Univerzita Karlova v Praze
Právnická fakulta

Petra Dubenská

INTERNETOVÁ A POČÍTAČOVÁ KRIMINALITA

Diplomová práce

Vedoucí diplomové práce: **doc. JUDr. Tomáš Gřivna, Ph.D.**

Katedra: **Katedra trestního práva**

Datum vypracování práce (uzavření rukopisu): **24.3.2013**

Prohlašuji, že jsem předkládanou diplomovou práci vypracovala samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 24.3.2013 Podpis:

Obsah

Úvod

Technický pokrok vedl na přelomu 20. a 21. století k rozvoji informačních technologií v takovém rozsahu, že život člověka a vývoj lidské společnosti jsou dnes již přímo závislé na informačních technologiích, které se tak staly nezbytnou podmínkou dalšího civilizačního pokroku. Znalosti a data šířené za pomoci informačních technologií se postupně týkají všech sfér lidské činnosti a zásadním způsobem prohlubují globalizaci světa. V demokratických společenstvích nejsou využívání informačních technologií kladeny - nad rámec potřebný pro zachování tradičních sociálních norem a ekonomických pravidel - žádné překážky, v autoritativních režimech je využívání informačních technologií omezováno.

Zrychlení informačního toku ve všech oblastech lidské činnosti za využití informačně-komunikačních technologií dává nebývalý prostor k získávání nových informací v relativně krátkém čase, umožňuje jejich další zpracování a výměnu. Otevřenost a přístupnost k informacím prostřednictvím internetu však způsobuje jeho zranitelnost a otevírá možnosti jeho zneužití. V souvislosti s dynamickým rozvojem informačních technologií se objevily nové formy sociální patologie spočívající převážně v nemravném a asociálním jednání běžných uživatelů internetu (verbální urážky anonymních diskutérů pod články či v chatech, zkreslování vlastní identity za účelem dosahování nezasloužených výhod, "pařanství" atd.). Došlo k nárůstu psychických poruch způsobených subjektivním ztotožňováním virtuální reality se skutečným vnějším světem.[1] Tato sociální patologie vyúsťuje v jednání amorální či pseudokriminální (tzv. virtuální zločiny v kyberprostoru[2]) a v těch nejzávažnějších případech až v jednání kriminální. Počítačová a informační kriminalita (kybernetická kriminalita, kyberkriminalita) se přitom neustále mění a postupuje od primitivních způsobů ke způsobům stále sofistikovanějším, které využívají nových metod a postupů.

[1] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[2] GŘIVNA, Tomáš. Existují virtuální trestné činy?. In: *Pocta Otovi Novotnému k 80. narozeninám*. Vyd. 1. Praha: ASPI, 2008, s. 28-35. ISBN 978-80-7357-365-2.

Počítač je využíván buď jako prostředek k páchání různorodé trestné činnosti, anebo se sám stává napadeným objektem. [3]

Jelikož přenos dat za využití informačně-komunikačních technologií není územně nijak omezen a probíhá bez ohledu na existující hranice mezi jednotlivými státy, bylo nezbytné dosáhnout harmonizace trestněprávních norem těchto států tak, aby odhalování pachatelů a jejich postih mohlo být úspěšné.[4] Základní celosvětovou normou se stala Úmluva Rady Evropy č. 185 o počítačové kriminalitě přijatá dne 23.11.2001, která byla v roce 2003 doplněna o Dodatkový protokol rozšiřující trestní postih na činy s xenofobním a rasovým obsahem spáchaným pomocí počítačových systémů.

Trestní zákoník (zák. čís. 40/2009 Sb.) včlenil skutkové podstaty činů vymezených v Úmluvě do svých ustanovení, přičemž zachoval vlastní systematizaci trestných činů podle druhového objektu. Byť v této diplomové práci volím svoji vlastní kategorizaci kybernetických trestných činů z hlediska významnosti "kybernetického znaku" ve skutkové podstatě jednotlivých trestných činů (viz níže bod 2.4), domnívám se, že s ohledem na předpokládané prorůstání kybernetické kriminality do dalších oblastí lidského života nezbude než sjednotit kritéria členění kybernetických trestných činů v právní teorii s kritérii členění v trestním zákoníku. Lze totiž předpokládat, že "kybernetický prvek" považovaný v dnešní době v trestných činech za specifický, se postupem času stane běžnou součástí skutkové podstaty standardních trestných činů.

Téma *Internetová a počítačová kriminalita* jsem si vybrala pro jeho aktuálnost a nosnost, neboť i do budoucna lze předpokládat trvalost či spíše nárůst této trestné činnosti a - na to reagující - rozvíjející se ochranu proti ní v rámci legislativní a bezpečnostní politiky našeho státu i celé Evropské unie.

[3] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[4] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

1 Kyberkriminalita obecně

1.1 Vymezení základních pojmů

Pojem **kyberkriminalita** český právní řád nezná a v právní teorii byl tento pojem s určitými výhradami akceptován až na základě mezinárodního vlivu Úmluvy o počítačové kriminalitě ze dne 23.11.2001.[5] Předchozí odborné disputace k vymezení správného názvu se ubíraly od užších pojmů "počítačová kriminalita" a „internetová kriminalita“, přes přesnější pojem "informační kriminalita" až po moderní, ale nevžitý název "kybernalita".[6] Kybernetickou kriminalitou, neboli kyberkriminalitou tedy lze rozumět páchání kybernetických trestných činů.

U již ustáleného pojmu **kybernetický trestný čin** (kyberzločin) se další odborné diskuse vedou především k vymezení jeho obsahu, resp. definice. Různí autoři dospívají k různým vymezením, avšak v obecné poloze se jejich definice "protínají" ve znaku, že kybernetickým trestným činem je takový **trestný čin, který buď informačně-komunikační technologie ohrožuje, anebo je využívá** (buď je objektem nebo nástrojem).[7] Při takovémto vymezení by však pojem kybernetický trestný čin zahrnoval i tradiční trestný čin, k jehož spáchání bylo užito informačně-komunikačních technologií (např. e-mailovou zprávou spáchané vydírání podle § 175 tr.zák.); při takto širokém pojetí by se ovšem mohly kyberzločinem stát téměř všechny existující trestné činy, což by s postupným pronikáním informačně-komunikačních technologií do všech sfér konání člověka vedlo dříve či později k zániku pojmu kyberzločin. (Proč označovat specifickým pojmem něco, co je standardní.) Ještě paradoxnější by byla opačná situace, kdy by počítačově zcela negramotný pachatel spáchal bez ohrožení či využití informačně-komunikační technologie "kybernetický" trestný čin. (Např. trestný čin výroba a jiné nakládání s dětskou pornografií podle § 192 tr.zák. spáchaný tradičním

[5] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[6] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[7] Tato definice má rovněž základ v Úmluvě o počítačové kriminalitě ze dne 23.11.2001, která tyto dvě kategorie kyberzločinů doplňuje o trestné činy vztahující se k obsahu počítačových dat a o trestné činy související s porušením autorského práva.

způsobem.) Sama bych proto považovala za **kybernetický trestný čin** takový trestný čin, který by současně splňoval dvě podmínky:

a) má kybernetický znak (tj. ohrožení či využití informačně-komunikační technologie) uvedený ve skutkové podstatě a současně

b) byl skutečně spáchán tak, že buď ohrozil či využil informačně-komunikační technologii.

Z hlediska právní teorie by pak byly za kybernetické trestné činy považovány především trestné činy podle § 230, § 231 a 232 tr.zák., které nemohou být spáchány jiným jednáním než ohrožením či využitím informačně-komunikační technologie. Tyto tři trestné činy, u nichž nutně musí být vždy naplněny obě podmínky ad a) i ad b) shora, by mohly být označeny za absolutně kybernetické trestné činy (absolutní kyberzločiny). Ve smyslu uvedené definice by dále byly za kybernetické trestné činy považovány takové trestné činy, u nichž je jedním ze znaků skutkové podstaty charakterizujících objekt, objektivní stránku či subjekt[8] kybernetický prvek (tj. ohrožení či využití informačně-komunikační technologie) a současně byly s využitím tohoto znaku skutečně spáchány. Tyto by mohly být označeny za relativně (či potenciálně) kybernetické trestné činy (relativní kyberzločiny) s eventuelním rozlišením toho, zda kybernetický znak mají již v základní skutkové podstatě či pouze jako zvlášť přitěžující okolnost (viz níže bod 2.4)

Pojem **kyberprostor** (cyberspace) se postupně rozšířil z beletristické literatury[9] do odborné technické i právnické literatury tak frekventovaně, že v současné době jej lze chápat již jako *terminus technicus*.[10] V obecném pojetí je pojem kyberprostor

---

[8] např. u trestného činu porušení tajemství dopravovaných zpráv podle § 182 tr.zák., u něhož v odstavci pátém je subjektem zaměstnanec provozovatele počítačového systému či osoba vykonávající komunikační činnost

[9] Termín kyberprostor jako první použil v roce 1982 americký spisovatel science fiction William Ford Gibson v povídce Burning Chrome, v širší povědomí pak tento termín (jakož i termíny virtuální realita, Matrix a Internet) vstoupil v roce 1984 v jeho románu Neuromancer, kde jej popsal takto: *"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…"* - viz JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[10] v návrhu zákona o kybernetické bezpečnosti, předloženém v době dokončování této diplomové práce k připomínkovému řízení, je pojem kybernetický prostor vymezen takto: "digitální

používán ve smyslu protikladu k reálnému světu (realspace), tedy pro označení virtuálního světa vytvářeného moderními informačně-komunikačními technologiemi. Je vymezován jako imaginární prostor bez hmotné podstaty, který je však na reálném světu závislý. Vytvářejí jej jako společný virtuální prostor připojením se na komunikační a informační služby jednotliví uživatelé propojených počítačových systémů. Toto na času a prostoru nezávislé fiktivní prostředí, vyznačující se možností skryté či změněné identity, přináší dříve netušené a i dnes ne zcela předvídatelné možnosti vzájemné sociální interakce.[11] Vedle převažujících pozitivních stránek jsou s takovýmto prostředím nutně spojeny i sociálně patologické jevy, které - především kvůli prostředí anonymity - jsou svůdné i pro jinak bezúhonné osoby, které by se tradičního kriminálního jednání nedopustily.

Počítačem se rozumí funkční jednotka, která může provádět rozsáhlé výpočty, včetně mnoha aritmetických a logických operací, bez zásahu člověka a podle určitého programu. Jde o zařízení schopné přijímat data, samostatně je zpracovávat podle předem zadaného programu a poskytovat výsledky takového zpracování.[12]

Data v obecné podobě představují interpretovatelnou a formalizovanou reprezentaci informace vhodnou pro komunikaci, interpretaci nebo zpracování.[13] V informatice představují data veškeré informace v digitální (číselné) podobě určené k počítačovému zpracování. Data - např. číslo, text, obrázek, zvuk atd. - jsou zapsána (kódována) v podobě posloupností čísel (bajtů) a uloženy např. v operační paměti počítače nebo na datovém nosiči. Stejným způsobem je kromě dat uložený sled instrukcí tvořící počítačový program, který určuje, jak má počítač data zpracovávat.[14]

---

prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací"

[11] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[12] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[13] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[14] Přispěvatelé Wikipedie, Data (počítače) [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 31. 12. 2012, 17:20 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Data_(po%C4%8D%C3%ADta%C4%8De)&oldid=9505041>

Informace je poznatek týkající se jakýchkoli objektů, jako jsou fakta, události, věci, procesy nebo myšlenky, včetně pojmů, které mají v určitých souvislostech zvláštní význam. Jde o sdělení, jež je v dané situaci nové, pravdivé a má určitou hodnotu. Má nehmotný charakter a jeho nositelem je signál, který umožňuje s informací nakládat i po zániku jejího původního zdroje. Informační tok je realizován sledem kódových znaků. Jednotkou informace ve výpočetní technice je jeden bit, který představuje elementární množství informace umožňující rozlišit mezi dvěma stavy.[15]

Informačně-komunikační technologie (zkráceně ICT, z anglického Information and Communication Technologies) zahrnuje veškeré informační technologie používané pro komunikaci a práci s informacemi. Původní koncept informačních technologií (IT) byl doplněn o prvek komunikace, kdy mezi sebou začaly komunikovat jednotlivé počítače či uzavřené sítě. Informačně-komunikační technologie jsou nejen hardwarové prvky (počítače, servery, atd.), nýbrž i softwarové vybavení (operační systémy, síťové protokoly, internetové vyhledávače atd.). Společným jmenovatelem těchto technologií se stala přítomnost dat a sítí.[16]

Informačně-komunikační síť je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači. Jde o funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem. Umožňují uživatelům komunikaci podle určitých pravidel sdílení a využívání společných zdrojů nebo výměny informací. V poslední době jsou všechny sítě postupně spojovány do globální celosvětové sítě zvané internet.[17]

Internet je informační a komunikační systém, který se skládá z různých subjektů a objektů právních vztahů. Díky rozvoji počítačových informačních a komunikačních technologií má internet kromě jiného i povahu prostředku, jehož

---

[15] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[16] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[17] Přispěvatelé Wikipedie, Počítačová síť [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 26. 02. 2013, 11:46 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5&oldid=9795140>

prostřednictvím lze veřejně šířit informace. S ohledem na celosvětovou propojenost a rozšířenost počítačových médií je virtuální svět internetu považován za veřejný prostředek, neboť je používán právě pro zveřejňování a šíření informací.[18] Internet je počítačovou sítí, která funguje jako přenosové médium umožňující využívání určitých služeb, z nichž nejvýznamnější je přenos informací, tj. znalostí, které je možné jakoukoli formou sdělovat a jde o poznatek týkající se jakýchkoliv objektů, fakt, událostí, věcí procesů, myšlenek, který mají v daném kontextu specifický význam.[19] Mezi mnoha informačně-komunikačními sítěmi je internet specifickou sítí, která používá speciální komunikační protokol, a to internetový protokol (IP). Uvnitř internetu samotného existuje mnoho způsobů komunikace prostřednictvím služby world wide web (WWW), která umožňuje přístup k webovým stránkám, e-mailovým účtům, službám internetového chatování (internet relay chat - IRC, Googletalk), přenos souborů (File Transfer Protocol - FTP), internetovou telefonii (Voip).[20]

E-mailová adresa představuje elektronickou službu spočívající v elektronické poště, která je definována jako telekomunikační služba instalovaná převážně na standardních počítačových sítích. Je určena k přenosu zpráv mezi počítačovými pracovišti, k ukládání těchto zpráv do paměťových schránek, k třídění a předzpracování zpráv. Vyznačuje se efektivním a levným provozem.[21] Ochrana podle § 89 a násl. zák. č. 127/2005 Sb., o elektronických komunikacích, přísluší obsahu elektronicky rozesílané zprávy, kdežto e-mailová adresa jako identifikační místo umožňující elektronický přenos zprávy uvedené ochrany nepožívá. Nepožívá však ani ochrany podle zákona č. 101/2000 Sb., o ochraně osobních údajů. E-mailovou adresu lze přidělit pouze určitému uživateli, a to na základě smlouvy uzavřené s poskytovatelem připojení (providerem), u něhož vznikne systém o osobách (náležitostí smlouvy jsou totiž osobní údaje jméno, příjmení, adresa, rodné číslo apod.). Na něj se vztahují všechny povinnosti provozovatelů informačních systémů obsahujících osobní

[18] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. Vyd. 1. Praha: C. H. Beck, 2001, xxiv, 542 s. ISBN 80-717-9552-6.

[19] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. Vyd. 1. Praha: C. H. Beck, 2001, xxiv, 542 s. ISBN 80-717-9552-6.

[20] GŘIVNA, Tomáš a Radim, POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[21] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. Vyd. 1. Praha: C. H. Beck, 2001, xxiv, 542 s. ISBN 80-717-9552-6.

údaje občanů ve smyslu zákona č. 101/2000 Sb. Přiřadit konkrétní osobu k takové elektronické adrese může tedy pouze provider, a pokud by tak učinil někdo jiný, porušil by zákon on nebo někdo jiný, kdo by mu data poskytl. Existuje tedy sice propojení mezi adresou a identifikací osoby, a to ve smlouvě mezi uživatelem a poskytovatelem připojení, nicméně se nejedná o veřejně dostupný údaj. Bude-li mít někdo jakýmkoliv způsobem sesbíraný soubor existujících e-mailových adres bez dalších údajů, zejména bez výše uvedeného propojení s určitou fyzickou osobou, nejedná se tedy zřejmě o soubor obsahující osobní údaje a nevztahuje se na něj žádná ochrana z hlediska zák. č. 101/2000 Sb. Samotná elektronická (e-mailová) adresa nebo jiný identifikátor používaný na internetu není osobním údajem ve smyslu § 4 písm. a) zák. č. 101/2000 Sb. a nepožívá ochrany při izolovaném výskytu sama o sobě.[22]

E-mailová zpráva je textová, hlasová nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo koncovém zařízení uživatele, dokud ji uživatel nevyzvedne. Důvěrnost zpráv a s nimi spojené provozní a lokalizační údaje jsou chráněny podle § 89 a násl. zák. č. 127/2005 Sb., o elektronických komunikacích.[23] Podle § 89 zák. č. 127/2005 Sb. podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak. To nebrání technickému ukládání údajů, které je nezbytné pro přenos zpráv, aniž by byla dotčena zásada důvěrnosti. Zprávou se rozumí 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

[22] SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. Vyd. 1. Praha: C. H. Beck, 2001, xxiv, 542 s. ISBN 80-717-9552-6.

[23] HENDRYCH, Dušan. *Právnický slovník*. 3., podstatně rozš. vyd. V Praze: C.H. Beck, 2009, xxii, 1459 s. Beckovy odborné slovníky. ISBN 978-80-7400-059-1.

komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá (§ 89 odst. 2 zák. č. 127/2005 Sb.).

1.2 Mezinárodně právní souvislosti trestního postihu kyberkriminality

Základním problémem boje proti kyberkriminalitě je teritorialita práva. Pro současnou kyberkriminalitu je přitom typické, že se odehrává zároveň na území více států. Např. k samotnému skutku dojde na území jednoho státu, avšak jeho účinky nastanou na území státu jiného. Přestože za takové jednání lze většinou stíhat pachatele ve všech dotčených zemích, je s takovým stíháním spojena řada problémů vyplývající z rozdílné legislativy i z odlišnosti procesních postupů. Mezinárodní spolupráce v otázce úpravy a sjednocení trestněprávních norem v oblasti kyberkriminality se proto stala nutností.

Nejvýznamnější aktivitou v mezinárodní harmonizaci trestní jurisdikce se stala **Úmluva Rady Evropy č. 185 o počítačové kriminalitě přijatá dne 23.11.2001**. Úmluva vymezila řadu pojmů informačně-komunikačních technologií, v oblasti trestního práva hmotného definovala znaky skutkových podstat devíti kybernetických trestných činů, které rozdělila do čtyř skupin a devíti článků podle chráněného zájmu (viz níže bod 2.2) a stanovila základní postupy trestního procesního práva. Členské státy se v Úmluvě zavázaly provést taková legislativní opatření, která jejich orgánům umožní tyto trestné činy vyšetřovat a zajišťovat k tomu odpovídající důkazy. Cílem bylo zabránit situaci, kdy by některý z nově definovaných trestných činů nebyl v některém členském státu trestný nebo by orgány trestního řízení nedisponovaly procesními oprávněními potřebnými k vyšetření činu a k usvědčení pachatele. Úmluva obsahuje i úpravu postupů a vzájemnou asistenci při vydávání pachatelů a spolupráci při vyšetřování a získávání důkazních materiálů. Zavádí institut kontaktních center s nepřetržitým provozem, jejichž úkolem je koordinovat vzájemnou spolupráci orgánů trestního řízení. Za významný pokrok při budování mezinárodní trestní jurisdikce nad

kyberprostorem lze považovat to, že Úmluvu podepsaly a ratifikovaly USA.[24] Úmluva vstoupila v platnost 1.7.2004 a do současné doby ji podepsalo 47 států včetně České republiky, z čehož 36 států ji již ratifikovalo (v České republice nyní ratifikační proces probíhá).

Následně byla Úmluva doplněna o Dodatkový protokol ze dne 28.1.2003, který rozšířil trestní postih na činy s xenofobním a rasovým obsahem spáchaným pomocí počítačových systémů. Dodatkový protokol vstoupil v platnost 1.3.2005, avšak Česká republika jej nepodepsala.

