodu) použije pachatel získaný choulostivý materiál k vyhrožování či vydírání. Pachatel v některých případech může pod pohrůžkou zveřejnění takovéhoto materiálu požadovat zaslání dalších fotografií či videa a psychickým nátlakem tak nutí poškozeného k výrobě a pořizování dalších materiálů, které pachatel vyžaduje buď pro vlastní potřebu, nebo se záměrem je sdílet na Internetu (v případě dětí je sdílí v komunitách zaměřených na dětskou pornografii). Druhou variantou pachatelova jednání je užití získaného materiálu k jinému nátlaku (např. obnovení partnerského vztahu, provozování sexuálních aktivit, zaslání finanční částky atp.) pod pohrůžkou zveřejnění již v minulosti získaných fotografií či videa (původně pachateli dobrovolně zaslaných poškozeným).[618]

Z výsledků Výzkumu rizikového chování českých dětí v prostředí Internetu[619] 2014 zpracovaného Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s firmou Seznam.cz vyplývá, že 9,86 % dětí umístilo svou „sexy" fotografii či video, na kterých jsou částečně nebo úplně nazí, na Internet. Z celkového počtu 28 232 respondentů 12,14 % uvedlo, že takovýto materiál někomu přes Internet/mobilní telefon poslalo.

U sextingu je podíl oběti na činu neoddiskutovatelný, neboť právě ona je osobou, která vytvořila předmětnou fotografii nebo video, avšak po odeslání tohoto materiálu ztrácí oběť naprostou kontrolu nad dalším „životem" těchto dat.

Sexting mezi dospělými není trestným činem, přesto může dojít ke zneužití citlivých dat, které byly útočníkovi zaslány. Jako případ zneužití fotografií, které byly rozeslány v rámci sextingu mezi dospělými, je možné uvést případ nazvaný *Roztahovačky*. Jednalo se o fenomén, který vznikl v roce 2014 v rámci sociální sítě Facebook, kde bývalí partneři vyvěsili fotografie svých partnerek, které jim byly zaslány v rámci sextingu. Velmi často byly tyto fotografie doplněny o popisek.

618: Sexting.cz – *vše, co chcete vědět o sextingu* [online]. [cit. 18. 3. 2014]. Dostupné z: www.sexting.cz

619: *Výzkum rizikového chování českých dětí v prostředí internetu 2014.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace


Obrázek 80: Příklady zveřejněných fotografií s komentáři

Před tím, než Facebook začal hromadně blokovat tyto profily, existovala celá řada obdobných účtů. Mezi nejznámější patří: Roztahovačky (6 230 fanoušků), Největší roztahovačky republiky (6 381 fanoušků), Liberecké roztahovačky (6 934 fanoušků), Pražský roztahovačky (7 963 fanoušků), Zlínské roztahovačky (4 248 fanoušků), Plzeňské oztahovačky 2 (5 832 fanoušků), Pardubické roztahovačky (4 569 fanoušků), Pražské roztahovačky (9 656 fanoušků) aj.

V případě zveřejnění fotek jiné osoby bez jejího souhlasu je možné, aby se dotčená osoba domáhala ochrany svých práv v rámci občanskoprávního řízení (blíže viz **§ 84 OZ** – kap. 2.4.1 Ochrana soukromí). V případě, že osoba uvádí o jiném nepravdivý údaj (tak jako tomu zřejmě bylo v případu Roztahovaček), 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, je možné využít **§ 184** (Pomluva) TZK.

Specifickým případem je pak situace, kdy jsou získávány a zneužívány audiovizuální materiály zobrazující dítě. Pokud útočník vyzývá dítě k vytvoření a následnému zaslání fotografií, videa či online streamování před web kamerou (které dítě zachycují nahé, obnažené či jinak vzbuzující sexuální vzrušení), může se dopustit trestného činu dle **§ 193** (Zneužití dítěte k výrobě pornografie) TZK.

Sexting se také velmi často projevuje tak, že pachatel nutí oběť posílat další materiály (fotky, videa, live stream aj.) s tím, že mu vyhrožuje, že pokud je nepošle, tak materiály, které již má v držení, zveřejní na Internetu nebo je zpřístupní jeho rodině či přátelům. Tím se dopustí trestného činu dle **§ 175 odst. 1** (Vydírání) TZK.

Osoba dopouštějící se sextingu může dále svým jednáním naplnit i skutkovou podstatu trestného činu dle **§ 192** (Výroba a jiné nakládání s dětskou pornografií) či **§ 201** (Ohrožování výchovy dítěte) TZK.

Na možná rizika sextingu upozorňují mimo jiné následující materiály:

- Once Posted You Lost It https://www.youtube.com/watch?v=CE2Ru-jqyrY

**Sexting:**

- http://www.bezpecne-online.cz/viewdownload/4/78
- http://www.sexting.cz/

**Exposed (Vystavená):**

- www.youtube.com/watch?v=9uJOXOAQ9Qo

**Další videa:**

- http://cz.sheeplive.eu/fairytales/bez-kozisku-titulky
- https://www.youtube.com/watch?v=Mm5XKy3MPHU
- https://www.youtube.com/watch?v=ThxmgXMBpoM

### 4.14.4 Kyberstalking

Kyberstalking je složenina slov kyber a stalking. Původně bylo slovo stalking používáno lovci divoké zvěře a znamenalo stopování zvěře až k jejímu uštvání. Stalking v té podobě, tak jak je chápán dnes, byl poprvé použit v 90. letech 20. století v rámci studie Meloye,[620] který za stalking označil nebezpečné pronásledování známým či neznámým pachatelem, který pronásleduje oběť, a to takovým způsobem, že v ní vyvolává pocit nebezpečí, strachu. Toto pronásledování musí být dlouhodobější.

620: MELOY, Reid J. *STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRELIMINARY STUDIES.* [online]. [cit. 3. 10. 2015]. Dostupné z: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

Jirásek definuje stalking jako *„Nejrůznější druhy stopování a obtěžování s využitím elektronického média (zejm. prostřednictvím elektronické pošty a sociálních sítí), jejichž cílem je např. vzbudit v oběti pocit strachu. Informace o oběti pachatel získává nejčastěji z webových stránek, fór nebo jiných hromadných komunikačních nástrojů. Často je taková aktivita pouze mezistupněm k trestnému činu, který může zahrnovat výrazné omezování osobních práv oběti nebo zneužití chování oběti k provedení krádeže, podvodu, vydírání apod.*“[621]

Kyberstalking je takové jednání, které spočívá v opakovaném kontaktování oběti například zasíláním SMS zpráv, e-mailů, telefonáty, VoIP, messengery aj. Jednání útočníka se zpravidla stupňuje a zpravidla vyvolá u oběti obavy o svoje soukromí, zdraví či život. Pro *kyberstalkery* je typická jejich vytrvalost a systematičnost, přičemž není neobvyklé, aby měl kyberstalker vytvořenou celou řadu falešných identit, které využívá ke kontaktování oběti. Kyberstalker může demonstrovat i svoji moc a sílu, například tím, že zveřejní informace ze života oběti, které může získat z různých online zdrojů.

Stalking či kyberstalking je možné subsumovat, za splnění určitých podmínek, pod ustanovení **§ 354** (Nebezpečné pronásledování) TZK. Mezi základní podmínky patří, že útočník musí oběť dlouhodobě *„vytrvale prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktovat“* a toto jednání je způsobilé vzbudit v oběti důvodnou obavu o její život nebo zdraví nebo o život a zdraví osob jí blízkých. Okolností přitěžující dle **§ 354 odst. 2 písm. a)** TZK je ta skutečnost, že uvedený čin je spáchán na dítěti.

## 4.15 Identity theft

Identity theft je útok, při kterém dochází k odcizení virtuální identity,[622] respektive jde o převzetí kontroly (trvalé, nebo dočasné) nad touto identitou. Motivem jednání útočníka může být finanční zisk, ale i jiné výhody, například přístup k informacím o jiných osobách, přístup k firemním datům ad., které jsou spojené s faktem, že útočník vystupuje jménem jiné osoby.

Jednání útočníka zpravidla spočívá v několika protiprávních jednáních najednou. Prvním protiprávním jednáním při identity theft je prolomení přístupových údajů či instalaci malware do počítačového systému oběti s cílem získat přístupu k virtuální identitě.

621: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 29. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

622: Virtuální identitou se rozumí jakákoliv totožnost či avatar využívaný osobou pro interakci v rámci kyberprostoru (Např. e-mail, účet na sociální síti, ve hře, v různých online tržištích, v rámci počítačového systému aj.). Nezáleží na skutečnosti, zda je virtuální indentita pravá či falešná, tedy jestli představuje reálnou či osobu, či jde o zcela uměle vytvořenou identitu, bez reálného základu.

Po získání přístupu k identitě napadeného může dojít jak ke zneužití získaných informací pro útok na tuto osobu, tak ke zneužití identity s cílem útoku na jinou osobu. Vlastní útok na další oběť prostřednictvím odcizené identity je pro útočníka podstatně snazší, neboť tato druhá oběť standardně nemá žádné informace o záměně identity osoby (oběti první), s níž například pravidelně komunikuje a vyměňuje si citlivé údaje.

Pokud se v této souvislosti vrátím k problematice botnetů, tak jedním z typických úkolů malware, který je nainstalován při připojení počítačového systému do sítě botnet, je i automatická extrakce dat o uživatelích napadeného počítačového systému – tedy identity theft. Botmaster pak může kdykoliv získaná data využít tak, že se bude vydávat za určitou osobu či tato data prodá třetím osobám.[623]

Typicky jsou odcizené identity využívány k:

- provádění phishingových či malwarových útoků v rámci seznamu uživatelů, s nimiž osoba se odcizenou identitou komunikuje,
- rozesílání spamu,
- zisku informací, které nejsou veřejně dostupné (například informací o struktuře společnosti, nastavení bezpečnosti dalších služeb atd.),
- získávání přístupů do dalších služeb. Řada online služeb umožňuje, pouze na základě zadání e-mailové adresy, změnu hesla. Díky faktu, že útočník ovládá e-mailovou schránku napadeného, může dojít ke změně přístupových údajů i v celé řadě dalších služeb, které jsou s touto e-mailovou schránkou provázány.

Pokud dojde k překonání bezpečnostního opatření a získání neoprávněného přístupu k identitě oběti, dojde k naplnění znaků trestného činu dle **§ 230 odst. 1** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK. Při použití malware ke stejnému účelu se útočník dopustí jednání dle § 230 odst. 2 TZK. Pokud je cílem identity theft získat sobě nebo jinému neoprávněný prospěch, je možné uplatnit i ustanovení **§ 230 odst. 3** TZK. V případě, že útočník odcizí identitu s cílem oklamat jiného, tedy vyvolat v něm omyl s cílem obohatit se, mohlo by takové jednání být posouzeno i dle **§ 209** (Podvod) TZK.

623: Blíže viz PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011, s. 22 [online]. [cit. 17. 5. 2015]. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

## 4.16 APT (Advanced Persistent Threat)

Pojem APT je doslovně možné přeložit jako „pokročilá a trvalá hrozba". Jedná se o dlouhodobý systematický kybernetický útok, zaměřený na cílový počítačový systém, respektive na ICT cílové organizace. K vlastnímu útoku jsou využívány různé techniky a poměrně rozsáhlé zdroje, přičemž typicky může docházet k napadání sekundárních cílů (počítačových systémů organizace např. opakovanými DoS či jinými útoky) s cílem odvedení pozornosti od primárního cíle (infiltrace společnosti malwarem), který je následně napaden.

*„APT je obvykle zaměřena na vytěžení strategicky hodnotných utajených či neveřejných dat, omezení akceschopnosti cíle, nebo zaujetí pozice, která umožňuje budoucí realizaci zmiňovaného. Uskutečnění akcí, které definici APT naplňují, je spojeno s vysokou úrovní odborných znalostí, značnými finančními zdroji a schopností dlouhodobě se adaptovat na jednání oběti útoku. Charakteru APT tak nabývají především státní aktéři, potažmo jimi řízená a sponzorovaná uskupení, nebo specializované skupiny organizovaného zločinu."* [624]

Vlastní APT útok se typicky skládá:

- ze zisku informací o cíli útoku (sběr informací z otevřených zdrojů; využití sociálního inženýrství aj.)
- z vlastního útoku:
    - Výběr vhodných prostředků (malware, tvorba krycích identit aj.)
    - V případě, že je systém napadnutelný zvenčí, dochází k jeho napadání
    - Pokud je systém zvenčí nedostupný, dochází k využívání jiných technik zkombinovaných se sociálním inženýrstvím (např. Spear phishing, Identity Theft aj.)
- z převzetí kontroly nad některými počítačovými systémy, upevnění pozice uvnitř napadené počítačové sítě
- ze sběru dat a informací a jejich zasílání útočníkovi
- z vytěžení dat

Útočníci v průběhu APT útoku mohou využívat další různé typy útoků na zvolený cíl, v závislosti na datech a informacích, jež získali.

624: *Advanced Persistant Threat.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat

APT je možné zobrazit pomocí jeho životního cyklu:


Obrázek 81: Průběh APT útoku[625]

Vlastní APT útok může trvat od několika měsíců po řadu let a součástí útoku mohou být i poměrně dlouhá období, kdy je aktivita útočníků minimální. Výjimkou není ani vedení velkého počtu obdobných operací proti různým cílům současně.[626]

625: *Advanced Persistant Threat – life cycle.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

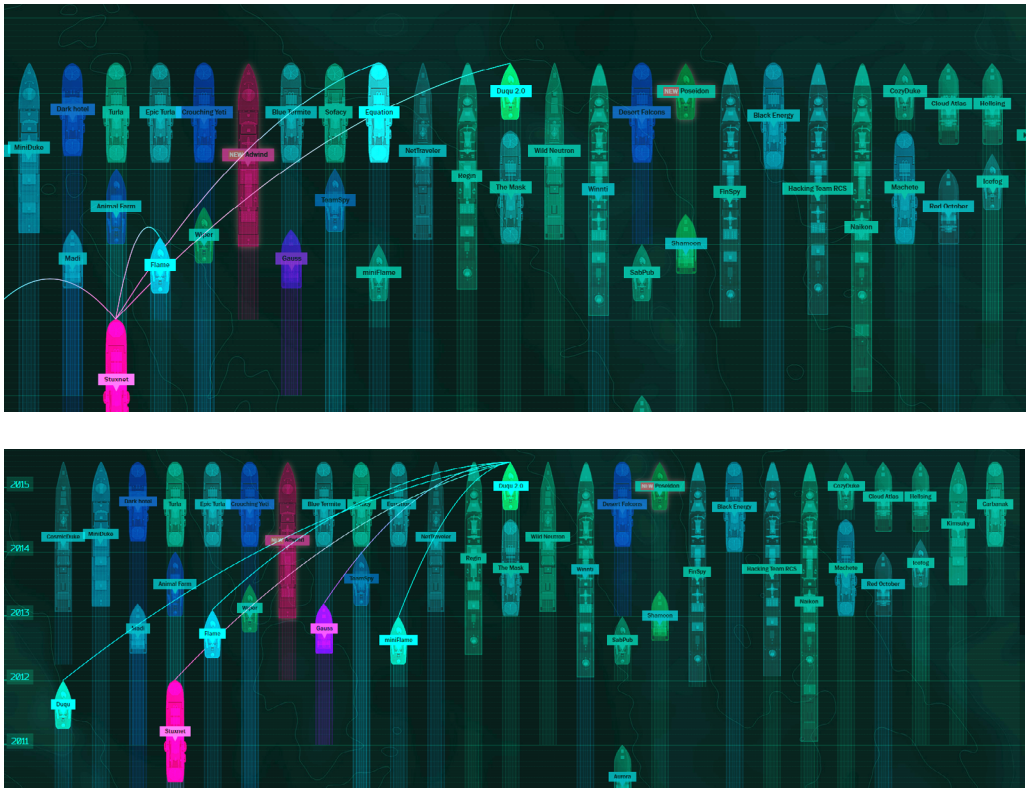
626: Blíže viz: *Advanced Persistant Threat.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat

*Advanced Persistant Threat (APT)*. [online]. [cit. 20. 8. 2016]. Dostupné z: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

*Advanced Persistent Threats: How They Work*. [online]. [cit. 10. 7. 2016]. Dostupné z: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1

*How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic).* [online]. [cit. 10. 7. 2016]. Dostupné z: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/

Na stránce společnosti Kasperky Lab (https://apt.securelist.com/#firstPage) jsou graficky znázorněny známé APT útoky, včetně uvedení informací o tom, kdy se poprvé objevil vzorek útočného malware, kdy byl objeven útok APT, kde primárně působí (geolokační informace, primárně napadané operační systémy, počet cílů aj.) atp. Následující dva printscreeny zobrazují primární vazbu malware Stuxnet (mimo jiné i na Duqu 2.0.) a následně vazbu Duqu 2.0 na další malware.




Obrázek 82: Zobrazení ATP útoků včetně jejich provázanosti[627]

Případný trestněprávní postih útočníka či útočníků provádějících APT útok pak zcela závisí na jejich jednání, které může mít např. podobu distribuce malware (viz kap. 4.3 Malware), některého z phishingových útoků (viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing), Identity Theft (viz kap. 4.15 Identity theft) aj.

627: *Targeted cyberattacks logbook.* [online]. [cit. 10. 7. 2016]. Dostupné z: https://apt.securelist.com/#secondPage

## 4.17 Kyberterorismus

V souvislosti s kybernetickými útoky nelze opomenout ani terorismus, který představuje jednu z aktuálních globálních hrozeb a lze sledovat jeho dynamický nárůst a rozšiřování do celého světa.

Terorismus můžeme rozdělit podle formy na *letální a neletální* formy, kde první skupina se vyznačuje použitím běžných prostředků pro realizaci násilí (*konvenční* – útoky páchané pomocí běžně dostupných bojových prostředků, např. střelných zbraní a *nekonvenční* – zneužití zbraní hromadného ničení). V oblasti Internetu jsou však **běžnější neletální formy terorismu**[628] nebo útoky, při kterých jsou využívány moderní nástroje v kombinaci s letálními prostředky.

Konvenční forma neletálního terorismu zahrnuje níže uvedené podskupiny:

- *Neozbrojený terorismus*.

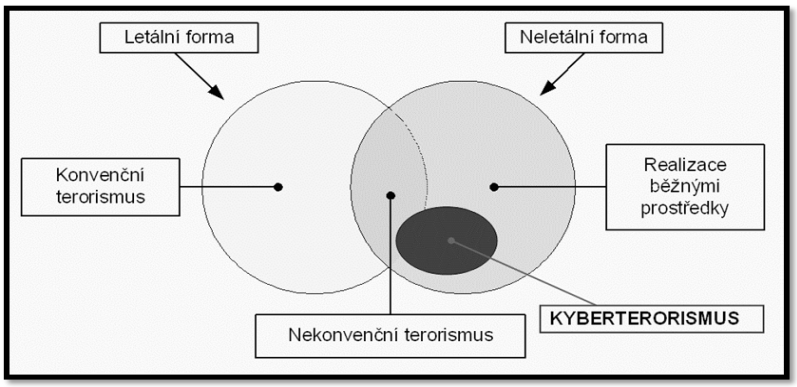
- *Kyberterorismus*, který patří mezi největší nebezpečí 21. století. Principem je především zneužívání ICT (včetně Internetu) jako prostředku a prostředí pro uskutečnění útoku. Jedná se, podobně jako u klasického konvenčního teroristického útoku, o plánovanou činnost motivovanou zpravidla politicky či nábožensky a realizovanou spíše malými, ne vojensky organizovanými strukturami. Cílem těchto skupin je především ovlivnění veřejného mínění. Vzhledem k rychlému šíření informačních a komunikačních technologií po celém světě představuje kyberterorismus významné nebezpečí a je teroristickými skupinami využíván ve stále rostoucí míře.[629]

- *Mediální terorismus*, při němž dochází k plánovanému zneužívání hromadných sdělovacích prostředků a jiných psychologických prostředků za účelem ovlivnění názorů celé populace, nebo cílových skupin obyvatelstva.

Nejvýstižněji tento vztah charakterizuje schéma uvedené na následujícím obrázku.

628: Nicméně je možné si představit i kombinaci těchto útoků. Blíže viz např.:
*Exclusive: Computer Virus Hits U.S. Drone Fleet.* [online]. [cit. 10. 7. 2016]. Dostupné z:
https://www.wired.com/2011/10/virus-hits-drone-fleet/

629: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 129




Obrázek 83: Zobrazení forem terorismu včetně kyberterorismu[630]

Globální charakter informatického a telekomunikačního prostředí umožňuje předávání informací a koordinaci teroristických aktivit v rámci celého světa. Uvádí se, že např. útok na WTC v New Yorku byl organizován právě s využitím Internetu.

Je možno uvést i další případy zneužití Internetu pro šíření závadných informací nebo pro psychologické operace související s mediálním terorismem. Internet se podstatnou měrou podílí na šíření propagandy, ideologie či zastrašování například v podobě zveřejnění poprav zajatců online,[631] získávání a mobilizaci nových aktivistů, sympatizantů či sponzorů, obhajobě teroristických činů a podněcování jednotlivců k jejich páchání. Internetové servery teroristických skupin často obsahují návody na výrobu improvizovaných zbraní, nebo propagandu zacílenou na mladší generaci.

Internet poskytuje zcela výjimečné možnosti extremistickým a teroristickým skupinám i jednotlivcům, a to zejména v oblasti rychlé a relativně utajené komunikace, kdy slouží ke vzájemné výměně informací a pokynů k plánování a koordinaci akcí nebo převodu finančních prostředků.

630: Srov: JIROVSKÝ, Václav. *Kyberterorismus*. ICT fórum/PERSONALIS 2006. [předneseno 27. 9. 2006]. Praha (prezentace na konferenci).

631: **Předložené URL není cenzurováno a obsahuje drastické záběry!** Viz např.:
*WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives - Graphic video.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive--blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382
*Disturbing ISIS video shows militants beheading four prisoners and gunman executing shoppers at market.* [online]. [cit. 20. 8. 2016]. Dostupné z:
http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017

Bezmála všechny teroristické skupiny a organizace provozují své internetové stránky. Obvykle jsou zveřejňovány v několika jazykových mutacích a nechybí ani speciální stránky zaměřené na děti a ženy obsahující pohádky či komiksy, do nichž jsou zapracovány například příběhy sebevražedných atentátníků.[632]


Obrázek 84: Webové stránky TravelWest.info po napadení útočníky

Z hlediska trestního práva pak uvedené jednání může naplňovat skutkové podstaty trestných činů **§ 311 odst. 2** (Teroristický útok), **§ 355** (Hanobení národa, rasy, etnické nebo jiné skupiny osob), **§ 356** (Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod), **§ 364** (Podněcování k trestnému činu), **§ 403** (Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka) a **§ 404** (Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka) TZK.

632: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 138 Dále viz např.: *Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html
*Islamic State Hacking Division*. [online]. [cit. 20. 8. 2016]. Dostupné z: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

## 4.18 Další útoky

Na závěr této kapitoly představím některé další útoky, k nimž v kyberprostoru dochází, avšak v mnohem menší míře, než jak tomu je u dříve popsaných jednání.

### 4.18.1 Cybersquatting, typosquatting

Pojem **cybersquatting** je složeninou anglických slov „*cybernetic*" (kybernetický) a „*squatting*" (nelegální obsazení domu). Squatting znamená nelegální obsazení určitého prostoru, v tomto případě určitého doménového jména. Pachatel si zaregistruje doménové jméno, jehož součástí je název některého známého produktu či instituce, např.: www.ministerstvovnitra.eu či www.barum.eu. Zpravidla pak dojde k nabídce ze strany držitele domény, aby si subjekt, jehož se doména dotýká, odkoupil doménové jméno za úplatu s tím, že pokud tak neučiní, bude na uvedených stránkách zobrazena například pornografie. Tato forma útoků měla svůj vrchol v době, kdy docházelo teprve ke vstupu společností na síť Internet, přičemž k těmto útokům docházelo i díky v té době nedostatečné právní úpravě. V současné době je již tato oblast dostatečně právně regulována.[633]

Tímto jednáním se pachatel vystavuje možnosti případného trestněprávního postihu pro trestné činy **§ 175** (Vydírání) a **§ 268** (Porušení práv k ochranné známce a jiným označením) TZK.

Právě velké množství problémů souvisejících se spory o doménová jména vedlo v roce 2004 k vydání pravidel k registraci doménových jmen[634] v doméně **.CZ**. Uvedená pravidla vydalo sdružení **CZ.NIC** (www.nic.cz). Spory o doménová jména .CZ jsou řešeny podle systému alternativního řešení sporů u Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky. Nejedná se o rozhodčí řízení dle zákona, ale jde o systém velmi podobný principům známým z UDRP a ADR.eu.

Pojem **typosquatting** je složený z anglických slov „*typographical*" (typografický) a již výše zmíněný „*squatting*". Jedná se o jednu z forem cybersquattingu. Při užití této metody se využívá registrace doménového jména, které je velmi podobné již existujícímu, řádně zaregistrovanému doménovému jménu, avšak na rozdíl od originálu nová webová adresa úmyslně obsahuje překlep. Na webovou stránku, která je zaregistrovaná s takovým překlepem v názvu, se pak dostane část uživatelů, která se chtěla dostat na stránku původní, ale dopustila se při zadávání webové adresy právě onoho překlepu. Tímto

633: K problematice registrace doménových jmen srov. např. HRUBEŠOVÁ, Helena. „*Proč si neregistrovat doménové jméno pod doménou nejvyššího stupně „.com" aneb jak je to s jurisdikcí amerických soudů*". [cit. 25. 9. 2010]. Dostupné na World Wide Web: http://www.itpravo.cz/index.shtml?x=1928185

634: Blíže viz *Pravidla registrace doménových jmen v ccTLD .cz.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.nic.cz/files/nic/PravidlaCZod20160515.pdf

způsobem se uměle navyšuje počet navštívení takto vytvořených parazitujících stránek. Takové jednání je pak mnohdy kvalifikovatelné jako nekalá soutěž, případně porušování práv k ochranné známce.[635]

### 4.18.2 Útoky na VoIP

Dalším útokem, ke kterému v současnosti dochází, je útok na VoIP ústředny, respektive na poskytovatele a uživatele těchto služeb. Velmi často jsou k útokům na VoIP využívány DoS či DDoS útoky. Dále dochází k útokům, při nichž se útočník snaží získat přístupová uživatelská jména, hesla a jiné obdobné údaje (viz kap. 4.15 Identity theft). Takovéto jednání je pak dle povahy případu možné kvalifikovat například dle **§ 230 odst. 1** (Neoprávněný přístup k počítačovému systému a nosiči informací) a **§ 205** (Krádež) TZK.

### 4.18.3 Kybernetické výpalné (Racketeering)

Podstatou uvedeného jednání je **vyvolání obavy z možného napadení počítačového systému, zničení, odcizení dat a poškození hardwaru**. Opět se jedná o klasický trestný čin, avšak páchaný novými prostředky, kdy nedochází k fyzickému kontaktu s obětí.

V tomto případě se jedná o odlišné jednání, než které bylo popsáno v kap. 4.4 Ransomware. Uživateli může být například vyhrožováno masivním DDoS útokem či jiným útokem, pokud nezaplatí požadovanou částu. Vyděrač v mnohých případech využívá i pouhé neznalosti uživatele. Uvedené jednání je možné postihnout dle **§ 175** (Vydírání) TZK. Pokud dojde například k odcizení přístupových údajů nebo instalaci malware ze strany útočníka, je možné využít i **§ 230** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK.

635: Blíže srov. *Pravidla a postupy.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.nic.cz/page/314/pravidla-a-postupy/

# 5 Trestněprávní ochrana před kyberkriminalitou

## 5 Trestněprávní ochrana před kyberkriminalitou

Snahy o právní regulaci a postih trestné činnosti páchané prostředky informačních a komunikačních technologií je možné vypozorovat de facto již od počátku těchto negativních aktivit. Kybernetická trestná činnost je značně odlišná od jiných druhů kriminality, přičemž tato odlišnost spočívá především v možnosti jejího dynamického vývoje a okamžité změny (dle úspěšnosti či neúspěšnosti toho kterého typu útoku), což ve vztahu k legislativě může přinášet určité problémy.

V trestním právu hmotném platí zásada, že není možné využít analogie k tíži pachatele (*in malam partem*).[636] Přesto je možné kybernetické útoky mnohdy subsumovat pod zákonné ustanovení určité skutkové podstaty, byť tato skutková podstata původně směřovala na „tradičnější způsoby" spáchání trestného činu (typicky se jedná například o útoky spojené s porušováním práv autorských, zneužívání dětí k výrobě pornografie aj.). Avšak existuje celá řada útoků nových, u nichž tato možnost v úvahu nepřichází. V takových případech se legislativci jednotlivých zemí zatím především snaží *ad hoc* reagovat na tyto nové druhy trestné činnosti a vyplňují tak slepá místa ve vnitrostátní právní úpravě.

Před vlastní analýzou stávající platné a účinné legislativy v oblasti kyberkriminality je třeba podotknout, že nejen v rámci Evropské unie je zřetelná snaha po implementaci účinnějších právních nástrojů, které by byly schopné včas a adekvátně reagovat na kyberkriminalitu. Dochází tak k postupnému odstraňování rozporů a nedostatků v právních normách členských států EU a dalších států, které se rozhodly aktivně zapojit do boje s kybernetickou trestnou činností.

Jedním z prvních dokumentů věnujících se problematice kyberkriminality, přijatých na mezinárodní úrovni, je **Manuál OSN o prevenci a kontrole trestných činů spojených s počítači** (Havana, 1990).[637]

*„Způsoby ochrany dat a informačních systémů jsou dnes předmětem nejednoho vědního výzkumu, ovšem toliko technická ochrana těchto systémů a dat bez právního podkladu může být neefektivní v důsledku nejasného vymezení, kam až je možno při takové ochraně zajít. V tomto kontextu se naplno projevuje nesoulad právních úprav jednotlivých států s právními úpravami států ostatních. Díky rozvoji počítačových a informačních technologií, které udávají mezinárodní charakter kybernetických trestných činů, je efektivní ochrana počítačových systémů a dat nemyslitelná bez existence mezinárodního resp. nadnárodního právního rámce, a to nejen mezi členskými státy EU, ale v celosvětovém měřítku."*[638]

636: Viz kap. 1.1 Kybernetická trestná činnost (Cybercrime).

637: *United Nations Manual on the prevention and control of computer-related crime.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

638: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 65

## 5.1 Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU

Na prvním místě je třeba zmínit Úmluvu o kyberkriminalitě a dodatkový protokol k ní, neboť se jedná o dva nejvýznamnější právní dokumenty, které přispívají k ochraně společnosti před kyberkriminalitou tím, že stanoví základní rámec trestných kybernetických činů a zároveň stanoví prostředky pro odhalování a vyšetřování této kriminality. Dále budou uvedeny právní dokumenty EU a ES, které souvisí s problematikou kyberkriminality.

### 5.1.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Úmluva o kyberkriminalitě představuje nejvýznamnější právní dokument týkající se kyberkriminality a jejím hlavním účelem je sjednotit národní právní úpravu v oblasti kyberkriminality. Výše uvedené se realizuje tím, že Úmluva o kyberkriminalitě stanoví smluvním stranám povinnost implementovat do národních právních řádů takové nástroje, které umožní postih definovaných kybernetických trestných činů. Právě důkladná definice skutkové podstaty trestného činu je podmínkou k tomu, aby bylo možné užít norem trestního práva v kyberprostoru. Dále Úmluva o kyberkriminalitě vytváří právní rámec pro jednotný a společný postup proti pachatelům těchto trestných činů bez ohledu na místo spáchání trestného činu.

Úmluvu o kyberkriminalitě schválil Výbor ministrů Rady Evropy na svém 109. zasedání dne 8. listopadu 2001. Úmluva o kyberkriminalitě byla otevřena k podpisu 23. listopadu 2001 v Budapešti.[639] V platnost vstoupila tato úmluva dne 1. července 2004.

Česká republika podepsala Úmluvu o kyberkriminalitě dne 9. února 2005 a ratifikovala ji 22. srpna 2013 s tím, že v ČR tato úmluva vstoupila v platnost 1. prosince 2013. Členské státy EU se zavázaly ratifikovat Úmluvu o kyberkriminalitě a včlenit do svých právních řádů taková ustanovení, která by umožňovala objasňovat a vyšetřovat uvedenou trestnou činnost.[640] Úmluva o kyberkriminalitě byla rovněž podepsána a ratifikována například Spojenými státy americkými, Japonskem aj. Polčák ke sjednocování mezinárodní právní úpravy věnující se problematice kyberkriminality uvádí, že *„rozvoj internetové trestní jurisdikce bude probíhat prostřednictvím dodatkových protokolů k Úmluvě, které postupně postihnou další konkrétní typy trestné činnosti či dokonce přestupků.*“[641]

639: Seznam států, které podepsaly a ratifikovaly Úmluvu o kyberkriminalitě, je možné nalézt na: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D
K 20.8.2016 podepsalo či ratifikovalo Úmluvu o kyberkriminalitě celkem 55 států (49 států ratifikovalo a 6 států podepsalo, avšak zatím neratifikovalo Úmluvu o kyberkriminalitě).

640: Tento závazek je dán v čl. 14–21 Úmluvy o kyberkriminalitě.

641: Blíže viz POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 16

Úmluva o kyberkriminalitě[642] se skládá z **preambule a 48 článků**, které jsou rozděleny do 4 kapitol:

1) **Používané pojmy** *(Use of terms)*

2) **Opatření, která mají být přijata na vnitrostátní úrovni** *(Measures to be taken at the national level)*
   - Část 1 – Trestní právo hmotné (*Substantive criminal law.* Čl. 2–13)
   - Část 2 – Procesní právo (*Procedural law.* Čl. 14–21)
   - Část 3 – Soudní pravomoc (*Judrisdiction.* Čl. 22*)*

3) **Mezinárodní spolupráce** *(International Co-operation)*
   - Část 1 – Obecné zásady (*General principles*. Čl. 23–28)
   - Část 2 – Zvláštní ustanovení (*Specific provisions.* Čl. 29–35)

4) **Závěrečná ustanovení** *(Final provisions)*

Významným krokem ke sjednocení práva je definování čtyř základních skupin trestných činů (viz kap. II; čl. 2–13) a zakotvení dalších obecných institutů z trestního práva hmotného.[643] Právě jednotné definování (pojmenování) kybernetických útoků umožní jejich efektivnější stíhání v zemích, které Úmluvu o kyberkriminalitě ratifikovaly. Konkrétně se jedná o:

1) **Trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů** (*Offences against the confidentiality, integrity and availability of computer data and systems*. Čl. 2-6),

2) **Trestné činy související s počítači** (*Computer-related offences*. Čl. 7-8),

3) **Trestné činy související s obsahem** (*Content-related offences*. Čl. 9),

4) **Trestné činy související s porušováním autorských práv a práv souvisejících** (*Offences related to infringements of copyright and related rights*. Čl. 10).

Z hlediska obecných hmotněprávních principů je dále definována trestněprávní odpovědnost za pokus a účastenství (*Attempt and aiding or abetting*. Čl. 11)[644] a trestněprávní odpovědnost právnické osoby (*Corporate liability*)[645] za trestný čin podle Úmluvy o kyberkriminalitě.

642: Kompletní znění Úmluvy v českém překladu je možné nalézt [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

643: Blíže k jednotlivým skupinám trestných činů viz kap. 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku.

644: Tento požadavek je v českém trestním právu zcela realizován instituty *pokus trestného činu* (§ 21 a 111 TZK) a *účastenství* (§ 24 a 111 TZK).

645: Trestněprávní odpovědnost právnických osob je v českém právním prostředí realizována na základě zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů.

### 5.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě

Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě,[646] který byl přijat 28. ledna 2003,[647] definuje okruh trestných činů, jimž se Úmluva o kyberkriminalitě nevěnuje. V Úmluvě o kyberkriminalitě chybí trestné činy, které spočívají v šíření určitého *„závadného materiálu"*.[648] Dodatkový protokol vymezuje trestné činy, jež spočívají především v šíření materiálů s obsahem rasistickým, xenofobním, či jinak projevujícím rasovou nesnášenlivost. Důvodem nezařazení předmětných trestných činů do Úmluvy o kyberkriminalitě bylo zejména podepsání a následné přijetí Úmluvy o kyberkriminalitě ze strany USA.[649]

Dodatkový protokol se skládá z **preambule** a **16 článků**, které jsou rozděleny do 4 kapitol:

1) **Obecná ustanovení** *(Common provisions)*

2) **Opatření, která mají být přijata na vnitrostátní úrovni** *(Measures to be taken at the national level)*

   - Článek 3 – Šíření rasistického a xenofobního materiálu skrze počítačový systém *(Dissemination of racist and xenophobic material through computer systems)*
   - Článek 4 – Rasisticky a xenofobně motivovaná výhrůžka *(Racist and xenophobic motivated threat)*
   - Článek 5 – Rasisticky a xenofobně motivovaná urážka *(Racist and xenophobic motivated insult)*
   - Článek 6 – Popírání, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti *(Denial, gross minimisation, approval or justification of genocide or crimes against humanity)*

646: *ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f

647: Seznam států, které podepsaly a ratifikovaly Dodatkový protokol, je možné nalézt na: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D
K 20. 8. 2016 podepsalo či ratifikovalo Úmluvu o kyberkriminalitě celkem 39 států (24 států ratifikovalo a 15 států podepsalo, avšak zatím neratifikovalo Úmluvu o kyberkriminalitě). Dodatkový protokol nepodepsalo a neratifikovalo např. Slovensko.

648: Vyjma dětské pornografie, která je přímo obsažena v čl. 9 Úmluvy o kyberkriminalitě.

649: Právě problematika rasismu a xenofobie je v USA tématem nacházejícím se v „šedé zóně", neboť některá prohlášení lze považovat za trestný čin a jiná naopak ne. Např. Ne všechny projevy rasismu jsou v **USA** považovány za trestný čin, viz **První dodatek Ústavy USA** – *Kongres nevydá žádný zákon, který by nerespektoval svobodu vyznání, nebo by obsahoval zákaz volného výkonu (bohoslužebných úkonů), nebo omezující svobodu slova nebo tisku nebo právo lidu pokojně se shromažďovat a podávat petici vládě s cílem nápravy křivd.* **Aby se jednalo o protiprávní jednání či trestný čin, je třeba prokázat reálnost hrozby, v opačném případě by se jednalo o narušení prvního dodatku.** Oproti tomu jsou projevy rasismu ve **Francii** či **SRN**, stejně jako v **ČR** považovány za trestný čin.

3) **Vztah mezi Úmluvou o kyberkriminalitě a Dodatkovým protokolem** *(Relations between the Convention and this Protocol)*

4) **Závěrečná ustanovení** *(Final provisions)*

V **kapitole první** je upraven účel Dodatkového protokolu a je zde vymezen pojem – rasistický a xenofobní materiál. Dle čl. 1 odst. 1 Dodatkového protokolu se rasistickým a xenofobním materiálem rozumí *„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.“*

### 5.1.3 Dokumenty EU/ES sloužící k harmonizaci právních úprav při potírání kybernetické trestné činnosti

Zejména díky specifičnosti spočívající v neohraničenosti kyberkriminality a potřebě efektivní mezinárodní spolupráce se EU snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možné tento negativní jev účinněji postihovat. Prostředkem pro sbližování práva jednotlivých zemí EU jsou především rámcová rozhodnutí, směrnice, a další dokumenty EU/ES. Z pohledu boje s kyberkriminalitou jsou nejvýznamnějšími následující dokumenty:

- *Směrnice Rady 91/250/EHS* o právní ochraně počítačových programů
- *Rozhodnutí Rady 92/242/EHS* o bezpečnosti informačních systémů
- *Směrnice Evropského parlamentu a Rady č. 98/34/ES* o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice *č. 98/48/ES*
- *Směrnice č. 2000/31/ES* o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“)
- *Rámcové rozhodnutí Rady 2000/375/JHA* o boji proti dětské pornografii na internetu
- *Rámcové rozhodnutí Rady 2001/413/SVV* o potírání podvodů a padělání bezhotovostních platebních prostředků
- *Směrnice Evropského parlamentu a Rady č. 2002/21/EC* o společném regulačním rámci pro sítě a služby elektronických komunikací (rámcová směrnice)
- *Směrnice Evropského parlamentu a Rady č. 2002/19/EC* o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice)

- *Směrnice Evropského parlamentu a Rady č. 2002/20/EC* o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice)

- *Směrnice Evropského parlamentu a Rady č. 2002/22/EC* o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě)

- *Směrnice Evropského parlamentu a Rady 2002/58/EC* týkající se zpracovávání osobních údajů a ochrany soukromí v oblasti elektronických komunikací (směrnice o ochraně údajů v elektronických komunikacích)

- *Směrnice Komise č. 2002/77/ES* o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami (soutěžní směrnice)

- *Rámcové rozhodnutí Rady EU č. 2002/584/JHA* o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy

- *Rámcové rozhodnutí Rady 2005/222/SVV* o útocích proti informačním systémům

- *Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů* - Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“) ze dne 15. 11. 2006

- *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů* k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007

- *Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti* ze dne 27. listopadu 2008

- *Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“* ze dne 30. 3. 2009[650]

- *Sdělení komise Radě a Evropskému parlamentu*, Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě. 2012

- *Nařízení Evropského parlamentu a Rady (EU) č. 526/2013*, o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004, ze dne 21. května 2013

650: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 76

- *Směrnice Evropského parlamentu a Rady 2013/40/EU*, o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, ze dne 12. srpna 2013

- *Nařízení Evropského parlamentu a Rady (EU) č. 513/2014*, kterým se jako součást Fondu pro vnitřní bezpečnost zřizuje nástroj pro finanční podporu policejní spolupráce, předcházení trestné činnosti, boje proti trestné činnosti a řešení krizí a zrušuje rozhodnutí Rady 2007/125/SVV, ze dne 16. dubna 2014

- *Nařízení Evropského parlamentu a Rady (EU) č. 910/2014*, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ze dne 23. července 2014

- *Nařízení Evropského parlamentu a Rady (EU) 2016/794*, o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV, ze dne 11. května 2016

- *Nařízení Evropského parlamentu a Rady (EU) 2016/679* ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

- *Směrnice Evropského parlamentu a Rady (EU) 2016/1148*, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, ze dne 6. července 2016 (NIS Directive)[651]

651: K některým uvedeným dokumentům blíže viz: VOLEVECKÝ, Petr. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. In *Trestní právo,* 2009, roč. 12, č. 7-8, s. 26–39. Veškeré předpisy práva EU jsou dostupné i v české verzi na *EUR-lex.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://eur-lex.europa.eu/homepage.html

### 5.1.4 Právní normy ČR

V souvislosti s kybernetickou trestnou činností a kybernetickou bezpečností je třeba uvést i právní normy ČR, které mají bezprostřední vztah k této problematice:

- Zákon č. 40/2009 Sb., trestní zákoník
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

## 5.2 Hmotněprávní aspekty kybernetické trestné činnosti

### 5.2.1 Kybernetické trestné činy ve zvláštní části trestního zákoníku

Trestní zákoník, který nabyl účinnosti 1. ledna 2010, zavedl v oblasti trestního práva hmotného řadu zásadních změn. Tyto změny se podstatným způsobem dotkly též znění skutkových podstat trestných činů. Z hlediska kybernetické trestné činnosti došlo k zavedení nových speciálních skutkových podstat, které jsou zaměřeny na kyberkriminalitu, respektive některé kybernetické útoky.

Kybernetické trestné činy jsou v nejobecnější rovině z hlediska využití informačních a komunikačních technologií děleny na trestné činy, při kterých jsou tyto prvky užity jako nástroj umožňující spáchání trestného činu, přičemž skutková podstata trestného činu obsahuje použití těchto prostředků jako znak skutkové podstaty, a na trestné činy, při kterých jsou prvky informačních a komunikačních technologií terčem útoku pachatele, tedy představují individuální objekt resp. hmotný předmět útoku.

Zákonodárce zařadil do zvláštní části trestního zákoníku řadu skutkových podstat trestných činů, které buď obsahují znaky mající vztah k informačním a komunikačním technologiím, nebo mohou být naplněny kybernetickým útokem. Mezi tyto činy je možné zařadit:

- § 180 neoprávněné nakládání s osobními údaji
- § 181 poškození cizích práv
- § 182 porušení tajemství dopravovaných zpráv
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 184 pomluva
- § 191 šíření pornografie
- § 192 výroba a jiné nakládání s dětskou pornografií
- § 193 zneužití dítěte k výrobě pornografie
- § 193b navazování nedovolených kontaktů s dítětem
- § 205 krádež
- § 206 neoprávněné užívání cizí věci
- § 209 podvod
- § 213 provozování nepoctivých her a sázek
- § 214 podílnictví
- § 216 legalizace výnosů z trestné činnosti
- § 228 poškození cizí věci
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
- § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
- § 236 výroba a držení padělatelského náčiní
- § 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití
- § 268 porušení práv k ochranné známce a jiným označením
- § 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem
- § 269 porušení chráněných průmyslových práv
- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- § 272 obecné ohrožení
- § 276 poškození a ohrožení provozu obecně prospěšného zařízení
- § 287 šíření toxikomanie
- § 290 získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou
- § 291 ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla
- § 311 teroristický útok
- § 316 vyzvědačství

- § 317 ohrožení utajované informace
- § 345 křivé obvinění
- § 348 padělání a pozměnění veřejné listiny
- § 353 nebezpečné vyhrožování
- § 354 nebezpečné pronásledování
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
- § 357 šíření poplašné zprávy
- § 361 účast na organizované zločinecké skupině
- § 364 podněcování k trestnému činu
- § 365 schvalování trestného činu
- § 400 genocidum
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
- § 404 projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka
- § 405 popírání, zpochybňování, schvalování a ospravedlňování genocidia
- § 407 podněcování útočné války

Tyto kybernetické trestné činy podle trestního zákoníku je možné třídit podle mnoha různých kritérií. Mezi nejčastěji používané třídění kybernetických trestných činů patří již výše zmíněné třídění na:[652]

a) **trestné činy, při jejichž páchání představují prostředky informačních a komunikačních technologií předmět ochrany** (tedy jsou terčem kybernetického útoku):
   - § 182 porušení tajemství dopravovaných zpráv
   - § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
   - § 206 neoprávněné užívání cizí věci
   - § 228 poškození cizí věci
   - § 230 neoprávněný přístup k počítačovému systému a nosiči informací
   - § 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
   - § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
   - § 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití
   - § 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem
   - § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
   - § 290 získání kontroly nad vzdušným dopravním prostředkem, civilním plavidlem a pevnou plošinou
   - § 291 ohrožení bezpečnosti vzdušného dopravního prostředku a civilního plavidla
   - § 311 teroristický útok
   - § 317 ohrožení utajované informace

652: Některé trestné činy je vzhledem k dikci jejich skutkových podstat možné zařadit do obou kategorií (tato ustanovení chrání prostředky informačních a komunikačních technologií, ale zároveň obsahují znaky zneužití těchto technologií).

b) **trestné činy, při jejichž páchání jsou prostředky informačních a komunikačních technologií užity ke spáchání trestného činu:**
   - § 180 neoprávněné nakládání s osobními údaji
   - § 181 poškození cizích práv
   - § 182 porušení tajemství dopravovaných zpráv
   - § 184 pomluva
   - § 191 šíření pornografie
   - § 192 výroba a jiné nakládání s dětskou pornografií
   - § 193 zneužití dítěte k výrobě pornografie
   - § 193b navazování nedovolených kontaktů s dítětem
   - § 205 krádež
   - § 209 podvod
   - § 213 provozování nepoctivých her a sázek
   - § 214 podílnictví
   - § 216 legalizace výnosů z trestné činnosti
   - § 230 neoprávněný přístup k počítačovému systému a nosiči informací
   - § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
   - § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
   - § 236 výroba a držení padělatelského náčiní
   - § 268 porušení práv k ochranné známce a jiným označením
   - § 269 porušení chráněných průmyslových práv
   - § 272 obecné ohrožení
   - § 276 poškození a ohrožení provozu obecně prospěšného zařízení
   - § 287 šíření toxikomanie
   - § 316 vyzvědačství
   - § 345 křivé obvinění
   - § 348 padělání a pozměnění veřejné listiny
   - § 353 nebezpečné vyhrožování
   - § 354 nebezpečné pronásledování
   - § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob
   - § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod
   - § 357 šíření poplašné zprávy
   - § 361 účast na organizované zločinecké skupině
   - § 364 podněcování k trestnému činu
   - § 365 schvalování trestného činu
   - § 400 genocidum
   - § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
   - § 407 podněcování útočné války

Vedle uvedených ustanovení zvláštní části trestního zákoníku se k problematice kybernetických trestných činů vztahuje též § 120 TZK, které stanovuje, že *„uvést někoho v omyl či využít něčího*

*omylu lze i provedením zásahu* **do počítačových informací nebo dat, zásahu do 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.*"

Při vymezení znaků skutkových podstat trestných činů, které je možné označit jako kybernetické trestné činy, užívá zákonodárce celé řady technických a odborných výrazů vztahujících se k informačním a komunikačním technologiím. Tyto výrazy ukazuje následující tabulka:

| Pojem | Výskyt ve skutkové podstatě |
|---|---|
| **veřejně přístupná počítačová síť** | § 180 neoprávněné nakládání s osobními údaji<br>§ 184 pomluva<br>§ 191 šíření pornografie<br>§ 192 výroba a jiné nakládání s dětskou pornografií<br>§ 287 šíření toxikomanie<br>§ 345 křivé obvinění<br>§ 355 hanobení národa, rasy, etnické nebo jiné skupiny osob<br>§ 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod<br>§ 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka<br>§ 407 podněcování útočné války |
| **síť elektronických komunikací** | § 182 porušení tajemství dopravovaných zpráv<br>§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat |
| **přenos prostřednictvím sítě elektronických komunikací** | § 182 porušení tajemství dopravovaných zpráv |
| **datová zpráva** | § 182 porušení tajemství dopravovaných zpráv |
| **elektromagnetické vyzařování z počítačového systému** | § 182 porušení tajemství dopravovaných zpráv |
| **počítačový systém** | § 182 porušení tajemství dopravovaných zpráv<br>§ 230 neoprávněný přístup k počítačovému systému a nosiči informací<br>§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat<br>§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti |
| **neveřejný přenos počítačových dat** | § 182 porušení tajemství dopravovaných zpráv |
| **počítačová data, data uložená v počítačovém systému** | § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí<br>§ 230 neoprávněný přístup k počítačovému systému a nosiči informací<br>§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat<br>§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti |

| | |
|---|---|
| **počítačové (pornografické) dílo** | § 191 šíření pornografie<br>§ 192 výroba a jiné nakládání s dětskou pornografií |
| **elektronické dílo** | § 191 šíření pornografie<br>§ 192 výroba a jiné nakládání s dětskou pornografií |
| **nosič informací** | § 230 neoprávněný přístup k počítačovému systému a nosiči informací<br>§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti |
| **programové a technické vybavení počítače** | § 230 neoprávněný přístup k počítačovému systému a nosiči informací<br>§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti<br>§ 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití<br>§ 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem |
| **funkčnost počítačového systému** | § 230 neoprávněný přístup k počítačovému systému a nosiči informací |
| **(jiné) zařízení pro zpracování dat** | § 230 neoprávněný přístup k počítačovému systému a nosiči informací<br>§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti |
| **počítačový program** | § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat<br>§ 236 výroba a držení padělatelského náčiní<br>§ 348 padělání a pozměnění veřejné listiny |
| **programové vybavení počítače** | § 264 zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití<br>§ 267 zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem |
| **počítačové heslo** | § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat |
| **přístupový kód** | § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat |
| **postup nebo jakýkoli jiný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části** | § 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat |
| **elektronické peníze** | § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku |
| **telekomunikační systém** | § 311 teroristický útok |
| **databáze** | § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi |
| **informační systém** | § 311 teroristický útok |
| **prostředky elektronických komunikací** | § 354 nebezpečné pronásledování |

### 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku

Jedním z hlavních důvodů rekodifikace českého trestního práva hmotného bylo zapracování mezinárodních smluv a rámcových rozhodnutí Rady Evropy v rámci harmonizace práva signatářských zemí. Je třeba konstatovat, že došlo k přiblížení ke standardům uvedeným a požadovaným Úmluvou o kyberkriminalitě. Při rozboru jednotlivých ustanovení upozorním i na nedostatky české právní úpravy.

Následující část monografie obsahuje rozbor těch ustanovení trestního zákoníku, která chrání před kyberkriminalitou. **Pořadí analyzovaných skutkových podstat neodpovídá jejich řazení v trestním zákoníku, ale klasifikaci uvedené v Úmluvě o kyberkriminalitě.**

U jednotlivých trestných činů budou obecně popsány jednotlivé znaky skutkové podstaty trestného činu. Primárně však bude pozornost zaměřena na zájmy chráněné jednotlivými ustanoveními, na jednání, kterým se jednotlivé trestné činy od sebe odlišují, případně na následek, který je vyžadován k dokonání trestného činu. Dále se budu věnovat znakům skutkové podstaty obsahujícím určitá specifika, která je odlišují od obecných požadavků, anebo jsou ve skutkové podstatě obsaženy fakultativní znaky, na které je třeba upozornit.

#### 5.2.2.1 Trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů

##### 5.2.2.1.1 Neoprávněný přístup (čl. 2)

Úmluva o kyberkriminalitě v čl. 2 stanoví, že každý ze signatářů přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, **aby** podle jejích vnitrostátních právních předpisů **byl trestným činem**, pokud je spáchán úmyslně, **neoprávněný přístup k celému počítačovému systému nebo jeho jakékoli části**. Daný stát může ponechat na svém uvážení, zda je k trestnosti činu třeba splnit další podmínky, které mohou spočívat ve:

- spáchání činu porušením bezpečnostních opatření,
- spáchání činu v úmyslu získat počítačová data nebo s jiným nečestným úmyslem,
- spáchání činu ve vztahu k počítačovému systému, který je spojen s jiným počítačovým systémem.

Neoprávněný přístup je možné subsumovat pod ustanovení **§ 230 odst. 1** TZK - **Neoprávněný přístup k počítačovému systému a nosiči informací.**

***„Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části**, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“*

V **odstavci 1** je uvedena skutková podstata základní, popisná, složitá.