K harmonizaci právní úpravy v boji proti kyberzločinu přispěla řada dalších mezinárodních smluv i legislativa Evropské unie. Mezi nejvýznamnější patří Rozhodnutí rady Evropské unie 92/242/EHS ze dne 31.3.1992 o bezpečnosti informačních systémů, Rámcové rozhodnutí Rady o boji proti dětské pornografii na internetu 2000/375/JHA ze dne 29.5.2000, Rámcové rozhodnutí Rady Evropské unie 2004/68/SVV ze dne 22.12.2003 o boji proti pohlavnímu vykořisťování dětí a dětské pornografii, Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24.2.2005 o útocích proti informačním systémům a Úmluva Rady Evropy o ochraně dětí před sexuálním vykořisťování a zneužíváním ze dne 25.10.2007.

Kontroverzní a mediálně známou se stala **Obchodní dohoda proti padělatelství** (Anti-Counterfeiting Trade Agreement, zkráceně ACTA), jejíž finální text byl zveřejněn v roce 2011. Jejím účelem bylo vytvoření mezinárodních standardů pro ochranu duševního vlastnictví. Ačkoliv konečný text dohody neobsahoval oproti původnímu znění tak přísná opatření, vyvolala dohoda řadu protestů, neboť zaváděla relativně tvrdé sankce a směřovala ke státním zásahům do svobodného internetu. Česká republika ji sice spolupodepsala, ale Evropským parlamentem nakonec přijata nebyla.[25]

---

[24] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, 388 s. Téma (Auditorium). ISBN 978-80-87284-22-3.

[25] znění dohody viz - http://register.consilium.europa.eu/pdf/sk/11/st12/st12196.sk11.pdf V říjnu 2011 podepsalo dohodu osm států, včetně USA, Kanady, Japonska, Austrálie, k nimž v lednu 2012 přistoupilo 22 států Evropské unie, včetně České republiky. Nedostatkem ACTA bylo, že jejími signatáři se nestaly Čína, Indie, Brazílie a Rusko, tedy země, jež jsou zdrojem většiny padělků. Evropský parlament čelící tlaku petic a demonstrantů na svém zasedání dne 4.7.2012 ACTA odmítl,

1.3 Úprava kyberkriminality v českém právním řádu

V českém právním řádu byl historicky první kybernetický trestný čin upraven v roce 1991 ve zcela nově vytvořené skutkové podstatě. Jednalo se o trestný čin **poškození a zneužití záznamu na nosiči informací podle § 257a**, který byl do tehdejšího trestního zákoníku (zák.čís. 140/1961 Sb.) vložen novelou čís. **557/1991 Sb., účinnou od 1. 1. 1992**. Objektem tohoto trestného činu byla ochrana dat uložených na nosiči informací proti neoprávněným změnám a proti jejich neoprávněnému použití. Předmětem ochrany byl nosič informací, jeho obsah a technické a programové vybavení počítače.[26] Tento nový trestný čin byl následně dvakrát změněn. Poprvé v roce 2002, kdy zákonem čís. 134/2002 Sb. byl první odstavec doplněn vedle tam již uvedeného počítače o *jiné telekomunikační zařízení* a současně bylo znění prvého odstavce zpřesněno, aby nevznikaly pochybnosti, že získání přístupu k nosiči informací nemusí být provedeno již v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě či jinému neoprávněný prospěch, jak ostatně začala dovozovat postupně se utvářející judikatura. Druhá změna, provedená zákonem č. 253/2006 Sb., se dotkla pouze trestu a v souvislosti se změnou týkající se trestu propadnutí věci (§ 55) byla vedle možnosti uložení trestu propadnutí věci doplněna možnost uložení trestu propadnutí jiné majetkové hodnoty.[27]

Druhým kybernetickým trestným činem v českém právním řádu byl trestný čin **porušování autorského práva podle § 152 předchozího trestního zákoníku** (zák.č. 140/1961 Sb.), ve znění novely čís. **121/2000 Sb., účinné od 1.12.2000**, která změnila dikci prvního odstavce § 152 tak, že neoprávněný zásah do autorských práv doplnila o zásah k *databázi.* Tato novela § 152 souvisela s přijetím nového autorského zákona -

---

když pro přijetí hlasovalo pouze 39 poslanců a proti přijetí 478 poslanců. Není ovšem vyloučeno, že smlouva bude předložena Evropskému parlamentu ke schválení znovu. Zdroj: http://technet.idnes.cz/acta-skoncila-europarlament-zamitl-actu-fdq-/sw_internet.aspx?c=A120704_132333_sw_internet_pka

[26] ŠÁMAL, Pavel a Stanislav RIZMAN. *Trestní zákon: Komentář*. 1. vyd. Praha: SEVT, 1994, XI, 1036 s. Komentované zákony (SEVT). ISBN 80-704-9097-7.

[27] Rozbor "Rozhodování soudů o skutcích posouzených podle § 257a TZ" provedený Institutem kriminologie a sociální prevence v rámci projektového úkolu nazvaného „Výzkum a analýza závažných forem trestné činnosti“ [online]. [cit. 2013-01-25]. Dostupné z: http://www.ok.cz/iksp/docs/kt_grivna.pdf

zákona čís. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů.[28]

Současnou úpravu kybernetických trestných činů pak s účinností od 1.1.2010 přinesl nový **trestní zákoník** (zák.čís. 40/2009 Sb., ve znění novely čís. 306/2009 Sb.), který byl v ustanoveních týkajících se kybernetických trestných činů (§ 192, § 311) novelizován zákonem čís. 330/2011 Sb., účinným od 1.12.2011. Kybernetickým trestným činům podle současné právní úpravy se podrobně věnuji v kapitole 2 a v kapitole 3.

Od roku 2011 probíhá v České republice legislativní proces k přípravě **zákona o kybernetické bezpečnosti**, který by měl zefektivnit ochranu českého kyberprostoru.[29] V květnu 2012 vláda schválila věcný záměr tohoto zákona, který obsahoval popis jak záměrů a cílů, kterých má být dosaženo, tak hlavních prostředků, jež přitom mají být použity. Věcný záměr vycházel z předpokladu, že poskytovatelem a uživatelem informačních systémů, sítí a služeb elektronických komunikací je nejen stát, ale i soukromoprávní subjekty, pro které má bezpečnost českého kyberprostoru značný ekonomický význam. Věcný záměr zahrnoval i komparaci zákonných úprav kybernetické bezpečnosti v jiných evropských zemích a v USA a posouzení souladu navrhované úpravy s mezinárodními smlouvami.[30] Začátkem roku 2013 bylo dokončeno paragrafové znění zákona s předpokládaným datem nabytí účinnosti dnem 1.1.2015 a nyní probíhá jeho připomínkové řízení. Předmětem úpravy zákona jsou práva a povinnosti orgánů veřejné moci, fyzických a právnických osob, působnost orgánů státní správy a jejich vzájemná spolupráce v oblasti kybernetické bezpečnosti. Zákon definuje systém zajištění kybernetické bezpečnosti, který tvoří bezpečnostní opatření, hlášení kybernetických bezpečnostních incidentů, protiopatření, oznamování

[28] Na rozdíl od trestného činu podle § 257a, který by patřil do kategorie absolutně kybernetických trestných činů, by trestný čin podle § 152 patřil do skupiny relativně (potenciálně) kybernetických trestných činů, neboť by mohl být spáchán zásahem i do jiného práva než do práva k databázi, resp. by mohl být spáchán bez ohrožení či využití informačně-komunikační technologie.

[29] Usnesením vlády ČR č. 781 ze dne 19. října 2011 byla ustavena Rada pro kybernetickou bezpečnost jako poradní orgán předsedy vlády pro oblast kybernetické bezpečnosti a vzniklo Národní centrum kybernetické bezpečnosti (NCKB) jako součást Národního bezpečnostního úřadu

[30] Věcný záměr zákona o kybernetické bezpečnosti – verze schválená vládou. [online]. [cit. 2013-01-25]. Dostupné z: http://www.nbu.cz/cs/aktuality/808-vecny-zamer-zakona-o-kyberneticke-bezpecnosti---verze-schvalena-vladou-/

kontaktních údajů a činnost dohledových pracovišť. Předpokládá rozdělení kyberprostoru na část spravovanou vládním CERT (Computer Emergency Response Team), jenž jako součást Národního bezpečnostního úřadu funguje již od září 2012, a na část spravovanou národním CERT, provozovaného soukromoprávním subjektem na základě veřejnoprávní smlouvy uzavírané s Národním bezpečnostním úřadem. Zákon kodifikuje nový právní režim *stav kybernetického nebezpečí*, který definuje jako stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací, a tím dojde nebo by mohlo dojít k porušení nebo ohrožení zájmu České republiky.[31] Nemusí být náhoda, že po předložení návrhu zákona k připomínkovému řízení se v březnu 2013 uskutečnily na několik tuzemských společností zdánlivě bezdůvodné masivní útoky typu DDoS, které mohou ovlivnit definitivní podobu zákona.

1.4 Typologie útoků pachatelů kyberkriminality

1.4.1 Hacking

Pojem hacking vznikl v 50. letech 20. století v souvislosti s vývojem prvního počítače *ENIAC*. V té době ještě neexistovali vývojáři softwaru, a proto si software museli přizpůsobovat sami pracovníci, kteří počítač obsluhovali. Tyto zásahy se označovaly anglickým pojmem „hacks“, který v překladu znamená „záseky“.[32] Prvotní hackerství tedy nebylo nezákonnou aktivitou, nýbrž spontánní činností směřující k počítačovému programování a k širšímu využití počítačů jejich uživateli. Vyžadovalo vysokou počítačovou vyspělost a postupně se rozvíjelo k nekonvenčnímu užití počítačových systémů. Hackerská kultura byla založena na principech otevřenosti kyberprostoru, volného přístupu k výsledkům duševní činnosti a jejich vzájemného sdílení za využití nadprůměrných počítačových znalostí. Tyto idealistické zásady

[31] Pracovní verze zákona o kybernetické bezpečnosti [online]. [cit. 2013-01-25]. Dostupné z: http://www.nbu.cz/cs/aktuality/599-informace-k-zakonu-o-kyberneticke-bezpecnosti/

[32] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

zůstaly v určité formě hackerství (hacking v užším slova smyslu) zachované do současnosti, ale v jiných případech se hackerství postupně členilo do mnoha specifických podskupin, které prvotní idealistické zásady, založené na pozitivních hodnotách, opouštěly a akceptovaly vlivy chování nejrůznějších zájmových socioskupin, pro něž byl motivem jednání majetkový profit či samoúčelné škodění. Hacking - v dnešním užším slova smyslu - představuje činnost spočívající v průniku do počítačových systémů jinak než standardní cestou bez úmyslu získávat či ničit informace nebo působit škodu. Motivem jednání pachatelů je prokazování vlastních schopností, takže průnik do počítačového systému je cílem sám o sobě. Hackerům stačí uspokojení z toho, když je jejich čin prezentován ve vlastní komunitě. Baví je zkoumat detaily programovatelných systémů, zjišťovat jejich slabiny a hledat metody, jak je vylepšit. Základním vyznáním hackera je svoboda jedince, sdílení získaných informací a neuznávání mocenských autorit. Prosazují myšlenku, že všechny informace by měly být volně dostupné zdarma a jakékoli legislativní či jiné omezení v přístupu k nim je nedůvodné. Pokud jejich jednání překročí hranici trestnosti, bývá kvalifikováno jako neoprávněný přístup k počítačovému systému podle § 230 odst.1 tr.zák.

1.4.2 Cracking

Jde o způsob zneužití hackerských metod k prolamování ochrany elektronických nebo programových produktů. Někteří autoři zahrnují pod cracking pouze páchání zlovolných skutků a bezdůvodného vandalismu,[33] jiní uvádějí jako motiv pachatelů neoprávněné užití produktu.[34] V případě neoprávněného užití práva duševního vlastnictví může jít buď o tzv. černé uživatele, jejichž záměrem je získání produktu pro vlastní potřebu, anebo o tzv. piráty, jejichž motivem je finanční profit.[35] Trestněprávní kvalifikace crackingu může značně rozdílná, pro zlovolné jednání bude typické naplnění skutkové podstaty trestného činu neoprávněný přístup k počítačovému systému podle § 230 odst. 2 tr.zák.

---

[33] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[34] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[35] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

1.4.3 Pirátství

Původní a nejzřejmější forma počítačového pirátství je **kopírování**. K jeho masovému rozvoji došlo v 90. letech minulého století v souvislosti s nástupem kompaktních disků a zejména s běžnou dostupností mechanik (CD-ROM, CD-R) umožňujících "vypalovat" data na disky.[36] S dalším rozvojem informačních technologií a nástupem internetu se počítačové pirátství stalo doprovodným fenoménem jeho používání. Pojem **warez** v počítačovém slangu označuje autorská díla, se kterými je nakládáno v rozporu s autorským právem.[37] Pirátství spočívalo prolomení ochrany produktu a jeho šíření prostřednictvím serverů poskytujících úložné místo pro data (např. RapidShare). Tento způsob pirátství je již dnes překonán a používá se spíše pro šíření tzv. **cracků**, tedy programů umožňujících zrušení ochrany u programových produktů, jejichž plné verze jsou sice k dispozici ke stažení z internetových stránek či jsou na reklamních nosičích (CD, DVD), ale jsou časově nebo jinak omezeny. V současné době jsou nejrozšířenějším typem pirátství programy **peer-to-peer** (P2P), které umožňují přímou komunikaci mezi jednotlivými uživateli za účelem výměny audiovizuálních a jiných souborů (nejčastěji hudebních nahrávek ve formátu MP3, filmů ve formátu MPEG a software).[38] Může se jednat buď o audiovizuální pirátství, které zasahuje do autorských práv k audiovizuálním dílům, anebo o softwarové pirátství, které porušuje práva k počítačovému programu. **Audiovizuálním pirátstvím** je užití filmového nebo hudebního díla formou rozmnožování díla mimo třístupňový test podle autorského zákona (viz níže bod 3.2.7), rozšiřování originálu nebo jeho rozmnoženiny, sdělování díla veřejnosti, přenos televizního vysílání, jestliže ve smyslu § 12 odst. 1 autorského zákona nedal autor k takovému užití díla souhlas. Typicky je tak audiovizuálním pirátstvím v prostředí uživatelů informačních technologií zejména zpřístupnění hudebního či filmového díla nahráním dat (up-load) do prostředí internetu nebo jeho zpřístupnění formou výměnných sítí (peer-to-peer), veřejné projekce filmových děl, umísťování odkazů (link) na dílo v prostředí webových stránek apod. **Softwarové**

[36] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[37] Přispěvatelé Wikipedie, Warez [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 1. 03. 2013, 13:28 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Warez&oldid=9808868>

[38] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

pirátství zpravidla zahrnuje jakékoliv nakládání s počítačovým programem v rozporu s autorským zákonem. Počítačový program, který není volně dostupný jako freeware či shareware, není možné ani užít ve smyslu třístupňového testu, neboť podle § 30 odst. 1 autorského zákona je odlišná právní úprava pro počítačové programy, elektronické databáze a architektonická díla. Zhotovení rozmnoženiny počítačového programu stažením z internetu či z jiné sítě, okopírování datového nosiče s počítačovým programem či jiný způsob vytvoření rozmnoženiny díla je užitím díla nikoliv pro vlastní potřebu a proto v rozporu s autorským zákonem, jestliže k takovému užití není ten, kdo počítačový program tímto způsobem užívá, podle autorského zákona oprávněn.[39] Z hlediska trestněprávní kvalifikace půjde o trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi podle § 270 tr.zák.

1.4.4 DoS a DDoS

Zkratka DoS znamená *Denial of Service*, neboli potlačení služby. Jde o techniku útoku na internetové služby nebo stránky, při kterém dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele. Cílem takového útoku je buď vnucení opakovaného resetu napadenému počítači, nebo narušení komunikace mezi serverem a obětí tak, aby jejich komunikace byla zcela nemožná nebo velmi pomalá. Většinou je jeho cílem útok v daném čase na jednu konkrétní službu. Existují ovšem i techniky, které umožňují distribuované útoky na vícero služeb v jednom čase. Distribuovaný DoS útok (DDoS, *Distributed Denial of Service attack*) je charakterizován větším množstvím počítačů, snažících se najednou zahltit cíl útoku. Útok je většinou veden bez vědomí majitelů útočících počítačů, neboť se jedná o důsledek napadení a úspěšného infikování těchto systémů. Jedním ze způsobů je infikování počítače malwarem, který má v sobě pevně danou IP adresu oběti útoku a datum, kdy se program pokusí na cíl zaútočit. Po úspěšném infikování počítače tedy již útočník s daným systémem nemusí nijak komunikovat a útok proběhne automaticky. Systém může být také napaden programem (*botem*), který poté běží jako rezidentní proces a čeká na příkazy útočníka (tvůrce *bota*). Takto napadený systém se nazývá

[39] VOLEVECKÝ, Petr. Kybernetická trestná činnost jako předmět vědeckovýzkumné činnosti. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2011, č. 5. ISSN 1211-2860.

zombie a společně s ostatními počítači, napadenými stejným programem, tvoří takzvaný *botnet*.[40]

1.4.5 Phishing

Jedná se o zcizení digitální identity uživatele za účelem jejího zneužití, především k převodu či výběru peněz z účtu. Princip phishingového útoku spočívá nejčastěji v zaslání podvrženého 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 který je uživatel vyzýván kliknout. Jako záminka slouží nejčastěji bezpečnostní mezera systému apod. Po kliknutí na přiložený odkaz se uživatel dostává na webovou stránku, která se svým vzhledem i funkcemi od pravé webové schránky téměř neliší. Ve skutečnosti je však uživatel přesměrován na padělanou webovou stránku, která originál více či méně zdařile imituje. Na této falešné stránce uživatel zadá své přihlašovací jméno a heslo. Tato uživatelem zadaná data jsou díky naprogramování falešné webové stránky automaticky odesílána útočníkovi.[41] Phishing naplňuje znaky skutkové podstaty trestného činu neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 tr.zák.

1.4.6 Pharming

Jedná se o škodlivější formu phishingu, kdy je útok veden přímo na DNS sever, tedy na server sloužící k překladu IP adres na doménová jména. Podaří-li se pachateli změnit záznam na DNS serveru, adresa, na niž je oběť přesměrována, není rozpoznatelná od skutečné webové stránky banky. Obdobně jako u phishingového útoku pak stránka slouží k získání identifikačních a důvěrných informací za účelem jejich zneužití.[42]

1.4.7 Card skimming

---

[40] Přispěvatelé Wikipedie, Denial of service [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 25. 02. 2013, 13:57 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Denial_of_service&oldid=9790754>

[41] JAMES, Lance. *Phishing bez záhad*. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

[42] JAMES, Lance. *Phishing bez záhad*. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

Jde o typ útoku, při němž jsou útočníkem pomocí čtečky karet získána data obsažená na magnetických pruzích platebních, debetních či jiných podobných karet. Tato data jsou následně využita k vyhotovení padělané platební karty, která je pak užívána k odčerpávání peněz z účtu poškozeného jako karta pravá. Tento typ kybernetického útoku se podobá phishingu, jsou zde však podstatné rozdíly. Pro oba typy útoků je společné to, že útočník pomocí informačních a komunikačních technologií a dalších technických zařízení získá přístup k peněžnímu účtu poškozeného. Rozdíl je však ve způsobu provedení. Skimmingové zařízení může být nainstalováno např. do čteček platebních karet na čerpacích stanicích, v restauracích či v hotovostních bankomatech apod. Skimmingový útok probíhá tak, že útočník nejprve získá přístup k zařízení, které je určené ke čtení uvedených karet a následně je do takového zařízení útočníkem nainstalovaný technický prostředek, který přečte data uložená na magnetickém proužku karty a tyto odešle pomocí komunikačního zařízení útočníkovi. Takto získaná data jsou poté přenesena na nový magnetický proužek jiné karty.[43] Z hlediska trestněprávní kvalifikace jde o trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 tr.zák.

1.4.8 Keylogging

Jedná se o tzv. odposlouchávání klávesnice za pomoci softwarového produktu či hardwarového zařízení a slouží k opatřování informací pro přípravu útoku. Softwarový keylogging je odposlouchávání pomocí programu (malware), který je umístěn v napadeném počítači tak, aby nebyl odhalitelný. Hardwarové odposlouchávání je realizováno za pomoci technického zařízení buď vloženého mezi klávesnici a počítač v podobě redukce mezi konektory, nebo přímo zabudovaného v těle klávesnice. V případně napadání bankomatů jde o překryvnou klávesnici doplněnou o kameru.[44] Jednání naplňuje znaky trestného činu neoprávněný přístup k počítačovému systému podle § 230 tr.zák. a trestného činu opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 tr.zák.

---

[43] VOLEVECKÝ, Petr. Phishing a card skiming z pohledu českého trestního práva. *Bezpečnostní teorie a praxe = Security theory and practice / Policejní akademie České republiky*. 2011, zvláštní číslo, díl. 2. ISSN 1801-8211.

[44] Přispěvatelé Wikipedie, Keylogger [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 15. 09. 2012, 23:05 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Keylogger&oldid=9028722>

1.4.9 Sniffing

Jde o neoprávněné monitorování a sledování (doslova "čmuchání") síťového provozu ke shromažďování informací potřebných pro přípravu útoku. Sniffer se může postavit mezi dva počítače, servery nebo libovolné aktivní prvky a následně mohou být zpracovávána zachycená data. Při této metodě může útočník také nepozorovaně data pozměňovat nebo spojení úplně přerušit. Postihnout jej lze jako trestné činy porušení tajemství dopravovaných zpráv podle § 182 tr.zák., porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle § 183 tr.zák., neoprávněný přístup k počítačovému systému podle § 230 tr.zák. anebo opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat podle § 231 tr.zák.

1.4.10 Phreaking

Jde o označení pro napojení se na cizí telefonní linku v rozvodnicích, veřejných telefonních budkách nebo přímo na nadzemní či podzemní telefonní vedení, díky čemuž lze zdarma surfovat po internetu či kamkoliv zdarma telefonovat, případně odposlouchávat cizí telefonní hovory. Lze postihnout jako trestný čin porušení tajemství dopravovaných zpráv podle § 182 tr.zák. nebo neoprávněný přístup k počítačovému systému podle § 230 tr.zák.

1.4.11 Spamming

Jedná se o rozesílání nevyžádaných sdělení masově šířených internetem. Původně se používalo především pro nevyžádané reklamní e-maily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace (diskuzní fóra, komentáře). Většina spamu je rozesílána distribuovaně z počítačů napadených počítačovým virem nebo červem. Vir nebo červ často na počítači otevírá tzv. zadní vrátka (backdoor), která umožňují útočníkovi počítač dálkově ovládat a zneužít jej mj. pro rozesílání spamu. Většinou jde o jednání trestně nepostižitelné. Odpovědnost ve správním řízení vyplývá z ustanovení § 118 odst.1 písm.i) zák.čís. 127/2005 Sb., o elektronických komunikacích, podle něhož se za správní delikt považuje zaslání nevyžádané zprávy nebo zpráv třetím osobám bez souhlasu držitele adresy elektronické pošty. Mezi spamy lze zařadit **hoax**, což je nevyžádaná e-mailová zpráva, která buď vyvolává falešný

poplach, nebo se snaží pobavit, případně obsahuje prosbu o pomoc. Může naplňovat skutkovou podstatu tradičního trestného činu šíření poplašné zprávy podle § 357 tr.zák. nebo i jiného trestného činu (§ 184 pomluva, § 356 podněcování k nenávisti, § 365 schvalování trestního činu atd.) Znaky spamu naplňuje i tzv. **tzv. nigerijský dopis**, což je označení pro různé typy podvodných sdělení, která jsou rozesílána internetem formou e-mailových zpráv. Většinou obsahují příslib vysokého finančního podílu z určité majetkové či účetní operace a po prvotním navázání kontaktu následují další sdělení posléze vyúsťující v žádost o převod určité finanční částky na účet do zahraničí. Dopisy jsou nejčastěji zasílány právě z Nigérie, případně z JAR, Zimbabwe, či jiných afrických zemí.[45] Mohou naplnit skutkovou podstatu tradičního trestného podvodu podle § 209 tr.zák.

1.4.12 Cybersquatting, typosquatting

Jde o blokování internetových domén spočívající v registraci a následném užívání doménového jména[46] ve zlé víře na úkor obchodní značky, názvu anebo jména jiné osoby. Ve většině případů je na zaregistrovanou doménu umístěna reklama a nabídka k prodeji domény. Běžným jevem je i přímá nabídka odprodeje domény vlastníkovi, na jehož úkor byla doména registrována. Je-li zaregistrována doména podobná a tudíž zaměnitelná se známou registrovanou značkou, nazývá se takové jednání **typosquating**.[47] Většinou půjde o jednání jen obtížně trestně postižitelné. Dosáhne-li hranice trestnosti, budou naplněny znaky skutkové podstaty tradičních trestných činů - poškození cizích práv podle § 181 tr.zák. nebo porušení předpisů o pravidlech hospodářské soutěže podle § 248 tr.zák., případně porušení práv k ochranné známce a jiným označením podle § 268 tr.zák.

---

[45] V českých médiích proběhl v roce 2003 případ, kdy nigerijský dopis byl motivem vraždy. Vraždu spáchal lékař, který kvůli reakci na nigerijský dopis přišel o značné finanční prostředky, a když se nedomohl pomoci na nigerijském velvyslanectví v Praze, zastřelil nigerijského diplomata a postřelil sekretáře velvyslanectví.

[46] POLČÁK, Radim. *Internet a proměny práva*. Praha: Auditorium, 2012, 388 s. Téma (Auditorium). ISBN 978-80-87284-22-3: *"V současné době hodnotí doménová jména část naší doktríny jako jiné majetkové hodnoty, druhá část doktrinálních názorů společně s dominantní judikaturou je toho názoru, že se v případě doménových jmen jedná "jen" o formu výkonu subjektivních práv plynoucích ze smluv."*

[47] Přispěvatelé Wikipedie, Cybersquatting [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 16. 10. 2012, 04:49 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Cybersquatting&oldid=9164703>

1.4.13 Cyberstalking

Viz níže bod 3.2.10 výklad k trestnému činu nebezpečné pronásledování podle § 354 tr.zák.

1.4.14 Denigration (očerňování, zostuzování)

Pachatel e-mailem odesílá škodlivá, nepravdivá nebo krutá prohlášení o oběti jiným uživatelům nebo takovéto informace jiným způsobem zpřístupňuje na internetových stránkách.[48] Jednání může být postiženo jako trestný čin pomluvy podle 184 tr.zák.

1.4.15 Masquerade / Impersonatin (přetvářka / vydávání se za někoho jiného)

Pachatel se vydává za někoho jiného a zasílá škodlivý materiál jiným osobám s cílem očernit osobu, za kterou se vydává.[49] Takové jednání lze kvalifikovat jako tradiční trestný čin poškození cizích práv podle 181 tr.zák.

1.4.16 Outing (odhalování intimností)

Jde o zveřejnění nebo zaslání materiálů, které obsahují citlivé nebo intimní informace o oběti, včetně přeposílání soukromých zpráv a fotografií.[50] Jednání může naplnit znaky skutkové podstaty trestného činu neoprávněné nakládání s osobními údaji podle § 180 tr.zák. nebo trestného činu porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle 183 tr.zák.

1.4.17 Kybergrooming (svádění)

Termín označuje chování uživatele internetu, které má v dítěti vzbudit falešnou důvěru a připravit ho na schůzku, jejímž cílem je oběť pohlavně zneužít. Grooming v širším smyslu označuje více druhů manipulativního chování.[51] Většinou jde o jednání trestně

---

[48] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, 217 s. ISBN 978-807-3875-459.

[49] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, 217 s. ISBN 978-807-3875-459.

[50] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, 217 s. ISBN 978-807-3875-459.

[51] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, 217 s. ISBN 978-807-3875-459.

nepostižitelné; spíše výjimečně může být prokázán trestný čin svádění k pohlavnímu styku podle § 202 tr.zák.

1.5 Technologie útoků pachatelů kyberkriminality

Technické prostředky používané k průniku do počítačových systémů mohou mít charakter buď hardwarového nástroje anebo softwarového nástroje:[52]

1.5.1 Hardwarové nástroje

1.5.1.1 **Čtečka karet**

Slouží ke hledání bezpečnostních děr v čipových kartách a ke kopírování údajů z nich.

1.5.1.2 **Skener**

Prostřednictvím otevřených portů počítače zjišťuje informace o otevřených službách, které na počítači běží a o jeho operačním systému. Může být zabudován např. do USB konektoru nebo do jiné součástky počítačového hardware.

1.5.1.3 **Keylogger**

Je fyzicky zabudován buď přímo do klávesnice počítače, nebo jde o zařízení vložené mezi klávesnici a počítač. Lze jím odhalit hesla zadávaná před spuštěním operačního systému či zjišťovat další data vyťukávaná znaky na klávesnici. Ochranou proti němu je využití tzv. softwarové klávesnice.

1.5.2 Softwarové nástroje

1.5.2.1 **Malware**

[52] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

Jde o zákeřný počítačový program určený ke vniknutí do počítačového systému a k jeho poškození. Mnoho dřívějších nakažlivých programů vzniklo jako experiment nebo žert a většinou se záměrem vůbec neškodit nebo pouze obtěžovat. Mladí programátoři, kteří studovali možnosti virů a techniky jejich psaní, vytvářeli takové programy proto, aby ukázali své schopnosti nebo aby viděli, jak dalece se mohou jejich výtvory rozšířit. Větší hrozbu představují programy navržené tak, aby poškozovaly nebo zcela mazaly data. Pod souhrnné označení malware se zahrnují počítačové viry, červi, trojské koně, spyware a adware:[53]

- **Viry:** Jde o program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“). Viry se na rozdíl od červů samy šířit nemohou.[54]
- **Červi:** Obdobně jako u virů jde o specifický počítačový program, který je schopen automatického rozesílání kopií sebe sama na jiné počítače. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření.[55]

---

[53] Přispěvatelé Wikipedie, Malware [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 20. 02. 2013, 16:27 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Malware&oldid=9764872>

[54] Přispěvatelé Wikipedie, Počítačový virus [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 20. 02. 2013, 15:01 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus&oldid=9764515>

[55] Přispěvatelé Wikipedie, Počítačový červ [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 2. 12. 2012, 16:32 UTC, [citováno 2. 03. 2013]

– **Trojské koně:** Jedná se o uživateli skryté části programu nebo aplikace se škodlivou funkcí. Trojský kůň může být samostatný program, který se tváří užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Někdy se trojský kůň vydává za program k odstraňování malware (dokonce jako takový může fungovat a odstraňovat konkurenční malware). Tato funkčnost slouží ale pouze jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá. V Microsoft Windows může trojský kůň využít toho, že řada programů včetně systémového správce souborů (exploreru) skrývá přípony souborů. Vypadá pak jako soubor s obrázkem, zvukem, archivem nebo čímkoliv jiným, přestože se ve skutečnosti jedná o spustitelný kód. Chce-li uživatel obrázek kliknutím zobrazit, je ve skutečnosti spuštěn trojský kůň. Trojský kůň může být přidán i do stávající aplikace a následně je upravená verze šířena například pomocí peer-to-peer sítí nebo warez serverů. Uživatel stažením kopie aplikace (nejčastěji bez platné licence nebo jako volně šířený program z nedůvěryhodného serveru) může získat pozměněnou kopii aplikace obsahující část programového kódu trojského koně dodaného třetí stranou. Rozdíl mezi počítačovým virem a trojským koněm spočívá v tom, že trojský kůň nedokáže sám infikovat další počítače nebo programy svojí kopií. Existují však počítačoví červi, které na napadeném počítači instalují různé trojské koně nebo vytvářejí trojské koně z programů, které se v napadeném systému nacházejí.[56]

– **Spyware:** Jedná se o program, který využívá internetu k odesílání dat z napadeného počítače bez vědomí jeho uživatele. Spyware představuje z hlediska bezpečnosti dat velkou hrozbu, protože odesílá různé informace (historii navštívených stránek, hesla) určenému uživateli, který tyto informace dále zpracovává. Někteří autoři spyware se hájí, že jejich program odesílá pouze data typu přehledu navštívených stránek či nainstalovaných programů za účelem zjištění potřeb nebo zájmů uživatele a s cílem tyto informace využít pro cílenou reklamu. Existují ale i spyware odesílající hesla a čísla kreditních karet nebo

<http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv&oldid=9375426>

[56] Přispěvatelé Wikipedie, Trojský kůň (program) [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 31. 01. 2013, 23:15 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Trojsk%C3%BD_k%C5%AF%C5%88_(program)&oldid=9669630>

spyware fungující jako zadní vrátka, tzv. **backdoors**, které po instalaci na napadený počítač umožňují jeho vzdálené řízení. Mezi spyware patří i tzv. softwarový **keylogger**, který skrytě sleduje znaky stištěné na klávesnici. Spyware se může šířit i prostřednictvím sítě peer-to-peer umožňující stahování hudby a videa od ostatních uživatelů.[57]

– **Adware:** Jde o program, jehož cílem je předání reklamního sdělení uživateli. Narozdíl od spyware se instaluje do počítače se souhlasem uživatele, nicméně kvůli určité reklamní aplikaci ztěžuje práci a obtěžuje. Reklamní aplikace mohou mít různý stupeň agresivity - od běžných bannerů až po neustále vyskakující pop-up okna nebo ikony v oznamovací oblasti. Programy obsahující adware na rozdíl od spyware neshromažďují tajně informace a neodesílají je přes internet bez souhlasu uživatele.[58]

1.5.2.2 Prolamovače hesel (Password crackers)

Jde o programy, které za pomoci nejrůznějších kombinací slov, znaků, písmen a čísel zkoušejí prolomit ochranu statických hesel. Postupně generují buď všechna ve vlastní databázi uložená slova (dictionary attack) anebo všechny v úvahu přicházejí znaky, písmena a číslice (brutte-force attack), a to s rychlostí až milionu znaků za vteřinu.[59]

1.5.2.3 Rootkity

Jde o speciální software, který maskuje svou přítomnost v počítači a dokáže se velmi dobře schovávat i před antivirovými programy. Využívá zranitelná místa operačních systémů a slouží pro skrývání činností prováděných bez souhlasu uživatele na operačním systému.[60]

---

[57] Přispěvatelé Wikipedie, Spyware [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 30. 01. 2013, 08:31 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Spyware&oldid=9661422>

[58] Přispěvatelé Wikipedie, Adware [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 18. 02. 2013, 11:28 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Adware&oldid=9752635>

[59] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[60] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

2 Systematizace kybernetických trestných činů

Při systémovém členění kybernetických trestných činů do různých kategorií a skupin lze použít různorodá **kriteria:**

2.1 Podle způsobu využití informačně-komunikačních technologií

V nejobecnější rovině jsou kybernetické trestné činy z hlediska využití informačně-komunikačních technologií děleny do dvou skupin na:

a) trestné činy směřující **proti** informačně-komunikačním technologiím (ICT), kdy je ICT přímo terčem útoku,

b) trestné činy spáchané **s využitím** počítačů, kdy informačně komunikační technologie je nástrojem ke spáchání trestného činu.[61]

Obdobou je dělení kybernetických trestných činů do tří skupin, vycházející ze samotné definice kybernetického trestného činu:

a) trestné činy **proti** informačně-komunikačním technologiím;

b) trestné činy, u nichž jsou informačně-komunikační technologie využity jako **nástroj** ke spáchání tradičního trestného činu;

c) trestné činy vztahující se k **obsahu** počítačových dat.[62]

Další možnou kategorizací kybernetických trestných činů, se kterou se lze setkat v odborné literatuře, je jejich dělení na tyto dvě skupiny:

a) **"tradiční"** protiprávní jednání, kde počítač pouze usnadňuje spáchání určitého trestného činu, ať už je jejich terčem (on-line krádež v bance) nebo pouze jejich nástrojem (např. šíření pornografie)

---

[61] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[62] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

b) **"nová"** protiprávní jednání, která se objevila až s nástupem moderních informačních technologií, ať už směřující proti ICT (např. hacking), či používající počítač v roli nástroje (např. cracking).[63]

2.2 Podle druhového objektu vymezeného v Úmluvě

Úmluva definovala znaky skutkových podstat devíti kybernetických trestných činů, které v devíti článcích rozdělila do čtyř skupin podle druhového objektu:

1) TRESTNÉ ČINY PROTI DŮVĚRNOSTI, INTEGRITĚ A DOSTUPNOSTI POČÍTAČOVÝCH DAT A SYSTÉMŮ:
čl. 2 - protiprávní přístup
čl. 3 - protiprávní zachycení informací
čl. 4 - zásah do dat
čl. 5 - zásah do systému
čl. 6 - zneužití zařízení

2) TRESTNÉ ČINY SOUVISEJÍCÍ S POČÍTAČI:
čl. 7 - falšování údajů související s počítači
čl. 8 - podvod související s počítači

3) TRESTNÉ ČINY SOUVISEJÍCÍ S OBSAHEM:
čl. 9 - trestné činy související s dětskou pornografií

4) TRESTNÉ ČINY SOUVISEJÍCÍ S PORUŠENÍM AUTORSKÉHO PRÁVA A PRÁV PŘÍBUZNÝCH AUTORSKÉMU PRÁVU:
čl. 10 - trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Toto rozdělení se ovšem nejeví jako optimální pro rozbor a výklad kybernetických trestných činů upravených trestním zákoníkem, neboť by vedlo k **znepřehlednění jednotlivých kybernetických trestných činů podle trestního zákoníku**. Např. trestný čin neoprávněný přístup k počítačovému systému a nosiči

[63] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

informací podle § 230 tr.zák. zahrnuje ve své skutkové podstatě znaky dokonce pěti jednání (pěti článků) podle Úmluvy:

- § 230 odst.l tr.zák. odpovídá čl. 2 Úmluvy - neoprávněný přístup k počítačovému systému nebo jeho části;
- § 230 odst.2 písm. a), b), d) tr.zák. odpovídá čl. 4 a čl. 5 Úmluvy - zásah do dat nebo do počítačového systému;
- § 230 odst.2 písm. c) tr.zák. odpovídá čl. 7 Úmluvy - falšování údajů související s počítači;
- § 230 odst. 3 písm. a) tr.zák. odpovídá čl. 8 Úmluvy - podvod související s počítači;
- § 230 odst.3 písm. b) tr.zák. odpovídá čl. 5 Úmluvy - zásah do systému.[64]

2.3 Podle druhového objektu vymezeného v trestním zákoníku

Kriteriem pro rozdělení kybernetických trestných činů do jednotlivých skupin může být druhový objekt, který je použit pro členění trestných činů v trestním zákoníku (v celkem třinácti hlavách), z nichž kybernetické trestné činy (tj. trestné činy s kybernetickým znakem ve skutkové podstatě) jsou obsaženy v těchto hlavách:

- v HLAVĚ II - TRESTNÉ ČINY PROTI SVOBODĚ A PRÁVŮM NA OCHRANU OSOBNOSTI, SOUKROMÍ A LISTOVNÍHO TAJEMSTVÍ:

§ 180 neoprávněné nakládání s osobními údaji
§ 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

- v HLAVĚ V - TRESTNÉ ČINY PROTI MAJETKU:

§ 230 neoprávněný přístup k počítačovému systému a nosiči informací
§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

[64] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

§ 232 poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

- v HLAVĚ VI - TRESTNÉ ČINY HOSPODÁŘSKÉ

§ 234 neoprávněné opatření, padělání a pozměnění platebního prostředku

§ 236 výroba a držení padělatelského náčiní

§ 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

- v HLAVĚ VII - TRESTNÉ ČINY OBECNĚ NEBEZPEČNÉ

§ 287 šíření toxikomanie

- v HLAVĚ IX - TRESTNÉ ČINY PROTI ČR, CIZÍMU STÁTU A MEZINÁRODNÍ ORGANIZACI

§ 311 teroristický útok

- v HLAVĚ X - TRESTNÉ ČINY PROTI POŘÁDKU VE VĚCECH VEŘEJNÝCH

§ 345 křivé obvinění

§ 348 padělání a pozměnění veřejné listiny

§ 354 nebezpečné pronásledování

§ 355 hanobení národa, rasy, etnické nebo jiné skupiny osob

§ 356 podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod

- v HLAVĚ XIII - TRESTNÉ ČINY PROTI LIDSKOSTI, PROTI MÍRU A VÁLEČNÉ TRESTNÉ ČINY

§ 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka

§ 407 podněcování útočné války

Jelikož do budoucna lze očekávat průnik kybernetických zločinů do skutkových podstat dalších (nyní standardních) trestných činů, jeví se systematizace kybernetických trestných činů podřizující se systematizaci trestního zákoníku jako nejpřehlednější s potenciálem do budoucna.