**Objektem** této skutkové podstaty je ochrana před neoprávněným vniknutím do počítačového

systému. Primárně je chráněna důvěrnost a bezpečnost jak počítačových systémů (či jejich částí), tak i počítačových dat. *„Teprve sekundárně jsou chráněny integrita a dostupnost počítačových dat a systémů."*[653] Zákon chrání před jednáním pachatele, které je možné označit jako hacking, cracking[654] či computer trespass.[655]

K pojmu počítačový systém viz kap. 1.2.3 Počítač (Počítačový systém). Částí **počítačového systému** se rozumí jak vlastní vnitřní vybavení počítačového systému, bez něhož by nebyla možná vlastní činnost tohoto systému, tak i periferie (viz kap.1.2.3.1 Hardware). Částí počítačového systému jsou i data (viz kap. 1.2.3.3 Data a informace).

Z hlediska **objektivní stránky** spočívá jednání pachatele v **překonání** bezpečnostního opatření **a získání přístupu** k počítačovému systému nebo jeho části. Pokud jde o formu, je zapotřebí jednání komisivního (aktivního jednání).

**Bezpečnostním opatřením** se rozumí jakékoli opatření, které slouží k zabránění volného přístupu k počítačovému systému nebo jeho části. Běžně se jedná např. o hesla, firewally, ale i přenosná paměťová media s klíči k přístupu do systému.

Pokud by útočník k překonání bezpečnostního opatření využil malware, který by byl do počítačového systému nainstalován (byť by instalaci provedla oběť činu), jako prostředku útoku, bylo by takové jednání možné definovat i jako zásah do počítačového systému.[656] Dle českého trestního práva by se útočník dopustil i jednání popsaného v § 230 odst. 2 písm. d) TZK.

Pojmem **neoprávněně** se rozumí takové jednání, které je v rozporu s právem (blíže viz kap. 5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru).

**Získáním přístupu** se rozumí stav, kdy může pachatel volně disponovat s předmětným počítačovým systémem či nosičem informací, jakož i s daty zde uloženými.

Zvláštností neoprávněného přístupu oproti jiným kybernetickým útokům je to, že samotné překonání bezpečnostního opatření může být cílem pachatelovy činnosti.[657] Na druhou stranu je zpravidla tato činnost jen prostředkem k závažnějšímu jednání.[658]

Z hlediska následku je v této skutkové podstatě vyžadován **následek poruchový**, který je dokonán již překonáním bezpečnostního opatření. Základní skutková podstata § 230 odst. 1 TZK

653: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012. s. 2304

654: Viz kap. 4.8 Hacking; 4.9 Cracking.

655: *Computer Trespass Law and Legal Definition*. [online]. [cit. 16. 7. 2016]. Dostupné z: https://definitions.uslegal.com/c/computer-trespass/

656: Viz čl. 5 Úmluvy o kyberkriminalitě.

657: Viz snaha Hackerů překonávat dosud nepřekonané a tím si stanovit nové meze svojí činnosti.

658: Např. vytvoření zombie v rámci sítě botnet aj.

v sobě nezahrnuje úmysl způsobit škodu, jinou újmu či získat sobě nebo jinému neoprávněný prospěch apod. (tyto okolnosti jsou znaky kvalifikovaných skutkových podstat uvedených v § 230 odst. 3 a násl. TZK - jedná se o okolnosti zvláště přitěžující.[659]).

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Pokud jde o **subjektivní** stránku, je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

V souvislosti s tímto trestným činem vystupuje do popředí celá řada otázek.

První z otázek bezesporu je, zda má na trestnost činu vliv míra zabezpečení počítačového systému nebo jeho části. Reálně je možné si představit situaci, při které osoba přijde k počítači svého kolegy a zadá přístupové heslo napsané na lístku u monitoru napadeného počítače. Případně je nalezen USB disk, na kterém je napsáno přístupové heslo k tomuto disku. Je možné si představit i tu situaci, kdy pachatel překoná hesla následujícího typu (*user:* admin, *password:* admin; nebo *user:* Hana B., *password:* Hana B.; *user:* XY, *password:* 1234). Je třeba uvést, že i v těchto případech je jednání pachatele možné postihnout dle předmětného ustanovení trestního zákoníku, neboť bylo překonáno bezpečnostní opatření, byť by takové bezpečnostní opatření zjevně neplnilo svoji funkci. **Pro naplnění jednání není rozhodující, jak sofistikované toto bezpečnostní opatření bylo. Podstatné je, že pachatel překoná určitou překážku.**

Druhou otázkou může být řešení přístupu k nezabezpečenému počítačovému systému nebo jeho části. Běžně půjde například o to, že si pracovník firmy nijak nezabezpečí svůj počítač (např. při odchodu na toaletu) a kolega k němu získá přístup, aniž by naplnil znaky jiné skutkové podstaty trestného činu (např. § 230 odst. 2 TZK). Dle současné trestněprávní nauky by takové jednání pachatele nebylo z pohledu trestního práva postižitelné. Trestní právo je prostředkem ultima ratio a primárně by mělo dojít k využití jiných odvětví práva (viz § 12 odst. 2 TZK), přičemž v tomto případě je třeba posoudit i míru společenské škodlivosti (viz § 12 odst. 2 a § 39 odst. 2 TZK) výše popsaného jednání.

Na druhou stranu je však třeba na tuto problematiku pohlížet i v souladu s ustanoveními **Listiny** (kdy je v **čl. 10** zaručena ochrana soukromí[660]). Je pak otázkou, zda by bylo vhodné včlenit do § 230 TZK novou základní skutkovou podstatu, která by postihovala úmyslné neoprávněné získání přístupu k počítačovému systému nebo jeho části, bez ohledu na překonání či nepřekonání bezpečnostního opatření.[661] Domnívám se, že výše popsané jednání zmíněného kolegy bez

659: Blíže k otázce zavinění při těchto okolnostech: viz § 17 písm. a) TZK – těžší následek a § 17 písm. b) TZK – jiná skutečnost.

660: *„Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.“*

661: Sama Úmluva o kyberkriminalitě v čl. 2 umožňuje postihovat i takovýto druh jednání.

dalšího (např. naplnění znaků § 230 odst. 2 TZK) by nebylo natolik škodlivé, aby se jednalo o trestný čin. Případnou újmu by v takto popsaném případě bylo třeba řešit prostředky například občanského práva.

Poslední otázkou pak je činnost, která naplňuje znaky této skutkové podstaty, avšak je prováděna oprávněně,[662] ale například bez vědomí koncového uživatele. Typicky se může jednat o penetrační testování bezpečnosti počítačového systému ze strany správce takovéhoto systému s cílem zvýšení bezpečnosti. V rámci tohoto testu pak budou například automatickým programem určeným k prolamování hesel překonána výše uvedená hesla. V okamžiku překonání takového „*bezpečnostního opatření*" by se dle dikce zákona správce dopouštěl trestného činu dle § 230 odst. 1 TZK. Jsem toho názoru, že v tomto případě nebude jednání správce protiprávní (viz § 13 odst. 1 TZK),[663] byť může jednat bez oprávnění uživatele, jehož bezpečnostní opatření byla překonána, neboť cílem jeho činnosti je zvýšit zabezpečení počítačového systému a případně upozornit na zjištěné nedostatky.[664]

#### 5.2.2.1.2 Neoprávněné zachycení informací (čl. 3)

Podle tohoto článku Úmluvy o kyberkriminalitě by smluvní strany měly přijmout taková legislativní opatření, **aby se trestným činem stal skutek spočívající v úmyslném, neoprávněném, technickými prostředky provedeném odposlechu neveřejného přenosu[665] počítačových dat do počítačového systému, z něj[666] nebo v jeho rámci,[667] včetně elektromagnetického vyzařování z počítačového systému přenášejícího taková počítačová data**. Daný stát může ponechat na svém uvážení, zda je k trestnosti činu třeba splnit další podmínky, které mohou spočívat:

- ve vyžadování specifického (nečestného) úmyslu,
- v tom, že se jednalo o útok na počítačový systém, který je propojen s dalším počítačovým systémem.

662: Například v souladu s některými okolnostmi vylučujícími protiprávnost – viz kap. 5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru.

663: *Trestný čin je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.*

664: Blíže viz kap. 5.3.

665: Z dikce tohoto článku vyplývá, že tento znak se vztahuje ke způsobu přenosu dat, nikoliv k jejich obsahu. Bude se tedy vztahovat na neveřejné přenosy byť i veřejně dostupných dat, naopak na veřejné přenosy neveřejných dat dopadat nebude.

666: Např. dva počítačové systémy propojené připojením (např. LAN, Bluetooth, IrDA aj.).

667: Např. přenos dat mezi USB a harddiskem počítače.

Jednání popsané v čl. 3 Úmluvy o kyberkriminalitě je možné charakterizovat jako kybernetický útok mající povahu sniffingu.[668] České trestní právo umožňuje uvedené jednání postihnout dle **§ 182** TZK - **Porušení tajemství dopravovaných zpráv.**

*(1)* ***Kdo úmyslně poruší tajemství***

*a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,*
*b)* ***datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli****, který zprávu přijímá, nebo*
*c)* ***neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data****.*

*bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.*

*(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch*

*a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo* ***přenosu prostřednictvím sítě elektronických komunikací****, který nebyl určen jemu, nebo*
*b) takového tajemství využije.*

*(3) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,*
*b) spáchá-li takový čin ze zavrženíhodné pohnutky,*
*c) způsobí-li takovým činem značnou škodu, nebo*
*d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.*

*(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako úřední osoba,*
*b) způsobí-li takovým činem škodu velkého rozsahu, nebo*
*c) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.*

668: Viz kap. 4.11 Sniffing.

*(5)* ***Zaměstnanec*** *provozovatele poštovních služeb,* ***telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti,*** *který*

*a)* ***spáchá čin uvedený v odstavci 1 nebo 2****,*
*b)* ***jinému úmyslně umožní spáchat takový čin****, nebo*
*c)* ***pozmění nebo potlačí*** *písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo* ***zprávu podanou neveřejným přenosem počítačových dat****, telefonicky, telegraficky* ***nebo jiným podobným způsobem,***

*bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.*

*(6) Odnětím svobody na tři léta až deset let bude pachatel potrestán,*

*a) způsobí-li činem uvedeným v odstavci 5 škodu velkého rozsahu, nebo*
*b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.*

V **odstavcích 1, 2 a 5** se jedná o základní skutkové podstaty, popisné, složité. V odstavcích **3, 4 a 6** se jedná o kvalifikované skutkové podstaty.

**Objektem** § 182 odst. 1 TZK je **ochrana tajemství přepravovaných zpráv**. Za přepravované zprávy se nepovažují již doručené či rozepsané, avšak neodeslané, byť jsou uchovávány v soukromí (tyto zprávy jsou chráněny jako jakákoli jiná data – viz § 230 TZK).

Pokud jde o kybernetickou trestnou činnost, pak z hlediska **objektivní stránky** standardně spočívá jednání pachatele v **porušení tajemství**:

*b)* ***datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli****, který zprávu přijímá, nebo*
*c)* ***neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data****,*

Pojmy používané v § 182 odst. 1 písm. b) TZK vycházejí z definic uvedených v zákoně o elektronických komunikacích. Tento zákon v § 2 písm. a) uvádí, že **účastníkem** *je každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb.* **Uživatelem** [dle § 2 písm. b) ZoEK] je *každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací.* **Sítí elektronických komunikací** [dle § 2 písm. h) ZoEK] *jsou přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo*

*paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.*

Problém však spatřuji v tom, že trestní zákoník vychází při definování výše uvedených pojmů právě ze zákona o elektronických komunikacích, avšak nikde v § 182 odst. 2 písm. b) a c) na tento zákon explicitně neodkazuje jako na normu *lex specialis.*

Domnívám se proto, že toto pojetí, restriktivně vykládající[669] výše uvedené pojmy je minimálně sporné, nebo neodpovídá skutečnosti. Pokud bychom je přijali, pak by byla působnost trestního zákoníku zúžena de facto na porušení tajemství dopravovaných zpráv, respektive zásah do nich, pouze v rámci veřejných poskytovatelů připojení (viz kap. 2.5.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZoEK). Neoprávněný zásah do přenášených zpráv by dle tohoto zužujícího pojetí nemohl být u ostatních poskytovatelů (ne jen poskytovatelů připojení[670]), postižen prostředky trestního práva. Pokud bychom akceptovali uvedené zužující pojetí, pak by § 182 TZK nechránil osoby, které využívají jiné připojení (datový přenost) než dle zákona o elektronických komunikacích (např. vysokoškolské, podnikové či jiné počítačové sítě aj.), což je nepřijatelné.

**Vhodnější a přesnější definice výše uvedených pojmů by pak, bez ohledu na to o jakého ISP půjde, zněla:**

- **Účastníkem** ***je každý, kdo uzavřel s poskytovatelem služby informační společnosti smlouvu na poskytování těchto služeb, případně každý, kdo využívá některou službu informační společnosti.***
- **Uživatelem** je každý, ***kdo využívá nebo žádá službu elektronických komunikací.***
- **Sítí elektronických komunikací** jsou přenosové systémy, ***počítačové systémy***, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.

669: Srov. mimo jiné i: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1811–1812

670: Tvrzení, že se uvedené ustanovení může vztahovat na všechny poskytovatele služeb informační společnosti, tedy jak na ISP připojení a ISP služeb, vyplývá ze skutečnosti, že i ISP služeb:

- je zpravidla správcem počítačové sítě (tedy sítě elektronických komunikací);
- vykonává správu nad neveřejným přenosem počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data.

Pojmem **datová zpráva**, dle trestního zákoníku, se rozumí jakákoliv zpráva přenášená v podobě dat. K pojmu data viz kap. 1.2.3.3 Data a informace.

**Textovou zprávou** se rozumí zpráva přenášená v podobě textového sdělení, např. text e-mailové zprávy, SMS zpráva, komunikace pomocí instant messengerů a dalších programů pro přenos psaných zpráv. Textovou zprávou se rozumí i informace uveřejněné v písemné podobě pomocí chatu aj.

**Hlasová zpráva** je zpráva přenášená v podobě záznamu hlasu člověka. Může se jednat o telekomunikaci vedenou prostřednictvím klasického telefonního přístroje (včetně mobilního telefonu), ale i o komunikaci uskutečněnou skrze speciální software, k tomu určený (např. Skype aj.).

**Zvukovou zprávou** se rozumí jakákoli zpráva v podobě záznamu zvuku.

**Obrazovou zprávou** je jakýkoliv obrazový záznam určitého stavu, děje, procesu nebo jevu zachycený pomocí technického zařízení, a to nejenom ze záznamu, ale i online.[671] Může se jednat například o fotografii, video, MMS zprávu, Skype video komunikaci atp.

Pojem **elektromagnetické vyzařování** užívaný uvedeným ustanovením je možné definovat jako vyzařování, které počítač emituje během svých operací. Toto vyzařování samo o sobě není možné považovat za data, ale je z něj možné data zrekonstruovat.[672]

**Jednání** je v této skutkové podstatě vyjádřeno slovem *„poruší tajemství"*, přičemž v rámci ochrany před kyberkriminalitou se jedná o jakoukoli činnost pachatele, která směřuje k neoprávněnému seznámení se s obsahem přepravované zásilky v podobě přepravované zprávy v síti elektronických komunikací nebo neveřejného přenosu počítačových dat. Jak již bylo uvedeno výše, tak **chráněny nejsou zprávy již doručené či rozepsané, avšak neodeslané**, byť jsou uchovávány v soukromí.

**Tajemstvím** *„je chráněn obsah dopravovaných zpráv bez ohledu na jejich formu či hodnotu pro adresáta, odesílatele či pachatele."*[673] Zákon rozlišuje porušování tajemství dopravovaných zpráv (§ 182 odst. 1 TZK) od případů, kdy je toto porušování prostředkem ke způsobení škody jinému nebo získání neoprávněného prospěchu pro sebe nebo jiného (§ 182 odst. 2 TZK).

671: Srov. ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1811

672: Jedná se o emise (tedy záření) z počítačového systému, který taková data obsahuje. Jako příklad zneužití takovéhoto vyzařování je možné uvést projekt AirHopper sloužící k získávání dat z izolovaného počítačového systému. Blíže viz např: *"AirHopper" Malware Uses Radio Signals to Steal Data from Isolated Computers.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.securityweek.com/airhopper-malware-uses-radio-signals-steal-data-isolated-computers
*How to leak sensitive data from an isolated computer (air-gap) to a near by mobile phone – AirHopper.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.youtube.com/watch?v=2OzTWiGl1rM

673: JELÍNEK, Jiří a kolektiv: *Trestní zákoník a trestní řád s poznámkami a judikaturou***.** Praha: Leges 2009, s. 228

Podstatným znakem tohoto trestného činu je i **neveřejnost** předmětného přenosu dat. Tento znak skutkové podstaty trestného činu se vztahuje na způsob přenosu, nikoli na jeho obsah. Může tedy nastat případ, kdy bude neveřejně přenášena veřejně známá a dostupná informace, i v tomto případě by se pachatel dopustil, za splnění dalších podmínek uvedených v § 182 TZK, tohoto trestného činu.[674]

**Následek** je poruchový.

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost, nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Pokud jde o **subjektivní** stránku, je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

**V odstavci 5** se jedná o základní skutkovou podstatu, chránící stejný objekt, avšak je zde uveden **speciální subjekt**, kterým je **zaměstnanec provozovatele** poštovních služeb, **telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti.** Tento speciální subjekt bude přísněji potrestán, pokud se dopustí některého z jednání uvedených v odstavci 1 nebo 2, nebo se dopustí specifického jednání uvedeného v § 182 odst. 5 písm. b) a c) TZK. Dle těchto dvou specifických ustanovení bude zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti odpovědný pokud:

- *jinému úmyslně umožní spáchat takový čin,*[675] *nebo*
- *pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem.*

Pokud jde o **subjektivní** stránku, je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

#### 5.2.2.1.3 Zásah do dat (čl. 4)

Článek 4 Úmluvy o kyberkriminalitě stanoví smluvním stranám povinnost přijmout taková legislativní a jiná opatření, **aby se trestným činem stal skutek spočívající v úmyslném poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat**. Smluvní strany mají právo si stanovit, že výše popsané jednání bude trestným činem pouze tehdy, pokud bude způsobena závažná škoda (typicky se jedná o výši škody, která je určena ratifikujícím státem).

674: Blíže viz GŘIVNA, Tomáš a Radim POLČÁK (eds.) *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 113

675: Jedná se o účastenství ve formě pomoci [viz § 24 odst. 1 písm. c)], přičemž v tomto případě je účastenství ve formě pomoci povýšeno na dokonaný trestný čin.

Za kybernetické útoky, které zasahují do dat (dle znění čl. 4 Úmluvy o kyberkriminalitě), je možné primárně považovat útoky malware, hacking, DoS a DDoSaj.[676] České trestní právo umožňuje některé[677] z uvedených jednání postihnout dle **§ 230 odst. 2 písm. a) a b)** TZK.

*(2)* ***Kdo získá přístup*** *k počítačovému systému nebo k nosiči informací a*

*a)* ***neoprávněně užije*** *data uložená v počítačovém systému nebo na nosiči informací,*
*b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně* ***vymaže*** *nebo jinak* ***zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými****,…*

**V odstavci 2** je uvedena skutková podstata základní, popisná, složitá.

**Objektem** této skutkové podstaty je ochrana počítačových dat a programů před neoprávněnou manipulací s nimi (tj. před způsobením škody v podobě narušení integrity, dostupnosti, nesprávné funkčnosti, neoprávněného užívání dat či programů).

Toto ustanovení postihuje neoprávněné nakládání s daty či zásahy do vybavení počítačového systému po získání přístupu k němu. Nezáleží na tom, zda k získání přístupu došlo oprávněně či neoprávněně, neboť tato skutková podstata postihuje **neoprávněnou manipulaci s daty**.

Z hlediska **objektivní stránky** spočívá jednání pachatele v **získání přístupu** k počítačovému systému, nebo nosiči informací **a**:

a) neoprávněném **užití dat**,
b) neoprávněném **vymazání dat, nebo jejich jiném zničení, poškození, změnění, potlačení, snížení kvality, či učinění neupotřebitelnými**,
c) Pokud jde o formu, je zapotřebí jednání komisivního.

Obecně k pojmu **získání přístupu** viz § 230 odst. 1 TZK. Pro naplnění znaků skutkové podstaty dle § 230 odst. 2 TZK **není rozhodující, zda pachatel získal přístup** k počítačovému systému nebo nosiči informací **neoprávněně, či oprávněně**.

**Neoprávněným užitím dat** se rozumí jakékoli nedovolené nakládání s daty uloženými v počítačovém systému či na nosiči informací. Neoprávněné je takové užití dat, které je v rozporu s právní normou (např. § 40 a násl. AZ), nebo je činěno v rozporu se stanoveným účelem či bez souhlasu oprávněné osoby.[678]

676: viz kap. 4.3 Malware; 4.8 Hacking; 4.12 DoS, DDoS, DRDoS útoky.

677: Viz možnosti trestněprávního postihu útoků DoS a DDoS – kap. 4.12 DoS, DDoS, DRDoS útoky.

678: Srov. ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2309

**Neoprávněným vymazáním dat** se rozumí fyzické odstranění dat z počítačového systému či nosiče informací.

**Jiným zničením** může mimo jiné být fyzická destrukce např. počítačového systému či nosiče informací, na jejichž základě dojde k trvalé nedostupnosti dat.

**Poškozením** se rozumí stav, kdy pachatel změní např. integritu, dostupnost, kvalitu či jiné další atributy dat, a to buď trvale, či dočasně. Poškozená data je možné, u určitých případů, navrátit do „původního stavu", avšak pro naplnění zde uvedeného jednání není tato skutečnost rozhodující.

**Změněním dat** se rozumí stav, kdy pachatel např. doplní data stávající daty novými, pozměňují obsah, rozsah, hodnotu, uspořádání či jiné atributy dat. Změněním se rozumí i zakódování dat tak, aby k nim jejich původní vlastník neměl přístup.

**Potlačením** se rozumí stav, kdy data původní sice existují, ale oprávněná osoba k nim již nadále nemá přístup.

**Následek** je v této skutkové podstatě **poruchový.**

**Hmotným předmětem útoku** u tohoto ustanovení může být jak počítačový systém nebo nosič informací [viz § 230 odst. 3 písm. b) TZK], tak především **data** v něm uložená (viz kap. 2.4.2 Věci a virtuální majetek). Ve vztahu k datům lze toto tvrzení zdůvodnit tím, že pachatel neútočí přímo (fyzicky) na počítačový systém nebo na nosič informací, ale na data v něm uložená (zpravidla tak činí virtuálně). Toto tvrzení pak zcela koresponduje s tím, že prakticky všechna bezpečnostní opatření (viz § 230 odst. 1 TZK), jež je třeba překonat, jsou také virtuální. K zásahům do dat se nejběžněji využívá malware, u něhož není nezbytná instalace do napadeného počítačového systému (i když není vyloučena).

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost, nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

Souběh s § 230 odst. 1 TZK je možný. Je možné si reálně představit situaci, kdy pachatel překoná bezpečnostní opatření, a tím získá přístup k počítačovému systému nebo jeho části a následně provede některé z jednání popsaných § 230 odst. 2 TZK (např. data zničí, vymaže, poškodí aj.).

Na závěr rozboru ustanovení chránícího před zásahem do dat je třeba upozornit na tři okolnosti. První z nich je činnost osoby, která nebude jednat neoprávněně. Zpravidla půjde o případy testování bezpečnosti počítačového systému z důvodu zvýšení jeho zabezpečení, dále pak půjde

o nahrávání aktualizací, „záplat“ či rekonfiguraci operačního systému počítače.[679]

Druhou spornou otázkou je vymezení pojmu potlačení dat. Z dikce uvedené v komentáři k trestnímu zákoníku vyplývá, že takovýmto potlačením by mohlo být pouhé přesunutí dat z jedné složky v počítači do složky jiné (byť umístěné na stejném nosiči informací).[680] Je otázkou, zda by takovéto jednání bylo natolik společensky škodlivé, aby se jednalo o trestný čin.

V neposlední řadě je třeba vymezit data jakožto hmotný předmět útoku, neboť s tímto pojmem zákonitě vyvstává otázka hodnoty dat a informací zničených, pozměněných, poškozených kybernetickým útokem. Je zřejmé, že ve vztahu k naplnění skutkové podstaty trestného činu není otázka hodnoty dat rozhodující, avšak je zásadní v případě nároku na náhradu škody/újmy v adhezním řízení. Jednou z možností vyčíslení hodnoty dat je užití „strojového času“ či doby, kterou musela poškozená osoba strávit obnovou po zásahu do dat. V případě nevratitelného poškození dat je vyčíslení jejich hodnoty značně obtížné a bude záležet na posouzení soudu (ať již občansko či trestněprávního).

#### 5.2.2.1.4 Zásah do systému (čl. 5)

Článek 5 Úmluvy o kyberkriminalitě stanoví smluvním stranám povinnost přijmout taková legislativní a jiná opatření, **aby se trestným činem stal skutek spočívající v úmyslném, neoprávněném závažném omezení funkčnosti počítačového systému, které je zapříčiněno vkládáním, přenášením, poškozením, vymazáním, snížením kvality, pozměněním nebo potlačením počítačových dat**.

Článek 4 Úmluvy o kyberkriminalitě se věnuje ochraně dat počítačového systému, jejichž narušení nemusí nutně vést k poškození počítačového systém, kdežto článek 5 Úmluvy o kyberkriminalitě chrání fungování počítačového systému jako celku. Nezávažná, drobná či snadno napravitelná narušení fungování počítačového systému by neměla být podle tohoto článku postihována.

Výkladem *argumentum a minori ad maius* lze dovodit, že na danou skupinu kybernetických útoků lze použít ustanovení uvedená v předchozí podkapitole, neboť je-li pachatel trestně odpovědný za to, že pronikl do systému a neoprávněně manipuloval s daty, tím spíše musí být odpovědný,

679: V těchto případech zpravidla uživatel sám aktivně souhlasí s provedením uvedené činnosti.

680: **Potlačením dat se rozumí zabránění jejich upotřebitelnosti**. Tvůrce zákona vysvětluje „nadbytečnost“ dvou synonymních pojmů v komentáři takto:
„*Učinit neupotřebitelnými znamená sice zachování dosavadních dat, ale jednáním pachatele dojde k tomu, že je nelze nadále využívat k původnímu účelu (zakódováním dat, znemožněním získání dat s příslušného nosiče apod.). Potlačením dat jsou případy, kdy data dále existují beze změny, ale pachatel s nimi naložil tak, že je nelze dohledat na jejich původním umístění.*“
Srov. ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2309

zasáhne-li celý systém.[681] České trestní právo umožňuje uvedené jednání postihnout dle **§ 230 odst. 2 písm. d)** TZK a v **§ 230 odst. 3 písm. b)** TZK.

*(2)* ***Kdo získá přístup k počítačovému systému nebo k nosiči informací a***

*d)* ***neoprávněně vloží*** *data do počítačového systému nebo na nosič informací* ***nebo učiní jiný zásah*** *do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,*

*(3) Odnětím svobody na šest měsíců až čtyři léta, zákazem činnosti nebo propadnutím věci bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2*

*b)* ***v úmyslu neoprávněně omezit funkčnost počítačového systému*** *nebo jiného technického zařízení pro zpracování dat.*

**Objektem** této skutkové podstaty je ochrana počítačových systémů před neoprávněnou manipulací s nimi a zájem na jejich řádném fungování.

Z hlediska **objektivní stránky** spočívá jednání pachatele v **neoprávněném vložení dat**[682] do počítačového systému (nebo na nosič informací) **nebo učinění jiného zásahu** do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat. Pokud jde o formu, je zapotřebí jednání komisivního.

Půjde o jakékoli jiné jednání,[683] vyjma kybernetických útoků uvedených v § 230 odst. 2 písm. a) až c) TZK. Podmínkou trestnosti dle tohoto ustanovení je, aby byla předmětná data vložena do počítače či jiného zařízení (běžně je k takovémuto jednání využíván již zmíněný malware). Jednání mající podobu DoS či DDoS útoku[684] je možné postihnout pouze u určitých typů těchto útoků (při vkládání dat do počítačového systému).

Z hlediska následku je v této skutkové podstatě vyžadován **následek poruchový.**

**Hmotným předmětem útoku** je dle dikce § 230 odst. 2 písm. d) TZK počítač nebo jiné technické zařízení pro zpracování dat. Užití pojmů jiné technické zařízení pro zpracování dat či počítač

681: Bude se tedy především jednat o útoky: malware, hacking, DoS a DDoS, masivní spamové a phishingové kampaně aj.
682: **Vložení dat či jiný zásah** do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, je další formou počítačové sabotáže vedle poškození dat [viz § 230 odst. 2 písm. b) TZK].
683: Zpravidla se bude jednat o ochromení činnosti počítače nebo jiného technického zařízení pro zpracování dat, zablokování funkce programů, narušení propojení jednotlivých částí hardwaru aj.
Blíže viz ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2309
684: Viz kap. 4.12 DoS, DDoS, DRDoS útoky.

je dle mého názoru nadbytečné, neboť tyto pojmy jsou zahrnuty v pojmu počítačový systém.

V § 230 dost. 3 písm. b) TZK se z hlediska závažnosti jedná o kvalifikovanou skutkovou podstatu trestného činu, která obsahuje okolnost zvláště přitěžující a podmiňující použití vyšší trestní sazby. Jedná se o jinou skutečnost [viz § 17 písm. b) TZK], ke které je vyžadováno zavinění úmyslné.

U této jiné skutečnosti je podstatná i okolnost, že pachatel tak učiní v *„úmyslu **neoprávněně** omezit funkčnost…*“, neboť pak nebude trestné jednání osob, které oprávněně omezí funkčnost takovéhoto zařízení, např. v úmyslu zabránit kybernetickým útokům na nich či z nich vykonávaných. Tato kvalifikovaná skutková podstata reaguje na problematiku DoS a DDoS útoků, avšak podmínkou je, aby se pachatel dopustil některého z jednání uvedeného v § 230 odst. 1 či 2 TZK. Je třeba konstatovat, že ne ve všech případech těchto útoků je třeba, aby pachatel získal přístup k počítačovému systému či jeho datům.

#### 5.2.2.1.5 Zneužití zařízení (čl. 6)

Podle článku 6 Úmluvy o kyberkriminalitě mají smluvní strany povinnost přijmout taková legislativní a jiná opatření, která budou nezbytná k tomu, **aby** podle jejích vnitrostátních právních předpisů **byly trestnými činy, pokud jsou spáchány úmyslně a neoprávněně**:

a) **výroba, prodej, opatření za účelem použití, dovoz, distribuce nebo jiné zpřístupnění:**
   - **i. zařízení, včetně počítačového programu, vytvořeného nebo přizpůsobeného zejména za účelem spáchání kteréhokoli z trestných činů stanovených podle článků 2–5;**
   - **ii. počítačového hesla, přístupového kódu nebo podobných dat, pomocí nichž lze získat přístup do celého počítačového systému nebo do jakékoli jeho části**

s tím úmyslem, že jej bude použito pro účely spáchání kteréhokoli z trestných činů stanovených podle článků 2 až 5;

b) **a držení jedné z položek uvedených v odstavcích (a) i. nebo (a) ii. shora s tím úmyslem, že bude použita pro účely spáchání kteréhokoli z trestných činů stanovených v článcích 2 až 5.** Strana může zákonem stanovit, že trestní odpovědnost vzniká až při držení několika takových položek.

Toto ustanovení nemá být vykládáno tak, že rozšiřuje trestní odpovědnost na každé nakládání s uvedenými prostředky. K trestní odpovědnosti je vždy v těchto případech vyžadováno držení těchto prostředků v úmyslu spáchat některý z uvedených trestných činů podle článků 2 až 5 Úmluvy o kyberkriminalitě. Stejně tak toto ustanovení nedopadá na situace, kdy je testováno zabezpečení počítačového systému před škodlivými programy tím způsobem, že je počítačový systém autory bezpečnostních opatření úmyslně vystavován uvedeným hrozbám. Každá smluvní

strana si může navíc ve svém právním řádu upravit tuto skutkovou podstatu tak, že nebude dopadat na případy uvedené pod bodem a) ii).[685]

Zneužití zařízení je nejčastěji pácháno pomocích kybernetických útoků typu: malware, sniffing, cracking[686] aj. Dle českého trestního práva je možné takové útoky postihnout dle **§ 231 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat)** TZK.

*(1)* ***Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv*** *podle § 182 odst. 1 písm. b), c)* ***nebo trestný čin neoprávněného přístupu k počítačovému systému*** *a nosiči informací podle § 230 odst. 1, 2* ***vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává***

*a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo*
*b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,*

*bude potrestán odnětím svobody až na dvě léta, propadnutím věci nebo zákazem činnosti.*

V **odstavci 1** je uvedena skutková podstata základní, odkazovací, složitá.

**Objektem** je zájem *„na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolovaného opatření a přechovávání zařízení, nástrojů a prostředků, jež primárně slouží ke spáchání trestných činů porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1,2.“*[687]

Z hlediska **objektivní stránky** je jednání vyjádřeno alternativně: *„vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává“*. Pokud jde o formu, je zapotřebí jednání komisivního. **Následek** je poruchový.

Základní skutková podstata § 231 odst. 1 TZK vyžaduje, aby byly kumulativně splněny následující znaky:

685: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 70

686: viz kap. 4.3 Malware; 4.11 Sniffing; 4.9 Cracking. Přičemž tato trestná činnost se odehrává zpravidla ve třech rovinách:
1. ve snaze o trestný čin **porušení tajemství dopravovaných zpráv** (keyloggery, sniffery)
2. ve snaze o trestný čin **neoprávněného přístupu k počítačovému systému** (cracky, keyloggery, backdoors)
3. ve snaze o **porušení autorských práv** (cracky, patche, keygeny).

687: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2010, s. 2317

1) úmysl spáchat některý z uvedených trestných činů [§ 182 odst. 1 písm. b), c) nebo § 230 odst. 1, 2 TZK]

2) jednání pachatele, které spočívá ve vyrobení, uvedení do oběhu, dovezení, vyvezení, provezení, nabízení, zprostředkování, prodeji nebo jiném zpřístupnění, opatření (sobě nebo jinému) nebo přechovávání:

    a) zařízení nebo jeho součásti, postupu, nástroje nebo jakéhokoli jiného prostředku, včetně počítačového programu, vytvořeného nebo přizpůsobeného k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
    b) počítačového hesla, přístupového kódu, data, postupu nebo jakéhokoli jiného podobného prostředku, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části.

Jednání fyzické nebo právnické osoby spočívající ve výrobě, získání, či přechovávání uvedeného zařízení nebo hesla, bez naplnění fakultativního znaku subjektivní stránky skutkové podstaty trestného činu – motivu (úmyslu spáchat některý z uvedených trestných činů), není trestné. Pouhé držení prostředků uvedených v § 230 odst. 1 TZK pod písmeny a) a b) nelze kriminalizovat, neboť tyto prostředky je třeba využívat např. k vývoji nových aplikací a systémů, testování bezpečnosti počítačových systémů či jejich částí, k soudně znalecké činnosti aj.

**Vyrobením** se rozumí vlastní zhotovení (vytvoření) některého z prostředků uvedených v § 231 odst. 1 TZK pod písmeny a) a b). Vyrobení se v tomto případě bude rozumět i stanovení postupu (návodu), jímž bude možné spáchat některý z uvedených trestných činů.

**Uvedením do oběhu** se rozumí zpřístupnění některého z prostředků uvedených v § 231 odst. 1 TZK pod písmeny a) a b) širokému okruhu osob.

**Dovezením** se rozumí stav, kdy osoba dopraví zboží pocházející z cizího státu na území České republiky.

**Vyvezením** se rozumí stav, kdy osoba dopraví zboží pocházející z České republiky na území cizího státu.

**Provezením** (tranzitem) se rozumí stav, kdy je zboží přepravováno přes území České republiky.

**Nabízením** se rozumí zpřístupňování některého z prostředků uvedených v § 231 odst. 1 TZK pod písmeny a) a b) jiné osobě.

**Zprostředkováním** se rozumí poskytnutí určité formy pomoci, při které je pachatel v roli mediátora mezi osobou, která disponuje některým z prostředků uvedených v § 231 odst. 1 TZK pod písmeny a) a b) a osobou, která si tyto prostředky chce opatřit.

**Prodáním** se rozumí činnost spočívající ve směně zboží nebo služeb za peníze, případně jiné zboží či služby.

Pojmy **jinak zpřístupní** a **opatří** charakterizují situaci, kdy je některý z prostředků uvedených v § 231 odst. 1 TZK pod písmeny a) a b) např. darován či zapůjčen.

**Přechováváním** se rozumí jakýkoli způsob držení některého z prostředků uvedených v § 231 odst. 1 TZK pod písmeny a) a b). Pachatel nemusí mít uvedené prostředky přímo u sebe, stačí, že je má ve své moci a může s nimi disponovat (např. aplikace uložené v rámci sítě na jiném místě, v cloudu aj.).

**Přístupovým zařízením** se rozumí hardware, jehož pomocí je možné získat neoprávněný přístup k počítačovému systému nebo jeho části, anebo porušit tajemství dopravovaných zpráv. Takovéto zařízení je vždy spojeno se softwarem. Pokud se přístupové zařízení skládá z částí, pak k naplnění uvedené skutkové podstaty postačí i disponování s touto částí.

**Postupem** se rozumí uvedení podrobného návodu, jak spáchat některý z uvedených trestných činů. Nestačí, pokud je návod uveden pouze v hrubých rysech. Je třeba, aby tento návod byl rozpracován do detailů.

**Nástrojem** se rozumí jak prostředek sloužící k překonání fyzických bezpečnostních opatření, tak i např. počítačový program, či jeho část sloužící k překonání bezpečnostních opatření v rámci počítačových systémů.

**Počítačový program, síť elektronických komunikací, počítačový systém, nebo jeho část.**[688]

**Počítačové heslo** je prostředek sloužící pro ověření totožnosti (autentizaci) uživatele. Uživatel se jím prokazuje při přístupu ke službám, jeho znalostí prokazuje oprávnění ke službě přistupovat. Heslo je tvořeno řetězcem znaků.

**Přístupový kód** je ekvivalentem počítačového hesla. Zpravidla je uživateli přidělen a ten má omezené možnosti jeho změny (např. PIN kód aj.).

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

688: Viz kap. 1.2.3 Počítač (Počítačový systém); 1.2.3.2 Software; 5.2.2.1 Trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů; 5.2.2.2 Trestné činy ve vztahu k počítači.

Příprava dle § 20 odst. 1 TZK k tomuto činu není sama o sobě trestná, neboť se nejedná o zvlášť závažný zločin,[689] avšak uvedené ustanovení de facto kriminalizuje jednání, které mají povahu přípravy k trestnému činu (jedná se **předčasně dokonaný trestný čin**), neboť stanoví, že trestné je držení uvedených prostředků v úmyslu spáchat některý z uvedených trestných činů.

Na tomto místě je opět třeba uvést již dříve zmíněnou premisu týkající se otázky protiprávnosti, respektive oprávněnosti držení takovýchto zařízení osobami, jež zabezpečují činnost počítačových systémů, za předpokladu, že jich není zneužito ke spáchání trestného činu.[690]

### 5.2.2.2 Trestné činy ve vztahu k počítači

Do této skupiny jsou dle Úmluvy o kyberkriminalitě řazeny **trestné činy padělání a podvodu**. Padělám se však nemyslí vytváření hmotných padělků, jak jsou uvedeny v § 233, 234 a v § 244 až 246 TZK, nýbrž jde o padělání či pozměňování dat uložených v počítači.

#### 5.2.2.2.1 Padělání související s počítači (čl. 7)

Článek 7 Úmluvy o kyberkriminalitě stanoví smluvním stranám povinnost přijmout taková legislativní a jiná opatření, **aby se trestným činem stal skutek spočívající v úmyslném a neoprávněném vkládání, pozměnění, vymazání nebo potlačení počítačových dat, které povede ke vzniku nepravých (padělaných) dat s úmyslem vydávat tato data za pravá** (nebo aby na základě nich bylo jednáno tak, jako by byla data pravá), a to bez ohledu na skutečnost, zda jsou tato data přímo čitelná a srozumitelná či nikoli. Jednotlivé strany mohou stanovit, že ke vzniku trestní odpovědnosti za výše uvedené jednání je třeba ještě naplnit pohnutku v podobě úmyslu podvést jiného, nebo jednat v jiném (nečestném) úmyslu pachatele.

České trestní právo umožňuje jednání uvedené v článku 7 Úmluvy o kyberkriminalitě postihnout dle **§ 230 odst. 2 písm. c)** TZK.

*(2)* ***Kdo získá přístup*** *k počítačovému systému nebo k nosiči informací* ***a***

*c)* ***padělá nebo pozmění data*** *uložená v počítačovém systému nebo na nosiči informací* ***tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá****, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo*

689: Viz § 14 odst. 3 TZK.

690: Dále viz kap. 5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru.

*bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.*

**Objektem** této skutkové podstaty je ochrana počítačových dat (jejich pravosti) před neoprávněnou manipulací s nimi (tj. před způsobením škody v podobě narušení integrity, nesprávné funkčnosti, neoprávněného užívání dat).

**Jednání** má dvě formy, které jsou dány alternativně, vyjádřené slovy „*padělá nebo pozmění data…*". **Paděláním** se rozumí úplné vyhotovení dat nových (nepravých), která jsou odlišná od dat původních (pravých).[691] **Pozměněním dat** se rozumí modifikace dat původních (jedná se např. o změnu výše částky či číslo účtu příjemce při elektronickém bankovnictví).

**Následek** je poruchový. Alternativně je vyjádřen **účinek**: „*… aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá…*". **Hmotným předmětem útoku** u tohoto ustanovení jsou **data**.

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK). Subjektivní stránka obsahuje také fakultativní znak, **cíl činu**, jímž je pachatelův zájem na tom, aby byla data považována za pravá.

Pro správné pochopení je třeba uvést, že do kategorie počítačového padělání nebude zahrnuto padělání klasické, byť je velmi často při výrobě padělaných cenin počítač využíván. Avšak v tomto případě nejsou počítač a zejména data v něm uložená hmotným předmětem útoku, nýbrž prostředkem k vytvoření padělku.

#### 5.2.2.2.2 Podvod související s počítači (čl. 8)

Článek 8 Úmluvy o kyberkriminalitě stanoví smluvním stranám povinnost přijmout taková legislativní a jiná opatření, **aby se trestným činem stal skutek spočívající v úmyslném a neoprávněném způsobení škody na majetku jiného vkládáním, pozměňováním, vymazáním nebo potlačením počítačových dat nebo jiným zásahem do fungování počítačového systému, s úmyslem získat sobě nebo jinému majetkový prospěch**.

Tento článek Úmluvy o kyberkriminalitě v podstatě zavádí speciální druh podvodu, resp. podvod spáchaný zvláštním, specifickým způsobem – zásahem do počítačových dat nebo do funkcí počítačového systému.

691: Srov. ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2311

Do této kategorie protiprávních jednání se bude řadit zejména internetový podvod ve všech svých podobách, zejména pak phishing, pharming a spear phishing.[692] Zároveň sem spadají kombinované útoky (viz phishing v širším slova smyslu), kdy je například užito phishingového útoku, instalace malware do počítačového systému (nebo systémů) oběti a následné odčerpání finančních prostředků.

Na základě vlastní činnosti pachatele (viz kap. 4.6.1 Phishing – v užším slova smyslu a v širším slova smyslu), pak přichází v úvahu různé možnosti jeho případné trestněprávní odpovědnosti.

Pokud jde o phishing v užším slova smyslu (tedy případ, kdy útočník nezíská přístup k počítačovému systému nebo nosiči informací), je možné užít § **209** (Podvod) **a § 234** (Neoprávněné opatření, padělání a pozměnění platebního prostředku) TZK.

V případě phishingu v širším slova smyslu (případ, kdy typicky dochází k instalaci malware do počítačového systému a následnému odčerpání finančních prostředků) je možné využít § **209** (Podvod) **a § 230 odst. 2** (Neoprávněný přístup k počítačovému systému a nosiči informací) TZK.[693] K rozboru § 230 odst. 2 písm. d) TZK viz kap. 5.2.2.1.4 Zásah do systému (čl. 5). K rozboru ustanovení § 209 odst. 1 TZK:

*Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*

**Objektem** této skutkové podstaty je ochrana majetkových práv bez ohledu na formu vlastnictví.

Z hlediska **objektivní stránky** spočívá jednání pachatele v **obohacení se** tím, že:

- uvede někoho v omyl,
- využije něčího omylu nebo
- zamlčí podstatné skutečnosti.

Z § 120 (Uvedení někoho v omyl a využití něčího omylu prostřednictvím technického zařízení) TZK jednoznačně vyplývá, že *„**uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat**, zásahu do 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.“*

692: Viz kap. 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing. Jde o jeden z nejběžnějších typů kybernetických útoků.
693: Podvodu lze dosáhnout daty nejen zamlčenými, ale i neoprávněně vloženými daty - viz **§ 230 odst. 2 písm. d)** TZK.

Pokud jde o formu jednání, může být jednání jak komisivní, tak i omisivní. **Následek** je poruchový. V této skutkové podstatě je vyjádřen i účinek trestného činu v podobě způsobení škody nikoli nepatrné.[694]

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

V případě phishingu, pharmingu a podobných útoků přichází v úvahu (dle povahy vlastního útoku) i jednočinný souběh s trestným činem dle § 234 TZK, který stanoví, že trestné je i opatření, zpřístupnění, přijetí, přechovávání platebního prostředku jiného bez oprávnění. Platebním prostředkem jsou míněny i **elektronické peníze**.[695]

### 5.2.2.3 Trestné činy se vztahem k obsahu počítače

Do této skupiny kybernetických útoků jsou řazena jednání spočívající ve výrobě, držení, šíření atp. nezákonných materiálů prostřednictvím Internetu. Pokud jde o doslovné znění Úmluvy o kyberkriminalitě, tak ta do této skupiny **řadí veškeré trestné činy, které mají povahu zneužívání dětí či jinak souvisí s dětskou pornografií**. Dodatkový protokol umožnil, aby státy, které jej ratifikovaly, poskytly ochranu i před trestnými činy souvisejícími s projevy, podporou a šířením rasismu a xenofobie. Z tohoto důvodu je následující kapitola rozdělena na dvě subkapitoly, řešící každou problematiku zvlášť.

Trestné činy spočívající v držení, výrobě a šíření uvedených materiálů je samozřejmě možné spáchat i jinými způsoby než prostřednictvím počítačového systému a ICT, avšak právě tyto technologie umožnily jejich masivní rozmach, neboť podporují sdílení a ukládání velkého počtu dat v relativně krátkém čase. Dále poskytují uživateli zdání anonymity a umožňují mu uvedená data velmi rychle zničit.

694: Viz § 138 TZK – jedná se o škodu dosahující částky nejméně 5 000 Kč.

695: Blíže viz ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2354–2355
Elektronické peníze jsou druhem *elektronického platebního prostředku* (srov. § 15 zák. č. 124/2002 Sb., o platebním styku), jímž se rozumí:

a) prostředek vzdáleného přístupu k peněžní hodnotě (jako je např. elektronická platební karta – viz bod III shora), při jehož užívání se zpravidla vyžaduje identifikace držitele osobním identifikačním číslem přiděleným vydavatelem nebo identifikace jiným způsobem,

b) elektronický peněžní prostředek (tzv. elektronické peníze).

*Elektronickými penězi* se tedy rozumí elektronický peněžní prostředek jako platební prostředek, který uchovává peněžní hodnotu v elektronické podobě. Elektronickými penězi je peněžní hodnota, která představuje pohledávku za vydavatelem, je uchovávaná na elektronickém peněžním prostředku, je vydávaná proti přijetí peněžních prostředků.

#### 5.2.2.3.1 Trestné činy související s dětskou pornografií (čl. 9)

Článek 9 Úmluvy o kyberkriminalitě stanoví smluvním stranám povinnost přijmout taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů **bylo trestným činem**, pokud je spácháno úmyslně a neoprávněně následující **jednání**:

a) **výroba dětské pornografie** za účelem její distribuce prostřednictvím počítačového systému;
b) **nabízení nebo zpřístupňování dětské pornografie** prostřednictvím počítačového systému;
c) **distribuce nebo přenos dětské pornografie** prostřednictvím počítačového systému;
d) **opatřování dětské pornografie** prostřednictvím počítačového systému pro sebe nebo pro jiného;
e) **uchovávání dětské pornografie** v počítačovém systému nebo na médiu pro ukládání počítačových dat.

2) Pro účely výše uvedeného odstavce 1 "dětská pornografie" bude zahrnovat pornografický materiál, který vizuálně znázorňuje:

a) nezletilou osobu, která se účastní sexuálně jednoznačného chování;
b) osobu, jež se zdá být nezletilou, která se účastní sexuálně jednoznačného chování;
c) realistické zobrazení představující nezletilou osobu, která se účastní sexuálně jednoznačného chování.

3) Pro účely odstavce 2 shora bude termín "nezletilý" zahrnovat všechny osoby mladší 18 let.

Strana však může stanovit nižší věkovou hranici, která ale nesmí být nižší než 16 let.

4) Každá strana si může vyhradit právo nepoužít vcelku nebo zčásti odstavce 1 (d) a 1 (e), a 2 (b) a 2 (c).

Trestné činy související s dětskou pornografií lze postihnout dle následujících ustanovení trestního zákoníku, a to **§ 192 (Výroba a jiné nakládání s dětskou pornografií), § 193 (Zneužití dítěte k výrobě pornografie), § 193a (Účast na pornografickém představení) a § 193b (Navazování nedovolených kontaktů s dítětem).**

Dítě má na základě článku 34 Úmluvy o právech dítěte (z 20. listopadu 1989, New York)[696] právo na ochranu před sexuálním zneužíváním:

„***Vlády jednotlivých zemí by měly ochraňovat děti před všemi možnými sexuálními útoky a zneužíváním***. *Tomuto tématu se podrobně věnuje takzvaný opční protokol zaměřený na téma dětské prostituce a dětské pornografie.*"

696: Dále jen **Úmluva o právech dítěte.** Dítětem se dle této úmluvy rozumí osoba mladší 18 let.

Pojem **dítě** používaný v trestním zákoníku zcela respektuje Úmluvou o právech dítěte a v § 126 stanoví, že *„dítětem se rozumí osoba mladší osmnácti let, pokud trestní zákon nestanoví jinak."* Ve vztahu k výše uvedeným ustanovením trestního zákoníku bude tedy vždy ochrana poskytována osobě mladší 18 let.

Dětskou pornografií se dle trestního zákoníku rozumí *„pornografické dílo, které zobrazuje nebo jinak využívá dítě*. **Za pornografické dílo zobrazující dítě lze pokládat** např. **snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení**, dále pak **snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku** s nimi, **popř. i jiné obdobně sexuálně dráždivé snímky dětí**. Nejde-li o takové snímky, pak závěr o pornografickém charakteru díla nelze bez dalšího dovozovat jen z toho, že jsou za účelem uspokojení osob trpících sexuální deviací (tj. v tomto případě osob, pro které jsou sexuálně atraktivní nedospělé osoby) zpřístupňovány takovými prostředky, které tyto osoby vyhledávají (R 35/2005)."[697]

*§ 192 Výroba a jiné nakládání s dětskou pornografií*

*(1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, bude potrestán odnětím svobody až na dva roky.*

***(2) Stejně bude potrestán ten, kdo prostřednictvím informační nebo komunikační technologie získá přístup k dětské pornografii.***

*(3) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, anebo kdo kořistí z takového pornografického díla, bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci.*

**V odstavcích 1, 2 a 3** jsou uvedeny skutkové podstaty základní, popisné a složité.

**Objektem** těchto skutkových podstat je ochrana zdravého mravního vývoje dětí a zejména ochrana dětí před jejich zneužíváním k výrobě pornografických děl.

Z hlediska **objektivní stránky** spočívá jednání pachatele v:

- přechovávání pornografického díla, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem;

697: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1891

- získání přístupu k dětské pornografii prostřednictvím informačních nebo komunikačních technologií;
- vyrobení, dovezení, vyvezení, provezení, nabídnutí, činění veřejně přístupným, zprostředkování, uvedení do oběhu, prodání, nebo že nebo jinak jinému opatří; pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem, nebo
- kořistění z takového pornografického díla.

**Přechováváním** se rozumí jakýkoli způsob držení dětské pornografie. Pro naplnění skutkové podstaty není rozhodující, jak dlouho byla dětská pornografie držena, stejně jako není nutné, aby měl pachatel dětskou pornografii přímo u sebe (např. doma, na pracovišti, ve svém počítači), postačí, že ji má ve své moci (např. uloženou v e-mailové poště, cloudovém úložišti apod.).[698]

**Získáním přístupu** se rozumí vědomé, úmyslné jednání pachatele. K tomu, aby daná osoba mohla být činěna odpovědnou, je třeba, aby na internetovou stránku, na níž je dětská pornografie k dispozici, vstoupila úmyslně a byla si zároveň vědoma toho, že tam lze takové snímky nalézt.[699] Pokud tedy uživatel náhodně objeví stránky s dětskou pornografií, nebude jeho jednání postižitelné dle § 192 odst. 2 TZK.

**Kořistěním** se rozumí jakýkoli způsob získávání majetkového prospěchu z pornografického díla, které zobrazuje nebo jinak využívá dítě nebo osobu. *„Kořistit bude např. osoba, která za úplatu pronajme prostor pro výrobu takového díla nebo za úplatu zhotoví reklamní předměty, „pronajme" pro takové dílo prostor na svém serveru, umístí úplatně na svých stránkách odkaz na webové stránky s takovým dílem (za předpokladu, že ví, o jaké pornografické dílo jde)."*[700]

Jednání je dáno alternativně. V § 192 odst. 1 TZK je možné jak komisivní, tak omisivní jednání. V § 192 odst. 2 a 3 TZK je zapotřebí jednání komisivního. **Následek** je poruchový.

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost, nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

698: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1892

699: Srov. Směrnice Evropského parlamentu a Rady 2011/92/EU, ze dne 13. prosince 2011, o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV. [online]. [cit. 22. 8. 2016]. Dostupné z:
http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32011L0093&from=CS

700: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1894

**V případě ustanovení výroby a jiného nakládání s dětskou pornografií je třeba upozornit na kvalifikační okolnost** (jinou skutečnost**), uvedenou v § 192 odst. 4 písm. b) TZK:**

*(4) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 3*

*b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo*

Ustanovení § 117 odst. 2 uvádí, že trestný čin je spáchán veřejně, jestliže je spáchán obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí, **veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem**.