2.4 Podle důležitosti kybernetického znaku

Já sama v této diplomové práci, která je rozsahem omezena a měla by zdůraznit především "ryzí" kybernetické trestné činy, používám pro rozdělení do skupin jako kritérium stupeň důležitosti kybernetického znaku (jímž rozumím využití či zasažení informačně-komunikační technologie) ve skutkové podstatě toho kterého trestného činu a dospívám k tomuto dělení:

a) absolutně kybernetické trestné činy (ryzí kybernetické trestné činy), u nichž jsou znaky skutkové podstaty charakterizující objekt, objektivní stránku a subjekt vymezeny tak, že nemohou být spáchány jinak než za využití, resp. zasažení informačně-komunikačních technologií. Jde o tyto tři trestné činy:
- § 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

b) relativně kybernetické trestné činy obsahující v základní skutkové podstatě kybernetický znak (tj. využití, resp. zasažení informačně-komunikačních technologií). Jde o trestné činy, jejichž skutkové podstaty jsou vymezeny tak, že mohou být naplněny i jinak než využitím či zasažením informačně-komunikačních technologií. Za kybernetické trestné činy je lze označit pouze v určitých případech. Užití informačně-komunikačních technologií je toliko jedním z možných znaků základní skutkové podstaty. Jedná se o těchto 10 trestných činů:
§ 182 porušení tajemství dopravovaných zpráv
§ 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
§ 191 šíření pornografie,
§ 192 výroba a jiné nakládání s dětskou pornografií
§ 234 neoprávněné opatření, padělání a pozměnění platebního prostředku
§ 236 výroba a držení padělatelského náčiní

§ 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

§ 311 teroristický útok

§ 348 padělání a pozměnění veřejné listiny

§ 354 nebezpečné pronásledování

c) relativně kybernetické trestné činy obsahující kybernetický znak nikoli v základní skutkové podstatě, nýbrž toliko jako okolnost podmiňující použití vyšší trestní sazby (okolnost zvlášť přitěžující). Jedná se o těchto osm trestných činů:

§ 180 neoprávněné nakládání s osobními údaji

§ 184 pomluva

§ 287 šíření toxikomanie

§ 345 křivé obvinění

§ 355 hanobení národa, rasy, etnické nebo jiné skupiny osob

§ 356 podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod

§ 403 založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka

§ 407 podněcování útočné války

3 Kybernetické trestné činy podle trestního zákoníku

3.1 Absolutně kybernetické trestné činy

Jedná se o ryzí kybernetické trestné činy, u nichž jsou znaky skutkové podstaty charakterizující objekt, objektivní stránku a subjekt vymezeny tak, že nemohou být spáchány jinak než za využití, resp. zasažení informačně-komunikačních technologií. Jde o tyto tři trestné činy:

3.1.1 § 230 trestního zákoníku - Neoprávněný přístup k počítačovému systému a nosiči informací

a) Neoprávněný přístup - § 230 odst. 1 tr.zák. :

Chráněným zájmem (objektem) je ochrana důvěrnosti počítačových dat a počítačového systému před ohrožením jejich bezpečnosti.[65] Z hlediska dosavadní obecné kriminality jde o obdobnou situaci jako při neoprávněném vstupu do cizího obydlí, kdy je chráněno soukromí člověka ve vlastním obydlí (trestný čin porušování domovní svobody podle § 178 tr.zák.). V Úmluvě je tento trestný čin vymezen v čl. 2 - Protiprávní přístup.

Vymezená skutková podstata z hlediska znaků charakterizujících objektivní stránku postihuje jakékoliv jednání spočívající v porušení bezpečnostního opatření počítačového systému, jehož následkem je získání neoprávněného přístupu k tomuto systému nebo k jeho části. K trestnosti takového jednání tedy dostačuje pouhé neoprávněné **vniknutí** do počítačového systému (i z pouhé zvědavosti), které pachateli umožní využití informačního obsahu nebo volnou dispozici s počítačovým systémem. Není nutné, aby pachatel do takto napadeného („nabouraného“) počítače jakýmkoliv dalším způsobem dále zasahoval, získával z takového počítače data, mazal je apod. Podmínkou trestnosti je ovšem **překonání bezpečnostního opatření**, které si Česká

[65] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

republika prohlášením podle čl. 40 Úmluvy zachovala jako znak k omezení rozsahu trestnosti. Pojem *bezpečnostní opatření* není ve výkladových ustanoveních trestního zákoníku (hlava VIII, § 110 až § 139) nijak vymezen. V odborné literatuře je definován jako jakékoliv opatření, které může průnik do počítačového systému ztížit a jehož cílem je zabránit volnému přístupu, přičemž na míře zabezpečení nezáleží.[66] Může se jednat například o zabezpečovací software, hardware, užívání vstupních a bezpečnostních hesel, o systém vymezení uživatelských práv, ale i o zavedený režim užívání počítačových systémů na pracovišti a přístup k nim a k jejich částem, zajištění místnosti s počítačovým systémem pomocí technických zařízení apod. Bezpečnostním opatřením mohou být taktéž možnosti operačního systému počítače bránit neoprávněným průnikům a ovládání počítače prostřednictvím sítě internet, nastavení integrovaného firewallu, který je schopen zamezit ukládání škodlivých programů na pevný disk počítače, apod.[67] V trestní praxi může výklad pojmu *bezpečnostní opatření* přinášet řadu problémů, které při neexistující judikatuře nebudou vždy jednoznačně řešitelné. Např. Volevecký považuje ve svém článku "Úmluva o kybernetické kriminalitě a neoprávněný zásah do počítačového systému" zveřejněném v časopisu Bezpečnostní teorie a praxe 2/2010[68] za sporné, *"zda lze za bezpečnostní opatření označit i instalaci takového počítačového programu, který je schopen pouze detekovat útoky na počítačový systém, avšak nikoliv jim bránit"*. Obdobně by mohlo být otázkou, zda lze pod pojem bezpečnostní opatření zařadit i monitorovací kamerový systém na počítačovém pracovišti. Podle mého názoru vniknutí do počítače skrytě chráněného programem toliko detekujícím či monitorujícím útok nemůže k naplnění skutkové podstaty tohoto trestného činu stačit, neboť i z hlediska subjektivního vnímání pachatele (z hlediska zavinění) musí být naplněn znak ***překonání,*** což nutně musí vyžadovat alespoň minimální úsilí pachatele. Pokud ovšem pachatel úmyslně vyřadí z provozu monitorovací kamerový systém na počítačovém pracovišti (byť jen zakrytím objektivu kamery), bylo by možno i takové jednání považovat za *překonání*

[66] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[67] VOLEVECKÝ, Petr. Úmluva o kybernetické kriminalitě a neoprávněný zásah do počítačového systému. *Bezpečnostní teorie a praxe = Security theory and practice / Policejní akademie České republiky*. roč. 2010, č. 2. ISSN 1801-8211.

[68] VOLEVECKÝ, Petr. Úmluva o kybernetické kriminalitě a neoprávněný zásah do počítačového systému. *Bezpečnostní teorie a praxe = Security theory and practice / Policejní akademie České republiky*. roč. 2010, č. 2. ISSN 1801-8211.

bezpečnostního opatření. I když ve většině případů bude mít bezpečnostní opatření svůj původ v samotném počítači, do něhož se pachatel "nabourává", ze samotného vymezení skutkové podstaty to nevyplývá. Pak by ovšem bylo nutno považovat za *překonání bezpečnostního opatření* i např. otevření paklíčem uzamčené místnosti s jinak nezajištěným počítačem. Při absolvování studijní praxe u soudu jsem byla konfrontována s latentními formy této počítačové kriminality odehrávající se mezi rozvádějícími se manžely, kteří si navzájem vnikají do e-mailové korespondence za účelem prokázání nevěry druhého. V té souvislosti se nabízí otázka, zda je *překonáním bezpečnostního opatření* proniknutí do soukromé e-mailové korespondence manžela při využití hesla, které není mezi manžely utajováno. Podle mého úsudku by o ***překonání*** *bezpečnostního opatření* nešlo, neboť *překonání* musí již pojmově vyžadovat úsilí větší než nepatrné intenzity.

Trestní zákoník ve svých výkladových ustanoveních neobsahuje ani výklad pojmu *počítačový systém,* který je jedním ze znaků objektivní stránky. Úmluva jej definuje jako jakékoli zařízení nebo skupinu vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Současně Úmluva vymezuje i ostatní nezbytné pojmy - *počítačová data, poskytovatel služeb, provozní data*. Podpůrně lze při hledání obsahu pojmu *počítačový systém* použít ČSN 369001, která sice nedefinuje přímo pojem počítačový systém, ale definuje pojem *počítač* jako *„stroj na zpracování dat provádějící samočinně posloupnosti různých aritmetických a logických operací“.*[69] *Počítačový systém* sestává z technického zařízení (hardware) a programového vybavení (software), které je určeno ke zpracování digitálních dat. Většinou jej tvoří vícero zařízení, označovaných jako základní zpracovávací jednotka a periferní zařízení (tiskárna, monitor, čtecí či zapisovací zařízení). Více počítačových systémů navzájem propojených tvoří *síť.* Internet je globální síť sestávající z mnoha navzájem propojených sítí, které používají tytéž protokoly.[70]

[69] VOLEVECKÝ, Petr. Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2009, č. 4. ISSN 1211-2860.

[70] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

Způsobení škody či jiné újmy není znakem základní skutkové podstaty podle odstavce prvého § 230 tr.zák.; je až okolností podmiňující použití vyšší trestní sazby podle odstavce třetího, čtvrtého a pátého. V odstavci třetím je formulována kvalifikovaná skutková podstata, k jejímuž naplnění je třeba specifického úmyslu pachatele, a to pod písm.a) úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, pod písm.b) úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Až v odstavcích čtvrtém a pátém je znakem skutkové podstaty **výše** způsobené škody. (U odstavce třetího znak v podobě *úmyslu způsobit jinému škodu nebo jinou újmu*, resp. *v úmyslu získat sobě nebo jinému neoprávněný prospěch*, neobsahuje žádnou konkrétní výši škody, resp. prospěchu, který ostatně může být i imaterielní.) Vedle výše způsobené škody jsou dalšími okolnostmi podmiňujícími použití vyšší trestní sazby podle odstavce čtvrtého členství pachatele v organizované skupině, zisk stanoveného prospěchu a způsobení vážné poruchy v činnosti právnické osoby, fyzické osoby - podnikatele nebo orgánu veřejné moci. Vyjma členství v organizované skupině, k němuž je vyžadováno zavinění úmyslné, dostačuje k naplnění dalších znaků zavinění nedbalostní.

b) Neoprávněné nakládání s daty - § 230 odst.2 tr.zák:

Předmětem ochrany je integrita a dostupnost počítačových dat a počítačových systémů před neoprávněnými zásahy, jež mohou mít vliv na existenci, kvalitu a správnost dat, a před jejich neoprávněným užíváním. Ochrana počítačového systému, nosičů informací a dat představuje individuální objekt; sekundárně jsou tímto zákonným ustanovením chráněny i další zájmy, například projevy osobní povahy, obchodní vztahy, autorská díla, atd.[71] Z hlediska obecné kriminality jde u § 230 odst.2 písm.a/ o obdobu trestného činu krádeže podle § 205 tr.zák., u § 230 odst.2 písm.b/,d/, odst.3 písm.b) o obdobu trestného činu poškození cizí věci podle § 228 tr.zák., u § 230 odst.2 písm.c/ o obdobu trestného činu padělání a pozměnění veřejné listiny podle § 348 nebo neoprávněné opatření, padělání a pozměnění platebního prostředku podle §

[71] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

234 tr.zák. a u § 230 odst.3 písm.a/ o obdobu trestného činu podvodu podle § 209 tr.zák. V Úmluvě je skutková podstata tohoto trestného činu naplňující znaky podle odst.2 písm.a),b),d), odst.3 písm.b) vymezena v čl. 4 - Zásah do dat a v čl. 5 - Zásah do systému; skutková podstata naplňující znaky podle odst.2 písm.c) v čl. 7 - Falšování údajů související s počítači; skutková podstata naplňující znaky podle odst.3 písm.a) v čl. 8 - Podvod související s počítači.

Na rozdíl od skutkové podstaty podle odstavce prvého § 230 může být předmětem útoku pachatele nejen počítačový systém, nýbrž i **nosič informací.** Nosičem informací se rozumí jakýkoli nosič dat v informační technice, ať již na magnetickém principu (disketa, pevný disk, magnetooptický disk, magnetická páska), optickém principu (CD, DVD, Blu-Ray, HD DVD) či elektronickém principu (USB flash disk, paměťové karty - Secure Digital, Multimedia Card, Memory Stick, xD-Picture Card). Neelektronické datové nosiče pro psaní a kreslení, ruční či strojové (papír, tabule, fotopapír) ani zvukový magnetofonový záznam či obrazový videozáznam na nosiči VHS či BETA nelze za nosiče informací ve smyslu znaku dané skutkové podstaty považovat.[72]

Oproti skutkové podstatě podle odstavce prvého není znakem objektivní stránky *překonání bezpečnostního opatření* při vniknutí, nýbrž další (závažnější) jednání vymezené pod písmeny a) až d), které lze zjednodušeně souhrnně označit jako **neoprávněné nakládání** s daty uloženými v počítačovém systému nebo na nosiči informací. Trestného činu se dopustí pachatel, který získá - byť i oprávněný či jen náhodný - přístup k počítačovému systému nebo nosiči informací a zároveň naplní alespoň jednu z těchto čtyř dalších okolností uvedených v odstavci druhém pod písm. a) až d):

ad a) **Neoprávněné užití dat:**

Toto jednání zahrnuje jakoukoli nepovolenou manipulaci s daty uloženými v počítačovém systému nebo na nosiči ve prospěch pachatele či jiné s ním spřízněné osoby. Tento znak je naplněn i jen pouhým zkopírování dat bez souhlasu oprávněné

[72] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

osoby, aniž by muselo následovat využití dat. Někdy bývá toto jednání označováno jako ***počítačová špionáž.***

ad b) **Destrukce dat:**

Vymazání nebo jiné zničení, poškození, změna, potlačení, snížení kvality dat nebo učinění je neupotřebitelnými obsahuje taxativní výčet veškerých destruktivních jednání vůči datům, které bývá označováno jako ***počítačová sabotáž***. Tohoto jednání se pachatel může dopustit buď primitivní destrukcí samotného hardwarového (technického) zařízení počítače či nosiče dat nebo sofistikovaným napadením jeho softwarového (programového) vybavení. K zásahům do programového vybavení počítače se často používá škodlivého softwaru – malware, mezi něž patří viry, červy, trojské koně a spyware.

ad c) **Falšování dat:**

Falšováním se rozumí jednání spočívající v padělání nebo pozměnění dat se specifickým (druhotným) úmyslem pachatele, aby padělaná či pozměněná data byla považována za pravá nebo aby s nimi jako pravými bylo jednáno.

ad d) **Neoprávněné vložení dat:**

Toto jednání je obdobou počítačové sabotáže. Trestné je zde neoprávněné vložení dat do počítače, nebo jiný zásah do jeho hardwaru nebo softwaru.[73]

Způsobení škody či jiné újmy není znakem základní skutkové podstaty podle odstavce druhého § 230 tr.zák.; je až okolností podmiňující použití vyšší trestní sazby podle odstavce třetího, čtvrtého a pátého. V odstavci třetím je formulována kvalifikovaná skutková podstata, k jejímuž naplnění je třeba specifického úmyslu pachatele, a to pod písm.a) úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, pod písm.b) úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat. Až v odstavcích čtvrtém a pátém je znakem skutkové podstaty **výše** způsobené škody. (U odstavce třetího znak v podobě *úmyslu způsobit jinému škodu nebo jinou újmu*, resp. *v úmyslu získat sobě nebo jinému neoprávněný prospěch*, neobsahuje žádnou

[73] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

konkrétní výši škody, resp. prospěchu, který ostatně může být i imaterielní.) Jelikož jednání kvalifikované v § 230 odst.2 písm.a) je obdobou trestného činu krádeže a jednání kvalifikované v § 230 odst.3 písm.a) obdobou trestného činu podvodu (čl. 8 Úmluvy - Podvod související s počítači), lze souhlasit s argumentací autorů Gřivny a Polčáka v publikaci *Kyberkriminalita a právo*[74], že neexistuje důvod, aby jednání pachatele kvalifikované podle odstavce 4, při němž byla způsobena škoda značná či získán značný prospěch, a podle odstavce 5, při němž byla způsobena škoda velkého rozsahu či získán takový prospěch, ohrožovalo pachatele nižší trestní sazbou než v případě spáchání trestného činu krádeže podle § 205 či podvodu podle § 209 tr.zák. Řešením je možnost kvalifikace takového jednání jako souběh trestného činu podle § 230 odst.2 písm.a) tr.zák. s trestným činem podle § 205 (bude-li prokázán znak *přisvojení si cizí věci*) a trestného činu podle § 230 odst.3 písm.a) tr.zák. s trestným činem § 209 tr.zák. (bude-li naplněn znak *uvedení někoho v omyl*). [75] [76] V této souvislosti je třeba zmínit ustanovení § 120 tr.zák., podle něhož 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.

3.1.2 § 231 trestního zákoníku - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

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

[74] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

[75] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[76] GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4..

počítačovému systému a nosiči informací podle § 230 odst.1,2.[77] V obecné rovině lze tento trestný čin podřadit přípravě trestného jednání podle 20 tr.zák., která je ovšem trestná jen v případě zvlášť závažných zločinů (§ 14 odst.3). V Úmluvě je tento trestný čin vymezen v čl. 6 - Zneužití zařízení.

Tato skutková podstata kriminalizuje jednání, které časově předchází získání či vyzrazení dopravovaných zpráv, spočívající v nakládání či přechovávání přístupového zařízení nebo hesla k počítačovému systému. Důvodem je zvýšení a posílení ochrany vybraným zájmům (počítačovým datům a přepravovaným informacím) požívající "standardní" ochrany trestním zákonem.

Vymezená skutková podstata z hlediska znaků charakterizujících subjektivní stránku obsahuje specifický úmysl pachatele spáchat jiný **taxativně vymezený** trestný čin. Samotné jednání, které po objektivní stránce naplňuje znaky skutkové podstaty (prodej či zpřístupňování různých prolamovačů hesel), není trestné, není-li **současně** prokázán tento specifický úmysl pachatele 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. Jednání pachatele naplňující sice znaky objektivní stránky, avšak činěné v úmyslu spáchat jiný trestný čin, nemůže být postiženo podle tohoto ustanovení, ale může být kvalifikováno jako příprava či pokus jiného trestného činu, k jehož dokonání směřuje.

Prostředky, které jsou předmětem neoprávněného nakládání, mohou být buď přístupová zařízení vytvořená nebo přizpůsobená k dosažení neoprávněného přístupu, nebo hesla, kódy, data, za jejichž pomoci lze přístup získat. Nejfrekventovanějším přístupovým zařízením bývá čtečka bankovních karet, mezi prolamovače hesel patří počítačové programy ve formě trojských koní, červů, keylogeru apod.

[77] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

3.1.3 § 232 trestního zákoníku - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Objektem je ochrana dat a technického či programového vybavení počítače nebo jiného technického zařízení pro zpracování dat před hrubým nedbalostním jednáním, pokud takovým jednáním byla způsobena značná škoda. Z hlediska obecné kriminality jde o postih obdobného jednání jako při spáchání trestného činu poškození a ohrožení provozu obecně prospěšného zařízení z nedbalosti podle § 277 tr.zák., u něhož ovšem není znakem základní skutkové podstaty způsobení škody a škoda velkého rozsahu je až ve druhém odstavci okolností podmiňující použití vyšší trestní sazby. V Úmluvě tento trestný čin obsažen není.

Vymezená skutková podstata z hlediska znaků charakterizujících objektivní stránku postihuje jednání spočívající v porušení povinností ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté, jímž byla destruována či pozměněna data v počítačovém systému nebo na nosiči, anebo jím byl učiněn zásah do hardwaru nebo softwaru počítače. Podmínkou trestnosti je minimální výše způsobené škody 500.000 Kč (značná škoda); zvlášť přitěžující okolností podle odstavce druhého je způsobení škody nejméně 5.000.000 Kč (škoda velkého rozsahu).

K naplnění subjektivní stránky vyžaduje zákon **hrubou nedbalost**, která je v § 16 odst.2 definována jako přístup pachatele k požadavku náležité opatrnosti svědčící o jeho zřejmé ***bezohlednosti*** k zájmům chráněným trestním zákonem. Většinou se bude jednat o nedbalost vědomou (zřejmě hraničící s nepřímým úmyslem, tak jak je tomu při projevu ***lhostejnosti*** pachatele k chráněným zájmům[78]), byť – výjimečně či spíše jen teoreticky - může jít i o nedbalost nevědomou. Zřejmá bezohlednost je totiž ve zřejmém protikladu s nevědomostí pachatele, že může způsobem uvedeným v trestním zákoně porušit zájem takovým zákonem chráněný, na čemž nemůže příliš změnit fakt, že to vědět měl a mohl. Naopak to, že pachatel věděl o možných následcích, ale bez

[78] nález Ústavního soudu sp.zn. III.ÚS 722/09 ze dne 7.1.2010

přiměřených důvodů spoléhal, že je nezpůsobí (nedbalost vědomá), vyjadřuje již samo o sobě určitý stupeň (míru) jeho bezohlednosti. Pojem "**bez-ohlednosti"** přece znamená, že pachatel **nebere ohledy** na zájmy chráněné trestním zákonem, což předpokládá jeho vědomost o možných následcích.

3.2 Relativně kybernetické trestné činy s kybernetickým znakem v základní skutkové podstatě

Jedná se o potencionální kybernetické trestné činy, které **v základní** skutkové podstatě obsahují jako znak využití, resp. zasažení informačně-komunikačních technologií, avšak skutková podstata takových trestných činů může být naplněna i jinak než využitím či zasažením informačně-komunikačních technologií. Užití informačně-komunikačních technologií je tak jen jedním z možných znaků základní skutkové podstaty. Jde o těchto 10 trestných činů:

3.2.1 § 182 trestního zákoníku - Porušení tajemství dopravovaných zpráv

a) Porušení tajemství - § 182 odst. 1 písm.b), c) tr.zák. :

Chráněným zájmem (objektem) je ochrana práva na soukromí datové komunikace, kterou v obecné netrestní rovině garantuje čl. 13 Listiny základních práv a svobod. Z hlediska obecné kriminality jde o postih obdobného jednání jako při spáchání trestného činu porušení tajemství dopravovaných zpráv podle § 182 odst.1 písm.a) tr.zák. V podstatě jde o rozšíření tohoto tradičního trestného činu, vztahujícího se na listinnou (telegrafickou, telefonickou) zprávu přepravovanou poštou či jinou dopravní službou, o zprávy dopravované prostřednictvím sítě elektronických komunikací. V Úmluvě je tento trestný čin vymezen v čl. 3 - Protiprávní zachycení informací.

Trestný čin podle této skutkové podstaty je dokonán již v okamžiku zachycení zprávy v síti elektronických komunikací, aniž by se pachatel seznámil s obsahem takové přepravované zprávy. Stejně tak pro vznik trestní odpovědnosti není nutné, aby pachatel zprávě rozuměl. Naopak podmínkou pro vznik trestní odpovědnosti je to, že musí jít o porušení tajemství zprávy dopravované, tedy ještě nedoručené. Za doručenou zprávu je možné považovat například doručený email, SMS či MMS zprávu doručenou na mobilní telefon, a to i tehdy, jestliže se s obsahem těchto zpráv adresát ještě neseznámil. Toto ustanovení tedy nechrání zprávy již dopravené.[79] Pokud jsou dopravené zprávy uchovávány v soukromí, vztahuje se na jejich ochranu ust. § 183 tr.zák. Jestliže v soukromí uchovávány nejsou, požívají již jen netrestní ochrany podle ustanovení na ochranu osobnosti podle § 11 občanského zákoníku.

Účastníkem elektronické komunikace je každý, kdo uzavřel se subjektem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb. Uživatelem je ten, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací. Sítí elektronických komunikací jsou míněny přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, které umožňují přenos signálu po vedení, rádiem, optickým kabelem 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. Datová zpráva v nejširším slova smyslu je v podstatě jakákoliv zpráva přenášená v podobě dat. Textová zpráva je zpráva přenášená v podobě textového sdělení, například text emailové zprávy, SMS zpráva, komunikace v podobě programu ICQ, QUIP, chat v aplikaci FACEBOOK apod. Hlasová zpráva je zpráva přenášená v podobě záznamu hlasu člověka. Půjde zejména o telekomunikační proces pomocí telefonu, programu SKYPE apod. Zvuková zpráva je potom jakákoliv zpráva v podobě záznamu zvuku, z tohoto úhlu pohledu je zvuková zpráva pojmem širším než zpráva hlasová. Obrazová zpráva je jakýkoliv obrazový záznam, včetně přenosu on-line, přenášený v síti

[79] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

elektronických komunikací. Může jít o fotografii, malbu, filmovou sekvenci, MMS zprávu apod. [80]

b) Prozrazení nebo využití tajemství - § 182 odst. 2 tr.zák. :

Chráněným zájmem zde již není přepravovaná zpráva, ale vlastní tajemství, které je obsahem přepravované zprávy. Z hlediska objektivní stránky spočívá jednání právě v prozrazení nebo využití takového tajemství, o němž se pachatel v zákoně uvedeným způsobem dozvěděl.

Pachatel *prozradí* tajemství, jestliže jej sdělí jakýmkoliv způsobem další osobě. *Využitím* tajemství se rozumí uplatnění znalosti tajemství jakýmkoliv způsobem s tím, že toto jednání směřuje ke způsobení škody jinému nebo opatření neoprávněného prospěchu pachateli či jinému.

Z hlediska subjektivní stránky je vyžadován úmysl přímý, neboť podle dikce zákona pachatel musí prozradit nebo využít tajemství ve snaze způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch. Prozrazení tajemství bez tohoto specifického úmyslu nebude trestně postižitelné podle tohoto ustanovení, a to ani tehdy, jestliže jinému bude škoda skutečně způsobena.[81]

Z hlediska kybernetické trestné činnosti je významný též odstavec pátý skutkové podstaty tohoto trestného činu. Zde se nachází kvalifikovaná skutková podstata, ve které je okolností zvlášť přitěžující jiná skutečnost rozvíjející znak subjektu, jímž je zde zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti.

---

[80] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

[81] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

3.2.2 § 183 trestního zákoníku - Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

Toto ustanovení – na rozdíl od předchozí skutkové podstaty § 182 - chrání tajemství již doručené listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného. Znaky objektivní stránky jsou naplněny tím, že pachatel zveřejní, zpřístupní další osobě nebo jiným způsobem použije tajemství výše uvedených listin, písemností nebo dat či jiných obdobných dokumentů (odst. 1), resp. jedná uvedeným způsobem v úmyslu získat pro sebe nebo pro jiného majetkový nebo jiný prospěch, způsobit jinému škodu nebo jinou vážnou újmu, anebo ohrozit jeho společenskou vážnost (odst. 2).

Z hlediska kybernetické trestné činnosti představuje zejména zveřejnění, zpřístupnění nebo jiné použití v soukromí uchovávaných počítačových dat na datovém nosiči (zejména pevný disk počítače) typický kybernetický útok. Z hlediska vymezení znaků skutkové podstaty je nerozhodný obsah či rozsah dat, která se stala terčem útoku. V soukromí uchovávaná data mohou mít podobu fotografie, obrázku, textu, počítačového programu, počítačové databáze, zvukového či hlasového záznamu, filmového záznamu apod. Půjde například o doručené emailové zprávy, doručené SMS a MMS zprávy přechovávané v podobě dat v paměti mobilního telefonu, ale též o databáze podnikatele obsahující seznam a kontakty klientů, účetnictví vedené v elektronické podobě, záznamy a jiná zdravotní dokumentace lékaře o pacientech, která je vedená v elektronické podobě.[82]

Při mé studijní praxi byl u Okresního soudu v Jindřichově Hradci projednáván případ pachatele, na kterého byl státním zástupcem podán návrh na potrestání za jednání kvalifikované jako trestný čin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí podle 183 odst.1,2 tr.zák. spočívající ve zveřejnění na internetových stránkách intimních fotografií jeho bývalé partnerky. [83] Fotografie

[82] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

[83] sp.zn. 3T 103/2011 Okresního soudu v Jindřichově Hradci (viz příloha na str. 80 - 81)

pachatel pořídil svým vlastním fotoaparátem s konkludentním souhlasem poškozené v době, kdy spolu udržovali utajený milenecký poměr, a měl je uloženy ve vlastním počítači. Motivem zveřejnění na internetových stránkách byla zhrzenost a msta pachatele za to, že se s ním poškozená rozešla a vrátila se k manželovi. Okresní soud dospěl k závěru, že skutková podstata trestného činu podle § 183 tr.zák. není naplněna ve znaku *"uchovávání v soukromí **jiného**"*, neboť pachatel měl fotografie vždy uloženy jen ve vlastním počítači. Přestože jednání pachatele mělo na poškozenou fatální tíživý dopad vedoucí k rozpadu jejích rodinných vztahů, byla věc toliko postoupena příslušnému orgánu jako přestupek proti občanskému soužití podle § 49 odst.1 písm.a) zák.čís. 200/1990 Sb., neboť jednání pachatele nenaplňovalo skutkovou podstatu ani jiného trestného činu. Následně se poškozená v občanskoprávním řízení domáhala ochrany podle § 11 občanského zákoníku a byla jí přiznána vysoká peněžitá satisfakce podle § 13 odst.2 občanského zákoníku. Úvahy zákonodárců *de lege ferenda* by měly vést k úpravě, která by takovéto zavrženíhodné jednání postihla i trestněprávně.

Z hlediska subjektivní stránky je v prvém odstavci vyžadováno zavinění úmyslné, a to jak úmysl přímý, tak i nepřímý; v odstavci druhém je vyžadován úmysl přímý.

Podle uvedených ustanovení je možné postihovat různé projevy kybernetické trestné činnosti – krádeže dat na zakázku, počítačovou špionáž apod.

Způsobení škody či jiné újmy není znakem základní skutkové podstaty podle odstavce prvého; je až okolností podmiňující použití vyšší trestní sazby podle odstavce třetího a čtvrtého. V odstavci druhém je formulována kvalifikovaná skutková podstata, k jejímuž naplnění je třeba specifického úmyslu pachatele získat pro sebe nebo pro jiného majetkový nebo jiný prospěch, způsobit jinému škodu nebo jinou vážnou újmu anebo ohrozit jeho společenskou vážnost. Až v odstavcích třetím a čtvrtém je znakem skutkové podstaty mj. výše způsobené škody. Vedle výše způsobené škody jsou dalšími okolnostmi podmiňujícími použití vyšší trestní sazby podle odst.3 a 4 členství pachatele v organizované skupině, spáchání činu z důvodu rasové, etnické, národnostní, politické či náboženské nesnášenlivosti anebo spáchání činu v úmyslu

získat pro sebe či jiného značný prospěch (odst.3), resp. prospěch velkého rozsahu (odst.4).

3.2.3 § 191 trestního zákoníku - Šíření pornografie

V odstavci prvém a druhém jsou vymezeny dvě samostatné skutkové podstaty; objektem je v prvém odstavci zájem na ochraně mravopočestnosti dospělých před obtěžováním tzv. tvrdou pornografií, v druhém odstavci zájem na ochraně mravního rozvoje a výchovy osob mladších 18 let před negativním působením jakékoli pornografie.[84] V Úmluvě tento trestný čin vymezen není, a to ani ve vztahu k druhému odstavci týkajícímu se ochrany před pornografií osob mladších 18 let.

V odstavci prvém je vymezena objektivní stránka jako výroba, dovoz, vývoz, provoz, nabízení, veřejné zpřístupňování, zprostředkování, uvádění do oběhu, prodej nebo jiné opatřování **zakázaného druhu** pornografického díla pro jiného. Zakázaným pornografickým dílem je takové dílo, v němž se v sexuálním kontextu projevuje **násilí či neúcta k člověku (ponižování, týrání, zraňování), nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem**. Může se jednat o dílo fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo. Byť na rozdíl od odstavce druhého není explicitně zmíněno dílo písemné, nepochybně i takové dílo (stejně jako dílo výtvarné) v případě popisů velmi brutálních či zoofilních praktik může být subsumovatelné pod *"jiné pornografického dílo"*. Dílem ve smyslu tohoto ustanovení není myšleno dílo autorské podle § 2 odst.1 autorského zákona; není však vyloučeno, že autorské dílo naplní znaky díla pornografického. Z hlediska šíření zakázaného druhu pornografie jako **kybernetického trestného činu** bude zřejmě *počítačovým* či *elektronickým* dílem nejen dílo zobrazující virtuální podobu člověka či zvířete vygenerovanou v počítačovém programu (např. v počítačové pornografické hře), nýbrž i dílo zachycující skutečného člověka či zvíře na fotografii, ve filmu, či v audionahrávce zaznamenané v elektronické podobě - např. na nosiči informací.

[84] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

Počítačové dílo tedy většinou nebude tvořit v rámci této skutkové podstaty samostatný druh díla (počítačové dílo v užším slova smyslu), nýbrž bude představovat formu záznamu děl ostatních (např. filmové dílo zaznamenané v elektronické podobě v paměti počítače nebo na jiném nosiči dat jako multimediální soubor s koncovkou .avi, .mpeg, .vaw, .mov apod., fotografie v podobě souboru s koncovkou .jpg, .jpeg, .bmp apod.).[85]

Odstavec druhý postihuje pachatele za jednání spočívající v šíření či jiném nakládání **jakékoliv pornografie ve vztahu k osobám mladším 18 let**.

Jasné a jednoznačné vymezení pojmu pornografie neexistuje. V nejobecnějším slova smyslu se jedná o *„znázorňování sexuálních motivů za účelem vyvolání pohlavního vzrušení"*. [86] Podle důvodové zprávy k návrhu trestního zákoníku, která vychází z ustálené judikatury, se za *"pornografické dílo považuje jakýkoli předmět, který zvláště intenzivním a vtíravým způsobem zasahuje a podněcuje samotný sexuální pud. Současně takové dílo hrubě porušuje uznávané morální normy společnosti a vyvolává pocit studu. Pro pornografický charakter je rozhodující obsah celého díla, nikoli jen určitá část, výseč, kapitola, úryvek apod. Závadný obsah může být vyjádřen slovně, písemně, zvukem, obrazem, zobrazením (plošným i prostorovým) nebo i kombinací těchto způsobů. Pouhé zobrazení nahého lidského těla, např. při koupání, modelu v ateliéru nebo v exteriéru, k reklamním účelům apod., není pornografií. Za pornografii nelze považovat ani umělecké dílo, byť by zobrazovalo nejintimnější chvíle lidí, příp. i vyvolávalo sexuální vzrušení či vzbuzovalo pocit studu nebo ošklivosti. Předměty historicky cenné, byť by jinak měly pornografický charakter, sem též nelze zařadit. Předměty svou povahou určené k vědeckým, uměleckým, osvětovým cílům nelze považovat za pornografická díla (např. fotografie genitálií v učebnici soudního lékařství, osvětový film znázorňující sexuální chování lidí se zaměřením na předcházení nechtěnému těhotenství, pohlavním chorobám apod.)."* [87]

---

[85] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

[86] DUNOVSKÝ, Jiří. *Problematika dětských práv a komerčního sexuálního zneužívání dětí u nás a ve světě*. Vyd. 1. Praha: Grada, 2005, 251 s. ISBN 80-247-1201-6.

[87] Důvodová zpráva k návrhu trestního zákoníku - zák. č. 40/2009 Sb. [online]. [cit. 2013-01-25]. Dostupné z: http://trestnizakonik.cz/navrh/duvodova-zprava.html

Trestně odpovědný podle odstavce druhého je ten, kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo buď nabízí, přenechává nebo zpřístupňuje dítěti, nebo na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje. Oproti odstavci prvému je zde výslovně zmíněno i dílo písemné. Dílo výtvarné sice výslovně uvedeno není, ale i takové dílo, zejména pokud se bude blížit tzv. tvrdé pornografii, může být kriminalizováno jako *jiné pornografické dílo*. Z hlediska kybernetické kriminality je třeba zmínit, že provozování běžně dostupných pornografických internetových stránek sice může naplňovat znaky skutkové podstaty odstavce druhého po stránce objektivní, avšak minimálně nepřímý úmysl (srozumění pachatele s tím, že si takové stránky budou prohlížet děti) by zřejmě prokazatelný nebyl, a to především na stránkách, které výslovně upozorňují na přístupnost osobám jen starším 18 let.[88] Dokonce i v případě, že by běžně dostupné internetové stránky takové varovné upozornění neobsahovaly, takže by bylo možno dovodit *lhostejnost* pachatele k následku, by byl nepřímý úmysl pachatele prokazatelný jen obtížně.[89]

Z hlediska označení pornografie za kybernetický trestný čin je dále významný odstavec třetí této skutkové podstaty. Zákonodárce zde zařazuje jako zvlášť přitěžující okolnost způsob spáchání trestného činu ***prostřednictvím veřejně přístupné počítačové sítě nebo jiným, obdobně účinným způsobem***. Jelikož nejrozšířenější veřejně přístupnou počítačovou sítí je internet a nejpoužívanější formou elektronické komunikace e-mailová zpráva (textová, hlasová, nebo obrazová zpráva, která může být uložena v síti nebo koncovém zařízení uživatele, dokud ji uživatel nevyzvedne), byla v soudní praxi posledních let opakovaně řešena otázka, zda rozesílání pornografických děl formou e-mailových zpráv po internetu naplňuje znak šíření pornografie ***veřejně přístupnou počítačovou sítí.*** Tato otázka byla rozdílně a rozporuplně posuzována

[88] GŘIVNA, Tomáš. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. *Bulletin advokacie*. Praha: Česká advokátní komora v Praze, 2009, č. 10. ISSN 1210-6348.