K problematice **spáchání činu veřejně přístupnou počítačovou sítí** se mimo jiné vyjádřil Nejvyšší soud (Tpjn 300/2012, stanovisko kolegia z 30. 1. 2013 – Rt 20/2013) následovně:

*„Rozesílání pornografických děl prostřednictvím e-mailové pošty mezi e-mailovými schránkami, chráněnými individuálními přístupovými hesly, nenaplňuje znak veřejně přístupná počítačová síť ve smyslu ustanovení § 205 odst. 2, odst. 3 písm. b) TZK ani ve smyslu ustanovení § 191 odst. 3 písm. b) a ustanovení § 192 odst. 3 písm. b)*[701] *TZK.“* [702]

**V případě rozesílání pornografických děl na větší počet e-mailových adres,** je-li význam tohoto jednání pro šíření díla právě s ohledem na počet oslovených adresátů srovnatelný se spácháním trestného činu tiskem, filmem, rozhlasem, televizí nebo veřejně přístupnou počítačovou sítí, **naplňuje znak „jiným obdobně účinným způsobem“** ve smyslu §191 odst. 4 písm. b) a §192 odst. 4 písm. b) TZK**. Rozeslání pornografických děl např. 163 adresátům splňuje tuto podmínku.**

To však neznamená, že by uvedená podmínka srovnatelnosti nemohla být splněna i v případě menšího počtu adresátů. Podle názoru trestního kolegia tomu tak bude **zpravidla**, když jejich počet bude tvořit **několik desítek**.[703]

Ustanovení § 192 umožňuje postihovat celou řadu jednání, při nichž je dítě zneužito pro výrobu dětské pornografie (viz kap. 4.13 Šíření závadového obsahu). Dále však umožňuje postihovat i některá jednání mající povahu sextingu.

701: V současnosti § 192 odst. 4 písm. b) TZK

702: Blíže viz Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30.1.2013. [online]. [cit. 8. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?openDocument&Highlight=0

703: Blíže viz i Nález Ústavního soudu I. ÚS 1428/13 ze dne 20. 8. 2013. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/I-1428-13.pdf

*§ 193 Zneužití dítěte k výrobě pornografie*

*(1) Kdo přiměje, zjedná, najme, zláká, svede nebo zneužije dítě k výrobě pornografického díla nebo kořistí z účasti dítěte na takovém pornografickém díle, bude potrestán odnětím svobody na jeden rok až pět let.*

V **odstavci 1** je uvedena skutková podstata základní, popisná, složitá.

**Objektem** této skutkové podstaty je ochrana zdravého mravního vývoje dětí a zejména ochrana dětí před jejich zneužíváním k výrobě pornografických děl, ale i svoboda rozhodování.

Z hlediska **objektivní stránky** spočívá jednání pachatele v tom, že:

- přiměje,
- zjedná,
- najme,
- zláká,
- svede nebo
- zneužije dítě k výrobě pornografického díla nebo
- kořistí z účasti dítěte na takovém pornografickém díle.

Jednání je dáno alternativně. Pokud jde o formu, je zapotřebí jednání komisivního.

**Zjednáním** se rozumí uzavření dohody mezi dítětem a pachatelem, že se bude dítě podílet na výrobě pornografického díla. Dohoda předpokládá souhlasný projev vůle obou stran.

**Najmutím** se rozumí dohoda mezi dítětem a pachatelem, že se bude dítě podílet na výrobě pornografického díla, ovšem za úplatu. Úplata přitom nemusí mít vždy peněžní podobu.

**Zlákáním** je získání dítěte k účasti zejména předestíráním určitých výhod, pozitiv apod. (nikoli však úplatou), zejména když dítě váhá.

**Svedením** se rozumí úmyslné vzbuzení rozhodnutí (jinak než zlákáním) v dítěti účastnit se na výrobě pornografického díla.

**Zneužít dítě** může osoba, která má vůči němu určitá práva a nebo povinnosti (např. rodič, jiná osoba, která je povinna o dítě pečovat nebo se o ně starat), nemusí jít o formalizovaný vztah.[704]

**Následek** je poruchový.

704: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 1899

**Hmotným předmětem** útoku je dítě, tedy osoba mladší 18 let.

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

*§ 193a Účast na pornografickém představení*

*Kdo se účastní pornografického představení nebo jiného obdobného vystoupení, ve kterém účinkuje dítě, bude potrestán odnětím svobody až na dvě léta.*

**Objektem** této skutkové podstaty je ochrana zdravého mravního vývoje dětí a zejména ochrana dětí před jejich zneužíváním v podobě aktivní účasti na pornografickém představení, nebo jiném obdobném vystoupení. Zároveň je chráněna i svoboda rozhodování dítěte.

**Jednání** je vyjádřeno tak, že se pachatel účastní pornografického představení nebo jiného obdobného vystoupení.

**Pornografickým představením** nebo jiným obdobným vystoupením se může rozumět takové živé vystoupení určené určitému publiku, a to i prostřednictvím informačních a komunikačních technologií.

**Následek** je poruchový.

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost, nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

*§ 193b Navazování nedovolených kontaktů s dítětem*

*Kdo navrhne setkání dítěti mladšímu patnácti let v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta.*

**Objektem** této skutkové podstaty je ochrana zdravého mravního vývoje dětí a zejména ochrana dětí před jejich zneužíváním.

**Jednání** je vyjádřeno tak, že pachatel navrhne setkání v úmyslu spáchat některý z uvedených trestných činů. V tomto případě se jedná o předčasně dokonaný trestný čin (konkrétně ve stádiu

pokusu). Pro trestnost činu pachatele stačí navržení daného setkání s uvedeným úmyslem. Není podstatné, zda se má jednání (v podobě setkání) uskutečnit v reálném nebo virtuálním světě. **Hmotným předmětem útoku** je dítě mladší patnácti let.

**Následek** je ohrožovací.

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK). Subjektivní stránka obsahuje také fakultativní znak, **motiv činu**, jímž je pachatelův zájem dopustit se trestného činu podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiného sexuálně motivovaného trestného činu.

Uvedené ustanovení umožňuje postihovat jednání mající například podobu groomingu či kybergroomingu.[705]

Domnívám se, že úprava uvedená v § 193b TZK, chránící děti před groomingem či kybergroomingem, je nedostačující, neboť se zaměřuje pouze na ochranu dětí mladších patnácti let. Jsem přesvědčen o tom, že výše uvedeným jednáním jsou stejnou měrou ohroženy jak děti mladší patnácti let, tak děti mladší osmnácti let. I díky tomu, že § 193b odkazuje na § 192 a 193, ve kterých je chráněno dítě (tedy osoba mladší 18 let), by bylo mnohem koncepčnější a vhodnější rozšířit ochranu poskytovanou tímto ustanovením i na děti mladší osmnácti let. Vlastní ustanovení § 193b TZK by pak mohlo znít:

*„Kdo navrhne setkání **dítěti** v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta.“*

#### 5.2.2.3.2 Šíření rasismu a xenofobie

Problematika šíření rasismu a xenofobie je v Dodatkovém protokolu rozdělena na následující okruhy:

a) šíření rasistických a xenofobních materiálů (**§ 356 a 403** TZK)
b) rasisticky a xenofobně motivovaná pohrůžka (**§ 352** TZK)
c) rasisticky a xenofobně motivovaná urážka (**§ 355** TZK)
d) popření, hrubé snižování, schvalování nebo ospravedlnění genocidy nebo zločinů proti lidskosti (**§ 405** TZK).

705: Viz kap. 4.14.2 Kybergrooming.

**Objektem** v bodech a), b) a c) je společenský zájem na ochraně základních lidských práv (uvedených v **čl. 1, čl. 3, čl. 15 a čl. 24** Listiny), zejména jsou chráněny osoby před jakoukoli formou diskriminace.

U trestného činu dle § 405 TZK je individuálním objektem zájem na nezkreslování historických skutečností, spojených s potlačováním práv a svobod člověka.

**Jednání** je v uvedených skutkových podstatách vyjádřeno např. slovy: *„…podněcuje k nenávisti k některému národu, rasa, etnické skupině… se spolčí nebo srotí… založí, podporuje nebo propaguje hnutí, které prokazatelně směřuje k potlačení práv a svobod člověka… aj.“*

**Následek** je ve všech případech poruchový.

**Subjekt** je ve všech případech obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je v základních skutkových podstatách uvedených trestných činů vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK).

### 5.2.2.4 Trestné činy se vztahem k autorským nebo obdobným právům (čl. 10)

Článek 10 Úmluvy o kyberkriminalitě stanoví smluvním stranám povinnost přijmout taková legislativní a jiná opatření, **aby se trestným činem stal skutek spočívající v porušení autorského práva**, jak je definováno právními předpisy této strany podle závazků, které přijala na základě Pařížské revize z 24. července 1971 Bernské Úmluvy o ochraně literárních a uměleckých děl, Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy Světové organizace duševního vlastnictví (WIPO) o právu autorském, s výjimkou jakýchkoli osobnostních práv stanovených těmi to úmluvami, pokud jsou tyto činy spáchány záměrně, v komerčním měřítku a prostřednictvím počítačového systému.

Každá strana zároveň přijme taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem porušení práv souvisejících s právem autorským, tak jak jsou definována právními předpisy této strany podle závazků, které přijala na základě Mezinárodní úmluvy o ochraně výkonných umělců, výrobců zvukových snímků a rozhlasových organizací (Římská úmluva), Dohody o obchodních aspektech práv k duševnímu vlastnictví a Smlouvy WIPO o výkonech výkonných umělců a o zvukových záznamech, s výjimkou jakýchkoli osobnostních práv stanovených těmito úmluvami, pokud jsou tyto činy spáchány záměrně, v komerčním měřítku a prostřednictvím počítačového systému.

Strana si může vyhradit právo nestanovit trestní odpovědnost podle odstavců 1 a 2 tohoto článku v omezeném rozsahu okolností, pokud jsou dostupná jiná účinná nápravná opatření a pokud tato výhrada neomezuje mezinárodní závazky strany stanovené v mezinárodních dokumentech uvedených v odstavcích 1 a 2 tohoto článku.

Trestné činy spadající právě pod čl. 10 Úmluvy o kyberkriminalitě mají nejčastěji formu kybernetických útoků typu: internetové pirátství, cracking, warez aj.[706] Jedná se o jedny z nejrozšířenějších protiprávních aktivit, které se odehrávají v kyberprostoru. České trestní právo umožňuje uvedené jednání postihnout dle **§ 270** (**Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi)** TZK.

*§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi*

*(1) Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*

V **odstavci 1** se nachází základní skutková podstata blanketní, složitá. Ustanovení § 270 TZK je blanketní právní normou odkazující zejména, avšak nikoli výhradně,[707] na autorský zákon.

**Objektem** této skutkové podstaty je ochrana duševní činnosti (*vědecké a literární, hudební, výtvarné, audiovizuální a jiné umělecké tvůrčí činnosti a požitků z ní plynoucích*), ale i práva například výrobců zvukového záznamu a zvukově obrazového záznamu, softwarového díla, práva rozhlasového a televizního vysílatele a práva pořizovatele databáze.[708] Blíže k vymezení pojmu autorského díla viz kap. 4.10.3 Autorské právo.

Z hlediska **objektivní stránky** spočívá jednání v tom, že pachatel **neoprávněně zasáhne nikoli nepatrně** do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi.

Pokud jde o formu **jednání**, bude u tohoto trestného činu převažovat jednání v komisivní formě. **Následek** je poruchový, což vyplývá z gramatického výkladu § 270 odst. 1 TZK: *„Kdo neoprávněně **zasáhne**…“*. Ve vztahu k audiovizuálním dílům a softwaru to znamená porušení pravidel upravujících nakládání s autorsky chráněnými díly ve smyslu autorského zákona. Porušení příslušné normy je zde způsobeno buďto neoprávněným nakládáním s dílem způsobem, který přísluší pouze autorovi, nebo jiným způsobem.

706: Viz kap. 4.10 Internetové (počítačové) pirátství; 4.9 Cracking.

707: Blíže viz kap. 4.10.2 Legislativní rámec.

708: Blíže viz ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2737

V ustanovení § 270 TZK je uveden i **účinek**, tj. zasáhne do chráněných práv nikoli nepatrně. Vyhodnocení účinku je rozhodné pro posouzení jednání pachatele z hlediska určení, zda se jedná trestný čin.

*„Skutečnosti nasvědčující tomu, že se jedná o* ***zásah nikoliv nepatrný, musí být posouzeny nikoliv paušálně, ale případ od případu. Významnou roli pro konstatování míry porušení autorských práv a práv souvisejících s právem autorským bude hrát zejména způsob provedení, doba trvání a rozsah poškození autorských práv a práv souvisejících s právem autorským, význam konkrétního porušeného práva apod.*** *“* [709]

**Do práva autorského neoprávněně zasahuje ten, kdo se dopustí jednání uvedeného v § 43 AZ** [tj. obchází účinné technické prostředky ochrany práv podle autorského zákona, vyrábí, dováží, přijímá, rozšiřuje, prodává, pronajímá, propaguje prodej nebo pronájem nebo drží k obchodnímu účelu výrobky nebo součástky nebo poskytuje služby (které jsou za účelem obcházení účinných technických prostředků nabízeny, propagovány nebo uváděny na trh; mají vedle obcházení účinných technických prostředků jen omezený obchodně významný účel nebo jiné užití; nebo jsou určeny, vyráběny, upravovány nebo prováděny především s cílem umožnit nebo usnadnit obcházení účinných technických prostředků)], **§ 44 AZ** (tj. bez svolení autora způsobuje, umožňuje, usnadňuje nebo zastírá porušování práva autorského tím, že odstraňuje nebo mění jakoukoli elektronickou informaci o správě práv k dílu, nebo rozšiřuje, dováží nebo přijímá za účelem rozšiřování, vysílá nebo sděluje veřejnosti, a to i způsobem podle § 18 odst. 2 AZ, dílo, ze kterého byla informace o správě práv nedovoleně odstraněna nebo změněna.) **a § 45 AZ** (tj. pro své dílo používá názvu nebo vnější úpravy již použitých po právu jiným autorem pro dílo téhož druhu, jestliže by to mohlo vyvolat nebezpečí záměny obou děl, pokud nevyplývá z povahy díla nebo jeho určení jinak.).

Takto vymezené jednání pachatele může spočívat v nesmírně různorodé škále činností [Blíže viz kap. 4.10 Internetové (počítačové) pirátství].

**Subjekt** je zde obecný, skutková podstata nevyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení. Pachatelem může být jakákoli fyzická či právnická osoba.

Z hlediska **subjektivní** stránky je vyžadováno zavinění úmyslné (viz § 13 odst. 2 TZK). Úmysl se v tomto případě musí vztahovat na všechny ostatní znaky skutkové podstaty trestného činu (tj. skutečnost, že jde o zásah nikoli nepatrný; zásah do chráněných práv aj.), včetně znaku protiprávnosti (…*Kdo neoprávněně zasáhne*…).

709: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 107

Úmysl se také *„musí vztahovat i na pachatelovo vědomí, že jde o dílo jako výsledek tvůrčí činnosti autora, jako duševní výtvor spočívající v individuálním ztvárnění myšlenky nebo že obdobně jde o umělecký výkon výkonného umělce, zvukový nebo zvukově obrazový záznam anebo o rozhlasové nebo televizní vysílání či databázi (v tomto rozsahu jde o tzv. normativní znaky skutkové podstaty, u kterých se v případě omylu postupuje podle zásad o omylu skutkovém ve smyslu § 18 TZK). Není však nutné, aby pachatel znal přesný rozsah uvedených práv autora či jiných oprávněných osob tak, jak jsou vymezena zákonem. Postačí, že pachatel si je alespoň v hrubých rysech vědom toho, že nakládá s dílem, výkonem výkonného umělce, zvukovým či obrazovým záznamem nebo rozhlasovým či televizním pořadem anebo databází, které jsou chráněny autorským právem.“*[710]

V případě porušování práv autorských a práv s tímto právem souvisejících (§ 270 TZK) je mnohdy **problematické určení výše škody.** Často je autory, či různými organizacemi, které chrání práva autorů **škoda značně nadhodnocena.** Uváděny jsou různé hypotézy poškozených vypočítávající vzniklou škodu:

- počet stažení odpovídá počtu případných návštěv kina (tj. počet stažení x cena vstupenky), či zakoupení originálního nosiče (tj. počet stažení x cena např. originálního DVD aj.),
- kdyby film nebyl ke stažení ještě před uvedením do kin, byla by návštěvnost vyšší o počet osob, které si film stáhly, což představuje ušlý zisk

K problematice určení výše škody se mimo jiné vyjádřil Nejvyšší soud (5 Tdo 171/2014 ze dne 8. 10. 2014) následovně:

***„Zatímco značný rozsah trestné činnosti obviněného R. R., kterým zákon podmiňuje použití vyšší trestní sazby podle § 270 odst. 2 písm. c) TZK, byl soudem prvního stupně objektivně zjištěn, stejný závěr nelze učinit o kvalifikačním znaku škody velkého rozsahu*** *podle § 270 odst. 3 písm. a) TZK.* ***Soudem prvního stupně stanovená výše škody částkou 11 041 514 Kč neodpovídá skutkovým zjištěním, naopak je s nimi v rozporu.*** *Při vyčíslení škody ve formě ušlého zisku se totiž přihlíží jen k té újmě, která vznikla nerozmnožením majetkových hodnot poškozeného, které bylo jinak možné reálně očekávat.*

***Z trestněprávního hlediska nemůže být vymezení výše škody v podobě ztráty na zisku ryze hypotetické.*** *Nelze-li konkrétní ušlý zisk zjistit pro nedostatek skutkových podkladů, z nichž by vyplynulo, jakého příjmu (zisku) by nositelé dotčených autorských a s nimi souvisejících práv dosáhli, kdyby obviněnému umožnili legálně zpřístupňovat ve stejné době a shodným způsobem chráněná audiovizuální a zvuková díla, nelze škodu stanovit náhradními způsoby, byť jinak akceptovatelnými při rozhodování o odškodnění.*

710: Blíže viz ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012, s. 2753

***Soud prvního stupně stanovil škodu ve formě ušlého zisku oprávněných distributorů chráněných děl jako násobek obviněným neoprávněně rozmnožených a jinými uživateli Internetu stažených děl a ceny, za kterou se v rozhodné době prodával jejich originální nosič.***

***Tvrzení soudu prvního stupně*** *o konkrétní finanční ztrátě jednotlivých nositelů práv chráněných autorským zákonem* ***stojí totiž na čistě hypotetickém a nijak nepodloženém základě, že každý uživatel Internetu, který si zdarma stáhl z datového úložiště konkrétní film nebo jiný audiovizuální nebo hudební záznam, by si jinak koupil jeho legální DVD nebo CD nosič.*** *Otázkou příčinné souvislosti mezi neoprávněným zveřejněním díla na Internetu a počtem prodaných originálních nosičů typu DVD nebo CD se soud prvního stupně blíže nezabýval.* "[711]

Z uvedeného rozhodnutí jasně vyplývá požadavek na reálné (nikoli pouze hypotetické) určení vzniklé škody. V případě porušování práv autorských a práv s nimi souvisejících se tak více než jinde musí posuzovat **případ od případu. Nelze učinit paušální závěry o vzniklé škodě či ušlém zisku.**

### 5.2.2.5 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZK)

Český zákonodárce nad rámec Úmluvy o kyberkriminalitě vymezil skutkovou podstatu, která umožňuje postih **poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZK).**

*(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté*

*a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo*
*b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,*
*a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci.*

V **odstavci 1** je uvedena skutková podstata základní, blanketní, složitá.

711: Blíže viz Rozhodnutí Nejvyššího soudu 5 Tdo 171/2014, ze dne 8.10.2014. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/675636E6F4A8497FC1257DB6003698A6?openDocument&Highlight=0

**Objektem** této skutkové podstaty je ochrana počítačového systému (jak hardwarové, tak i softwarové části tohoto systému), nosiče informací a dat v tomto systému či na nosiči uložených, před jejich poškozením, zničením, či jinou modifikací z nedbalosti.

Z hlediska **objektivní stránky** je jednání vyjádřeno alternativně: *„zničí, poškodí, pozmění nebo učiní neupotřebitelnými"* nebo *„učiní zásah"*. Pokud jde o formu, je jednání možné jak ve formě konání, tak i opomenutí. **Následek** je poruchový.

Oproti ustanovení § 230 odst. 2 písm. b) TZK je v tomto ustanovení vyžadováno, aby:

1) k uvedenému jednání došlo v důsledku porušení povinnosti, která vyplývá ze zaměstnání, povolání, postavení nebo funkce nebo je uložena podle zákona nebo je smluvně převzata;
2) nastal účinek, v podobě způsobení značné škody na cizím majetku.[712]

K pojmům: *„zničí, poškodí, pozmění nebo učiní neupotřebitelnými"* nebo *„učiní zásah"* viz § 230 TZK.

**Subjekt** je zde speciální, skutková podstata vyžaduje, aby pachatel měl zvláštní vlastnost, způsobilost nebo postavení (viz § 114 TZK). Pachatelem může být pouze fyzická či právnická osoba, která vykonává zaměstnání, povolání, postavení nebo funkci, nebo má jiné povinnosti uložené mu podle zákona nebo smluvně převzaté. Pachateli tohoto trestného činu budou z povahy věci zpravidla správci počítačových systémů, technici IT, či jiní pracovníci ICT.

Z hlediska **subjektivní** stránky je v základní skutkové podstatě třeba zavinění nedbalostní a je třeba, aby se jednalo o **hrubou nedbalost** (viz § 16 odst. 2 TZK). Jde o případ, kdy přístup pachatele k požadavku náležité opatrnosti, svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákoníkem.

I přes tuto podmínku je kriminalizace uvedeného jednání značně diskutabilní. Důvodů je hned několik. Je zřejmé, že nesprávnou manipulací s počítačovým systémem mohou vzniknout značné škody, které jsou pro některé společnosti otázkou existence či neexistence. Na druhou stranu je možné uvedenou škodu způsobit i jedinou nesprávnou rutinní operací. Další otázkou například bude, co je považováno za jednání z hrubé nedbalosti u počítačových systémů. Bude se jednat o případ, kdy správce takovéhoto systému zjevně zanedbává svoje pracovní povinnosti a neaktualizuje systém, jeho ochranné prvky apod. například po dobu 3 měsíců? Zřejmě ano. Avšak do stejné situace se dle mého názoru může dostat i správce počítačového systému, který uvedenou činnost zodpovědně provádí, avšak v den, kdy slaví narozeniny své dcery, se dozví o novém útoku malware a z důvodu požití alkoholu a své nezastupitelnosti není schopen reagovat na tuto informaci okamžitě. V případě, že by zareagoval ihned po obdržení informace, by bylo možné učinit taková opatření, aby počítačový systém nebyl tímto útokem dotčen. V případě prodlení

712: Značnou škodou je škoda alespoň ve výši 500 000 Kč (§ 138 odst. 1 TZK).

je však celý počítačový systém nenávratně zničen a škoda způsobená útokem malware je téměř nevyčíslitelná.

V tomto případě více než kdy jindy **je třeba mít na zřeteli zásadu subsidiarity trestní represe** (viz § 12 odst. 2 TZK) **a princip ultima ratio**.

### 5.2.2.6 Ostatní ustanovení trestního zákoníku mající vztah ke kybernetické kriminalitě

Další druhy trestné činnosti spáchané prostřednictvím ICT lze subsumovat i pod jiná ustanovení trestního zákona.

Existuje skupina trestných činů, při nichž dochází k **neoprávněnému užití informací**, často za využití možností Internetu (ten pak slouží jako nástroj ke spáchání určitých trestných činů, nikoli tedy jako napadený objekt). V této souvislosti je možné uvést ustanovení § 316 (Vyzvědačství), § 317 a 318 (Ohrožení utajované informace), § 255 (Zneužití informace a postavení v obchodním styku), § 180 (Neoprávněné nakládání s osobními údaji) TZK. V případě tohoto protiprávního jednání jde o zneužití či vyzrazení chráněných informací.

Samostatným trestným činem pak je **poškozování cizí** věci dle § 228 TZK. Díky kybernetickému útoku může v některých případech dojít i k poškození či zničení počítače (hardwaru). Takovéto poškození zpravidla převyšuje škodu nikoli nepatrnou, která je vyžadována tímto ustanovením.

**Trestné činy páchané např. s cílem zatajení příjmů či snížení daňové povinnosti** jsou mnohdy provedeny díky zásahům do technického či programového vybavení počítače. Jedná se o ustanovení § 254 (Zkreslování údajů o stavu hospodaření a jmění), § 264 (Zkreslení údajů a nevedení podkladů ohledně vývozu zboží a technologií dvojího užití), § 267 (Zkreslení údajů a nevedení podkladů ohledně zahraničního obchodu s vojenským materiálem), § 240 (Zkrácení daně, poplatku a podobné povinné platby). V souvislosti s hospodářskými trestnými činy je třeba zmínit i ustanovení § 236 (Výroba a držení padělatelského náčiní),[713] § 268 (Porušování práv k ochranné známce a jiným označením), § 269 (Porušení chráněných průmyslových práv, které nebyly uvedeny v rámci ochrany práva autorského, i když pod tuto ochranu spadají) TZK.

Trestné **činy páchané s cílem vyjádření svého názoru, či podpory prostřednictvím Internetu.**[714] V tomto případě půjde o § 364 (Podněcování k trestnému činu), § 365 (Schvalování

713: Trestné je i držení programu určeného k padělání. Stejně tak je trestné držení uvedeného programu i u trestného činu dle **§ 348 odst. 1** TZK.

714: V mnohých případech je prostřednictvím Internetu ne jen šířen závadný materiál, ale vyjádřením názoru či podpory může dojít k zásahu do práv jiného. V uvedených případech přichází v úvahu i trestněprávní odpovědnost pachatele za takové jednání.

trestného činu), § 355 (Hanobení národa, etnické skupiny, rasy a přesvědčení), § 357 (Šíření poplašné zprávy), § 358 (Výtržnictví) a § 184 (Pomluva) TZK.

**K zásahu do majetkových práv** dochází nejčastěji převodem finanční hotovosti z jednoho účtu na druhý pomocí počítače. Jedná se zejména o ustanovení § 205 (Krádež), § 206 (Zpronevěra), § 207 (Neoprávněné užívání cizí věci), § 209 (Podvod), § 213 (Provozování nepoctivých her a sázek. Právě k nim v poslední době dochází ve stále větší míře; jedná se zejména o internetové hry typu letadlo či pyramida; účastníci tak nemají záruku objektivnosti hry a zisk náleží organizátorům hry) TZK.

V poslední době velmi aktuální oblastí, v níž dochází ke **zneužití ICT, je jejich využití k podpoře terorismu a nátlaku na jedince**. Dochází zde k útokům na komunikační, dopravní systémy, letecký provoz aj. Půjde o ustanovení § 175 (Vydírání), § 311 odst. 2 (Teroristický útok), § 314 (Sabotáž), § 276 (Poškození a ohrožení provozu obecně prospěšného zařízení) TZK aj.

V trestním zákoníku je uvedena řada skutkových podstat, u nichž je kvalifikační okolností skutečnost, že **pachatel spáchá čin veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem**.

Jde o následující skutkové podstaty: Neoprávněné nakládání s osobními údaji § 180 odst. 3 písm. b), Pomluva § 184 odst. 2, Šíření pornografie § 191 odst. 3 písm. b), Výroba a jiné nakládání s dětskou pornografií § 192 odst. 3 písm. b), Šíření toxikomanie § 287 odst. 2 písm. c), Křivé obvinění § 345 odst. 3 písm. b), Hanobení národa, rasy, etnické nebo jiné skupiny osob § 355 odst. 2 písm. b), Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod § 356 odst. 3 písm. a), Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka § 403 odst. 2 písm. a), Podněcování útočné války § 407 odst. 2 písm. b) TZK.

## 5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru

Kyberprostor a aktivity uživatelů v něm mohou mít celou řadu podob, od naprosto legálních aktivit až po ty nezákonné. Nicméně tento virtuální prostor v mnoha oblastech představuje „šedou zónu", která vznikla díky doslova raketovému rozmachu technologií a pomalejší reakci práva na tento fenomén. Technologie a služby s nimi spojené umožňují díky svým funkcím a vlastnostem překonávat teritoriální hranice světa reálného, zároveň však ponechávají primárně na uživateli, jak důkladně si uvedené technologie a služby zabezpečí před případným kybernetickým útokem. I s velmi kvalitními znalostmi však není možné být připraven na všechny myslitelné hroby či útoky z kyberprostoru.

Do popředí se tak dostávají různé proaktivní snahy organizací[715] či společností, které se pokouší varovat, chránit, edukovat atp. uživatele, případně jim pomoci s opravou bezpečnostních chyb v jejich počítačových systémech.

Při snaze o zvyšování bezpečnosti počítačových systémů či počítačových sítí je možné legálně provádět celou řadu řadu činností, přičemž některé z nich mohou spočívat i v samotném, cíleném testování (např. zabezpečení, nastavení, zranitelnosti aj.) těchto systémů. Podle toho, v jakém rozsahu k testování dochází, je možné rozlišit:

- **cílené, předem dojednané testování,**
- **necílené** (zpravidla plošné)**, předem nedojednané testování**

počítačových systémů a počítačových sítí. Na základě tohoto rozdělení je v konkrétním případu možné aplikovat různé okolnosti vylučující protiprávnost (viz § 28-32 TZK),[716] které zaručují testujícímu subjektu jeho beztrestnost za předpokladu, že jsou splněny podmínky v těchto okolnostech uvedené.

V případě cíleného předem dojednaného testování bude zpravidla využito institutu svolení poškozeného (viz § 30 TZK a blíže viz kap. 5.3 Možnosti využití okolností vylučujících protiprávnost v rámci provádění bezpečnostních testů v kyberprostoru),[717] neboť osoba, která si testování objedná, se s testujícím subjektem domluví na vlastních podmínkách provádění testování.

715: Například CSIRT, CERT týmy, www.virustotal.com, https://www.shadowserver.org aj.

716: Ve vztahu k ICT zřejmě nedojde k využití institutů nutné obrany (§ 29 TZK) a oprávněného použití zbraně (§ 32 TZK). Nejčastěji dojde k využití institutu **svolení poškozeného** (§ 30 TZK) a **přípustného rizika** (§ 31 TZK). Viz kap. 5.3.2 Aplikace institutů trestního práva na činnosti sdružení CZ.NIC.

V praxi však může dojít i k využití **krajní nouze** (§ 28 TZK). Krajní nouzi by bylo možné využít, pokud by hrozilo nebezpečí některému ze zájmů chráněných trestním zákonem, za podmínky, že by **nebylo možno toto nebezpečí za daných okolností odvrátit jinak** (**subsidiarita**) anebo **způsobený následek je zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil** (**proporcionalita**). Anebo byl ten, komu nebezpečí hrozilo, povinen je snášet.

Z uvedených znaků explicitně vymezím znak proporcionality. V případě proporcionality se srovnávají na straně jedné ohrožené chráněné zájmy a na straně druhé zájmy, které byly obětovány. Krajní nouze bude vyloučena v případech, kdy je podle průměrného individuálního úsudku zřejmé (jasně patrné), že je obětovaný zájem rovnocenný nebo ještě závažnější než ohrožený zájem. K záchraně vlastního života nelze usmrtit jiného. Tuto podmínku krajní nouze je třeba posoudit v jednotlivém případě zvlášť s přihlédnutím ke všem konkrétním okolnostem a souvislostem.

Krajní nouzi tedy bude zřejmě možné využít například při ohrožení významnějších informačních a komunikačních systémů (např. kritická infrastruktura, serverovny aj.), kdy nebude možné nebezpečí odvrátit jinak, než například vypnutím systémů jiných (např. část sítě či počítačové systémy jiné, které jsou využívány osobami, které s nebezpečím nemají nic společného).

Blíže viz NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010, s. 157

717: Využití pojmu svolení poškozeného vychází z dikce trestního práva hmotného. Tento ustálený termín však ne zcela přesně vystihuje situaci, ke které v praxi dochází. Pokud osoba souhlasí s omezením, porušením či jiným zásahem do svých práv, pak není poškozeným.

Problém může nastat v případě provádění necíleného, předem neobjednaného či nedomluveného testování. Byť toto testování může přispět k zabezpečení jednotlivých počítačových systémů, může být zároveň zásahem do práv a svobod.

Právě tento případný střet vedl sdružení CZ.NIC k žádosti o vypracování právní analýzy možností provádění bezpečnostních testů počítačových sítí v rámci výzkumu a vývoje.[718] V rámci této analýzy jsem se snažil využít zejména prostředků trestního práva. **Domnívám se, že tato analýza může sloužit i jiným subjektům, které se se věnují problematice kybernetické bezpečnosti. Závěry zde uvedené lze použít jako vhodný základ při řešení obdobných případů** (za splnění srovnatelných podmínek), proto ji čtenáři předkládám (včetně uvedení klíčových prvků, které vedly k vyvození závěrů v rámci vlastní analýzy).

Je třeba uvést, že **každý případ je třeba posuzovat individuálně vzhledem k jeho specifikům.** Není možné přijmout paušální závěr, který by povoloval, či zamítal tu kterou činnost. Předložená analýza představuje jedno z možných východisek při zvyšování bezpečnosti v rámci kyberprostoru.

Vlastní analýza se skládala z:

- charakteristiky dožadujícího subjektu (CZ.NIC) a vymezení zkoumaných otázek;
- aplikace institutů trestního práva hmotného na činnost daného subjektu;
- vymezení dalších možných právních norem, které mohou být prováděnou činností dotčeny.

### 5.3.1 Charakteristika sdružení CZ.NIC a vymezení zkoumaných otázek

Z hlediska vlastního předmětu zkoumání bylo třeba nejprve vymezit:

1) sdružení CZ.NIC a jeho činnost jak v rámci reálného, tak virtuálního světa,
2) vlastní předmět zkoumání.

Tyto dvě oblasti byly nezbytným předpokladem pro korektní analýzu toho, zda a za jakých podmínek může sdružení CZ.NIC realizovat *„bezpečnostní analýzy počítačových sítí v rámci výzkumu a vývoje."*

#### 5.3.1.1 Charakteristika sdružení CZ.NIC, z. s. p. o.

Zájmové sdružení právnických osob CZ.NIC bylo založeno v roce 1998 a má více než 100 členů. Hlavní činností sdružení je provozování registru doménových jmen .CZ, zabezpečování provozu domény nejvyšší úrovně .CZ a osvěta v oblasti doménových jmen. V současné době se sdružení

718: V této kapitole je použita analýza, kterou jsem vypracoval na základě žádosti sdružení CZ.NIC.

věnuje rozšiřování technologie DNSSEC a služby mojeID,[719] rozvoji systému správy domén a podpoře nových technologií a projektů prospěšných pro internetovou infrastrukturu v České republice.

Sdružení také provozuje CZ.NIC-CSIRT (interní bezpečnostní tým, který byl založen 1. 6. 2008 a akreditován 26. 8. 2010) a Národní bezpečnostní tým CSIRT.CZ provozovaný od 1. 1. 2011, který od 1. ledna 2015 plní funkci Národního CERT dle § 17 zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Oba dva bezpečnostní týmy provozované sdružením CZ.NIC deklarují poskytování služeb v oblasti bezpečnosti. Mezi tyto služby mimo jiné patří:

- řešení a koordinace řešení bezpečnostních incidentů.
- osvětová a školící činnost.
- **proaktivní služby v oblasti bezpečnosti.**

*„V roce 2013 stál CZ.NIC u vzniku bezpečnostního projektu FENIX.*[720] *CZ.NIC je členem sdružení EURid spravujícího evropskou doménu EU a dalších obdobně zaměřených mezinárodních společností (CENTR, ccNSO a další). CZ.NIC chrání důvěrnost aktiv proti neautorizovanému vyzrazení. Sdružení implementuje bezpečnostní politiku informací konzistentně, plánovitě a ekonomicky efektivně. V roce 2013 získal CZ.NIC certifikaci systému managementu bezpečnosti informací (ISMS), podle normy ISO 27001.“*[721] Sdružení CZ.NIC dále vyvíjí i další aktivity v oblasti bezpečnosti.[722]

Sdružení CZ.NIC svojí dlouhodobou činností prokázalo, že je etablovaným a dlouhodobě uznávaným subjektem zabývajícím kybernetickou bezpečností.

Činnost spočívající v *„bezpečnostní analýze počítačových sítí v rámci výzkumu a vývoje“* je možné zařadit pod výše uvedené proaktivní služby v oblasti bezpečnosti, jejichž cílem je zvýšit bezpečnost informačních a komunikačních systémů nacházejících se v IP prostoru ČR, jakož i zvýšit vlastní bezpečnost koncových uživatelů.

719: **DNSSEC** je rozšíření systému DNS, které zvyšuje bezpečnost služby doménových jmen. Principem DNS je překlad jmenných internetových adres, jako například www.nic.cz nebo www.dobradomena.cz, na adresy číselné, kterým počítače rozumějí a jejichž pomocí dokážou zajistit zobrazování webových stránek, odesílání e-mailů, telefonování po Internetu a další běžné internetové služby. DNSSEC zvyšuje bezpečnost při používání DNS tím, že brání podvržení falešných, pozměněných či neúplných údajů o doménových jménech. Více informací na internetové adrese www.dnssec.cz.
**MojeID** je služba, díky níž mají uživatelé českého Internetu možnost používat pro přihlašování na různé internetové stránky a k různým webovým službám jednotné identifikační údaje (uživatelské jméno a heslo). S využitím mojeID není potřeba zakládat vždy nový účet a procházet opakovaně procesem registrace. MojeID umožňuje udržovat údaje o jeho držiteli na jednom bezpečném místě a stále aktuální. MojeID je možné využívat u všech služeb, jejichž provozovatelé podporují přímo službu mojeID či alespoň technologii OpenID. Více informací o této službě je k dispozici na internetové adrese www.mojeid.cz. Služba je pro koncové uživatele poskytována zdarma.

720: Projekt bezpečná VLAN. Blíže viz: http://fe.nix.cz/.

721: *O sdružení CZ.NIC.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.nic.cz/page/351/. A dále vlastní zkušenosti s činností a aktivitami sdružení CZ.NIC.

722: Blíže viz *Projekty pro koncové uživatele.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.nic.cz/page/2086/

V případě sdružení CZ.NIC sleduje jeho proaktivní činnost stejný účel jako trestní zákoník sám, a proto je otázkou, zda činnost, která je v souladu s právem, může být, aniž by došlo k excesu, protiprávní.

Tato skutečnost je významná zejména z pohledu možného využití okolností vylučujících protiprávnost,[723] zejména přípustného rizika.

#### 5.3.1.2 Vlastní předmět zkoumání

Ze žádosti sdružení CZ.NIC vyplynulo, že toto sdružení by mělo zájem provádět neinvazivní analýzy bezpečnosti počítačových sítí a k nim připojených veřejně dostupných systémů či služeb. Analýzy by měly být zaměřeny zejména na služby veřejně dostupné ze sítě Internet a na vyhledávání známých i neznámých bezpečnostních zranitelností.

Vlastní analytickou činnost by pak bylo na základě žádosti možné rozdělit do následujících kategorií:

1) **Zisk a analýza volně dostupných informací (Pasivní analýza)**
2) **Skenování zranitelnosti (Aktivní analýza)**
3) **Aktivní testování zabezpečení informačních a komunikačních technologií**

Jednotlivé druhy jednání jsou následně definovány v kapitolách 5.3.2.1 Zisk a analýza volně dostupných informací (pasivní analýza) až 5.3.2.3 Aktivní testování zabezpečení ICT (Přístup k počítačovému systému a nosiči informací), včetně uvedení případné právní kvalifikace.

Dle popisu činnosti by měly být v rámci jednotlivých analýz zejména detekovány:

- systémy a služby používající slabé nebo standardní autentizační údaje pro přihlášení (zejména autentizační údaje přednastavené výrobcem, prodejcem či poskytovatelem systému nebo služby);
- chyby v software či firmware zařízení používaných k provozování těchto systémů a služeb;
- zařízení používaná k provozování těchto systémů a služeb, která používají zastaralý, zranitelný či špatně nakonfigurovaný software nebo firmware.

  *V rámci analýz by tak bylo možné detekovat například:*

  - *zranitelnost ROM-0 ve firmware domácích routerů,*
  - *standardní přihlašovací údaje do domácích routerů,*
  - *standardní přihlašovací údaje do webových kamer,*
  - *zranitelné verze webových frameworků,*

723: Viz kap. 5.3.2 Aplikace institutů trestního práva na činnosti sdružení CZ.NIC a 5.3.2.3 Aktivní testování zabezpečení ICT (Přístup k počítačovému systému a nosiči informací).

- *zranitelnost HeartBleed,*
- *otevřené přístupy do domácích/firemních sítí přes IPv6,*
- *řídící mechanismy botnetů,*
- *DoS útoky.*

Dále bylo stanoveno, že vlastní analýzy mají být prováděny v tzv. „českém Internetu", tedy v sítích IPv4 a IPv6, které se nacházejí v adresním prostoru registrovaném v České republice nebo spadající do prostoru České republiky dle dostupných databází GeoIP a také služby, které jsou poskytovány doménách v doméně nejvyšší úrovně .CZ.

Vlastní analytická činnost by dle vyjádření sdružení CZ.NIC, měla být zpravidla prováděna bez vědomí dotčených osob,[724] neboť se často jedná o osoby, které vůbec netuší, že jejich počítačový systém je nebo by mohl být zranitelný. Získaná data by měla být zpracovávána za účelem vyhledávání nových ohrožení a sledování aktivity útočníků směřující ke zneužití známých hrozeb.

Výstupem analýzy by měl být seznam ohrožených systémů či služeb, který bude postoupen internímu bezpečnostnímu týmu či CSIRT.CZ. Tyto týmy by následně měly kontaktovat držitele dotčených doménových jmen či IP adres, popřípadě vlastníky/správce těchto systémů či služeb, s upozorněním na nalezené zranitelnosti.

Tato činnost koresponduje i s § 2901 OZ, který stanoví, *„že vyžadují-li to okolnosti případu nebo zvyklosti soukromého života,* ***má povinnost zakročit na ochranu jiného každý****, kdo vytvořil nebezpečnou situaci nebo kdo nad ní má kontrolu, anebo odůvodňuje-li to povaha poměru mezi osobami. Stejnou povinnost má ten,* ***kdo může podle svých možností a schopností snadno odvrátit újmu, o níž ví nebo musí vědět, že hrozící závažností zjevně převyšuje, co je třeba k zákroku vynaložit.*****"**

### 5.3.1.3 Výklad použitý při analýze zkoumaných otázek

Z hlediska aplikace trestního práva je třeba uvést, že účelem výkladu trestních zákonů je zjišťování pravého smyslu dané právní normy, zejména při její aplikaci.

Stejně jako v teorii práva, tak i v trestním právu je třeba rozlišovat druhy výkladů **podle toho, kdo zákon vykládá** (výklad autentický, legální, soudní a vědecký), **podle závaznosti** (výklad závazný a nikoli závazný), **podle metod a prostředků výkladu** (výklad gramatický, historický, systematický, logický a teleologický) a **podle poměru výkladu k doslovnému znění zákona** (výklad doslovný, extenzivní a restriktivní).

V rámci řešení zkoumaného problému bylo využito zejména výkladu **podle toho, kdo zákon**

724: Jednalo by se tedy primárně o necílené (plošné), předem nedojednané testování.

**vykládá** (dle subjektu, autora výkladu). Konkrétně došlo k aplikaci **výkladu autentického**[725] **a vědeckého** *(doktrinálního)*.[726] Předkládaná analýza tedy nemusí být nutně brána jako jediný správný a závazný výklad. Jedná se především o souhrn mých poznatků a zkušeností z oblasti aplikace práva v prostředí Internetu.

Co se týče právní závaznosti jednotlivých druhů výkladu, pak je třeba uvést, že právně závazný je pouze **výklad soudní** (*definitione a patriori*).

Jedná se o nejčastěji využívaný druh výkladu, neboť se jedná o výklad podávaný státními orgány. Uvedený výklad je součástí rozhodnutí jednotlivých případů a je závazný pouze pro konkrétní případ, který se uvedeným rozhodnutím řeší. Pro jiný orgán, a to ani pro orgán řešící obdobný případ, není tento druh výkladu právně závazný.

Samostatným druhem soudního výkladu jsou pak stanoviska Nejvyššího soudu. Tato judikatura vydávaná **Nejvyšším soudem** ve **Sbírce rozhodnutí a stanovisek** není pro soudy nižšího stupně (či jiné orgány činné v trestním řízení) právně závazná. Judikatura je však významná z hlediska sjednocování praxe orgánů činných v trestním řízení.

### 5.3.2 Aplikace institutů trestního práva na činnosti sdružení CZ.NIC

Před vlastním rozborem zkoumaného tématu bylo třeba vymezit jeden ze základních principů trestního práva, kterým je **subsidiární úloha trestní represe**. Tato zásada deklaruje, že trestního práva má být užito jako krajního prostředku (*ultima ratio*), pouze v případech, kdy nepostačuje uplatnění odpovědnosti dle jiného právního předpisu.[727]

Pokud by v případě porušení právní normy byl dostačující postih dle jiného právního předpisu, než předpisu trestněprávního, má tento předpis přednost před trestním právem. Výjimkou je případ, kdy jsou naplněny všechny znaky trestného činu, včetně společenské škodlivosti a protiprávnosti.

725: Jedná se o výklad podaný orgánem, který právní normu sám vydal (příp. byl výslovně k výkladu právní normy zmocněn právním řádem). Tento výklad je považován za druh výkladu legálního.

726: Tento výklad bývá často označován za výklad teoretický a je podáván jak pracovníky teorie, tak i praxe. Nejčastěji bývá tento výklad obsažen v odborných monografiích, učebnicích, článcích, komentářích aj. Uvedený druh výkladu není právně závazný, ale díky autoritě zpracovatele odborné publikace může vědecký výklad ovlivňovat orgány činné v trestním řízení a může přispívat i ke zdokonalování platné zákonné úpravy.

Pro předkládanou zprávu byl využit zejména výklad vědecký, který je interpretován tvůrcem trestního zákoníku v publikaci: ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář.* 2. vydání. Praha: C. H. Beck, 2012.

ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vydání. Praha: C. H. Beck, 2012.

727: Např. občanského, či správního práva.

Pro posouzení skutečnosti, zda se v daném případě jedná o trestný čin, je třeba vyjít ze samotné definice trestného činu, uvedené v § 13 odst. 1 TZK *„Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně.“*

**Protiprávnost**
Pokud schází v konkrétním případě znak protiprávnosti, nejedná se o trestný čin. Protiprávnost de facto znamená rozpor určitého jednání s právním řádem jakožto celkem. Protiprávnost je významná i z hlediska aplikace některé z okolností vylučujících protiprávnost. V případě aplikace těchto okolností se od počátku nejedná o trestný čin.

Definování protiprávnosti a okolností vylučujících protiprávnost je stěžejní pro vymezení možné trestněprávní odpovědnosti CZ.NIC za níže popsaná jednání.

**Trestné činy postihující zásah do ICT**
Z hlediska trestního práva je stěžejním ustanovením zabývajícím se zásahem do integrity ICT, jakož i dat zde uložených, ustanovení § 230 TZK. Toto ustanovení obsahuje dvě základní skutkové podstaty trestných činů, kterých by se sdružení CZ.NIC v rámci své činnosti mohlo teoreticky dopustit.

Ustanovení § 230 odst. 1 TZK **chrání před neoprávněným vniknutím do počítačového systému.**[728] Ustanovení § 230 odst. 2 TZK postihuje **neoprávněné nakládání s daty či zásahy do vybavení počítačového systému po získání přístupu k němu**. Nezáleží na tom, zda k získání přístupu došlo oprávněně či neoprávněně, neboť tato základní skutková podstata **postihuje neoprávněnou manipulaci s daty.**[729]

**Test proporcionality**[730]
Je vhodné, aby případná analytická a testovací činnost CZ.NIC byla v souladu s **testem proporcionality**, který je standardně využíván při posuzování, zda právní norma nezasahuje do základních lidských práv v míře větší než nezbytné.

Test proporcionality je soudy využíván v jiném kontextu, ale analogicky by za použití tohoto principu bylo možné vydefinovat prostor, ve kterém se může sporná činnost odehrávat. Test proporcionality je však především instrumentem, který by měl vymezit vlastní činnost sdružení CZ.NIC (způsob provádění, použité metody, prostředky aj.). Vlastní test proporcionality není schopen odvrátit případnou legální odpovědnost, nicméně může posílit postavení CZ.NIC v případném sporu.

728: **Některé aktivity popsané sdružením CZ.NIC by mohly formálně naplnit znaky skutkové podstaty tohoto činu.** Blíže viz kap. 5.2.2.1.1 Neoprávněný přístup (čl. 2).

729: Blíže viz kap. 5.2.2.1.3 Zásah do dat (čl. 4) a 5.2.2.1.4 Zásah do systému (čl. 5).

730: Blíže viz kap. 2.5.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZoEK.

Test proporcionality je **standardním právním nástrojem jak soudů mezinárodních, tak soudů ústavních (národních),** posuzuje-li se **konflikt ustanovení právního řádu, sledující ochranu ústavně zaručeného práva či veřejného zájmu, s jiným základním právem či svobodou.** Tato obecná zásada zahrnuje tři kritéria posuzování přípustnosti zásahu:

1) **princip vhodnosti** *(způsobilosti naplnění účelu), dle něhož* ***musí být příslušné opatření vůbec schopno dosáhnout zamýšleného cíle****, jímž je ochrana jiného základního práva nebo veřejného statku;*

2) **princip potřebnosti**, *dle něhož* ***je povoleno použití pouze prostředku nejšetrnějšího k dosažení požadovaného účelu*** *(zásahu do základních práv a svobod),* ***z více možných prostředků;***

3) **princip přiměřenosti** *(v užším smyslu), dle kterého* ***újma na základním právu nesmí být nepřiměřená ve vztahu k zamýšlenému cíli****, tj. opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních.*

### 5.3.2.1 Zisk a analýza volně dostupných informací (pasivní analýza)

Pasivní analýza je činnost spočívající v zisku volně dostupných informací z prostředí sítí informačních a komunikačních technologií. Vlastní analýza by měla být prováděna bez vědomí a souhlasu poskytovatelů a uživatelů služeb ICT. Tato analýza by měla mít neinvazivní povahu.

V rámci analytické činnosti by měla být testována i zranitelnost ROM-0.[731]

Při analýze zranitelnosti by mělo dle vyjádření CZ.NIC docházet k *„testování analyzovaných serverů prostřednictvím standardních požadavků s využitím běžných síťových komunikačních protokolů. Analýza bude prováděna nad hlavičkami a metadaty získanými ze síťové komunikace, případně nad zdrojovými kódy načtených webových stránek. U některých zranitelností může server vrátit i data, která je možné považovat za citlivá. Taková data však nebudou, dle sdělení CZ.NIC, nikde ukládána a samotná detekce zranitelnosti bude identifikována pouze na základě velikosti uvedených dat.“*

731: Blíže viz: Tomáš HLAVÁČEK. *Analýza: Zranitelnost „ROM-0“ postihuje 1,5 milionu domácích routerů.* [online]. [cit.20.12.2015]. Dostupné z: http://www.root.cz/clanky/analyza-zranitelnost-rom-0-postihuje-1-5-milionu-domacich-routeru/

**Definice ROM-0**

*„Jedná se o chybu nedostatečné kontroly přístupu ve webovém rozhraní pro správu routeru. Ve zkratce jde o to, že router umožňuje* ***vyexportovat a stáhnout celou konfiguraci*** *v podobě binárního souboru. Součástí konfigurace jsou, mimo jiné, i přístupová hesla k webovému administračnímu rozhraní. Chyba pak spočívá v tom, že tento soubor lze stáhnout, aniž je před tím vyžadováno heslo – stačí pouze znát jednoduché URL tohoto souboru. A kritická je tato chyba proto, že značné množství routerů ve výchozím nastavení umožňuje konfiguraci stáhnout i přes WAN rozhraní, tedy odkudkoliv z internetu.“*

Zpracování těchto dat umožní získat konkrétní představu o počítačovém systému. Lze tak zjistit například verzi firmware určitého síťového prvku, jaký webový server a v jaké verzi je pro provoz stránek používán, verzi a typ databázového systému, použité skriptovací jazyky a jejich verze, verzi operačního systému, nainstalované moduly a další informace. Rozsah a kvalita získaných informací závisí na nastavení konkrétního systému i na použitých testovacích metodách. Z takto získaných informací je možné zjistit například: neaktualizované části počítačového systému, včetně informace, jaké konkrétní zranitelnosti tyto neaktuální části ohrožují.

Vlastní sběr informací z „otevřeného prostoru" Internetu není ojedinělou a neobvyklou činností. Ke sběru a analýze dat veřejně sdílených, ať jednotlivými prvky ICT či samotnými uživateli, dochází v současnosti naprosto běžně, přičemž tento prostředek může být využit jak k legálním, tak k nelegálním účelům.

**Právě povaha účelu je významným hlediskem zakládajícím případnou trestněprávní odpovědnost.**

**V případě pasivní analýzy volně dostupných informací nedochází k naplnění skutkové podstaty trestného činu dle § 230 odst. 1 TZK.** U pasivní analýzy nedojde k překonání bezpečnostního opatření a získání neoprávněného přístupu k počítačovému systému nebo jeho části.

Vlastní získání a shromažďování volně dostupných informací by za určitých okolností mohlo být považováno za přípravu (§ 20 TZK) k trestnému činu dle § 230 odst. 1 TZK. Avšak příprava k tomuto trestnému činu není trestná.[732]

Dále by takovéto jednání mohlo naplňovat znaky skutkové podstaty dle § 231 odst. 1 písm. b) TZK:[733]

*(1)* ***Kdo v úmyslu spáchat trestný čin*** *porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací* ***podle § 230 odst. 1, 2*** *vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní,* ***sobě nebo jinému opatří nebo přechovává***

- *a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo*
- *b)* ***počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,…***

732: Viz § 20 odst. 1 a § 14 opdst. 3 TZK

733: Blíže viz kap. 5.2.2.1.5 Zneužití zařízení (čl. 6).

Z tohoto hlediska je nejvýznamnější již zmiňovaný účel provádění pasivní analýzy. Pokud je účelem této analýzy objevit případné zranitelnosti počítačových systémů a o těchto zranitelnostech informovat dotčené subjekty, nelze dovozovat skutečnost, že by sdružení CZ.NIC mělo úmysl spáchat trestný čin.

Takto popsaná činnost je naopak proaktivním opatřením, které má případné trestné činnosti předcházet. Součástí této aktivity je i varování uživatelů, respektive upozornění na nedostatky v oblasti zajištění bezpečnosti ICT, včetně uvedení doporučení sloužících k nápravě závadného stavu.

Příkladem takovéto proaktivní činnosti sdružení CZ.NIC v oblasti ochrany před zranitelností ROM-0 je možnost dobrovolného otestování vlastního počítačového systému na uvedenou zranitelnost. V případě pozitivního testu jsou uživateli sdělena doporučení, jak tuto zranitelnost odstranit. Vlastní testování probíhá na URL: http://rom-0.cz/.

V případě aktivity spočívající v testování zranitelnosti ROM-0 opět **není možné sdružení CZ.NIC prokázat úmysl spáchat trestný čin** dle § 231 odst. 1 písm. b) TZK. U vlastního testování této zranitelnosti je třeba zohlednit skutečnost, zda došlo k získání přístupu k počítačovému systému, či jeho části (viz § 230 odst. 1 či 2 TZK).

Z hlediska technického nutně nemusí dojít k získání přístupu k počítačovému systému, nebo jeho části. Toto zařízení pouze odpoví na požadavek zaslaný na konkrétní URL a odešle konfigurační soubor zařízení.

***Doporučení k provádění analýzy ROM-0:***

1) Využít institutu svolení poškozeného (§ 30 TZK – viz kap. 5.3.2.3).
2) Při testování pouze zjistit (identifikovat), zda se zranitelnost ROM-0 na konkrétním prvku ICT nachází. Vlastní konfigurační soubor nestahovat.[734]
3) Případně využít institutu přípustného rizika (§ 31 TZK – viz kap. 5.3.2.3).

### 5.3.2.2 Skenování zranitelnosti (aktivní analýza)

Při zjišťování zranitelnosti (typicky skenování komunikačních portů počítačového systému) dochází de facto k činnosti, kterou při kybernetických útocích provádí útočník při detekci bezpečnostních slabin (nedostatků) cílového systému. Prostřednictvím této aktivní analýzy je možné zjistit např.: zda je systém spuštěn, zda komunikuje s jinými systémy, jaké komunikační kanály (porty) jsou pro komunikaci vyhrazeny, jaké služby či aplikace jsou spuštěny aj. Na základě těchto

734: Za určitých okolností (viz: **získání přístupu k počítačovému systému nebo jeho části**) by takové jednání mohlo být považováno za jednání popsané v § 230 odst. 2 písm. a) TZK.

dat si pak případný útočník může učinit představu o slabinách cílového systému a je tak schopen úspěšněji provést útok samotný.

**Obdobná činnost, spočívající v aktivní analýze ICT a jejich zranitelností, je však současně standardně prováděna i bezpečnostními experty např. při auditech informačních a komunikačních systémů, při jejich penetračním testování a jiných obdobných činnostech. Smyslem a účelem této činnosti je zvýšit bezpečnost těchto systémů a zamezit tak právě neoprávněnému přístupu k nim.** Takovéto testování se standardně děje se souhlasem vlastníka (provozovatele) daného počítačového systému.

Při skenování zranitelností dochází k odeslání řady příkazů (požadavků) na analyzovaný systém. Tento systém pak odešle požadované údaje zpět.

Na základě skutečností uvedených v kap. 5.3.2.1 Zisk a analýza volně dostupných informací (pasivní analýza), je možné zcela vyloučit trestněprávní odpovědnost pro jednání uvedené v § 230 odst. 1 či odst. 2 TZK. V případě skenování portů nedochází k překonání bezpečnostního opatření a zejména není získán přístup k počítačovému systému či jeho části. Vlastní data jsou získána od analyzovaného systému na základě standardních požadavků komunikačního protokolu.

Trestněprávní odpovědnost by zřejmě nebylo možné vyvodit ani v případě, kdyby se uvedené jednání sdružení CZ.NIC svou povahou blížilo např. DoS útoku.[735] Vlastní skenování zranitelností nenaplní jednání uvedené v § 230 odst. 2. písm. b) TZK, neboť zákonodárce stanovil podmínku, že útočník: „***získá přístup** k počítačovému systému nebo k nosiči informací **a data** uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, **potlačí**, sníží jejich kvalitu nebo je učiní neupotřebitelnými.*“

Vlastní aktivní analýza (včetně skenování portů) neznamená automaticky získání přístupu k počítačovému systému nebo k nosiči informací (viz kap. 5.2.2.1.1).

Stejně tak **je možné vyloučit,** s odkazem na kap. 5.2.2.1.5, **trestněprávní odpovědnost pro jednání popsané v § 231 TZK. Pokud je účelem této analýzy objevit případné zranitelnosti systému a o těchto zranitelnostech informovat dotčené subjekty, nelze dovozovat skutečnost, že by sdružení CZ.NIC mělo úmysl spáchat trestný čin popsaný v § 231 TZK.**

Pokud by však analytickou činností došlo k omezení či celkovému potlačení funkčnosti systému, není vyloučena případná občanskoprávní odpovědnost za způsobenou škodu.

735: Viz kap. 4.12 DoS, DDoS, DRDoS útoky. **Vlastní skenování zranitelností**, tedy odesílání řady požadavků na cílová ICT zařízení **může mít povahu DoS útoku, neboť se nejedná o vyžádaný, či předpokládaný tok dat. Může docházet k abnormálnímu vytížení dotazovaných portů.**

***Doporučení při provádění aktivního skenování:***

1) Vlastní aktivní skenování provádět automaticky s omezením zaslaných požadavků na konkrétní počítačový system tak, aby nedošlo k zahlcení uvedeného systému.
2) Využít institutu svolení poškozeného (§ 30 TZK – viz kap. 5.3.2.3).
3) Případně využít institutu přípustného rizika (§ 31 TZK – viz kap. 5.3.2.3).

Závěrečné shrnutí pro kap. 5.3.2.1 Zisk a analýza volně dostupných informací (pasivní analýza) a 5.3.2.2 Skenování zranitelnosti (aktivní analýza):

V případě legitimní bezpečnostní analýzy, jejímž cílem je zvýšení kybernetické bezpečnosti a informování dotčených subjektů o možných bezpečnostních hrozbách, nedochází k naplnění skutkových podstat dle § 230 a 231 TZK ze strany sdružení CZ.NIC.

V uvedených případech není možné prokázat úmysl spáchat trestný čin. Popsaná činnost má proaktivní bezpečnostní charakter. Při vlastním jednání je však třeba se vyvarovat aktivit, jakož i excesů, které by za určitých okolností mohly vést k případné trestně či občanskoprávní odpovědnosti.

### 5.3.2.3 Aktivní testování zabezpečení ICT (Přístup k počítačovému systému a nosiči informací)

Aktivní testování zabezpečení ICT je z hlediska analýzy případné trestněprávní odpovědnosti za provádění bezpečnostních testů zřejmě nejproblematičtější.

Cílem sdružení CZ.NIC by bylo vytvoření databáze běžně používaných přístupových údajů k počítačovým systémům. V databázi budou uvedeny jak výrobci standardně používané výchozí přístupové údaje do různých počítačových systémů (např. routery, IP kamery aj.), tak také nejčastěji používaná triviální hesla, představující pro dané systémy značné riziko (*admin, 123456, qwertz, heslo1* apod.)

Tato databáze by měla být následně využita softwarovým nástrojem k automatickému procházení zařízení dostupných prostřednictvím sítě Internet a k pokusům o přihlášení do těchto zařízení s využitím přístupových údajů uložených v databázi (čili bude využívat „slovníkový útok" tak, jak tomu je v případě skutečného útočníka).

V případě úspěšného přihlášení s pomocí některého z přístupových údajů zaznamená výše popsaný automatizovaný nástroj informaci o:

- úspěšném použití přihlašovacích údajů,
- testovaném zařízení, kterého se záznam týká a
- jeho identifikaci v rámci sítě pro další využití.

Dle sdělení CZ.NIC: *„je cílem testování pouze identifikovat zranitelnost, kterou slabé přístupové heslo představuje. Se zařízením nebude CZ.NIC nijak dále nakládat ani do něj dále přistupovat.“*

*V rámci dalšího využití plánuje CZ.NIC vytvářet pro své potřeby statistické analýzy nad získanými daty a také předávat informace o nalezených zranitelnostech a vhodných způsobech zabezpečení provozovatelům jednotlivých zranitelných zařízení.“*

Pokud by CZ.NIC výše uvedenou činnost prováděl, mohl by formálně naplnit znaky skutkové podstaty trestného činu dle § 230 odst. 1 TZK, neboť při výše popsané činnosti dochází k neoprávněnému přístupu k počítačovému systému a nosiči informací tím, že je překonáno bezpečnostního opatření.

**Bezpečnostním opatřením** se rozumí jakékoli opatření, které slouží k zabránění volného přístupu k počítačovému systému nebo jeho části. **Pro naplnění jednání není rozhodující, jak sofistikované toto bezpečnostní opatření bylo.** Podstatné je, že pachatel překoná určitou překážku.

**Touto překážkou je** paradoxně míněno **i standardní bezpečnostní nastavení (vytvořené výrobcem) konkrétního prvku ICT, byť se jedná o obecně známou informaci.**

Z popisu činnosti sdružení CZ.NIC[736] však vyplývá, že toto sdružení provádí řadu proaktivních úkonů, které mají za cíl zvýšit bezpečnost „Internetu ČR“, jakož i bezpečnost koncových uživatelů.

Pro nasazení aktivního testování zabezpečení ICT spatřuji možná východiska v aplikaci následujících okolností vylučujících protiprávnost:

1) **Svolení poškozeného (§ 30 TZK)**
2) **Přípustné riziko (§ 31 TZK)**

**Ad. 1 Svolení poškozeného (§ 30 TZK)**
Svolení poškozeného vylučuje protiprávnost při splnění následujících podmínek:

- svolení musí dát pouze oprávněná osoba,
- jde o svolení vážné, dobrovolné, určité, srozumitelné a nevyvolané lstí,
- svolení je dáno osobou schopnou učinit závazný projev a
- je dáno osobou před činem nebo současně s ním.

Svolení může vyplývat ze situace a nemusí být učiněno výslovně. Pokud se někdo domníval, že svolení bylo za shora uvedených podmínek dáno (jednal v omylu), je vyloučena jeho trestní odpovědnost za úmyslný trestný čin, nikoliv za trestný čin spáchaný z nedbalosti (§ 18 odst. 4 TZK).

736: Viz kap. 5.3.1.1 Charakteristika sdružení CZ.NIC, z.s.p.o.

Je-li takové svolení dáno až po spáchání činu, je pachatel beztrestný, mohl-li důvodně předpokládat, že osoba, která může o svých zájmech oprávněně rozhodovat, by tento souhlas jinak udělila vzhledem k okolnostem případu a svým poměrům.[737]

Svolením poškozeného je v případě aktivního testování zabezpečení ICT, vyloučena odpovědnost testujícího za případné trestné činy uvedené v § 230–231 TZK.

***Doporučení:***

- Aplikace institutu svolení poškozeného v maximální možné míře, zejména pak v případech, kdy **dochází k vyžádanému testování zranitelností a zabezpečení ICT**.[738]
- Vlastní svolení může mít povahu EULA, se kterou bude testovaný subjekt seznámen před vlastním zahájením testování. V EULA by měl být subjekt upozorněn na povahu a způsob vlastního testování, stejně jako na možnost způsobení škody (např. v podobě dočasné nefunkčnosti systému ICT aj.).
- Zálohování souhlasů poškozených.
- Maximální možná automatizace systému, včetně zálohy prováděných úkonů.
- Pokud je překonáno standardní bezpečnostní opatření a není v podmínkách EULA dohodnuto jinak, ukončit vlastní testování a předat testovanému subjektu informace o nalezených zranitelnostech.

**Ad. 2 Přípustné riziko (§ 31 TZK)**
Podstatou přípustného rizika je skutečnost, že určité nové technologie, poznatky vědy aj. je třeba vyzkoušet v praxi. Stejně tak tomu je i u společensky prospěšné činnosti. Z tohoto pohledu je nutné v nezbytné míře podstoupit určité riziko.

*„Rizikem se rozumí stav nejistoty, zda se vůbec v očekávané míře dostaví žádoucí následek, a to i při vědomí, že může dojít k následku negativnímu. Negativním následkem se pak rozumí porucha nebo ohrožení zájmu, který je chráněný trestním zákoníkem. Riziko spočívá v jednání, které, pokud nastane následek relevantní z hlediska trestního práva, by vedlo k trestní odpovědnosti.* “[739]

V případě, že však budou dodrženy níže popsané podmínky a pravidla, je vyloučena protiprávnost takového jednání.

Pro to, aby bylo konkrétní jednání možné posuzovat jako přípustné riziko, musí se dle nauky i praxe jednat o činnost:

737: Srov. § 30 odst. 2 TZK

738: Obdobně jako tomu je např. u testování zranitelnosti ROM-0.

739: ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 426.

1) **v souladu s dosaženým stavem poznání a informacemi**;
2) **v době rozhodování o dalším postupu;**
3) **v rámci zaměstnání, povolání, postavení nebo funkce;**
4) **společensky prospěšnou;**
5) **při níž dochází k ohrožení nebo porušení zájmu chráněného trestním zákoníkem;**
6) **jestliže společensky prospěšného výsledku nelze dosáhnout jinak (subsidiarita rizika).**

K některým výše uvedeným znakům uvádím:

**Ad 3)**
Institut přípustného rizika je možné aplikovat i na jednání právnické osoby (viz zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob[740]), neboť dle § 7 TOPO se právnická osoba může svým jednáním dopustit i trestných činů uvedených v § 230–232 TZK.

V rámci přípustného rizika jsou zároveň **kladeny vyšší nároky na subjekt, který jedná za podmínek přípustného rizika.** Obecně lze říci, že se musí jednat o **subjekt kvalifikovaný (profesionála)**, který jedná ***lege artis***, tedy v souladu s dosaženým stavem poznání a informacemi, které má v době rozhodování o dalším postupu. Tento subjekt musí být schopen posoudit míru hrozícího rizika.

**Ad 4)**
*„Riziko musí být postoupeno za účelem dosažení společensky nutných či potřebných hodnot, očekávaný výsledek musí být rentabilní ze společenského hlediska. Riziko je společensky prospěšné, jestliže se jeho podstoupením zvyšuje celková společenská efektivnost a produktivita práce, jestliže dochází k osobním, časovým a materiálním úsporám – je přitom samozřejmé, že výhoda, o kterou se usiluje, nesmí být neoprávněná.*“[741]

Teorie uvádí, že společensky prospěšnou činností je např. rozvoj výroby, **odstranění hrozícího nebezpečí**, pokrok techniky, medicíny aj.[742]

Z uvedené dikce je zřejmé, že upozornění uživatele na nezabezpečení systému či na jeho nízké zabezpečení je činností společensky prospěšnou, která mimo jiné může vést k výše uvedeným úsporám.

**Ad 6)**
Riziko není samoúčelné. Je k němu možné přistoupit pouze v případě, kdy není jiná možnost k dosažení společensky prospěšného cíle. **K riziku je možné přistoupit i v tom případě, pokud existuje jiná možnost dosažení společensky prospěšného cíle,**[743] **avšak cíle by bylo dosaženo**

740: Dále jen **TOPO** či **zákon o trestní odpovědnosti právnických osob**.

741: ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 428.

742: NOVOTNÝ, František a kolektiv. *Trestní zákoník 2010. Komentář.* Praha: Eurounion, 2010, s. 111

743: Např. osvěta, výuka uživatelů aj.

**s nepoměrně vysokými náklady** (zejména přesahujícími hodnotu sledovaného cíle) **nebo za dlouhou dobu** (zejména hrozí-li nebezpečí z prodlení).[744]

Při aktivním testování zabezpečení ICT dochází dle mého názoru i k naplnění podmínky subsidiarity přípustného rizika, neboť pokud by k tomuto testování nedošlo, tak reálně hrozí zneužití nezabezpečených počítačových systémů a jejich připojení např. do sítě botnet aj.

Nejde však o přípustné riziko, pokud výsledek, k němuž směřuje, zcela zřejmě neodpovídá míře rizika, anebo provádění této činnosti zřejmě odporuje požadavkům jiného právního předpisu, veřejnému zájmu, zásadám lidskosti nebo se příčí dobrým mravům (§ 31 odst. 2 TZK).

**Pokud sdružení CZ.NIC splňuje podmínky uvedené pod body 1-6 přípustného rizika, pak lze dovozovat tu skutečnost, že aktivní testování zabezpečení ICT je možné provádět s odkazem na institut přípustného rizika.**

***Doporučení pro vlastní aplikaci:***

- Jasné definování a transparentní zveřejnění informací o možném aktivním testování zabezpečení ICT v IP prostoru ČR.
- Provádět tuto činnost jako společensky prospěšnou činnost. V rámci této činnosti provádět osvětu. Zveřejňovat obecná doporučení sloužící k vyššímu zabezpečení ICT systémů před obdobnými útoky.
- Aktivním testováním zjišťovat pouze zranitelnost systému, případně jeho nízké či nefunkční zabezpečení.
- Při zjištění, že je možné, po překonání bezpečnostního opatření získat neoprávněný přístup k počítačovému systému a nosiči informací, testovací činnost ukončit a neprodleně o této zranitelnosti informovat správce (vlastníka, či uživatele) takovéhoto systému.

Závěrečné shrnutí:

**V případě aktivního testování zabezpečení ICT je vhodné v co nejvyšší možné míře využít institut svolení poškozeného.**

**V ostatních případech je možné, za zákonem stanovených podmínek, provádět aktivní testování zabezpečení ICT s odkazem na institut přípustného rizika.**

**Při vlastním jednání je třeba se vyvarovat aktivit, jakož i excesů, které by za určitých okolností mohly vést k případné trestně či občanskoprávní odpovědnosti.**

744: Srov. ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář*. 2. vydání. Praha: C. H. Beck, 2012, s. 428.

### 5.3.3 Právní normy, které mohou být analýzami sdružení CZ.NIC dále dotčeny

Při provádění aktivit popsaných v kap. 5.3.2 Aplikace institutů trestního práva na činnosti sdružení CZ.NIC může dojít k implementaci i dalších právních norem a je třeba upozornit na určité povinnosti vyplývající zejména ze:

1) Zákona č. 101/2000 Sb., **o ochraně osobních údajů**, ve znění pozdějších předpisů.[745]
2) Zákona č. 89/2012 Sb., **občanský zákoník**, ve znění pozdějších předpisů.
3) Zákona č. 181/2014 Sb., **o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**, ve znění pozdějších předpisů.

**Ad. 1** V případě provádění činností popsaných v kap. 5.3.2 je zřejmé, že sdružení CZ.NIC bude shromažďovat údaje o testovaných, napadených, zranitelných informačních a komunikačních systémech, jakož i jejich případných uživatelích. V takovém případě[746] vyvstane sdružení CZ. NIC povinnost nakládat s uvedenými daty v souladu se zákonem o ochraně osobních údajů.

**Ad. 2** Při provádění činností popsaných v kap. 5.3.2 může dojít za určitých okolností ke vzniku případné občanskoprávní odpovědnosti za škodu. V takovém případě zřejmě dojde k využití § 2909 a násl. OZ. Zároveň je možné využít i § 2901 OZ (viz výše).

**Ad. 3** Dle ZKB jsou orgány a osoby uvedené v § 3 písm. b) až e) **povinny detekovat kybernetické bezpečnostní události**. Dle § 7 odst. 1) ZKB se kybernetickou bezpečnostní událostí rozumí **událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.**

Dopad činnosti sdružení CZ.NIC na subjekty definované v ZKB může být dvojího charakteru:

1) **Negativní**
Analytická a testovací činnost sdružení CZ.NIC může u testovaného subjektu (v případě, že si nebude vědom testování) evokovat pocit, že v jeho infrastruktuře byl identifikován kybernetický bezpečnostní incident, případně, že dochází ke kybernetické bezpečnostní události. Tuto situaci vyhodnotí a následně informuje národní, vládní či vlastní CERT/CSIRT.

2) **Pozitivní**
Činnosti prováděné sdružením CZ.NIC mohou napomoci subjektům s detekováním kybernetických bezpečnostních událostí či kybernetických bezpečnostních incidentů. Vlastní závěry testování mohou pomoci subjektům se zabezpečením jejich systémů.

745: Dále jen **zákon o ochraně osobních údajů** či **ZOOU**.

746: Pokud se bude jednat o osobní údaje dle § 4 písm. a ZOOU.

### 5.3.4 Shrnutí studie

Sdružení CZ.NIC, jakožto právnická osoba, je oprávněno provozovat (vykonávat) takovou činnost, která není zákonem výslovně zakázána. Toto sdružení je etablovaným a dlouhodobě uznávaným subjektem zabývajícím se kybernetickou bezpečností, který v rámci své činnosti vyvíjí řadu aktivit, které mají vést ke zvýšení bezpečnosti jak kybernetického prostoru ČR, tak uživatelů samotných.

Výše popsané aktivity (analýzy), jimiž se sdružení CZ.NIC hodlá zabývat, je dle mého názoru možné řadit pod **proaktivní služby v oblasti bezpečnosti**. Vlastní aplikace proaktivních opatření s sebou může přinášet určité nejasnosti, zejména v oblasti případné intervence do práv jiných subjektů.

Byť jsou aktivity popsané v kap. 5.3.2 (zejména pak aktivní testování zabezpečení ICT – kap. 5.3.2.3) určitým zásahem do práv testovaného subjektu, lze konstatovat, že není možné v reálném čase, za předpokladu vynaložení adekvátních prostředků a úsilí, výše popsanou zranitelnost zabezpečit jiným způsobem. Plošné varování uživatelů není zpravidla efektivní.

Všechny popsané aktivity sloužící ke zjišťování zranitelností ICT, či vlastní průnik do ICT, jsou útočníky běžně používány. Není možné připustit, aby se sdružení CZ.NIC chovalo stejně jako útočník. Na druhou stranu je však třeba aktivně vystupovat a zvyšovat zabezpečení jednotlivých prvků ICT, v důsledku čehož může dojít k vyššímu zabezpečení celé sítě Internet. Nezbytným předpokladem této činnosti je, aby uživatelé byli minimálně upozorněni na slabiny a nedostatky využívaného systému.

Proaktivní činnost, kterou hodlá sdružení CZ.NIC v této oblasti provádět, může výrazně zvýšit bezpečnost jak jednotlivých uživatelů ICT, tak celé sítě Internet v ČR.

Domnívám se, že pokud budou ze strany sdružení CZ.NIC či jiného subjektu jasně a transparentně nastaveny procesy provádění aktivit popsaných v kap. 5.3.2 Aplikace institutů trestního práva na činnosti sdružení CZ.NIC a budou zároveň dodrženy podmínky uvedené u jednotlivých institutů, nemělo by v takovém případě dojít k trestněprávnímu postihu za toto jednání. Je vhodné, aby současně docházelo k poskytování zejména metodické a další odborné pomoci uživatelům počítačových systémů.

**V případě aktivního testování zabezpečení ICT je vhodné v co nejvyšší možné míře využít institut svolení poškozeného. V ostatních případech je dle mého názoru možné, za zákonem stanovených podmínek provádět aktivní testování zabezpečení ICT s odkazem na institut přípustného rizika.**

**Při všech typech analytické či testovací činnosti je třeba se vyvarovat nežádoucích aktivit popsaných v jednotlivých subkapitolách, jakož i excesů, které by za určitých okolností mohly vést k případné trestně či občanskoprávní odpovědnosti.**

# 6 Trestněprocesní a kriminalistické aspekty odhalování, prověřování a vyšetřování kyberkriminality

# 6 Trestněprocesní a kriminalistické aspekty odhalování, prověřování a vyšetřování kyberkriminality

Obsahem této kapitoly je vymezení některých kriminalistických a procesněprávních aspektů souvisejících s **odhalováním, prověřováním a vyšetřováním kyberkriminality**. Kapitola je rozdělena na kriminalistickou a trestněprocesní část, přičemž může dojít k prolínání těchto dvou vědních disciplín, neboť spolu, zejména v oblasti kriminalistické taktiky a metodiky, úzce souvisí.

## 6.1 Kriminalistická metodika vyšetřování kybernetické kriminality

Kyberkriminalita může být namířena proti počítačům, jejich hardwaru, softwaru, datům, sítím, nebo v ní vystupuje počítač jen jako nástroj páchání trestného činu, případně je počítačová síť a k ní připojená zařízení prostředím, ve kterém se trestná činnost odehrává. Obtížnost sledování projevů kyberkriminality mimo jiné spočívá i v tom, že se uvedené jednání odehrává v prostředí, které je objektivně pouze obtížně vnímatelné. Dění v kyberprostoru je možné sledovat pouze za pomoci jiného počítače.[747]

***„Počítače v podstatě neumožňují páchat novou neetickou a trestnou činnost, poskytují jen novou technologii a nové způsoby na páchání již známých trestných činů.“***[748]

S tímto tvrzením je možné souhlasit pouze částečně. V kapitole č. 4 Projevy kyberkriminality, kde jsou demonstrovány některé z kybernetických útoků, jsem uvedl, že značná část kyberkriminality využívá či přenáší notoricky známé druhy protiprávního jednání (např. podvody, porušování práv autorských, krádeže, šikanu aj.) do prostředí nového, ve kterém je lze páchat „lépe, rychleji, efektivněji“ než ve světě reálném. **Mezi ryze kybernetické útoky, tedy „nové“ útoky, které nemají obdobu ve světě reálném, je možné zařadit např. hacking, DoS a DDoS útoky, botnety aj.**

S ohledem na specifický charakter kyberkriminality, která se mnohdy zcela vymyká běžným hranicím obecné i hospodářské kriminality, bylo třeba v průběhu posledních patnácti let vyvinout zvláštní metodiku, která použití typických prostředků dokazování rozvíjí, specifikuje a upřesňuje. Tento postup je neustále doplňován tak, jak dochází k dalším, novým způsobům kybernetických útoků či útokům, které pouze využívají prostředky ICT k efektivnějšímu páchání kriminality. Samotné vyšetřování kyberkriminality by měly vést specializované týmy složené z odborníků na danou problematiku.

747: JIROVSKÝ, V. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 19

748: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 249

### 6.1.1 Digitální stopa

*„Stále častěji se součástí důkazního materiálu, a to nejen v oblasti počítačové kriminality nebo kriminality informační, ale v podstatě u většiny dalších trestných činů, zejména v oblasti hospodářské, trestných činů proti majetku a trestných činů proti pořádku ve věcech veřejných, stávají rovněž digitální stopy.“*[749]

Z tohoto důvodu považuji za nezbytné tento základní technický pojmem, související s problematikou zajišťování dat, vymezit. Různí autoři používají mnohdy synonymně pro označení digitální stopy i pojem počítačová stopa. S vývojem informačních a komunikačních technologií je v současnosti spíše upřednostňován pojem digitální stopa, neboť její pojetí je extenzivnější, než jak tomu je u stopy počítačové. Nicméně, aby měl čtenář možnost vytvořit si vlastní názor, uvedu různé definice těchto pojmů.

*„**Počítačovou stopu** lze charakterizovat jako **změnu na nosiči informací**, vzniklou v souvislosti s trestným činem, při jehož páchání byla použita výpočetní technika a která je zjistitelná za pomoci současných metod, prostředků a operací. Tyto stopy se nacházejí na pevném disku, vyměnitelných paměťových médiích, CD ROM, disketách atp.“*[750]

Porada a Straus dále uvádějí, že *„počítačová stopa je stopou, která obsahuje vnitřní, funkční, dynamickou aj. (významovou) informaci odraženého objektu. Objekty, které zanechávají v počítačových stopách uvedené vlastnosti, jsou člověk, data a technika.“*[751]

Casey definuje počítačovou (digitální stopu) jako: *„jakákoli data uložená nebo přenesená za použití počítače, která podporují nebo prolamují teorii o tom, jak se čin stal, či která pomáhají vysvětlit záměry pachatele, nebo jeho alibi.“*[752]

Smejkal shrnuje poznatky Porady a Raka[753] a uvádí, že *„každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami. V oblasti IT/IS jsou tedy především digitální stopy, které lze definovat podle SWGDE (Scientific Working Group on Digital Evidence[754]) jako **jakékoliv informace s vypovídající hodnotou, uložené nebo přenášené v digitální podobě.** Z hlediska trestního či správního řízení je ale pro nás možná užitečnější definice International Organization of Computer Evidence*

749: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 492

750: STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 275

751: PORADA, Viktor a Jiří STRAUS. *Kriminalistické stopy. Teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, 2012, s. 280. ISBN 978-80-7380-396-4

752: Srov. CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 12 a násl.

753: Blíže viz RAK, Roman a Viktor PORADA. Charakteristiky a specifika digitálních stop. *Bezpečnostní teorie a praxe*, 2005, č. 1, s. 71–84, resp. PORADA, Viktor a Roman RAK. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství*, XVII., 2006, č. 1, s. 3–21; PORADA, Viktor a Petr ŠEDIVÝ. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94–114.

754: Blíže viz https://www.swgde.org/

*(IOCE), která definovala původně digitální stopu jako* ***jakoukoli informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz.*** "[755]

Dle serveru USLegal je digitální či elektronickou stopou (důkazem): *„jakákoli důkazní informace uložená, či přenášená digitálně."* Soudy připustily využití digitálních důkazů v řízení před soudem. Jedná se především o e-maily, digitální fotografie, elektronicky zpracované dokumenty, historie instant message (ne jen SMS, ale i zprávy odeslané pomocí instant messengerů), tabulkové procesory, historie z internetových prohlížečů, databáze, obsah počítačových pamětí (RAM), zálohy počítačových dat aj.[756]

**Domnívám se, že za digitální stopu je možné označit jakákoli data či informace přenesená, vytvořená, uložená či modifikovaná za použití počítačového systému.** Ne v každém případě se digitální stopa může (či musí) stát důkazem v řízení před soudem, avšak přesto může sloužit pro zisk dalších informací či dat, které se důkazem stát mohou. Z tohoto důvodu jsem přesvědčen o tom, že omezovat tento pojem ve vztahu použitelnosti digitální stopy jako důkazu je chyba.

Z hlediska kriminalistiky se **stopou rozumí jakákoli změna** v materiálním prostředí nebo ve vědomí člověka, která je zjistitelná, zajistitelná a využitelná současnými metodami, prostředky a postupy, mající příčinnou, prostorovou nebo časovou souvislost s kriminalisticky relevantní událostí.[757] Dle trestního práva procesního je **důkazem přímý poznatek** o předmětu důkazu, získaný orgánem činným v trestním řízení z důkazního prostředku v průběhu procesu dokazování.[758]

**Digitální (počítačová) stopa** má oproti klasickým stopám významná specifika, neboť je zpravidla značně objemná (co se velikosti dat týče), dynamická a může být rozmístěna kdekoli v kyberprostoru. **Životnost** takovéto stopy **může být velmi krátká**[759] a jakékoli průtahy jak v postupu před zahájením trestního stíhání, tak ve vyšetřování nutně vedou k její ztrátě. I díky tomu se snižuje objasněnost kyberkriminality.

V rámci trestné činnosti páchané v kyberprostoru dochází k zanechání celé řady takovýchto stop, ať již na paměťových médiích napadeného počítače, harddiscích serverů jednotlivých

755: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 492

756: Překlad autora: *Digital Evidence & Legal Definition.* [online]. [cit. 20. 2. 2014]. Dostupné z: http://definitions.uslegal.com/d/digital-evidence/. V evropském právu je možné využít **čl. 46** *Nařízení Evropského parlamentu a Rady (EU) č. 910/2014*, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS), podle kterého: **„Elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu."**

757: Srov. STRAUS, Jiří. *Úvod do kriminalistiky.* 3. vyd. Plzeň: Aleš Čeněk, 2012, s. 74. ISBN 978-80-7380-367-4.

758: *„**Důkazem** se rozumí informace plynoucí z procesních úkonů, kterou se orgán činný v trestním řízení přesvědčuje o skutečnosti důležité buď pro rozhodnutí věci, nebo pro správný postup v trestním procesu."*
Viz FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015, s. 330

759: Někdy se však může jednat i o stopu relativně velmi stálou (například stejná data replikovaná na řadě různých počítačových systémů, či uložená off-line).

poskytovatelů, či v prostředí samotném. Mimo uvedené materiální počítačové stopy je možné zajistit i jiné stopy, neboť v souvislosti s kyberkriminalitou vznikají například i **stopy písemné**[760] a především **stopy ve vědomí osob (paměťové stopy), které trestnou činnost vnímaly**. Jako samostatný zdroj stop pak může sloužit počítačový systém, zejména jeho komponenty, konfigurace a způsob jeho připojení k síti.

Mezi nejvýznamnější odlišnosti digitálních důkazů oproti stopám jiným patří dle mého názoru zejména:

- nestálost;[761]
- dostupnost (dosažitelnost);[762]
- proces zajištění;[763]
- reprodukovatelnost.[764]

760: Např. korespondence mezi prodejci nelegálního softwaru, účetní a jiné doklady aj.

761: Data přenášená prostřednictvím ICT, stejně jako přenos samotný, po sobě zanechávají stopu. Tato stopa je však relativně nestálá a zpravidla záleží na ISP či uživateli, zda, v jakém rozsahu a zejména jak dlouho tyto údaje uchovává. Někteří ISP, zejména ti, na něž se vztahuje **§ 3 ZSIS a** dále zákon o elektronických komunikacích, mají povinnost dle **§ 97 odst. 3 ZoEK** uchovávat provozní a lokalizační údaje po dobu 6 měsíců.

762: Data mohou být ukládána na různá paměťová nebo záznamová média (případně datový nosič či nosič informací), není rozhodující, zda se jedná o externí nebo interní prostředek k zápisu a uchovávání dat. Může se jednat o harddisky (HDD), operační paměti (RAM), diskety, kompaktní disky s různou hustotou zápisu (CD, DVD, Blu-Ray), paměťové karty (SD, MMC, CF karty, SDHC aj.), elektronické paměti typu USB (flashdisky) apod. **Zároveň je možné ukládat data do datových prostorů poskytovaných jednotlivými ISP, typicky jde o cloudové služby.** V takovýchto případech je z hlediska dostupnosti důležité, kde se nachází cloud provider, respektive, kde se nachází daný hardware.

Srov např. *Google odhalil technologické vnitřnosti: provozuje více než 100 tisíc serverů*. [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.svobodnymonitor.cz/byznys/google-odhalil-technologicke-vnitrnosti-provozuje-vice- nez-100-tisic-serveru/

V případě zemětřesení spojeného s vlnou tsunami v Japonsku či Thajsku je pravděpodobné, že zařízení dislokovaná v těchto destinacích, jakož i cloudy na nich běžící, nebudou po určitou dobu dostupné.

763: Vlastní proces zajištění digitálních stop je procesním úkonem, při kterém dochází k fixaci dat, zpravidla v nezměněné podobě. Nezměněnou podobu dat může např. zajistit provedení tzv. bitové kopie (bitová kopie systému je kopií veškerých dat na svazku jednotky. Bitová kopie systému standardně obsahuje jednotku nebo jednotky požadované pro běh operačního systému. Obsahuje informace o operačním systému, jeho nastavení, programy a soubory. Kopírován je bit po bitu (včetně volného prostoru) z paměťového media.

Některé způsoby zajištění dat však vytvoří kopii změněnou (např. obsahující označení vytvoření kopie, nástroje tvorby kopie aj.). Tato změna je de facto zásahem do celistvosti a unikátnosti dat, která jsou zajišťována, a může být namítáno, že se jedná o data jiná, pozměněná orgány činnými v trestním řízení.

764: Vlastní data jsou v mnoha případech uložena v podobě, která není „reálně reprodukovatelná". K reprodukci dat je zapotřebí určité aplikace či programu, který data převede do vnímatelné podoby. Vložení takovýchto dat do popsaných aplikací opět změní jejich podobu a strukturu.

Porada a Bruna uvádí další možná specifika digitálních stop. K některým specifikům jsou přidány mé vlastní komentáře. Mezi vlastnosti digitálních stop dle těchto autorů patří:[765]

- *nehmotnost digitálních stop,*[766]
- *latentnost digitálních stop,*[767]
- *manipulovatelnost s časem v počítačových systémech,*[768]
- *způsob uchování záznamů,*
- *dynamika činnosti počítačových systémů,*
- *komplexnost prostředí,*
- *vysoký stupeň interní a externí interakce probíhajících procesů,*
- *velký geografický rozsah prostoru s digitálními stopami.*

Z hlediska trestního práva procesního je v současnosti počítačová (digitální) stopa subsumována pod ustanovení § 112 odst. 1 či odst. 2 TŘ.[769]

Jsem toho přesvědčení, že subsumpce digitální stopy pod ustanovení dopadající na věcný či listinný důkaz není zcela vhodná a ne vždy je touto subsumpcí možné postihnout veškerá specifika digitální stopy.

765: PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management.* [online]. [cit. 24. 8. 2016], s. 3. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

766: K uvedenému znaku je dle mého názoru třeba podotknout, že sice digitální stopa je možná nehmotná, avšak nemůže fungovat bez hmotného substrátu (počítačového systému, nosiče dat aj.), na kterém zanechává hmotný otisk. Viz kap. 1.2.1 Kyberprostor (Cyberspace) a 1.2.3.3 Data a informace.

767: I ve vztahu k latentnosti je dle mého názoru třeba podotknout, že některé stopy sice mohou být skryté, avšak vždy je v počítačovém systému (uživatele či ISP) zanechána informace (data o určité činnosti). Primárně je tedy třeba hledat stopy na správných místech, respektive u osob, které tyto stopy mohou mít. Otázkou je, po jak dlouho dobu jsou tyto informace zaznamenávány (viz relativní nestálost digitálních stop). Blíže viz kap. 1.4 ISP (Internet Service Provider) a 3 Anonymita uživatele.

768: Toto specifikum představuje skutečně závažný problém, neboť čas (časové pásmo, datum aj.) je možné nastavit v jednotlivých počítačových systémech dle pokynu uživatele. Nicméně pokud počítačový systém provádí interakci s jiným počítačovým systémem nebo systémy, je možné vypozorovat rozdíly v nastavení času počítačových systémů a i toto rozdílné nastavení pak může být využito v trestním řízení, jakožto jeden z markantů počítačového systému.

769: Blíže viz kap. 6.3.1 Věcné a listinné důkazy.

### 6.1.2 Kriminální situace

Kriminální situace je tvořena souhrnem podmínek a okolností, které umožňují páchání kyberkriminality. Tyto podmínky předurčují nejen způsoby páchání trestných činů, ale i zákonitosti vzniku a zániku stop. Jedná se zejména o:

- úroveň právního režimu, právní a technickou ochranu dat a počítačových systémů,
- úroveň rozvoje informačních a komunikačních technologií v dané lokalitě,
- úroveň odborné připravenosti a technického vybavení orgánů činných v trestním řízení,
- úroveň kontrolní činnosti a opatření přijatých proti kumulaci funkcí pracovníků výpočetních středisek,
- specifika prostředí, ve kterém je tato trestná činnost páchána (virtuální prostředí tvořené informačními a komunikačními systémy),
- specifické postavení pachatele kyberkriminality (zpravidla se jedná odborně připravené pachatele).[770]

### 6.1.3 Zvláštnosti předmětu vyšetřování

Předmět dokazování je obecně vymezen v § 89 odst. 1 TŘ, je však specifický pro každý druh kriminality. Níže uvedený výčet není konečný a v rámci různých druhů trestných činů spáchaných prostřednictvím počítačových systémů je odlišný.

V případě kyberkriminality je třeba zejména zjišťovat:

- zda se jedná o jeden či více skutků,

- informace o vlastním útoku
  - zda došlo k zaznamenávání aktivit: útočníka a informací o zdroji útoku (např. při DoS a DDoS útocích);
  - struktura a délka útoku (typy použitých útoků, jejich časové rozložení aj.),
  - časový úsek od doby útoku do doby zajištění počítačových systémů a paměťových médií,
  - škodu způsobenou kybernetickým útokem (a to jak škodu primární tak sekundární[771]),

- informace o počítačovém systému:
  - který počítačový systém je koncovým přípojným bodem (v rámci sítě);

770: Srov. STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 271 a násl.

771: Primární škoda je způsobena např. nefunkčností, či poškozením počítačového systému. Sekundární pak typicky spočívá v uvedení počítačového systému do původního stavu.

  - na kterém počítačovém systému došlo k protiprávnímu jednání;
  - který počítačový systém byl cílem útoku,
  - verze operačního systému, software další významné informace o napadeném počítačovém systému,
  - jakým způsobem je (byl) počítačový systém zapojen do počítačové sítě (případně informace o připojených periferií),

- informace o datech:
  - jakou povahu mají napadená, poškozená, odcizená, potlačená data (např. při útoku ransomware aj.),
  - co je obsahem paměťových médií (harddisk, přenosná media aj.) včetně informace o nainstalované software,
  - originálnost (nezměněnost) uložených dat a informací, včetně zjištění kdo a v jakém rozsahu případně manipuloval s daty a informacemi,

- informace o pachateli:
  - jakým způsobem došlo k nelegálnímu jednání a zda se na něm podílelo více osob,
  - rozsah znalostí pachatele o informačních a komunikačních technologiích,
  - rozsah oprávnění pachatele k nakládání s počítačovým systémem (systémy)
  - motiv pachatele,

- okolnosti, které umožnily spáchání trestného činu,

- informace o nastavených oprávněních pro přístup k jednotlivým službám, počítačovým systémům, datovým úložištím aj.

### 6.1.4 Zvláštnosti podnětů k vyšetřování

Jedním z významných a již zmíněných specifik kyberkriminality je její páchání relativně skrytě, v kyberprostoru (např. v Darknetu). Díky tomu je možné i velmi rychle působit (ovlivňovat, či ničit) na případné stopy, které by mohly vést k pachateli (typicky se jedná o informace vztahující se k připojení počítačových systémů do sítě, registrační údaje uživatelů v rámci poskytovaných služeb aj.). Mnohdy nejsou okamžitě patrné ani následky trestné činnosti, díky čemuž může být páchána relativně nepozorovaně po delší dobu [viz kap. 4.16 APT (Advanced Persistent Threat)].

Obecně je možné podněty k vyšetřování rozdělit do následujících skupin:

1) *Oznámení fyzických či právnických osob (včetně organizací, které se věnují např. ochraně práv autorských aj.)*

2) *Oznámení od organizací, které se věnují problematice kybernetické bezpečnosti (např. CSIRT, CERT týmy aj.)*
3) *Oznámení dalších organizací (např. Internet Hotline – http://www.internet-hotline.cz/ aj.), včetně oznámení ze strany ISP*
4) *Vlastní operativně pátrací činnost orgánů činných v trestním řízení*

### 6.1.5 Zvláštnosti vyšetřovacích verzí a organizace vyšetřování

Ve vztahu ke kyberkriminalitě se vytvářejí **verze** zejména **ke způsobu spáchání** trestného činu. Konrád uvádí, že je možné vytýčit tyto verze:

- *verze o neoprávněném zásahu do vstupních dat,*
- *verze o provedení neoprávněných změn v uložených datech,*
- *verze o provedení neoprávněných pokynů k počítačovým operacím,*
- *verze o neoprávněném proniknutí do počítačových systémů a jeho databází,*
- *verze o napadení cizího počítače, jeho programového vybavení a souborů dat v databázích* (nejčastěji se jedná o napadení pomocí malware aj.),[772]

Viktoryová mimo zde uvedené verze uvádí ještě:[773]

- *verze o zneužití počítače a jeho komunikačních prostředků* (jsou vytyčovány zejména v případech podvodů spáchaných pomocí počítače),
- *verze o neoprávněném přístupu pachatele k datům:*
  - verze o neoprávněném převodu finančních prostředků z napadeného účtu na účet jiný,
  - verze o úpravě vytvořeného souboru pro elektronický bankovní styk (typicky Phishing a Pharming).

Domnívám se, že výše uvedené verze je možné doplnit o:

- **verze o neoprávněném vniknutí do počítačového systému** (typicky hacking),
- **verze o potlačení služeb či činnosti počítačového systému** (např. DoS, DDoS),
- **verze o podvodném získání informací bez provedení neoprávněného zásahu do počítačového systému** (např. zisk informací pomocí internetových podvodů či identity theft) aj.

S nárůstem a vývojem kyberkriminality, zejména pak s její rozmanitostí, dojde bezpochyby k vývoji a obměně uvedených vytýčených verzí.

772: STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 284 a násl.

773: Blíže VIKTORYOVÁ, Jana, Ján PALAREC, Jaroslav BLATNICKÝ, Viktor PORADA. *Metodika vyšetřovania počítačovej kriminality a softwarového pirátstva.* Bratislava: Akadémia policejného zboru SR, 2004, s. 36 a násl.

### 6.1.6 Zvláštnosti následných úkonů

V rámci následných úkonů se zaměřím pouze na výslech obviněného a svědka, neboť expertiza je obsahem kapitoly 6.5 Znalec. U kyberkriminality je významná velmi precizní příprava na samotný výslech. Zároveň jsou předpokládány určité znalosti a zkušenosti vyslýchajícího s touto trestnou činností.[774] Pokud se na trestné činnosti podílí více osob, je vhodné nejprve vyslýchat osoby, které mají menší podíl na trestné činnosti, neboť mohou být významným zdrojem informací pro orgán činný v trestním řízení. Samotný **výslech obviněného** se řídí obecnými pravidly uvedenými v § 92 a násl. TŘ. Je třeba jej modifikovat v návaznosti na konkrétní typy kyberkriminality. Obecně lze stanovit, že je vhodné zaměřit se na zjištění těchto skutečností:

- osobní, majetkové, výdělkové poměry a předchozí tresty (§ 91 TŘ),
- informace vztahující se k úmyslu spáchat trestný čin,
- informace o podílu osoby na trestném činu, případně existenci spolupachatelů (jejich podíl na trestné činnosti),
- informace o způsobu spáchání trestného činu (otázky týkající se utajení trestné činnosti, vlastního postupu pachatele, atd.):
  - využití sociálního inženýrství či jiných netechnických prostředků,
  - popis mechanismů zásahu do počítačového systému či programového vybavení počítačového systému (následky těchto zásahů – jaká data byla pozměněna, potlačena, odstraněna, atd.),
  - jakým způsobem se pachatel dozvěděl, kterou činnost je třeba v rámci kybernetického útoku provést, či zda jde o jeho vlastní invenci,
  - jakým způsobem maskoval svoji činnost aj.
- informace o tom, co bylo trestným činem získáno (finanční prostředky, informace, nelegální materiály - např. dětská pornografie aj.) a jak byl tento zisk využit.[775]

**Svědky lze rozdělit do dvou skupin:**

1) Svědky podávající výpověď ke způsobu zavádění dat do počítače, k prováděným operacím, ke způsobu spáchání. Jde de facto o „svědky odborníky".
2) Svědky, kteří podávají výpověď k neodborným otázkám (osobním, pracovním a jiným poměrům obviněného).[776]

774: Pokud nemá orgán činný v trestním řízení dostatečné zkušenosti a znalosti v oblasti ICT, může dle **§ 157 odst. 3 TŘ využít odborné pomoci konzultanta**, který má znalost ze speciálního oboru. Státní zástupce nebo policejní orgán využije konzultanta zejména v závažných a skutkově složitých případech. Tuto možnost má i soud (viz § 183 odst. 2 TŘ).

775: Srov. STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 285 a násl.
Srov. VIKTORYOVÁ, Jana, Ján PALAREC, Jaroslav BLATNICKÝ, Viktor PORADA. *Metodika vyšetřovania počítačovej kriminality a softwarového pirátstva.* Bratislava: Akadémia policejného zboru SR, 2004, s. 48 a násl.

776: Blíže STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 285 a násl.

Samotný **výslech svědka** se řídí obecnými pravidly uvedenými v § 99 a násl. TŘ. Je třeba jej modifikovat v návaznosti na konkrétní typy kyberkriminality. Typické otázky pokládané znalci jsou náplní kapitoly 6.5 Znalec, proto se na tomto místě zaměřím na otázky pokládané ostatním svědkům. Obecně lze stanovit, že je vhodné zaměřit se na zjištění těchto skutečností:

- Informace o vlastním útoku (obdobně jako v kap. 6.1.3 Zvláštnosti předmětu vyšetřování)
- které osoby měly přístup k počítačovému systému, kdo je oprávněn obsluhovat počítačový systém a instalovat do něj software,
- kdy se osoba dozvěděla o neoprávněném zásahu do počítačového systému či jeho vybavení,
- počet periferií a paměťových médií (nosičů informací) připojených k počítačovému systému,
- oblasti, do kterých měl uživatel (či počítačový systém) v rámci sítě povolen přístup,
- zda byla způsobena škoda či jiná újma. Pokud ano, jaká.
- u společnosti, která počítačový systém dodala či jej spravuje, je třeba zjistit:
  - kteří pracovníci odběratele pracovali s daným software,
  - zda došlo k reklamaci jejich produktu či jeho části,
  - zda byly provedeny úpravy programového vybavení či systému. Pokud ano, z jakého důvodu.
  - zda tato společnost provádí správu nainstalovaných programů,
  - jestli je možné provést výpis vstupů do počítače aj.

## 6.2 Trestněprocesní postup při odhalování, prověřování a vyšetřování kyberkriminality

V následující subkapitole budou popsána určitá specifika úkonů spojených se zjišťováním, zda se stal skutek, zda je tento skutek trestným činem, kdo je jeho pachatelem, jakož i další podstatné okolnosti mající vliv na posouzení povahy a závažnosti činu, osobních poměrů pachatele, stanovení následku (výše škody) a okolnosti, které vedly k trestní činnosti nebo umožnily její spáchání.[777]

### 6.2.1 Specifika přijetí trestního oznámení a prověřování

Každé trestní řízení začíná sepsáním záznamu o zahájení úkonů trestního řízení nebo provedením neodkladných a neopakovatelných úkonů, které mu bezprostředně předcházejí, a nebyly-li tyto úkony provedeny, zahájením trestního stíhání.[778] Orgány činné v trestním řízení se o skutečnosti, že byl spáchán trestný čin v rámci Internetu, nejčastěji dozvídají na základě trestních oznámení.[779]

777: Viz § 89 odst. 1 TŘ

778: § 12 odst. 10 TŘ

779: Dozvídat se tyto skutečnosti mohou též z vlastní činnosti či jiných podnětů. Ve vztahu ke kyberkriminalitě jsou však nejběžnější právě trestní oznámení (jakožto druh podání viz § 59 TŘ).

Přijetí oznámení od oznamovatele, jeho precizní zpracování a **zajištění prvotních informací a důkazů** je při řešení kyberkriminality životně důležité. V této fázi trestního řízení je třeba **co nejpreciznějí zajistit informace týkající se vlastního kybernetického útoku**. Pokud je to možné, je třeba od oznamovatele (např. poškozeného) zajistit data v co nejméně změněné podobě [např. originály e-mailových zpráv, nosič informací (paměťové médium) či celý počítačový systém, atp.], pokud to není možné, pak získat například kopie těchto dat, printscreeny aj.

Významným zdrojem informací je propojení počítačového systému do sítě a přidělení IP adresy (viz kap. 1.3.2 Internet Protocol a IP adresa). **Pro identifikaci počítačového systému** (a případně útočníka) **je třeba znát** kromě **IP adresy i datum a přesný čas připojení počítačového systému do počítačové sítě**. **Díky své jedinečnosti a unikátnosti je právě IP adresa jedním z klíčových identifikátorů sloužících k identifikaci pachatele kyberkriminality.** K vlastnímu zjištění koncového počítačového systému je však třeba znát principy připojování těchto systémů do počítačové sítě a principy využívané k přidělování IP adresy (viz kap. 1.3 Počítačové sítě a jejich fungování a NAT – poznámka č. 132).

Na základě procesu připojování[780] počítačového systému do různých počítačových sítí (a podsítí) či k různým službám (např. e-mail, sociální sítě, cloudová úložiště aj.) je možné zjistit například zdroj útoku a jiné informace. Dílčí informace je možné získat od jednotlivých ISP (poskytovatelů služeb informační společnosti) v závislosti na poskytované službě.

Pachatel v rámci páchání trestné činnosti v kyberprostoru nemusí a mnohdy nemá povědomí o té skutečnosti, že ISP poskytující připojení či jinou službu drží a uchovává informace o počítačových systémech, včetně informace o IP adrese, času a délce používání dané služby.

Významnými mohu být i informace o procesu identifikace, respektive autentizace uživatele ve vztahu k jednotlivým používaným počítačovým systémům a zejména službám. Tyto informace je možné korelovat a v souvislosti s dalšími informacemi mohou pomoci vytvořit profil uživatele počítačového systému. Zároveň je z nich možné získat další významné informace (např. další využívané služby či počítačové systémy aj.) pro trestní řízení.

V případě podání trestního oznámení dle § 59 odst. 4 TŘ (pokud zákon pro podání určitého druhu nevyžaduje další náležitosti) musí být z podání patrné:

- kterému orgánu činnému v trestním řízení je určeno,
- kdo jej činí,
- které věci se týká a co sleduje, a
- musí být podepsáno a datováno.

780: Viz kap. 1.3 Počítačové sítě a jejich fungování a 1.4 ISP (Internet Service Provider).

Je-li oznamovatel zároveň poškozeným nebo jeho zmocněncem, musí být vyslechnut též o tom, zda žádá, aby soud rozhodl v trestním řízení o jeho nároku na náhradu škody.

**Státní orgány jsou povinny neprodleně oznamova**t státnímu zástupci nebo policejním orgánům **skutečnosti nasvědčující tomu, že byl spáchán trestný čin** (§ 8 odst. 1 TŘ).

Pokud je z obsahu trestního oznámení patrné, že jde o trestný čin, případně kdo je jeho pachatelem, a není bezprostředně nutné provést úkony sloužící k zabránění pokračování trestného činu nebo k odvrácení hrozícího nebezpečí, postupuje policejní orgán v souladu se svou věcnou příslušností, a to tak, že je sepsán **záznam o zahájení úkonů trestního řízení** (§ 158 odst. 3 TŘ), **ve kterém uvede:**[781]

- **skutkové okolnosti,**
- **způsob, jakým se o nich dozvěděl.**

Pro další postup v trestním řízení je nezbytná existence právě záznamu o zahájení úkonů trestního řízení dle § 158 odst. 3 TŘ. Bez něj není možné uskutečnit další trestněprocesní postupy. Obecně je doporučeno, aby orgány činné v trestním řízení (OČTR) postupovaly standardně jako v případech běžných trestních oznámení.[782]


Obrázek 85: Zjednodušené schéma zahájení úkonů trestního řízení

Na základě analýzy obsahu trestního oznámení a s přihlédnutím ke všem informacím získaným při prověřování skutečností nasvědčujících tomu, že byl spáchán trestný čin, by měl orgán činný v trestním řízení určit, o jaký druh kybernetického útoku se jedná, včetně subsumpce uvedeného jednání pod znaky skutkové podstaty některého z trestných činů. Po zahájení úkonů trestního řízení v konkrétní věci dle § 158 odst. 3 TŘ se orgány činné v trestním řízení v tomto stadiu trestního řízení snaží zajistit další informace a důkazy nasvědčující tomu, že byl spáchán skutek

781: Blíže NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009, s. 256
782: Viz tamtéž s. 254

a že tento skutek je trestným činem a zejména se snaží určit pachatele tohoto skutku, proti kterému by bylo možné zahájit trestní stíhání.