[89] nález Ústavního soudu sp.zn. III.ÚS 722/09 ze dne 7.1.2010: *"Sama lhostejnost ve vztahu k následku nestačí k naplnění volní složky nepřímého úmyslu."* Tento názor, vycházející z obecné trestněprávní zásady "in dubio pro reo", zasahuje do běžně uznávané definice nepřímého úmyslu jakožto jednání, kdy pachatel nepočítá s žádnou konkrétní okolností, jež mohla zabránit následku, který si představoval jako možný, a to ať už by šlo o jeho vlastní zásah nebo o zásah někoho jiného - viz JELÍNEK, Jiří. Trestní právo hmotné: obecná část, zvláštní část. 2. vyd. Praha: Leges, 2010, 904 s. Student (Leges). ISBN 978-80-87212-49-3.

nejen soudy prvého a druhého stupně, nýbrž dokonce i Nejvyšším soudem, jehož judikatura se k této nové problematice teprve postupně vyvíjí a sjednocuje. Nejprve Nejvyšší soud v usnesení ze dne 12.1.2011 sp.zn. 8 Tdo 1467/2010 zaujal názor, že pachatel, který rozeslal soubory s pornografií prostřednictvím internetové sítě celkem 163 adresátům na jejich elektronické e-mailové adresy, tímto jednáním znak *využití veřejně přístupné počítačové sítě* naplnil. (Současně připustil, že v případě opačného výkladu lze v dané konkrétní věci vzhledem k vysokému počtu adresátů dovodit naplnění znaku *jiným obdobně účinným způsobem*.) Oproti tomu v usnesení ze dne 4.5.2011 sp.zn. 3 Tdo 414/2011 dospěl Nejvyšší soud k závěru, že pachatel, který v pěti případech rozeslal pornografický materiál na pět konkrétních e-mailových adres, sice *"využil k šíření pornografických děl veřejně přístupnou počítačovou síť ovšem způsobem nikoli veřejně přístupným",* což odůvodnil úvahou, že *"z povahy těchto zpráv vyplývá, že k jejich obsahu si mohou legálně zjednat přístup pouze odesílatel a příjemce, popřípadě snad omezený okruh osob činných pro poskytovatele připojení, resp. že k pornografickým dílům měli přístup toliko konkrétní adresáti e-mailových zpráv, nikoli široký, předem nevymezený okruh osob, jak by tomu bylo v případě, že byl skutek spáchán např. televizí, filmem nebo vystavením takového pornografického díla na veřejně přístupných stránkách internetu"*. Obdobný názor pak Nejvyšší soud zaujal i v rozhodnutí ze dne 1.6.2011 sp.zn. 3 Tdo 669/2011, kde dále rozvedl, že *"přestože by bylo možno hovořit o tom, že v obecné rovině jednání obviněného znaky skutkové podstaty v odstavci třetím naplňuje, s ohledem na počet e-mailových adres, na které byly zprávy zasílány (32 prokázaných případů přeposílání e-mailové zprávy na 18 odlišných e-mailových adres), nelze dospět k závěru, že jeho jednání vykazuje takovou hromadnou účinnost, jakou má na mysli ustanovení odstavce třetího"*. Rozdílný výklad byl následně sjednocen stanoviskem trestního kolegia Nejvyššího soudu sp. zn. Tpjn 300/2012, které bylo přijato v následujícím znění: *"Rozesílání pornografických děl prostřednictvím elektronické pošty mezi tzv. e-mailovými schránkami, chráněnými individuálními přístupovými* hesly, ***nenaplňuje znak 'veřejně přístupná počítačová síť'*** *ve smyslu ustanovení § 191 odst. 3 písm. b) a ustanovení § 192 odst. 3 písm. b) tr. zákoníku. V případě rozesílání takových 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 týchž výše uvedených zákonných ustanovení." Z tohoto sjednocujícího stanoviska pak vycházelo např. rozhodnutí Nejvyššího soudu ze dne 28.11.2012 sp.zn. 6 Tdo 1401/2012, které rozeslání pornografických materiálů v prokázaných nejméně 100 případech na přesně neustavené e-mailové adresy sice nekvalifikovalo jako šíření *prostřednictvím veřejně přístupné počítačové sítě*, avšak posoudilo jej jako *jiný obdobně účinný způsob*.

3.2.4 § 192 trestního zákoníku - Výroba a jiné nakládání s dětskou pornografií

Objektem je zájem společnosti na ochraně mravního vývoje dětí a ochraně před jejich sexuálním zneužíváním.[90] V Úmluvě je tento trestný čin uveden v čl. 9 - Trestné činy související s dětskou pornografií, v němž je vymezena i samotná definice pornografického díla zahrnující mj. i *"osobu, **jež vyhlíží** jako nezletilá, provádějící viditelný sexuální akt"* a *"**realistické zobrazení** nezletilé osoby provádějící viditelný sexuální akt"* s tím, že smluvní státy si mohou ve vnitrostátní úpravě vyhradit nepovažovat takovéto materiály za dětskou pornografii. Podle novely trestního zákoníku čís. 330/2011 Sb., účinné od 1.12.2011, byla trestnost v prvém i druhém odstavci § 191 rozšířena i na dílo **zobrazující nebo jinak využívající osobu, jež se jeví být dítětem.** Tím bylo v České republice naplněno rámcové rozhodnutí Rady Evropské unie 2004/68/SVV ze dne 22.12.2003 o boji proti pohlavnímu využívání dětí a dětské pornografii, které v definici pornografického díla - obdobně jako Úmluva - uvádí mj. i *"realistické znázornění neexistujícího dítěte, které se aktivně nebo pasivně účastní jednoznačně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte"*.

Trestní zákoník – na rozdíl od Úmluvy i od rámcového rozhodnutí Rady Evropské unie 2004/68/SVV ze dne 22.12.2003 - definici dětské pornografie

[90] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

neobsahuje, a proto ji lze dovozovat pouze výkladem. V odborné literatuře je za dětskou pornografii považován obrazový, textový nebo zvukový materiál, který využívá dítě v sexuálním kontextu.[91] Dítětem je osoba mladší 18 let (§ 126 tr.zák.). Z hlediska vymezení dětské pornografie podle trestního zákoníku lze využít demonstrativní vymezení pornografického díla uvedené v Důvodové zprávě k návrhu trestního zákoníku (viz shora bod 2.3)[92], k němuž je třeba doplnit ***zobrazení či využití dítěte nebo osoby, jež se jeví být dítětem, v sexuálním kontextu.*** Pro vymezení pojmu dětská pornografie lze využít i existující judikaturu, např. usnesení Nejvyššího soudu ze dne 28.12.2004 sp.zn. 7 Tdo 1077/2004-I: *"Závěr o pornografickém charakteru díla nelze dovozovat bez dalšího jen z toho, že je prezentováno za účelem uspokojení osob trpících sexuální deviací (pedofilií, hebefilií či efebofilií), na místech nebo v médiích, které tyto osoby vyhledávají. Podle Nejvyššího soudu lze ... za pornografii jednoznačně považovat snímky obnažených dětských modelů v polohách vyzývavě prezentujících pohlaví, resp. zaujímajících polohy stimulující představu sexuálního styku s nimi. ... Ve světle této argumentace pak naproti tomu za pornografické nebude možno označit snímky zachycující oblečené dětské modely ani modely částečně či plně obnažené, které shora uvedená kritéria nenaplňují, takže u normálního jedince nevzbuzují sexuální asociace a působí sexuálně stimulujícím způsobem toliko na jedince pohlavně deviantního."* [93]

V souvislosti s přijetím novely čís. **330/2011 Sb.**, která trestnost v prvém i druhém odstavci rozšířila i na dílo ***zobrazující nebo jinak využívající osobu, jež se jeví být dítětem***, vyvstala otázka, zda lze za dětskou pornografii považovat zobrazení virtuálního (neexistujícího) dítěte v sexuálním kontextu. Před přijetím této novely byl akceptován názor, který jednak historickým výkladem[94], a jednak teleologickým výkladem opřeným o vymezení objektu, jakož i výkladem vycházejícím z principu

[91] CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Vyd. 1. Praha: Portál, 2003, 201 s. ISBN 80-717-8739-6.

[92] Důvodová zpráva k návrhu trestního zákoníku - zák. č. 40/2009 Sb. [online]. [cit. 2013-01-25]. Dostupné z: http://trestnizakonik.cz/navrh/duvodova-zprava.html

[93] *Sbírka soudních rozhodnutí a stanovisek Nejvyššího soudu ČR, částka 6/2005, č. 35, str. 426 - 427*

[94] HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti?. In: *Pocta Otovi Novotnému k 80. narozeninám*. Vyd. 1. Praha: ASPI, 2008. ISBN 978-80-7357-365-2.

subsidiarity trestní represe[95], dospěl ke všeobecně respektovanému závěru, že držení pornografie zobrazující virtuální dítě není trestné. Tento názor ovšem od 1.12.2011, kdy vstoupila v účinnost novela kriminalizující dílo *zobrazující osobu, jež se jeví být dítětem*, je použitelný již jen částečně. Nadále bude platit ve vztahu k dílům literárním, kresleným či animovaným, jakož i k takovým počítačovým virtuálním zobrazením dětí, které se nebudou (tzv. na první pohled) jevit jako skutečné děti. Za zobrazení *osoby, jež se jeví být dítětem*, totiž nelze považovat toliko skutečně existující osobu starší 18 let, která - ať již sama o sobě či za pomoci úprav svého zevnějšku - bude budit zdání, že je mladší 18 let. Při využití stále sofistikovanější počítačové technologie lze dosáhnout naprosto dokonalého zobrazení podoby dítěte, jež se bude jevit jako dítě skutečně existující, ale přitom půjde jen o počítačovým programem vytvořenou virtuální fikci. Pak i toto fiktivní dítě bude naplňovat znak *zobrazení osoby, jež se jeví být dítětem.* Důvodem této úpravy je zřejmě fakt, že při naprosto věrném virtuálním zobrazení neexistujícího dítěte nebude rozpoznatelné, které dílo zobrazuje fikci a které skutečnost. Kvůli zobrazování naprosto věrných virtuálních či kompilovaných zobrazení by vznikla řada problémů v souvislosti s prokazováním takové trestné činnosti, a to jak z hlediska naplnění znaků charakterizujících objektivní stránku tak i z hlediska zavinění. Při počítačových úpravách zobrazení jak existujících dětí, tak i jejich virtuálních podob by bylo neprůkazné, zda jde jen o fikci či o upravenou skutečnost. K vyvinění pachatele by při presumpci neviny stačilo pouhé jeho tvrzení, že byl přesvědčen o virtualitě zobrazení dítěte. Zavinění (minimálně ve formě nepřímého úmyslu) by bylo neprokazatelné zejména tehdy, pokud by si pachatel opatřoval dětskou pornografii ze zdrojů (např. internetových stránek) obsahujících upozornění (nepravdivé), že jde o virtuální pornografii. S takto opatřenou dětskou pornografií by pak mohl - relativně beztrestně - dále nakládat. Nově přijatá úprava tedy brání tomu, aby pod rouškou virtuální fikce mohla být šířena dětská pornografie, u které by nebylo zjistitelné, zda jde o fikci či realitu.

Pomocí dokonalých počítačových technik může docházet i ke kompilaci (spojení, prolínání) zobrazení existující dospělé osoby provádějící sexuální akt s

[95] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

obrazem **existujícího dítěte bez sexuálního kontextu** (např. snímku existujícího nahatého dítěte v běžné situaci), avšak výsledkem bude zcela reálný pornografický obraz **existujícího** dítěte, u něhož nebude zjistitelné, zda jde o kompilát dvou realit či realitu jedinou. I takovýto kompilát, který využije zobrazení existujícího dítě v asexuální situaci, je zřejmě podle uvedené novely trestný, neboť obecnější pojem *"osoba, jež se jeví být dítětem"* v sobě zahrnuje i užší pojem *"dítě (existující), jež se jeví být dítětem, které se (zdánlivě) účastní sexuálního jednání"*. ("*Jevit se*" v sobě zahrnuje nejen *"zdánlivě vypadat"*, nýbrž i *"skutečně být"*.) Paradoxem je, že takovýto kompilát dvou reálných zobrazení by nebyl podřaditelný pod žádnou ze tří konkrétních vymezení dětské pornografie podle Rámcového rozhodnutí Rady - viz následující odstavec.

Otázkou zůstává, zda úmyslem zákonodárce při přijetí novely čís. 330/2011 Sb. bylo skutečně kriminalizovat pornografická zobrazení fiktivních dětí, či zda k tomu došlo spíše nedomyšlením všech souvislostí. Rámcové rozhodnutí Rady 2004/68/SVV ze dne 22. prosince 2003, které bylo naplněno uvedenou novelou, vymezuje v článku 1 písm. b) dětskou pornografii jako 1) *zobrazení* ***skutečného dítěte*** *aktivně nebo pasivně se účastnícího jednoznačně sexuálního jednání, a to včetně dráždivého vystavování přirození nebo ohanbí dítěte,* dále 2) *zobrazení* ***skutečné osoby se vzhledem dítěte****, která se aktivně nebo pasivně účastní takového jednání* nebo 3) ***realistické znázornění neexistujícího dítěte****, které se aktivně nebo pasivně účastní takového jednání.* Pak ovšem zůstává nevysvětleno, proč novela čís. 330/2011 Sb. tyto nové pojmy, které jsou zcela jednoznačné a obdobně jsou vymezeny i v Úmluvě, nepřebrala a proč dva jasné nové pojmy nahradila nejednoznačným pojmem jedním.

Jazykový výklad ovšem spíše svědčí o úmyslu zákonodárce nahradit oba konkrétnější pojmy jedním pojmem obecnějším. Slova *"osoba, jež se jeví být dítětem"* totiž nelze posuzovat izolovaně, nýbrž ve vztahu ke slovu *"zobrazení"*, takže jde o výklad celkového slovního spojení *"zobrazení osoby, jež se jeví být dítětem"*. Pak ovšem pojem *"zobrazení osoby"*, který není provázen žádným dalším vymezením, omezením či upřesněním (vyjma znaku *jevit se dítětem*), lze jazykově a logicky

vykládat jako ***jakékoliv*** *zobrazení osoby* (*jež se reálně jeví být existujícím dítětem*), tedy i zobrazení virtuální (virtuální zobrazení fiktivní osoby jevící se být dítětem).

Rozhodujícím kritériem rozhraní mezi trestností a beztrestností je **míra realističnosti** zobrazené osoby a této klíčové otázky se nepochybně bude týkat budoucí - zatím neexistující - judikatura. Lze předpokládat, že judikatorní výklad pojmu *"zobrazení osoby jevící se být dítětem"* bude spíše zužující, tedy ve smyslu požadavku na věrně realistické zobrazení fikce, nerozeznatelné ani při vynaložení náležité pečlivosti od reality.

Mohu-li v této souvislosti vyjádřit svůj názor na kriminalizaci virtuální dětské pornografie, nezbývá mi než uvést, že ji nepovažuji za přínosnou, neboť prioritní by měla být ochrana dětí před zneužíváním devianty. Byť mi jsou známy názory, podle nichž může prohlížení dětské pornografie podnítit pachatele k realizaci jeho představ[96], naprostá většina odborníků z oboru sexuologie potvrzuje, že náhradní způsob ukájení spolu se získáním náhledu na svoji úchylku vede k výraznému snížení recidivy pedofilních pachatelů, takže zákaz virtuální dětské pornografie může vést přesně k opačnému výsledku, tedy k nárůstu pohlavního zneužívání dětí devianty.[97] Řešením by podle mého názoru bylo vyhradit nakládání s virtuální dětskou pornografií lékařským sexuologickým ústavům pod dohledem státu (obdobně jako je tomu v případě nakládání s léky, návykovými látkami a jedy). Pokud by k tomu přistoupila absolutní záruka zajištění lékařského tajemství, mohlo by to i neevidované osoby pedofilního zaměření motivovat ke kontaktování takových ústavů. Jsem přesvědčena o tom, že k takovémuto řešení dříve či později skutečně dojde, ale spíše později než dříve.

V odstavci prvém je skutková podstata vymezena tak, že trestné je již pouhé přechovávání pornografie. Z pohledu vymezení kybernetické trestné činnosti bude připadat v úvahu zejména přechovávání dětské pornografie v podobě digitálního

[96] HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti?. In: *Pocta Otovi Novotnému k 80. narozeninám*. Vyd. 1. Praha: ASPI, 2008. ISBN 978-80-7357-365-2.

[97] DIAMOND, Milton a Ayako UCHIYAMA. Pornography, Rape and Sex Crimes in Japan. International journal of law and psychiatry. 1999, č. 22. ISSN 0160-2527 [online]. [cit. 2013-01-25]. Dostupné z: http://www.hawaii.edu/PCSS/biblio/articles/1961to1999/1999-pornography-rape-sex-crimes-japan.html

záznamu na nosiči dat - na pevném disku počítače nebo na některém paměťovém zařízení (CD, DVD, Blu-Ray, HD DVD, USB flash disk, paměťové karty). O naplnění znaku *přechovávání* nepůjde v případě automatického ukládání dat zaznamenávajících dětskou pornografii do vyrovnávací paměti počítače, ani při ukládání dočasných internetových souborů na pevný disk počítače. Z toho vyplývá, že pouhé prohlížení dětské pornografie na internetových stránkách trestné není. V případě užití speciálních počítačových serverů umožňujících uskladnění dat bez ohledu na jejich obsah (který provozovatel takové služby nemá ani možnost žádným způsobem ověřovat a takové uložení je nepřístupné ostatním uživatelům) je však znak *přechování* naplněn. [98] [99]

V odstavci druhém zahrnuje skutková podstata jakékoli nakládání s dětskou pornografií, včetně její výroby, zveřejňování, zprostředkování atd., přičemž oproti vymezení § 191 obsahuje navíc znak kořistění z dětského pornografického díla.

Okolnosti podmiňující použití vyšší trestní sazby podle odstavců třetího a čtvrtého jsou vymezeny shodně jako u § 191, což i zde znamená, že rozesílání dětské pornografie prostřednictvím zprávy veřejně dostupné služby elektronických komunikací (nejčastěji e-mailem) na určitou koncovou adresu, určenou konkrétnímu konečnému uživateli, nenaplňuje znak *užití veřejně přístupné počítačové sítě*. V případě tohoto způsobu šíření dětské pornografie v hromadném rozsahu či většímu počtu příjemců, však není vyloučeno naplnění znaku *jiným obdobně účinným způsobem* (viz podrobný výklad v předchozím bodu 3.2.4 - § 192 Šíření pornografie).

3.2.5 § 234 trestního zákoníku - Neoprávněné opatření, padělání a pozměnění platebního prostředku

[98] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[99] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

Skutková podstata byla v trestním zákoníku vymezena v souladu s Rámcovým rozhodnutím Rady Evropské unie č. 2001/413/JVV ze dne 28.5.2001, o boji proti podvodům a padělání v oblasti bezhotovostních platebních prostředků.

Objektem je ochrana tuzemských i zahraničních platebních prostředků a zájem na řádném fungování bezhotovostního platebního styku. Bezhotovostní styk se realizuje formou bezhotovostních platebních prostředků a je upraven v § 708 až 715 obchodního zákoníku a v zák.čís. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech. Bezhotovostní platební styk probíhá zpravidla prostřednictvím bank a dělí se na klientský a mezibankovní. Mezi nejvýznamnější platební prostředky patří platební karta, elektronické peníze, příkaz k zúčtování ve formě příkazu k úhradě nebo příkazu k inkasu, cestovní šek, záruční šeková karta, šek, směnka, dokumentární akreditiv, dokumentární inkaso a další.[100]

Za elektronické peníze bývají označovány i systémy umožňující tzv. homebanking, který klientům banky umožňuje správu bankovního účtu za pomoci mobilního telefonu prostřednictvím internetových služeb (např. systém Genius, Internetbanking). Bezhotovostní elektronický převod peněz je možný nejen v rámci bank, ale i prostřednictvím dalších systémů, jako jsou např. PayPal, BidPay, MoneyBookers, Neteller, StormPay či E-gold. Napadání systému homebanking a dalších podobných systémů bývá označováno jako tzv. **phishing** nebo **pharming** a představuje jednu z nejčastějších forem kybernetické trestné činnosti, která směřuje k odčerpání peněz z účtu. [101]

Znaky objektivní stránky jsou naplněny tím, že pachatel sobě nebo jinému bez souhlasu oprávněného držitele opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného, zejména nepřenosnou platební kartu identifikovatelnou podle jména nebo čísla, elektronické peníze, příkaz k zúčtování, cestovní šek nebo záruční šekovou

[100] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[101] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

kartu. Kvůli tomu, že typy platebních prostředků se neustále mění, je jejich výčet ve skutkové podstatě pouze demonstrativní. Opatřením se rozumí jakýkoliv způsob získání platebního prostředku ve hmotné podobě (např. opatření platební karty). Zpřístupněním se rozumí jakýkoliv způsob učinění platebního prostředku dostupným, a to i v elektronické podobě, například ve formě poskytnutí potřebných prostředků (např. návodu) na internetových stránkách. Přijetí zahrnuje především úmyslné převzetí takového platebního prostředku osobou, která s ním nakládá při placení nebo zúčtování, jako například jednání prodavače, který úmyslně přijme nepřenosnou platební kartu jiného zpravidla v dohodě s osobou, která ji předkládá při placení zboží nebo služby. Přechováváním se rozumí dispozice s platebním prostředkem, a to i tehdy, když pachatel s takovým platebním prostředkem dále nenakládá.[102]

V odstavci druhém je oproti prvnímu odstavci změna v hmotném předmětu útoku, jímž je padělaný nebo pozměněný platební prostředek (oproti legálnímu platebnímu prostředku v odstavci prvém), který pachatel sobě nebo jinému opatří, zpřístupní, přijme nebo přechovává.

Podle odstavce třetího je trestně odpovědný ten, kdo padělá nebo pozmění platební prostředek v úmyslu použít jej jako pravý, resp. kdo takový prostředek jako pravý použije. Z hlediska kybernetické trestné činnosti by to mělo přispět k postihování pachatelů za phishingové útoky na homebanking a na další služby umožňující elektronické platby.

V odstavcích čtvrtém a pátém jsou uvedeny okolnosti podmiňující použití vyšší trestní sazby, kde za zdůraznění stojí zvlášť přitěžující okolnost podle odst.5 písm.b) spočívající ve spáchání činu jako člen organizované skupiny působící ve více (tedy nejméně dvou) státech, k čemuž dochází právě v případě phishingu. Vyšší stupeň společenské škodlivosti pak v odstavci šestém nachází svůj výraz v trestnosti i jen přípravy.

[102] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

3.2.6 § 236 trestního zákoníku - Výroba a držení padělatelského náčiní

Stejně jako u předchozího trestného činu byla tato skutková podstata zařazena do trestního zákoníku v souvislosti s Rámcovým rozhodnutím Rady Evropské unie č. 2001/413/JVV ze dne 28.5.2001, o boji proti podvodům a padělání v oblasti bezhotovostních platebních prostředků.

Objektem je ochrana tuzemských a zahraničních peněz, platebních prostředků a cenných papírů před padělaním a pozměněním (§ 238).

Z hlediska kybernetické trestné činnosti je zde nastolena trestní odpovědnost za nakládání s nástroji, zařízením, součástí zařízení, postupem, pomůckou nebo jakýmkoliv jiným prostředkem, a to včetně počítačového programu, který je vytvořený nebo přizpůsobený k padělání nebo pozměnění peněz nebo prvků sloužících k ochraně peněz proti padělání anebo vytvořený nebo přizpůsobený k padělání nebo pozměnění platebních prostředků. Toto ustanovení tedy působí subsidiárně vůči trestným činům spočívajícím v padělání peněz a též vůči trestnému činu podle § 234 neoprávněné opatření, padělání a pozměnění platebního prostředku. Ochrana peněz a platebních prostředků představuje zároveň také individuální objekt u této skutkové podstaty. [103]

Znaky charakterizující objektivní stránku jsou vymezeny obdobně jako u trestného činu podle § 231. Ovšem zatímco z hlediska subjektivní stránky u trestného činu podle § 231 nastává trestní odpovědnost pouze tehdy, nakládá-li pachatel s uvedeným zařízením v úmyslu spáchat trestný čin porušení tajemství přepravovaných zpráv podle § 182 odst. 1 písm. b) a c) tr.zák. nebo neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 1 nebo 2 tr.zák., u této skutkové podstaty se takováto omezující podmínka nevyskytuje. Postačí, že se jedná o

[103] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

zařízení vytvořené nebo přizpůsobené k padělání nebo pozměnění platebních prostředků.[104]

3.2.7 § 270 trestního zákoníku - Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi

Objektem je ochrana především vědecké a literární, hudební, výtvarné, audiovizuální a jiné umělecké tvůrčí činnosti a požitků z ní plynoucích, jakož i práv výrobců zvukových či zvukově obrazových záznamů, práv rozhlasového nebo televizního vysílání a práv pořizovatelů databází.[105]

V prostředí informačních a komunikačních technologií patří tento trestný čin k nejčastějším projevům kybernetické trestné činnosti, a to především ve vztahu k filmovým a hudebním dílům a k počítačovým programům.

Objektivní stránka spočívá v jednání pachatele, jímž neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi. Jedná se o blanketní normu, odkazující na zákon upravující práva autora k jeho autorskému dílu, práva související s právem autorským a práva k databázi, což při případné změně takového zákona nebude přinášet nutnost změny i tohoto trestního ustanovení. Nyní jde o zákon číslo 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Tento zákon v sobě zapracovává příslušné předpisy Evropského parlamentu a Rady Evropských společenství a upravuje práva autora k jeho autorskému dílu, práva související s právem autorským, právo pořizovatele k jím pořízené databázi, dále upravuje ochranu práv podle tohoto zákona a kolektivní správu práv autorských a práv souvisejících s právem autorským.

---

[104] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

[105] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

Předmětem práva autorského je **dílo**. Dílem je míněno dílo literární a jiné dílo umělecké a dílo vědecké, které je jedinečným výsledkem tvůrčí činnosti autora a je vyjádřeno v jakékoli objektivně vnímatelné podobě včetně podoby elektronické, trvale nebo dočasně, bez ohledu na jeho rozsah, účel nebo význam. Dílem je zejména dílo slovesné vyjádřené řečí nebo písmem, dílo hudební, dílo dramatické a dílo hudebně dramatické, dílo choreografické a dílo pantomimické, dílo fotografické a dílo vyjádřené postupem podobným fotografii, dílo audiovizuální, jako je dílo kinematografické, dílo výtvarné, jako je dílo malířské, grafické a sochařské, dílo architektonické včetně díla urbanistického, dílo užitého umění a dílo kartografické. Za dílo se považuje též počítačový program, je-li původní v tom smyslu, že je autorovým vlastním duševním výtvorem.

Souborným dílem je databáze, 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. Jiná kritéria se pro stanovení způsobilosti počítačového programu a databáze k ochraně neuplatňují. Fotografie a dílo vyjádřené postupem podobným fotografii, které jsou původní, jsou chráněny jako dílo fotografické. Předmětem práva autorského je také dílo vzniklé tvůrčím zpracováním díla jiného, včetně překladu díla do jiného jazyka. Tím není dotčeno právo autora zpracovaného nebo přeloženého díla.

Podle autorského zákona se však neposkytuje ochrana všem dílům. Ochrana se nevztahuje na úřední dílo (právní předpis, rozhodnutí, opatření obecné povahy, veřejná listina, veřejně přístupný rejstřík a sbírka jeho listin, úřední návrh úředního díla a jiná přípravná úřední dokumentace, včetně úředního překladu takového díla, sněmovní a senátní publikace, obecní kroniky, státní symbol a symbol jednotky územní samosprávy a jiná taková díla, u nichž je veřejný zájem na vyloučení z ochrany). Ochrana se též neposkytuje výtvorům tradiční lidové kultury, není-li pravé jméno autora obecně známo a nejde-li o dílo anonymní nebo o dílo pseudonymní. Dílem vůbec není zejména námět díla sám o sobě, denní zpráva nebo jiný údaj sám o sobě,

myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a podobný předmět sám o sobě (§ 2 odst. 6 autorského zákona).

Ne všechny zásahy do práva autorského musí být nutně zásahy neoprávněné. Za splnění určitých podmínek autorský zákon umožňuje zásahy do autorských práv provádět, aniž by se ten, kdo do těchto práv zasahuje, vystavoval nebezpečí trestního či jiného postihu. Tyto výjimky a omezení autorského práva se nazývají volné užití a bezúplatné zákonné licence.

Podle § 29 autorského zákona je dílo užito v souladu se zákonem pouze tehdy, jestliže takové užití vyhovuje tzv. třístupňovému testu, tedy jestliže výjimky a omezení se uplatňují pouze v případech stanovených zákonem, jestliže takové užití díla není v rozporu s běžným způsobem užití díla a konečně pokud takovým užitím díla nejsou nepřiměřeně dotčeny oprávněné zájmy autora díla. Pokud nakládání s dílem nesplňuje byť i jen jednu z uvedených podmínek, jedná se o porušení práva autorského nebo práv souvisejících s právem autorským.

Volné užití díla je takové užití díla, které užívá pro osobní potřebu fyzická osoba, přičemž účelem užití díla není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu. Do práva autorského nezasahuje ten, kdo pro svou osobní potřebu zhotoví záznam, rozmnoženinu nebo napodobeninu díla. Z hlediska kybernetické trestné činnosti je důležité, že podle autorského zákona není možné do volného užití díla zahrnout počítačový program, elektronickou databázi ani pořizování záznamu audiovizuálních děl při jejich provozování (např. pořizování záznamu filmového díla prostřednictvím kamery či jiného záznamového zařízení při promítání v kině, tzv. camcording). Volné užití díla však není nadřazeno právu autora opatřit své dílo ochrannými prvky pro ochranu svých práv (např. prvky zabraňující rozmnožování software). [106]

[106] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

Objektivní stránka spočívá v různém jednání pachatele, jímž porušuje některé z práv chráněných touto skutkovou podstatou. Z hlediska kybernetické trestné činnosti dochází v souvislosti s porušováním autorských práv v prostředí informačních a komunikačních technologií nejčastěji k neoprávněným zásahům do práv autora k audiovizuálním dílům (tzv. **audiovizuální pirátství**) nebo do práv k počítačovému programu (**softwarové pirátství**).

Audiovizuální pirátství spočívá nejčastěji v neoprávněném šíření audiovizuálních děl pomocí počítačových sítí, v opatřování záznamu filmových děl přímo při promítání v kině a jejich následné uložení ke stažení do kyberprostoru, v šíření originálních nosičů s filmovým či hudebním dílem v rozporu s licenčním ujednáním, dále ve výrobě a šíření padělků originálních filmových či hudebních děl s následnou veřejnou projekcí filmových děl v rozporu s licenčním ujednáním. **Softwarové pirátství** spočívá v šíření softwarových produktů, v zásazích do softwarových produktů, v nelegální výrobě softwarových produktů a v užívání softwarových produktů v rozporu s licenčním ujednáním. Jde o porušení autorského práva již samotným obstaráním softwarového produktu, aniž by bylo nutno s ním dále nakládat. Již tedy například obstarání software stažením z internetu, aniž by byl software dále nainstalován, používán či šířen, může být za splnění ostatních znaků trestné podle této skutkové podstaty.

V souvislosti se stále více dostupným internetem dochází k porušení autorských práv nejčastěji právě za využití této sítě. Umístění audiovizuálního díla či softwarového produktu do kybernetického prostředí internetu (upload) naplňuje znak šíření díla ve smyslu autorského zákona a 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 autorského zákona. Stažení díla (download) z prostředí internetu nemusí být za všech podmínek protiprávní (např. v případě obstarání díla za podmínek volného užití dle § 29 a násl. autorského zákona).[107] Volevecký dospívá k závěru, že

[107] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

stažení filmového či hudebního díla z prostředí 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 třístupňovým testem, neboť jsou tímto jednáním nepřiměřeně dotčeny zájmy nositele autorských práv). [108]

Nejvyšší soud se problematikou, zda je pro pořízení legální rozmnoženiny nezbytný legálně získaný zdroj, zabývá v rozhodnutí ze dne 25. 3.2009 sp.zn. 5 Tdo 234/2009 a dospívá k závěru, že *„ze znění ustanovení § 30 odst. 1 písm. a) autorského zákona nelze 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 rozmnoženin 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 rozmnožení, 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. Ustanovení § 30 autorského zákona totiž ani nestanoví podmínku oprávněného uživatele, jak to činí autorský zákon v jiných ustanoveních, např. § 36 nebo § 66. (srovnej Telec, I., Tůma, P. Autorský zákon. Komentář. 1. vydání. Praha: C. H. Beck, 2007, s. 347, 348). Z tohoto hlediska tedy nelze při jednoznačné a pochybnosti nevzbuzující dikci zákona vztahující se k volnému užití díla argumentovat blíže nezdůvodněným účelem či duchem autorského zákona nebo podle názoru soudu absurdním příkladem. Výklad zákona je totiž třeba podávat standardními metodami výkladu právních norem (zejména na základě*

[108] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

jazykového, logického, systematického, historického, ale i teleologického výkladu). V této souvislosti je však třeba zdůraznit, že i v naznačených směrech platí povinnost výkonu tohoto omezení autorského práva v souladu s výše zmíněným tříkrokovým testem. Autorsko právní důsledky pořízení rozmnoženiny díla pro osobní potřebu např. z protiprávně pořízeného zdroje je tedy třeba posuzovat vždy podle konkrétních okolností případu. Ani zde tedy nelze vycházet z paušálního výkladu o dovolenosti či zakázanosti pořízení rozmnoženiny díla pro osobní potřebu z nelegálního zdroje. Svůj význam zde tedy má především skutečnost, zda pořízení takové rozmnoženiny je v rozporu s běžným způsobem užití díla a jsou nepřiměřeně dotčeny oprávněné zájmy autora ve smyslu § 29 odst. 1 autorského zákona.“ [109]

Peer-to-peer sítě (P2P) je označení typu počítačových sítí, ve kterých spolu komunikují přímo jednotliví uživatelé. Jde především o výměnné sítě, prostřednictvím kterých si mnoho uživatelů může vyměňovat data. Příkladem takových sítí jsou např. Gnutella či původní verze Napsteru. Jde o jiný způsob zpřístupňování děl než centralizovaný přístup, při němž se data zveřejní na jednom místě. Ten, kdo data stahuje, vystupuje zároveň aktivně v roli serveru, tedy toho, kdo data poskytuje, byť třeba jen určitou dobu. Nejpoužívanější nástroj pro P2P distribuci velkých souborů je BitTorrent. Technologie BitTorrent využívá tzv. torrent souborů, které jsou určeny k lokalizaci děl, dílo není součástí torrent souboru. Aby bylo možné vytvořit a uložit torrent soubor odkazující na umístění určitého díla, uživatel, který má v úmyslu takové dílo sdílet, tzv. „seeder“, musí mít uloženou kopii díla na svém počítači, kterou „leacher“ od něj stahuje. Na tuto kopii pak torrent soubor směřuje. Torrenty se dají vyhledat googlem nebo na zvlášť vytvořených stránkách, tzv. bitTorrent indexech, jako je třeba isoHunt nebo The Pirate Bay, které umožňují ukládání a vyhledávání torrentů. The Pirate Bay se stal za dobu své existence terčem různých soudních sporů a byl kritizován ze strany velkých mediálních společností. Musel vícekrát měnit sídlo a na čas byl pozastaven. Jeho provozovatelé byli švédským soudem odsouzeni k trestu odnětí svobody v trvání jednoho roku a byli povinni zaplatit pokutu ve výši zhruba 30 milionů švédských korun. Rozsudek byl založen na trestněprávní odpovědnosti obžalovaných spočívající v účastenství na trestném činu porušování autorských práv.

[109] usnesení Nejvyššího soudu ČR ze dne 25. 3.2009 sp.zn. 5 Tdo 234/2009

Z fungování BitTorrentu vyplývá, že každý uživatel, který tímto způsobem stahuje data, je zároveň v daný okamžik poskytuje i ostatním uživatelům, tj. stává se alespoň na určitou dobu a v omezené míře i subjektem, který data zpřístupňuje, a proto porušuje autorský zákon tím, že neoprávněně sděluje dílo veřejnosti podle § 18 AutZ.[110]

3.2.8 § 311 trestního zákoníku - Teroristický útok

Objektem je především ústavní zřízení a obranyschopnost České republiky, demokratické principy, na nichž je republika založena, základní hospodářská struktura státu, jakož i život a zdraví obyvatel republiky.[111]

Znak kybernetického trestného činu je v široce vymezené skutkové podstatě dán v odst.1 písm. c), v němž je jako jeden z možných znaků objektivní stránky skutkové podstaty uveden útok na telekomunikační a informační systém. Útok na telekomunikační či informační systémy je jen jeden ze způsobů spáchání trestného činu teroristický útok a charakter kybernetického trestného činu může, ale nemusí splňovat. Trestného činu teroristický útok se z hlediska kybernetické trestné činnosti dopustí ten, kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla, zničí nebo poškodí ve větší míře telekomunikační systém, včetně informačního systému. Vymezení těchto znaků vychází zejména ze závazků obsažených v mezinárodních úmluvách, které se Česká republika zavázala plnit.[112]

---

[110] ČERMÁK, Jiří. Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent s přihlédnutím k rozsudku ve věci The Pirate Bay. *Právní rozhledy: časopis pro všechna právní odvětví*. Praha: C. H. Beck, 2010, č. 8. ISSN 1210-6410.

[111] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[112] VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2010, č. 7. ISSN 1211-2860.

Telekomunikačním systémem se rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou telekomunikační činnost s využitím sítí elektronických komunikací.[113]

Informačním systémem je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. Informační činností se rozumí získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků (§ 2 zákona č. 365/2000 Sb., o informačních systémech).

Je nerozhodné, jakým způsobem pachatel uvedené systémy poškodí nebo zničí, podstatné je, že tak učiní ve větší míře. Podle odstavce druhého je trestně odpovědný i ten, kdo tímto útokem vyhrožuje nebo kdo takový útok finančně, materiálně nebo jinak podporuje.

3.2.9 § 348 trestního zákoníku - Padělání a pozměnění veřejné listiny

Objektem je zájem na řádném a zákonném chodu státního aparátu a důvěra v pravost a pravdivost veřejných listin.[114]

Znak kybernetického trestného činu je vymezen v především v té části skutkové podstaty, v níž se hovoří o výrobě a dalším nakládání nástrojem či jiným

[113] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

[114] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

prostředkem, včetně počítačového programu, vytvořeném nebo přizpůsobeném k padělání nebo pozměnění veřejné listiny. Objektivní stránka je vymezena obdobně jako u trestných činů podle § 231 a 236. Zvýšená společenská škodlivost tohoto jednání našla svůj výraz v tom, že jde o vymezení skutkové podstaty, která je vlastně jen přípravou k samotnému padělání či pozměnění veřejné listiny.

3.2.10 § 354 trestního zákoníku - Nebezpečné pronásledování

V českém právu jde o nový trestný čin, pro který se vžil název *stalking*. Může, ale nemusí být spáchán jako trestný čin kybernetický. Znak kybernetického trestného činu je obsažen ve vymezení skutkové podstaty v odst. 1 písm.c) - dlouhodobé a vytrvalé pronásledování nebo jiné kontaktování, písemně nebo jinak, prostřednictvím prostředků elektronických komunikací. K trestnosti musí být splněna podmínka, že takové jednání je způsobilé v poškozeném vzbudit důvodnou obavu o zdraví či život jeho samotného či osob blízkých. Nevyžaduje se, aby tato obava u poškozeného skutečně vznikla.

Jako kybernetický trestný čin může být spáchán např. vytrvalým nebo soustavným zasíláním e-mailových zpráv, SMS či MMS zpráv, uskutečňováním opakovaných telefonických hovorů, zneužíváním internetových diskusních fór (chat rooms) apod. Může se jednat i o zasílání nebezpečných programů (viry, trojské koně, počítačové červy), zveřejňování důvěrných či intimních informací nebo o audiovizuální záznamy zobrazující poškozeného (např. pomocí FACEBOOK, YOUTUBE), získávání osobních dat z počítače jiné osoby, zasílání vzkazů na Skype, ICQ, VoIP, QUIP apod. Musí být ovšem splněna podmínka dlouhodobosti a vytrvalosti takového jednání, nestačí jen občasné či ojedinělé. Podle právní teorie[115] se opakováním rozumí více než 10 pokusů o kontakt, trvajícím obdobím pak nejméně čtyři týdny.

[115] ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

3.3 Relativně kybernetické trestné činy s kybernetickým znakem jako okolnosti zvlášť přitěžující

Jedná se o potencionální kybernetické trestné činy, které obsahují kybernetický znak (tj. využití nebo zasažení informačně-komunikačních technologií) nikoli v základní skutkové podstatě, nýbrž **toliko jako okolnost podmiňující použití vyšší trestní sazby** ve smyslu § 17 tr.zák. Jde o těchto osm trestných činů:

§ 180 - Neoprávněné nakládání s osobními údaji
§ 184 - Pomluva
§ 287 - Šíření toxikomanie
§ 345 - Křivé obvinění
§ 355 - Hanobení národa, rasy, etnické nebo jiné skupiny osob
§ 356 - Podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod
§ 403 - Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka
§ 407 - Podněcování útočné války

U všech osmi trestných činů je znak podmiňující použití vyšší trestní sazby vymezen shodně - jako spáchání činu ***veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem***.

Za ***veřejně přístupnou počítačovou síť*** se považuje funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především ***internet*** a jiné podobné informační systémy (viz bod 1.1).

Podle aktuální judikatury **rozesílání zpráv "*prostřednictvím elektronické pošty mezi tzv. e-mailovými schránkami, chráněnými individuálními přístupovými hesly, nenaplňuje znak veřejně přístupná počítačová síť*".**[116] Ovšem v případě rozesílání

[116] stanovisko trestního kolegia Nejvyššího soudu sp.zn. Tpjn 300/2012

zpráv na větší počet e-mailových adres, je-li význam tohoto jednání s ohledem na počet oslovených adresátů srovnatelný se spácháním činu tiskem, filmem, rozhlasem, televizí nebo veřejně přístupnou počítačovou sítí, může naplňovat znak *jiným obdobně účinným způsobem* (blíže k této problematice - viz bod 3.2.3 § 191 Šíření pornografie).