#### 6.2.1.1 Určení místní příslušnosti OČTŘ

V této fázi trestního řízení bývá často řešena otázka určení místní příslušnosti orgánu činného v trestním řízení, byl-li spáchán trestný čin v kyberprostoru. Ve vztahu k určení této příslušnosti je třeba užít § 18 TŘ, kde je uvedeno:

1) *Řízení koná soud, v jehož obvodu byl trestný čin spáchán.*
2) *Nelze-li místo činu zjistit nebo byl-li čin spáchán v cizině, koná řízení soud, v jehož obvodu obviněný bydlí, pracuje nebo se zdržuje; jestliže se nedají tato místa zjistit nebo jsou mimo území České republiky, koná řízení soud, v jehož obvodu čin vyšel najevo.*

Ustanovení **§ 18 odst. 1** TŘ, dle kterého koná řízení soud, v jehož obvodu byl trestný čin spáchán, **nelze ve většině případů aplikovat**, neboť z důvodu specifičnosti (celosvětového charakteru) Internetu nelze zjistit místo spáchání trestného činu (neexistuje lokalizovatelné místo - místem spáchání činu je virtuální kyberprostor).

Z tohoto důvodu je třeba užít § 18 odst. 2 TŘ, které uvádí: **„nelze-li místo činu zjistit** *nebo byl-li čin spáchán v cizině, koná řízení soud, v jehož obvodu obviněný bydlí* (v tento okamžik však obviněného neznáme), *pracuje, nebo se zdržuje; jestliže se nedají tato místa zjistit nebo jsou mimo území České republiky,* **koná řízení soud, v jehož obvodu čin vyšel najevo.“**

Pojmem **„vyšel najevo“** (tzv. ***forum scientiae***) se charakterizuje místo, kde se poprvé některý z orgánů činných v trestním řízení dozvěděl o spáchání trestného činu (např. z oznámení o trestném činu); z tohoto důvodu není možné výraz „vyšel najevo“ ztotožňovat jen se zahájením trestního stíhání dle § 160 odst. 1 TŘ. Pokud vyšel čin najevo na více místech, řeší se otázka místní příslušnosti dle § 22 TŘ.[783]

**Je důležité, aby případy kyberkriminality byly již od počátku řešeny dle místní příslušnosti** (v řadě případů tedy tam, kde čin vyšel najevo)**, neboť jakékoli časové zdržení může mít za následek možnou ztrátu dat (důkazů).**

783: Blíže FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015, s. 143-144

### 6.2.1.2 Součinnost státních orgánů, fyzických a právnických osob

Ustanovení § 7 TŘ a následující řeší problematiku součinnosti státních orgánů, fyzických a právnických osob. Ustanovení § 7 TŘ deklaruje povinnost vzájemné součinnosti orgánů činných v trestním řízení při plnění úkolů vyplývajících z trestního řádu.

Dle § 8 odst. 1 TŘ jsou *„**státní orgány, právnické a fyzické osoby povinny bez zbytečného odkladu,** a nestanoví-li zvláštní předpis jinak, **i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů.**“*

Toto ustanovení umožňuje podstatně zrychlit trestní řízení[784] a zároveň se jím omezuje používání dalších instrumentů trestního řádu, které mají intenzivnější dopad na základní lidská práva a svobody, na míru nezbytně nutnou pro splnění účelu trestního řízení.[785]

**Vlastní dožádání mohou být uplatňována v průběhu celého trestního řízení a mohou mít rozličnou povahu.** Vzhledem ke specifičnosti kyberkriminality uvedu některé typické dotazy dle § 8 odst. 1 TŘ, které jsem rozdělil podle toho, k čemu směřují:

1) **IP adresa**
   - Zjištění smluvního vztahu - typicky se jedná o zjišťování informací, které poskytovatel služby zaznamenává, typicky při uzavření smlouvy či její změně:
     - zjištění uživatele, který uzavřel smlouvu, nebo je oprávněn čerpat plnění;
     - zjištění, zda je IP adresa sdílená;
     - umístění přípojného bodu (geolokace);
     - kopie smluv uzavřených mezi uživatelem a poskytovatelem služby;
     - kopie faktur, příkazů k platbám a podobně.
   - Zjištění umístění sdružovacího zařízení (AP, ROUTER) veřejné IP adresy
   - Zjištění, zda mají uživatelé za NAT přidělené statické, nebo dynamické IP adresy
   - Zjištění jedinečného identifikátorů uživatelů za NAT (MAC adresa, vnitřní IP adresa)

Pokud je třeba kontaktovat přímo „vlastníka“ (operátora, poskytovatele) konkrétní IP adresy s tím, že veřejně dostupné informace jsou nedostačující a **smyslem dotazu je pouze zjistit**, zda je konkrétní IP adresa statická, dynamická, zda je „natovaná“, je možné využít ustanovení § 8 odst. 1 TŘ.[786]

784: Viz **zásada rychlosti trestního řízení**.

785: Viz **princip minimalizace zásahu do zákonem chráněných lidských práv a svobod**.

786: Smyslem výše popsané činnosti je pouze „ověření stavu“, resp. zjištění dalších informací nezbytných pro další postup orgánů činných v trestním řízení.

2) **e-mail**
   - Informace o uživateli
   - Zjištění identifikačních a registračních údajů
   - Informace, zda byl využit institut zapomenuté heslo,
     - Změna hesla
     - Vyplnění nového formuláře
   - Vyhledání všech účtů určitého uživatele (vystupujícího pod určitým identifikátorem)
   - Informace jaké všechny služby uživatel využívá
   - Datum založení schránky
   - Zjištění některých informací z adresáře (např. počet osob aj.)
   - Informace o službě v rozsahu IP adres serverů dané služby
   - Provedení zálohy obsahu e-mailu pro účely pozdějšího vydání věci na základě příslušného rozhodnutí

3) **webové stránky**
   - Provedení zálohy obsahu pro účely pozdějšího vydání věci na základě příslušného rozhodnutí
   - Zjištění majitele a provozovatele stránky, autora, poskytovatele hostingu, držitele doménového jména
   - Datum a čas zřízení stránky
   - Provedení zálohy obsahu stránky veřejně přístupných služeb
   - Informace, jaké všechny služby uživatel využívá aj.

4) **chat**
   - Zjištění registračních a identifikačních údajů vztahujících se k profilu uživatele
   - Provedení zálohy obsahu chatu pro účely pozdějšího vydání věci na základě příslušného rozhodnutí
   - Vyhledávání jiných účtů dle profilu
   - Zjištění obsahu komunikace ve veřejných místnostech
   - Informace, jaké všechny služby uživatel využívá aj.

Pokud se v případě výše uvedených informacích jedná o informace „organizačně technické", které jsou ISP známy z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ.

Pokud však poskytovatel služby tuto informaci nemá a je nucen např. provést analýzu provozu sítě (respektive je možné tyto informace získat pouze na základě analýzy provozních a lokalizačních údajů), pak je na místě o tuto informaci žádat prostřednictvím § 88a TŘ, neboť jde o zjišťování údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo údajů, na něž se vztahuje ochrana osobních a zprostředkovacích dat.

Je třeba uvést, že **ustanovení § 8 odst. 1 TŘ neslouží a nelze využít ke zjištění provozních a lokalizačních či obsahových údajů** (respektive k výpisu LogFile[787]). Ke zjišťování těchto informací slouží jiné, dále popsané instituty trestního práva procesního. Ve vztahu k poskytnutí „logů/výpisů" na základě § 8 odst. 1 TŘ zkonstatoval Ústavní soud ČR protiústavnost takto získaných důkazů,[788] neboť se jedná o obcházení ustanovení § 88 či 88a TŘ.

Nicméně pokud orgán činný v trestním řízení využije § 8 odst. 1 TŘ k žádosti, která spočívá ve „zmrazení (freezing)"[789] požadovaných dat u osoby, jež těmito daty disponuje, pak se nejedná o postup, který by byl v rozporu s právem. Smyslem takovéto žádosti je zachovat digitální stopu a zabránit jejímu případnému poškození či zničení. Vlastní zálohu dat, provozních a lokalizačních údajů či jiných informací provádí dožadovaný subjekt svými prostředky, přičemž data či jiné informace jsou stále v jeho dispozici a k předání orgánům činným v trestním řízení dochází až na základě využití jiných zákonných zmocnění.

Pro orgány činné v trestním řízení je jedním z nejdůležitějších úkonů, nejen v rámci postupu před zahájením trestního stíhání, určení uživatele (osoby, nikoli jen počítačového systému), který se protiprávního jednání v kyberprostoru dopustil. Je třeba, aby došlo k respektování základní zásady trestního řízení, konkrétně zásady stíhání jen ze zákonných důvodů a způsobem, který stanoví trestní řád.[790] *„Podmínkou trestního stíhání je, že prověřováním podle § 158 zjištěné a odůvodněné skutečnosti nasvědčují tomu, že byl spáchán trestný čin, a* ***je-li dostatečně odůvodněn závěr, že jej spáchala určitá osoba,*** *jestliže jsou splněny i další zákonné podmínky.* "[791]

V rámci činnosti orgánů činných v trestním řízení, již ve fázi postupu před zahájením trestního stíhání, musí dojít ne jen k identifikaci počítačového systému, z něhož byl veden útok, ale zejména osoby, která tento útok realizovala. K tomuto zjištění napomáhají některé zajišťovací úkony uvedené v kap. 6.4 Specifika zajišťovacích úkonů.

Pokud by v průběhu postupu před zahájením trestního stíhání nedošlo ke zjištění konkrétní osoby, která trestný čin spáchala, přicházel by v úvahu postup dle § 159a odst. 5 (Odložení věci) TŘ. Usnesení o odložení věci má povahu prozatímního rozhodnutí, tj. ačkoli jsou s ním spojeny účinky právní moci, nečiní v případě nabytí právní moci překážku věci rozhodnuté ve smyslu § 11 odst. 1 písm. f) TŘ.[792] Pokud vyjdou najevo nové skutečnosti svědčící o tom, že osoba spáchala trestný čin, bylo by možné v trestním řízení pokračovat.

787: Záznam událostí, ať již operačního systému, jiného software, či komunikace mezi uživateli či komponenty ICT.

788: Blíže viz kap. 6.4.5 Odposlech a záznam telekomunikačního provozu.

789: Blíže viz čl. 16 Úmluvy o kyberkriminalitě.

790: § 2 odst. 1 TŘ

791: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015, s. 89

792: Tamtéž s. 483

## 6.3 Specifika dokazování kyberkriminality

Za **důkazní prostředek** je možné označit **zákonem upravený způsob získání informace** (skutečnosti, která má být zjištěna - srov. § 89 odst. 1 TŘ).[793] *„Důkazním prostředkem je zdroj,*[794] *z něhož orgán činný v trestním řízení důkazy čerpá (výpovědi osob, věci). Je to určitá forma, jejímž prostřednictvím orgán činný v trestním řízení nabývá potřebných poznatků.* "[795] Trestní řád obsahuje **demonstrativní výčet** důkazních prostředků, kterými lze získat důkazy.

*„**Za důkaz může sloužit vše, co může přispět k objasnění věci**, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Každá ze stran může důkaz vyhledat, předložit nebo jeho provedení navrhnout. Skutečnost, že důkaz nevyhledal nebo nevyžádal orgán činný v trestním řízení, není důvodem k odmítnutí takového důkazu.* "[796]

Při odhalování, objasňování a vyšetřování kyberkriminality je možné užít všechny dostupné prostředky dokazování, které trestní řád při respektování základních zásad trestního řízení nabízí. V této kapitole popíši jen některé důkazy a důkazní prostředky, které nejčastěji slouží k odhalování a objasňování kyberkriminality.

### 6.3.1 Věcné a listinné důkazy

#### 6.3.1.1 Věcné důkazy

Dle § 112 odst. 1 TŘ se za **věcné důkazy** považují ty **předměty**, kterými nebo na kterých byl trestný čin spáchán, jakož i **jiné předměty prokazující či vyvracející dokazovanou skutečnost**. Tyto předměty mohou být prostředkem k odhalení a objasnění trestného činu, jeho pachatele a případných stop.

V zákoně uvedená definice je jen demonstrativním výčtem. Mezi věcné důkazy je potřeba počítat i *„všechny věci, které vznikly v důsledku trestného činu, resp. všechny věci, jejichž prostřednictvím lze dokumentovat skutkový, resp. skutečný průběh trestného činu.* "[797]

793: NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009. s. 228

794: Je třeba uvést, že důkazním prostředkem není zdroj, ale způsob získání relevantní informace pro trestní řízení. Důkazní prostředek je proces, nikoli nositel informace.

795: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 330

796: § 89 odst. 2 TŘ

797: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 397

U kyberkriminality budou nejčastěji **věcným důkazem vlastní počítačové systémy a paměťová média** (ve všech svých formách) obsahující určitá data a informace. Domnívám se, že dle výše uvedené charakteristiky **je možné** tato **data a informace považovat za věcný důkaz**, i když nemohou existovat bez paměťového média.[798] Jako příklad „neexistence" paměťového media při zajišťování věcí (dat) důležitých pro trestní řízení je možné uvést případ, kdy jsou data uložena v cloudu.[799] V tomto případě se nemusí na zajišťovaných paměťových mediích či počítačovém systému uživatele nacházet ani kopie dat v cloudu uložených.

### 6.3.1.2 Listinné důkazy

Za **listinný důkaz** dle § 112 odst. 2 TŘ je pak možné považovat ty **listiny, které svým obsahem** potvrzují či vyvracejí dokazovanou skutečnost. Typickým **listinným důkazem** u kyberkriminality jsou **data či informace po jejich vytištění na tiskárně.**

*„Zajímavou formou důkazu může být **elektronický záznam na počítači**. **Do doby, kdy je záznam v elektronické podobě, může být definován obecně jako důkaz věcný. V okamžiku, kdy je záznam vytištěn na tiskárně, mohl by být považován za důkaz listinný.** Podobně tomu může být s přepisem zvukového záznamu. Plně to platí zejména o použitelnosti dokumentace použití operativně pátracích prostředků (§ 158b odst. 3).*

*Ten, kdo má u sebe věc důležitou pro trestní řízení, je povinen ji předložit, popřípadě vydat (§ 78). **Tato povinnost se nevztahuje na listinu, jejíž obsah se týká okolnosti, o které platí zákaz výslechu,** ledaže došlo ke zproštění povinnosti zachovat věc v tajnosti nebo ke zproštění povinnosti mlčenlivosti (§ 78 odst. 2, § 99).* "[800]

798: Míněno je tím paměťové médium, které je možné fyzicky zajistit jako důkaz v rámci provádění jednotlivých důkazních prostředků.

799: **Cloud computing** je termín užívaný pro systém umožňující užívání (sdílené) počítačových technologií (jak hardware, tak i software) více uživateli (prostřednictvím sítě) formou poskytované služby.
*Cloud Computing Begins to Gain Traction on Wall Street* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.wallstreetandtech.com/it-infrastructure/212700913
Cloud computingem se rozumí poskytování služeb, programů (aplikací), prostoru pro ukládání (resp. meziukládání) dat aj. Smyslem Cloud computingu je efektivnější utilizace výpočetního výkonu a aplikací. Další možnou definicí Cloud computingu je, že jde o *„poskytování výpočetních služeb uživatelům prostřednictvím síťové architektury, která umožňuje vzdálený přístup k těmto službám. Tyto služby jsou zpravidla poskytovány třetí stranou."*
*Security authorization. An Approach for Community Cloud Computing Environments* [online]. [cit. 15. 4. 2012]. Dostupné z: www.federalnewsradio.com/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

800: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015, s. 397

Trestní řád vlastní pojem listina nedefinuje, avšak za listinu je třeba považovat jakýkoli předmět, na němž je písemný nebo jiný grafický projev zachycen. Může se jednat o papír, ale i jiné médium schopné zaznamenat psaný či kreslený projev.

#### 6.3.1.3 Digitální důkazy

Subsumpce digitální stopy buď pod ustanovení věcného, či listinného důkazu není zcela vhodná a ne vždy je touto subsumpcí možné postihnout veškerá specifika digitální stopy.[801]

Z výše uvedených důvodů jsem přesvědčen, že by bylo vhodné zavést novou kategorii důkazů: **důkaz digitální**. Vlastní ustanovení definující digitální důkaz by bylo možné zařadit do § 112 odst. 3 TŘ např. v následujícím znění:

***Digitálním důkazem jsou jakákoli data či informace, jež byly přeneseny, vytvořeny, uloženy či modifikovány za použití počítačového systému a které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu.***

### 6.4 Specifika zajišťovacích úkonů

„*Úkony směřující k zajištění osob a věcí pro účely trestního řízení jsou závažnými zásahy do práv a svobod občanů, zaručených Listinou základních práv a svobod (Hl. II odd. 1) a jsou přípustné jen tehdy, jsou-li pro jejich výkon dány zákonné podmínky, čl. 8, 12, 13 Listiny.*“[802]

Obecně je možné rozdělit zajišťovací úkony na **úkony sloužící k zajištění osob** a **úkony sloužící k zajištění věcí (a informací)**. Vzhledem ke specifičnosti kyberkriminality se v této subkapitole zaměřím především na některé z úkonů sloužící k zajištění věcí a informací.

**Za věci důležité pro trestní řízení je nutno považovat:**
1) předměty, které lze považovat za věcné důkazy ve smyslu § 112 odst. 1 TŘ,
2) listiny, které lze považovat za listinné důkazy ve smyslu § 112 odst. 2 TŘ,
3) předměty, na něž by se mohl vztahovat trest propadnutí věci (§ 70 TZK) nebo ochranné opatření zabrání věci (§ 101 TZK).[803]

801: Blíže viz kap. 6.1.1 Digitální stopa.

802: NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009, s. 159

803: Blíže viz tamtéž s. 181

Konrád uvádí, že počátečními úkony při vyšetřování počítačové kriminality jsou zejména:

1) *ohledání místa činu,*
2) *domovní prohlídka a prohlídka jiných prostor,*
3) *zajišťovací úkony pro počítačovou expertizu a vyhledávání počítačových stop a důkazů.*[804]

K těmto úkonům by pak bylo možné dále přiřadit:

4) vydání a odnětí věci,
5) odposlech a záznam telekomunikačního provozu,
6) operativně pátrací prostředky.

### 6.4.1 Vydání a odnětí věci

Vydání a odnětí věci důležité pro trestní řízení je vymezeno ustanoveními § 78 a 79 TŘ. Věcí se dle § 489 OZ rozumí **vše, co je rozdílné od osoby** (fyzické či právnické) **a co slouží potřebě lidí**.[805]

Vydání věci je upraveno v § 78 TŘ, kde je zakotvena **povinnost** každého **předložit věc** důležitou pro trestní řízení na výzvu orgánů činných v trestním řízení, **případně** tuto **věc vydat** (tzv. ediční povinnost). **Oprávnění vyzvat k vydání věci** mají předseda senátu a v přípravném řízení státní zástupce a policejní orgán. Policejní orgán nepotřebuje k vydání výzvy předchozí souhlas státního zástupce (jestliže nelze předchozího souhlasu dosáhnout a věc nesnese odkladu).[806] Výzva k vydání věci má formu **opatření**. Není tedy žádným způsobem formalizována (**forma** není stanovena, výzva k vydání věci může být dána ústně nebo písemně).

Držitel věci musí být poučen o následcích neuposlechnutí výzvy. Pokud osoba výzvy neuposlechne, může jí být věc odňata, případně jí může být uložena pořádková pokuta (viz § 66 TŘ). Povinnost vydat věc se nevztahuje na věci (zejména listiny, analogicky pak i na data), jejichž obsah se týká okolností, o kterých platí zákaz výslechu,[807] ledaže došlo k zproštění povinnosti zachovat věc v tajnosti nebo ke zproštění mlčenlivosti (§ 99 TŘ).

V rámci kyberkriminality se v praxi bude nejčastěji jednat o zajišťování počítačových systémů (počítače, servery, mobilní telefony, tablety, datová úložiště, switche, routery aj.) včetně některých periférií (externí rozmnožovací zařízení, 3D tiskárny aj.), interních či externích paměťových médií [harddisky (interní či externí), flash paměti, USB disky aj.], dalších prostředků sloužících ke komunikaci (zejména SIM karty aj.), jednotlivých účtů uživatele (v některých případech

804: KONRÁD, Zdeněk, Viktor PORADA a Jiří STRAUS. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování.* Plzeň: 2015, s. 351–352.

805: Blíže viz kap. 2.4.2 Věci a virtuální majetek.

806: Viz § 72 odst. 2, 3 TŘ

807: Blíže viz kap. 6.4.4 Prohlídka jiných prostor a pozemků. Konkrétně: Nález Ústavního soudu IV. ÚS 2/02, ze dne 28. 3. 2002 (U 11/25 SbNU 385).

k zajištění virtuálních účtů může být vhodnější využít § 79e TŘ sloužící k zajištění práv k věci), dalších listin nesoucích informace důležité pro trestní řízení (kontakty, seznamy aj.) spotřebního datového a kancelářského materiálu apod. V případě zjištění, že pachatel svou trestnou činností získal prostředky, které následně dále užil (např. zakoupení elektroniky či jiné věci) je možné osobu vyzvat, aby uvedené předměty vydala. Pokud tak neučiní, je možné jí je odejmout.

**Pokud nebyla věc** dobrovolně **vydána** osobou, která ji má u sebe, **může být** na příkaz předsedy senátu a **v přípravném řízení na příkaz státního zástupce či policejního orgánu odňata.**[808] Příkaz k odnětí věci je rozhodnutím *sui generis* a není proti němu přípustný opravný prostředek. K odnětí věci by měla být přibrána nezúčastněná osoba (tzv. *extraneus* - svědek úkonu). Přítomnost nezúčastněné osoby není obligatorní, ale je žádoucí. Od přítomnosti nezúčastněné osoby lze upustit jen ve výjimečných případech, kdy není možné její účast hned zajistit a pro naléhavost věci nelze úkon odložit.[809]

O vydání věci je sepsán protokol (§ 55 TŘ), u kterého je nutné detailně popsat věc, kterou osoba vydává, aby nemohla být zaměněna za jinou. Také je to třeba z důvodu případného následného vydání či vrácení věci, neboť popis věci se musí přesně shodovat s popisem věci, jak bude uváděn v usnesení o vrácení věci.[810] V případě počítačových systémů se jedná zejména o číselné označení výrobce na vnějším obalu počítačového systému, název výrobce, další případné markanty (např. poškození, polepky, barva aj.). Je vhodné počítačový systém označit unikátním číslem a fotograficky zadokumentovat.

Osobě, která věc vydala nebo jíž byla věc odňata, vydá orgán provádějící tento úkon písemné potvrzení o převzetí věci nebo opis protokolu, a to i v případě, že jej osoba nevyžaduje.

Vzhledem ke specifické povaze kyberkriminality uvedu některé další případy, na něž lze uplatnit instituty vydání a odnětí věci:

- **data** (k zajištění obsahu údajů nacházejících se na datovém nosiči lze využít ustanovení § 78, 79, 82 a násl., § 113 TŘ),[811] **přičemž nezáleží na lokaci dat** (fyzicky přítomný počítačový systém, či online dostupný systém),
- **e-mailová zpráva.** Takovouto zprávu **je za splnění dalších podmínek trestního řádu třeba považovat za věc důležitou pro trestní řízení**, kterou lze vyžádat podle § 78 TŘ nebo odejmout podle

808: Policejní orgán potřebuje k odnětí věci předchozí souhlas státního zástupce, vyjma případu, kdy nebylo možné předchozího souhlasu dosáhnout a věc nesnese odkladu.

809: Blíže NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009, s. 186

810: Srov. ust. § 80 a § 81 TŘ.

811: V některých případech (zajištění obsahu e-mailové elektronické komunikace na zajištěném datovém nosiči – tj. již uložených dat) je možné využít ustanovení § 158d 1, 3 TŘ. Pokud se na data, respektive proces jejich přenosu vztahuje ustanovení speciální (např. § 88 a § 88a TŘ), je třeba užít tohoto ustanovení speciálního.

Blíže viz stanovisko **Nejvyššího státního zastupitelství 1 SL 760/2014.** *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, ze dne 26. 1. 2015.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

§ 79 TŘ. V současné době je možné takovýto postup považovat za správný, na rozdíl od názoru, podle něhož se na takovou zprávu vztahují § 86–87c TŘ o zadržení a otevření zásilek, jejich záměně a sledování, protože tato ustanovení se vztahují na zásilky **v průběhu jejich přepravy.**[812]

- **zjištění obsahu e-mailové komunikace v zajištěném datovém nosiči (počítačovém systému) uskutečněné do doby jeho zajištění orgány činnými v trestním řízení**[813]
- **provedení zálohy obsahu** (např. webové stránky, cloudového úložiště či jiného prostoru typicky svázaného s účtem uživatele) **pro účely pozdějšího vydání věci na základě**

812: Srov. FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6 vyd. Praha: Wolters Kluwer, 2015, s. 316

Dále viz: Rozhodnutí Nejvyššího soudu **11 Tdo 349/2009**, ze dne 21. 5. 2009. [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/FBA92F6969DDC460C1257A4E00656CA9?openDocument&Highlight=0

**Výňatek z uvedeného usnasení:**

Při jazykovém výkladu zmíněného ustanovení je třeba nejprve vyjít z jeho dikce, kde zákonodárce užil přídavného jména „podávané", jež je odvozeno od slovesa „podávat", tedy nedokonavého vidu, nikoli slovesa „podat" v dokonavém vidu. Nejedná se tedy o zprávu „podanou" jiným takovým veřejným zařízením, ale o zprávu „podávanou" a tento průběhový tvar je třeba vztahovat k okamžiku, kdy pachatel poruší tajemství zprávy. Tomuto výkladu navíc odpovídá i název ustanovení § 239 TZK, kde je užito gramaticky obdobné přídavné jméno „dopravovaných".

Ochrana se tedy poskytuje dopravované zprávě v době jejího „**podávání**", tedy v průběhu doručování, podobně jako je zpráva obsažená v listovní zásilce doručované poštou chráněna po dobu její přepravy. Jedná se o proces, jehož počátek je možno ohraničit odesláním zprávy z počítače odesílatele (nebo z jiného počítače, s nímž právě odesílatel pracuje). Konec uvedeného procesu je pak nutno vnímat v okamžiku doručení zprávy do e-mailové schránky příjemce. Tímto okamžikem je totiž proces dopravy zprávy ukončen a v e-mailové schránce zpráva také zůstává, pokud ji adresát neodstraní (nevymaže). Příjemce zprávy má do e-mailové schránky takový přístup, který je zabezpečen pomocí hesla, může si přitom zjednat přístup do této schránky zpravidla z kteréhokoli počítače připojeného k Internetu, takže zpráva nacházející se v e-mailové schránce je již zcela v jeho dispozici.

Nejvyšší soud nadto upozorňuje, že i úprava obsažená v novém trestní zákoníku užívá obdobné formulace v ustanovení § 182 odst. 1 písm. b): „Kdo úmyslně poruší tajemství ... datové, textové, hlasové, zvukové či obrazové zprávy **posílané** prostřednictvím sítě elektronických komunikací ...". Pokud by zákonodárce zamýšlel rozšířit v tomto směru trestněprávní ochranu tak, jak vyplývá z právního názoru zaujatého soudy nižších soudů v této projednávané věci, měl možnost formulovat toto ustanovení přesněji a výslovně v něm uvést, že zpráva se má za doručenou až po jejím přečtení, vyslechnutí či jiném poznání jejího obsahu příjemcem, nebo jinak výslovně stanovit konec ochrany tajemství takové zprávy.

Z technické povahy elektronické pošty, která v praxi výrazně omezuje možnosti potenciálních pachatelů porušit tajemství e-mailové zprávy v průběhu jejího podávání, nelze tudíž dovozovat, že by ochrana takové dopravované zprávy měla být doplněna rozšiřujícím výkladem. Ustanovení § 239 TZK vyjadřuje ochranu ústavně zaručených práv – práva na soukromí a listovního tajemství. Ustanovení čl. 13 Listiny vymezuje zajisté širší oblast soukromého života, než jak ji chrání trestní zákon. Ovšem ochrana práv zakotvených v posledně citovaném ustanovení je současně zaručena také prostředky jiných právních odvětví než trestního práva, např. prostřednictvím institutu ochrany osobnosti v občanském zákoníku. V souladu se zásadou minimalizace trestní represe proto Nejvyšší soud zastává názor, že ustanovení § 239 odst. 1 písm. b) TZK je třeba vykládat uvedeným způsobem.

813: Blíže viz stanovisko **Nejvyššího státního zastupitelství 1 SL 760/2014.** *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, ze dne 26. 1. 2015.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

**příslušného rozhodnutí** (dále je možné pro zisk těchto informací využít i ustanovení § 8 odst. 1, § 82 a násl., § 113 TŘ),
- **vydání obsahů veřejně nepřístupných služeb,**
- **zjištění obsahu komunikace ve veřejných či neveřejných chatovacích místnostech** (dále je možné pro zisk těchto informací využít i ustanovení § 82 a násl., § 113 TŘ. Obsah dat není možné žádat na podkladě ustanovení § 88a TŘ. Obsah probíhající komunikace je možné zajistit pomocí ustanovení § 88 TŘ.).

### 6.4.2 Zajištění nehmotné věci a zajištění peněžních prostředků na účtu u banky

Trestní řád obsahuje i speciální ustanovení, která umožňují zajištění nehmotné věci, náhradní hodnoty, peněžních prostředků na účtu u banky a zaknihovaných cenných papírů.[814]

Ve většině případů pachatelé zisky z tohoto druhu trestné činnosti použijí k okamžité spotřebě, k nákupu spotřebního materiálu pro svoji další činnost, k nákupu počítačových systémů aj. V těchto případech je možné užít institutu zajištění věci (viz kap. 6.4.1 Vydání a odnětí věci).

Pokud pachatel užil prostředky získané kyberkriminalitou např. na projekty, podíly v obchodních společnostech, nákupy služeb (např. webhosting, serverhosting, předplacené služby aj.), bylo by možné užít institutu **zajištění nehmotné věci**, neboť takovýto materiál je výnosem z trestné činnosti. Institutu zajištění nehmotné věci lze dále využít i v případech, kdy je nehmotná věc určena ke spáchání trestného činu nebo k jeho spáchání byla užita (v případě webových stránek půjde např. o stránky, na nichž je umístěn protiprávní materiál - např. fotografie a videa zobrazující zneužívání dětí, propagující rasismus aj.).

U zajištění nehmotné věci je zajišťován výkon práva disponovat s určitou věcí. *„Smysl spočívá především v tom, že obviněnému či jiné osobě je zamezeno s majetkem nakládat – čímž může např. docházet k pokračování v trestné činnosti a vzniku škod – a předejít tak jeho zničení, poškození, ale především zcizení nebo zmenšení. Jednodušeji řečeno obviněný či jiná osoba zůstává vlastníkem majetku, ale je omezen v nakládání s ním.*“[815]

Je-li to zapotřebí pro účely zajištění, lze v usnesení o zajištění nehmotné věci nebo i v dodatečném usnesení zakázat nebo omezit také výkon dalších práv souvisejících se zajištěnou nehmotnou věcí, a to včetně práv teprve v budoucnu vzniklých.[816]

O zajištění nehmotné věci **rozhoduje předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán.** Policejní orgán potřebuje k takovému rozhodnutí předchozí souhlas

814: Srov. ustanovení § 79e, 79f a § 79a až 79c TŘ

815: *Policie vám může vypnout doménu. Co říká zákon?* [online]. [cit. 24. 8. 2016]. Dostupné z: https://www.root.cz/clanky/policie-vam-muze-vypnout-domenu-co-rika-zakon/

816: Viz § 79e odst. 2 TŘ

státního zástupce, vyjma naléhavých případů, kdy věc nesnese odkladu. Uvedené rozhodnutí má formu *usnesení* a je proti němu přípustná stížnost.

Běžně se lze v praxi také setkat se situací, kdy pachatel výnosy z kyberkriminality vkládá či přesouvá na účet banky. Pokud zjištěné skutečnosti nasvědčují tomu, že prostředky na účtu banky jsou výnosem z trestné činnosti nebo jsou určeny ke spáchání trestného činu nebo k jeho spáchání byly užity, může **předseda senátu a v přípravném řízení státní zástupce nebo policejní orgán** rozhodnout o zajištění peněžních prostředků na účtu (případně prostředků na účet dodatečně došlých). Policejní orgán potřebuje k takovému rozhodnutí předchozí souhlas státního zástupce, vyjma naléhavých případů, kdy věc nesnese odkladu. Uvedené rozhodnutí má formu *usnesení* a je proti němu přípustná stížnost.

Mnohdy bývá problém určit, na jaký konkrétní účet pachatel výnosy z trestné činnosti ukládá, neboť pachatelé mají pro své potřeby založeno více bankovních účtů a pro zahlazení stop mezi nimi provádějí převody různých finančních částek, kdy jsou nelegální výnosy směšovány s běžnými příjmy pachatele.

V případě, že lze předpokládat, že alespoň část finančních prostředků na účtu u banky je určena ke spáchání trestného činu nebo k jeho spáchání byla užita nebo je výnosem z trestné činnosti, lze zajistit alespoň část takových prostředků, případně veškeré prostředky na účtu u banky do vyřešení otázky, které z těchto prostředků byly získány nelegálním způsobem.

Problém v současnosti představují **virtuální měny** (typicky Bitcoin, Litecoin aj.) či jiné virtuální kredity (např. kredit v online kasinu aj.). Tyto prostředky nejsou mnohdy uznávány jakožto peněžní prostředky (peníze), byť tuto funkci zcela jistě plní. Nicméně s odkazem na § 79e TŘ je i takovéto prostředky možné zajistit. Pokud akceptuji tvrzení, že se nejedná o peněžní prostředky (a zejména fakt, že tyto virtuální měny nejsou drženy na účtu banky), tak je třeba uznat, že jde o věc (v tomto případě nehmotnou), vůči které mohu omezit právo k disponování s ní (viz právě § 79e TŘ).

### 6.4.3 Domovní prohlídka

Domovní prohlídka je jedním ze zajišťovacích úkonů umožňujících velmi intenzivní zásah do základních lidských práv a svobod.[817] Vlastní prohlídku je možné vykonat, existuje-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení (trvalé či přechodné bydliště, ubytovny, vysokoškolské koleje, pronajaté místnosti určené k bydlení) nebo v prostorách k nim náležejících (např. garáž v domě, sklepní kóje, půda domu, kolna aj.) se nachází věc nebo osoba důležitá pro trestní řízení.

817: Konkrétně čl. 12 Listiny:

***1) Obydlí je nedotknutelné**. Není dovoleno do něj vstoupit bez souhlasu toho, kdo v něm bydlí.*

***2) Domovní prohlídka je přípustná jen pro účely trestního řízení, a to na písemný odůvodněný příkaz soudce**. Způsob provedení domovní prohlídky stanoví zákon.*

*3) Jiné zásahy do nedotknutelnosti obydlí mohou být zákonem dovoleny, jen je-li to v demokratické společnosti nezbytné pro ochranu života nebo zdraví osob, pro ochranu práv a svobod druhých anebo pro odvrácení závažného ohrožení veřejné bezpečnosti a pořádku. Pokud je obydlí užíváno také pro podnikání nebo provozování jiné hospodářské činnosti, mohou být takové zásahy zákonem dovoleny, též je-li to nezbytné pro plnění úkolů veřejné správy.*

**Domovní prohlídku je oprávněn nařídit předseda senátu a v přípravném řízení na návrh státního zástupce soudce.** Domovní prohlídku vykonává na příkaz předsedy senátu či soudce policejní orgán. Příkaz k domovní prohlídce je rozhodnutím *sui generis*. Příkaz musí být písemný a odůvodněný.

Provádění domovní prohlídky, osobní prohlídky a prohlídky jiných prostor se řídí ustanovením § 82 TŘ. Příkaz k domovní prohlídce jsou povinny orgány činné v trestním řízení doručit osobě, u níž se prohlídka koná, při prohlídce, a není-li to možné, nejpozději do 24 hodin po odpadnutí překážky, která brání doručení.[818]

Vlastní domovní prohlídce a prohlídce jiných prostor a pozemků má předcházet výslech osoby, u které se má takový úkon vykonat. Předchozího výslechu není třeba, jestliže věc nesnese odkladu a výslech nelze provést okamžitě.[819] **Účelem předchozího výslechu je** zjistit, zda se v obydlí, jiném prostoru nebo na pozemku nachází věc nebo osoba důležitá pro trestní řízení a **dosáhnout dobrovolného vydání hledané věci nebo odstranění jiného důvodu prohlídky.**

Orgán, který vykonává domovní prohlídku nebo prohlídku jiných prostor je povinen umožnit osobě, u níž se takový úkon koná, nebo některému dospělému členu její domácnosti nebo v případě prohlídky jiných prostor též jejímu zaměstnanci účast při prohlídce. O právu účasti při prohlídce je povinen tyto osoby poučit. K vlastnímu výkonu domovní prohlídky je třeba přibrat osobu nezúčastněnou.[820] Osoba, u níž má být provedena domovní prohlídka, prohlídka jiných prostor a pozemku, osobní prohlídka nebo vstup do obydlí, je povinna tyto úkony strpět. Neumožní-li osoba provedení takového úkonu, jsou orgány provádějící úkon oprávněny po předchozí marné výzvě překonat odpor takové osoby nebo jí vytvořenou překážku.[821]

Domovní prohlídku je možné provést i jako neodkladný úkon (viz § 160 odst. 4 TŘ). Avšak v takovém případě je třeba respektovat i Nález Ústavního soudu III. ÚS 287/96, který k provedení domovní prohlídky jako neodkladného úkonu dále uvádí: *„I když lze v zásadě připustit, že za jistých okolností (skutečností dostatečně zřejmých)* ***může mít domovní prohlídka v konkrétní věci charakter neodkladného úkonu*** *(§ 160 odst. 4 TŘ)* ***a že jako taková je ex lege přípustná*** *(§ 83 odst. 1 al. 2 TŘ), jde v takovém případě o zvlášť závažný zásah do ústavně zaručeného základního práva na domovní svobodu,* ***a proto také rozhodnutí, na jehož základě má být takový úkon proveden, musí být i z tohoto hlediska zvláštní závažnosti přiměřeně a dostatečně zdůvodněno.***"[822]

Dle rozhodnutí Nejvyššího soudu, který se zabýval případem počítačové kriminality, ve vztahu k neodkladnosti domovní prohlídky konstatoval, že se jednalo o neodkladný úkon vzhledem ke specifičnosti dané trestné činnosti (zejména možnosti zmaření účelu trestního řízení). V tomto

818: § 83 odst. 2 TŘ

819: § 84 TŘ

820: § 85 TŘ

821: § 85a TŘ

822: Nález Ústavního soudu III. ÚS 287/96 ze dne 22. 5. 1997 k ústavnosti domovní prohlídky. [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=28795&pos=1&cnt=1&typ=result

případě ani chybějící odůvodnění neodkladného nebo neopakovatelného úkonu a časový odstup mezi vydáním příkazu k domovní prohlídce a její vlastní realizací neměl vliv na jeho zákonnost.[823]

823: Blíže viz Rozhodnutí Nejvyššího soudu 5do 1312/2010, ze dne 15. 12. 2010. [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/DE1E219419DEA02EC1257A4E006525B9?openDocument&Highlight=0

**Z uvedeného rozhodnutí vztahujícího se ke kyberkriminalitě cituji:**

Ze spisového materiálu byly Nejvyšším soudem zjištěny následující skutečnosti. **V odůvodnění příkazu k domovní prohlídce** ze dne 4. 7. 2006, sp. zn. 0 Nt 1725/2006, **soudkyně uvedla, že vzhledem k doposud zjištěným skutečnostem lze důvodně předpokládat, že se ve specifikované nemovitosti mohou nacházet věci důležité pro trestní řízení a jeví se tudíž jako neodkladný a neopakovatelný úkon provedení domovní prohlídky** (č. l. 61 spisu). K. H., jako spoluvlastník nemovitosti, v níž byla provedena domovní prohlídka, byla vyslechnuta dne 27. 7. 2006 v 10.30 hodin (č. l. 62 spisu). Protokol o provedení domovní prohlídky dne 27. 7. 2006 je založen na č. l. 63 a násl. spisu. Prohlídce byla přítomna nezúčastněná osoba a matka obviněného K. H. Obviněný O. H. byl vyslechnut dne 3. 8. 2006, kdy využil svého práva a odmítl k věci vypovídat. Státní zástupce Okresního státní zastupitelství dne 2. 10. 2006 reagoval na námitky obhájkyně obviněného sdělením, že vzhledem k tomu, že K. H. lze považovat za osobu, u níž se prohlídka koná ve smyslu ustanovení § 83 odst. 1, § 84 a § 85 odst. 1, 4 TŘ, byl výkon domovní prohlídky proveden v souladu s trestním řádem i přes nepřítomnost obviněného. **Neodkladnost a neopakovatelnost úkonu sice nebyly v příkazu soudu dostatečně podrobně odůvodněny, nicméně vyplývají z podstaty věci týkající se tzv. počítačové kriminality, kde je třeba vždy takový úkon z hlediska časových souvislostí jeho provedení vždy pečlivě naplánovat. Proto zmíněný formální nedostatek odůvodnění neodkladnosti a neopakovatelnosti tohoto úkonu sám o sobě nemůže znamenat nezákonnost domovní prohlídky a nepoužitelnost důkazů při ní opatřených.** Zásah do softwarového či hardwarového vybavení počítače nebo úprava na něm uložených dat před tím, než by byl odborně zjištěn a zadokumentován jeho reálný stav, by znamenal zmaření objasňování skutečností závažných pro trestní stíhání. Toto závažné riziko dostatečně odůvodňuje kvalifikaci napadeného úkonu jako neodkladného a neopakovatelného (srov. i vyjádření státního zástupce Okresního státního zastupitelství v Olomouci na č. l. 145).

Nejvyšší soud dodává, že pojem neodkladného úkonu je vztahován k okamžiku zahájení trestního stíhání, zatímco pojem neopakovatelného úkonu až k řízení před soudem. Neodkladnými jsou takové úkony, které vzhledem k nebezpečí jejich zmaření, zničení nebo ztráty by nesnesly z hlediska účelu trestního řízení odkladu do doby, než bude zahájeno trestní stíhání. Mezi takovéto úkony mj. patří domovní prohlídka a prohlídka jiných prostor a pozemků podle ustanovení § 82 odst. 1, 2 TŘ, § 83 a § 83a TŘ. S ohledem na uvedené nelze přisvědčit obviněnému ani v té části námitek, kde uvádí, že ačkoliv byl příkaz k domovní prohlídce vydán jako neodkladný a neopakovatelný úkon, proveden byl více než tři týdny od vydání soudního příkazu. **K namítanému časovému odstupu od vydání příkazu k domovní prohlídce ve vztahu k jejímu vlastnímu provedení, považuje za nutné Nejvyšší soud zdůraznit, že je to otázka taktiky vedení přípravného řízení, jež je plně v kompetenci orgánů činných v přípravném řízení, a proto pouze tato skutečnost nemůže zpochybnit závěr o neodkladnosti a neopakovatelnosti předmětného úkonu.** S ohledem na závěry týkající se souboru kontakty.php , které byly uvedeny shora, je možno mít za to, že zde byly dostatečné podklady pro provedení domovní prohlídky u obviněného, resp. jeho rodičů, neboť právě s ohledem na to, bylo možné relevantně doložit a zdůvodnit podezření o spojení obviněného O. H. s předmětnou trestnou činností, která tudíž zakládala důvodné podezření ve smyslu ustanovení § 83 odst. 1 TŘ, že se v daném obydlí nachází věc důležitá pro trestní řízení. Z těchto důvodů bylo třeba odmítnout i tuto námitku obviněného týkající se nezákonnosti a protiústavnosti provedené domovní prohlídky, neboť orgány činné v trestním řízení se s ní řádně vypořádaly již v průběhu přípravného řízení a ani Nejvyšší soud z jejich strany žádné pochybení nezjistil.

O provedení domovní prohlídky je orgán činný v trestním řízení povinen sepsat (zpravidla při úkonu nebo bezprostředně po něm) protokol (viz § 55 odst. 1 TŘ), kde je třeba mimo jiné uvést, zda byl uskutečněn předchozí výslech, popřípadě označit důvody, proč nebyl. Pokud došlo při prohlídce k vydání nebo odnětí věci, je třeba, aby protokol obsahoval takový popis věci, aby nemohla být zaměněna s jinou. Ze seznamu vydaných nebo odňatých věcí musí být zřejmé, které věci byly dobrovolně vydány po předchozím výslechu a které byly nalezeny a odňaty při prohlídce.[824]

Specifikum domovní prohlídky či prohlídky jiných prostor a pozemků v případě kyberkriminality spočívá především v charakteru zajišťovaných věcí. Zejména je třeba se zaměřit na:

- **zajištění počítačových systémů a dalších věcí** (předměty, zařízení aj.), které mohou souviset s kybernetickou kriminalitou. Jedná se například o:
  - počítače,
  - servery,
  - datová úložiště,
  - mobilní telefony a tablety,
  - herní konzole (např. Xbox aj.),[825]
  - televizní systémy,[826]
  - tiskárny,[827]
  - paměťová média (nosiče informací),[828]

- **připojení jednotlivých počítačových systémů k síti Internet**
  - zjištění způsobů připojení u jednotlivých systémů,
  - identifikace jednotlivých ISP poskytujících připojení či služby,
  - připojení ke vzdáleným datovým úložištím aj.

- **připojení počítačových systémů do lokální sítě**
  - určení (zaznamenání) topologie sítě,[829]

824: Srov. NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009, s. 201

825: Byly zaznamenány případy, kdy byla modifikována herní konzole Xbox, tak aby fungovala jako „standardní" počítač. V tomto počítači pak byla nalezena dětská pornografie. Blíže viz např.:
*Sex Predator Uses Xbox Live to Victimize 10-Year-Old.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.escapistmagazine.com/news/view/103121-Sex-Predator-Uses-Xbox-Live-to-Victimize-10-Year-Old
HOLT, Thomas, Adam BOSSLER a Kathryn SEIGFRIED-SPELLAR. *Cybercrime and digital forensics:an introduction.* First published. London: Routledge, 2015, s. 331.

826: Některé televize či televizní systémy jsou schopny plnit funkci „standardního" počítače (např. TV s OS Android, Apple TV aj.).

827: Zejména síťové tiskárny mohou díky svým funkcím plnit některé úlohy počítačového systému (např. odesílat e-maily aj.).

828: Tato paměťová média (např. externí harddisky, flash disky, paměťové karty, CD, DVD aj.) mohou být útočníkem úmyslně skryta či maskována (např. jako kniha, zapalovač, baterka, hračka, přívěšek aj.), mohou být připojena do počítačového systému (např. televize, herní konzole aj.) či jeho periferie (např. tiskárny, monitoru aj.).

829: Vlastní privátní (PAN) síť může využívat různé techniky propojení jednotlivých počítačových systémů k této síti, přičemž fyzicky mohou být vzájemně propojené systémy umístěny i v různých místnostech, budovách, či částech obce.

- propojení počítačových mezi sebou (přímé propojení bez zapojení do sítě),
- umístění jednotlivých počítačových systémů v síti,
- určení oprávnění pro přístup jednotlivých osob k jednotlivým částem sítě, či do počítačových systémů,

- **zjištění dalších relevantních informací.**

Neodborné zajištění především počítačových systémů, nosičů informací (paměťových médií) či dat samotných může vést k poškození či zničení digitálních stop. Z důvodu zajišťování specifických stop, (zejména v případě zajišťování dat bez vlastního zajištění počítačového systému – například vytváření identické kopie paměťového média aj.), je ve většině případů nezbytná účast znalce z oboru informačních technologií nebo zvlášť vyškoleného kriminalistického technika či policisty specialisty při vlastní prohlídce, případně je třeba s takovouto osobou konzultovat vlastní postup prohlídky.

Po zajištění věci (typicky počítačového systému či nosiče informací) je nutné přijmout takové opatření, aby přístup k datům mohl mít v budoucnu jako první znalec. K tomu jsou užívány metody zaslepení vstupně-výstupních zařízení včetně elektrického konektoru papírovými pásy, které po přilepení označí svým podpisem policejní orgán i osoba na úkonu nezúčastněná.

Další zvláštností kyberkriminality je **možnost vzájemného provázání jednotlivých kybernetických útoků** [viz kap 4.16 APT (Advanced Persistent Threat), 4.6 Phishing, Pharming, Spear Phishing, Vishing, Smishing, 4.5 Spam, 4.3 Malware aj.]. V případě provádění domovní prohlídky na základě skutečností nasvědčujících spáchání některého druhu kyberkriminality **je vhodné specifikovat příkaz k domovní prohlídce** (případně prohlídce jiných prostor a pozemků) **tak, aby bylo možné zajistit veškeré** věci (např. počítačové systémy, předměty, zařízení, data aj.), **které mohou s kybernetickou trestnou činností souviset** (tj. věc je určena ke spáchání trestného činu nebo k jeho spáchání byla užita nebo je výnosem z trestné činnosti). V případě, že by příkaz k prohlídce byl konkretizován pouze na prověřovanou věc, tedy na konkrétní kybernetický trestný čin (např. na zajištění věcí souvisejících s porušováním práv autorských), pak by při nálezu dalších materiálů (např. dětské pornografie) bylo třeba tento příkaz rozšířit.[830]

830: Problém v tomto případě může nastat, pokud je věc (např. počítačový systém či nosič informací) již předána znalci ke znaleckému zkoumání a tento až svojí činností zjistí přítomnost v příkladu uvedené dětské pornografie.
V takovémto případě je zřejmě nejvhodnějším postupem přijetí podnětu od znalce (viz § 59 TŘ) a zahájení úkonů trestního řízení dle § 158 odst. 3 TŘ ve vztahu k nově zjištěné trestné činnosti (dětské pornografii). Znalec, který tuto trestnou činnost objevil, by pak ve věci dětské pornografie nemohl vystupovat jako znalec.

### 6.4.4 Prohlídka jiných prostor a pozemků

Prohlídku jiných prostor a pozemků lze vykonat, pokud jsou splněny stejné zákonné důvody, jako tomu je v případě domovní prohlídky, je-li důvodné podezření, že v prostorech nesloužících k bydlení (jiných prostorech) a pozemků, které však nejsou veřejně přístupné, se nachází věc nebo osoba důležitá pro trestní řízení.

**Prohlídku jiných prostor a pozemků je oprávněn nařídit předseda senátu a v přípravném řízení na návrh státního zástupce soudce. Bez příkazu může policejní orgán provést prohlídku** jiných prostor nebo pozemků, **jestliže vydání příkazu nelze předem dosáhnout a věc nesnese odkladu.** Policejní orgán je však povinen si bezodkladně dodatečně vyžádat souhlas orgánu oprávněného k vydání příkazu; v přípravném řízení tak činí prostřednictvím státního zástupce. **Pokud oprávněný orgán souhlas dodatečně neudělí, nelze výsledek prohlídky použít v dalším řízení jako důkaz. Bez příkazu může policejní orgán provést prohlídku** jiných prostor nebo pozemků **také tehdy, pokud uživatel dotčených prostor nebo pozemků písemně prohlásí, že s prohlídkou souhlasí, a své prohlášení předá policejnímu orgánu.** O tomto úkonu však musí policejní orgán bezodkladně vyrozumět předsedu senátu oprávněného k vydání příkazu a v přípravném řízení státního zástupce.[831]

Prohlídku jiných prostor a pozemků vykonává na příkaz předsedy senátu či soudce policejní orgán. Příkaz k prohlídce jiných prostor a pozemků je rozhodnutím *sui generis*. Příkaz musí být písemný a odůvodněný.

Provádění prohlídky jiných prostor se řídí ustanovením § 82 TŘ. K vlastnímu výkonu prohlídky viz kap. 6.4.3 Domovní prohlídka.

V případě domovní prohlídky, prohlídky jiných prostor či pozemků, případně při uplatnění institutů vydání či odnětí věci může v případě zajišťování počítačových systémů či dat dojít k situaci, kdy se na určité informace obsažené v počítačovém systému či na určitá data může vztahovat povinnost vyplývající ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Touto problematikou se zabýval Ústavní soud a v dané situaci je třeba vycházet z Usnesení Ústavního soudu U 11/25 SbNU 385 (IV. ÚS 2/02 ze dne 28. 3. 2002),[832] kde je mimo jiné uvedeno:

„***Při výkonu prohlídky** jiných prostor, **pro jejíž nařízení byly splněny zákonné podmínky, lze jako věci důležité pro trestní řízení zajistit i výpočetní techniku a záznamová media, případně jejich***

831: § 83a odst. 2 a 3 TŘ

832: Nález Ústavního soudu IV. ÚS 2/02, ze dne 28. 3. 2002 (U 11/25 SbNU 385). *Nařízení a provedení prohlídky jiných prostor. Povinnost mlčenlivosti.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=43001&pos=1&cnt=1&typ=result

***kopie, i když existuje možnost, že zajištěné nosiče*** *informací* ***obsahují*** *vedle záznamů o skutečnostech důležitých pro trestní řízení* ***i informace o skutečnostech, které se netýkají probíhajícího trestního řízení a ke kterým se váže státem uložená nebo uznaná povinnost mlčenlivosti.***

*Je-li dáno důvodné podezření, jako tomu bylo v daném případě, že nosiče informací obsahují údaje a informace důležité pro trestní řízení, jsou-li tedy splněny podmínky pro zajištění těchto nosičů, nemůže tvrzení osoby, u níž se prohlídka provádí, či tvrzení jiné osoby při prohlídce přítomné, že nosiče informací obsahují i informace, ve vztahu k nimž je tato osoba vázána povinností mlčenlivosti, zabránit zajištění těchto nosičů.* ***Nelze-li toto tvrzení v průběhu prohlídky ověřit a není-li možno oddělit část nosičů informací, které jsou věcmi důležitými pro trestní řízení, od těch nosičů, které obsahují informace netýkající se trestního řízení a jsou chráněny státem uloženou povinností mlčenlivosti, je třeba při provádění prohlídky s prvkem výpočetní techniky zajistit a zadokumentovat veškerou výpočetní techniku a záznamová media, u nichž lze důvodně předpokládat, že obsahují informace důležité pro trestní řízení.***

***Je-li prohlídka jiných prostor*** *(stejně jako domovní prohlídka)* ***prováděna s cílem nalézt a zajistit předměty, které se mohou stát věcnými důkazy*** *ve smyslu § 112 odst. 1 trestního řádu,* ***a je-li tohoto cíle dosahováno postupem dle příslušných ustanovení trestního řádu, nelze považovat za nedovolené porušení povinnosti mlčenlivosti skutečnost, že nosiče informací obsahují i údaje pro probíhající trestní řízení nepodstatné a nepoužitelné, neboť tento cíl nebyl provedením prohlídky sledován, jedná se pouze o vedlejší produkt prohlídky, kterému nebylo možno zabránit, a nikoliv o záměrné získávání údajů chráněných povinností mlčenlivosti způsobem, který by byl v rozporu s předpisy upravujícími prolomení povinnosti mlčenlivosti.“***

V případě kyberkriminality se institut prohlídky jiných prostor a pozemků využije v prostorách, které neslouží k bydlení, jako jsou živnostenské provozovny, sídla či provozovny právnických osob, prodejny a servisy výpočetní techniky, kanceláře, serverovny, datová centra aj.