Závěr

Problematika kybernetické kriminality je jen dílčí problematikou z komplexního celku kybernetického práva. Přestože nezbývá než se smířit s tím, že úprava kybernetického práva bude vždy o něco pozadu za kybernetickými technologiemi, mělo by zaostávání práva za technickým vývojem být co nejmenší. V oblasti trestního práva to znamená včas a rychle (tedy obdobně dynamicky, jako postupuje technický vývoj kybertechnologií) reagovat na nové formy protispolečenského jednání v kyberprostoru a na zneužívání nebývalých možností, které kyberprostor poskytuje. *De lege ferenda* by měly být řešitelné dva aktuální problémy, s nimiž jsem se setkala v souvislosti s vypracováváním této diplomové práce:

1) V bodu 3.2.2 (str. 48-49) uvádím trestní kauzu Okresního soudu v Jindřichově Hradci sp.zn. 3T 103/2011, která přes podání návrhu na potrestání na pachatele, jenž na internetové stránky umístil intimní fotografie své bývalé partnerky, skončila postoupením věci přestupkovému orgánu, jelikož soud dospěl k závěru, že prokazovaný skutek nelze podřadit pod skutkovou podstatu přečinu podle § 183 trestního zákoníku ani pod skutkovou podstatu kteréhokoli jiného přečinu.[117] Zvážíme-li, že trestní zákoník kriminalizuje jednání, kdy dokonce i jen z nedbalosti jsou zveřejněny osobní údaje typu data narození, rodného čísla a bydliště konkrétní osoby (tedy relativně neškodné, resp. neškodící údaje), jeví se jako absurdní, že je trestně nepostižitelné jednání pachatele, který se zlým úmyslem umístí na běžně dostupné internetové stránky fotografie konkrétní osoby zachycující ji v ryze intimní situaci (tzv. outing). Okresní soud v Jindřichově Hradci důvodně dospěl k závěru, že skutková podstata § 183 tr.zák. nebyla naplněna proto, že nešlo o fotografie *uchovávané v soukromí **jiného*** (nafotil si je sám pachatel), a přitom současně zvážil a vyloučil kvalifikaci podle jiného ustanovení trestního zákona (např. trestného činu neoprávněné nakládání s osobními údaji podle § 180 tr.zák. či poškození cizích práv podle § 181 tr.zák.). Podle mého názoru by tato zjevná mezera trestního zákona měla být

[117] viz příloha na str. 80 - 81 (usnesení Okresního soudu v Jindřichově Hradci ze dne 17.1.2012 čj. 3T 103/2011-23)

odstraněna, a to buď novelizací ustanovení § 183 (např. vypuštěním slova *jiného* či novou dikcí celé skutkové věty) nebo novelizací ustanovení § 180 či § 181 tr.zák., případně novou úpravou samostatného trestného činu.

2) *De lege lata* je jen obtížně trestně postižitelné chování uživatele internetu, který pod falešnou identitou navazuje kontakt s dítětem a předstíráním zájmu o jeho běžné životní starosti se v něm snaží vzbudit důvěru a vylákat ho na osobní setkání, jehož cílem je dítě pohlavně zneužít (tzv. kybergrooming). Jak vyplývá z masmédií, počet těchto případů každoročně výrazně narůstá, přičemž je obtížné je odhalit a dosáhnout potrestání pachatele.[118] Jelikož stupeň společenské škodlivosti takovéhoto jednání je velmi vysoký, měly by zákonodárné orgány zvážit vytvoření nové skutkové podstaty trestného činu, jímž by toto jednání bylo postižitelné.

Lze předvídat, že do virtuálního světa kyberprostoru se bude postupně přesouvat stále větší část lidských aktivit, počínaje zájmovými a relaxačními činnostmi, přes pracovní a výukové aktivity, až po uspokojování duchovních, citových a fyziologických potřeb. Tak jako v pravěku ovlivnil zásadním způsobem vývoj člověka objev ohně a v novověku vynález elektřiny, tak v budoucnu to bude virtuální svět kyberprostoru.

[118] ŠEVELA, Vladimír. Devianti on-line. *Mladá fronta dnes*. Praha: MAFRA, a.s, 2013, 25.2. ISSN 1210-1168.

Seznam literatury

publikace:

ČERMÁK, Jiří. *Internet a autorské právo*. 2. aktualizované a rozšířené vyd. Praha: Linde Praha, 2003, 251 p. ISBN 80-720-1423-4.

DUNOVSKÝ, Jiří. *Problematika dětských práv a komerčního sexuálního zneužívání dětí u nás a ve světě*. Vyd. 1. Praha: Grada, 2005, 251 s. ISBN 80-247-1201-6.

GŘIVNA, Tomáš. Existují virtuální trestné činy?. In: *Pocta Otovi Novotnému k 80. narozeninám*. Vyd. 1. Praha: ASPI, 2008, s. 28-35. ISBN 978-80-7357-365-2.

GŘIVNA, Tomáš a Radim, POLČÁK. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.

HENDRYCH, Dušan. *Právnický slovník*. 3., podstatně rozš. vyd. V Praze: C.H. Beck, 2009, xxii, 1459 s. Beckovy odborné slovníky. ISBN 978-80-7400-059-1.

HERCZEG, Jiří. Virtuální dětská pornografie: Zločin bez oběti?. In: *Pocta Otovi Novotnému k 80. narozeninám*. Vyd. 1. Praha: ASPI, 2008, s. 36-49. ISBN 978-80-7357-365-2.

HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. 1. vyd. Praha: Triton, 2012, 217 s. ISBN 978-807-3875-459.

CHMELÍK, Jan. *Mravnost, pornografie a mravnostní kriminalita*. Vyd. 1. Praha: Portál, 2003, 201 s. ISBN 80-717-8739-6.

JAMES, Lance. *Phishing bez záhad*. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

JELÍNEK, Jiří. *Trestní právo hmotné: obecná část, zvláštní část*. 2. vyd. Praha: Leges, 2010, 904 s. Student (Leges). ISBN 978-80-87212-49-3.

JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

KRÁL, Mojmír. *Bezpečnost domácího počítače: prakticky a názorně*. 1. vyd. Praha: Grada, 2006, 334 s. ISBN 80-247-1408-6.

MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

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

(Auditorium). ISBN 978-80-87284-22-3.

SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. Vyd. 1. Praha: C. H. Beck, 2001, xxiv, 542 s. ISBN 80-717-9552-6.

ŠÁMAL, Pavel. *Trestní zákoník: komentář*. 2. vyd. Praha: C.H. Beck, 2012, xvi, 1450 s. Velké komentáře. ISBN 978-807-4004-285.

ŠÁMAL, Pavel a Stanislav, RIZMAN. *Trestní zákoník: Komentář*. 1. vyd. Praha: SEVT, 1994, XI, 1036 s. Komentované zákony (SEVT). ISBN 80-704-9097-7.

články z periodik:

ČERMÁK, Jiří. Ochrana autorského práva v prostředí peer to peer sítí typu BitTorrent s přihlédnutím k rozsudku ve věci The Pirate Bay. *Právní rozhledy: časopis pro všechna právní odvětví*. Praha: C. H. Beck, 2010, č. 8. ISSN 1210-6410.

GŘIVNA, Tomáš. Trestné činy proti lidské důstojnosti v sexuální oblasti v novém trestním zákoníku. *Bulletin advokacie*. Praha: Česká advokátní komora v Praze, 2009, č. 10. ISSN 1210-6348.

ŠEVELA, Vladimír. Devianti on-line. *Mladá fronta dnes*. Praha: MAFRA, a.s, 2013, 25.2. ISSN 1210-1168.

VOLEVECKÝ, Petr. Kybernetické trestné činy v trestním zákoníku. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2011, č. 5. ISSN 1211-2860.

VOLEVECKÝ, Petr. Dětská pornografie jako kybernetický trestný čin ve světle Úmluvy o počítačové kriminalitě. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2009, č. 4. ISSN 1211-2860.

VOLEVECKÝ, Petr. Kybernetická trestná činnost jako předmět vědeckovýzkumné činnosti. *Trestní právo: odborný časopis pro trestní právo a obory související*. 2011, č. 5. ISSN 1211-2860.

VOLEVECKÝ, Petr. Phishing a card skiming z pohledu českého trestního práva. *Bezpečnostní teorie a praxe = Security theory and practice / Policejní akademie České republiky*. 2011, zvláštní číslo, díl. 2. ISSN 1801-8211.

internetové zdroje:

DIAMOND, Milton a Ayako UCHIYAMA. Pornography, Rape and Sex Crimes in Japan. International journal of law and psychiatry. 1999, č. 22. ISSN 0160-2527 [online]. [cit. 2013-01-25]. Dostupné z: http://www.hawaii.edu/PCSS/biblio/articles/1961to1999/1999-pornography-rape-sex-crimes-japan.html

Důvodová zpráva k návrhu trestního zákoníku - zák. č. 40/2009 Sb. [online]. [cit. 2013-01-25]. Dostupné z: http://trestnizakonik.cz/navrh/duvodova-zprava.html

Pracovní verze zákona o kybernetické bezpečnosti [online]. [cit. 2013-01-25]. Dostupné z: http://www.nbu.cz/cs/aktuality/599-informace-k-zakonu-o-kyberneticke-bezpecnosti/

Přispěvatelé Wikipedie, Adware [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 18. 02. 2013, 11:28 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Adware&oldid=9752635>

Přispěvatelé Wikipedie, Cybersquatting [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 16. 10. 2012, 04:49 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Cybersquatting&oldid=9164703>

Přispěvatelé Wikipedie, Data (počítače) [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 31. 12. 2012, 17:20 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Data_(po%C4%8D%C3%ADta%C4%8De)&oldid=9505041>

Přispěvatelé Wikipedie, Denial of service [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 25. 02. 2013, 13:57 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Denial_of_service&oldid=9790754>

Přispěvatelé Wikipedie, Keylogger [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 15. 09. 2012, 23:05 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Keylogger&oldid=9028722>

Přispěvatelé Wikipedie, Malware [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 20. 02. 2013, 16:27 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Malware&oldid=9764872>

Přispěvatelé Wikipedie, Počítačový červ [online], Wikipedie: Otevřená encyklopedie, c2012, Datum poslední revize 2. 12. 2012, 16:32 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv&oldid=9375426>

Přispěvatelé Wikipedie, Počítačová síť [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 26. 02. 2013, 11:46 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5&oldid=9795140>

Přispěvatelé Wikipedie, Počítačový virus [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 20. 02. 2013, 15:01 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus&oldid=9764515>

Přispěvatelé Wikipedie, Spyware [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 30. 01. 2013, 08:31 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Spyware&oldid=9661422>

Přispěvatelé Wikipedie, Trojský kůň (program) [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 31. 01. 2013, 23:15 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Trojsk%C3%BD_k%C5%AF%C5%88_(program)&oldid=9669630>

Přispěvatelé Wikipedie, Warez [online], Wikipedie: Otevřená encyklopedie, c2013, Datum poslední revize 1. 03. 2013, 13:28 UTC, [citováno 2. 03. 2013] <http://cs.wikipedia.org/w/index.php?title=Warez&oldid=9808868>

Rozbor "Rozhodování soudů o skutcích posouzených podle § 257a TZ" provedený Institutem kriminologie a sociální prevence v rámci projektového úkolu nazvaného „Výzkum a analýza závažných forem trestné činnosti“ [online]. [cit. 2013-01-25]. Dostupné z: http://www.ok.cz/iksp/docs/kt_grivna.pdf

Věcný záměr zákona o kybernetické bezpečnosti – verze schválená vládou. [online]. [cit. 2013-01-25]. Dostupné z: http://www.nbu.cz/cs/aktuality/808-vecny-zamer-zakona-o-kyberneticke-bezpecnosti---verze-schvalena-vladou-/

judikatura:

nález Ústavního soudu sp.zn. III.ÚS 722/09

stanovisko trestního kolegia Nejvyššího soudu sp.zn. Tpjn 300/2012

usnesení Nejvyššího soudu sp.zn. 7 Tdo 1077/2004-I

usnesení Nejvyššího soudu sp.zn. 5 Tdo 234/2009

usnesení Nejvyššího soudu sp.zn. 8 Tdo 1467/2010

usnesení Nejvyššího soudu sp.zn. 3 Tdo 414/2011

usnesení Nejvyššího soudu sp.zn. 3 Tdo 669/2011

usnesení Nejvyššího soudu sp.zn. 6 Tdo 1401/2012

usnesení Okresního soudu v Jindřichově Hradci sp.zn. 3T 103/2011

Příloha

3 T 103/2011-23

U s n e s e n í

Samosoudce Okresního soudu v Jindřichově Hradci rozhodl dne **17.1.2012** v trestní věci obv. [redacted] pro přečin dle § 183 odst.1,2 trestního zákoníku, - **t a k t o :**

Dle § 314c odst.1 písm.a) trestního řádu z důvodu § 188 odst.1 písm.b) a § 171 odst.1 trestního řádu se trestní věc obv. [redacted], pro přečin porušení tajemství listin a jiných dokumentů uchovávaných v soukromí dle § 183 odst.1,2 trestního zákoníku, jehož se měl dopustit tím, že v přesně nezjištěné době počátkem roku 2011 zpřístupnil choulostivé fotografie poškozené [redacted] a to tak, že nejméně ve třech případech tyto vložil na internetové stránky www.albumfotek.cz a dále je rozeslal na osm e-mailových adres bez souhlasu oprávněné, kdy tyto fotografie byly následně přeposílány mezi příslušníky vojenského útvaru č.6069 v Jindřichově Hradci, kde je poškozená zaměstnána, a to v úmyslu ohrozit její vážnost u spoluobčanů a narušit její rodinné a pracovní vztahy, **p o s t u p u j e k projednání a rozhodnutí Městskému úřadu v Jindřichově Hradci.**

O d ů v o d n ě n í :

Na obv. [redacted] byl u soudu podán návrh na potrestání pro shora popsaný přečin, jehož se měl obviněný dopustit výše popsaným skutkem.

Samosoudce návrh na potrestání přezkoumal ze všech hledisek uvedených v § 181 odst.1 a § 186 trestního řádu a dospěl poté k následujícím závěrům:

Není nejmenších pochyb, že skutek, který je předmětem návrhu na potrestání, obviněný skutečně spáchal, důkazy, jež má soud k dispozici, jsou takového charakteru, že o skutkových tvrzeních návrhu na potrestání skutečně nejsou žádné pochybnosti. Je však třeba zkoumat, zda takto prokazované jednání skutečně naplňuje skutkovou podstatu žalovaného přečinu.

Přečinu dle § 183 odst.1,2 trestního zákoníku se dopustí ten, kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu počítačových dat nebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije. Dle přesvědčení soudu v dané věci o naplnění předmětné skutkové podstaty skutečně nejde. Je zcela evidentní, že obviněný choulostivé fotografie poškozené [redacted] sám pořídil a uchovával je ve svém počítači, odkud jej teprve vložil na zmíněné internetové stránky či rozeslal na další e-mailové adresy. V žádném případě tak není prokázáno, že by obžalovaný neoprávněně porušil tajemství fotografií uchovávaných

v soukromí jiného. Lze jen poznamenat, že návrh na potrestání nedostatečně cituje zákonné znění ustanovení § 183 odst.1 trestního zákoníku, kdy zřejmě nedopatřením nezmiňuje právě zásadní výraz – „jiného“, v důsledku toho pak zjevně dochází v podaném návrhu na potrestání k nesprávné právní úvaze.

Lze tak shrnout, že z výše uvedeného hlediska skutečně nemůže již o navrhovaný přečin, dle přesvědčení soudu nelze prokazovaný skutek podřadit ani pod skutkovou podstatu kteréhokoli jiného přečinu a v žalovaném jednání lze spatřovat maximálně přestupek, nejspíše přestupek proti občanskému soužití dle § 49 odst.1 písm.a) přestupkového zákona.

Orgánem věcně i místně příslušným pro projednání takovéhoto přestupku je pak Městský úřad v Jindřichově Hradci, jemuž je tímto rozhodnutím věc postoupena k dalšímu řízení.

P o u č e n í : **Proti tomuto usnesení může obviněný i státní zástupce podat stížnost do 3 dnů od jeho oznámení u podepsaného soudu.**

V Jindřichově Hradci dne 17.1.2012

Za správnost vyhotovení:
Michaela Tomanová

JUDr. Vlastimil Sítař,v.r.
samosoudce

Abstrakt

Ve své práci, sestávající ze tří základních kapitol, jsem se zaměřila na podání přehledu kybernetické kriminality se zdůrazněním aktuálních kybernetických trestných činů vymezených v současném trestním zákoníku (zák.čís. 40/2009 Sb.). Využívám faktu, že jde o problematiku novou, která - v některých momentech - poskytuje prostor k vyjádření vlastního názoru, byť limitovaného postavením neerudované studentky právnické fakulty.

V úvodu prvé kapitoly uvádím základní pojmy související s kybernetickou kriminalitou, včetně pokusu o vlastní (užší) vymezení pojmu kybernetického trestného činu, dále pokračuji zmíněním mezinárodně právních souvislostí trestního postihu kyberkriminality a jejich dopadem do trestní úpravy v České republice. Prvou kapitolu uzavírá přehled specifických způsobů a technik útoků pachatelů kyberkriminality.

Ve druhé kapitole jsem se pokusila nastínit možné členění kybernetických trestných činů do jednotlivých skupin podle několika různých kritérií - podle způsobu využití informačně-komunikačních technologií pachatelem, podle druhového objektu vymezeného v mezinárodní Úmluvě o kybernetické kriminalitě, podle druhového objektu použitého v českém trestním zákoníku a podle důležitosti kybernetického znaku uvedeného ve skutkové podstatě trestného činu.

Stěžejní je kapitola třetí, která zahrnuje výklad jednotlivých kybernetických trestných činů vymezených v platném trestním zákoníku se zaměřením na aktuální judikatorní problematiku. Trestné činy jsou rozčleněny do tří skupin podle významu kybernetického znaku charakterizujícího jeho skutkovou podstatu. Podrobnější výklad je podáván u kybernetických trestných činů obsahujících kybernetický znak (využití či zasažení informačně-komunikačních technologií) v základní skutkové podstatě. U zbývajících trestných činů, které obsahují kybernetický znak pouze jako zvlášť přitěžující okolnost, je uváděn jen jejich stručný přehled.

Závěr práce obsahuje úvahy *de lege ferenda.*

Internet a computer criminality

Abstract

In my work, which comprises three basic chapters, I have focused on providing an overview of cybernetic criminality with a stress laid on contemporary criminal offences defined in the current Penal Code (Act No. 40/2009 Coll.). I make use of the fact these are new issues that – in some moments – afford an opportunity to formulate one's views even to a non-erudite student of faculty of law.

In the introduction to the first chapter, I have indicated the fundamental concepts relating to cybercrime, inclusive of an attempt at the proper (narrower) definition of the cybernetic criminal offence. I have also mentioned international legal context of criminal sanctions for cybercrime and their impact upon the penal legislation in the Czech Republic. The first chapter is finalized by an overview of specific ways and techniques of attacks by cybercrime offenders.

In the second chapter I have tried to outline the possible division of the cybernetic criminal offences into individual groups according to various different criteria – according to the manner of utilising of information and communication technologies by the perpetrator, to the subject of protected interest defined in the international Convention on Cybercrime, to the subject of protected interest applied in the Czech Penal Code, and to the significance of the cybernetic element stated in the body of the crime.

The third chapter is principal; it comprises the interpretation of the individual cybercriminal acts defined in the current Penal Code, with a focus on the relevant judicial issues. Offences are divided into three groups according to the significance of the cybernetic element characteristic of their bodies. A more detailed construction is provided with cybercrimes containing a cybernetic element (utilisation or affecting of information-communication technologies) in the fundamental body. The rest of

offences that contain cybernetic element only as especially aggravating circumstance, are listed in brief.

The end contains *de lege ferenda* deliberation.

Klíčová slova / key words

kybernetický trestný čin, počítač, internet
cybernetic crime, computer, internet