Specifikum prohlídky jiných prostor a pozemků, stejně tak i domovní prohlídky v případech kyberkriminality spočívá v charakteru věcí, které hodlá policejní orgán získávat jako věcné důkazy. Jedná se zejména o věci informatického typu, programové vybavení, které bývá umístěno na pevných discích počítačů nebo na paměťových médiích. Jejich zajištění je takřka obligatorně nutné provádět za účasti znalce, neboť neodborné zacházení při zajišťování by mohlo způsobit ztrátu dat a zmaření účelu prohlídky. V případě aktivní účasti znalce z oboru informačních technologií na místě prohlídky je možné, a zpravidla i vhodné, zajistit důkazní materiál pomocí otisku dat na technologické zařízení znalce a vytvořit tak tzv. zrcadlovou kopii jakéhokoliv pevného disku (USB, HDD typu PATA, SATA I a II.).

Ke specifikům provádění prohlídky jiných prostor a pozemků a zajišťovaným věcem blíže viz kap. 6.4.3 Domovní prohlídka.

Zajišťování všech nosičů informací (paměťových médií) či celých počítačových systémů (např. serverů, datových úložišť aj.) se zejména v rámci prohlídky jiných prostor a pozemků nejeví vždy jako vhodné. Při zajištění nosiče informací či celého počítačového systému by případně mohla hrozit ekonomická a funkční destrukce společnosti nebo jednotlivce. Takový stav by rozhodně prohlídkou neměl být vytvořen, vždy však záleží na všech okolnostech konkrétního případu, neboť je třeba brát v úvahu i následné užití institutu propadnutí věci či zabrání věci.[833] Mělo by docházet k **naplnění základní zásady minimalizace a subsidiarity zásahů do základních lidských práv a svobod.**

### 6.4.5 Odposlech a záznam telekomunikačního provozu

Instituty odposlechu a záznamu telekomunikačního provozu jsou stěžejní pro odhalování a vyšetřování kyberkriminality. Zejména § 88a TŘ je velmi významný při odhalování pachatele kyberkriminality, neboť umožňuje zjistit **údaje o telekomunikačním provozu**. Uvedené dva instituty jsou zajišťovacími úkony umožňujícími jeden z nejintenzivnějších zásahů do základních lidských práv a svobod.[834]

#### 6.4.5.1 Telekomunikační provoz

Stěžejním bodem, významným pro využití § 88 a 88a TŘ, případně jiných ustanovení trestního řádu je **definování pojmu telekomunikační provoz.**[835] V následující části se pokusím předložit možná východiska právě při definování tohoto pojmu. K vlastnímu definování byla využita ustanovení zákona o elektronických komunikacích, trestního zákoníku, Úmluvy o kyberkriminalitě, komentáře k trestnímu řádu, jakož i nález Ústavního soudu.

1) **Definice dle zákona o elektronických komunikacích**
Jediným místem, kde zákon definuje přímo **telekomunikační provoz** je § 136 odst. 20 písm. a) ZoEK, kde je uvedeno, že pokud zvláštní právní předpis využívá pojem, telekomunikační provoz, **rozumí se tím přenášená zpráva** podle tohoto zákona.

833: § 70 a § 101 TZK

834: Konkrétně čl. 13 Listiny:

*Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon.* ***Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.***

835: Tento pojem vycházel ze zákona č. 151/2000 Sb., o telekomunikacích a změně dalších zákonů, který v § 1 písm. b) definoval, že upravuje i podmínky pro poskytování telekomunikačních služeb. Viz online:
http://itpravo.cz/plne_zneni/telekomunikacni_zakon.txt.
Zákon byl nahrazen zákonem o elektronických komunikacích, který s pojmem „telekomunikace" pracuje pouze minimálně.

Takovouto zprávou je dle § 89 odst. 2 ZoEK **jakákoli informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací**, s výjimkou informace přenášené jako součást veřejného rozhlasového nebo televizního vysílání sítí elektronických komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá.[836]

**Službou elektronických komunikací** [§ 2 písm. n) ZoEK] je **služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb** v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovanými službami elektronických komunikací; **nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.**

**Významným pojmem je síť elektronických komunikací** [§ 2 písm. h) ZoEK], která je definována jako **přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně** družicových sítí, **pevných sítí s komutací okruhů nebo paketů** a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.

Ve vztahu k problematice popisované v této knize je možné uvést, že pojem síť elektronických komunikací v sobě zahrnuje i počítačovou síť,[837] bez ohledu na to, zda je provozována subjektem spadajícím pod působnost zákona o elektronických komunikacích.[838]

Zákon o elektronických komunikacích pak dále vymezuje v § 2 písm. o) **veřejně dostupnou službu elektronických komunikací, kterou je služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.**

Poslední dvě definice sloužící k vlastnímu vymezení pojmu telekomunikační provoz jsou spojeny s vymezením pojmů:

836: Ve vztahu k výše uvedenému se tedy bude jednat o **obsahové zprávy**, na které je možné aplikovat § 88 TŘ, a dále **pak údaje provozní a lokalizační** (viz § 90 a 91 ZoEK), na které je možné aplikovat § 88a TŘ.

**Provozními údaji** (§ 90 odst. 1 ZoEK) se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.

**Lokalizačními údaji** (§ 91 odst. 1 ZoEK) se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.

837: Viz kap. 1.3 Počítačové sítě a jejich fungování.

838: Blíže viz rozdělení ISP – kap. 1.4 ISP (Internet Service Provider) a 2.5 Odpovědnost poskytovatele služeb informační společnosti.

- provozovatel **veřejných telekomunikačních sítí a podnikatel poskytující telekomunikační služby.** Tyto pojmy jsou definovány v § 136 odst. 10 ZoEK, kde je uvedeno, že se jedná o **subjekty**, které vykonávají telekomunikační činnosti na základě telekomunikační licence nebo osvědčení o registraci podle generální licence, jsou povinni splnit oznamovací povinnost podle § 13 nejpozději do 1 měsíce ode dne vydání všeobecného oprávnění.
- **Telekomunikační služba** [§ 136 odst. 20 písm. c) ZoEK], kterou **se rozumí služba elektronických komunikací podle tohoto zákona.**

Je třeba uvést, že veškeré výše uvedené pojmy primárně slouží pro účely zákona o elektronických komunikacích, jehož účelem je upravit podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací.[839]

Nicméně tyto definice, alespoň v hrubých rysech, vymezují některé běžně užívané pojmy.

2) **Definice dle trestního zákoníku**
Významným ustanovením trestního zákoníku, které se vztahuje k pojmu telekomunikační provoz je **§ 182 (Porušení tajemství dopravovaných zpráv) TZK.**[840]

Toto ustanovení se vztahuje na protiprávní aktivity, které zasáhnou zájem chráněný trestním zákoníkem.

Již dříve bylo uvedeno, že ačkoliv vychází trestní zákoník při definování některých pojmů právě ze zákona o elektronických komunikacích, nikde v § 182 TZK není na tento zákon přímo odkazováno jako na normu *lex specialis*. Z tohoto důvodu není možné přijmout zužující pojetí (prezentované zákonem o elektronických komunikacích) výše uvedených pojmů, ve vztahu k působnosti trestního zákoníku akceptovat.[841]

3) **Definice dle Úmluvy o kyberkriminalitě**
Úmluva o kyberkriminalitě, která je součástí právního řádu České republiky ve vztahu k „telekomunikačnímu provozu", definuje dva významné pojmy:

- **poskytovatel služby** [čl. 1 písm. c) Úmluvy o kyberkriminalitě], kde je uvedeno, že poskytovatelem služby je:
  - jakýkoli veřejný nebo soukromý subjekt, **který uživatelům své služby umožňuje komunikovat prostřednictvím počítačového systému**, a
  - jakýkoli jiný subjekt, **který zpracovává nebo uchovává počítačová data pro takovou komunikační službu nebo pro uživatele takové služby.**

839: **Tento zákon se nevztahuje na obsah služeb poskytovaných prostřednictvím sítí elektronických komunikací**, jako je obsah rozhlasového a televizního vysílání, finančních služeb **a některých služeb informační společnosti, není-li dále stanoveno jinak.** Viz § 1 odst. 1, 2 ZoEK.

840: Blíže viz kap. 5.2.2.1.2 Neoprávněné zachycení informací (čl. 3) a 4.11 Sniffing.

841: Blíže viz kap. 5.2.2.1.2 Neoprávněné zachycení informací (čl. 3).

- **provozní data,** která znamenají **jakákoli počítačová data vztahující se ke komunikaci prostřednictvím počítačového systému**, vytvořená počítačovým systémem, jakožto součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby.

Byť Úmluva o kyberkriminalitě přímo nedefinuje pojem telekomunikace, tak pracuje s pojmem provozní data, který je možné (ve vztahu k českému právu) právě k telekomunikaci přiřadit jakožto její součást.

Z tohoto vymezení pak vyplývá, že provozní data, tedy data, jež jsou součástí komunikace, jsou **data vytvořená počítačovým systémem jakožto součástí komunikačního řetězce, uvádějící původ, cíl, cestu, čas, datum, objem nebo trvání komunikace nebo typ příslušné služby.** Z hlediska technického se tedy jedná například o případy, kdy dojde k propojení (spárování) dvou mobilních telefonů pomocí Bluetooth či dvou samostatných počítačů pomocí síťového kabelu (bez jiného připojení k datové či jiné síti). I v rámci komunikace mezi těmito zařízeními pak bude docházet k předávání provozních dat, případně k předávání vlastního obsahu.

4) **Definice dle trestního řádu**
Šámal uvádí, že telekomunikační činnost je možné definovat **jako komunikaci, ke které dochází za využití telefonu, telefaxu, mobilního telefonu, vysílačky či jiného telekomunikačního zařízení <u>včetně zpráv zasílaných elektronickou poštou</u>**.

Jde tedy o „***činnost telekomunikačních zařízení (počítačových systémů), která spočívá v přepravě nebo směrování jak obsahu komunikace*** *(např. hovorů nebo zpráv),* ***tak i souvisejících provozních údajů*** *(např. doprovodných dat identifikujících určité účastnické stanice, datum, čas zahájení, dobu trvání, popřípadě čas ukončení souvisejících činnosti zájmové účastnické adresy, přístupový bod v síti, výpis aktivního a pasivního volání, takzvaný detailbilling apod.).*“ [842]

Pokud bychom akceptovali definici telekomunikačního provozu pouze dle zákona o elektronických komunikacích a v jeho mezích, byla by tato definice v řadě případů v přímém rozporu s trestním řádem. Odesílání a přijímání zpráv zasílaných elektronickou poštou (a analogicky i jinými komunikačními kanály – viz instant messenger, Skype aj.) totiž zpravidla spadá do působnosti jiných ISP než ISP, kteří poskytují veřejně dostupnou službu připojení.[843]

K telekomunikačnímu provozu a právu na ochranu zpráv podávaných telefonem se vyjádřil i Ústavní soud ČR ve sp. Zn II. ÚS 502/2000, ze dne 22. 1. 2000. Z tohoto nálezu vyplývá, že **získávání „logů/výpisů“ na základě např. § 8 odst. 1 TŘ je nezákonné, neboť jde o obcházení § 88 TŘ.** V době rozhodování soudu neexistovalo ustanovení § 88a TŘ, avšak působnost tohoto

842: ŠÁMAL, Pavel a kol.: *Trestní řád I. § 1 až 156. Komentář*. 7. vydání. Praha: C. H. Beck, 2013, s. 1198.
843: Blíže viz kap. <u>1.4 ISP (Internet Service Provider)</u> a dělení ISP v ČR: <u>2.5 Odpovědnost poskytovatele služeb informační společnosti</u>.

rozhodnutí lze analogicky vztáhnout právě i na § 88a TŘ. Stejně tak je možné tento nález aplikovat i na komunikaci, která je prováděna pomocí počítačového systému (nikoli pouze telefonu).

Z vlastního nálezu uvádím:

*„Současná právní úprava nezná institut poskytování či pořizování evidence telekomunikačního provozu pro účely trestního stíhání či plnění úkolů policie (či institut jinak nazvaný, ale obsahově shodný).* ***Neznamená to však, že by příslušné státní orgány nebyly oprávněny za žádných okolností tuto evidenci pořizovat či vyžadovat. S ohledem na to, že jsou stanovena pravidla pro odposlech a záznam telekomunikačního provozu ze strany těchto orgánů, která umožňují kromě dalších údajů pořídit především obsah telefonické zprávy, je možné postupovat podle těchto pravidel i při pořizování či získávání těchto "dalších" údajů****, tj. při evidování telekomunikačního provozu.* ***Orgány činné v trestním řízení****, resp. policejní orgány před zahájením trestního stíhání,* ***jsou tedy v případě pořizování či získávání evidence telekomunikačního provozu povinny postupovat přiměřeně podle § 88 trestního řádu.*** *“* [844]

Na závěr uvedu shrnutí vyplývající z jednotlivých definic:

1) **Úmluva o kyberkriminalitě** definuje **provozní data jako jakákoli data vytvořená počítačovým systémem.**
2) Trestní zákoník se vztahuje na ochranu tajemství všech dopravovaných zpráv (viz § 182 TZK) bez ohledu na to, jakými komunikačními kanály či ISP jsou tyto zprávy přenášeny.
3) **Trestní řád neomezuje telekomunikační provoz pouze na činnost spadající pod zákon o elektronických komunikacích, byť jej částečně využívá při definování tohoto pojmu.**
4) Zákon o elektronických komunikacích se explicitně zaměřuje **pouze na veřejné poskytovatele připojení**. **Restriktivně vymezuje definice právě pro účely tohoto zákona.**
5) V případě telekomunikace nezáleží na geolokaci, ani jiných podmínkách. **Určujícím prvkem je předání informací mezi systémy (počítačovými), které toto předání umožňují.** Vychází se ze skutečného smyslu tohoto slova, tedy: *„tele“* – na dálku a *„communication“* – komunikace.
6) **K telekomunikačnímu provozu tedy dochází ne jen u ISP, kteří spadají pod působnost zákona o elektronických komunikacích, ale i u ostatních ISP.** Zároveň může k telekomunikaci docházet i u fyzických či právnických osob, které např. provozují počítačové sítě, propojují počítačové systémy aj.
7) Může dojít k případnému **střetu dvou norem práva veřejného** (zákona o elektronických komunikacích a trestního řádu), avšak z výše uvedených definic jasně vyplývá, že **jakákoliv restrikce** (tedy i tvrzení, že o telekomunikační provoz nejde v případě počítačových systémů,

844: Nález Ústavního soudu ČR č. **II. ÚS 502/2000**, ze dne 22. 1. 2000. *Právo na ochranu zpráv podávaných telefonem.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=36243&pos=1&cnt=1&typ=result

které nejsou propojeny na základě zákona o elektronických komunikacích) **by byla zásahem do ústavně garantovaných práv a svobod** (viz čl. 13 a viz nález II. ÚS 502/2000[845]).

845: Dále cituji z nálezu:
**V daném případě společnost Eurotel pořídila výpis z telefonního účtu stěžovatele, ve kterém bylo uvedeno mj. číslo volané stanice, datum a čas počátku hovoru, doba jeho trvání, označení základové stanice, která zajišťovala hovor v okamžiku spojení a označení základové stanice, která hovor zajišťovala v momentu ukončení, přičemž tento výpis poskytla na základě blíže nespecifikované žádosti orgánům policie bez souhlasu stěžovatele.**
**Dle názoru Ústavního soudu**, který se tímto ztotožňuje s rozsudkem Evropského soudu pro lidská práva ze dne 2. 8. 1984 ve věci Malone proti Spojenému království, **je třeba považovat výše uvedené údaje, a zvláště pak volaná čísla, za nedílnou součást komunikace uskutečněné prostřednictvím telefonu. Soukromí každého člověka je hodno zásadní (ústavní) ochrany nejen ve vztahu k vlastnímu obsahu podávaných zpráv, ale i ve vztahu k výše uvedeným údajům. Lze tedy konstatovat, že čl. 13 Listiny zakládá i ochranu tajemství volaných čísel a dalších souvisejících údajů, jako je datum a čas hovoru, doba jeho trvání, v případě volání mobilním telefonem i označení základových stanic zajišťujících hovor.**
**Jestliže ústavní pořádek České republiky připouští průlom této ochrany, děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených základních práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a dále tím, aby takové činy byly zjištěny a potrestány.** Přípustný je tedy pouze zásah do základního práva nebo svobody člověka ze strany státní moci, jestliže jde o zásah nezbytný ve výše uvedeném smyslu. **K tomu, aby nebyly překročeny meze nezbytnosti, musí existovat systém adekvátních a dostatečných záruk, skládající se z odpovídajících právních předpisů a účinné kontroly jejich dodržování.** Tyto právní předpisy musí být přesné ve svých formulacích, aby daly občanům dostatečnou informaci o okolnostech a podmínkách, za kterých jsou státní orgány oprávněny k zásahu do soukromí; přesně musí být definovány i pravomoci udělené příslušným orgánům a způsob jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování (viz také shora citovaný rozsudek Evropského soudu pro lidská práva). V případě, že tyto zásady nebudou ze strany státní moci respektovány, jsou zásahy do uvedeného základního práva vyloučeny a dojde-li k nim, stávají se protiústavními.
Současná právní úprava nezná institut poskytování či pořizování evidence telekomunikačního provozu pro účely trestního stíhání či plnění úkolů policie (či institut jinak nazvaný, ale obsahově shodný). **Neznamená to však, že by příslušné státní orgány nebyly oprávněny za žádných okolností tuto evidenci pořizovat či vyžadovat. S ohledem na to, že jsou stanovena pravidla pro odposlech a záznam telekomunikačního provozu ze strany těchto orgánů, která umožňují kromě dalších údajů pořídit především obsah telefonické zprávy, je možné postupovat podle těchto pravidel i při pořizování či získávání těchto "dalších" údajů**, tj. při evidování telekomunikačního provozu. **Orgány činné v trestním řízení**, resp. policejní orgány před zahájením trestního stíhání, **jsou tedy v případě pořizování či získávání evidence telekomunikačního provozu povinny postupovat přiměřeně podle § 88 trestního řádu**, resp. podle § 36 zákona č. 283/1991 Sb., o Policii ČR, ve znění pozdějších předpisů, a to tak, že pojem "záznam" se vztahuje také na údaje získané evidováním telekomunikačního provozu ve vztahu ke konkrétní osobě nebo osobám. Touto ústavně konformní interpretací citovaných ustanovení lze dosáhnout účinné kontroly před neoprávněnými zásahy do daného základního práva ze strany státních orgánů, když současně nebude vyloučena pro tyto orgány možnost pořizovat nepochybně často nezbytný typ důkazů pro plnění svých funkcí, a to případně do doby přijetí specifické právní úpravy ohledně pořizování těchto údajů. K tomu je třeba poznamenat, že dle názoru Ústavního soudu by pravidlům Úmluvy o ochraně lidských práv a základních svobod mnohem lépe vyhověla speciální zákonná úprava, která, jak bylo shora uvedeno, zatím chybí.
**Na základě výše uvedených závěrů Ústavního soudu lze konstatovat, že předmětný důkaz byl pro účely trestního řízení pořízen protiprávně, v důsledku čehož je zařazení takového důkazu do spisu a jeho provádění nejen nezákonné, ale i ústavně zcela nepřípustné.**

### 6.4.5.2 Odposlech a záznam telekomunikačního provozu

K zajištění **obsahu přenášených informací včetně provozních a lokalizačních údajů je využíváno institutu odposlechu a záznamu telekomunikačního provozu dle § 88 TŘ**. Dle § 88 odst. 1 TŘ je možné nařídit odposlech a záznam telekomunikačního provozu pouze u zločinů, na které zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, dále pro vyjmenované zločiny,[846] i když je horní hranice trestu svobody nižší než osm let, nebo pokud se jedná o jiné úmyslné trestné činy, k jejichž stíhání zavazuje vyhlášená mezinárodní smlouva.

Díky ratifikaci Úmluvy o kyberkriminalitě a Dodatkovému protokolu je možné využít institut odposlechu a záznamu telekomunikačního provozu i na řadu kybernetických trestných činů, u nichž nejsou splněny první dvě podmínky uvedené v § 88 odst. 1 TŘ (tj. jde o zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, nebo zločin explicitně uvedený v § 88 odst. 1 TŘ). Úmluva o kyberkriminalitě definuje úmyslné trestné činy, k jejichž stíhání nás zavazuje. Konkrétně se jedná o trestné činy uvedené nyní v § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací), § 231 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) TZK.

- **Trestné činy proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů**
  - Neoprávněný přístup (čl. 2 Úmluvy o kyberkriminalitě) - **§ 230 odst. 1 TZK**
  - Neoprávněné zachycení informací (čl. 3 Úmluvy o kyberkriminalitě) - **§ 182** TZK
  - Zásah do dat (čl. 4 Úmluvy o kyberkriminalitě) - **§ 230 odst. 2 písm. a) a b) TZK**
  - Zásah do systému (čl. 5 Úmluvy o kyberkriminalitě) - **§ 230 odst. 2 písm. d)** TZK
  - Zneužití zařízení (čl. 6 Úmluvy o kyberkriminalitě) - **§ 231 TZK**

- **Trestné činy ve vztahu k počítači**
  - Padělání související s počítači (čl. 7 Úmluvy o kyberkriminalitě) - **§ 230 odst. 2 písm. c) TZK**
  - Podvod související s počítači (čl. 8 Úmluvy o kyberkriminalitě) - § **209 a § 230 odst. 2 TZK**
- **Trestné činy se vztahem k obsahu počítače**
  - Trestné činy související s dětskou pornografií (čl. 9 Úmluvy o kyberkriminalitě) - **§ 192, 193a, 193, 193b TZK**
  - Šíření rasismu a xenofobie - **§ 356, 403, 352, 355, 405** TZK

- **Trestné činy se vztahem k autorským nebo obdobným právům - § 270 TZK**[847]

Existuje však řada kybernetických trestných činů, které nejsou v § 88 TŘ ani v Úmluvě o kyberkriminalitě (případně jiné mezinárodní smlouvě) přímo vyjádřeny, a v takovém případě by

846: § 226 (Pletichy v insolvenčním řízení), § 248 odst. 1 písm. e) a odst. 2 až 4 (Porušení předpisů o pravidlech hospodářské soutěže), § 256 (Zjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě), § 257 (Pletichy při zadání veřejné zakázky a při veřejné soutěži), § 258 (Pletichy při veřejné dražbě), § 329 (Zneužití pravomoci úřední osoby) TZK.

847: Ke všem trestným činům blíže viz kap. 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku.

odvolávání se na Úmluvu o kyberkriminalitě mohlo znamenat nepřípustné rozšiřování podmínek užití institutu odposlechu a záznamu telekomunikačního provozu.

Mezi tyto činy patří zejména:

- § 180 neoprávněné nakládání s osobními údaji,
- § 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,
- § 184 pomluva,
- § 191 šíření pornografie,
- § 287 šíření toxikomanie,
- § 345 křivé obvinění,
- § 348 padělání a pozměnění veřejné listiny,
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob,
- § 356 podněcování k nenávisti vůči skupině osob nebo k omezování práv a svobod,
- § 357 šíření poplašné zprávy,
- § 364 podněcování k trestnému činu,
- § 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka,
- § 407 podněcování útočné války.

Institutu odposlechu a záznamu telekomunikačního provozu je také možné využít i bez příkazu, pokud s tím uživatel odposlouchávané stanice souhlasí a je vedeno trestní řízení pro trestný čin dle § 168 (Obchodování s lidmi), § 169 (Svěření dítěte do moci jiného), § 171 (Omezování osobní svobody), **§ 175 (Vydírání)**, § 200 (Únosu dítěte a osoby stižené duševní poruchou), § 352 (Násilí proti skupině obyvatelů a proti jednotlivci), **§ 353 (Nebezpečného vyhrožování)** nebo **§ 354 (Nebezpečného pronásledování)**.

Ve vztahu ke kyberkriminalitě je z výše uvedených trestných činů možné využít zejména § 175 (např. ransomware, šikana aj.), § 353 (např. šíření závadového obsahu aj.), § 354 (např. kyberstalking) TZK.

Jsem názoru, že by bylo vhodné doplnit § 88 odst. 5 TŘ minimálně o tyto trestné činy, jichž se pachatel může v rámci kyberkriminality dopustit: **§ 177** TZK (Útisk), **§ 230** TZK (Neoprávněný přístup k počítačovému systému a nosiči informací). U zde uvedených trestných činů je uživatel, který s odposlechem a záznamem telekomunikačního provozu své účastnické stanice souhlasí, zároveň v procesním postavení poškozeného.

Důvody a podmínky odposlechu a záznamu telekomunikačního zařízení jsou uvedeny v § 88 odst. 1 TŘ. **Důvodem** je získání významných skutečností[848] důležitých pro trestní řízení. **Podmínkou** je, že nelze skutečnosti významné pro trestní řízení získat jinak nebo je jejich získání podstatně ztížené.[849]

848: Jedná se o skutečnosti, které je třeba dokazovat - viz § 89 odst. 1 TŘ.

849: Blíže NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009, s. 218

Odposlech a záznam telekomunikačního provozu provádí, pro potřeby všech orgánů činných v trestním řízení, Policie České republiky.[850] Kontrolu při použití odposlechu a záznamu telekomunikačního provozu vykonává Poslanecká sněmovna ČR, která k tomuto účelu zřizuje kontrolní orgán. Tuto kontrolu vykonává v příslušných útvarech Policie po předchozím vyrozumění ministra vnitra.[851]

Odposlech a záznam telekomunikačního provozu mezi obhájcem a obviněným je nepřípustný. Pokud policejní orgán při odposlechu a záznamu telekomunikačního provozu zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam odposlechu bezodkladně zničit a informace, které se v této souvislosti dozvěděl, nijak nepoužít.[852]

Odposlech a záznam telekomunikačního provozu může být vykonán i před zahájením trestního stíhání jako neodkladný nebo neopakovatelný úkon.[853]

Příkaz k odposlechu a záznamu telekomunikačního provozu je oprávněn vydat **předseda senátu a v přípravném řízení na návrh státního zástupce soudce.** Příkaz k odposlechu a záznamu telekomunikačního provozu je rozhodnutím *sui generis*. Příkaz musí být písemný a odůvodněný. **Odposlech** a záznam telekomunikačního provozu dle § 88 TŘ **je realizován od okamžiku vydání rozhodnutí do budoucna.** V příkazu musí být uvedeny:

- obecné náležitosti,[854]
- uživatelská adresa či zařízení,
- osoba uživatele, je-li její totožnost známa,

850: Konkrétně ÚZČ.

851: ŠÁMAL, Pavel a kol.: *Trestní řád I. § 1 až 156. Komentář*. 7. vydání. Praha: C. H. Beck, 2013, s. 1205

852: § 88 odst. 1 TŘ

853: Srov. Rozhodnutí Nejvyššího soudu 5 Tdo 459/2007, ze dne 3.5.2007 [online]. [cit. 25. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/1056AA7881B123EEC1257A4E0064DE83?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 15 Tdo 510/2013, ze dne 26.6.2013 [online]. [cit. 25. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/592226D3401E2466C1257BAD0044D215?openDocument&Highlight=0

Odposlech a záznam telekomunikačního provozu pro účely trestního řízení je upraven v ustanovení § 88 TŘ, které připouští i provedení takových úkonů před zahájením trestního stíhání, jde-li o úkony neodkladné či neopakovatelné ve smyslu ustanovení §160 odst. 4 TŘ.

854: Označení orgánu, den a místo rozhodnutí, uvedení zákonných ustanovení, které ukládají povinnost. Dále pak konkrétní odkaz na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje.

- doba, po kterou bude odposlech a záznam telekomunikačního provozu uskutečňován,[855]
- odůvodnění.[856]

Opis příkazu k odposlechu a záznamu telekomunikačního provozu se bezodkladně doručí policejnímu orgánu, který tento úkon provádí. V přípravném řízení je soudce povinen doručit opis příkazu i státnímu zástupci.[857]

Ustanovení **§ 88 odst. 5** TŘ umožňuje provést odposlech a záznam telekomunikačního provozu i bez tohoto příkazu, pokud je vedeno trestní řízení pro jeden ze zde taxativně uvedených trestných činů.

Odposlechem a záznamem telekomunikačního provozu je mimo jiné[858] možné zjistit i obsah zpráv přenášených telefony (bez rozdílu, zda se jedná o pevnou linku či mobilní telefon), telefaxy, radiostanicemi a jinými elektronickými komunikačními zařízeními. Je tedy možné zjistit i obsah zpráv posílaných počítačovými systémy (např. nedoručených e-mailových zpráv, komunikace VoIP, instant messengerové zprávy aj.).

Policejní orgán je povinen průběžně vyhodnocovat, zda i nadále trvají důvody, které vedly k vydání příkazu k odposlechu a záznamu telekomunikačního provozu. Pokud důvody pominuly, je policejní orgán povinen odposlech a záznam telekomunikačního provozu ihned ukončit, a to i před skončením doby uvedené v § 88 odst. 2 TŘ (tedy doby, na kterou byly odposlech a záznam telekomunikačního provozu povoleny). Tuto skutečnost bezodkladně písemně oznámí předsedovi senátu, který příkaz k odposlechu a záznamu telekomunikačního provozu vydal, a v přípravném řízení rovněž státnímu zástupci a soudci.[859]

Státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvého stupně po pravomocném skončení věci informuje o nařízeném odposlechu a záznamu telekomunikačního provozu uživatele odposlouchávané stanice.[860] Tento přístup je v souladu s judikaturou Evropského soudu pro lidská práva navazující

855: Tato doba nesmí být delší než čtyři měsíce, lze ji však opakovaně prodlužovat o maximálně další čtyři měsíce.

856: Je třeba uvést konkrétní skutkové okolnosti, a vysvětlit důvody, proč nelze sledovaného účelu dosáhnout jinak nebo proč by bylo jinak jeho dosažení podstatně ztížené.

857: Viz § 88 odst. 2 TŘ

858: Dále je možné zajistit i provozní a lokalizační údaje.

859: § 88 odst. 3 TŘ

860: § 88 odst. 8 TŘ

na čl. 8 Evropské úmluvy o ochraně lidských práv,[861] podle které vždy (kdy je to možné a kdy to nepopírá smysl tajného odposlechu) musí být osoba dodatečně seznámena s tím, že její hovory byly odposlouchávány, a musí mít k dispozici opravný prostředek, jímž může namítat nezákonnost nebo bezdůvodnost odposlechu.[862] Informace podávaná uživateli odposlouchávané stanice musí obsahovat:

- označení soudu, který příkaz vydal,
- délku trvání odposlechu,
- datum ukončení odposlechu,
- poučení o opravném prostředku.

Výše uvedená informace nemusí být podána v řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti na organizované zločinecké skupině, nebo pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel trestního řízení, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv a svobod osob.[863]

Využití odposlechu a záznamu telekomunikačního provozu dle § 88 TŘ bude v případech kyberkriminality možné zejména k:

- **zajištění dat (obsahu komunikace) doposud neuskutečněné (budoucí, či probíhající) komunikace (online).** Zajistit je možné jakoukoli komunikaci, která bude probíhat (např. VoIP, komunikaci skrze Skype, jiné instant messengery atp.)
- **zjištění obsahu budoucí e-mailové elektronické komunikace (online)**

V obou případech je nutné, aby soudce stanovil počátek a konec doby realizace vlastního úkonu, přičemž tato doba nesmí přesáhnout čtyři měsíce. Pokud nestanoví počátek, lze se domnívat, že počátkem je den vydání příkazu. Datum ukončení však chybět nemůže.

861: Blíže viz *Evropská úmluva o ochraně lidských práv.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

**Článek 8** Právo na respektování soukromého a rodinného života

(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

(2) Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

862: ŠÁMAL, Pavel a kol.: *Trestní řád I. § 1 až 156 : komentář*. 7. vydání. Praha: C. H. Beck, 2013, s. 1214

863: § 88 odst. 9 TŘ

- **zjištění obsahu e-mailové elektronické komunikace v zajištěném datovém nosiči uskutečněné v době po jeho zajištění orgány činnými v trestním řízení (tzn. online)**

Pokud bude orgán činný v trestním řízení předpokládat, že by se v době po zajištění věci [počítačového systému (typicky počítače, mobilu aj.), e-mailové schránky, datového nosiče aj.] mohla ve vztahu k této zajištěné věci, jako technickému zařízení, uskutečnit pro objasnění věci důkazně významná elektronická komunikace, se kterou nebude mít příjemce možnost se seznámit, bude muset být vydán příkaz dle ustanovení § 88 TŘ (to platí pro hlasové, textové, datové, obrazové či jiné přenosy). Ke zjištění obsahu e-mailové elektronické komunikace uskutečněné v době po zajištění datového nosiče orgánem činným v trestním řízení je tedy třeba příkazu soudce podle § 88 TŘ (pokud již předmětný příkaz nebyl vydán před zajištěním datového nosiče a doba jeho platnosti stále trvá). Postup podle § 88a TŘ je vyloučen, neboť dochází k zajištění obsahu dat.

**Ustanovení § 88 TŘ je ve vztahu speciality k ustanovení o sledování osob a věcí** (blíže viz kap. 6.4.6.1 Sledování osob a věcí).[864]

### 6.4.5.3 Zjištění údajů o telekomunikačním provozu

Základní rozdíl mezi § 88 a § 88a TŘ spočívá v povaze zajišťovaných dat resp. informací.[865] Na základě § 88a TŘ mohou orgány činné v trestním řízení **zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat.** Zajišťovány jsou tedy provozní a lokalizační případně další systémové údaje,[866] avšak není zaznamenáván obsah zpráv, tak jak tomu je v případě § 88 TŘ.

Využití § 88a TŘ je jedním ze stěžejních prostředků sloužícím k získání informací a důkazů důležitých pro trestní řízení, zejména tím, že se snaží zrekonstruovat skutkový děj, který se zpravidla odehrál v minulosti.

**Důvodem** využití § 88a TŘ je získání významných skutečností[867] důležitých pro trestní řízení vedené pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní

---

864: Blíže viz stanovisko **Nejvyššího státního zastupitelství 1 SL 760/2014.** *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, ze dne 26. 1. 2015.* [online]. [cit. 24. 8. 2016]. Dostupné z:
http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

865: Ustanovení § 88a TŘ bylo zákonodárcem vloženo za ustanovení § 88 TŘ a nese společný název avšak povaha zajišťovaných informací resp. dat je odlišná. V § 88a TŘ dochází pouze ke zjišťování údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat. **Dále jen údaje o telekomunikačním provozu.**

866: Viz kap. 2.5.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZoEK.

867: Jedná se o skutečnosti, které je třeba dokazovat - viz § 89 odst. 1 TŘ.

sazby nejméně tři roky, jiný vyjmenovaný trestný čin[868] nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána (konkrétně Úmluva o kyberkriminalitě a Dodatkový protokol).[869] **Podmínkou** využití § 88a TŘ je, že nelze skutečnosti významné pro trestní řízení získat jinak nebo bylo-li by jejich získání podstatně ztížené.[870]

Příkaz ke zjištění údajů o telekomunikačním provozu je oprávněn vydat **příkaz předseda senátu a v přípravném řízení na návrh státního zástupce soudce.** Tento příkaz je rozhodnutím *sui generis*. Příkaz musí být písemný a odůvodněný. V příkazu musí být uvedeny:

- obecné náležitosti,[871]
- časový úsek, za který mají být údaje sděleny,
- údaje o uživateli (pokud se příkaz vztahuje k uživateli, musí být uvedena totožnost, je-li známa),
- účel zjišťování údajů (zejména informace o trestném činu, pro který je vedeno trestní řízení nebo pro který bylo zahájeno trestní stíhání),
- jakým způsobem mají být údaje sděleny (písemně, elektronicky aj.),
- odůvodnění.[872]

Bez příkazu je možné zjistit údaje o telekomunikačním provozu pouze tehdy, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení.[873]

Zjištění údajů o telekomunikačním provozu dle § 88a TŘ **je možné realizovat jak do minulosti, tak do budoucnosti.** Toto tvrzení vychází z jazykového výkladu § 88a: *„Je-li třeba zjistit údaje o telekomunikačním provozu…* “[874]

Jelikož toto ustanovení neodkazuje na zákon o elektronických informacích jako na *lex specialis*, lze vyvozovat, že je možné žádat údaje o telekomunikačním provozu i po dobu delší než 6 měsíců

868: **§ 182 (Porušení tajemství dopravovaných zpráv), § 209 (Podvod), § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací), § 231 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat)**, **§ 353 (Nebezpečné vyhrožování) § 354 (Nebezpečné pronásledování), § 357 (Šíření poplašné zprávy), § 364 (Podněcování k trestnému činu)**, § 365 (Schvalování trestného činu) TZK.
Většina zde uvedených trestných činů může být spáchána v kyberprostoru – viz kap. 4 Projevy kyberkriminality.
869: Blíže viz kap. 5.1.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě a 5.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě.
870: Blíže NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009, s. 218
871: Označení orgánu, den a místo rozhodnutí, uvedení zákonných ustanovení, které ukládají povinnost. Dále pak konkrétní odkaz na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje.
872: Je třeba uvést konkrétní skutkové okolnosti a vysvětlit důvody, proč nelze sledovaného účelu dosáhnout jinak nebo proč by bylo jinak jeho dosažení podstatně ztížené.
873: § 88a odst. 4 TŘ
874: V předchozí právní úpravě § 88a TŘ byla uvedena podmínka: *„o uskutečněném telekomunikačním provozu…* “, tato podmínka však v současné právní úpravě není.

do minulosti, samozřejmě za předpokladu, že je konkrétní dožadovaný subjekt má. Zároveň je možné § 88a TŘ využít ke zjištění údajů o telekomunikačním provozu směrem do budoucnosti. Příkladem může být sledování přístupů k serveru obsahujícímu např. dětskou pornografii a následná identifikace počítačových systémů na základě přístupů k tomuto serveru. **Z tohoto pohledu je významné, aby předseda senátu, případně soudce přesně stanovil časový úsek, po který má být tento institut do budoucnosti uplatňován.** Pokud soudce nestanoví dobu, do kdy má být zjištění údajů o telekomunikačním provozu prováděno je otázkou, zda je analogicky možné využít § 88 TŘ, který stanoví maximální délku odposlechu a záznamu telekomunikačního provozu na 4 měsíce.

Osobně se domnívám, že v tomto případě není možné tuto analogii využít, neboť § 88a TŘ nikde nestanoví lhůtu, po kterou má být zjištění údajů o telekomunikačním provozu prováděno, tak jako tomu je právě v § 88 odst. 2 TŘ.

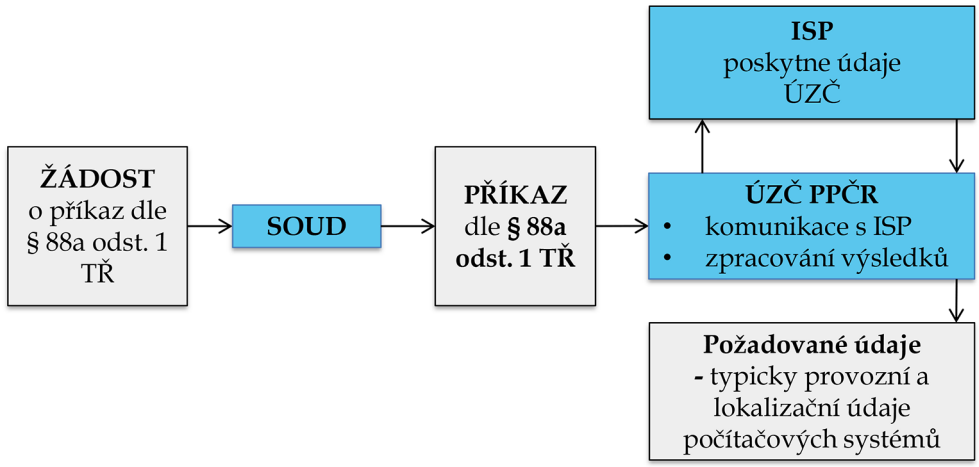
Pokud má zjištění údajů o telekomunikačním provozu sloužit jako důkaz, je třeba, aby byl doplněn o protokol, ve kterém je uvedeno: místo, čas, způsob a obsah provedeného záznamu, jakož i označení osoby, která takovýto záznam pořídila.[875]

*„Při automaticky prováděném záznamu telekomunikačního provozu je za „osobu, která záznam pořídila" ve smyslu § 88 odst. 2 TŘ, nutno považovat útvar zvláštních činností* (ÚZČ) *služby kriminální policie a vyšetřování Policie ČR, a nikoli fyzickou osobu, která aktivovala a deaktivovala odposlech na uživatelské adrese zadávacího terminálu, jelikož ta se samostatným procesem odposlechu a záznamu telekomunikačního provozu nemá žádnou skutečnou vazbu a nenese ani bezprostřední odpovědnost za průběh odposlechu záznamu."* (viz Rt. 4 Tz 31/2004).

V případě nařízení zjišťování údajů o telekomunikačním provozu vzniká obdobná povinnost informovat osobu uživatele, jako je tomu v případě odposlechu a záznamu telekomunikačního provozu.[876]

875: Srov. FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 316

876: Viz § 88a odst. 2 a 3 TŘ




Obrázek 86: Zjednodušené schéma zajištění informací a důkazů od ISP

Institut dle § 88a TŘ může být využit například ke zjištění **údajů o telekomunikačním provozu bez zjišťování obsahu přenášených zpráv.** Jedná se například o:

1) **IP adresa**
   - zjištění uživatele, který v daný čas disponoval konkrétní IP adresou
   - umístění přípojného bodu
   - zjištění všech uživatelů za NAT (dle poskytnutí neveřejných IP adres)
   - zjištění všech uživatelů za NAT dle zjištěných identifikátorů (MAC adresa, neveřejná IP, datum čas, navštívené URL aj. Zjištění, zda mají uživatelé za NAT přidělené statické, nebo dynamické IP adresy – jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ.)
   - zjištění jedinečných identifikátorů uživatelů za NAT (MAC adresa, IP adresa v rámci subsítě aj. - jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ)

2) **e-mail**
   - zjištění přístupu do schránky - logy sice vytváří provozovatel, vypovídají však o uživateli a mají tedy charakter provozních a lokalizačních údajů. U telefonní služby tyto údaje rovněž vytváří a disponuje s nimi výhradně poskytovatel, přesto o jejich ochraně nikdo nepochybuje a užití § 88a se považuje za zcela samozřejmé. Vzhledem k charakteru e-mailové komunikace je možné tuto analogii použít[877]

877: Nález Ústavního soudu ČR č. II. ÚS 502/2000, ze dne 22. 1. 2000. *Právo na ochranu zpráv podávaných telefonem.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=36243&pos=1&cnt=1&typ=result

- informace o posledním přihlášení v rozsahu (datum, čas, IP adresa)
- zjištění identifikačních a registračních (provozních) údajů – jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ
- vkládání obsahu (kdy, co a odkud bylo vloženo) – jde-li o vkládání obsahu do budoucna, je třeba využít § 88 TŘ
- celkové využití kapacity e-mailové schránky, počet nastavených filtrů a adres nebo čísel mobilních telefonů, na něž jsou zprávy přeposílány nebo avizovány
- počet osob v adresáři, uložených zpráv, vlastních složek

3) **Webová stránka**
   - zjištění logů administrátora stránek (vkládání obsahu a správy stránky)
   - zjištění logů přístupu na stránky do oblasti veřejně přístupných služeb
   - zjištění logů přístupu na stránky do oblasti veřejně nepřístupných služeb (zajištěné např. heslem)
   - informace, jaké všechny služby uživatel využívá – jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ
   - zjištění logů vložených příspěvků – jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ
   - zjištění IP adresy zřízení profilu – jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ
   - vyhledávání jiných účtů dle profilu – jedná-li se o organizačně technickou informaci, která je ISP známa z jeho činnosti, je dostačující využít žádosti podle ustanovení § 8 odst. 1 TŘ

### 6.4.6 Operativně pátrací prostředky

*„**Velmi důležitou formou úkonů**, jejichž procesní hodnota je bez ohledu na procesní stadium nesporná, **jsou operativně pátrací prostředky** (§ 158b–158e TŘ).“*[878]

Operativně pátrací prostředky bývají zpravidla využity v přípravném řízení, tedy jak ve fázi postupu před zahájením trestního stíhání, tak v průběhu vyšetřování. Po podání obžaloby o jejich použití rozhoduje předseda senátu soudu prvního stupně i bez návrhu státního zástupce.[879] Mezi tyto prostředky patří:

878: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 481

879: § 158f TŘ

a) předstíraný převod,
b) sledování osob a věcí,
c) použití agenta.[880]

Vlastní použití operativně pátracích prostředků **nesmí sledovat jiný zájem než získání skutečností důležitých pro trestní řízení**. **Tyto prostředky je možné použít jen tehdy, nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené.** Zároveň je v případě použití operativně pátracích prostředků explicitně vyjádřena zásada přiměřenosti (zdrženlivosti).[881]

Operativně pátrací prostředky mají zvláštní postavení mezi důkazními prostředky,[882] neboť ustanovení § 158b odst. 3 TŘ stanoví, že *„zvukové, obrazové a jiné záznamy získané při použití operativně pátracích prostředků způsobem odpovídajícím ustanovením tohoto zákona lze použít jako důkaz.*"

### 6.4.6.1 Sledování osob a věcí

Z hlediska kyberkriminality lze využít zejména institut **sledování osob a věcí** (§ 158d TŘ), kterým se dle tohoto ustanovení rozumí *„získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky.*"

Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít.[883]

Vlastní sledování osob a věcí je možné, podle povahy povolování tohoto institutu, rozdělit na dvě oblasti:

- sledování, při kterém mají být **pořizovány zvukové, obrazové nebo jiné záznamy**, lze uskutečnit pouze na základě písemného **povolení státního zástupce** (§ 158d odst. 2 TŘ)
- sledování, kterým je **zasahováno do** nedotknutelnosti obydlí, do **listovního tajemství nebo pokud má být zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků**, lze je uskutečnit **jen na základě předchozího povolení soudce. (§ 158d odst. 3 TŘ)**

880: Viz § 158b odst. 1 TŘ

881: Blíže viz § 158b odst. 2 TŘ. **Zásada přiměřenosti (zdrženlivosti znamená), že do práv a svobod osob**, jichž se takové úkony dotýkají lze **zasahovat jen v odůvodněných případech na základě zákona a v nezbytné míře pro zajištění účelu trestního řízení**.

882: Viz kap. 6.4.6 Operativně pátrací prostředky.

883: Viz § 158d odst. 1 TŘ

Obdobně, jako tomu je u odposlechu a záznamu telekomunikačního provozu, platí i v případě využití institutu dle § 158d odst. 3 TŘ povinnost sepsat protokol s náležitostmi uvedenými v § 55 a 55a TŘ[884] tak, aby bylo možno zjištěné skutečnosti použít jako důkaz.

Ustanovení § 158d odst. 3 TŘ umožňuje zásah ***„do listovního tajemství nebo zjišťování obsahu jiných písemností a záznamů uchovávaných v soukromí.“*** Na základě znění zákona tedy dochází ke **zjištění obsahu již uskutečněné e-mailové komunikace.**

K této problematice se vyjadřoval v usnesení Ústavní soud ve III. ÚS 3812/2012, ze dne 3. 10. 2013 - *Ke sledování dat uložených v počítačích v rámci institutu sledování osob a věcí pro účely trestního řízení.*[885] V rozhodnutí bylo mimo jiné uvedeno:

*„Ústavní soud se především ztotožňuje se závěry Vrchního soudu v Praze, pokud jde o otázku, zda orgány činné v trestním řízení překročily rámec institutu sledování osob a věcí dle § 158d TŘ, resp. zda tyto orgány postupovaly v mezích povolení vydaného ke sledování soudem.* ***Sledováním osob a věcí se dle citovaného ustanovení rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem nebo jinými prostředky.*** *Z dikce zákona jasně vyplývá, že* ***v rámci tohoto úkonu lze pořizovat záznamy nejrůznějšího druhu a se souhlasem soudce může být v přiměřené míře zasahováno do práva na soukromí dotčených osob. Z hlediska ústavněprávní kontroly je podstatné, že soud ve svém povolení dostatečně jasně specifikoval okruh počítačů, které mají být sledovány.*** *V rámci sledování elektronických zařízení z povahy věci plyne, že předmětem sledování budou právě data na těchto zařízeních uložená, jejichž otisk lze pořídit za využití utajené operativně pátrací techniky.* ***Pořízení otisku elektronických dat lze povolit postupem dle § 158d odst. 3 TŘ, pokud jde o data na sledovaných počítačích již uložená, nikoli o data telekomunikačního provozu.“***

Institut sledování osob a věcí dle § 158d odst. 3 TŘ lze aplikovat na data již uložená v počítačovém systému, nikoli na data, která do tohoto systému budou teprve přenesena (data mající povahu telekomunikačního provozu). K zajištění takovýchto dat je třeba využít § 88 případně § 88a TŘ.

Institut ustanovení § 158d odst. 3 TŘ je přitom možné použít na zprávy, které se aktuálně v e-mailové schránce nacházejí, jsou odeslané, odstraněné (nikoli permanentně), rozepsané, přijaté (doručené). A to včetně těch, které si zatím příjemce nepřečetl, pokud měl objektivně možnost s touto schránkou v daný čas disponovat (tj. měl možnost se do schránky přihlásit a rozhodnout se, že doručenou zprávu uchová, či trvale odstraní). **Analogicky je možné využít toto ustanovení i na kontakty, službu kalendář, messenger aj., pokud je uživateli ponechána možnost objektivní správy svého účtu.**

884: Viz § 158d odst. 7 TŘ

885: Viz Nález Ústavního soudu III. ÚS 3812/2012, ze dne 3. 10. 2013. *Ke sledování dat uložených v počítačích v rámci institutu sledování osob a věcí pro účely trestního řízení.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=81007&pos=1&cnt=1&typ=result

K problematice zajišťování e-mailových zpráv v jednotlivých fázích jejich přenosu dále vydalo stanovisko i **Nejvyšší státní zastupitelství (viz 1 SL 760/2014.** *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, ze dne 26. 1. 2015.).*[886] Z tohoto stanoviska vyjímám pouze závěry:

- ***Zjišťování obsahu elektronické komunikace uskutečněné po zajištění datového nosiče orgánem činným v trestním řízení je možné v reálném čase postupem podle § 88 trestního řádu**, nikoli už podle § 88a trestního řádu.*

- ***Aktuální obsah e-mailové schránky je určován vůlí uživatele a lze jej zjišťovat postupem podle § 158d odst. 3 trestního řádu**, který je možno považovat za zákonnou licenci prolamující ústavně zaručené právo na ochranu soukromí v e-mailové schránce se nacházejících záznamů, a to podle platné právní úpravy v případě trestního řízení pro kterýkoli úmyslný trestný čin.*

- ***Zjišťování e-mailové komunikace v reálném čase je možné jen postupem podle § 88 odst. 1 trestního řádu, neboť se stejně jako telekomunikační provoz uskutečňuje rovněž v síti elektronických komunikací. Postup podle § 88a trestního řádu není v takovém případě možný.***

Sledování osob a věcí dle § 158d odst. 3 TŘ může být v oblasti kyberkriminality například využito k:

- **provedení zálohy obsahu stránky veřejně nepřístupných služeb pro účely pozdějšího vydání věci na základě příslušného rozhodnutí,**
- **vydání obsahů veřejných nepřístupných služeb,**
- **zjištění obsahu e-mailové schránky včetně obsahu uložených zpráv,**
- **zjištění kontaktů z adresáře,**
- **provedení zálohy obsahu e-mailové schránky.**

### 6.4.6.2 Použití agenta

Dalším operativně pátracím prostředkem, který by bylo možné využít v případě kyberkriminality, je použití agenta (§ 158e TŘ).

Policejní orgán, pokud se jedná o útvar Policie České republiky nebo Generální inspekce bezpečnostních sborů, je oprávněn použít agenta v případech, že je vedeno trestní řízení pro zločin,

886: Blíže viz stanovisko **Nejvyššího státního zastupitelství 1 SL 760/2014.** *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, ze dne 26. 1. 2015.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, nebo pro některý z vyjmenovaných trestných činů[887] nebo **pro jiný úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána.** Stejně jako v případě odposlechu a záznamu telekomunikačního provozu dle § 88 a 88a TŘ jsou těmito mezinárodními smlouvami Úmluva o kyberkriminalitě a Dodatkový protokol.

*„**Použití agenta** (§ 158e) vytváří možnost infiltrace policie do kriminálního prostředí, v němž se páchají nejzávažnější činy. Tyto prostředky neposkytují přímý poznatek pro orgány činné v trestním řízení, jenž by měl charakter důkazu. Ostatně trestní řád zdůrazňuje použitelnost zvukových, obrazových a jiných záznamů získaných při použití těchto prostředků jako důkazu (§ 159b odst. 3), a nikoli těchto prostředků přímo.“* [888]

Agentem je příslušník Policie České republiky nebo Generální inspekce bezpečnostních sborů, který plní úkoly uložené mu řídicím policejním orgánem, vystupující zpravidla se zastíráním skutečného účelu své činnosti. Je-li to k použití agenta, jeho přípravě nebo k jeho ochraně nutné, je k zastírání jeho totožnosti možné:

- vytvořit legendu o jiné osobní existenci a osobní údaje vyplývající z této legendy zavést do informačních systémů provozovaných podle zvláštních zákonů,
- provádět hospodářské činnosti, k jejichž vykonávání je třeba zvláštní oprávnění, povolení či registrace,
- zastírat příslušnost k Policii České republiky nebo ke Generální inspekci bezpečnostních sborů.[889]

Použití agenta povoluje na návrh státního zástupce vrchního státního zastupitelství soudce vrchního soudu. V povolení musí být uveden:

- účel použití,
- doba, po kterou bude agent použit,
- údaje umožňující identifikaci agenta.

Na základě nového návrhu, obsahujícího vyhodnocení dosavadní činnosti agenta, lze dobu povolení prodloužit, a to i opakovaně.[890]

887: § 248 odst. 1 písm. e) a odst. 2 až 4 (Porušení předpisů o pravidlech hospodářské soutěže), § 256 (Zjednání výhody při zadání veřejné zakázky, při veřejné soutěži a veřejné dražbě), § 257 (Pletichy při zadání veřejné zakázky a při veřejné soutěži), § 258 (Pletichy při veřejné dražbě, § 329 (Zneužití pravomoci úřední osoby), § 331 (Přijetí úplatku), § 332 (Podplácení), § 333 (Nepřímé úplatkářství) TZK.

888: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní*. 6. vyd. Praha: Wolters Kluwer, 2015, s. 358

889: § 158e odst. 2 TŘ

890: § 158e odst. 4 TŘ

V případě kyberkriminality je možné si představit situace, kdy bude agent použit například k odhalení trestné činnosti související se zneužíváním dětí k výrobě pornografie (např. k infiltraci těchto skupin v rámci Darknetu), v rámci odhalování útoků spáchaných ve prospěch organizované skupiny aj.

## 6.5 Znalec

Znalec je subjektem trestního řízení a je zpravidla přibrán za účelem objasnění konkrétní skutečnosti důležité pro trestní řízení, jejíž objasnění takových odborných znalostí vyžaduje (např. v oboru lékařství, písma, stavebnictví, ekonomie, účetnictví, chemie, techniky a technologie).[891]

Znalecká a tlumočnická činnost se řídí zákonem č. 36/1967 Sb., o znalcích a tlumočnících[892] a vyhláškou ministerstva spravedlnosti č. 37/1967 Sb., o provedení zákona o znalcích a tlumočnících.

Zákon o znalcích a tlumočnících také stanoví, že znaleckou činnost mohou vykonávat i znalecké ústavy – právnické osoby nebo jejich organizační složky, které jsou specializovány na znaleckou činnost a jsou zapsány do seznamu znaleckých ústavů (do seznamu znaleckých ústavů se zapisují vysoké školy nebo jejich součásti a veřejné výzkumné instituce, případně jiné osoby veřejného práva nebo jejich organizační složky vykonávající vědeckovýzkumnou činnost v příslušném oboru).[893] Na základě § 21 odst. 3 ZoZT mohou znalecké posudky a odborná vyjádření zpracovávat i znalci Policie ČR na Kriminalistickém ústavu Praha nebo na odborech kriminalistických technik a expertíz krajských ředitelstvích Policie ČR.

*„**Znalecký posudek je samostatným důkazním prostředkem, kterým si orgány činné v trestním řízení nebo strany (§ 110a, § 89 odst. 2 a § 12 odst. 6) opatřují od osob nebo orgánů k tomu zvláště odborně způsobilých – znalců odborné skutkové poznatky.** Znalce je třeba přibrat tehdy, jestliže pro **složitost posuzované otázky** není postačující vyžádat odborné vyjádření.“*[894]

V ustanovení § 158 odst. 3 TŘ je uvedeno, že objasnění a prověření skutečností nasvědčujících tomu, že byl spáchán trestný čin, opatřuje policejní orgán potřebné podklady a nezbytná vysvětlení a zajišťuje stopy trestného činu. V rámci toho je oprávněn, zejména vyžadovat odborné vyjádření od příslušných orgánů, a je-li toho pro posouzení věci třeba, též znalecké posudky.

891: Srov. FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 384

892: Dále jen **zákon o znalcích a tlumočnících** či **ZoZT**.

893: Viz § 21 odst. 3 ZoZT

894: FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015, s. 383

Vzhledem ke specifičnosti kyberkriminality a vysokým požadavkům na odborné znalosti je v řadě případů vhodné přibrat znalce k vlastnímu ohledání (viz § 113 a násl. TŘ), a případně také ke zkoumání počítačového systému a nosiče informací či dat v těchto systémech uložených.

Znalec se v případech kyberkriminality může **ohledání místa** účastnit de facto ze dvou důvodů:

1) **Účast znalce při ohledání na místě činu v roli konzultanta**
   Vzhledem k odborným znalostem a zkušenostem by v případech kyberkriminality měl být znalec přítomen při zajišťování počítačových systémů, a to buď v pozici konzultanta, nebo subjektu, který tyto systémy sám zajišťuje. Vzhledem ke specifikům uvedeným v kap. 6.4.3 Domovní prohlídka a 6.4.4 Prohlídka jiných prostor a pozemků je jeho přítomnost mnohdy nezbytná. Neodborné zajišťování ICT by mohlo způsobit zničení digitálních stop a tím zmařit účel prohlídek. Znalec také zpravidla provádí dokumentaci, zda a jakým způsobem jsou počítačové systémy zapojeny do počítačové sítě, případně zjišťuje další relevantní skutečnosti.

2) **Účast znalce z důvodu zajištění počítačových systémů, dat aj.**
   Znalec zpravidla na místě nezajišťuje digitální stopy jako takové, nýbrž zajistí celé počítačové systémy nebo nosiče informací. Pokud není možné zajistit systém celý, dochází zpravidla k vytvoření kopií digitálních dat z ICT na místě činu a identické (bitové) kopie[895] paměťových médií znalcem. Identická kopie se vytváří zpravidla tehdy, pokud by zajištění celého počítačového systému nebo nosičů informací mohlo mít negativní dopad do práv třetích osob, nebo by mohlo dojít k ohrožení chodu společnosti (organizace).

   Obecně existují dva důvody pro vytváření identických kopií nosičů informací:

   1) **Vytvořená kopie digitálních dat je identická s originálem.** Není tedy zasahováno do originálu, který může být v případě jeho zajištění předložen soudu. Pokud není zajištěn originál, pak identická kopie, zajištěná správným způsobem, může originál nahradit, neboť je jeho přesnou kopií.

   2) **Náchylnost digitálních dat ke změně.** V případě práce s daty dochází činností osoby, která tato data zkoumá ke změně dat. Z tohoto důvodu probíhá vlastní zkoumání na kopiích, kde může dojít i k destrukci dat, bez toho, že by byl poškozen originál.

Hlavní část využití znalce v rámci trestního řízení však spočívá v jeho vlastní znalecké činnosti, jejímž výstupem je znalecký posudek. V něm znalec odpovídá na otázky, které mu zadavatel (zpravidla orgán činný v trestním řízení) položil, přičemž mu nepřísluší hodnotit důkazy a také neřeší právní otázky. Znalecký posudek je zpracován zpravidla písemně, nicméně v oblasti

895: Jedná se o kopii paměťového média, která je vytvořena tak, že každý jeden bit je překopírován, aby odpovídal originálu. Kopírována tedy nejsou jen data, ale i volný prostor. Bitová kopie je tak identická s originálem.

kyberkriminality se nelze vyhnout elektronické podobě (k posudku jsou běžně připojena vybraná zajištěná data v elektronické podobě na nosičích informací - paměťových médiích).

Obecně by měl orgán činný v trestním řízení od znalce zpravidla vyžadovat následující úkony:

- **Vytvoření identické kopie nosiče informací** (např. harddisk počítače, přenosná paměťová media aj.)**,**
- **zkopírování dat z počítače,**
- **obnovení všech smazaných dat nosiče informací,**
- **ověření komunikace uživatele ze záznamů uložených v počítačovém systému.**

Níže uvedené otázky je možné modifikovat a upravovat. Uvedené otázky je vhodné konzultovat s přibraným znalcem s ohledem na specifika konkrétního případu (např. zajištěný počítačový systém, šifrování paměťových médií aj.).

Některé typické otázky pokládané znalci při **zkoumání počítačového systému či nosiče informací:**[896]

**Proveďte základní popis a výpis hardwarové konfigurace zkoumaného počítačového systému**

1) Proveďte základní popis a výpis hardwarové konfigurace zkoumaného počítačového systému.

2) Vytvořte identickou kopii předložených nosičů informací na vhodná média a přiložte k výsledku zkoumání (pro následné doplnění zkoumání či možný revizní posudek).

3) Zjistěte a zadokumentujte rozdělení datových médií na partition a jednotlivé (nalezené) stručně popište.

4) Zadokumentujte souborovou strukturu (výpis všech souborů) předložených datových médií, včetně smazaných souborů, které v této struktuře vhodně označte.

5) Proveďte obnovu smazaných dat na předložených datových nosičích informací.

6) Vyhledejte a zadokumentujte na předložených nosičích informací (paměťových médiích) veškeré zaheslované (zašifrované) soubory a pokuste se je dešifrovat (najít klíč), kdy výsledek v přehledném formátu zadokumentujte.

7) Zadokumentujte uživatelské účty počítače a definujte přístupová práva k těmto účtům přiřazená (administrátor počítače, uživatel s omezeným přístupem apod.), určete přístupová hesla k těmto uživatelským účtům.

896: Zdrojem, pro otázky pokládané znalci, byly jednak osobní konzultace se znalci a dále bylo čerpáno i ze zdrojů PČR.

8) Zadokumentujte parametry internetového připojení a zjistěte, jaká nastavení internetového připojení byla používána.

9) Zadokumentujte veškerou nalezenou e-mailovou komunikaci, proveďte export veškerých zpráv.

10) Zadokumentujte historii internetové komunikace (ICQ, Skype aj.) uložené v počítačovém systému, včetně obnovených dat.

11) Zadokumentujte a analyzujte soubory kancelářského balíku Microsoft office a uveďte u nich dostupné informace.

12) V existujících a v obnovených datech proveďte vyhledávání dat s následujícími slovními řetězci: ..XX..., ..XY.., ..YY.. atp.

13) V existujících a v obnovených datech proveďte vyhledávání souborů archivačních programů (7-Zip, ZIP, RAR, ARJ aj.) a proveďte jejich extrakci.

14) Zadokumentujte a analyzujte grafické soubory a uveďte u nich dostupné EXIF informace.

15) Zadokumentujte historii navštívených webových stránek v internetových prohlížečích včetně k tomuto připojených dat.

16) Zpřístupněte výpis včetně náhledů všech souborů a složek v textovém, obrazovém a filmovém formátu (např. s erotickým obsahem v oblasti např. dětské pornografii, sodomie aj.). V případě volby této otázky je nezbytné, aby zadavatel sám při osobní konzultaci na znaleckém pracovišti určil, ze zpřístupněného výpisu, zájmové soubory. Znalci nepřísluší hodnotit, zda jde o pornografii, kde je hranice pornografie a nesmí hodnotit možný věk.

17) Pořiďte výpis veškerého nainstalovaného software a rozlište, zda se jedná o software komerční nebo volně šiřitelný.

18) U komerčního software stanovte vlastníka autorských práv, jeho zastoupení v ČR a cenu licence programu.

19) Z pevného disku zajištěného počítače pořiďte výpis software, digitalizovaného videa a audio souborů, které byly nabízeny volně ke stažení, např. prostřednictvím výměnných sítí.

20) Zjistěte, zda na předložené výpočetní technice (hardwarové vybavení) mohl být spuštěn software ..XX.., ...YY...

21) Zkontrolujte počítačový systém, zda se v něm nenachází škodlivý software, kterým by mohl někdo jiný, mimo uživatele, ovládat počítačový systém a tím získat přístupové kódy k platební kartě, které měl poškozený uvedené v počítači v některém z textových souborů.

22) Vyjádřete se k zabezpečení počítačového systému ohledně možného průniku z vnějšku. Popište, jestli zajištěný počítačový systém jevil stopy po takovémto proniknutí, jaké mohly mít následky, či s jakým cílem bylo do tohoto systému proniknuto.

23) Uveďte další skutečnosti mající vztah k vyšetřovanému případu, pokud je považujete za potřebné v posudku uvést.

# 7 Náměty de lege ferenda

# 7 Náměty de lege ferenda

V této monografii jsem prezentoval svoje názory, podněty a připomínky zejména k problematice kybernetické kriminality a působnosti práva ve vztahu k ní. Předkládány byly některé náměty de lege ferenda, jejichž cílem bylo zejména zpřesnit úpravu trestněprávní ochrany před kyberkriminalitou. V této kapitole budou uvedené návrhy sumarizovány a doplněny o náměty nové, dosud neuvedené.

Kapitola náměty de lege ferenda bude rozdělena do dvou subkapitol, z nichž první se věnuje otázkám trestněprávní ochrany před kyberkriminalitou a druhá trestněprocesním prostředkům sloužícím k odhalování, prověřování a vyšetřování tohoto fenoménu.

**Východiskem pro úspěšný boj s kyberkriminalitou je ratifikace Úmluvy o kyberkriminalitě do právního řádu dané země**. Smyslem Úmluvy o kyberkriminalitě je zavedení společných minimálních standardů v oblasti hmotněprávní (výčet relevantních trestných činů), procesněprávní (doporučení pro procesní postup při odhalování, prověřování a vyšetřování kyberkriminality) a v oblasti mezinárodní spolupráce při boji s kyberkriminalitou. V České republice došlo k implementaci hmotněprávní části Úmluvy o kyberkriminalitě kodifikací trestního práva hmotného v podobě trestního zákoníku (viz zejména trestné činy dle § 230–232 TZK, s účinností od 1. 1. 2010). Do současnosti však nedošlo k výraznějším změnám (rekodifikaci) v oblasti trestního práva procesního, které by v sobě promítaly instituty zakotvené v Úmluvě o kyberkriminalitě. Tato absence procesněprávních institutů značně ztěžuje zajišťování a předávání dat, která souvisejí s kybernetickou trestnou činností.

## 7.1 Trestní právo hmotné

Z hlediska trestního práva hmotného by dle mého názoru bylo především vhodné v trestním zákoníku sjednotit obecně užívanou terminologii. Jde především o duplicitní užívání dvou pojmů: **počítač** a **počítačový systém**. Uvedené pojmy byly definovány v kap. 1.2.3 Počítač (Počítačový systém) a z těchto definic vyplývá, že pojem počítačový systém je pojmem širším a zahrnuje v sobě i pojem počítač. Z tohoto důvodu **by bylo vhodné sjednotit terminologii užívanou trestním zákoníkem tak, aby byl jednotně používán pouze pojem počítačový systém**.[897]

### 7.1.1 Místní působnost trestního zákoníku

Problematika určení místní působnosti byla v práci uvedena zejména v kap. 2 Působnost práva v kyberprostoru a 2.2.1 Prostředky trestního práva hmotného. Určení místní příslušnosti, ve vztahu

897: **Pojem počítač** je např. v § 120, § 230 odst. 2 písm. d), § 264 odst. 2, § 267 odst. 2 al. 2 TZK.

ke kyberkriminalitě, je v praxi často řešenou otázkou. Domnívám se proto, že by bylo vhodné upravit § 4 odst. 1 TZK a vložit do něj alineu č. 2, která by stanovila:

***„Podle zákona České republiky se posuzuje i trestnost činu, který byl spáchán v prostředí počítačových sítí."***

Uvedenými dalšími podmínkami by bylo buď naplnění dikce zákona uvedená v § 4 odst. 2 a 3, či § 7 odst. 2 TZK.

### 7.1.2 Trestněprávní ochrana před neoprávněným přístupem k počítačovému systému

Dosud trestněprávně neřešenou otázkou je získání přístupu k nezabezpečenému počítačovému systému nebo jeho části. Byť je takové protiprávní jednání pachateli umožněno neopatrným jednáním uživatele počítačového systému, nic to nemění na faktu, že pachatel získal přístup k počítačovému systému nebo jeho části bez svolení oprávněné osoby. Uvedeným jednáním pachatel nepřekoná bezpečnostní opatření, proto nelze využít § 230 odst. 1 TZK. Na tuto problematiku je však třeba pohlížet i v souladu s ustanoveními **Listiny** (kdy je v **čl. 10** zaručena ochrana soukromí), a proto se domnívám, že by bylo vhodné včlenit do § 230 novou základní skutkovou podstatu, která by postihovala úmyslné neoprávněné získání přístupu k počítačovému systému nebo jeho části, bez ohledu na překonání, či nepřekonání bezpečnostního opatření.[898]

***„Kdo neoprávněně získá přístup k počítačovému systému, nebo jeho části…"***

### 7.1.3 Ochrana dětí před kybergroomingem

Úprava uvedená v § 193b TZK chránící děti před groomingem či kybergroomingem je nedostačující, neboť se zaměřuje pouze na ochranu dětí mladších patnácti let. Jsem přesvědčen o tom, že výše uvedeným jednáním jsou stejnou měrou ohroženy jak děti mladší patnácti let, tak děti mladší osmnácti let. I díky tomu, že § 193b odkazuje na § 192 a 193 TZK, ve kterých je chráněno dítě (tedy osoba mladší 18 let), by bylo mnohem koncepčnější a vhodnější rozšířit ochranu poskytovanou tímto ustanovením i na děti mladší osmnácti let. Vlastní ustanovení § 193b TZK by pak mohlo znít:

*„Kdo navrhne setkání **dítěti** v úmyslu spáchat trestný čin podle § 187 odst. 1, § 192, 193, § 202 odst. 2 nebo jiný sexuálně motivovaný trestný čin, bude potrestán odnětím svobody až na dvě léta."*

898: Úmluva o kyberkriminalitě v čl. 2 umožňuje postihovat i takovýto druh jednání.

### 7.1.4 Trestněprávní ochrana před DoS a DDoS útoky

Současná trestněprávní úprava nemá vhodný nástroj pro postih útoků typu DoS a DDoS, neboť v mnoha případech z technického hlediska při těchto útocích **nedochází k získání přístupu k počítačovému systému** nebo jeho části, nebo to alespoň není primárním cílem.[899] Právě získání přístupu je však určujícím kritériem § 230 odst. 2 TZK. Využití analogie *in malam partem* není možné.

Z výše uvedených důvodů jsem přesvědčen o nutnosti včlenění do právní úpravy ČR samostatné skutkové podstaty trestného činu, která by chránila počítačový systém právě před útoky DoS, DDoS aj. a která by zejména respektovala čl. 4 Úmluvy o kyberkriminalitě. Domnívám se, že by bylo vhodné doplnit § 230 TZK o novou základní skutkovou, která by chránila počítačový systém právě před těmito útoky. Bylo by možné užít např. následující znění:

***„Kdo bez oprávnění brání užívání počítačového systému…"***

### 7.1.5 Botnet

Botnet je jedním z nejúčinnějších prostředků pro páchání de facto jakéhokoliv druhu kyberkriminality. Jsem toho názoru, že je třeba efektivněji chránit uživatele právě před zneužíváním jejich počítačových systémů v rámci sítě Botnet. Byť je možné pachatele, který zapojí počítačový systém do sítě Botnet (typicky díky instalaci malware na tento počítačový systém), stíhat pro trestný čin dle § 230 odst. 2 písm. d) TZK, tak se domnívám, že tímto ustanovením není dostatečně zohledněna nebezpečnost jednání útočníka.

Vlastní ochrana před uvedeným protiprávním jednáním může mít dvě roviny. V první rovině jde o zvýšení ochrany majetkových práv tím, že dojde k doplnění § 207 TZK o základní skutkovou podstatu, jejíž znění by mohlo být následovné: ***„Kdo bez souhlasu oprávněné osoby užije počítačový systém."***

Tímto ustanovením by byla vymezena i okolnost, která spočívá v zásahu do majetkového práva jiného. V případě neoprávněného užívání cizí věci ve vztahu k počítačovému systému není řešením snížení škody z nikoli malé na nikoli nepatrnou (viz § 207 odst. 1 al. 1 TZK), neboť cena řady počítačových systémů je v současnosti nižší i než hodnota nikoli nepatrná (tedy nejméně 5 000 Kč) a přesto jsou tyto počítačové systémy schopny zcela plnit zadanou činnost v rámci sítě botnet.

899: Blíže viz kap. 4.12 DoS, DDoS, DRDoS útoky.

Druhá rovina, která vystihuje závažnost jednání útočníka, pak spočívá ve včlenění nové kvalifikační okolnosti do § 230 odst. 3 TZK, přičemž tato okolnost by mohla znít následovně:

***„připojí počítačový systém do počítačové sítě s úmyslem spáchat trestný čin, či jej v této síti se stejným úmyslem užije,"***

### 7.1.6 Sankce a trestnost přípravy

Povaha a závažnost některých kybernetických útoků není trestním zákoníkem nijak zohledněna. K postihu řady kybernetických útoků jsou primárně využívána ustanovení, která odráží jejich povahu ve světě reálném.

Ne vždy je však ve vztahu ke kyberkriminalitě možné využít prostředků trestního práva hmotného. V mnoha případech kyberkriminality absentuje možnost potrestat útočníka za přípravu k některým kybernetickým trestným činům. Vhodným příkladem pro demonstrování tohoto stavu jsou phishingové útoky. V jejich případě je argumentace, že jednání útočníka, který si zatím pouze obstarává informace nezbytné pro provedení kybernetického útoku, může být postihnuto dle přípravy (§ 20 TZK) k podvodu (§ 209 TZK) či za podvod samotný (při odčerpání hotovosti), částečně chybná. Pokud dojde k finančnímu obohacení pachatele, je bezesporu možné použít ustanovení o trestném činu podvodu, stejně jako je možné užít § 234 (Neoprávněné opatření, padělání a pozměnění platebního prostředku) TZK. Pokud bychom však řešili trestnost přípravy k tomuto trestnému činu, nebude činnost phishera trestná, neboť příprava bude trestná pouze za zvlášť závažný zločin, kterým podvod v základní skutkové podstatě není. Pokud tedy phisher bude pouze získávat „citlivá data" a nijak jich nevyužije, respektive nebude mít úmysl spáchat zvlášť závažný zločin dle § 209 odst. 5 TZK, nebude trestně odpovědný. Phisherovu činnost nebude v mnoha případech možné postihnout ani podle § 230 a 231 TZK, neboť získané informace budou zadávány samotnými uživateli na jeho vlastních internetových stránkách.

Obdobná situace může nastat i v případě jiných kybernetických trestných činů, kde bude vlastní útok rozdělen do několika fází, přičemž první z nich bude spočívat ve vlastní přípravě (shromažďování dat a informací) útoku vlastního.

Zásadní rozdíl mezi světem virtuálním a reálným spočívá především v možnosti vytvoření relativně jednoduchého kybernetického útoku, který může mít i značný (mnohdy i celosvětový) dopad. Právě ona možnost cílení útoku na téměř neomezený počet potenciálních obětí, navíc v relativně krátké době, s relativně velkou úspěšností a možností velmi rychlé změny (flexibility) jednotlivých útoků činí některé projevy kyberkriminality značně nebezpečné. Domnívám se proto, že koncepčně vhodným řešením by byla **změna** (navýšení) **sankcí v případě § 230 TZK** tak, aby tyto sankce více odpovídaly povaze a závažnosti činu, a aby byla příprava k tomuto trestnému činu trestná (viz § 20 odst. 1 a § 14 odst. 3 TZK). Navýšení sankcí pak koresponduje například

s § 233 či 234 TZK. Činnost kyberútočníka může být svým rozsahem či závažností srovnatelná s těmito ustanoveními.

Vlastní § 230 TZK po případných změnách (včetně zohlednění DoS a DDoS útoků, činnosti spojené s Botnet aj.) by mohlo například znít:

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

*1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.*

***2) Kdo úmyslným protiprávním jednáním bez oprávnění brání užívání počítačového systému, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.***

*3) Kdo získá přístup k počítačovému systému nebo k nosiči informací a*

*a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,*

*b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,*

*c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo*

*d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,*

*bude potrestán odnětím svobody **jeden rok až pět let**, zákazem činnosti nebo propadnutím věci.*

*4) Odnětím svobody na **tři léta až osm let**, zákazem činnosti nebo propadnutím věci bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2*

*a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch,*

*b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat, **nebo***

***c) úmyslně připojí počítačový systém do počítačové sítě s úmyslem spáchat trestný čin, či jej v této síti se stejným úmyslem užije.***

*5) Odnětím svobody na **pět až deset let** nebo peněžitým trestem bude pachatel potrestán,*

*a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,*

*b) způsobí-li takovým činem značnou škodu,*

*c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,*

*d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo*

*e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.*

*6) Odnětím svobody na **osm až dvanáct let** bude pachatel potrestán,*

***a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny působící ve více státech,***

*b) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo*

*c) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.*

***7) Příprava je trestná.***

### 7.1.7 Rozšíření oznamovací povinnosti

V současnosti se oznamovací povinnost vztahuje pouze na některé trestné činy, které jsou páchány v kyberprostoru. Domnívám se, že by bylo vhodné rozšířit ustanovení **§ 368** (**Neoznámení trestného činu**) o další trestné činy, u kterých by měla osoba povinnost je oznámit, pokud se o nich hodnověrně dozví. Navrhoval bych rozšíření minimálně o trestné činy **§ 192** (Výroba a jiné nakládání s dětskou pornografií), **§ 193b** (Navazování nedovolených kontaktů s dítětem), **§ 209** (Podvod) TZK.

### 7.1.8 Doplnění kvalifikačních okolností

Dalším z mých námětů de lege ferenda je doplnění některých kvalifikovaných skutkových podstat o okolnosti zvláště přitěžující: **spáchá-li čin veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.** Toto rozšíření u vybraných skutkových podstat by lépe postihovalo jednání pachatele. Jednalo by se o **§ 209** (Podvod), **§ 213** (Provozování nepoctivých her a sázek), **§ 252** (Neoprávněné provozování loterie a podobné sázkové hry), **§ 255** (Zneužití

informace a postavení v obchodním styku), **§ 311** (Teroristický útok), **§ 353** (Nebezpečné vyhrožování) a **§ 357** (Šíření poplašné zprávy).

## 7.2 Trestní právo procesní

V rámci sjednocování mezinárodní a národní právní úpravy by bylo vhodné implementovat do českého trestního práva instituty uvedené v kapitole třetí Úmluvy o kyberkriminalitě, které by umožňovaly rychlé zajištění a využití počítačových dat (viz čl. 16–21). Úmluva o kyberkriminalitě bezprostředně zavazuje státy k přijetí opatření, s cílem efektivního využití počítačových dat k odhalení a usvědčení pachatele. Za tímto účelem stanoví přijetí následujících procesních opatření:[900]

1) urychlené uchování uložených počítačových dat (**čl. 16** Úmluvy o kyberkriminalitě),
2) urychlené zachování a urychlené částečné zpřístupnění provozních dat (**čl. 17** Úmluvy o kyberkriminalitě),[901]
3) příkaz k předložení dat (**čl. 18** Úmluvy o kyberkriminalitě),
4) prohlídka a zajištění uložených počítačových dat (**čl. 19** Úmluvy o kyberkriminalitě),
5) shromažďování provozních dat v reálném čase (**čl. 20** Úmluvy o kyberkriminalitě),[902]
6) odposlech obsahových dat (**čl. 21** Úmluvy o kyberkriminalitě).[903]

### 7.2.1 Urychlené uchování uložených počítačových dat

Dle čl. 16 odst. 1 Úmluvy o kyberkriminalitě je každá strana povinna přijmout „*legislativní a jiná opatření, která budou nezbytná k tomu,* ***aby umožnila svým příslušným orgánům přikázat anebo obdobně zajistit urychlené uchování specifických počítačových dat, včetně provozních dat****, které byly uloženy prostřednictvím počítačového systému, zejména pokud existují důvody pro přesvědčení, že tato počítačová data jsou zvláště ohrožená ztrátou nebo pozměněním.*“

Ustanovení čl. 16 odst. 2 Úmluvy o kyberkriminalitě uvádí, že „*v případech, kdy strana uplatňuje ustanovení výše uvedeného odstavce 1 pomocí* ***příkazu určité osobě, aby zachovala specifikovaná uložená počítačová data v držení této osoby nebo pod její kontrolou****, tato strana přijme taková legislativní a jiná opatření, která mohou být nezbytná pro* ***uložení povinnosti této osobě, aby zachovala a udržovala neporušenost takových počítačových dat po nezbytné období, nejvýše po 90 dnů, aby***

900: Blíže viz GŘIVNA, Tomáš a Radim POLČÁK, (eds.). *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 123

901: V případě urychleného zachování dat je možné využít § 8 TŘ. Ve vztahu k poskytnutí provozních dat je v ČR možné využít § 88a či 88 TŘ.

902: Příkaz k zajišťování a shromažďování provozních dat v reálném čase je součástí § 88a TŘ.

903: Odposlech obsahových dat je v ČR možné realizovat na základě § 88 TŘ.

***mohly příslušné orgány požádat o jejich zpřístupnění. Strana může umožnit následné obnovení takového příkazu.“***

K žádosti o urychlené uchování uložených počítačových dat je v ČR možné využít § 8 TŘ. Smyslem takovéhoto úkonu je zachovat data v nezměněné podobě a zabránit jejich případnému poškození či zničení. Vlastní zálohu dat, provozních a lokalizačních údajů či jiných informací provádí dožadovaný subjekt svými prostředky, přičemž data či jiné informace jsou stále v jeho dispozici a k předání orgánům činným v trestním řízení dochází až na základě využití jiných zákonných zmocnění.

Pokud by chtěl zákonodárce zcela respektovat požadavky vyplývající z čl. 16 Úmluvy o kyberkriminalitě, bylo by třeba ustanovení § 8 TŘ doplnit a zejména vymezit dobu, po kterou mají být počítačová data uchována po doručení příkazu.

### 7.2.2 Příkaz k předložení, prohlídka a zajištění uložených počítačových dat

Data je třeba považovat za věc (viz kap. 2.4.2 Věci a virtuální majetek) a z tohoto důvodu je v případě jejich zajištění možné uplatnit instituty uvedené v § 78 či 79 (vydání či odnětí věci), případě v § 158d odst. 3 (sledování osob a věcí) TŘ. Tato ustanovení umožňují orgánům činným v trestním řízení získat data, která se nacházejí v počítačovém systému nebo na nosiči informací.

Byť je uvedená ustanovení možné uplatnit, nekorespondují zcela s čl. 18 a 19 Úmluvy o kyberkriminalitě a zejména nevystihují reálně možné situace, kdy orgány činné v trestním řízení vyžadují od různých subjektů předložení či vydání dat. Bylo by proto vhodné modifikovat § 78 a 79 (vydání či odnětí věci) TŘ tak, aby bylo zřejmé, že dochází k zajištění věci v podobě dat.[904] Vlastní ustanovení by pak například mohla znít:

*§ 78*
*Povinnost k předložení nebo vydání věci*

*(1) Kdo má u sebe věc, která může sloužit pro důkazní účely, je povinen ji na vyzvání předložit soudu, státnímu zástupci nebo policejnímu orgánu; je-li ji nutno pro účely náležitého zjištění skutečností důležitých pro trestní řízení zajistit, je povinen takovou věc na vyzvání těmto orgánům vydat. Při vyzvání je třeba ho upozornit na to, že nevyhoví-li výzvě, může mu být věc odňata, jakož i na jiné následky nevyhovění (§ 66). Vyzvat k předložení nebo vydání věci je oprávněn předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán.*

904: Děkuji Mgr. Lence Trešlové a Mgr. Michalu Píšovi za jejich komentáře, připomínky a úpravy předloženého námětu Prohlídky a vydání dat. Mgr. Lence Trešlové dále děkuji za poskytnuté materiály vztahující se k zajištění věcí.

*(2) Povinnost podle odstavce 1 se nevztahuje na listinu nebo na jiný hmotný nosič obsahující obrazový, zvukový nebo datový záznam, jejichž obsah se týká okolnosti, o které platí zákaz výslechu, ledaže došlo k zproštění povinnosti zachovat věc v tajnosti nebo k zproštění povinnosti mlčenlivosti.*

*(3) Nikoho nelze nutit, aby vydal věc, jež v době, kdy je požádáno o její předložení nebo vydání, může sloužit jako důkaz proti němu nebo proti jeho osobě blízké; tím nejsou dotčena ustanovení o odnětí věci, domovní prohlídce, prohlídce jiných prostor a pozemků a osobní prohlídce.*

*(4) Je-li to potřebné pro účely zabránění zmaření propadnutí nebo zabrání věci, orgán činný v trestním řízení uvedený v odstavci 1 vydá příkaz, že osoba, jíž byla věc zajištěna, nesmí po dobu zajištění takovou věc převést na jinou osobu nebo ji zatížit. Právní jednání učiněné v rozporu s tímto zákazem je neplatné; soud k neplatnosti přihlédne i bez návrhu. O tom je třeba tuto osobu poučit.*

*(5) Osobě, která předložila nebo vydala věc, jež může sloužit pro důkazní účely, vydá orgán, který úkon provedl, ihned písemné potvrzení o převzetí věci nebo opis protokolu; věc v nich musí být dostatečně přesně popsána, tak, aby bylo možné určit její totožnost.*

*(6) Orgán činný v trestním řízení, kterému byla vydána věc, jež může sloužit pro důkazní účely, ji převezme do úschovy.*

*(7) Osoba, které byla věc zajištěna, má právo kdykoli žádat o vrácení takové věci. O takové žádosti musí orgán činný v trestním řízení uvedený v odstavci 1 neodkladně rozhodnout. Byla-li žádost zamítnuta, může ji tato osoba, neuvede-li v ní nové důvody, opakovat až po uplynutí 30 dnů od právní moci rozhodnutí.*

***(8) Jsou-li věcí uvedenou v odstavci 1 data, která jsou uložena v počítačovém systému nebo na nosiči informací, může být ten, kdo je má u sebe, vyzván k umožnění pořízení si jejich kopie nebo poskytnutí jiné potřebné součinnosti k jejich zpřístupnění; odstavce 1 až 3 a 6 se použijí přiměřeně**.*

*§ 79*
*Odnětí věci*

*(1) Nebyla-li věc, která může sloužit pro důkazní účely, na vyzvání vydána tím, kdo ji má u sebe, může mu být na příkaz předsedy senátu a v přípravném řízení na příkaz státního zástupce nebo policejního orgánu odňata. Policejní orgán potřebuje k vydání takového příkazu předchozí souhlas státního zástupce; bez předchozího souhlasu může být příkaz policejním orgánem vydán jen tehdy, jestliže nelze předchozího souhlasu dosáhnout a věc nesnese odkladu.*

*(2) Nevykoná-li orgán, který příkaz k odnětí věci vydal, odnětí věci sám, provede je na podkladě příkazu policejní orgán.*

*(3) K odnětí věci se podle možnosti přibere osoba, která není na věci zúčastněna.*

*(4) Na odňatou věc se obdobně použije § 78 odst. 4 až 7**; jsou-li takovou věcí data, která jsou uložena v počítačovém systému nebo na nosiči informací, použije se obdobně § 78 odst. 2 a 6**.*

Druhou možností je vytvoření samostatného ustanovení, které by se vztahovalo pouze na zajišťování počítačových dat. Domnívám se však, že takovéto speciální ustanovení je nadbytečné, neboť je možné využít instituty obecné (viz výše). Mimo jiné by toto speciální ustanovení i neúměrně zatížilo orgány činných v trestním řízení, neboť na každý zajišťovaný počítačový systém by bylo třeba vydat příkaz. Pro úplnost a představu čtenáře však uvádím i možné znění tohoto ustanovení:

***Prohlídka a vydání počítačových dat***

***(1) Je-li toho třeba k objasnění skutečností důležitých pro trestní řízení, je předseda senátu a v přípravném řízení soudce na návrh státního zástupce oprávněn nařídit osobě, která drží nebo má pod svojí kontrolou data uložená v počítačovém systému nebo na nosiči informací, anebo poskytovateli služeb informační společnosti, aby***

***a) umožnili orgánům činným v trestním řízení provést prohlídku takových dat,***

***b) umožnili orgánům činným v trestním řízení vytvoření kopie takových dat,***

***c) znemožnili přístup k takovým datům jiným osobám,***

***d) vydali taková data, včetně provozních a lokalizačních údajů vztahujících se k těmto datům.***

***(2) Povinnost podle odstavce 1 se nevztahuje na data, jejichž obsah se týká okolnosti, o které platí zákaz výslechu, ledaže došlo ke zproštění povinnosti zachovat věc v tajnosti nebo ke zproštění povinnosti mlčenlivosti.***

***(3) Nikoho nelze nutit, aby vydal data, jež v době, kdy je požádáno o jejich vydání, mohou sloužit jako důkaz proti němu nebo proti jeho osobě blízké; tím nejsou dotčena ustanovení o prohlídce takových dat a vytvoření si jejich kopie a o odnětí věci.***

***(4) V příkazu podle odstavce 1 písm. c) musí být uvedena doba, po kterou má být znemožněn přístup k datům; tato doba nesmí být delší než 90 dní. Tato doba může být novým příkazem prodloužena nejdéle o 90 dní, a to i opakovaně. Příkaz musí obsahovat poučení o následcích neuposlechnutí příkazu (§ 66, 79).***

***(5) Nesplní-li ten, vůči němuž příkaz uvedený v odstavci 1 směřuje, povinnost uloženou v příkazu, aniž by byly splněny důvody uvedené v odstavcích 2 a 3, postupuje se obdobně podle § 79.***

### 7.2.3 Digitální důkaz

Dalším námětem de lege ferenda je zavedení pojmu digitální důkaz (blíže viz kap. 6.3.1.3 Digitální důkazy). Vlastní ustanovení definující digitální důkaz by bylo možné zařadit do § 112 odst. 3 TŘ např. v následujícím znění:

***Digitálním důkazem jsou jakákoli data či informace, jež byly přeneseny, vytvořeny, uloženy či modifikovány za použití počítačového systému a které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu.***

### 7.2.4 Virtuální (krypto) měna

*„Je to pro mě šok, vůbec netuším, co to je, a pokud vím, tak nikdo bitcoinem neplatí. Ta měna nemá nějakou dobrou pověst. To bude asi nějaký omyl, fakt to není v pořádku."*
Andrej Babiš (Český rozhlas, 22. 1. 2015)

V kyberprostoru jsou ve stále větší míře realizovány transakce za pomoci různých virtuálních měn. Nejznámější z nich je Bitcoin, avšak není měnou jedinou.[905] Virtuální měna, byť je technicky používána jako platidlo, není z hlediska práva za měnu či elektronické peníze zpravidla uznána.[906] Dle českého trestního práva je virtuální měnu možné považovat za věc, zřejmě za věc nehmotnou, ve vztahu k níž má uživatel dispoziční právo. Bylo by tedy možné užít institutu § 79e TŘ.

905: Viz např. *Crypto-Currency Market Capitalizations.* [online]. [cit. 1. 9. 2016]. Dostupné z: https://coinmarketcap.com/

906: Viz například neuznání Bitcoinů za elektronické peníze. Blíže viz *Electronic Money Directive (2009/110/ES; EMD).* [online]. [cit. 1. 9. 2016]. Dostupné z: http://ec.europa.eu/finance/payments/emoney/index_en.htm; http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32009L0110&from=en
*Směna tradičních měn za jednotky virtuální měny „bitcoin" je osvobozena od DPH.* [online]. [cit. 1. 9. 2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128cs.pdf
Opačný přístup je možné nalézt např v některých státech USA:
V srpnu roku 2013 označil texaský federální soud bitcoin za měnu, jež by měla podléhat shodné regulaci jako například dolar [SEC v. Shavers, Case No. 4:13-CV-416 (E.D.Tex) ze dne 6.8.2013]
SOMMEROVÁ, Klára a Klára SETVÁKOVÁ. *Právní a daňové souvislosti kryptoměn.* [online]. [cit. 1. 9. 2016]. Dostupné z: https://prezi.com/7kprkksznutn/untitled-prezi/
Dále viz SOMMEROVÁ, Klára. *Kryptoměny v praxi. Výzva pro právní regulaci.* [online]. [cit. 1. 9. 2016]. Dostupné z: http://www.epravo.cz/top/clanky/kryptomeny-v-praxi-vyzva-pro-pravni-regulaci-96942.html

Otázkou ovšem je, zda by vhodnějším řešením nebylo uznat virtuální měnu jako platidlo, neboť tuto funkci již dávno plní, a v tom případě ji zajišťovat na základě specifického ustanovení, které by ve vztahu ke krypto měnám muselo být vytvořeno. Užití § 79a (Zajištění peněžních prostředků na účtu u banky) TŘ není ve vztahu ke kryptoměnám možné využít, neboť jednou z klíčových vlastností těchto platidel je jejich decentralizovanost.

Náměty obsažené v této kapitole jsou zaměřeny primárně na oblast trestního práva, nicméně využití pouze prostředků trestního práva pro řešení fenoménu kyberkriminality není účinné. Jsem přesvědčen o tom, že je třeba hledat možná východiska daného problému například ve větším zapojení organizací a samotných uživatelů do procesu budování bezpečnosti, ve zvyšování obecného podvědomí a vzdělanosti v oblasti fungování informačních a komunikačních technologií včetně upozornění na možná rizika či hrozby.

# Závěr

*„Nestačí vědět, vědění se musí použít.“*
Johan Wolfgang von Goethe

## Závěr

Jsem pevně přesvědčen o tom, že kyberprostor se nesmí stát prostředím, kde by bylo možné beztrestně páchat jakoukoliv trestnou činnost. Na druhou stranu je třeba nastavit pravidla a podmínky tak, aby se nestal ani prostředím, v němž bude převládat cenzura a represe. Vyvážení těchto dvou rovin je klíčovým předpokladem pro uplatňování a zejména respektování pravidel v kyberprostoru, ať již legálních, či morálních.

Cílem této monografie nebylo do detailu popsat veškeré aspekty, které mohou souviset s kyberkriminalitou, ale měla čtenáři především osvětlit dílčí, mnohdy ne zcela vnímané souvislosti mezi informačními a komunikačními technologiemi, právem a bezpečností. Zároveň měla ukázat možnosti trestněprávního postihu některých protiprávních aktivit online, včetně možnosti odhalování a vyšetřování této kriminality.

V rámci naplnění tohoto cíle došlo nejdříve k popsání základních pojmů, které s danou problematikou bezprostředně souvisejí a které jsou v dalších částech monografie využívány. Samostatná pozornost pak byla věnována obecné otázce působnosti práva v kyberprostoru a možnosti odpovědnosti nejen uživatele, ale i poskytovatele služeb informační společnosti. Domnívám se, že současná právní úprava ČR dostatečně odráží zejména právní dokumenty Rady Evropy a Evropské unie, avšak jako nedostatek lze spatřovat nedostatečnou informovanost subjektů o možnosti právní odpovědnosti poskytovatele služeb informační společnosti za určité úkony, či za jejich neučinění.

Pro běžného uživatele jsou dle mého názoru stěžejní především kapitoly 3 a 4. Kapitola 3 je věnována problematice anonymity uživatele, digitálním stopám a projektům, které jsme se studenty Policejní akademie ČR realizovali a jejichž cílem bylo demonstrovat, jak relativně jednoduché je dostat se za použití sociálního inženýrství k uživatelům sociálních sítí.

Jak jsem již uvedl v úvodu: uvědomuji si, že moje svoboda, včetně jisté míry „anonymity" na Internetu, je v současnosti utopií. Uživatelé by měli poznat a zejména porozumět tomu, jaké digitální stopy svojí interakcí v kyberprostoru zanechávají, neboť toto poznání jim poskytne právo volby ve vztahu k ICT a službám poskytovaným online.

Kapitola 4 pak popisuje jednotlivé kybernetické útoky, přičemž tyto útoky jsou demonstrovány na případech z praxe a pokud je to možné, je u těchto skutků uvedena i jejich případná trestněprávní kvalifikace.

Světlo do možností trestněprávního postihu kyberkriminality de lege lata měla také vnést kapitola č. 5, jejíž přínos lze spatřovat zejména v klasifikaci forem kyberkriminality a dále v subsumpci jednotlivých zločinů definovaných Úmluvou o kyberkriminalitě pod ustanovení trestního zákoníku, včetně uvedení námětů de lege ferenda. Domnívám se, že de lege ferenda by mělo dojít k **ujednocení právních pojmů a legislativy** související s touto kriminalitou, zejména

ve všech zemích Evropské unie tak, aby ji bylo možné postihnout obdobným způsobem. Takovýto koncept by mohl být základem pro úspěšný boj s kyberkriminalitou, která je nejspecifičtější právě neomezeností a nevázaností na konkrétní teritorium.

Pokud jde o aplikaci případných trestněprávních norem na určité druhy kybernetických útoků, je třeba uvést, že není možné stíhat prostředky trestního práva sebenebezpečnější jednání, které není zakotveno v rámci trestních kodexů té které země. Trestní právo je prostředkem *ultima ratio* a jako takové musí být značně precizní, aby nezasahovalo do práv a svobod osob ve větší míře, než je nezbytně nutné.

Kapitola 6 měla čtenáři přiblížit možnosti (zákonné instituty), kterými disponují orgány činné v trestním řízení při prověřování, odhalování a vyšetřování kyberkriminality. Domnívám se, že je nezbytně nutné poskytnout orgánům činným v trestním řízení legální a dostatečně efektivní prostředky, umožňující jim zamezit protiprávnímu jednání pachatele kyberkriminality, včetně zajištění důkazů o této činnosti. V rámci některých úkonů trestního řízení je zasahováno do práv a oprávněných zájmů fyzických a právnických osob. Tento zásah je možný pouze na základě zákona a v jeho mezích. Není rozhodující, jak přísně budou nastavena pravidla pro to, aby se orgán činný v trestním řízení mohl dostat k datům důležitým pro toto řízení, podstatné je, že bude mít na základě zákona možnost takový úkon učinit a tak naplnit zásadu legality spočívající v povinnosti stíhat všechny trestné činy, o nichž se dozví.

Vedle státu se ochranou kyberprostoru a jeho uživatelů zabývají různé soukromé organizace. Domnívám se, že pokud chceme účinně s kyberkriminalitou bojovat, mělo by dojít k efektivnější spolupráci soukromých organizací (zejména IT odborníků, CSIRT týmů aj.) se složkami veřejné (státní) správy, či s orgány činnými v trestním řízení tak, aby bylo možné včas a adekvátně reagovat na stále sofistikovanější formy kyberkriminality či kyber útoků.

Jak jsem uvedl v úvodu: ***„Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný.“***

Mým názorem je, že **nemá smysl se oprošťovat od ICT a služeb, které jsou s těmito technologiemi spojené. Účelem této monografie nebylo donutit uživatele odinstalovat si Facebook a nepoužívat Google či jiné služby. Smyslem bylo upozornit na možná rizika spojená s užíváním informačních a komunikačních technologií a služeb s nimi spojených.** V této souvislosti je třeba připomenout citát *Scientia est potentia* (**vědění je moc, v poznání a znalostech je síla, vědění je síla**). V případě ICT a služeb s nimi spojených je třeba poznat, co tyto technologie a služby představují, co činí a k čemu slouží.

Redukce negativních jevů v kyberprostoru a snaha o změnu tak nutně musí začít u koncových uživatelů, neboť v kyberprostoru jsou to právě oni, kdo je typickou první obětí útočníka. Zároveň jsou uživatelé autoritou, která může definovat, jaké služby, data či informace budou v kyberprostoru vyhledávány, ukládány a poskytovány.

Věřím, že výchova a vzdělávání uživatelů má být nezbytnou součástí prostupu informačních a komunikačních technologií do našich životů. Budování informační gramotnosti by mělo být neodmyslitelně spojeno s tvorbou, distribucí a podporou produktů, či služeb, které jsou s informačními a komunikačními technologiemi spojeny. Vlastní vzdělávání v této oblasti, či spíše seznamování se s možnými hrozbami, riziky a negativy IT, by mělo být součástí výuky všech forem studia na všech úrovních školství.

*„Nikdo nedělá větší chybu než ten, kdo nedělá nic v domnění, že to málo, co udělat může, nemá smysl.“*
Edmund Burke

# Seznam použitých pramenů a dalších zdrojů

## Seznam použitých pramenů a dalších zdrojů

*"AirHopper" Malware Uses Radio Signals to Steal Data from Isolated Computers.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.securityweek.com/airhopper-malware-uses-radio-signals-steal-data-isolated-computers

*"Flat Fee Music" & The MUSIC LIKE WATER MANIFESTO.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.futuristgerd.com/2006/01/15/flat-fee-music/

„*Souhlasím s VOP? Odkliknu a jedu…* " [online]. [cit. 10. 7. 2016]. Dostupné z: https://konferencesecurity.cz/

*10 Most Expensive Virtual Items Ever Sold.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.youtube.com/watch?v=VUNRl3kAATk

*10 Most notorious hackers od all time.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://hacked.com/hackers/

*10 Most Notorious Hacking Groups.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.hackread.com/10-most-notorious-hacking-groups/

*10 of the Most Expensive Virtual Items In Video Games.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.therichest.com/rich-list/most-popular/10-of-the-most-expensive-virtual-items-in--video-games/

*11 Most Expensive Virtual Items in Video Games.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.insidermonkey.com/blog/11-most-expensive-virtual-items-in-video-games-377679/2/

*1986 - Hackerův manifest.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://blisty.cz/art/14662.html Originální znění je možné nalézt Phrack.org. [online]. [cit.16.8.2015]. Dostupné z: http://phrack.org/issues/7/3.html

*7 Types of Hackers You Should Know.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://www.cybrary.it/0p3n/types-of-hackers/

*Addresses and Names* [online]. [cit. 9. 7. 2016]. Dostupné z: http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_addresses

*Advanced Persistant Threat – life cycle.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

*Advanced Persistant Threat (APT).* [online]. [cit. 20. 8. 2016]. Dostupné z: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

*Advanced Persistant Threat.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.isouvislosti.cz/advanced-persistent-threat

*Advanced Persistent Threats: How They Work.* [online]. [cit. 10. 7. 2016]. Dostupné z: https://www.symantec.com/theme.jsp?themeid=apt-infographic-1

*Adware.* [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking

AMPRATWUM, Edward Fokuoh. Advanced Fee Fraud "419" and Investor Confidence in the Economies of Sub-Sahara Africa (SSA). *Journal of Financial Crime*, 2009, roč. 16, č. 1, s. 66–79 ISSN 1359-0790

*Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení.* [online]. [cit. 2. 10. 2008]. Dostupné z: http://www.mvcr.cz/dokument/2006/informacni.doc

*Android Ransomware now targerts your Smart TV, Too!* [online]. [cit. 14. 8. 2016]. Dostupné z: https://thehackernews.com/2016/06/smart-tv-ransomware.html

*Android SMS worm Selfmite returns, more aggressive than ever.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html

*Android version market share distribution among smartphone owners as of May 2016.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

*Android Worm on Chinese Valentine's day.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/

ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit. 10. 6. 2016]. Dostupné z: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

*Augmented reality.* [online]. [cit. 10. 7. 2016]. Dostupné z: http://www.oxforddictionaries.com/definition/english/augmented-reality

BALIGA, Arati, Liviu IFTODE a Xiaoxin CHEN. Automated Containment of Rootkits Attacks. *Computers & Security*, 2008, roč. 27, č. 7–8, s. 323–334.

BARLOW, Perry, John. *A Declaration of the Independence of Cyberspace.* [online]. [cit. 23. 9. 2014]. Dostupné z: https://www.eff.org/cyberspace-independence .
Český zdroj: http://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru

BAUDIŠ, Pavel. Programy typu rootkit. Další hrozba pro Windows. *CHIP*, 2005, č. 7, s. 14

*Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.hackread.com/fake-android-prisma-app-phishing-malware/

BHATTACHARYYA Dhruba Kumar a Jugal Kumar KALITA. *DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance.* Chapman and Hall/CRC 2016. ISBN 978-1-4987-2965-9.

*Botnet – Historical List of Botnets.* [online]. [cit. 15. 8. 2016]. Dostupné z: http://www.liquisearch.com/botnet/historical_list_of_botnets

*Botnet.* [cit. 8. 7. 2016]. Dostupné z: http://research.omicsgroup.org/index.php/Botnet

*Botnet.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://en.wikipedia.org/wiki/Botnet

*Botnets.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6

*Botnety: nová internetová hrozba.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.lupa.cz/clanky/botnety-internetova-hrozba/

*Bots and Botnets – A growing Threat.* [online]. [cit. 11. 8. 2016]. Dostupné z: https://us.norton.com/botnet/

BOUŠKA, Petr. *OSI model.* [online]. [cit. 8. 7. 2016]. Dostupné z: http://www.samuraj-cz.com/clanek/osi-model/

*Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani--nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cit. 10. 4. 2015]. Dostupné z: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

CARL, Glenn, Richard BROOKS a Rai SURESH. Wavelet Based Denial-of-Service Detection. C*omputers & Security*, 2006, roč. 25, č. 8, s. 600–615

CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004. ISBN 0-12-163104-4.

*Central processing unit* [online]. [cit. 4. 4. 2016]. Dostupné z: https://www.oxforddictionaries.com/definition/english/central-processing-unit

*Cloud Computing Begins to Gain Traction on Wall Street* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.wallstreetandtech.com/it-infrastructure/212700913

*CNN on pedophile sex in Second Life.* [online]. [cit. 18. 6. 2009]. Dostupné z: http://www.youtube.com/watch?v=AQM-SiiaipE

*Co je pharming?* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.kaspersky.com/cz/internet-security-center/definitions/pharming

*Co je pirátství.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.stoppiratstvi.cz/cs/o-piratstvi/co-je-piratstvi.shtml ; či http://www.filmynejsouzadarmo.cz/cs/o-piratstvi/

*Co je to botnet a jak se šíří?* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.youtube.com/watch?v=ywXqDon5Xtg

*Co je to kyberšikana a jak se projevuje?* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

*Co znamená přípona souboru SCR.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.solvusoft.com/cs/file-extensions/file-extension-scr/

*Combating Cybercrime in a Digital Age.* [online]. [cit. 7. 5. 2016]. Dostupné z: https://www.europol.europa.eu/ec3

*Computer* [online]. [cit. 7. 5. 2016]. Dostupné z: http://www.oxforddictionaries.com/definition/english/computer

*Computer system.* Překlad autora. [online]. [cit. 16. 2. 2010]. Dostupné z: http://www.its.bldrdoc.gov/fs-1037/dir-008/_1198.htm

*Computer-generated 'Sweetie' catches online predators.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.bbc.com/news/uk-24818769

*Computer Trespass Law and Legal Definition*. [online]. [cit. 16. 7. 2016]. Dostupné z: https://definitions.uslegal.com/c/computer-trespass/

*Convicted spammer challenging Va. law* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

*Crypto-Currency Market Capitalizations.* [online]. [cit. 1. 9. 2016]. Dostupné z: https://coinmarketcap.com/

*Current World Population.* [online]. [cit. 10. 8. 2015]. Dostupné z: http://www.worldometers.info/world-population/

*Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism--How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html

*Cybercrime*. [online]. [cit. 1. 2. 2015]. Dostupné z: http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime

ČERNÁ, Monika a Michal ČERNÝ. *Úvod do problematiky sociálních sítí*. [online]. [cit. 12. 5. 2015]. Dostupné z: http://clanky.rvp.cz/clanek/o/g/15075/UVOD-DO-PROBLEMATIKY-SOCIALNICH-SITI.html/

ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit. 9. 8. 2015]. Dostupné z: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

*Čo sa skrýva v prílohe podvodných e-mailov?* [online]. [cit. 15. 8. 2016]. Dostupné z: https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/

*Data retention unconstitutional in its present form.* [online]. [cit. 16. 7. 2016]. Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

*Delokalizace právních vztahů na internetu* [online]. [cit. 15. 4. 2012]. Dostupné z: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html

*Digital Attack Map –Top daily DDoS attack worldwide.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.digitalattackmap.com/

*Digital Evidence & Legal Definition.* [online]. [cit. 20. 2. 2014]. Dostupné z: http://definitions.uslegal.com/d/digital-evidence/

*Digital, Social & Mobile Worldwide in 2015.* [online]. [cit. 9. 8. 2015]. Dostupné z: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015

*Distribuované výpočty.* [online]. [cit. 2. 11. 2013]. Dostupné z: http://dc.czechnationalteam.cz/

*Disturbing ISIS video shows militants beheading four prisoners and gunman executing shoppers at market.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017

DOČEKAL, Daniel. Bruce Schneier: *Internet věcí přinese útoky, které si neumíme představit.* [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/

DOČEKAL, Daniel. *Google: Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele.* [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.lupa.cz/clanky/google-adware--napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/

DOČEKAL, Daniel. *Největší sociální sítě na světě? Facebook je sice jednička, ale….* [online]. [cit. 20. 8. 2015]. Dostupné z: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

DOČEKAL, Daniel. *Studie: Filmové pirátství nepoškozuje Hollywood, může mu i prospět.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.lupa.cz/clanky/studie-filmove-piratstvi-neposkozuje-hollywood-muze-mu-i-prospet/

DODGE, Ronald. C., Curtis CARVE a Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, roč. 26, č. 1, s. 73–80.

*Does Microsoft call about computer being infected with virus?* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.computerhope.com/issues/ch001385.htm

*Dvanáctiletá dívka se zabila po téměř roční šikaně na internetu.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer--rocni-sikane-na-internetu.html; http://www.ceskatelevize.cz/ct24/svet/246314-dalsi-sebe-vrazda-kvuli-socialnim-sitim-divka-skocila-z-veze/

EDELSON, Eve. The 419 Scam: Information Warfare on the Spam Front and a Proposal for Local Filtering. *Computers & Security*, 2003, roč. 22, č. 5, s. 392–401 ISSN 0167-4048

*Electronic Money Directive (2009/110/ES; EMD)*. [online]. [cit. 1. 9. 2016]. Dostupné z: http://ec.europa.eu/finance/payments/emoney/index_en.htm; http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32009L0110&from=en

ELIÁŠ, Karel. *Věc, jako pojem soukromého práva.* [online]. [cit. 6. 6. 2016]. Dostupné z: http://www.pavelpetr.cz/soubory/29/87/Karel_Elias_Vec_jako_pojem_soukromeho_prava.pdf

ENGLEHARDT, Steven a Ardvin NARAYANAN. *Online tracking: A 1-million-site measurement and analysis.* [online]. [cit. 5. 8. 2016]. Dostupné z: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

*ESC radí, jak poznat podvody na internetu.* [online]. [cit. 30. 8. 2016]. Dostupné z: http://www.evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu-27250

*Estonia recovers from massive DDoS attack.* [online]. [cit. 4. 3. 2015] Dostupné z: http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

*Evoluční teorie v podání spear phishingu.* [online]. [cit. 15. 2. 2010]. Dostupné z: http://connect.zive.cz/content/evolucni-teorie-v-podani-spear-phishingu

*Evropská úmluva o ochraně lidských práv.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

*Exclusive: Computer Virus Hits U.S. Drone Fleet.* [online]. [cit. 10. 7. 2016]. Dostupné z: https://www.wired.com/2011/10/virus-hits-drone-fleet/

*Facebook will soon be able to ID you in any photo.* [online]. [cit. 9. 8. 2015]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

*FBI Exploits Flash Vulnerability to Breach Tor Network Security.* [online]. [cit. 23. 7. 2016]. Dostupné z: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/

FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní.* 6. vyd. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-750-8.

FIALOVÁ, Eva. Krádež virtuálních předmětů v příkladech nizozemské judikatury. *Revue pro právo a technologie*, 2010, roč. 1, č. 1. [online]. [cit. 15. 7. 2016]. Dostupné z: https://journals.muni.cz/revue/article/view/3980/pdf

*Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy.* [online]. [cit. 10. 7. 2016]. Dostupné z: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

*First Amendment.* [online]. [cit. 10. 7. 2016]. Dostupné z: https://www.law.cornell.edu/constitution/first_amendment

*Flappy Bird Clones Help Mobile Malware Rates Soar.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx

*FLocker Mobile Ransomware Crosses to Smart TV.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/

*France drops controversial 'Hadopi law' after spending millions.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy

FRANCESCHI-BICCHIERAI, Lorenzo. *The Silk Road Online Drug Marketplace by the Numbers.* [online]. [cit. 16. 6. 2016]. Dostupné z: http://mashable.com/2013/10/04/silk-road-by-the-numbers/#9USbF1JntiqU

*Francie zakáže internetové pirátství.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.blisty.cz/2009/5/13/art46807.html

*Free DDoS Service! Max 5 min!* [online]. [cit. 19. 8. 2016]. Dostupné z: http://hackforums.net/showthread.php?tid=3065539

*Fridge caught sending spam emails in botnet attack.* [online]. [cit. 17. 5. 2016]. Dostupné z: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

*German Bundestag Passes New Data Retention Law.* [online]. [cit. 16. 7. 2016]. Dostupné z: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes--new-data-retention-law/

*German Federal Constitutional Court rejects data retention law.* [online]. [cit. 16. 7. 2016]. Dostupné z: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/

GONZÁLES-TALAVÁN, Guillermo. A Simple, Configurable SMTP Anti-spam Filter: Greylists. *Computers & Security*, 2006, roč. 25, č. 3, s. 229–236. ISSN 0167-4048

GOODMAN, Marc. *A vision of crimes in the future.* [online]. [cit. 13. 11. 2014]. Dostupné z: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

*Google odhalil technologické vnitřnosti: provozuje více než 100 tisíc serverů.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.svobodnymonitor.cz/byznys/google-odhalil-technologicke-vnitrnosti-provozuje-vice-nez-100-tisic-serveru/

*Google says the best phishing scams have a 45-percent success rate.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/

GREENBERG, Andy. *Hackers remotely koll a Jeep on the highwaty – with me in it.* [online]. [cit. 4. 5. 2016]. Dostupné z: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. V české verzi dostupné např. na: http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani--auta-f1l-/automoto.aspx?c=A150723_135910_automoto_fdv

GRIFFITHS, Mark. Computer Crime and Hacking: a Serious Issue for the Police? *The Police Journal,* 2000, roč. 73, č. 1, s. 18–24.

GŘIVNA, Tomáš a Radim POLČÁK (eds.) *Kyberkriminalita a právo.* Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

GŘIVNA, Tomáš, Miroslav SHEINOST, Ivana ZOUBKOVÁ a kol. *Kriminologie.* 4. vyd. Praha: Eolters Kluwer, 2014. ISBN 978-80-7478-614-3.

GUZMAN, Andrew. PAUWELYN, Joost H. B. *International Trade Law*. Aspen Publishers, 2012. ISBN 978-1-4548-0539-7.

*Hackeři se vydávají za Anonymous a hrozí útokem českým firmám.* [online]. [cit.16.8.2015]. Dostupné z: http://www.lupa.cz/clanky/hackeri-vydavajici-se-za-anonymous-hrozi-utokem--na-ceske-firmy-chteji-zaplatit/

*Hackeři ukradli Američanům data o novém typu bojových stíhaček.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://digiweb.ihned.cz/c1-36816420-hackeri-ukradli-americanum-data-o-novem-typu-bojovych-stihacek

*Hackeři vám už brzy ukradnou data přímo z klávesnice*. [online]. [cit. 16. 8. 2015]. Dostupné z: http://digiweb.ihned.cz/c1-29295240-hackeri-vam-brzy-ukradnou-data-primo-z-klavesnice

*Hackeři zaútočili na uživatele Facebooku*. [online]. [cit. 16. 8. 2015]. Dostupné z: http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla

HAINES, Lester. *Online gamer stabbed over „stolen" cybersword.* [online]. [cit. 3. 10. 2006]. Dostupné z: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

HASMAN, Simon a Ray HUNT. A Taxonomy of Network and Computer Attacks. *Computers & Security*, 2005, roč. 24, č. 1, s. 32–43

HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* 1. Vyd. Praha: Computer Press, 1997. ISBN 80-7226-023-5.

HILL, Kashmir. *These two Diablo III players stole virtual armor and gold — and got prosecuted IRL*. [online]. [cit. 10. 8. 2015]. Dostupné z: http://fusion.net/story/137157/two-diablo-iii-players--now-have-criminal-records-for-stealing-virtual-items-from-other-players/

*Historical list of botnets.* [online]. [cit. 15. 8. 2016]. Dostupné z: http://jpdias.me/botnet-lab//history/historical-list-of-botnets.html

*Historical Maps of Computer Networks*. [online]. [cit. 10. 7. 2016]. Dostupné z: https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

*HOIC.* [online]. [cit. 18. 8. 2016]. Dostupné z: https://npercoco.typepad.com/.a/6a0133f264aa62970b0167612ea130970b-pi

HOLT, Thomas, Adam BOSSLER a Kathryn SEIGFRIED-SPELLAR. *Cybercrime and digital forensics: an introduction.* First published. London: Routledge, 2015. ISBN 978-1-138-0229-7.

HOŘEJŠÍ, Jaromír. *Falešný exekuční příkaz ohrožuje uživatele českých bank.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/

*How do APTs work? The Lifecycle of Advanced Persistent Threats (Infographic).* [online]. [cit. 10. 7. 2016]. Dostupné z: https://blogs.sophos.com/2014/04/11/how-do-apts-work-the-lifecycle-of-advanced-persistent-threats-infographic/

*How to leak sensitive data from an isolated computer (air-gap) to a near by mobile phone – AirHopper.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.youtube.com/watch?v=2OzTWiGl1rM

*How to use Wireshark to capture, Filter and inspect Packets.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

HRUBEŠOVÁ, Helena. „*Proč si neregistrovat doménové jméno pod doménou nejvyššího stupně „.com" aneb jak je to s jurisdikcí amerických soudů*". [cit. 25. 9. 2010]. Dostupné na World Wide Web: http://www.itpravo.cz/index.shtml?x=1928185

HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN 978-80-904248-8-3.

CHOO, Kim-Kwang Raymond. *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences* [online]. Canberra: Australian Institute of Criminology, c2009, xi, s. 108 [cit. 19. 3. 2014]. ISBN 978-1-921532-33-7. Dostupné z: http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf

*Interesting Statistics On Mobile Strategies for Digital Transformations.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

*Internet censorship.* [online]. [cit. 10. 8. 2016]. Dostupné z: http://www.deliveringdata.com/2010_10_01_archive.html

*Internet History of 1980s.* [online]. [cit. 7. 6. 2016]. Dostupné z: http://www.computerhistory.org/internethistory/1980s/

*Internet map* [online]. [cit. 4. 7. 2016]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/d/d2/Internet_map_1024.jpg

*Internet of Things (IoT).* [online]. [cit. 15. 7. 2016]. Dostupné z: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

*Internet, připojení k němu a možný rozvoj (Část 2 – Historie a vývoj Internetu).* [online]. [cit. 10. 2. 2008]. Dostupné z: http://www.internetprovsechny.cz/clanek.php?cid=163

*Islamic State Hacking Division.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

*Jedinečný identifikátor zařízení.* [online]. [cit. 14. 6. 2016]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/key-terms/#toc-terms-unique-device-id

JELÍNEK, Jiří a kolektiv: *Trestní zákoník a trestní řád s poznámkami a judikaturou***.** Praha: Leges 2009. ISBN 978-80-87212-22-6.

*Jessica Logan – The rest of the Story.* [cit. 8. 8. 2016]. Dostupné z: http://nobullying.com/jessica-logan/

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-397-0. Dostupné z: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/; https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke--bezpecnosti---druhe-vydani/

JIROVSKÝ, Václav a Oldřich KRULÍK. Základní definice vztahující se k tématu. *Security magazín*, 2007, roč. 14, č. 2. ISSN 1210–8723

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

JIROVSKÝ, Václav. *Kyberterorismus.* ICT fórum/PERSONALIS 2006. [předneseno 27. 9. 2006]. Praha (prezentace na konferenci).

JOHNSON, David R. a David POST. *The Rise of Law in Cyberspace.* [online]. [cit. 10. 7. 2016]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535

*Judge, 69, who downloaded child porn facing 'catastrophic humiliation'.* [online]. [cit. 1. 9. 2009]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

*Junipers' Mobile Threats Report: Mobile malware attacks grew over 600%.* [online]. [cit. 17. 5. 2016]. Dostupné z: http://searchnetworking.techtarget.com/news/2240203163/Junipers-Mobile-Threats-Report-Mobile-malware-attacks-grew-over-600

*K čemu slouží facebookový „like" scam* [online]. [cit. 14. 8. 2016]. Dostupné z: https://blog.nic.cz/2013/08/06/k-cemu-slouzi-facebookovy-like-scam/

KELLY, Grodon. *Report: 97% Of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/#62a95de97d53

*Kevin Mitnick Case: 1999.* [online]. [cit. 2. 11. 2011]. Dostupné z: http://www.encyclopedia.com/doc/1G2-3498200381.html

KNAPP, Viktor. *Teorie práva.* Praha: C. H. Beck, 1999. ISBN 80-7179-028-1.

KOLOUCH, Jan a Andrea KROPÁČOVÁ. Liability for Own Device and Data and Applications Stored therein. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14).* [B.m.], c2014, s. 321–324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1. ISSN 1790-5109.

KOLOUCH, Jan a Andrera KROPÁČOVÁ. Ransomware. In: ZHUANG, Xiaodong. *Recent Advances in Computer Science: Proceedings of the 19th International Conference on Computers*. B.m.: B.n., 2015, s. 304–307. Recent Advances in Computer Engineering Series, [Nr. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109. Dostupné též online: http://www.inase.org/library/2015/zakynthos/bypaper/COMPUTERS/COMPUTERS-49.pdf

KOLOUCH, Jan a Josef SOUČEK. Několik poznámek k specifikům dokazování softwarové kriminality. *Trestní právo,* 2007, roč. 12, č. 12, s. 6–12. ISSN 1211-2860.

KOLOUCH, Jan a Petr VOLEVECKÝ. Trestněprávní aspekty phishingového útoku. *Trestní právo,* 2008. roč. 12, č. 9, s. 5–12. ISSN 1211-2860.

KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN a Terezie JANÍKOVÁ. neBezpečné chování na Facebooku. In: *Sborník příspěvků ke konferenci: Sociální sítě. Mobilní aplikace.* Plzeň: Západočeská univerzita v Plzni, 2014, s. 39–47 ISBN 978-80-261-0362-2.

KOLOUCH, Jan. Cloud Computing: Právní aspekty. In: *Sborník příspěvků ke konferenci: Cloudy a cloudová řešení.* Plzeň: Západočeská univerzita v Plzni, 2013, s. 22-33. ISBN 978-80-261-0254-0.

KOLOUCH, Jan. Procesněprávní aspekty zajištění dat. In: Záhora, J. (ed.): *Aktuálné problémy prípravného konania trestného.* Praha: Leges, 2014, s. 228 – 241 ISBN 978-80-7502-030-7.

KOLOUCH, Jan. Pseudoanonymita – bezpečnostní riziko pro uživatele Internetu. *DSM – data security management*. 2015. Roč. 19, číslo 3, s. 24-29 ISSN 1211-8737.

KOLOUCH, Jan. Trestně právní odpovědnost za DoS, DDoS útoky v ČR. In: *Aktuálne otázky trestního prava v teórii a praxi: Zborník príspevkov zo 4. ročníka interdisciplinárnej celoštátnej vedeckej konferencie s medzinárodnou účasťou.* [online]. Bratislava: Akadémia Policajného zboru v Bratislave [cit. 07. júla 2016], s. 120–129. ISBN 978-80-8054-683-0. Dostupné z: www.akademiapz.sk

KOLOUCH, Jan. Trestněprávní aspekty odhalování, prověřování a vyšetřování internetové trestné činnosti. In: *Integrácia a unifikácia práva Európskej únie v oblasti trestného zákonodárstva: zborník príspevkov z medzinárodnej virtuálnej interdisciplinárnej vedeckej konferencie*. Ed. Jaroslav Klátik. Banská Bystrica: Univerzita Mateja Bela, 2008, s. 84-102. ISBN 978-80-8083-681-8.

KOLOUCH, Jan. Zajišťovací úkony a důkazní prostředky využitelné v rámci boje se softwarovou a internetovou trestnou činností. In: *Predsúdne konanie: zborník príspevkov z celoštátneho seminára s medzinárodnou účasťou*. Bratislava: Akadémia Policajného zboru v Bratislave, 2008, s. 62–76. ISBN 978-80-8054-454-6.

KONRÁD, Zdeněk, Viktor PORADA a Jiří STRAUS. Kriminalistika: kriminalistická taktika a metodiky vyšetřování. Plzeň: 2015, s. 351-352. ISBN 978-80-7380-547-0.

KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. vyd. [cit. 19. 3. 2014]. Dostupné z: http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a

KUCHTA, Josef a kol. *Kurs trestního práva. Trestní právo hmotné. Zvláštní část*. Praha: C. H. Beck, 2009. ISBN 978-80-7400-047-8.

*Kybergrooming.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

*Kybergrooming.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

*Kyberšikana I, II.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy

LANCE, James. *Phishing bez záhad*. Praha: Grada, 2007. ISBN 978-80-247-1766-1.

LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář*. Praha: C. H. Beck, 2014. ISBN 978-80-7400-529-9.

*Leading social networks worldwide as of April 2016, ranked by number of active users (in millions).* [online]. [cit. 20. 8. 2015]. Dostupné z: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

*Legislativní proces z hlediska Poslanecké sněmovny.* [online]. [cit. 18. 8. 2009]. Dostupné z: http://www.pravnik.cz/a/94/legislativni-proces-z-hlediska-poslanecke-snemovny.html

LESSIG, Lawrence. *Code v. 2. str.* 6 Dostupný v plném znění (Angl.) [online]. [cit. 13. 3. 2008]. Dostupné z: http://pdf.codev2.cc/Lessig-Codev2.pdf

LEVY, Steven. *Hackers: Heroes of the Computer Revolution* Sebastopol, CA: O'Reilly edia. ISBN 978-1449388393, s. 32–41. Dostupné i online: https://e11c1b148f6c7c56754c9184e0d1c52ac-4d888f9-www.googledrive.com/host/0ByAMXZl2-PZ0WjBPYmhaWVVRN0E

LI, Tao, GUAN, Zhihong, WU, Xianyong. Modeling and Analyzing the Spread of Active Worms Based on P2P Systems. *Computers & Security*, 2007, roč. 26, č. 3, s. 213–218.

*Likvidace fotografií, dokumentů aneb nový „policejní virus" na scéně.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.viry.cz/likvidace-fotografii-dokumentu-aneb-novy-policejni-virus-na-scene/

*LOIC*. [online]. [cit. 18. 8. 2016]. Dostupné z: https://i.ytimg.com/vi/QAbXGy0HbrY/maxresdefault.jpg

LOUDA, Pavel. *Darknet: Tak vypadá horší stránka internetu.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://computerworld.cz/internet-a-komunikace/darknet-temna-strana-internetu-52610

*Main memory* [online]. [cit. 4. 4. 2016]. Dostupné z: https://www.oxforddictionaries.com/definition/english/main-memory?q=main+memory

*Malware, mayhem, and the McColo takedown.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/

MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO a Pedro GARCÍA-TEODORO. Evaluation of a Low-rate DoS Attack Against Application Servers. *Computers & Security*, 2008, roč. 27, č. 7-8, s. 335–354.

MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6.

Matějka, Michal. *Počítačová kriminalita*. Praha: Computer Press, 2002. ISBN 80-7226-419-2.

MELOY Reid, J. *STALKING (OBSESSIONAL FOLLOWING): A REVIEW OF SOME PRE-LIMINARY STUDIES.* [online]. [cit. 3. 10. 2015]. Dostupné z: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

MINAŘÍK, Pavel. *Wireshark – Paketová analýza pro všechny.* [online]. [cit. 18. 8. 2016]. Dostupné z: https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm

MITNICK, Kevin D. a William L. SIMON. *Ghost in the wires: my adventures as the world's most wanted hacker*. New York: Little, Brown & Co, 2012. ISBN 9780316037723.

MITNICK, Kevin D. a William L. SIMON. *Umění klamu*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

MITNICK, Kevin D. *The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley, c2006. ISBN 0-471-78266-1.

*Mobile Threat Report. What's on the Horizon for 2016.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

MUELLER, Robert. [online]. [cit. 3. 4. 2013]. Dostupné z: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Nález Ústavního soudu ČR č. II. ÚS 502/2000, ze dne 22. 1. 2000. *Právo na ochranu zpráv podávaných telefonem.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=36243&pos=1&cnt=1&typ=result

Nález Ústavního soudu I. ÚS 1428/13 ze dne 20. 8. 2013. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.usoud.cz/fileadmin/user_upload/Tiskova_mluvci/I-1428-13.pdf

Nález Ústavního soudu III. ÚS 287/96 ze dne 22. 5. 1997 k ústavnosti domovní prohlídky. [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=28795&pos=1&cnt=1&typ=result

Nález Ústavního soudu III. ÚS 3812/2012, ze dne 3. 10. 2013. *Ke sledování dat uložených v počítačích v rámci institutu sledování osob a věcí pro účely trestního řízení.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=81007&pos=1&cnt=1&typ=result

Nález Ústavního soudu IV. ÚS 2/02, ze dne 28. 3. 2002 (U 11/25 SbNU 385). *Nařízení a provedení prohlídky jiných prostor. Povinnost mlčenlivosti.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=43001&pos=1&cnt=1&typ=result

Nález Ústavního soudu Pl. ÚS 41/11, ze dne 22. 3. 2011. *Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=4&typ=result

*NAT.* [online]. [cit. 16. 6. 2016]. Dostupné z: https://www.abclinuxu.cz/slovnik/nat

*National legal challenges to the Data Retention Directive.* [online]. [cit. 16. 7. 2016]. Dostupné z: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html

NEJEDLÝ, Jan a Tereza ŠMIGOLOVÁ. *Kyberkriminalita na sociálních sítích.* Praha 2015. Studentská vědecká a odborná činnost, Policejní akademie ČR v Praze, Sekce právní vědy. Vedoucí práce Jan Kolouch.

NEJEDLÝ, Jan. *Dítě, jako cíl kyberpredátora.* Praha 2015. Studentská vědecká a odborná činnost, Policejní akademie ČR v Praze, Sekce právní vědy. Vedoucí práce Jan Kolouch.

*Nejrozšířenější Internetovou hrozbou roku 2009 byl červ Conficker, vede už i v Česku* [online]. [cit. 24. 2. 2010]. Dostupné z: http://digiweb.ihned.cz/pocitace/c1-39858750-nejrozsirenejsi--internetovou-hrozbou-roku-2009-byl-cerv-conficker-vede-uz-i-v-cesku

*Největší hackerský útok potvrzen. V ohrožení jsou stovky miliónů uživatelů.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html

*Největší sociální sítě na světě? Facebook je sice jednička, ale…* [online]. [cit. 10. 8. 2015]. Dostupné z: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

*Nejznámější počítačoví hackeři a jejich útoky.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.stream.cz/top-5/10004402-nejznamejsi-pocitacovi-hackeri-a-jejich-utoky

NELSON, Adrian. *Some questions and answers about Facebook.* [online]. [cit. 16. 7. 2016]. Dostupné z: http://www.rotarydistrict9800.com.au/news/14135/some-questions-and-answers-about-facebook/?no_follow=1

*Network Layers.* [online]. [cit. 8. 7. 2016]. Dostupné z: http://www.comptechdoc.org/independent/networking/protocol/protlayers.html

*Network vulnerabilities and the OSI model.* [online]. [cit. 8. 7. 2016]. Dostupné z: http://cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model/

*Network.* [online]. [cit. 4. 5. 2016]. Dostupné z: https://www.oxforddictionaries.com/definition/english/network

*New Ransomware Encrypts Your Game Files.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/

NIGAM, Ruchna. *A timeline of Mobile Botnets.* [online]. [cit. 12. 7. 2016]. Dostupné z: https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf

*Nikdy nevíš.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.youtube.com/watch?v=O79-0FUeYrk&list=PLQe7s_lKdHIAycTLmN_ojbey-joyldxRh

*Nizozemci vytvořili virtuální dívku. Pomohla lapit přes tisíc pedofilů.* [online]. [cit. 19. 8. 2016]. Dostupné z: http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-/zahranicni.aspx?c=A131106_210025_zahranicni_zt

NOVOTNÝ, František a kolektiv. *Trestní zákoník 2010. Komentář.* Eurounion. Praha 2010. ISBN 978-80-7317-084-4.

NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010. ISBN 978-80-7380-291-2.

NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní.* Plzeň: Aleš Čeněk, 2009. ISBN 978-80-7380-237-0.

NUTIL, Petr. *Darknet, aneb cesta do hlubin internetu* [online]. [cit. 10. 5. 2016]. Dostupné z: http://www.kurzy.cz/zpravy/382630-darknet-aneb-cesta-do-hlubin-internetu/

*OSA chce i poplatek za nové mobily, maximálně 90 korun z každého.* [online]. [cit. 23. 8. 2016]. Dostupné z: http://ekonomika.idnes.cz/osa-chce-penize-i-z-mobilu-maximalne-90-korun-z--kazdeho-p0e-/test.aspx?c=A160819_092317_test_suj

*OWASP, XSS* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

PADRTA, Aleš a Karel NYKLES. *Ransomware – „policejní virus" na pitevním stole.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.root.cz/clanky/ransomware-policejni-virus-na-pitevnim-stole/

PADRTA, Aleš. *Zamyšlení nad aktuálními bezpečnostními problémy.* [online]. [cit. 18. 8. 2016]. Dostupné z: http://www.saferinternet.cz/attachments/article/457/CESNET_aktualni_bezpecnostni_problemy.pdf

*Password Sniffer Spy.* [online]. [cit. 18. 8. 2016]. Dostupné z: http://securityxploded.com/password-sniffer-spy.php

PERRIN, Andrew. *Social Media Usage: 2005-2015* [online]. [cit. 16. 7. 2016]. Dostupné z: http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

PERSIN, Coby. *The Dangerous of Socila Media.* [online]. [cit. 6. 8. 2016]. Dostupné z: https://www.youtube.com/watch?v=6jMhMVEjEQg

PETERKA, Jiří. *Terminologie datových sítí.* [online]. [cit. 10. 11. 2015]. Dostupné z: http://www.earchiv.cz/b00/b0003002.php3

PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10. 11. 2015].
Dostupné z: http://www.earchiv.cz/b14/b0428001.php3

*Phishing Activity Tresnds Report.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

*Phishing by the Numbers: Must-Know Phishing Statistics 2016.* [online]. [cit. 14. 8. 2016].
Dostupné z: https://blog.barkly.com/phishing-statistics-2016

PLETZER, Valentin. Demaskovaný spyware. *CHIP*, 2007, č. 10, s. 116–120.

PLOHMANN, Daniel, Elmar GERHARDS-PADILLA a Felix LEDER. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, 2011. [online]. [cit. 17. 5. 2015]. Dostupné z: https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

*PODVODNÉ EMAILY hrozí exekucí, nic neplaťte a neotvírejte!* [online]. [cit. 15. 8. 2016]. Dostupné z: http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-ne-platte-a-neotvirejte.html

*Podvodníci mění taktiku. Našli novou cestu, jak vybílit lidem účty.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html

*Podvody s falešnými webkamerami řádí i v ČR.* [online]. [cit. 7. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sociotechnika/637-podvody-s-falenymi-webkamerami-

POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kolektiv. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, Právnická fakulta, 2015. ISBN 978-80-210-8073-7.

POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007. ISBN 978-80-251-1777-4.

*Police investigate Habbo Hotel virtual furniture theft.* [online]. [cit. 17. 3. 2013]. Dostupné z: http://www.bbc.com/news/10207486

*Policejní ransomware.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000

*Policie vám může vypnout doménu. Co říká zákon?* [online]. [cit. 24. 8. 2016]. Dostupné z: https://www.root.cz/clanky/policie-vam-muze-vypnout-domenu-co-rika-zakon/

PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

PORADA, Viktor a Jiří STRAUS. *Kriminalistické stopy. Teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, 2012. ISBN 978-80-7380-396-4.

PORADA, Viktor a Petr ŠEDIVÝ. Praktická využitelnost kriminalistických a forenzních aplikací v oblasti počítačové/kybernetické kriminality. *Karlovarská právní revue*, 2012, č. 3, s. 94–114.

PORADA, Viktor a Roman RAK. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství*, XVII., 2006, č. 1, s. 3–21

PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování počítačové kriminality.* Praha: Policejní akademie České republiky, 1998. ISBN 80-85981-75-0.

PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování softwarového pirátství.* Praha: Policejní akademie, 1999. ISBN 80-7251-4024-X.

*Postřehy z bezpečnosti: Ransomware šestkrát jinak.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/

*Pozor na zprávu o údajné neuhrazené pohledávce – jedná se o podvod.* [online]. [cit. 5. 8. 2016]. Dostupné z: https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/

*Pozor na zprávu o výzvě k úhradě před exekucí – jedná se o podvod.* [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.csirt.cz/news/security/?page=87

*POŽÁR, Josef. Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-38-5.

*Pravidla a postupy.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.nic.cz/page/314/pravidla-a-postupy/

*Pravidla registrace doménových jmen v ccTLD .cz.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.nic.cz/files/nic/PravidlaCZod20160515.pdf

*Prohlášení o právech a povinnostech.* [online]. [cit. 6. 8. 2016]. Dostupné z: https://www.facebook.com/legal/terms

*Projekty pro koncové uživatele.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://www.nic.cz/page/2086/

PROSISE, Chris a Kevin MANDIA. *Počítačový útok, detekce, obrana a okamžitá náprava.*, 1. vyd. Praha: Computer Press, 2002. ISBN 80-7226-682-9.

PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville : McGraw-Hill, 2003. ISBN 0-07-222696-X.

PŘIBYL, Tomáš. Seznamte se s rootkity. *PC World*, 2007, č. 9, s. 108–110.

*Přísný zákon proti hudebním a filmovým pirátům Francii nepomohl.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi-/sw_internet.asp?c=A100330_095705_sw_internet_vse

*Rady pro bezpečné používání sociálních sítí* [online]. [cit. 24. 3. 2014]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/rady.aspx

RAK, Roman a Radek KUMMER. Informační hrozby v letech 2007 – 2017. *Security magazín*, 2007, roč. 14, č. 1. ISSN 1210–8723

RAK, Roman a Viktor PORADA. Charakteristiky a specifika digitálních stop. *Bezpečnostní teorie a praxe*, 2005, č. 1, s. 71–84,

*Ransomware.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

REED, Chris. *Internet Law.* Cambridge: Cambridge University Press, 2004. ISBN: 9780521605229.

*Regional internet registries.* [online]. [cit. 4. 8. 2015]. Dostupné z: https://www.nro.net/about-the-nro/regional-internet-registries

*Riziková komunikace: Kybergrooming* [online]. [cit. 19. 3. 2014]. Dostupné z: http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming

Rozhodnutí Nejvyššího soudu 11 Tdo 349/2009, ze dne 21.5.2009. [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/FBA92F6969DDC460C1257A4E00656CA9?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 15 Tdo 510/2013, ze dne 26.6.2013 [online]. [cit. 25. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/592226D3401E2466C1257BAD0044D215?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 4 Tz 265/2000, ze dne 16.1.2001. [online]. [cit. 13. 3. 2008]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 5 Tdo 171/2014, ze dne 8.10.2014. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/675636E6F4A8497FC1257DB6003698A6?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 5 Tdo 234/2009, ze dne 25.3.2009. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/0873CA8A4A362534C1257A4E0066BE88?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 5 Tdo 459/2007, ze dne 3.5.2007 [online]. [cit. 25. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/1056AA7881B123EEC1257A4E0064DE83?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 5 Tdo 631/2003, ze dne 18.6.2003. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/48AEF52C74365354C1257A4E0069A613?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 5do 1312/2010, ze dne 15. 12. 2010. [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/DE1E219419DEA02EC1257A4E006525B9?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu 8 Tdo 137/2013, ze dne 27.2.2013. [online]. [cit. 15. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/763AE1D4853A3985C1257B5C004F46EE?openDocument&Highlight=0

Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30.1.2013. [online]. [cit. 8. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?openDocument&Highlight=0

Rozhodnutí Nejvyššího správního soudu 1 As 90/2008, ze dne 4. 2. 2009. [online]. [cit. 8. 7. 2016]. Dostupné z: http://nssoud.cz/files/SOUDNI_VYKON/2008/0090_1As__0800189A_prevedeno.pdf

Rozsudek Soudního dvora (čtvrtého senátu) ze dne 10.4.2014. ACI Adam BV a další proti Stichting de Thuiskopie a Stichting Onderhandelingen Thuiskopie vergoeding. [online]. [cit. 15. 7. 2016]. Dostupné z: http://curia.europa.eu/juris/liste.jsf?num=C-435/12; http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5419c26a-a775041c0a292b59941c66783.e34KaxiLc3eQc40LaxqMbN4Pa3mMe0?text=&doci-d=150786&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=203878

Rozsudek soudního dvora (velkého senátu) EU C-131/12, ze dne 13.5.2014. [online]. [cit. 24. 3. 2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf;jsessio-nid=9ea7d2dc30d59c3214d6fafa4d6cae2ede058bf9fcdb.e34KaxiLc3qMb40Rch0SaxuNb3z0?-text=&docid=152065&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&-cid=272305

Rozsudek ze dne 30. května 2007: *Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593.* [online]. [cit. 1. 6. 2016]. Dostupné z: https://h2o.law.harvard.edu/cases/4435

RYAN, Thomas. *Getting In Bed with Robin Sage.* [online]. [cit. 5. 9. 2013]. Dostupné z: http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting--In-Bed-With-Robin-Sage-v1.0.pdf

*Second Life 'child abuse' claim.* [online]. [cit. 16. 6. 2009]. Dostupné z: http://news.bbc.co.uk/2/hi/technology/6638331.stm

*Security authorization. An Approach for Community Cloud Computing Environments* [online]. [cit. 15. 4. 2012]. Dostupné z: www.federalnewsradio.com/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

*Sex Predator Uses Xbox Live to Victimize 10-Year-Old.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.escapistmagazine.com/news/view/103121-Sex-Predator-Uses-Xbox-Live-to-Victi-mize-10-Year-Old

Sexting.cz – *vše, co chcete vědět o sextingu* [online]. [cit. 18. 3. 2014]. Dostupné z: www.sexting.cz

SHNEIER, Bruce. *The Seven Types of Hackers.* [online]. [cit. 16. 8. 2015]. Dostupné z: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

SCHNEIER, Bruce. *Crime: The Internet's Next Big Thing.* [online]. [cit. 6. 11. 2007]. Dostupné z: https://www.schneier.com/crypto-gram/archives/2002/1215.html

SCHNEIER, Bruce. *The Internet of Things Will Turn Large-Scale Hacks into a Real World Disasters.* [online]. [cit. 10. 8. 2016]. Dostupné z: https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis. *Computers & Security*, 2007, roč. 26, č. 5, s. 361–372. ISSN 0167-4048.

*Six teens arrested for virtual crime in Habbo Hotel.* [online]. [cit. 17. 3. 2013]. Dostupné z: http://www.technologytell.com/gaming/18923/six-teens-arrested-for-virtual-crime-in-habbo-hotel/

*Sledování zásilky České pošty aneb nová havěť.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/

SLÍŽEK, David. *Evropský soud ve sporu s Googlem: vyhledávače musí na požádání měnit minulost.* [online]. [cit. 4. 11. 2015]. Dostupné z: http://www.lupa.cz/clanky/evropsky-soud-ve-sporu-s-googlem-vyhledavace-musi-na-pozadani-menit-minulost/

*Slovníkový útok.* [online]. [cit. 30. 8. 2016]. Dostupné z: https://managementmania.com/cs/slovnikovy-utok

SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo.* Praha: C. H. Beck, 1995. ISBN 80-7179-009-5.

SMEJKAL, Vladimír. *Internet a $$$.* 2. aktualiz. a rozš. vyd. Praha: Grada, 2001. ISBN 80-247-0058-1.

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

SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. aktualiz. a rozš. vyd. Praha: C. H. Beck, 2004. ISBN 80-247-0058-1.

*Směna tradičních měn za jednotky virtuální měny „bitcoin" je osvobozena od DPH.* [online]. [cit. 1. 9. 2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128cs.pdf

SMITH, Craig. *By the Numbers: 100 Amazing Google Search Statistics and Facts.* [online]. [cit. 4. 8. 2016]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/

*Smluvní podmínky společnosti Google.* [online]. [cit. 14. 6. 2016]. Dostupné z: https://www.google.cz/intl/cs/policies/terms/regional.html

SOMMEROVÁ, Klára a Klára SETVÁKOVÁ. *Právní a daňové souvislosti kryptoměn.* [online]. [cit. 1. 9. 2016]. Dostupné z: https://prezi.com/7kprkksznutn/untitled-prezi/

SOMMEROVÁ, Klára. *Kryptoměny v praxi. Výzva pro právní regulaci.* [online]. [cit. 1. 9. 2016]. Dostupné z: http://www.epravo.cz/top/clanky/kryptomeny-v-praxi-vyzva-pro-pravni-regulaci-96942.html

Soudní dvůr Evropské unie. Tisková zpráva č. 54/14, ze dne 8. 4. 2014. Rozsudek ve spojených věcech C-293/12 a C-594/12. [online]. [cit. 15. 7. 2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

*Spam Statistics and Facts.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.spamlaws.com/spam-stats.html

*Spam statistics*. [online]. [cit. 14. 8. 2016]. Dostupné z: https://www.spamcop.net/spamstats.shtml

SPITZER, Manfred. *Digitátlní demence.* Brno: Host, 2014. ISBN 978-80-7294-872-7.

*Spyware.* [cit. 8. 1. 2008]. Dostupné na World Wide Web: http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9

Stanovisko Generálního advokáta Pedra Cruz Villalóna. Věc C-293/12 a C-594/12. [online]. [cit. 15. 7. 2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

Stanovisko Generálního advokáta SAUGMANDSGAARD ØE, ze dne 19. 7. 2016. Ve spojených věcech C-203/15 a C-698/15. [online]. [cit. 10. 8. 2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

stanovisko Nejvyššího státního zastupitelství 1 SL 760/2014. *Stanovisko ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek, ze dne 26. 1. 2015.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://www.nsz.cz/images/stories/PDF/Stanoviska_Proces/2015/1_SL_760-2014.pdf

STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006. ISBN 80-86898-66-0.

STRAUS, Jiří. *Úvod do kriminalistiky.* 3. vyd. Plzeň: Aleš Čeněk, 2012. ISBN 978-80-7380-367-4.

*Stuxnet.* [online]. [cit. 23. 7. 2016]. Dostupné z:https://cs.wikipedia.org/wiki/Stuxnet

SUCHÁNEK, Jaroslav a kol. *Kriminalistická problematika při odhalování, vyšetřování a prevenci softwarového pirátství – sborník odborných sdělení ze semináře uskutečněného na PA ČR dne 26. 1. 1999.* Praha: PA ČR, 1999. ISBN-80-85981-50-5.

SUCHÁNEK, Jsroslav a kol. *Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality – sborník odborných sdělení ze semináře uskutečněného na PA ČR dne 23. 12. 1996.* Praha: PA ČR, 1997. ISBN-80-85981-50-5.

*Surface Web, Deep Web, Dark Web – What's the Difference.* [online]. [cit. 20. 7. 2016]. Dostupné z: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

SVETLÍK, Marian. Počítače a kriminalita. In: *Sborník odborných sdělení ze semináře uskutečněného na Policejní akademii dne 26. 1. 1999*. Praha: Policení akademie 1999, s. 93–97

SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23.9.2014)

ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář.* 2. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7400-428-5.

ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. vyd. Praha: C. H. Beck, 2012. ISBN 974-80-7400-4285

ŠÁMAL, Pavel a kol.: *Trestní řád I. § 1 až 156. Komentář*. 7. vydání. Praha: C. H. Beck, 2013. ISBN 978-80-7400-465-0

*Škodlivý kód cílí na mobily, šíří se jako lavina*. [online]. [cit. 17. 5. 2016]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html

ŠTOČEK, Milan. *V Hitlerově duchu proti Hitlerovi.* [online]. [cit. 10. 7. 2016]. Dostupné z: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

ŠTUDENTOVÁ, Milada. Trestněprávní aspekty související se zasíláním e-mailů a zveřejňováním materiálů na webových stránkách. *Trestní právo*, 2007, roč. 13. č 7–8, s. 27–33. ISSN 1211-2860

ŠEJNOHA, Josef. *Systém kriminalistického vzdělání (Psychologie zločinu a zločinnosti).* Praha: F. Kodym, 1936.

*Targeted cyberattacks logbook.* [online]. [cit. 10. 7. 2016]. Dostupné z: https://apt.securelist.com/#secondPage

TAYLOR, Harriet. *How the „Internet of Things" could be fatal.* [online]. [cit. 17. 6. 2016]. Dostupné z: http://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html

*TCP handshake krok za krokem.* [online]. [cit. 18. 8. 2016]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000

*The „Deep Web" is Not All Dark.* [online]. [cit. 12. 5. 2016]. Dostupné z: http://www.deepwebtech.com/deepweb-not-darkweb/

*The dark Web explained.* [online]. [cit. 20. 7. 2016]. Dostupné z: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html

*The fragmentation of Android has new records: 24 000 different devices.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

*The Malware Museum @ Internet Archive*. [online]. [cit. 17. 5. 2016]. Dostupné z: https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/

The OSI Model's Seven Layers Defined and Functions Explained. [online]. [cit. 8. 7. 2016]. Dostupné z: *https://sarvesict.blogspot.cz/2015/11/the-osi-models-seven-layers-defined-and.html* .

*The testimony of an ex-hacker.* [online]. [cit. 26. 9. 2008]. Dostupné z: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

*The very first mobile malware: how Kaspersky Lab discovered Cabir.* [online]. [cit. 1. 8. 2016]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

THOMAS, Douglas. *Criminality on the Electronic Frontier. In Cybercrime.* London: Routledge, 2003. s. 17 a násl.

*Tip of the month July 2016 – Avoid getting hooked by Phishing*. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/

Tomáš HLAVÁČEK. *Analýza: Zranitelnost „ROM-0" postihuje 1,5 milionu domácích routerů.* [online]. [cit. 20. 12. 2015]. Dostupné z: http://www.root.cz/clanky/analyza-zranitelnost-rom-0-postihuje-1-5-milionu-domacich-routeru/

*Top Spammer Sentenced to Nearly Four Years.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.pcworld.com/article/148780/spam.html

*Tor security advisory: "relay early" traffic confirmation attack.* [online]. [cit. 23. 7. 2016]. Dostupné z: https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

*Types of Hacker Motivations.* [online]. [cit. 6. 8. 2015]. Dostupné z: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/

*Types of Malware.* [online]. [cit. 17. 5. 2016]. Dostupné z: http://www.kaspersky.com/internet-security-center/threats/types-of-malware

U. S. Attorney's Office. *Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court.* [online]. [cit. 18. 6. 2016]. Dostupné z: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court

*Uhraďte dluhy, toto je exekuční příkaz. Komora varuje před další vlnou podvodných e-mailů* [online]. [cit.15. 8. 2016]. Dostupné z: http://zpravy.aktualne.cz/finance/falesne-exekuce-jsou-zpet-komora-varuje-pred-dalsi-vlnou-pod/r~cbdac6de765111e599c80025900fea04/

*Úmluva o kyberkriminalitě.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERM-PublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

*United Nations Manual on the prevention and control of computer-related crime.* [online]. [cit. 20. 8. 2016]. Dostupné z: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

UNUCHEK, Roman a Victor, CHEBYSHEV. *Mobile malware evolution 2015.* [online]. [cit. 14. 8. 2016]. Dostupné z: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/

*Války síťových robotů– jak fungují sítě botnets.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://tmp.testnet-8.net/docs/h9_botnet.pdf

*Vejce dražší než vaše auto. Deset luxusních virtuálních předmětů.* [online]. [cit. 15. 7. 2016]. Dostupné z: http://bonusweb.idnes.cz/nejdrazsi-virtualni-predmety-dko-/Magazin.aspx?c=A150930_082546_bw-magazin_anb

VIKTORYOVÁ, Jana, BANGO, Dezider a kol. *Vyšetřování vybraných druhů trestných činů.* Bratislava: Akadémia policajného zboru, 2007. ISBN 978-80-8054-416-4.

VIKTORYOVÁ, Jana, Ján PALAREC, Jaroslav BLATNICKÝ, Viktor PORADA. *Metodika vyšetřovania počítačovej kriminality a softwarového pirátstva.* Bratislava: Akadémia policejného zboru SR, 2004. ISBN-80-8054-323-2

*Víte co je KYBERŠIKANA?* [online]. [cit. 19. 8. 2016]. Dostupné z: http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

VLACHOVÁ, Marta. *E-Bezpeci: Trestná činnost spojená s internetovou kriminalitou* [online]. [cit. 29. 6. 2015]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226

VOKROUHLÍKOVÁ Kateřina a Zuzana PRŮCHOVÁ. *Naháči a prdeláči – fotky jen pro rodinu!* [online]. [cit. 19. 8. 2016]. Dostupné z: https://blog.nic.cz/2016/08/16/nahaci-a-prdelaci-fotky-jen-pro-rodinu/

VOLEVECKÝ, Petr a Jan STACH. Jak se krade pomocí Internetu – Phishing v praxi. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [cit. 14. 8. 2016]. Dostupné z: http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html

VOLEVECKÝ, Petr a Milan ŠUBRT. Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. *Trestní právo*, 2008, roč. 13, č. 4, s. 14–22. ISSN 1211-2860.

VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo*, 2010, roč. 14, č. 7–8, s. 34 a násl. ISSN 1211-2860.

VOLEVECKÝ, Petr. Kybernetická trestná činnost v mezinárodních dokumentech a v dokumentech ES/EU. *Trestní právo,* 2009, roč. 12, č. 7–8, s. 26-39. ISSN 1211-2860.

VOŽENÍLEK, David. *Promazání „sušenek" nepomůže, na internetu vás prozradí i baterie.* [online]. [cit. 4. 8. 2016]. Dostupné z: http://mobil.idnes.cz/sledovani-telefonu-na-internetu--stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

*Výzkum rizikového chování českých dětí v prostředí internetu 2014.* [online]. [cit. 19. 8. 2016]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace

*W32. Tinba (Tinybanker).* [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

*Warning! Over 900 Milion Android Phones Vulnerable to New „QuadRooter" Attack.* [online]. [cit. 10. 8. 2016]. Dostupné z: https://thehackernews.com/2016/08/hack-android-phone.html

*WATCH: ISIS Downs Prisoners Alive & Blows Hostages Up With RPG & Kills Others With Explosives - Graphic video.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up--with-rpg-kills-others-with-explosives-graphic-video-132382

*What is Internet of Things.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/internet-of-things

*What is the OSI Model* [online]. [cit. 8. 7. 2016]. Dostupné z: http://blog.buildingautomationmonthly.com/what-is-the-osi-model/

WILSON Tracy, V. *How Phishing Works.* [online]. [cit. 14. 8. 2016]. Dostupné z: http://computer.howstuffworks.com/phishing.htm

*World Internet Users and 2015 Population Stats.* [online]. [cit. 9. 8. 2015]. Dostupné z: http://www.internetworldstats.com/stats.htm

*Yahoo řeší, jestli má hacker opravdu údaje o 200 milionech účtů.* [online]. [cit. 16. 8. 2015]. Dostupné z: http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/

YAR, Majid. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal*, 2005, roč. 44, č. 4, s. 387–399.

*Zásady ochrany osobních údajů.* [online]. [cit. 14. 6. 2016]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/

ZETTER, Kim. *Is It Possible for Passengers to Hack Commwrcial Aircraft?* [online]. [cit. 5. 5. 2016]. Dostupné z: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/

*Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají možnost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit. 4. 4. 2014]. Dostupné z: https://www.google.cz/intl/cs/policies/?fg=1

*Znovu se objevily podvodné zprávy*. [online]. [cit. 15. 8. 2016]. Dostupné z: https://www.csirt.cz/news/security/?page=97

# Rejstřík

## Rejstřík

## C



## D

Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy

Za tuto publikaci odpovídá pouze její autor. Evropská unie nenese odpovědnost za jakékoli využití informací v ní obsažených.

**Recenzenti**
JUDr. Petr Hostaš
Dr. iur. et. JUDr. Helena Krejčíková, Ph.D.
Ing. Aleš Padrta, Ph.D.
doc. Ing. Miroslav Vozňák, Ph.D.

**CYBERCRIME**
JUDr. Jan Kolouch, Ph.D.

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2016
Kniha vyšla jako 14. publikace v Edici CZ.NIC.

© 2016 Jan Kolouch
Toto autorské dílo podléhá licenci Creative Commons (http://creativecommons.org/licenses/by-nd/3.0/cz/), a to za předpokladu, že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Dílo může být překládáno a následně šířeno v písemné či elektronické formě na území kteréhokoliv státu.

ISBN 978-80-88168-15-7 (tištěná verze)
ISBN 978-80-88168-16-4 (ve formátu EPUB)
ISBN 978-80-88168-17-1 (ve formátu MOBI)
ISBN 978-80-88168-18-8 (ve formátu PDF)

cz.nic | SPRÁVCE DOMÉNY CZ

**Summary**
Life without information and communication technologies (ICT) has become unthinkable for our society. However, regardless of how beneficial for the human race these technologies are, their use is also connected with a whole range of negative aspects. It is necessary to keep in mind that information and data and their use possess a great economic and political potential.

The monograph CyberCrime deals with the actual issue of cyberattacks and cybercrimes in virtual reality. It would be inacceptable if a cyberspace became the environment in which crimes could be committed without any punishment. Nevertheless, there is only one starting point for the combat against a criminality in cyberspace, i.e. the cyberspace itself. It is essential to understand what cyberspace represents, which principles it relies on, which kind of criminality could be present there and what the possibilities are of both criminal justice and especially the users themselves regarding the illegal activities.

The author describes technical aspect of ICT and the way how the ICT is used to commit a cyberattack or a cybercrime. Though, the core of the monograph lies in the problematics of the application of law in a cyberspace, incl. the issue of legal responsibility of a user and an internet service provider and civil and criminal liability of the attackers for their illegal activities. For a common user, especially chapters focusing on the anonymity and digital traces could be helpful, together with cases describing how social engineering via social networks can easily be used in order to reach and endanger the users.

The main part of the book is a description of cyberattacks which can be considered cybercrimes. The reader can find the subsumption of those attacks under legal provisions of the Czech Criminal code. The demarcation of potential criminal liability of cyber attackers could help the user and criminal justice to conduct a correct legal classification of any illegal activity. Besides, another goal of the monograph is to introduce the legal instruments available for criminal justice during pre-trial procedure.

Worldwide, legal and security aspects of cyberspace are heavily discussed, in order to take action capable of responding adequately to cyber criminality. The monograph CyberCrime shall help its readers to orientate themselves both in technical and legal areas which are directly related to cyber criminality.

Edice CZ.NIC

**O knize** Kniha CyberCrime obsahuje technické části, které čtenářům pomohou orientovat se ve světě malware, phishingu, darknetu, botnetů a dalších, pro ne zcela technicky zaměřeného uživatele matoucích a odstrašujících pojmů. Zároveň však kniha obsahuje i právní výklad: analyzuje kybernetickou kriminalitu z pohledu jednotlivých paragrafů, a umožňuje tak získat velké množství cenných informací i těm čtenářům, kteří sice ovládají všechny ty zvláštní technické pojmy, ale svět právních klasifikací, paragrafů a odstavců je jim cizí a neorientují se v něm.

**O autorovi** Jan Kolouch dlouhodobě působí na Policejní akademii ČR v Praze na pozici odborného asistenta na katedře trestního práva. Dále také vyučuje na katedře počítačových systémů na FIT ČVUT. Na obou vysokých školách je garantem předmětů, které se věnují problematice kybernetické kriminality. Současně od roku 2008 působí i v rámci sdružení CESNET z.s.p.o.
V minulosti také, mimo jiné, pracoval jako vedoucí oddělení informačních technologií na Policejní akademii ČR v Praze. Na řadě aktivit spolupracuje i se sdružením CZ.NIC.
Těžištěm jeho odborného zájmu je problematika aplikovatelnosti práva a odpovědnosti za protiprávní jednání v kyberprostoru. Jan Kolouch se také věnuje dalším projektům a školením v oblasti bezpečnosti v ICT, boje s kyberzločinem, ochraně uživatelů aj., jak na národní, tak mezinárodní úrovni. Byl rovněž členem expertních skupin European Union Agency for Network and Information Security (ENISA).
Jan Kolouch se snaží zvyšovat informovanost laické i odborné veřejnosti zejména v oblasti kybernetické kriminality a kybernetické bezpečnosti.

**O edici** Edice CZ.NIC je jedním z osvětových projektů správce české domény nejvyšší úrovně. Cílem tohoto projektu je vydávat odborné, ale i populární publikace spojené s Internetem a jeho technologiemi. Kromě tištěných verzí vychází v této edici současně i elektronická podoba knih. Ty je možné najít na stránkách knihy.nic.cz.

**knihy.nic.cz**

knihy.nic.cz
ISBN 978-80-88168-18-8
9 788088 168188 >